Cuprins

Notaţii

$a \mid b$	a divide b
$a \sim b$	a este asociat în divizibilitate cu b
(a, b)	cel mai mare divizor comun pentru a şi b
$[a, b]$	cel mai mic multiplu comun pentru a şi b
$\boldsymbol{Z}[i]$	inelul întregilor lui Gauss
$(f_n)_{n\geq 0}$	şirul lui Fibonacci
$p^\alpha \| n$	p^α este cea mai mare putere a lui p care divide n
$ord_p n$	ordinul lui n la p
p_n	al $n-$lea număr prim
$\pi(x)$	numărul numerelor prime $\leq x$, $x > 0$
F_n	număr Fermat
$[x]$	partea întreagă a numărului x
$[a_0; a_1, \ldots, a_n]$	fracţie continuă
$\frac{p_k}{q_k}$	$k-$convergenta unei fracţii continue
$a \equiv b \ (mod\ n)$	a este congruent cu b modulo n
$\bar{a} \ (mod\ n)$	inversul lui a modulo n
ϕ	funcţia lui Euler
$\sigma(n)$	suma divizorilor pozitivi ai lui n
$\tau(n)$	numărul divizorilor pozitivi ai lui n
M_n	număr Mersenne
$ord_n a$	ordinul lui a mod n
$ind_r a \ (mod\ n)$	indicele aritmetic al lui a relativ la r modulo n
$\lambda(n)$	exponent universal minimal al lui n
$\lambda_0(n)$	$\pm 1-$exponent maximal al lui n

$\left(\frac{a}{n}\right)$	simbol Legendre sau Jacobi
$\mathcal{A}$	alfabet de definiţie
$\mathcal{M}$	spaţiul de mesaje
$\mathcal{C}$	spaţiul textului cifrat
$\mathcal{K}$	spaţiul cheilor
E_e	funcţie de criptare
D_d	funcţie de decriptare
DES	Data Encryption Standard
$TDES$	Triplu DES
DLP	problema logaritmului discret
$U(\boldsymbol{Z}_n)$	grupul unităţilor inelului $\boldsymbol{Z}_n$
$log_g b$	logaritmul discret al lui b în baza g
DSA	Digital Standard Algorithm
Ψ_k	cel mai mic număr tare pseudoprim cu primele k numere prime alese ca baze

Capitolul 1

Numere întregi

1.1 Divizibilitate în N

Dacă considerăm două numere naturale a şi b, spunem că a *divide* b şi scriem $a \mid b$ dacă există un număr natural c astfel încât $b = a \cdot c$. În acest caz, a se numeşte divizor al lui b. Este evident că orice număr $n > 1$ are cel puţin doi divizori: pe 1 şi pe el însuşi. Prin *divizor propriu al lui* n înţelegem un divizor diferit de numărul n, iar prin *divizor netrivial al lui* n, un divizor diferit de 1 şi n.

Relaţia $\mid$ definită pe $\boldsymbol{N}$ se numeşte *relaţie de divizibilitate* pe $\boldsymbol{N}$. Se arată uşor că aceasta este o relaţie de ordine pe $\boldsymbol{N}$.

Prin definiţie, un *număr prim* este un număr mai mare decât 1 care nu are alţi divizori în afară de 1 şi el însuşi. Un număr se numeşte *compus* dacă are cel puţin un divizor netrivial.

Lemă 1.1.1 *Orice număr natural, mai mare decât 1, are un divizor prim.*

Demonstraţie. Pentru a demonstra afirmaţia, reducem la absurd şi presupunem că există un număr $n > 1$ care nu are divizori primi. Dacă notăm mulţimea acestor numere cu S, cum ea este nevidă şi $\boldsymbol{N}$ este bine ordonată, există un cel mai mic element în S. Fie acesta n_0. n_0 este atunci un număr compus, deci $n_0 = a \cdot b$, cu $1 < a, b < n_0$. Pentru a nu contrazice alegerea lui n_0, $a \notin S$, adică a are un divizor prim care va fi divizor şi pentru n_0, ceea ce contrazice faptul că $n_0 \in S$. □

Teoremă 1.1.1 *Dacă n este un număr compus, atunci el are cel puţin un divizor prim $\leq \sqrt{n}$.*

Demonstraţie. Cum n este compus, fie $n = ab$, cu $1 < a \leq b < n$. Dacă $a > \sqrt{n}$, atunci $n = ab > n$, fals. Deci, $a \leq \sqrt{n}$. Din lema 1.1.1, a are un divizor prim. Deci, n are un divizor prim $\leq \sqrt{n}$. □

Observaţie 1.1.1 *1) Pentru a verifica dacă un număr este prim e suficient să verificăm dacă are divizori primi $\leq \sqrt{n}$, ţinând cont de forma echivalentă a teoremei anterioare: Dacă numărul n nu are factori primi $\leq \sqrt{n}$, atunci el este prim.*
2) Teorema anterioară poate fi folosită pentru a determina numerele prime $\leq n$ (vezi capitolul 10.1.).

Teoremă 1.1.2 (Teorema împărţirii cu rest) *Pentru două numere naturale m, n cu $n \neq 0$, există numerele naturale q, r astfel încât $m = nq + r$ şi $r < n$. În plus, q şi r sunt unic determinate.*

Demonstraţie. Considerăm mulţimea

$$A = \{s \in \mathbf{N} \mid \exists k \in \mathbf{N},\ m = nk + s\}.$$

Din $m = n \cdot 0 + m$, $m \in A$. Deci, mulţimea A nu este vidă. Atunci, cum $\boldsymbol{N}$ este bine ordonată, există r un cel mai mic element din A. Rezultă, $m = nq + r$, pentru un $q \in \mathbf{N}$. Rămâne să arătăm că $r < n$. Dacă presupunem că $r \geq n$, atunci $r = n + u$, pentru un $u \in \mathbf{N}$ şi $m = nq + r = nq + n + u = n(q + 1) + u$. Astfel, $u \in A$. Dar $r \leq u$. Obţinem $r = u$, de unde $n = 0$, fals. Deci, $r < n$. Astfel, afirmaţia de existenţă din enunţul teoremei este demonstrată. Pentru a arăta că q şi r sunt unice, presupunem $m = nq+r = np+s$ unde $r, s < n$. Dacă $q < p$, atunci $p = q + u$, $u \neq 0$. Obţinem $nq + r = n(q + u) + s = nq + (nu + s)$, adică $r = nu + s$. Dar, cum $n \neq 0$ şi $u \geq 1$, rezultă $nu \geq n$. Atunci, $r = nu + s \geq n + s \geq n$, ceea ce contrazice faptul că $r < n$. Astfel, $p = q$, de unde rezultă imediat $r = s$. □

Numerele q şi r care apar în enunţul teoremei se numesc *câtul* şi *restul* împărţirii lui m la n.

1.2 Relaţia de divizibilitate pe $\boldsymbol{Z}$

Fie numerele întregi a şi b. Spunem că a *divide* b şi scriem $a \mid b$ dacă există un întreg c astfel încât $b = a \cdot c$. Ca şi în cazul relaţiei de divizibilitate definite pe $\boldsymbol{N}$, ea este reflexivă şi tranzitivă, dar nu mai este antisimetrică. De exemplu, $2 \mid -2$ şi $-2 \mid 2$.

Pentru a putea obţine o relaţie de echivalenţă pe $\boldsymbol{Z}$, definim relaţia numită *asociere în divizibilitate*, prin:

$$x \sim y \Leftrightarrow x = \pm y.$$

Definiţie 1.2.1 *Fie a, b numere întregi. Spunem că un număr întreg d este un cel mai mare divizor comun al numerelor a, b dacă:*
1. $d \mid a$ şi $d \mid b$.
2. Pentru orice $d' \mid a$ şi $d' \mid b$, rezultă $d' \mid d$.

Un cel mai mare divizor comun al lui a şi b este unic determinat, mai puţin o asociere în divizibilitate. Putem presupune că acesta este un număr natural. Un astfel de cel mai mare divizor comun este unic determinat şi îl notăm $d = (a, b)$.

Dacă $(a, b) = 1$, spunem că numerele a şi b sunt *prime între ele* sau *relativ prime*.

Propoziţie 1.2.1 *Fie a, b numere întregi şi $d = (a, b)$.*
Atunci, $a = a'd$, $b = b'd$, unde a', b' sunt numere întregi prime între ele.

Din definiţia celui mai mare divizor comun d a două numere a, b, rezultă că $d \mid (a - b)$. Euclid[1] a folosit acest rezultat pentru a determina cel mai mare divizor comun a două numere naturale folosind metoda *scăderii repetate a numărului mic din cel mare*.

[1] Euclid (circa 350 î.e.n.) este autorul celui mai faimos text matematic scris vreodată, *Elemente*, considerat ca fiind cea mai citită carte ştiinţifică din lume. Timp de două milenii, a constituit materialul de bază după care s-a predat matematica. În această carte, Euclid realizează o introducere în geometria plană şi în teoria numerelor. Algoritmul său se găseşte în cartea a VII-a din cele XIII care alcătuiesc lucrarea, iar demonstrarea teoremei care precizează că există o infinitate de numere prime se află în cartea a IX-a. Euclid a predat la faimoasa Academie din Alexandria şi a mai scris cărţi de astronomie, optică, muzică, mecanică.

Algoritmul funcţionează după cum urmează:

Presupunem numerele naturale $a > b$. Fie $a_1 = a,\ b_1 = b$. Pentru fiecare pereche (a_i, b_i) formăm perechea (a_{i+1}, b_{i+1}) unde

$$a_{i+1} = \max\{b_i, a_i - b_i\},\ b_{i+1} = \min\{b_i, a_i - b_i\}.$$

Acest proces formează numere din ce în ce mai mici, deci se va opri. Vom obţine $a_k = b_k$, caz în care vom concluziona că $c.m.m.d.c.(a, b) = a_k = b_k$. Algoritmul funcţionează corect deoarece
$c.m.m.d.c.(a_1, b_1) = c.m.m.d.c.(a_2, b_2) = \ldots = c.m.m.d.c.(a_k, b_k)$.

De exemplu, alegem $a = 34, b = 19$. Algoritmul realizează perechile următoare:
$(a_1, b_1) = (34, 19)$
$(a_2, b_2) = (19, 34 - 19) = (19, 15)$
$(a_3, b_3) = (15, 19 - 15) = (15, 4)$
$(a_4, b_4) = (15 - 4, 4) = (11, 4)$
$(a_5, b_5) = (11 - 4, 4) = (7, 4)$
$(a_6, b_6) = (4, 7 - 4) = (4, 3)$
$(a_7, b_7) = (3, 4 - 3) = (3, 1)$
$(a_8, b_8) = (3 - 1, 1) = (2, 1)$
$(a_9, b_9) = (2 - 1, 1) = (1, 1)$
de unde obţinem $c.m.m.n.c.(34, 19) = c.m.m.d.c.(1, 1) = 1$.

Pentru a fi mai rapid, acest algoritm este de obicei îmbunătăţit înlocuind scăderile repetate cu împărţiri.
Pentru aceasta, reamintim teorema împărţirii cu rest pentru numerele întregi:

Teoremă 1.2.1 (Teorema împărţirii cu rest)
Fie $a, b \in \mathbf{Z}$ cu $b \neq 0$. Atunci, există $q, r \in \mathbf{Z}$ astfel ca $a = bq + r$ unde $0 \leq r < |b|$. În plus, numerele q şi r care verifică aceste proprietăţi sunt unic determinate.

Demonstraţie. Pentru $a = 0$, avem $a = b \cdot 0 + 0$ şi $0 < |b|$. Putem lua astfel, $q = 0,\ r = 0$. Dacă $a > 0, b > 0$, putem aplica teorema 1.1.2. Dacă $a > 0, b < 0$ aplicăm teorema 1.1.2 pentru a şi $-b$. Rezultă astfel $a = (-b)q' + r',\ q',\ r' \in \mathbf{N},\ 0 \leq r' < -b = |b|$. Luând $q = -q'$ şi $r = r'$, rezultă $a = bq + r$ cu $0 \leq r < -b = |b|$.
Dacă $a < 0, b > 0$, aplicăm teorema pentru $-a$ şi b, obţinând
$-a = bq' + r',\ 0 \leq r' < b$. Dacă $r' = 0$, atunci $a = -bq'$ şi alegem $q =$

$-q',\ r=0$. Pentru cazul $0<r'$, avem $a=-bq'-r'=b(-q'-1)+(b-r')$. Alegem $q=-q'-1, r=b-r'$. Cum $0<r'<b$, obţinem $0<r<b=|b|$. Dacă $a<0, b<0$, aplicăm aceeaşi teoremă pentru numerele naturale $-a$ şi $-b$. Avem, $-a=-bq'+r',\ 0\leq r'<-b$. Dacă $r'=0$, alegem $q=q'$ şi $r=0$. Dacă $r'>0$, avem $a=bq'-r'=b(q'+1)+(-b-r')$. Luăm $q=q'+1,\ r=-b-r'$. Cum $0<r'<-b$, rezultă $0<r<-b=|b|$.

Să demonstrăm acum unicitatea numerelor q şi r astfel determinate. Presupunem că $bq+r=bq'+r'$ cu $0\leq r,r'<|b|$. Rezultă $b(q-q')=r'-r$, deci $|b|\cdot|q-q'|=|r-r'|$. Cum r şi r' sunt numere naturale cu $0\leq r,r'<|b|$, avem $|r-r'|<|b|$. Astfel, $|b|\cdot|q-q'|<|b|$, de unde $|q-q'|<1$.
Atunci, $q=q'$ şi apoi $r=r'$. □

Lemă 1.2.1 *Fie $a,b,q,r\in\mathbf{Z}$ astfel ca $a=bq+r$. Atunci, cel mai mare divizor comun al lui a şi b există dacă şi numai dacă cel mai mare divizor comun al lui b şi r există. În plus, avem $(a,b)=(b,r)$.*

Demonstraţie. Presupunem că $d=(a,b)$ există. Din $d\mid a$ şi $d\mid b$, rezultă $d\mid r$. Dacă presupunem că d' este un divizor comun al lui b şi r, rezultă $d'\mid bq+r$, adică $d'\mid a$. Atunci, $d'\mid d$ şi astfel, $d=(b,r)$. Afirmaţia reciprocă se demonstrează la fel. □

Teoremă 1.2.2 (Algoritmul lui Euclid) *Pentru orice două numere întregi există un cel mai mare divizor comun.*

Demonstraţie. Fie a şi b cele două numere întregi. Dacă $b=0$, atunci, $(a,b)=a$. Dacă $b\neq 0$, aplicăm teorema 1.2.1. Există $q_2\in\boldsymbol{Z},\ r_2\in\boldsymbol{N}$ astfel încât

$$a=bq_2+r_2,\quad 0\leq r_2<\mid b\mid .\quad (E_1)$$

Cazul când un rest va fi zero va fi tratat mai târziu.
Dacă $r_2\neq 0$, există $q_3\in\boldsymbol{Z},\ r_3\in\boldsymbol{N}$ astfel încât

$$b=r_2q_3+r_3,\ 0\leq r_3<r_2.\quad (E_2)$$

Dacă $r_3\neq 0$, există $q_4\in\boldsymbol{Z},\ r_4\in\boldsymbol{N}$ astfel încât

$$r_2=r_3q_4+r_4,\quad 0\leq r_4<r_3.\quad (E_3)$$

$$\vdots$$

Dacă $r_k \neq 0$, există $q_{k+1} \in \boldsymbol{Z},\ r_{k+1} \in \boldsymbol{N}$ astfel încât

$$r_{k-1} = r_k q_{k+1} + r_{k+1},\ 0 \leq r_{k+1} < r_k \quad (E_k)$$

$$\vdots$$

Obţinem astfel că resturile verifică relaţiile:

$$| b | > r_2 > r_3 > \ldots > r_k > r_{k+1} \geq 0. \tag{1.1}$$

Dacă ţinem cont că mulţimea numerelor naturale este bine ordonată, există un rang n astfel încât $r_{n+1} = 0$.
Ultimele două relaţii din lanţul de împărţiri cu rest sunt:

$$r_{n-2} = r_{n-1} q_n + r_n \quad (E_{n-1})$$
$$r_{n-1} = r_n q_{n+1} \quad (E_n)$$

Din relaţia (E_n) rezultă $r_n = (r_n, r_{n-1})$.
Din relaţiile $(E_{n-1}), \ldots, (E_k), \ldots, (E_2), (E_1)$, aplicând lema anterioară, obţinem:
$r_n = (r_n, r_{n-1}) = (r_{n-1}, r_{n-2}) = \ldots = (r_2, r_3) = (b, r_2) = (a, b)$. □

Pentru a uniformiza relaţiile $(E_1), (E_2), \ldots, (E_n)$, facem notaţiile $a = r_0$ şi $b = r_1$. Astfel, relaţiile din algoritmul lui Euclid pot fi scrise sub forma:

$$r_{k-1} = r_k q_{k+1} + r_{k+1},\ 1 \leq k \leq n,\ r_{n+1} = 0. \quad (E_k)$$

Dacă privim relaţiile (E_k) ale algoritmului lui Euclid, obţinem

$$\frac{r_{k-1}}{r_k} = q_{k+1} + \frac{r_{k+1}}{r_k}$$

unde $q_{k+1} \in \boldsymbol{Z}$ şi $0 \leq \frac{r_{k+1}}{r_k} < 1$.
De aici putem concluziona că $q_{k+1} = \left[\frac{r_{k-1}}{r_k}\right]$.

Forma în care folosim împărţiri pentru a realiza algoritmul lui Euclid nu este doar mai rapidă Ea are o aplicabilitate mult mai largă decât

varianta scăderilor succesive, putând fi folosită în orice inele euclidiene, de exemplu în inelul *întregilor lui Gauss,* $\boldsymbol{Z}[\mathrm{i}]$ (vezi [9]).

Aplicarea algoritmului pentru numere întregi se reduce la aplicarea acestuia pentru numere naturale. În rolul lui b se poate alege cel mai mic dintre cele două numere.

În anumite situaţii poate fi necesar să cunoaştem numărul de împărţiri din algoritmul lui Euclid.

Pentru a putea da un răspuns referitor la această problemă, trebuie să definim mai întâi şirul lui Fibonacci[2].

Fie $(f_n)_{n\geq 1}$ şirul definit prin $f_1 = f_2 = 1$ şi, $f_{n+1} = f_n + f_{n-1}$, pentru $n \geq 2$.

Folosind inducţia matematică, se demonstrează uşor că, pentru orice $n \geq 3$,

$$f_n > \left(\frac{1+\sqrt{5}}{2}\right)^{n-2}.$$

Cu ajutorul acestui rezultat, putem demonstra următoarea teoremă[3]:

Teoremă 1.2.3 (Lamé) *Numărul de împărţiri din algoritmul lui Euclid pentru $a, b \in \mathbf{N}^*$ cu $a > b$ nu depăşeşte de cinci ori numărul cifrelor din scrierea în baza 10 a lui b.*

Demonstraţie. Considerăm algoritmul lui Euclid pentru numerele a şi b :

$$a = r_0,\ b = r_1,\ r_{k-1} = r_k q_{k+1} + r_{k+1},\ 1 \leq k \leq n,\ r_{n+1} = 0.$$

În acest caz, $q_i \geq 1,\ 2 \leq i \leq n$ şi $q_{n+1} \geq 2$, pentru că altfel, $r_{n-1} = r_n$. Observăm că $r_n \geq 1 = f_2$ şi $r_{n-1} = r_n q_{n+1} \geq 2f_2 = f_3$.

---

[2]Fibonacci, născut în Pisa, era negustor care călătorea în Orientul Mijlociu. Aici a luat contact cu lucrările matematice ale arabilor. În cartea sa *Liber Abaci,* introduce notaţia arabă pentru cifre, efectuează operaţii cu numere fracţionare (a introdus linia de fracţie şi denumirea de *fractus*), studiază, pentru prima dată, sumarea unei serii recurente ai cărei termeni sunt numerele Fibonacci şi introduce, tot pentru prima dată în Europa, numerele negative.

[3]Gabriel Lamé (1795-1870) a fost inginer, absolvent al Şcolii Politehnice din Paris. Principalele sale contribuţii au fost în fizica matematică. A făcut multe descoperiri şi în teoria numerelor, Gauss considerându-l cel mai important matematician francez al timpului său.

Prin inducţie matematică, se arată că $r_{n-i} \geq f_{i+2}$, $0 \leq i \leq n$. În particular, $b = r_1 \geq f_{n+1} > \alpha^{n-1}$, unde $\alpha = \dfrac{1+\sqrt{5}}{2}$.

Presupunem că b are s cifre în scrierea sa în baza 10. Atunci, $b < 10^s$ de unde obţinem $\alpha^{n-1} < 10^s$. Astfel, $(n-1)\lg\alpha < s$. Dacă ţinem cont de relaţia $\dfrac{1}{5} < \lg\alpha$, rezultă în final $n \leq 5s$. □

Considerăm acum problema inversă: Să vedem dacă se pot determina două numere naturale a şi b astfel încât algoritmul lui Euclid aplicat acestora să se realizeze prin n împărţiri.

Teoremă 1.2.4 *Dacă $(f_n)_{n\geq 1}$ este şirul lui Fibonacci, aplicarea algoritmului lui Euclid pentru f_{n+2} şi f_{n+1} necesită exact n împărţiri.*

Demonstraţie. Dacă ţinem cont de modul de definire al acestui şir, obţinem că $f_{n+1} > f_n$, pentru $n \geq 2$. Algoritmul lui Euclid, în acest caz, este dat de relaţiile:
$f_{n+2} = f_{n+1} \cdot 1 + f_n,\ 0 < f_n < f_{n+1}$
$f_{n+1} = f_n \cdot 1 + f_{n-1},\ 0 < f_{n-1} < f_n$
$\vdots$
$f_4 = f_3 \cdot 1 + f_2,\ 0 < f_2 < f_3$
$f_3 = f_2 \cdot 2.$
Observăm că sunt exact n împărţiri. Cum $(f_{n+2}, f_{n+1}) = f_2 = 1$, pentru orice n, rezultă că orice doi termeni consecutivi ai şirului sunt relativ primi. □

Algoritm 1.2.1 (Algoritmul lui Euclid)
INPUT: două numere naturale a, b cu $a \geq b$.
OUTPUT: cel mai mare divizor comun pentru a şi b.
1. *Cât timp $b \neq 0$, execută:*
   1.1. $r \leftarrow a \bmod b,\ a \leftarrow b,\ b \leftarrow r$.
2. *Returnează* a.

Algoritmul lui Euclid poate fi extins pentru a determina pe lângă cel mai mare divizor comun d a două numere a, b şi o scriere a acestuia ca o combinaţie liniară a numerelor iniţiale: $d = au + bv$. Coeficienţii u, v ai combinaţiei se numesc *coeficienţi Bézout* (vezi [9]).

Teoremă 1.2.5 *Fie $a, b \in \mathbf{Z}$ cu $b \neq 0$. Construim, prin recurenţă, vectorii: $(w_k)_{0 \leq k \leq n+1}$, $w_k = (t_k, u_k, v_k)$ din $\mathbf{Z}^3$ astfel:*

$$w_0 = (a, 1, 0),\ w_1 = (b, 0, 1),$$
$$w_{k+1} = w_{k-1} - q_{k+1} w_k,\ 1 \leq k \leq n$$

unde q_{k+1} sunt câturile din algoritmul lui Euclid pentru numerele a, b. Atunci:

$$t_k = r_k = u_k a + v_k b, \quad 0 \leq k \leq n+1 \quad (B_k)$$

Relaţiile B_k poartă numele de *relaţiile lui Bézout.*

Cum algoritmul lui Euclid şi relaţiile lui Bézout se pot realiza simultan, putem cuprinde rezultatele într-un tabel de forma:

k	0	1	2	...	k	...	n	n+1
t_k	a	b	r_2	...	r_k	...	r_n	r_{n+1}
u_k	1	0	u_2	...	u_k	...	u_n	u_{n+1}
v_k	0	1	v_2	...	v_k	...	v_n	v_{n+1}
q_k			q_2	...	q_k	...	q_n	q_{n+1}

De exemplu, pentru $a = 34$ şi $b = 19$, obţinem:

$$(34, 19) = 1 = 34 \cdot (-5) + 19 \cdot 9$$

după cum reiese din tabelul:

k	0	1	2	3	4	5	6
t_k	34	19	15	4	3	1	0
u_k	1	0	1	-1	4	-5	19
v_k	0	1	-1	2	-7	9	-34
q_k			1	1	3	1	3

Acest algoritm poartă numele de *algoritmul extins al lui Euclid* şi este prezentat în continuare:

Algoritm 1.2.2 (Algoritmul extins al lui Euclid)
INPUT: două numere naturale a, b *cu* $a \geq b$.
OUTPUT: $d = (a, b)$ *şi două numere întregi* u, v *cu* $d = au + vb$.
1. Dacă $b = 0$, *atunci* $d \leftarrow a,\ u \leftarrow 1,\ v \leftarrow 0$,
returnează (d, u, v) *şi se opreşte.*
2. $u_1 \leftarrow 1,\ u_2 \leftarrow 0,\ v_1 \leftarrow 0,\ v_2 \leftarrow 1$
3. Cât timp $b > 0$ *execută:*
3.1. $q \leftarrow [a/b],\ r \leftarrow a - qb,\ u \leftarrow u_1 - qu_2,\ v \leftarrow v_1 - bv_2$.
3.2. $a \leftarrow b,\ b \leftarrow r, u_1 \leftarrow u_2,\ u_2 \leftarrow u,\ v_1 \leftarrow v_2,\ v_2 \leftarrow v$.
4. $d \leftarrow a, u \leftarrow u_1,\ v \leftarrow v_1$ *şi returnează* (d, u, v).

1.3 Teorema fundamentală a aritmeticii

Propoziţie 1.3.1 *Orice număr natural* $n \geq 2$ *este produs de numere prime.*

Demonstraţie. Presupunem că mulţimea A a numerelor naturale $n \geq 2$ care nu se scriu ca produs de numere prime este nevidă. Atunci, cum $\boldsymbol{N}$ este bine ordonată, fie n_0 un prim element al lui A. Astfel, $n_0 = ab$ unde $1 < a, b < n_0$ pentru că n_0 nu este prim. Dar, pentru a nu contrazice alegerea lui n_0, $a, b \notin A$. Astfel, a, b sunt fiecare produs de numere prime, de unde şi n_0 este la fel, afirmaţie ce contrazice $n_0 \in A$. □

Observaţie 1.3.1 *Dacă* $n \in \mathbf{Z} \setminus \{-1, 0, 1\}$, *cum* $n = sgn(n) \cdot \mid n \mid$, *obţinem* $n = up_1p_2 \dots p_k$ *unde* $u = \pm 1$, *o unitate şi* $p_1, p_2, \dots, p_k$ *sunt numere prime nu neapărat distincte. Atunci, putem grupa toate numerele prime egale, şi putem scrie:*

$$n = up_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s},$$

cu u *unitate,* $p_1, \dots, p_s$ *numere prime distincte şi* $\alpha_1, \dots, \alpha_s \geq 1$. *În ultima relaţie putem face să apară orice număr prim, chiar dacă acesta nu este divizor pentru* n, *punându-l la puterea 0.*
Astfel, $n = u \prod_{p \in P} p^{\alpha_p}$ *unde* P *este mulţimea numerelor prime şi* $\alpha_p > 0$.

Propoziţie 1.3.2 *Fie a, b, c numere întregi astfel încât $c \mid ab$ şi a, c sunt relativ prime. Atunci, $c \mid b$.*

Demonstraţie.[4] Din $(a, c) = 1$, rezultă că există numerele întregi u, v pentru care $1 = au + cv$. Atunci, $b = b \cdot 1 = (ab)u + (bv)c$. Cum $c \mid ab$, rezultă $c \mid b$. □

Corolar 1.3.1 *Fie p un număr prim şi a, b două numere întregi. Dacă $p \mid ab$, atunci $p \mid a$ sau $p \mid b$.*

Demonstraţie. Dacă $p \nmid a$, cum p este prim, $(a, p) = 1$. Din propoziţia anterioară, rezultă $p \mid b$. □

Definiţie 1.3.1 *Dacă p este un număr prim şi n un număr întreg, vom nota*[5] *$ord_p n = \alpha$ dacă $p^\alpha \mid n$ şi $p^{\alpha+1} \nmid n$, adică p^α este cea mai mare putere a lui p care divide n, unde $\alpha > 0$. Vom numi acest număr natural α, ordinul lui n la p.*

Corolar 1.3.2 *Pentru două numere întregi nenule a, b şi pentru orice număr prim p, are loc relaţia:*

$$ord_p(ab) = ord_p a + ord_p b.$$

Demonstraţie. Fie $ord_p a = n,\ ord_p b = m$.
Atunci, $a = p^n a',\ b = p^m b',\ p \nmid a',\ p \nmid b'$. Rezultă $ab = p^{n+m} a'b'$. Din corolarul 1.3.1, $p \nmid a'b'$. Astfel, $ord_p(ab) = n + m$. □

Teoremă 1.3.1 (Teorema fundamentală a aritmeticii) *Orice număr întreg nenul n, diferit de ± 1, poate fi scris în mod unic (mai puţin ordinea factorilor) ca produs de numere prime de forma $n = u \prod_{p \in P} p^{\alpha_p}$ unde P este mulţimea numerelor prime şi doar un număr finit din numerele naturale α_p sunt nenule.*

Demonstraţie. Produsul se poate scrie de fapt sub forma

$$n = u p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s},$$

[4] Această proprietate a fost demonstrată de Euclid.
[5] mai poate fi întâlnită notaţia $p^\alpha || n$

cu u unitate, $p_1, \ldots, p_s$ numere prime distincte şi $\alpha_1, \ldots, \alpha_s \geq 1$. Din corolarul 1.3.2, pentru un număr prim q,

$$ord_q n = ord_q u + \sum_{p \in P} \alpha_p ord_q p.$$

Cum u este unitate, $ord_q u = 0$. $ord_q p = 1$ dacă $p = q$, altfel $ord_q p = 0$. Rezultă astfel că $\alpha_1 = ord_{p_1} n, \ldots, \alpha_s = ord_{p_s} n \geq 1$. □

Unicitatea descompunerii în factori primi a fost prima dată menţionată de Gauss,[6] în anul 1801. Forma canonică a descompunerii este aceea de a scrie numărul ca produs de numere prime distincte la puterile corespunzătoare, în ordine crescătoare, de exemplu: $12600 = 2^3 \cdot 3^9 \cdot 5^2 \cdot 7$.

Definiţie 1.3.2 *Fie a, b numere întregi. Spunem că m este un cel mai mic multiplu comun al numerelor a, b şi notăm $m = [a, b]$ dacă:*
1. $a \mid m$ şi $b \mid m$.
2. Pentru orice $a \mid m'$ şi $b \mid m'$, rezultă $m \mid m'$.

Propoziţie 1.3.3 *Fie $n = up_1^{\alpha_1} p_2^{\alpha_2} \ldots p_s^{\alpha_s}$ şi $m = vp_1^{\beta_1} p_2^{\beta_2} \ldots p_s^{\beta_s}$, unde u, v sunt unităţi, $p_1, \ldots, p_s$ numere prime distincte şi $\alpha_k,\ \beta_k \geq 0$ pentru $1 \leq k \leq s$. Atunci:*

$$(n, m) = \prod_{1 \leq k \leq s} p_k^{\min\{\alpha_k, \beta_k\}},$$

$$[n, m] = \prod_{1 \leq k \leq s} p_k^{\max\{\alpha_k, \beta_k\}}.$$

Obţinem astfel, $(n, m)[n, m] = \mid n \mid \cdot \mid m \mid$

[6] Karl Friedrich Gauss (1777-1855), fiul unui zidar, a fost unul dintre *copiii minune*. La 3 ani a descoperit o greşeală în statul de plată al tatălui său. La 8 ani a rezolvat rapid problema sumei primelor 100 de numere naturale. În anul 1796 a făcut o mare descoperire în domeniul geometric, ce nu mai progresase din antichitate, arătând că un poligon regulat cu 17 laturi poate fi construit cu rigla şi compasul. În 1799 a dat o demonstraţie riguroasă teoremei fundamentale a algebrei. Gauss a pus bazele teoriei moderne a numerelor prin lucrarea sa *Disquitiones Arithmeticae*, în 1801. Expresia sa favorită, *Matematica este regina ştiinţelor, iar teoria numerelor, regina matematicii*, subliniază pasiunea lui deosebită pentru această ştiinţă. Cele mai importante descoperiri ale sale au fost făcute de matematician în tinereţe, restul vieţii petrecându-l cu rafinarea lor. S-a dovedit că multe rezultate care sunt atribuite unor matematicieni au fost obţinute de Gauss mai înainte, el nepublicând toate studiile făcute. Gauss a fost considerat de matematicienii contemporani lui *Prinţul Matematicii*.

1.4 Numere prime

Numerele prime pot fi privite ca *blocuri* din care se formează numerele naturale, cum orice număr natural ≥ 2 este produs de numere prime.

Una dintre primele probleme studiate referitor la mulţimea numerelor prime a constat în stabilirea cardinalităţii acesteia: este mulţimea infinită sau nu?

Teoremă 1.4.1 (Euclid) *Există o infinitate de numere prime.*

Pentru această teoremă, oferim acum două demonstraţii, urmând ca, în 1.5, să mai fie propusă o alta.

Demonstraţie. 1. (Euclid) Presupunem, prin absurd, că mulţimea numerelor prime este finită. Astfel, presupunem că există doar n numere prime $p_1, p_2, \ldots, p_n$. Numărul $N = p_1 p_2 \ldots p_n + 1$ este mai mare decât 1, deci are un divizor prim. Cum fiecare $p_i \nmid N$, acesta va fi prim, adică $N = p_k$ pentru un $k \in \{1, \ldots, n\}$, ceea ce este absurd. □

Demonstraţie 2. Fie $P_n = n! + 1$, pentru $n \geq 1$. Din lema 1.1.1, pentru fiecare P_n găsim câte un divizor prim p_n. Dacă un $p_n \leq n$, atunci $p_n \mid n!$ şi cum $p_n \mid P_n$, rezultă $p_n = 1$, fals. Deci, $p_n > n$, pentru orice n. Am obţinut astfel că, pentru orice $n \geq 1$, există $p_n > n$ număr prim, ceea ce arată că mulţimea numerelor prime este infinită (Pentru $n = 1$ găsim p_1, apoi alegem $n = p_1$ şi obţinem un număr prim $> p_1$, etc.) □

Demonstraţia lui Euclid furnizează şi o anumită majorare pentru al $n-$ lea număr prim, pe care îl notăm cu p_n. Dacă p este un număr prim diferit de $p_1, p_2, \ldots, p_n$ şi $p \mid p_1 p_2 \ldots p_n + 1$, atunci:

$$p_{n+1} \leq p \leq p_1 p_2 \ldots p_n + 1.$$

Prin inducţie matematică după n, se poate demonstra uşor că

$$p_n < 2^{2^n}.$$

Mulţimea numerelor prime fiind infinită, a fost pusă apoi problema distribuţiei numerelor prime, problemă care poate fi rezumată astfel:

Definim funcţia

$$\pi : \boldsymbol{R}_+ \to \boldsymbol{N}$$

prin $\pi(x)$ este egal cu numărul numerelor prime $\leq x$.
Astfel, $\pi(1) = 0,\ \pi(2) = 1,\ \pi(3) = \pi(4) = 2$, etc.

S-a încercat găsirea unei formule de calcul pentru $\pi(x)$.

Este evident că $\pi(p_n) = n$ şi $p_{\pi(n)} = n$, pentru orice număr prim n.

Atunci, din $p_n < 2^{2^n}$, obţinem $\pi(2^{2^n}) \geq n$, pentru orice număr natural $n \geq 1$.

Propoziţie 1.4.1 *Pentru orice număr real $x > 1$, avem*

$$\pi(x) > \ln(\ln x).$$

Demonstraţie. Fie n cel mai mic număr întreg mai mare ca $\ln(\ln x)$. Atunci $n - 1 \leq \ln(\ln x) < n$, ceea ce este echivalent cu

$$e^{e^{n-1}} \leq x \leq e^{e^n}.$$

Dacă $x \geq e^{e^3}$, atunci $n \geq 4$ şi avem:

$$e^3 > (2,7)^3 = 19,683 > 16 = 2^4.$$

Astfel, $e^{n-1} = e^3 \cdot e^{n-4} > 2^4 \cdot 2^{n-4} = 2^n$. Deci,

$$x \geq e^{e^{n-1}} > e^{2^n} > 2^{2^n}.$$

Atunci,

$$\pi(x) \geq \pi(2^{2^n}) \geq n > \ln(\ln x).$$

Dacă $5 < x < e^{e^3}$, avem $\pi(x) \geq 3 > \ln(\ln x)$.
Dacă $2 \leq x \leq 5$, avem $e^e > e^2 > (2,7)^2 = 7,29 > 5 \geq x$, de unde $\pi(x) \geq 1 > \ln(\ln x)$.
Dacă $1 < x < 2$, avem $\ln(x) < 1$, de unde $\pi(x) = 0 > \ln(\ln x)$. □

O altă relaţie cunoscută apare în propoziţia următoare. Pentru demonstraţie, puteţi consulta, [16].

Propoziţie 1.4.2 *Pentru orice număr întreg pozitiv n, avem:*

$$\pi(x) \geq \frac{\ln x}{2 \ln 2}.$$

Un rezultat de bază legat de numerele prime este prezentat în următoarea teoremă:[7]

Teoremă 1.4.2 (Teorema numerelor prime)

$$\lim_{x\to\infty} \frac{\pi(x)}{\frac{x}{\ln x}} = 1$$

Pentru mai multe informaţii legate de funcţia π, se pot studia *inegalităţile lui Cebîşev*[8] în [5].

Teoremă 1.4.3 *Pentru orice număr natural $n \geq 1$, există cel puţin n numere naturale compuse consecutive.*

Demonstraţie. Considerăm numerele

$$(n+1)!+2,\ (n+1)!+3,\ldots,(n+1)!+n+1.$$

Este evident că pentru $2 \leq k \leq n+1$, $k \mid (n+1)!+k$, deci cele n numere construite iniţial sunt toate compuse. □

Observaţie 1.4.1 *1) Conform teoremei, putem construi 7 numere naturale consecutive compuse începând cu $8!+2 = 40322$. Dar, există 7 numere consecutive compuse mult mai mici, ca de exemplu:* $90, 91, 92, 93, 94, 95, 96$.
2) Teorema arată că distanţa dintre două numere prime este arbitrară.

Un număr prim p se numeşte *pereche,* dacă $p+2$ este tot prim. Nu se ştie dacă mulţimea acestor numere prime pereche este infinită sau nu.

Teoremă 1.4.4 (Dirichlet) *Fie a şi b numere naturale prime între ele. Atunci, progresia aritmetică $an+b$, $n \geq 1$ conţine o infinitate de numere prime.*

[7] Această teoremă a fost enunţată de Gauss în 1793. Demonstraţia ei a fost realizată abia în 1896, independent, de J. Hadamard şi de C.J. de la Vallée Poussin, folosind analiza complexă.

[8] Pafnuti Lvovici Cebîşev (1821-1894) a fost un matematician multilateral, care a îmbinat mereu teoria cu practica. A inventat 40 de mecanisme diferite (maşini de sortat, prăşitoare, mecanisme de vâslire, etc.), preocupare ce l-a condus la crearea unei noi ramuri matematice: teoria celei mai bune aproximări a funcţiilor. Pentru rezultatele deosebite obţinute în teoria numerelor, el a fost numit *învingătorul numerelor prime, care a forţat torentul lor capricios să intre în limitele algebrei.*

Această teoremă este cunoscută sub numele de *Teorema Dirichlet*[9] *pentru numere prime în progresie aritmetică*. Demonstraţia nu este prezentată aici. Ea poate fi studiată în [18] şi anumite cazuri particulare ale ei, în [5].

Una dintre problemele celebre nerezolvate despre numerele prime este următoarea afirmaţie, întâlnită şi sub numele de ***Conjectura lui Goldbach***[10]: *Orice număr par este suma a două numere prime.*

Încheiem acest subcapitol sublinind o problemă actuală de mare importanţă: determinarea de numere prime mari.

Astfel, în anul 1984, Samuel Yates a definit noţiunea de *număr prim titanic* ca fiind un număr prim cu cel puţin 1000 de cifre zecimale. La acea perioadă nu se cunoşteau decât 110 astfel de numere. În prezent, sunt de peste 1000 de ori mai multe. Cum computerele şi criptografia dau mare importanţă căutării de numere prime mari, dimensiunea acestora va continua să crească.

Cele mai mari numere prime cunoscute sunt, de cele mai multe ori, numere prime Mersenne M_p (vezi capitolul 4.4) deoarece testarea primalităţii lor se face descompunând uşor în factori pe $M_p + 1$ (va fi o putere a lui 2). Pe Internet sunt site-uri speciale care păstrează ca bază de date multe numere prime (pot fi şi 6000). Cărţile de specialitate, chiar dacă inserează aceste rezultate, nu vor putea oferi liste de actualitate, ţinând cont de perioada de timp care trece de la conceperea cărţii până la publicarea ei. Ele sunt însă importante pentru că pot furniza, mult mai pe larg, teoria matematică ce a stat la baza obţinerii rezultatelor practice.

---

[9] G.Lejeune Dirichlet (1805-1859) a studiat la Universitatea din Paris, un centru important pe plan mondial în matematică la aceea vreme. El a fost ales de către Gauss să-i succeadă la catedră, la Universitatea din Göttingen. Prin cartea sa de teoria numerelor, *Vorlesung über Zahlentheorie*, el a făcut ca descoperirile lui Gauss să fie accesibile majorităţii matematicienilor. A avut contribuţii importante şi în domeniul analizei matematice iar principiul său binecunoscut, cel *al cutiei*, este folosit în combinatorică şi teoria numerelor.

[10] Cristian Goldbach (1690-1764) a corespondat cu mulţi matematicieni eminenţi ai epocii, cum ar fi Euler şi Bernoulli. Alături de celebrele sale conjecturi, el a avut şi multe contribuţii importante în analiza matematică.

1.5 Numere Fermat

Propoziţie 1.5.1 *Dacă n este un număr natural şi $2^n + 1$ este număr prim, atunci n este o putere a lui 2.*

Demonstraţie. Presupunem că $n = 2^k m$ cu $k \in \boldsymbol{N}$ şi m număr impar. Deci,

$$\begin{aligned} 2^n + 1 &= \left(2^{2^k}\right)^m + 1 \\ &= \left(2^{2^k} + 1\right)\left[\left(2^{2^k}\right)^{m-1} - \left(2^{2^k}\right)^{m-2} + \ldots + 1\right]. \end{aligned}$$

Cum $2^n + 1$ este prim, rezultă că $2^{2^k} + 1 = 1$, ceea ce nu este posibil, sau $2^{2^k} + 1 = 2^n + 1$ de unde $n = 2^k$. □

Definiţie 1.5.1 *Numerele Fermat sunt numerele de forma*

$$F_n = 2^{2^n} + 1,\ n \geq 0.$$

Fermat[11] a afirmat că toate aceste numere sunt prime. Până în prezent se cunosc ca fiind prime doar numerele Fermat:

$$F_0 = 3,\ F_1 = 5,\ F_2 = 17,\ F_3 = 257,\ F_4 = 65537,$$

fără a putea preciza dacă există o infinitate de numere prime Fermat.

În 1732, Euler[12] a arătat că F_5 este compus, numărul fiind divizibil cu 641. Demonstraţia este foarte elegantă, fără multe calcule. Ea se

[11] Pierre de Fermat (1601-1665) era de profesie avocat. A fost probabil cel mai mare matematician amator din istorie. Pe parcursul vieţii nu a publicat nimic din descoperirile sale, dar a corespondat cu mulţi matematicieni contemporani lui despre acestea, de exemplu cu Mersenne. După moartea sa, fiul său a găsit toate notiţele sale şi le-a publicat.

[12] Leonard Euler (1707-1783) a fost fiul unui preot elveţian. Pe lângă teologie, îndrumat de Johann Bernoulli, a studiat şi matematica. La 16 ani şi-a obţinut doctoratul în filozofie. A scris peste 700 de cărţi şi articole, lăsând atâtea rezultate nepublicate încât Academia Imperială din Petersburg nu a sfârşit publicarea acestora decât după 47 de ani de la moartea sa. Cu toate că ultimii 17 ani din viaţă a fost orb, datorită memoriei sale excepţionale, a putut să-şi continue activitatea ştiinţifică până în ultimul moment.

bazează pe relaţia $641 = 5 \cdot 2^7 + 1 = 2^4 + 5^4$. Astfel,

$$\begin{aligned} F_5 &= 2^{2^5} + 1 = 2^{32} + 1 = 2^4 \cdot 2^{28} + 1 \\ &= (641 - 5^4)2^{28} + 1 = 641 \cdot 2^{28} - (5 \cdot 2^7)^4 + 1 \\ &= 641 \cdot 2^{28} - (641 - 1)^4 + 1 \\ &= 641(2^{28} - 641^3 + 4 \cdot 641^2 - 6 \cdot 641 + 4). \end{aligned}$$

Tot el, în 1770, a arătat că orice divizor al lui F_n trebuie să fie de forma $2^{n+1} \cdot k + 1$, cu $k \geq 0$. Acest rezultat a fost îmbunătăţit de Lucas, în 1878, prin teorema:

Teoremă 1.5.1 *Orice divizor prim al lui F_n, dacă există, este de forma $2^{n+2} \cdot k + 1$.*

Spre exemplu, pentru $F_3 = 257$ se caută divizori primi $\leq \sqrt{257} = 16, ...$ de forma $2^5 k + 1 = 32k + 1$. Cum astfel de factori nu există, F_3 este prim. La fel, pentru F_6 divizorii primi căutaţi ar fi de forma $2^8 k + 1 = 256k + 1 \leq \sqrt{F_6}$. După mai multe calcule se obţine $k = 1071$, şi astfel, $274177 \mid F_6$.

Lema următoare stă la baza unei proprietăţi importante a numerelor Fermat. Demonstraţia, folosind metoda inducţiei matematice, este foarte simplă şi o lăsăm ca exerciţiu pentru cititor.

Lemă 1.5.1 *Numerele Fermat verifică relaţia de recurenţă:*

$$F_0 F_1 F_2 \dots F_{n-1} = F_n - 2,$$

pentru $n \geq 1$.

Propoziţie 1.5.2 *Pentru $m, n \in \mathbf{N}$, distincte, numerele Fermat F_m şi F_n sunt prime între ele.*

Demonstraţie. Putem presupune $n > m$.
Din lema anterioară, $F_0 F_1 \dots F_m \dots F_{n-1} = F_n - 2$.
Fie $d = (F_n, F_m)$. Cum $d \mid F_n$ şi $d \mid F_0 F_1 \dots F_{n-1}$, obţinem că $d \mid 2$.
Dar, toate numerele Fermat sunt impare de unde rezultă $d = 1$. □

Folosind acest rezultat putem oferi o altă demonstraţie pentru teorema 1.4.1:
Fiecare număr Fermat este > 1, deci el va avea un factor prim. Fie

p_n un divizor prim al lui F_n, cu $n \in \boldsymbol{N}$. Dar, $(F_n, F_m) = 1$, pentru $m \neq n$. Obţinem astfel că divizorii p_n şi p_m sunt diferiţi. Cum mulţimea divizorilor p_n este infinită, există o infinitate de numere prime.

Descompunerea în factori primi a numerelor Fermat este foarte dificilă, ţinând cont de dimensiunea lor mare. De fapt, s-au factorizat complet doar numerele F_5 până la F_{11}.

Astfel, în 1880, Landry a factorizat F_6, metoda folosită nefiind publicată însă. F_7 a fost factorizat folosind metoda fracţiilor continue în 1975 de către Morrison şi Brillhart. Pentru F_8, în 1981, Brent şi Pollard au folosit o versiune a testului rho. Cu ajutorul metodei curbelor eliptice, în 1988, Brent a factorizat F_{11}.

F_{12} are 5 factori primi cunoscuţi, rămând un factor compus necunoscut de 1187 cifre. Pentru F_{13} situaţia este asemănătoare, ştiindu-se 4 factori primi iar cel compus, rămas de studiat, are 2391 cifre. Chiar dacă nu se cunoaşte factorizarea lui F_{14}, el este număr compus.

În prezent, se ştie că F_n este compus pentru $5 \leq n \leq 32$. Dintre acestea, singurele numere Fermat compuse pentru care nu este cunoscut nici un divizor prim sunt F_{14}, F_{20}, F_{22} şi F_{24}.

Numerele Fermat îşi găsesc importanţa în geometrie prin rezultatul dat de Galois în 1801. Acesta a stabilit că un poligon regulat cu n laturi este construibil cu rigla şi compasul dacă şi numai dacă $n = 2^k p_1 p_2 \dots p_r$, unde $k \in \boldsymbol{N}$ şi $p_1, \dots p_r$ sunt numere prime Fermat distincte.

De asemenea, aceste numere prezintă interes şi în teoria corpurilor finite. Astfel, dacă considerăm un corp K de ordin 2^{2^n}, grupul multiplicativ K^* este o sumă directă de n grupuri ciclice ale căror ordine sunt egale cu $F_0, F_1, \dots, F_{n-1}$. Folosind acest rezultat, pentru a determina ordinul unui element din K^* este necesar să cunoaştem descompunerea în factori primi a numerelor Fermat.

1.6 Ecuaţii liniare diofantice

Cele mai sinple ecuaţii liniare diofantice[13] sunt ecuaţii liniare în două variabile:

$$ax + by = c,\ a, b, c \in \boldsymbol{Z}. \tag{1.2}$$

Aceste ecuaţii pot avea o infinitate de soluţii sau nici una.

Studiului acestora se bazează pe proprietatea celui mai mare divizor comun a două numere de a fi scris ca o combinaţie liniară a numerelor considerate.

Teoremă 1.6.1 *Fie $a, b, c \in \mathbf{Z}$. Ecuaţia $ax + by = c$ are soluţii întregi dacă şi numai dacă $d \mid c$ unde $d = (a, b)$.*

Demonstraţie. Dacă $d = (a, b)$, atunci $d \mid ax + by = c$, pentru orice numere întregi x, y. Reciproc, dacă $d \mid c$, putem scrie $c = dc'$. Din teorema 1.2.5, există $u, v \in \boldsymbol{Z}$, pentru care $au + bv = d$. Obţinem astfel $c = a(uc') + b(vc')$, adică o soluţie particulară a ecuaţiei (1.2) este dată de $x_0 = uc',\ y_0 = vc'$. Mai mult, dacă ecuaţia are o soluţie, (x_0, y_0), ea va avea o infinitate de soluţii şi anume

$$x = x_0 + \frac{b}{d}\, t,\ y = y_0 - \frac{a}{d}\, t,\ t \in \boldsymbol{Z}. \quad \square$$

De exemplu, pentru că avem deja rezultatele algoritmului lui Euclid extins pentru numerele $a = 34,\ b = 19$, să rezolvăm în numere întregi ecuaţia: $34x + 19y = 14$.
Din $(34, 19) = 1 = 34(-5) + 19 \cdot 9$ şi $1 \mid 14$, ecuaţia are soluţii întregi.
O soluţie particulară este $x_0 = (-5)14 = -70,\ y_0 = 9 \cdot 14 = 126$.
Soluţia generală a ecuaţiei este dată de $x = -70 + 19t, y = 126 - 34t$, unde $t \in Z$.

[13] Diofante (aprox. 250 î.e.n.), cunoscut şi ca *tatăl algebrei*, a scris *Aritmetica*, prima carte de algebră cunoscută. Ea conţine, pentru prima dată, notaţii matematice pentru a reprezenta necunoscute şi puteri ale acestora în ecuaţii, în folosire sistematică. Despre viaţa sa, singura sursă de informaţii este o epigramă găsită într-o colecţie numită *Antologia Greacă*: *Diophantus şi-a petrecut 1/6 din viaţă în copilărie, 1/2 în tinereţe, iar 1/7, necăsătorit. După 5 ani de căsătorie, s-a născut un fiu care a murit cu 4 ani înaintea tatălui, având jumătate din vârsta tatălui.* De aici, se poate presupune că Diophantus a trăit 84 de ani.

Demonstraţia teoremei conduce la utilizarea următorului algoritm de rezolvare a ecuaţiilor liniare diofantice de forma (1.2):

Algoritm 1.6.1 (Rezolvarea ecuaţiei liniare diofantice)
INPUT: numerele naturale a, b, c.
OUTPUT: o soluţie particulară a ecuaţiei (1.2), dacă există soluţii întregi.
1. Aplică algoritmul 1.2.2 pentru numerele a, b
2. Dacă $c \bmod d \neq 0$, *returnează* ecuaţia nu are soluţii întregi *şi se opreşte.*
3. $x_0 \leftarrow uc/d,\ y_0 \leftarrow vc/d$
4. Returnează (x_0, y_0)

Exerciţii propuse

1. Fie a, m, n numere naturale. Arătaţi că

$$(a^m - 1, a^n - 1) = a^d - 1,$$

unde $d = (m, n)$.

2. Fie a, b două numere naturale, prime între ele, astfel încât $ab = c^n$. Arătaţi că există $d, e \in \boldsymbol{N}$ astfel ca $a = d^n$ şi $b = e^n$.

3. Arătaţi că restul împărţirii unui pătrat perfect la 16 este tot un pătrat perfect.

4. Dacă suma pătratelor a două numere întregi este divizibilă cu 11, arătaţi că şi suma lor este divizibilă cu 11.

5. Determinaţi $d = (184, 234)$ prin două metode. Aflaţi coeficienţii Bézout corespunzători.

6. Fie a, b, c numere naturale. Arătaţi că sunt verificate următoarele relaţii:

i) $[a, b, c](ab, ac, bc) = abc$.

ii) $([a, b], [a, c], [b, c]) = [(a, b), (a, c), (b, c)]$.

7. Determinaţi numerele naturale care pentru care:

i) $ab = 2400$ şi $(a, b) = 10$.

ii) $a + b = 36 \cdot (a, b)$ şi $[a, b] = 3850$.

8. Fie $n \in \boldsymbol{N}$. Arătaţi că exponentul la care apare numărul prim p în descompunerea lui $n!$ este egal cu:

$$\left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \dots .$$

9. Determinaţi numărul de zerouri din scrierea zecimală a numărului 100!.

10. Demonstraţi că $\dfrac{(m+n)!}{m! \cdot n!} \in \boldsymbol{N}$, pentru orice numere naturale m, n.

11. Fie a şi n două numere naturale. Arătaţi că dacă numărul $a^n - 1$ este prim, atunci $a = 2$ şi n este prim.

12. Să se determine numerele prime care se pot reprezenta atât ca sumă cât şi ca diferenţă de numere prime.

13. Dacă numărul $\overline{ab}$ este prim, atunci $2a - b$ este număr prim.

14. Să se determine numerele naturale n pentru care următoarele numere sunt toate prime:

$$n+1, n+5, n+7, n+11, n+13, n+17, n+23.$$

15. Verificaţi dacă F_4 este număr prim sau nu, folosind rezultatul teoremei 1.5.1.

16. Stabiliţi pentru ce valori ale numărului natural $n \in [50, 80]$, un poligon regulat cu n laturi se poate construi cu rigla şi compasul.

17. Să se rezolve, în numere întregi, ecuaţia $324x - 170y = 19$.

CAPITOLUL 2

Fracţii continue

2.1 Fracţii continue finite

Folosind algoritmul lui Euclid, putem exprima numerele raţionale sub forma unor fracţii continue.

De exemplu, fie $\frac{73}{19}$. Algoritmul lui Euclid aplicat numerelor 73 şi 19 constă în relaţiile:
$73 = 19 \cdot 3 + 16$
$19 = 16 \cdot 1 + 3$
$16 = 3 \cdot 5 + 1$
$3 = 1 \cdot 3.$
Atunci, putem scrie:
$$\frac{73}{19} = 3 + \frac{16}{19} = 3 + \frac{1}{\frac{19}{16}} = 3 + \frac{1}{1 + \frac{3}{16}} = 3 + \frac{1}{1 + \frac{1}{\frac{16}{3}}} = 3 + \frac{1}{1 + \frac{1}{5 + \frac{1}{3}}}.$$

Definiţie 2.1.1 *O fracţie continuă finită este o expresie de forma*

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots + \cfrac{1}{a_{n-1} + \cfrac{1}{a_n}}}}$$

unde $a_0, a_1, \ldots, a_n$ sunt numere reale, cu $a_1, \ldots, a_n$ pozitive şi o vom nota $[a_0 : a_1, a_2, \ldots, a_n]$. Aceste numere poartă numele de câturi parţiale.

Fracţia continuă se numeşte simplă dacă numerele reale $a_0, a_1, \ldots, a_n$ sunt numere întregi.

Teoremă 2.1.1 *Orice fracţie continuă finită simplă reprezintă un număr raţional.*

Demonstraţie. Procedăm prin inducţie matematică după n. Pentru $n = 1$, $[a_0; a_1] = a_0 + \frac{1}{a_1} = \frac{a_0 a_1 + 1}{a_1} \in \boldsymbol{Q}$.
Presupunem că afirmaţia este adevărată pentru fracţii continue, finite, simple de forma $[b_0; b_1, \ldots b_k]$. Arătăm că afirmaţia rămâne adevărată şi pentru $[a_0; a_1, \ldots a_k, a_{k+1}]$.
Avem egalitatea $[a_0; a_1, \ldots a_k, a_{k+1}] = a_0 + \frac{1}{[a_1; a_2, \ldots, a_{k+1}]}$. Din ipoteza de inducţie, $[a_1; a_2, \ldots, a_{k+1}]$ este număr raţional. Astfel, obţinem că şi $[a_0; a_1, \ldots a_k, a_{k+1}]$ este raţional. □

Teoremă 2.1.2 *Orice număr raţional se poate exprima ca o fracţie continuă finită simplă.*

Demonstraţie. Fie $x = \frac{a}{b}$ un număr raţional, unde $a, b \in \boldsymbol{Z}$, $b > 0$. Aplicăm algoritmul lui Euclid pentru $r_0 = a$ şi $r_1 = b$. Obţinem relaţiile:

$r_0 = r_1 q_2 + r_2, \qquad 0 < r_2 < r_1$
$r_1 = r_2 q_3 + r_3, \qquad 0 < r_3 < r_2$
$\vdots$
$r_{n-3} = r_{n-2} q_{n-1} + r_{n-1}, \quad 0 < r_{n-1} < r_{n-2}$
$r_{n-2} = r_{n-1} q_n + r_n, \qquad 0 < r_n < r_{n-1}$
$r_{n-1} = r_n q_{n+1}.$

Astfel,

$$\frac{a}{b} = \frac{r_0}{r_1} = q_2 + \frac{1}{\frac{r_1}{r_2}}$$

$$\frac{r_1}{r_2} = q_3 + \frac{1}{\frac{r_2}{r_3}}$$

$$\begin{aligned}
&\cdots\\
\frac{r_{n-3}}{r_{n-2}} &= q_{n-1} + \frac{1}{\frac{r_{n-2}}{r_{n-1}}}\\
\frac{r_{n-2}}{r_{n-1}} &= q_n + \frac{1}{\frac{r_{n-1}}{r_n}}\\
\frac{r_{n-1}}{r_n} &= q_{n+1}.
\end{aligned}$$

Remarcăm faptul că $q_3, \ldots, q_{n+1} > 0$. Înlocuind relaţiile, una câte una, rezultă:

$$\begin{aligned}
\frac{a}{b} &= q_2 + \frac{1}{q_3 + \frac{1}{\frac{r_2}{r_3}}} = q_2 + \frac{1}{q_3 + \frac{1}{q_4 + \frac{1}{\frac{r_3}{r_4}}}} = \ldots\\
&= [q_2; q_3, \ldots, q_{n+1}]. \quad \square
\end{aligned}$$

Prezentăm în continuare un algoritm de reprezentare a unui număr raţional sub forma unei fracţii continue:

Algoritm 2.1.1
INPUT: a/b, $a, b \in \mathbf{Z}$, $b \neq 0$.
OUTPUT: $[a_0; a_1, \ldots, a_n]$
1. $a_0 \leftarrow [a/b]$, $r \leftarrow a - a_0 b$, $a \leftarrow b$, $b \leftarrow r$.
2. $k \leftarrow 0$
3. *Cât timp* $r \neq 0$, *calculează:*
   3.1. $k \leftarrow k + 1$
   3.2. $a_k \leftarrow [a/b]$, $r \leftarrow a - a_k b$, $a \leftarrow b$, $b \leftarrow r$.
4. *Returnează* $[a_0; a_1, \ldots, a_n]$.

Observaţie 2.1.1 *Scrierea unui număr raţional sub forma unei fracţii continue finite simple nu este unică. Dacă considerăm* $x = [a_0; a_1, \ldots, a_n]$ *fracţia continuă finită simplă corespunzătoare numărului raţional* x, *pentru* $a_n > 1$, *putem scrie* $a_n = (a_n - 1) + 1$, *de unde*
$x = [a_0; a_1, \ldots, a_n - 1, 1]$.

De exemplu, $\frac{73}{19} = [3; 1, 5, 3] = [3; 1, 5, 2, 1]$.

De fapt, se poate arăta că un număr raţional se poate scrie ca o fracţie continuă finită simplă în exact două feluri, unul cu un număr impar de termeni iar altul cu un număr par de termeni.

Să vedem ce se poate obţine dintr-o fracţie continuă finită prin tăierea expresiei la paşi diferiţi.

Definiţie 2.1.2 *Fracţia continuă* $[a_0; a_1, \ldots, a_k]$, *cu* $0 \leq k \leq n$, *se numeşte* $k-$*convergenta fracţiei continue* $[a_0; a_1, \ldots, a_n]$ *şi o notăm* C_k.

Teoremă 2.1.3 *Fie* $a_0, a_1, \ldots, a_n$ *numere reale cu* $a_i > 0$ *pentru* $1 \leq i \leq n$.
Definim recursiv şirurile:

$$\begin{aligned} p_0 &= a_0 & q_0 &= 1 \\ p_1 &= a_0a_1 + 1 & q_1 &= a_1 \\ p_k &= a_kp_{k-1} + p_{k-2} & q_k &= a_kq_{k-1} + q_{k-2}, \quad 2 \leq k \leq n \end{aligned}$$

Atunci, $k-$*convergenta* $C_k = [a_0; a_1, \ldots, a_k] = \frac{p_k}{q_k}$.

Demonstraţie. Arătăm că această afirmaţie este adevărată folosind metoda inducţiei matematice.
Pentru $k = 0$, $C_0 = [a_0] = \frac{a_0}{1} = \frac{p_0}{q_0}$.
Dacă $k = 1$, $C_1 = [a_0; a_1] = a_0 + \frac{1}{a_1} = \frac{a_0a_1 + 1}{a_1} = \frac{p_1}{q_1}$.
Presupunem acum $C_k = [a_0; a_1, \ldots, a_k] = \frac{p_k}{q_k} = \frac{a_kp_{k-1} + p_{k-2}}{a_kq_{k-1} + q_{k-2}}$ pentru $2 < k < n$.
Din modul de definire a fiecărui p_i, q_i, observăm că numere reale p_{k-2}, $p_{k-1}, q_{k-2}, q_{k-1}$ depind doar de câturile parţiale $a_0, a_1, \ldots, a_{k-1}$. Astfel, putem înlocui în ultima relaţie a_k prin $a_k + \frac{1}{a_{k+1}}$. Atunci,

$$C_{k+1} \quad = \quad [a_0; a_1, \ldots, a_k, a_{k+1}] = \left[a_0; a_1, \ldots, a_k + \frac{1}{a_{k+1}}\right]$$

$$\begin{aligned} &= \frac{\left(a_k + \dfrac{1}{a_{k+1}}\right) p_{k-1} + p_{k-2}}{\left(a_k + \dfrac{1}{a_{k+1}}\right) q_{k-1} + q_{k-2}} \\ &= \frac{a_{k+1}\left(a_k p_{k-1} + p_{k-2}\right) + p_{k-1}}{a_{k+1}\left(a_k q_{k-1} + q_{k-2}\right) + q_{k-1}} \\ &= \frac{a_{k+1}p_k + p_{k-1}}{a_{k+1}q_k + q_{k-1}} = \frac{p_{k+1}}{q_{k+1}}. \quad \square \end{aligned}$$

Pentru exemplul nostru, $\frac{73}{19} = [3; 1, 5, 3]$, obţinem:

$p_0 = 3, \qquad q_0 = 1,$
$p_1 = 3 \cdot 1 + 1 = 4, \qquad q_1 = 1,$
$p_2 = 5 \cdot 4 + 3 = 23, \qquad q_2 = 5 \cdot 1 + 1 = 6$
$p_3 = 3 \cdot 23 + 4 = 73, \quad q_3 = 3 \cdot 6 + 1 = 19.$

Convergentele fracţiei continue sunt:

$$C_0 = \frac{p_0}{q_0} = 3, \quad C_1 = \frac{p_1}{q_1} = 4, \quad C_2 = \frac{p_2}{q_2} = \frac{23}{6}, \quad C_3 = \frac{p_3}{q_3} = \frac{73}{19}.$$

Propoziţie 2.1.1 *Fie $k \geq 1$, număr natural şi considerăm $C_k = \frac{p_k}{q_k}$, $k-$convergenta fracţiei continue $[a_0; a_1, \ldots, a_n]$, definită ca mai înainte. Atunci,*

$$p_k q_{k-1} - p_{k-1} q_k = (-1)^{k-1}.$$

Demonstraţie. Prin inducţie matematică după k.

Să verificăm relaţiile pentru exemplul anterior:

$p_1 q_0 - p_0 q_1 = 4 \cdot 1 - 3 \cdot 1 = 1,$
$p_2 q_1 - p_1 q_2 = 23 \cdot 1 - 4 \cdot 6 = -1,$
$p_3 q_2 - p_2 q_3 = 73 \cdot 6 - 23 \cdot 19 = 1.$

Corolar 2.1.1 *Fie C_k, $k-$convergenta fracţiei continue simple $[a_0; a_1, \ldots, a_n]$. Atunci, $(p_k, q_k) = 1$, pentru $1 \leq k \leq n$.*

Corolar 2.1.2 *Fie $C_k = \frac{p_k}{q_k}$ $k-$convergenta fracţiei continue $[a_0; a_1, \ldots, a_n]$. Atunci,*

$$C_k - C_{k-1} = \frac{(-1)^{k-1}}{q_k q_{k-1}}, \quad 1 \leq k \leq n,$$

$$C_k - C_{k-2} = \frac{a_k(-1)^k}{q_k q_{k-2}}, \quad 2 \leq k \leq n.$$

Următoarea teoremă va fi folosită la dezvoltarea fracţiilor continue infinite.

Teoremă 2.1.4 *Fie C_k $k-$convergenta fracţiei continue simple finite $[a_0; a_1, \ldots, a_n]$. Atunci,*

$$C_1 > C_3 > C_5 > \ldots$$
$$C_0 < C_2 < C_4 \ldots.$$

În plus, pentru orice număr impar $2i+1 \leq n$, şi orice număr par $2j \leq n$, $C_{2i+1} > C_{2j}$.

Demonstraţie. Din corolarul 2.1.2, $C_k - C_{k-2} = \frac{a_k(-1)^k}{q_k q_{k-2}}$. Astfel, pentru k impar, $C_k - C_{k-2} < 0$ iar pentru k număr par, $C_k > C_{k-2}$.
La fel, $C_{2m+1} - C_{2m} = \frac{(-1)^{2m}}{q_{2m} q_{2m-1}} > 0$. Deci, $C_{2m+1} > C_{2m}$.
În final, rezultă $C_{2i+1} > C_{2i+2j+1} > C_{2i+2j} > C_{2j}$. □

2.2 Fracţii continue infinite

Teoremă 2.2.1 *Fie $(a_n)_{n\geq 0}$ un şir de numere întregi cu $a_1, a_2, \ldots$ pozitivi şi fie $C_k = [a_0; a_1, \ldots, a_k]$. Atunci, există $\lim_{n\to\infty} C_n = \alpha$.*

Demonstraţie. Folosind teorema 2.1.4, avem

$$C_1 > C_3 > C_5 > \ldots > C_{2n-1} > C_{2n+1} > \ldots$$

$$C_0 < C_2 < C_4 < \ldots < C_{2n-2} < C_{2n} < \ldots$$

şi $C_{2j} < C_{2k+1}$, pentru orice j, k numere naturale. Astfel, obţinem că subşirurile $(C_{2n+1})_{n\geq 0}$ şi $(C_{2n})_{n\geq 0}$ sunt convergente.
Notăm $\lim_{n\to\infty} C_{2n+1} = \alpha_1$ şi $\lim_{n\to\infty} C_{2n} = \alpha_2$.
Din corolarul 2.1.2, $C_{2n+1} - C_{2n} = \frac{1}{q_{2n} q_{2n+1}}$.
Folosind inducţia matematică, se verifică uşor că $q_k \geq k$, pentru orice $k \geq 1$. Atunci, $C_{2n+1} - C_{2n} < \frac{1}{2n(2n+1)}$.

Astfel, $\lim_{n\to\infty}(C_{2n+1} - C_{2n}) = 0$.
De aici, $0 = \lim_{n\to\infty} C_{2n+1} - \lim_{n\to\infty} C_{2n} = \alpha_1 - \alpha_2$. Deci, $\alpha_1 = \alpha_2 = \alpha$. □

Observaţie 2.2.1 *α se numeşte valoarea fracţiei continue simple infinite $[a_0; a_1, a_2, a_3, \ldots]$.*

Teoremă 2.2.2 *Fie $(a_n)_{n\geq 0}$ un şir de numere întregi cu $a_1, a_2, \ldots$ pozitivi. Atunci, $[a_0; a_1, a_2, \ldots]$ este un număr iraţional.*

Demonstraţie. Fie $\alpha = [a_0; a_1, a_2, \ldots]$ şi $C_k = [a_0; a_1, \ldots, a_k] = \frac{p_k}{q_k}$, pentru k natural. Din teorema 2.2.1, $C_{2n} < \alpha < C_{2n+1}$, pentru n natural. Atunci, $0 < \alpha - C_{2n} < C_{2n+1} - C_{2n} = \frac{1}{q_{2n}q_{2n+1}}$. Astfel, $0 < \alpha - \frac{p_{2n}}{q_{2n}} < \frac{1}{q_{2n}q_{2n+1}}$.
Rezultă

$$0 < \alpha q_{2n} - p_{2n} < \frac{1}{q_{2n+1}}. \tag{2.1}$$

Reducem la absurd, şi presupunem că α este raţional. Fie $a, b \in \boldsymbol{Z}$, cu $b \neq 0$, pentru care $\alpha = \frac{a}{b}$.

Înmulţind relaţia (2.1) cu b, obţinem $0 < aq_{2n} - bp_{2n} < \frac{b}{q_{2n+1}}$. Cum $q_{2n+1} \geq 2n+1$, pentru orice n, există n_0 natural astfel ca $q_{2n_0+1} > b$, deci $\frac{b}{q_{2n_0+1}} < 1$.
Am obţinut astfel, că numărul întreg $aq_{2n_0} - bp_{2n_0} \in (0, 1)$, ceea ce fals. Rezultă α număr iraţional. □

Teoremă 2.2.3 *Fie $\alpha = \alpha_0$ un număr iraţional. Definim recursiv şirul de numere întregi $(a_n)_{n\geq 0}$ prin: $a_k = [\alpha_k]$, $\alpha_{k+1} = \frac{1}{\alpha_k - a_k}$, pentru $k \in \mathbf{N}$. Atunci, $\alpha = [a_0; a_1, a_2, \ldots]$.*

Demonstraţie. Arătăm, prin inducţie matematică, că $\alpha_k \notin \boldsymbol{Q}$, pentru orice k.
Pentru $k = 0$, $\alpha = \alpha_0$ este iraţional.
Presupunem α_k iraţional, pentru $k > 0$. Din modul de definire al şirului,

$$\alpha_k = a_k + \frac{1}{\alpha_{k+1}}. \tag{2.2}$$

Dacă α_{k+1} este raţional, rezultă α_k raţional, ceea ce contrazice ipoteza de inducţie. Deci, α_{k+1} este iraţional.

Din $\alpha_k \neq a_k$ şi $a_k < \alpha_k < a_k + 1$, rezultă $0 < \alpha_k - a_k < 1$ şi astfel, $\alpha_{k+1} = \dfrac{1}{\alpha_k - a_k} > 1$, pentru orice k natural.

Deci, $a_{k+1} = [\alpha_{k+1}] \geq 1$, adică $a_1, a_2, \ldots$ sunt pozitive.

Din (2.2),

$$\begin{aligned} \alpha &= \alpha_0 = a_0 + \frac{1}{\alpha_1} = [a_0; \alpha_1] \\ &= a_0 + \cfrac{1}{a_1 + \cfrac{1}{\alpha_2}} = [a_0; a_1, \alpha_2] \\ &= \ldots \\ &= [a_0; a_1, a_2, \ldots, a_k, \alpha_{k+1}]. \end{aligned}$$

Deci,

$$\alpha = [a_0; a_1, a_2 \ldots, a_k, \alpha_{k+1}] = \frac{\alpha_{k+1} p_k + p_{k-1}}{\alpha_{k+1} q_k + q_{k-1}}.$$

Fie $C_j = \dfrac{p_j}{q_j}$, $j-$convergenta fracţiei $[a_0; a_1, a_2, \ldots]$. Atunci, folosind propoziţia 2.1.1,

$$\begin{aligned} \alpha - C_k &= \frac{\alpha_{k+1} p_k + p_{k-1}}{\alpha_{k+1} q_k + q_{k-1}} - \frac{p_k}{q_k} = \frac{-\left(p_k q_{k-1} - p_{k-1} q_k\right)}{\left(\alpha_{k+1} q_k + q_{k-1}\right) q_k} = \\ &= \frac{(-1)^k}{\left(\alpha_{k+1} q_k + q_{k-1}\right) q_k}. \end{aligned}$$

Dar, $\alpha_{k+1} q_k + q_{k-1} > a_{k+1} q_k + q_{k-1} = q_{k+1}$. Obţinem
$\mid \alpha - C_k \mid < \dfrac{1}{q_k q_{k+1}} \leq \dfrac{1}{k(k+1)}$, de unde $\lim\limits_{k \to \infty} C_k = \alpha$. □

Teoremă 2.2.4 *Dacă două fracţii continue simple infinite* $[a_0; a_1, a_2, \ldots]$ *şi* $[b_0; b_1, b_2, \ldots]$ *reprezintă acelaşi număr iraţional, atunci* $a_k = b_k$, *pentru orice* $k \geq 0$.

Demonstraţie. Presupunem $\alpha = [a_0; a_1, a_2, \ldots]$. Atunci,

$$\alpha = \lim_{k \to \infty} [a_0; a_1, \ldots, a_k] = \lim_{k \to \infty} \left(a_0 + \frac{1}{[a_1; a_2, a_3, \ldots, a_k]} \right)$$

$$= \quad a_0 + \frac{1}{\lim\limits_{k\to\infty}[a_1; a_2, a_3, \ldots, a_k]} = a_0 + \frac{1}{[a_1; a_2, a_3, \ldots]}.$$

Din $C_0 = a_0$, $C_1 = a_0 + \frac{1}{a_1}$, rezultă:

$$a_0 < \alpha < a_0 + \frac{1}{a_1},$$

adică $a_0 = [\alpha]$.

Presupunem $[a_0; a_1, a_2, \ldots] = [b_0; b_1, b_2, \ldots]$. Astfel, am obţinut $a_0 = b_0 = [\alpha]$ şi $a_0 + \frac{1}{[a_1; a_2, \ldots]} = b_0 + \frac{1}{[b_1; b_2, \ldots]}$, de unde $[a_1; a_2, \ldots] = [b_1; b_2, \ldots]$.

Presupunem că $a_k = b_k$. Din $[a_{k+1}; a_{k+2}, \ldots] = [b_{k+1}; b_{k+2}, \ldots]$ rezultă $a_{k+1} = b_{k+1}$ şi $a_{k+1} + \frac{1}{[a_{k+2}; a_{k+3}, \ldots]} = b_{k+1} + \frac{1}{[b_{k+2}; b_{k+3}, \ldots]}$. Astfel, $[a_{k+2}; a_{k+3}, \ldots] = [b_{k+2}; b_{k+3}, \ldots]$. Deci, prin inducţie matematică, am arătat că $a_k = b_k$, pentru orice k. □

Să considerăm $\alpha = \sqrt{7}$. Folosind ultimele două teoreme, să găsim fracţia continuă infinită corespunzătoare.

$$a_0 = [\sqrt{7}] = 2, \quad \alpha_1 = \frac{1}{\sqrt{7} - 2} = \frac{\sqrt{7} + 2}{3},$$

$$a_1 = [\alpha_1] = 1, \quad \alpha_2 = \frac{1}{\frac{2 + \sqrt{7}}{3} - 1} = \frac{\sqrt{7} + 1}{2},$$

$$a_2 = [\alpha_2] = 1, \quad \alpha_3 = \frac{1}{\frac{\sqrt{7} + 1}{2} - 1} = \frac{\sqrt{7} + 1}{3},$$

$$a_3 = [\alpha_3] = 1, \quad \alpha_4 = \frac{1}{\frac{\sqrt{7} + 1}{3} - 1} = 2 + \sqrt{7},$$

$$a_4 = [\alpha_4] = 4, \quad \alpha_5 = \frac{1}{2 + \sqrt{7} - 4} = \frac{1}{\sqrt{7} - 2} = \alpha_1.$$

Obţinem astfel, $\sqrt{7} = [2; 1, 1, 1, 4, 1, 1, 1, 4, 1, 1, 1, 4, \ldots]$.

Convergentele unei fracţii continue simple infinite ale unui număr iraţional α sunt cele mai bune aproximări raţionale ale lui α, în sensul

că $\frac{p_k}{q_k}$ e mai aproape de α decât orice alt număr raţional cu numitorul mai mic decât q_k.

Prezentăm aceste teoreme fără demonstraţii. Pentru cei interesaţi, problema este abordată în detaliu în [5] şi [20].

Teoremă 2.2.5 *Fie α un număr iraţional şi $\frac{p_j}{q_j}$ $j-$convergentele fracţiei continue simple infinite corespunzătoare lui α.*

Dacă $r, s \in \mathbf{Z}$, cu $s > 0$, şi $k \in \mathbf{N}$, astfel ca

$$| s\alpha - r | < | q_k\alpha - p_k |,$$

atunci $s \geq q_{k+1}$.

Corolar 2.2.1 *Fie α un număr iraţional şi $\frac{p_j}{q_j}$ $j-$convergentele fracţiei continue simple infinite corespunzătoare lui α.*

Dacă $\frac{r}{s} \in \mathbf{Q}$, cu $r, s \in \mathbf{Z}$, $s > 0$, şi $k \in \mathbf{N}$ astfel încât

$$\left|\alpha - \frac{r}{s}\right| < \left|\alpha - \frac{p_k}{q_k}\right|,$$

atunci $s > q_k$.

De exemplu, fracţia continuă simplă a lui π este

$$[3; 7, 15, 1, 292, 1, 1, 1, 2, 1, 3, \ldots].$$

Convergentele: $3, \frac{22}{7}$, $\frac{333}{106}$, $\frac{355}{113}$, $\frac{103993}{33102}$, sunt cele mai bune aproximări raţionale ale lui π:
$\frac{22}{7}$ este cea mai bună aproximare a lui π cu numitor < 106,
$\frac{335}{113}$ este cea mai bună aproximare a lui π cu numitor < 33102, etc.

De asemenea, se poate arăta că orice suficient de apropiată aproximare raţională a unui număr iraţional trebuie să fie o convergentă a fracţiei corespunzătoare numărului iraţional luat în discuţie.

Teoremă 2.2.6 *Fie α un număr iraţional şi $\frac{r}{s} \in \mathbf{Q}$, cu $r, s \in \mathbf{Z}$, relativ prime, $s > 0$, cu proprietatea că $\left|\alpha - \frac{r}{s}\right| < \frac{1}{2s^2}$. Atunci, $\frac{r}{s}$ este o convergentă a fracţiei continue simple a lui α.*

2.3 Fracţii continue periodice

Definiţie 2.3.1 *O fracţie continuă infinită simplă $[a_0; a_1, a_2, \ldots]$ este periodică dacă există N şi k numere naturale astfel ca $a_n = a_{n+k}$, pentru orice $n \geq N$.*
Vom folosi notaţia $[a_0; a_1, \ldots a_{N-1}, \overline{a_N, a_{N+1}, \ldots, a_{N+k-1}}]$.

De exemplu, $\left[1; 2, \overline{3, 4}\right] = [1; 2, 3, 4, 3, 4, 3, 4, \ldots]$.

Definiţie 2.3.2 *Un număr real α se numeşte iraţional pătratic dacă α este iraţional şi este rădăcină a unui polinom de gradul al doilea cu coeficienţi întregi.*

Următoarele rezultate introductive sunt uşor de demonstrat, drept pentru care vor fi doar enunţate.

Lemă 2.3.1 *Numărul real α este iraţional pătratic dacă şi numai dacă există a, b, c numere întregi, cu $b > 0$, b nu este pătrat perfect şi $c \neq 0$, astfel încât $\alpha = \frac{a + \sqrt{b}}{c}$.*

Lemă 2.3.2 *Dacă α este număr iraţional pătratic şi $r, s, t, u \in \mathbf{Z}$, atunci $\frac{r\alpha + s}{t\alpha + u}$ este număr raţional sau iraţional pătratic.*

Definiţie 2.3.3 *Fie $\alpha = \frac{a + \sqrt{b}}{c}$ un număr iraţional pătratic.*
Atunci, $\alpha' = \frac{a - \sqrt{b}}{c}$ se numeşte conjugatul lui α.

Lemă 2.3.3 *Dacă α este un număr iraţional pătratic, rădăcină a polinomului $AX^2 + BX + C \in \mathbf{Z}[X]$, α' este cealaltă rădăcină a polinomului.*

Lemă 2.3.4 *Fie* $\alpha_1 = \frac{a_1 + \sqrt{b_1}}{c_2}$, $\alpha_2 = \frac{a_2 + \sqrt{b_2}}{c_2}$ *două numere raţionale sau iraţionale pătratice. Atunci:*

$$\begin{aligned}(\alpha_1 + \alpha_2)' &= \alpha_1' + \alpha_2' \\ (\alpha_1 - \alpha_2)' &= \alpha_1' - \alpha_2' \\ (\alpha_1 \cdot \alpha_2)' &= \alpha_1' \cdot \alpha_2' \\ \left(\frac{\alpha_1}{\alpha_2}\right)' &= \frac{\alpha_1'}{\alpha_2'}\end{aligned}$$

Lemă 2.3.5 *Dacă* α *este un număr iraţional pătratic, atunci există numerele întregi* P, Q, d *cu* $Q \neq 0$, $d > 0$ *nu este pătrat perfect,* $Q \mid d - P^2$ *astfel încât* $\alpha = \frac{P + \sqrt{d}}{Q}$.

Demonstraţie. Din lema 2.3.1, există $a, b, c \in \boldsymbol{Z}$ cu $c \neq 0$, $b > 0$ nu este pătrat perfect, pentru care $\alpha = \frac{a + \sqrt{b}}{c}$.

Atunci, putem scrie $\alpha = \frac{a \mid c \mid + \sqrt{bc^2}}{c \mid c \mid}$.

Facem notaţiile: $P = a \mid c \mid$, $Q = c \mid c \mid$ şi $d = bc^2$. Se observă că $P, Q, d \in \boldsymbol{Z}$, $Q \neq 0$, $d > 0$ nu e pătrat perfect.

Din $d - P^2 = bc^2 - a^2c^2 = c^2\left(b - a^2\right) = \pm Q\left(b - a^2\right)$, obţinem $Q \mid d - P^2$. □

Teorema următoare oferă un algoritm de determinare a fracţiei continue simple corespunzătoare unui iraţional pătratic.

Teoremă 2.3.1 *Fie* $\alpha = \frac{P_0 + \sqrt{d}}{Q_0}$ *un iraţional pătratic cu* $Q_0 \neq 0$, $d > 0$ *care nu este pătrat perfect şi* $Q_0 \mid d - P_0^2$.

Definim recursiv, pentru $k \geq 0$*:*

$$\begin{aligned}\alpha_k &= \frac{P_k + \sqrt{d}}{Q_k},\ a_k = [\alpha_k], \\ P_{k+1} &= a_k Q_k - P_k, \\ Q_{k+1} &= \frac{d - P_{k+1}^2}{Q_k}.\end{aligned}$$

Atunci, $\alpha = [a_0; a_1, a_2, \ldots]$.

Demonstraţie. Prin inducţie matematică arătăm că

$$P_k, Q_k \in \boldsymbol{Z},\ Q_k \neq 0,\ Q_k \mid d - P_k^2, \tag{2.3}$$

pentru $k \geq 0$.

Pentru $k = 0$, din ipoteza teoremei, relaţiile sunt verificate.

Presupunem că (2.3) este adevărată pentru k şi arătăm că ea rămâne adevărată pentru $k+1$.

$P_{k+1} = a_k Q_k - P_k$, deci $P_{k+1} \in \boldsymbol{Z}$.

$Q_{k+1} = \dfrac{d - P_{k+1}^2}{Q_k} = \dfrac{d - (a_k Q_k - P_k)^2}{Q_k} = \dfrac{d - P_k^2}{Q_k} + 2a_k P_k - a_k^2 Q_k \in \boldsymbol{Z}$

cum, din ipoteza de inducţie, $\dfrac{d - P_k^2}{Q_k} \in \boldsymbol{Z}$.

$d \neq P_{k+1}^2$, nefiind pătrat perfect. Atunci $Q_{k+1} = \dfrac{d - P_{k+1}^2}{Q_k} \neq 0$.

Din $Q_k = \dfrac{d - P_{k+1}^2}{Q_{k+1}} \in \boldsymbol{Z}$, rezultă $Q_{k+1} \mid d - P_{k+1}^2$.

Demonstrăm acum că $a_0, a_1, a_2, \ldots$ sunt câturile parţiale ale fracţiei continue corespunzătoare lui α. Pentru aceasta, folosim teorema 2.2.3 şi arătăm că $\alpha_{k+1} = \dfrac{1}{\alpha_k - a_k}$, pentru orice $k \geq 0$.

$$\begin{aligned}
\alpha_k - a_k &= \frac{P_k + \sqrt{d}}{Q_k} - a_k = \frac{\sqrt{d} - (a_k Q_k - P_k)}{Q_k} \\
&= \frac{\sqrt{d} - P_{k+1}}{Q_k} = \frac{\left(\sqrt{d} - P_{k+1}\right)\left(\sqrt{d} + P_{k+1}\right)}{Q_k\left(\sqrt{d} + P_{k+1}\right)} \\
&= \frac{Q_k Q_{k+1}}{Q_k\left(\sqrt{d} + P_{k+1}\right)} = \frac{Q_{k+1}}{\sqrt{d} + P_{k+1}} = \frac{1}{\alpha_{k+1}}. \quad \square
\end{aligned}$$

De exemplu, pentru $\alpha = \dfrac{2 + \sqrt{7}}{3}$ iraţional pătratic avem $P_0 = 2,\ d = 7,\ Q_0 = 3$. Atunci,

$$\begin{array}{cc}
a_0 = [\alpha] = 1 & a_1 = [\alpha_1] = 1 \\
P_1 = 1 \cdot 3 - 2 = 1 & P_2 = 1 \cdot 2 - 1 = 1
\end{array}$$

$$Q_1 = \frac{7-1}{3} = 2 \quad Q_2 = \frac{7-1}{2} = 3$$
$$\alpha_1 = \frac{1+\sqrt{7}}{2} \qquad \alpha_2 = \frac{1+\sqrt{7}}{3}$$

$$a_2 = [\alpha_2] = 1 \qquad a_3 = [\alpha_3] = 4$$
$$P_3 = 1 \cdot 3 - 1 = 2 \quad P_4 = 4 \cdot 1 - 2 = 2$$
$$Q_3 = \frac{7-4}{3} = 1 \qquad Q_4 = \frac{7-4}{1} = 3$$
$$\alpha_3 = 2 + \sqrt{7} \quad \alpha_4 = \frac{2+\sqrt{7}}{3} = \alpha_0.$$

Astfel, $\alpha = \dfrac{2+\sqrt{7}}{3} = \left[\overline{1; 1, 1, 4}\right]$.

Teoremă 2.3.2 (Lagrange) *Fracţiile continue simple infinite corespunzătoare pentru numere iraţionale sunt periodice dacă şi numai dacă numerele sunt iraţionale pătratice.*

Demonstraţie. Fie $\alpha = [a_0; a_1 \ldots, a_{N-1}, \overline{a_N, a_{N+1}, \ldots a_{N+k}}]$.
Notăm $\beta = [\overline{a_N; a_{N+1}, \ldots a_{N+k}}]$. Atunci, $\beta = [a_N; a_{N+1}, \ldots a_{N+k}, \beta]$.
Folosind rezultatul teoremei 2.1.3, $\beta = \dfrac{\beta p_k + p_{k-1}}{\beta q_k + q_{k-1}}$ unde $\dfrac{p_{k-1}}{q_{k-1}}$ şi $\dfrac{p_k}{q_k}$ sunt convergente ale fracţiei $[a_N; a_{N+1}, \ldots, a_{N+k}]$.
Cum fracţia continuă simplă a lui β este infinită, β este iraţional.
Din relaţia anterioară, $q_k\beta^2 + (q_{k-1} - p_k)\beta - p_{k-1} = 0$. Deci, β este iraţional pătratic.
Se observă că $\alpha = [a_0; a_1, \ldots, a_{N-1}, \beta]$. De aici,
$\alpha = \dfrac{\beta p_{N-1} + p_{N-2}}{\beta q_{N-1} + q_{N-2}}$ unde $\dfrac{p_{N-1}}{q_{N-1}}$ şi $\dfrac{p_{N-2}}{q_{N-2}}$ sunt convergentele fracţiei $[a_0; a_1, \ldots, a_{N-1}]$. Din lema 2.3.2, cum β este iraţional pătratic, rezultă α raţional sau iraţional pătratic. Fracţia continuă corespunzătoare lui α fiind infinită, α nu este raţional. Deci, α este iraţional pătratic.

Reciproc, considerăm acum α iraţional pătratic. Din lema 2.3.5, $\alpha = \dfrac{P_0 + \sqrt{d}}{Q_0}$, iar din teorema 2.3.1, $\alpha = [a_0; a_1, a_2, \ldots]$ unde $\alpha_k = \dfrac{P_k + \sqrt{d}}{Q_k}$, $a_k = [\alpha_k]$, $P_{k+1} = a_k Q_k - P_k$ şi $Q_{k+1} = \dfrac{d - P_{k+1}^2}{Q_k}$.

Cum $\alpha = [a_0; a_1, a_2, \ldots, \alpha_k]$, din teorema 2.2.3, rezultă
$\alpha = \dfrac{\alpha_k p_{k-1} + p_{k-2}}{\alpha_k q_{k-1} + q_{k-2}}$.
Prin conjugare, obţinem $\alpha' = \dfrac{\alpha'_k p_{k-1} + p_{k-2}}{\alpha'_k q_{k-1} + q_{k-2}}$ de unde,

$$\alpha'_k = \frac{-q_{k-2}}{q_{k-1}} \cdot \frac{\alpha' - \dfrac{p_{k-2}}{q_{k-2}}}{\alpha' - \dfrac{p_{k-1}}{q_{k-1}}}.$$

Convergentele $\dfrac{p_{k-1}}{q_{k-1}}$ şi $\dfrac{p_{k-2}}{q_{k-2}}$ tind la α, pentru $k \to \infty$.
Astfel, $\lim\limits_{k\to\infty} \dfrac{\alpha' - \dfrac{p_{k-2}}{q_{k-2}}}{\alpha' - \dfrac{p_{k-1}}{q_{k-1}}} = 1$.

Deci, există N natural astfel încât $\alpha'_k < 0$ pentru $k \geq N$. Cum $\alpha_k > 0$, pentru orice $k \geq 1$, rezultă
$\alpha_k - \alpha'_k = \dfrac{P_k + \sqrt{d}}{Q_k} - \dfrac{P_k - \sqrt{d}}{Q_k} = \dfrac{2\sqrt{d}}{Q_k} > 0$ pentru $k \geq N$. Astfel, $Q_k > 0$, pentru $k \geq N$.
Din $Q_k Q_{k+1} = d - P_{k+1}^2$, pentru $k \geq N$, obţinem:

$$Q_k \leq Q_k Q_{k+1} \leq d$$

şi

$$P_{k+1}^2 \leq P_{k+1}^2 + Q_k Q_{k+1} = d.$$

Deci, pentru $k \geq N$ avem:

$$-\sqrt{d} < P_{k+1} < \sqrt{d}, \quad 0 < Q_k \leq d.$$

Astfel, cum P_k, Q_k sunt numere întregi, există un număr finit de valori posibile pentru perechile (P_k, Q_k) cu $k \geq N$. Dar, $k \geq N$ ia o infinitate de valori şi astfel, există $i, j \in \boldsymbol{N}$, $i < j$, cu $P_i = P_j$ şi $Q_i = Q_j$. Din modul în care sunt definite, rezultă $\alpha_i = \alpha_j$. Atunci, $a_i = a_j$, $a_{i+1} = a_{j+1}, \ldots$. Obţinem că

$$\begin{aligned} \alpha &= [a_0; a_1, \ldots, a_{i-1}, a_i, a_{i+1}, \ldots, a_{j-1}, a_i, a_{i+1}, \ldots, a_{j-1}, \ldots] \\ &= [a_0; a_1, \ldots, a_{i-1}, \overline{a_i, a_{i+1}, \ldots, a_{j-1}}] \end{aligned}$$

este o fracţie continuă simplă periodică. □

Definiţie 2.3.4 *Fracţia continuă* $[a_0; a_1, a_2, \ldots]$ *se numeşte pur periodică dacă există* N, *număr natural, astfel încât* $a_k = a_{N+k}$, *pentru orice* $k \geq 0$, *adică*

$$[a_0; a_1, a_2, \ldots] = [\overline{a_0; a_1, a_2, \ldots, a_{N-1}}].$$

De exemplu, $\alpha = \dfrac{2+\sqrt{7}}{3} = [\overline{1; 1, 1, 4}]$ este o fracţie pur periodică.

Definiţie 2.3.5 *Un număr iraţional pătratic* α *se numeşte redus dacă* $\alpha > 1$ *şi* $-1 < \alpha' < 0$.

Teoremă 2.3.3 *Fracţia continuă simplă a unui număr iraţional pătratic* α *este pur periodică dacă şi numai dacă* α *este redus.*
Mai mult, dacă α *este redus şi* $\alpha = [\overline{a_0; a_1, a_2, \ldots, a_n}]$, *atunci fracţia continuă corespunzătoare lui* $-\dfrac{1}{\alpha'}$ *este* $[\overline{a_n; a_{n-1}, \ldots, a_1, a_0}]$.

Demonstraţie. Presupunem mai întâi că α este un număr iraţional pătratic redus. Din teorema 2.2.3, $\alpha = [a_0; a_1, a_2, \ldots]$ unde $\alpha = \alpha_0$, $a_k = [\alpha_k]$, $\alpha_{k+1} = \dfrac{1}{\alpha_k - a_k}$, pentru $k \geq 0$.
Atunci, $\dfrac{1}{\alpha_{k+1}} = \alpha_k - a_k$, şi, prin conjugare, $\dfrac{1}{\alpha'_{k+1}} = \alpha'_k - a_k$.

Arătăm, prin inducţie matematică, că $-1 < \alpha'_k < 0$, pentru orice $k \geq 0$. Cum α_0 este redus, afirmaţia este verificată pentru $k = 0$.
Presupunem că $-1 < \alpha'_k < 0$. Pentru că $\alpha_0 > 1$, avem $a_0 \geq 1$. De aici, $a_k \geq 1$, pentru $k \geq 0$.
Atunci $\dfrac{1}{\alpha'_{k+1}} = \alpha'_k - a_k < -1$ deci, $-1 < \alpha'_{k+1} < 0$.

Să observăm acum că, din $\alpha'_k = \dfrac{1}{\alpha'_{k+1}} + a_k$ şi $-1 < \alpha'_k < 0$, avem $-1 < a_k + \dfrac{1}{\alpha'_{k+1}}$. Atunci, $-1 - \dfrac{1}{\alpha'_{k+1}} < a_k < -\dfrac{1}{\alpha'_{k+1}}$, adică $a_k = \left[-\dfrac{1}{\alpha'_{k+1}}\right]$.

Conform teoremei 2.3.2, α fiind iraţional pătratic, există i, j numere întregi, cu $i < j$ astfel încât $\alpha_i = \alpha_j$, adică $-\dfrac{1}{\alpha'_i} = -\dfrac{1}{\alpha'_j}$. Deci, $a_{i-1} =$

a_{j-1}. Continuând, obţinem $\alpha_{j-2} = \alpha_{i-2}$, $\alpha_{j-3} = \alpha_{i-3}, \ldots \alpha_{j-i} = \alpha_0$. Rezultă astfel,

$$\begin{aligned} \alpha &= \alpha_0 = [a_0; a_1, \ldots, a_{j-i-1}, \alpha_{j-i}] \\ &= [a_0; a_1, \ldots, a_{j-i-1}, \alpha_0] = [\overline{a_0; a_1, \ldots a_{j-i-1}}] \end{aligned}$$

este fracţie continuă pur periodică.

Reciproc, presupunem acum α iraţional pătratic şi fracţia continuă $\alpha = [\overline{a_0; a_1, \ldots, a_k}]$ este pur periodică.

Din $\alpha = [a_0; a_1, \ldots, a_k, \alpha]$, rezultă $\alpha = \dfrac{\alpha p_k + p_{k-1}}{\alpha q_k + q_{k-1}}$ unde $\dfrac{p_{k-1}}{q_{k-1}}$ şi $\dfrac{p_k}{q_k}$ sunt convergentele fracţiei continue α. Obţinem:

$$q_k \alpha^2 + (q_{k-1} - p_k)\, \alpha - p_{k-1} = 0. \tag{2.4}$$

Fie β un iraţional pătratic astfel ca $\beta = [\overline{a_k; a_{k-1}, \ldots, a_1, a_0}]$. Atunci, $\beta = [a_k; a_{k-1}, \ldots, a_1, a_0, \beta]$.

La fel ca mai înainte, obţinem $\beta = \dfrac{\beta p'_k + p'_{k-1}}{\beta q'_k + q'_{k-1}}$ unde $\dfrac{p'_{k-1}}{q'_{k-1}}$ şi $\dfrac{p'_k}{q'_k}$ sunt convergentele fracţiei continue β.

Observăm că

$$\frac{p_k}{p_{k-1}} = [a_k; a_{k-1}, \ldots, a_1, a_0] = \frac{p'_k}{q'_k}$$

şi

$$\frac{q_k}{q_{k-1}} = [a_k; a_{k-1}, \ldots, a_2, a_1] = \frac{p'_{k-1}}{q'_{k-1}}.$$

Conform corolarului 2.1.1, convergentele $\dfrac{p_{k-1}}{q_{k-1}}$, $\dfrac{p_k}{q_k}$, $\dfrac{p'_{k-1}}{q'_{k-1}}$, $\dfrac{p'_k}{q'_k}$ sunt fracţii ireductibile.

Astfel, $p'_k = p_k$, $q'_k = p_{k-1}$, $p'_{k-1} = q_k$, $q'_{k-1} = q_{k-1}$.

Înlocuind, rezultă

$\beta = \dfrac{\beta p_k + q_k}{\beta p_{k-1} + q_{k-1}}$ adică $p_{k-1}\beta^2 + (q_{k-1} - p_k)\, \beta - q_k = 0$, relaţie pe care o putem scrie sub forma

$$q_k \left(-\frac{1}{\beta}\right)^2 + (q_{k-1} - p_k) \left(-\frac{1}{\beta}\right) - p_{k-1} = 0. \tag{2.5}$$

Din (2.4) şi (2.5), rezultă că cele două rădăcini ale ecuaţiei

$$q_k x^2 + (q_{k-1} - p_k)\, x - p_{k-1} = 0$$

sunt α şi $-\frac{1}{\beta}$. Deci, $\alpha' = -\frac{1}{\beta}$.
Cum $\beta = [\overline{a_k; a_{k-1}, \ldots, a_1, a_0}]$, $\beta > 1$. De aici,

$$-1 < \alpha' = -\frac{1}{\beta} < 0.$$

Astfel, am demonstrat că α este redus.
Din $\beta = -\frac{1}{\alpha'}$, rezultă $-\frac{1}{\alpha'} = [\overline{a_k; a_{k-1}, \ldots, a_1, a_0}]$. □

Încheiem capitolul precizând forma fracţiilor continue simple periodice pentru numere iraţionale pătratice de forma $\sqrt{d}$ cu d număr natural, care nu este pătrat perfect. Observăm că $\sqrt{d}$ nu este redus, cum conjugatul său $-\sqrt{d} \notin (-1, 0)$.
Dar, din $\left\lfloor \sqrt{d} \right\rfloor - \sqrt{d} \in (-1, 0)$, găsim că $\left\lfloor \sqrt{d} \right\rfloor + \sqrt{d}$ este iraţional pătratic redus.

Conform teoremei 2.3.3, fracţia continuă a lui $\left\lfloor \sqrt{d} \right\rfloor + \sqrt{d}$ este pur periodică. Primul cât parţial al acestei fracţii periodice este $\left\lfloor \left\lfloor \sqrt{d} \right\rfloor + \sqrt{d} \right\rfloor = 2\left\lfloor \sqrt{d} \right\rfloor = 2a_0$, unde $a_0 = \left\lfloor \sqrt{d} \right\rfloor$. Putem scrie:

$$\begin{aligned} \left\lfloor \sqrt{d} \right\rfloor + \sqrt{d} &= [\overline{2a_0; a_1, a_2, \ldots, a_n}] = \\ &= [2a_0; a_1, a_2, \ldots, a_n, \overline{2a_0, a_1, a_2, \ldots, a_n}]. \end{aligned}$$

De aici, scăzând a_0, rezultă:

$$\begin{aligned} \sqrt{d} &= [a_0; a_1, a_2, \ldots, a_n, 2a_0, a_1, a_2, \ldots, a_n, 2a_0, \ldots] = \\ &= [a_0; \overline{a_1, a_2, \ldots, a_n, 2a_0}]. \end{aligned}$$

Tot din teorema 2.3.3, ştim că fracţia continuă pentru $-\frac{1}{\left\lfloor \sqrt{d} \right\rfloor - \sqrt{d}} = \frac{1}{\sqrt{d} - \left\lfloor \sqrt{d} \right\rfloor}$ este $[\overline{a_n; a_{n-1}, \ldots, a_1, 2a_0}]$.

Observăm că $\sqrt{d} - \left[\sqrt{d}\right] = \left[0; \overline{a_1, a_2, \ldots, a_n, 2a_0}\right]$. De aici,
$\dfrac{1}{\sqrt{d} - \left[\sqrt{d}\right]} = \left[\overline{a_1; a_2, \ldots, a_n, 2a_0}\right]$.
Din teorema 2.2.4, reprezentarea unui număr iraţional sub forma unei fracţii continue simple infinite este unică. Aplicăm acest rezultat pentru $\dfrac{1}{\sqrt{d} - \left[\sqrt{d}\right]}$ şi obţinem $a_1 = a_n$, $a_2 = a_{n-1}, \ldots, a_n = a_1$.

Deci, partea periodică a fracţiei continue pentru $\sqrt{d}$ este simetrică de la primul termen până la penultimul. Astfel,
$\sqrt{d} = \left[a_0; \overline{a_1, a_2, \ldots, a_2, a_1, 2a_0}\right]$.

Spre exemplu, se poate verifica prin calcul $\sqrt{23} = \left[4; \overline{1, 3, 1, 8}\right]$.

Putem rezuma cele prezentate pentru a descrie un algoritm de dezvoltare a lui $\sqrt{d}$ în fracţie continuă unde $d \in \boldsymbol{N}$, nu este pătrat perfect.

Considerăm şirurile: $(a_k)_{k\geq 0}$, $(P_k)_{k\geq 0}$, $(Q_k)_{k\geq 0}$ definite ca în teorema 2.3.1:

$$\begin{aligned} a_0 = [\sqrt{d}],\ P_0 = 0,\ Q_0 = 1,\\ P_{k+1} = a_k Q_k - P_k,\\ Q_{k+1} = \frac{d - P_{k+1}^2}{Q_k},\\ a_{k+1} = \left[\frac{a_0 + P_{k+1}}{Q_{k+1}}\right], \end{aligned}$$

pentru $k \geq 0$.

Vom calcula termenii P_k, Q_k până când obţinem primul indice t pentru care $P_{t+1} = P_1$ şi $Q_{t+1} = Q_1$.

În [5], se precizează că pentru t număr par, $n = \dfrac{t}{2}$ este cel mai mic indice pentru care $P_{n+1} = P_n$, iar dacă t este impar, $n = \dfrac{t-1}{2}$ este cel mai mic indice pentru care $Q_{n+1} = Q_n$.

Ţinând cont de această observaţie, vom calcula termenii şirurilor până când $P_{n+1} = P_n$ sau $Q_{n+1} = Q_n$.

Atunci:

i) Dacă $P_{n+1} = P_n$, $\sqrt{d} = [a_0; \overline{a_1, \ldots, a_{n-1}, a_n, a_{n-1}, \ldots, a_1, 2a_0}]$, deci numărul termenilor din perioada minimă este par;

ii) Dacă $Q_{n+1} = Q_n$, $\sqrt{d} = [a_0; \overline{a_1, \ldots, a_{n-1}, a_n, a_n, a_{n-1}, \ldots, a_1, 2a_0}]$, deci lungimea perioadei minime este impară.

De exemplu, pentru $d = 809$, vom obţine:

$a_0 = \left[\sqrt{809}\right] = 28,\ P_0 = 0,\ Q_0 = 1$

$$P_1 = 28 \cdot 1 - 0 = 28 \quad Q_1 = \frac{809 - 28^2}{1} = 25 \quad a_1 = \left[\frac{28 + 28}{25}\right] = 2$$

$$P_2 = 2 \cdot 25 - 28 = 22 \quad Q_2 = \frac{809 - 22^2}{25} = 13 \quad a_2 = \left[\frac{28 + 22}{13}\right] = 3$$

$$P_3 = 3 \cdot 13 - 22 = 17 \quad Q_3 = \frac{809 - 17^2}{13} = 40 \quad a_3 = \left[\frac{28 + 17}{40}\right] = 1$$

$$P_4 = 1 \cdot 40 - 17 = 23 \quad Q_4 = \frac{809 - 23^2}{40} = 7 \quad a_4 = \left[\frac{28 + 23}{7}\right] = 7$$

$$P_5 = 7 \cdot 7 - 23 = 26 \quad Q_5 = \frac{809 - 26^2}{7} = 19 \quad a_5 = \left[\frac{28 + 26}{19}\right] = 2$$

$$P_6 = 2 \cdot 19 - 26 = 12 \quad Q_6 = \frac{809 - 12^2}{19} = 35 \quad a_6 = \left[\frac{28 + 12}{35}\right] = 1$$

$$P_7 = 1 \cdot 35 - 12 = 23 \quad Q_7 = \frac{809 - 23^2}{35} = 8 \quad a_7 = \left[\frac{28 + 23}{8}\right] = 6$$

$$P_8 = 6 \cdot 8 - 23 = 25 \quad Q_8 = \frac{809 - 25^2}{8} = 23 \quad a_8 = \left[\frac{28 + 25}{23}\right] = 2$$

$$P_9 = 2 \cdot 23 - 25 = 21 \quad Q_9 = \frac{809 - 21^2}{23} = 16 \quad a_9 = \left[\frac{28 + 21}{16}\right] = 3$$

$$P_{10} = 3 \cdot 16 - 21 = 27 \quad Q_{10} = \frac{809 - 27^2}{16} = 5 \quad a_{10} = \left[\frac{28 + 27}{5}\right] = 11$$

$$P_{11} = 11 \cdot 5 - 27 = 28 \quad Q_{11} = \frac{809 - 28^2}{5} = 5 \quad a_{11} = \left[\frac{28 + 28}{5}\right] = 11$$

Din $Q_{10} = Q_{11}$, rezultă:

$$\sqrt{809} = \left[28; \overline{2, 3, 1, 7, 2, 1, 6, 2, 3, 11, 11, 3, 2, 6, 1, 2, 7, 1, 3, 2, 56}\right].$$

Astfel, algoritmul propus va avea forma:

Algoritm 2.3.1 ($\sqrt{d}$ ca fracţie continuă)
INPUT: $d \in \mathbf{N}$ *care nu este pătrat perfect.*
OUTPUT: fracţia continuă corespunzătoare.

1. $a_0 \leftarrow [\sqrt{d}], P_0 \leftarrow 0, Q_0 \leftarrow 1$.
2. *Pentru* $i = 0, 1, 2, \ldots$ *efectuează:*
   2.1. $P_{i+1} \leftarrow a_i Q_i - P_i,\ Q_{i+1} \leftarrow (d - P_{i+1}^2)/Q_i,$
   $a_{i+1} \leftarrow [(a_0 + P_{i+1})/Q_{i+1}]$.
   2.2. Dacă $P_i = P_{i+1}$ *atunci returnează*
   $[a_0; \overline{a_1, \ldots, a_{i-1}, a_i, a_{i-1}, \ldots, a_1, 2a_0}]$ *şi se opreşte.*
   2.3. Dacă $Q_i = Q_{i+1}$ *atunci returnează*
   $[a_0; \overline{a_1, \ldots, a_i, a_i, \ldots, a_1, 2a_0}]$ *şi se opreşte.*
   2.4. $i \leftarrow i + 1$.

În [5], sunt precizate teoreme de reprezentare pentru numere întregi. O astfel de teoremă, stabileşte forma generală a numerelor naturale care se pot scrie ca sumă de două pătrate:

Teoremă 2.3.4 (Fermat-Euler) *Fie* $n > 1$, $n = 2^k \cdot n_1 \cdot n_2$, *unde* $k \in \mathbf{N}$, n_1 *este produsul factorilor primi impari de forma* $4k + 1$ *ai lui* n *iar* n_2 *este produsul celorlalţi factori primi impari ai lui* n *(de forma* $4k + 3$*).*

Ecuaţia $x^2 + y^2 = n$ *are soluţii întregi dacă şi numai dacă toţi exponenţii din descompunerea canonică a lui* n_2 *sunt pari.*

Mai mult, dacă ecuaţia are soluţii, ea va avea exact $4(d_1(n) - d_3(n))$ *soluţii întregi, unde* $d_s(n)$ *reprezintă numărul de divizori ai lui* n *de forma* $4k + s$, $s \in \{1, 3\}$.

Dacă particularizăm, şi alegem p, un număr prim de forma $4k + 1$, observăm că ne încadrăm în condiţiile teoremei. Astfel, ecuaţia

$$x^2 + y^2 = p$$

unde p este un număr prim de forma $4k+1$, va avea întotdeauna 2 soluţii în mulţimea numerelor naturale. Metoda de determinare a acestora este datorată lui Lagrange, care a stabilit că, pentru un astfel de număr prim, lungimea perioadei fracţiei continue corespunzătoare lui $\sqrt{p}$ este impară.

Deci, folosind rezultatele anterioare, obţinem

$$\sqrt{p} = [a_0; \overline{a_1, \ldots, a_n, a_n, \ldots, a_1, 2a_0}],$$

unde n este cel mai mic indice pentru care $Q_{n+1} = Q_n$.

Numărul $\alpha_{n+1} = [\overline{a_n; a_{n-1}, \ldots}]$ are perioada simetrică. Din teorema 2.3.3, $\alpha_{n+1} \cdot \alpha'_{n+1} = -1$. Pe de altă parte, păstrând notaţiile anterioare, $\alpha_{n+1} = \dfrac{P_{n+1} + \sqrt{p}}{Q_{n+1}}$ iar $\alpha'_{n+1} = \dfrac{P_{n+1} - \sqrt{p}}{Q_{n+1}}$.

Astfel, rezultă $p = P_{n+1}^2 + Q_{n+1}^2$, deci (P_{n+1}, Q_{n+1}) şi (Q_{n+1}, P_{n+1}) sunt soluţiile ecuaţiei.

Pentru exemplul anterior, $p = 809 = 4 \cdot 202 + 1$ este de forma dorită. Am obţinut $Q_{10} = Q_{11}$. Atunci, din $P_{11} = 28$, şi $Q_{11} = 5$, soluţiile naturale ale ecuaţiei $x^2 + y^2 = 809$ sunt $(28, 5), (5, 28)$.

Algoritmul prezentat anterior poate fi folosit pentru rezolvarea acestui tip de ecuaţii.

Algoritm 2.3.2 (rezolvarea ecuaţiei $x^2 + y^2 = p$)
INPUT: p număr prim, de forma $4k + 1$.
OUTPUT: soluţiile (x,y) ale ecuaţiei.

1. $a_0 \leftarrow [\sqrt{d}], P_0 \leftarrow 0, Q_0 \leftarrow 1$.

2. Pentru $i = 0, 1, 2, \ldots$ *efectuează:*

2.1. $P_{i+1} \leftarrow a_i Q_i - P_i,\ Q_{i+1} \leftarrow (d - P_{i+1}^2)/Q_i,$
$a_{i+1} \leftarrow [(a_0 + P_{i+1})/Q_{i+1}]$.

2.2. Dacă $Q_i = Q_{i+1}$ *atunci returnează*
$(P_{i+1}, Q_{i+1}); (Q_{i+1}, P_{i+1})$ *şi se opreşte.*

2.3. $i \leftarrow i + 1$.

Exerciţii propuse

1. Determinaţi numerele raţionale reprezentate de fracţiile continue simple:

i) $[2; 7]$,

ii) $[0; 5, 6]$,

iii) $[3; 7, 15, 1]$.

2. Determinaţi fracţiile continue simple corespunzătoare numerelor raţionale:

$$\frac{6}{5}, \frac{22}{7}, \frac{101}{29}, \frac{-23}{141}.$$

3. Dacă $\alpha \in \boldsymbol{Q}$, $\alpha > 1$, are fracţia continuă simplă $[a_0; a_1, \ldots, a_n]$, atunci arătaţi că fracţia continuă simplă corespunzătoare lui $\frac{1}{\alpha}$ este $[0; a_0, a_1, \ldots, a_n]$.

4. Determinaţi fracţiile continue simple corespunzătoare numerelor:

$$\sqrt{2}, \sqrt{3}, \frac{1+\sqrt{5}}{2}.$$

5. Determinaţi primele 5 câturi parţiale ale fracţiilor continue simple pentru:

$$\sqrt[3]{2}, 2\pi, \frac{e-1}{e+1}.$$

6. Fracţia continuă infinită corespunzătoare numărului e este $e = [2; 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, 8, \ldots]$.

i) Determinaţi primele 8 convergente ale fracţiei.

ii) Determinaţi cea mai bună aproximare a lui e cu numitor mai mic decât 100.

7. Fie $\alpha = [a_0; a_1, a_2, \ldots]$ un număr iraţional. Arătaţi că fracţia continuă simplă corespunzătoare lui $-\alpha$ este $[-a_0-1; 1, a_1-1, a_2, a_3, \ldots]$, dacă $a_1 > 1$ şi $[-a_0 - 1; a_2 + 1, a_3, \ldots]$, pentru $a_1 = 1$.

8. Determinaţi fracţiile continue simple pentru numerele:

i) $\sqrt{11}, \sqrt{23}, \sqrt{47}$,

ii) $\frac{1+\sqrt{3}}{2}, \frac{13-\sqrt{2}}{7}$.

9. Determinaţi iraţionalul pătratic a cărui dezvoltare în fracţie continuă simplă este:

i) $\left[2; 1, \overline{5}\right]$,

ii) $\left[\overline{2; 1, 5}\right]$.

10. Arătaţi că, dacă d este număr natural, fracţia continuă simplă pentru $\sqrt{d^2+1}$ este $\left[d; \overline{2d}\right]$. Folosind acest rezultat, determinaţi fracţiile continue pentru $\sqrt{101}, \sqrt{290}$.

11. Fie $d \geq 2$, număr natural. Arătaţi că:

i) $\sqrt{d^2-1} = \left[d-1; \overline{1, 2d-2}\right]$,

ii) $\sqrt{d^2-d} = \left[d-1; \overline{2, 2d-2}\right]$.

Folosind aceste rezultate, determinaţi fracţiile continue pentru $\sqrt{99}$ şi $\sqrt{110}$.

12. Care dintre următorii iraţionali pătratici

$$1+\sqrt{5}, 2+\sqrt{8}, 4+\sqrt{17}, \frac{11-\sqrt{10}}{9}, \frac{3+\sqrt{23}}{2}$$

au fracţiile continue pur periodice?

13. Rezolvaţi, în numere naturale ecuaţiile:

i) $x^2+y^2 = 1009$,

ii) $x^2+y^2 = 405$.

CAPITOLUL 3

Congruenţe

3.1 Noţiuni generale

Definiţie 3.1.1 *Fie m un număr natural nenul şi a, b două numere întregi. Spunem că a este congruent cu b modulo m dacă $m \mid a - b$. În acest caz, vom folosi notaţia $a \equiv b \ (mod\ m)$.*

Congruenţele apar foarte des în viaţa de zi cu zi. De exemplu, ceasul funcţionează modulo 12 sau 24 ore, calendarul modulo 12 luni sau modulo 7 pentru zile, metrul modulo 1000 mm, etc. Congruenţa cu doi este cel mai simplu tip de congruenţă, unde numerele congruente cu 0 sunt numite numere pare iar cele congruente cu 1, impare.

Unele dintre propoziţiile următoare au demonstraţiile foarte simple şi sunt propuse cititorului ca exerciţiu.

Propoziţie 3.1.1 *Dacă $a, b \in \mathbf{Z}$ iar $m \geq 2$ este un număr natural, atunci $a \equiv b \ (mod\ m)$ dacă şi numai dacă există k număr întreg pentru care $a = b + km$.*

Propoziţie 3.1.2 *Relaţia de congruenţă este o relaţie de echivalenţă pe mulţimea numerelor întregi $\mathbf{Z}$.*

Conform acestui rezultat, mulţimea $\boldsymbol{Z}$ este împărţită în clase de echivalenţă unde clasa de echivalenţă a numărului întreg a este formată din toate numerele întregi de forma $a + km$, cu $k \in \boldsymbol{Z}$.

Definiţie 3.1.2 *Un sistem complet de resturi modulo m este o mulţime de numere întregi astfel încât orice întreg este congruent modulo m cu un singur număr din mulţime.*

Spre exemplu:
1) $\{0, 1, \ldots, m-1\}$ se numeşte *mulţimea celor mai mici resturi pozitive modulo m.*
2) Pentru m natural impar, sistemul complet de resturi

$$\{-\frac{m-1}{2}, -\frac{m-3}{2}, \ldots, -1, 0, 1, \ldots, \frac{m-3}{2}, \frac{m-1}{2}\}$$

se numeşte *mulţimea celor mai mici resturi, în valoare absolută, modulo m.*

Propoziţie 3.1.3 *Fie a, b numere întregi, m număr natural nenul, astfel încât $a \equiv b \pmod m$. Atunci, pentru orice întreg c, au loc relaţiile:*

1) $a + c \equiv b + c \pmod m$,

2) $a - c \equiv b - c \pmod m$,

3) $ac \equiv bc \pmod m$.

Propoziţie 3.1.4 *Fie m un număr natural nenul şi a, b, c numere întregi unde $(c, m) = d$. Dacă $ac \equiv bc \pmod m$, atunci $a \equiv b \pmod{\frac{m}{d}}$.*

Demonstraţie. Din $ac \equiv bc \pmod m$, există $k \in \boldsymbol{Z}$ astfel ca $c(a-b) = km$. Cum $d = (c, m)$, obţinem $c = dc'$, $m = dm'$ cu $(c', m') = 1$. Rezultă $c'(a - b) = km'$, adică $m' \mid a - b$. □

În practică, apare mai des un caz particular al acestei propoziţii, şi anume:

Corolar 3.1.1 *Fie m un număr natural nenul şi a, b, c numere întregi unde $(c, m) = 1$.*
Dacă $ac \equiv bc \pmod m$, atunci $a \equiv b \pmod m$.

Propoziţie 3.1.5 *Dacă $a \equiv b \pmod m$ şi $c \equiv d \pmod m$, atunci,*

1) $a \pm c \equiv b \pm d \pmod m$,

2) $ac \equiv bd \ (mod\ m)$.

Propoziţie 3.1.6 *Dacă* $\{r_1, r_2, \ldots, r_m\}$ *este un sistem complet de resturi modulo* m *iar* $a \in \mathbf{N}$ *cu* $(a, m) = 1$, *atunci,*

$$\{ar_1 + b, ar_2 + b, \ldots, ar_m + b\}$$

este un sistem complet de resturi modulo m, *pentru orice* $b \in \mathbf{Z}$.

Demonstraţie. Cum mulţimea este formată din m elemente, este suficient să arătă că oricare două dintre acestea nu sunt congruente modulo m. Dacă presupunem că $ar_j + b \equiv ar_k + b \ (mod\ m)$, pentru $j \neq k$, atunci $ar_j \equiv ar_k \ (mod\ m)$. Din corolarul 3.1.1 rezultă $r_j \equiv r_k \ (mod\ m)$, ceea ce este fals. □

Propoziţie 3.1.7 *Dacă* $a \equiv b \ (mod\ m)$, *atunci* $a^k \equiv b^k \ (mod\ m)$, *pentru orice număr natural* k.

Propoziţie 3.1.8 *Dacă* $a \equiv b \ (mod\ m_1)$, $a \equiv b \ (mod\ m_2)$,..., $a \equiv b \ (mod\ m_k)$, *atunci* $a \equiv b \ (mod\ [m_1, m_2, \ldots, m_k])$.

O consecinţă imediată a acestei propoziţii este dată de:

Corolar 3.1.2 *Fie numerele naturale nenule* $m_1, m_2, \ldots, m_k$, *două câte două relativ prime.*
Dacă $a \equiv b \ (mod\ m_1)$, $a \equiv b \ (mod\ m_2), \ldots, a \equiv b \ (mod\ m_k)$, *atunci* $a \equiv b \ (mod\ m_1 \cdot m_2 \cdot \ldots \cdot m_k)$.

Ca o primă aplicaţie a congruenţelor, prezentăm o metodă rapidă de calcul pentru $b^n \ (mod\ m)$ unde b, n, m sunt numere naturale. Ea este denumită *metoda ridicării repetate la pătrat şi reducerii modulo* m, algoritmul presupunând doar ridicări la pătrat şi înmulţiri repetate cu numere naturale mai mici decât modulul. Această metodă, fiind deosebit de eficientă pentru valori mari ale lui n şi m, este des folosită în multe protocoale criptografice care implică exponenţieri modulare.

Pentru început, se scrie n în baza 2. Fie $n = (a_k a_{k-1} \ldots a_1 a_0)_2$. Atunci

$$b^n = b^{\sum_{j=0}^{k} 2^j a_j} = \left(b^{2^0}\right)^{a_0} \left(b^{2^1}\right)^{a_1} \ldots \left(b^{2^k}\right)^{a_k}.$$

Ţinând cont de această relaţie, calculăm întâi resturile modulo m ale lui $b, b^2, b^4, \ldots, b^{2^k}$ ridicând succesiv la pătrat şi reducând modulo m. După

aceea, înmulţim resturile modulo m ale lui b^{2^j} cu $a_j = 1$ şi reducem modulo m.

De exemplu, tabelul următor pune în evidenţă, pe paşi, calculul efectuat pentru 5^{596} $(mod\ 1234)$:

j	0	1	2	3	4	5	6	7	8	9
a_j	0	0	1	0	1	0	1	0	0	1
A	5	25	625	681	1011	369	421	779	947	925
N	1	1	625	625	67	67	1059	1059	1059	1013

unde, la fiecare pas j, am notat:
$A = 5^{2^j}\ (mod\ 1234)$ şi
$N = 5^{a_0}\left(5^2\right)^{a_1} \ldots \left(5^{2^j}\right)^{a_j}\ (mod\ 1234)$.

Algoritm 3.1.1 (Ridicare repetată la pătrat)
INPUT: numerele naturale b, n, m.
OUTPUT: $b^n\ (mod\ m)$

1. $N \leftarrow 1$. *Dacă* $n = 0$, *returnează* N *şi se opreşte.*
2. $A \leftarrow b$.
3. *Dacă* $a_0 = 1$, *atunci pune* $N \leftarrow b$
4. *Pentru* $j = 1, \ldots, k$ *calculează:*
   - 4.1. $A \leftarrow A^2\ mod\ m$
   - 4.2. *Dacă* $a_j = 1$, *atunci* $N \leftarrow A \cdot N\ mod\ m$
5. *returnează* N.

3.2 Congruenţe liniare

Definiţie 3.2.1 *O congruenţă de forma*

$$ax \equiv b\ (mod\ m) \tag{3.1}$$

unde $x \in \mathbf{Z}$ *este necunoscuta, poartă numele de congruenţă liniară într-o variabilă.*

Vom arăta că studiul lor se reduce la cel al ecuaţiilor diofantice în două variabile. Mai întâi, observăm că, dacă x este soluţie a congruenţei (3.1) iar $x \equiv x_1\ (mod\ m)$, atunci $ax \equiv ax_1\ (mod\ m)$ adică $ax_1 \equiv b\ (mod\ m)$ ceea ce arată că şi x_1 este soluţie pentru (3.1).

Teoremă 3.2.1 *Fie $a, b \in \mathbf{Z}$, m natural nenul şi $(a, m) = d$. Congruenţa $ax \equiv b \ (mod\ m)$ are soluţii dacă şi numai dacă $d \mid b$. În acest caz, congruenţa are exact d soluţii necongruente modulo m.*

Demonstraţie. Congruenţa (3.1) este echivalentă cu $ax - mk = b$, pentru un număr întreg k. Deci, (3.1) are soluţii dacă şi numai dacă există un întreg y astfel încât $ax - my = b$. Din teorema 1.6.1, congruenţa (3.1) va avea soluţii dacă şi numai dacă $d \mid b$.
Presupunem că există soluţii pentru congruenţa (3.1). Fie (x_0, y_0) o soluţie particulară a ecuaţiei diofantice ataşate. Atunci, soluţia generală a acesteia este dată de $x = x_0 + \frac{m}{d}t$, $y = y_0 + \frac{a}{d}t$ unde t este un parametru întreg. Deci, soluţiile congruenţei (3.1) sunt $x = x_0 + \frac{m}{d}t$, cu $t \in \boldsymbol{Z}$. Vedem câte dintre acestea nu sunt congruente modulo m. Pentru aceasta, stabilim când două soluţii $x_1 = x_0 + \frac{m}{d}t_1$ şi $x_2 = x_0 + \frac{m}{d}t_2$ sunt congruente modulo m.
Dacă $x_1 \equiv x_2 \ (mod\ m)$, obţinem că $\frac{m}{d}t_1 \equiv \frac{m}{d}t_2 \ (mod\ m)$. Folosind propoziţia 3.1.4, cum $\left(\frac{m}{d}, m\right) = \frac{m}{d}$, rezultă că $t_1 \equiv t_2 \ (mod\ d)$. Deci, un sistem complet de soluţii necongruente modulo m se obţine din $x = x_0 + \frac{m}{d}t$ când t parcurge un sistem complet de resturi modulo d. □

Această teoremă arată că rezolvarea congruenţelor liniare se reduce la rezolvarea ecuţiilor diofantice prezentate în 1.6. Astfel, algoritmul de rezolvare a acestui tip de congruenţe se va reduce la algoritmul 1.6.1.

Spre exemplu, să rezolvăm congruenţa liniară $6x \equiv 15 \ (mod\ 21)$.

Se observă că $(6, 21) = 3$ şi $3 \mid 15$, deci congruenţa are soluţii. Ea va avea 3 soluţii necongruente modulo 21. Rezolvăm ecuaţia $6x - 21y = 15$ folosind metoda prezentată în teorema 1.6.1:

k	0	1	2	3	4	5
r_k	6	-21	-15	-6	-3	0
u_k	1	0	1	-1	3	-7
v_k	0	1	1	0	1	-2
q_k			-1	1	2	2

Obţinem astfel:
$-3 = 6(3) - 21(1)$ de unde, $15 = 6(-15) - 21(-5)$.
Atunci, $x_0 = -15$, $y_0 = -5$ este o soluţie particulară a ecuaţiei.
Soluţiile necongruente modulo 21 ale congruenţei iniţiale sunt:
$x_1 \equiv -15 + 7t \ (mod\ 21)$, unde $t \in \{0, 1, 2\}$.
În final obţinem:
$x_1 \equiv 6 \ (mod\ 21)$, $x_2 \equiv 13 \ (mod\ 21)$, $x_3 \equiv 20 \ (mod\ 21)$.

Considerăm în continuare congruenţele de forma $ax \equiv 1 \ (mod\ m)$. Din teorema 3.2.1, acest tip de congruenţă are soluţii dacă şi numai dacă a şi m sunt numere relativ prime.

Definiţie 3.2.2 *Fie $a \in \mathbf{Z}$ şi $m \in \mathbf{N}^*$ numere relativ prime. O soluţie $\bar{a}$ a congruenţei $ax \equiv 1 \ (mod\ m)$ se numeşte invers modulo m al lui a.*

Spre exemplu:
$x \equiv 9 \ (mod\ 31)$ este soluţie a congruenţei $7x \equiv 1 \ (mod\ 31)$. Astfel, orice număr congruent cu 9 modulo 31 este invers pentru 7 modulo 31.

Algoritm 3.2.1 (Invers modulo m)
INPUT: numerele naturale a, m.
OUTPUT: $\bar{a} \ (mod\ m)$ dacă există.
1. Calculează $d = (a, m)$ şi u, v cu $au + mv = d$ folosind algoritmul 1.2.2.
2. Dacă $d > 1$, atunci returnează $\bar{a} \ (mod\ m)$ nu există *şi se opreşte.*
3. Returnează u.

Dacă cunoaştem inversul lui a modulo m, putem rezolva congruenţa $ax \equiv b \ (mod\ m)$ unde $(a, m) = 1$. Prin înmulţirea congruenţei cu $\bar{a}$, vom obţine $x \equiv \bar{a}b \ (mod\ m)$.

Astfel, pentru congruenţa rezolvată anterior, $6x \equiv 15 \ (mod\ 21)$, dacă ţinem cont de propoziţia 3.1.4, ea este echivalentă cu congruenţa $2x \equiv 5 \ (mod\ 7)$. Folosind propoziţia 3.1.3, putem să înmulţim congruenţa cu 4 care este inversul lui 2 modulo 7 şi vom obţine ca soluţie finală $x \equiv 6 \ (mod\ 7)$. Observăm că acestă soluţie este echivalentă cu cele trei soluţii necongruente modulo 21 găsite anterior.

Să vedem când un întreg este propriul său invers modulo un număr prim.

Propoziţie 3.2.1 *Fie p un număr prim şi $a \in \mathbf{Z}$ prim cu p. Atunci, a este propriul său invers modulo p dacă şi numai dacă $a \equiv \pm 1 \ (mod\ p)$.*

Demonstraţie. $a \cdot a \equiv a^2 \equiv 1 \ (mod\ p)$ este echivalent cu $p \mid a^2 - 1$ adică $p \mid a - 1$ sau $p \mid a + 1$. Deci, $a \equiv \pm 1 \ (mod\ p)$. □

3.3 Sisteme de congruenţe

Vom studia două tipuri de sisteme de congruenţe liniare şi anume sisteme de două sau mai multe congruenţe liniare într-o variabilă cu diferite module şi sisteme de congruenţe liniare în mai multe variabile dar toate cu acelaşi modul.

Teoremă 3.3.1 (Teorema chinezească a resturilor) *Sistemul*

$$(S)\ \begin{cases} x \equiv a_1 \ (mod\ m_1) \\ x \equiv a_2 \ (mod\ m_2) \\ ..... \\ x \equiv a_r \ (mod\ m_r) \end{cases}$$

are soluţie unică modulo $M = m_1 m_2 \dots m_r$, pentru $m_1, m_2, \dots, m_r$, numere naturale relativ prime, două câte două.

Demonstraţie.[1] Fie $M_k = \dfrac{M}{m_k}$ pentru $1 \leq k \leq r$. Pentru fiecare $j \neq k$, $(m_j, m_k) = 1$. Obţinem astfel că $(M_k, m_k) = 1$. Fie $\overline{M_k}$ un invers al lui M_k modulo m_k. Deci, $M_k \overline{M_k} \equiv 1 \ (mod\ m_k)$. Notăm

$$x = a_1 M_1 \overline{M_1} + a_2 M_2 \overline{M_2} + \ldots + a_r M_r \overline{M_r}$$

şi arătăm că este soluţie pentru sistem.
Pentru aceasta, considerăm un k fixat, $1 \leq k \leq r$. Atunci, $m_k \mid M_j$ pentru orice $j \neq k$. Astfel, $M_j \equiv 0 \ (mod\ m_k)$ pentru $j \neq k$. Obţinem $x \equiv a_k M_k \overline{M_k} \equiv a_k \ (mod\ m_k)$.

[1] Forma originală a teoremei, găsită în China aproximativ în anul 300 e.n., era aceea că pentru a, b prime între ele, fiecare $n = 0, 1, \dots, ab-1$ are o pereche distinctă de resturi la împărţirea cu a şi cu b.

În final, arătăm că x este singura soluţie a sistemului modulo M. Considerăm x_1, x_2 două soluţii ale sistemului (S).
Atunci, $x_1 \equiv x_2 \ (mod\ m_k)$ pentru $1 \leq k \leq r$.
Din propoziţia 3.1.8 rezultă acum că $x_1 \equiv x_2 \ (mod\ M)$, deci orice două soluţii ale sistemului sunt congruente modulo M. □

Spre exemplu, să rezolvăm următoarea problemă găsită în *Manualul de Matematică* al lui Sun Zi, problemă considerată un exemplu clasic al teoremei chinezeşti a resturilor:
Determinaţi un număr care împărţit la 3 dă restul 2, la împărţirea la 5, restul este 3 iar împărţit la 7 dă restul 2. Problema o putem transcrie sub forma sistemului:

$$(S_1)\ \begin{cases} x \equiv 2 \ (mod\ 3) \\ x \equiv 3 \ (mod\ 5) \\ x \equiv 2 \ (mod\ 7) \end{cases}$$

$M = 3 \cdot 5 \cdot 7 = 105$, $M_1 = \frac{105}{3} = 35$, $M_2 = \frac{105}{5} = 21$, $M_3 = \frac{105}{7} = 15$.
Pentru determinarea lui $\overline{M_1}$ rezolvăm $35\overline{M_1} \equiv 1 \ (mod\ 3)$. Astfel, $2\overline{M_1} \equiv 1 \ (mod\ 3)$, de unde $\overline{M_1} \equiv 2 \ (mod\ 3)$.
Analog, $\overline{M_2} \equiv 1 \ (mod\ 5)$ rezultă din $21\overline{M_2} \equiv 1 \ (mod\ 5)$.
La fel obţinem $\overline{M_3} \equiv 1 \ (mod\ 7)$.
Soluţia sistemului este:
$x = 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 = 233 \equiv 23 \ (mod\ 105)$.

Algoritmul de rezolvare a sistemelor corespunzătoare teoremei chinezeşti a resturilor urmăreşte demonstraţia teoremei şi este atribuit lui Gauss.

Algoritm 3.3.1 (Teorema chinezească a resturilor)
INPUT: numerele naturale $m_1, \ldots, m_r$ două câte două relativ prime şi $a_1, \ldots, a_r$ numere întregi.
OUTPUT: Soluţia $x \ (mod\ M)$ a sistemului (S).

1. *Calculează $M = m_1 m_2 \ldots m_r$.*
2. *Pune $x \leftarrow 0$. Pentru $k = 1, \ldots, r$ calculează:*
   - 2.1. *$M_k = \frac{M}{m_k}$ şi $\overline{M_k}$ mod m_k.*
   - 2.2. *$x \leftarrow x + a_k M_k \overline{M_k} \ (mod\ M)$.*
3. *Returnează x.*

O altă metodă de rezolvare a unui sistem de congruenţe de forma lui (S), în care modulele nu trebuie să fie neapărat două câte două prime între ele, este de a rezolva succesiv congruenţele din sistem. Ea poartă numele de *metodă iterativă*.

De exemplu, dacă considerăm sistemul anterior, (S_1), prima congruenţă arată că $x = 3t + 2$, unde $t \in \boldsymbol{Z}$.
Aceste numere trebuie să verifice congruenţa următoare din sistem, adică $3t + 2 \equiv 3 \ (mod\ 5)$ sau $3t \equiv 1 \ (mod\ 5)$. Atunci, $t \equiv 2 \ (mod\ 5)$ de unde $t = 5u + 2$ cu u număr întreg. Obţinem $x = 15u + 8$. Mai rămâne să vedem pentru ce valori ale lui u se verifică şi ultima congruenţă a sistemului.
$15u+8 \equiv 2 \ (mod\ 7)$ implică $u \equiv 1 \ (mod\ 7)$. Astfel, $u = 7v+1$, cu $v \in \boldsymbol{Z}$. În final, $x = 105v + 23 \equiv 23 \ (mod\ 105)$.

Vom considera acum sisteme de mai multe congruenţe liniare cu mai multe necunoscute, dar acelaşi modul.

Pentru început considerăm cazul în care sistemul este format din două congruenţe cu două necunoscute:

$$(S_2) \begin{cases} ax + by \equiv e \ (mod\ m) \\ cx + dy \equiv f \ (mod\ m) \end{cases}$$

cu $a, b, c, d, e, f \in \boldsymbol{Z}$, $m \in \boldsymbol{N}^*$, astfel încât $(\Delta, m) = 1$, $\Delta = ad - bc$.

Propoziţie 3.3.1 *Sistemul (S_2) are soluţie unică modulo m şi anume:*

$$x \equiv \bar{\Delta}(de - bf) \ (mod\ m)$$

$$y \equiv \bar{\Delta}(af - ce) \ (mod\ m).$$

Putem extinde modul de rezolvare la un sistem de n congruenţe liniare cu n necunoscute.

Pentru studiul acestora vom folosi matrice pătratice cu elemente numere întregi.

Definiţie 3.3.1 *Fie $A, B \in \mathcal{M}_{k,n}(\mathbf{Z})$. Spunem că matricele $A = (a_{ij})$ şi $B = (b_{ij})$ sunt congruente modulo m dacă $a_{ij} \equiv b_{ij} \ (mod\ m)$, pentru orice $i \in \{1, \ldots, k\}$, $j \in \{1, \ldots, n\}$.*
În acest caz, vom scrie $A \equiv B \ (mod\ m)$.

De exemplu,

$$\begin{pmatrix} 15 & 3 \\ 8 & 12 \end{pmatrix} \equiv \begin{pmatrix} 5 & 13 \\ -2 & 2 \end{pmatrix} \ (mod\ 10).$$

În continuare prezentăm câteva proprietăţi ale matricelor.

Propoziţie 3.3.2 *Fie $A, B \in \mathcal{M}_{k,l}(\mathbf{Z})$ aşa încât $A \equiv B\ (mod\ m)$. Atunci, pentru orice matrice $C \in \mathcal{M}_{l,n}(\mathbf{Z})$ şi orice $D \in \mathcal{M}_{p,k}(\mathbf{Z})$, au loc relaţiile $AC \equiv BC\ (mod\ m)$ şi $DA \equiv DB\ (mod\ m)$.*

Definiţie 3.3.2 *Dacă $A, \bar{A} \in \mathcal{M}_n(\mathbf{Z})$ verifică*

$$A\bar{A} \equiv \bar{A}A \equiv I_n\ (mod\ m),$$

atunci spunem că $\bar{A}$ este inversa matricei A modulo m.

Dacă considerăm că $\bar{A}$ este inversa lui A modulo m iar $B \equiv \bar{A}\ (mod\, m)$, propoziţia anterioară asigură că $BA \equiv I_n\ (mod\ m)$.
Invers, dacă B_1, B_2 sunt inverse ale matricei A modulo m, atunci, din $B_1A \equiv B_2A \equiv I_n\ (mod\ m)$ rezultă $B_1AB_1 \equiv B_2AB_1\ (mod\ m)$ şi astfel, $B_1 \equiv B_2\ (mod\ m)$.
De exemplu, din

$$\begin{pmatrix} 2 & 5 \\ 3 & 1 \end{pmatrix}\begin{pmatrix} 3 & 1 \\ 3 & 2 \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\ (mod\ 4)$$

$$\begin{pmatrix} 3 & 1 \\ 3 & 2 \end{pmatrix}\begin{pmatrix} 2 & 5 \\ 3 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\ (mod\ 4)$$

rezultă că $\begin{pmatrix} 3 & 1 \\ 3 & 2 \end{pmatrix}$ este inversa matricei $\begin{pmatrix} 2 & 5 \\ 3 & 1 \end{pmatrix}$ modulo 4.

Propoziţie 3.3.3 *Fie $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathcal{M}_2(\mathbf{Z})$ astfel încât $\Delta = \det(A) = ad - bc$ este relativ prim cu m.*
Atunci, matricea $\bar{A} = \bar{\Delta}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$ este inversa matricei A modulo m.

Presupunem acum că $A \in \mathcal{M}_n(\boldsymbol{Z})$ iar cu A^* notăm matricea adjunctă.

Propoziţie 3.3.4 *Pentru $A \in \mathcal{M}_n(\mathbf{Z})$ şi $m \in \mathbf{N}^*$ cu $\det(A) = \Delta$ şi m relativ prime, matricea $\bar{A} = \bar{\Delta}A^*$ este inversa lui A modulo m.*

De exemplu, considerăm matricea $A = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 5 \\ 1 & 4 & 6 \end{pmatrix}$ şi vrem să-i determinăm inversa modulo 7.
$\Delta = -4 \equiv 3 \ (mod\ 7)$. Obţinem $\bar{\Delta} \equiv 5 \ (mod\ 7)$.
$A^* = \begin{pmatrix} -8 & 0 & 4 \\ -1 & 3 & -2 \\ 2 & -2 & 0 \end{pmatrix} \equiv \begin{pmatrix} 6 & 0 & 4 \\ 6 & 3 & 5 \\ 2 & 5 & 0 \end{pmatrix} \ (mod\ 7)$.
Rezultă astfel:
$\bar{A} = 5A^* = \begin{pmatrix} 30 & 0 & 20 \\ 30 & 15 & 25 \\ 10 & 25 & 0 \end{pmatrix} \equiv \begin{pmatrix} 2 & 0 & 6 \\ 2 & 1 & 4 \\ 3 & 4 & 0 \end{pmatrix} \ (mod\ 7)$.

Putem să abordăm acum rezolvarea unui sistem de congruenţe de forma:

$$(S_n) \begin{cases} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n \equiv b_1 \ (mod\ m) \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n \equiv b_2 \ (mod\ m) \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_{n1}x_1 + a_{n2}x_2 + \ldots + a_{nn}x_n \equiv b_n \ (mod\ m) \end{cases}$$

Sistemul poate fi scris sub formă matriceală $AX \equiv B \ (mod\ m)$ unde $A = (a_{ij}) \in \mathcal{M}_n(\boldsymbol{Z})$, $X = \begin{pmatrix} x_1 \\ \ldots \\ x_n \end{pmatrix} \in \mathcal{M}_{n,1}(\boldsymbol{Z})$ şi
$B = \begin{pmatrix} b_1 \\ \ldots \\ b_n \end{pmatrix} \in \mathcal{M}_{n,1}(\boldsymbol{Z})$.
Presupunem că $\Delta = \det(A)$ şi m sunt relativ prime. Atunci există $\bar{A}$, inversa modulo m a lui A. Prin înmulţire cu aceasta, obţinem
$\bar{A}B \equiv \bar{A}AX \equiv X \ (mod\ m)$ ca soluţie a sistemului (S_n).

Să rezolvăm de exemplu sistemul:

$$\begin{cases} x + 2y + 3z \equiv 2 \ (mod\ 7) \\ x + 2y + 5z \equiv 1 \ (mod\ 7) \\ x + 4y + 6z \equiv 2 \ (mod\ 7) \end{cases}$$

Observăm că matricea asociată sistemului este matricea A pentru care am calculat deja inversa modulo 7. Soluţia sistemului se obţine atunci ca fiind:

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \bar{A} \begin{pmatrix} 2 \\ 1 \\ 2 \end{pmatrix} = \begin{pmatrix} 16 \\ 13 \\ 10 \end{pmatrix} \equiv \begin{pmatrix} 2 \\ 6 \\ 3 \end{pmatrix} \ (mod\ 7).$$

3.4 Congruenţe speciale

3.4.1 Teorema Wilson

Teoremă 3.4.1 (Wilson) *Dacă $p > 1$ este un număr prim, atunci*

$$(p-1)! \equiv -1\ (mod\ p).$$

Demonstraţie. Dacă $p = 2$, atunci $(p-1)! = 1 \equiv -1\ (mod\ 2)$. Considerăm acum $p > 2$ număr prim.
Atunci, pentru orice $1 \leq x \leq p-1$ există invers modulo p. Din propoziţia 3.2.1, $x = \bar{x}$ dacă şi numai dacă $x \equiv \pm 1\ (mod\ p)$. De aici, rezultă că putem grupa numerele naturale nenule mai mici decât p, mai puţin numerele 1 şi $p-1$ astfel încât produsul celor $\frac{p-3}{2}$ perechi să fie congruent cu 1 modulo p.
Deci, $2 \cdot 3 \cdot \ldots \cdot (p-3) \cdot (p-2) \equiv 1\ (mod\ p)$.
În final, $(p-1)! \equiv 1 \cdot (p-1) \equiv -1\ (mod\ p)$. □

Reciproca teoremei lui Wilson este adevărată:

Teoremă 3.4.2 *Dacă n este un număr natural astfel încât*

$$(n-1)! \equiv -1\ (mod\ n),$$

atunci n este prim.

Demonstraţie. Să reducem la absurd şi să presupunem că n este un număr compus. Atunci, $n = a \cdot b$ unde $1 < a, b < n$. Deci, $a \mid (n-1)!$. Din $n \mid (n-1)! + 1$, rezultă că $a \mid (n-1)! + 1$ şi, în final, $a \mid 1$, ceea ce este fals. □

Observăm că această teoremă oferă un test de primalitate. Pentru a testa dacă n este prim, calculăm $(n-1)! + 1$ şi vedem dacă el este divizibil cu n. Cu toate că pare foarte simplu, acest test este impracticabil deoarece necesită prea multe operaţii binare.

3.4.2 Mica Teoremă a lui Fermat

Teoremă 3.4.3 (Mica Teoremă a lui Fermat) *Fie $p \geq 2$, număr prim. Atunci, $a^{p-1} \equiv 1 \ (mod\ p)$, pentru orice număr întreg a prim cu p.*

Demonstraţie. Considerăm numerele întregi $a, 2a, \ldots, (p-1)a$. Observăm că $p \nmid ka$ pentru $1 \leq k \leq p-1$. De asemenea, $ja \neq ka \ (mod\ p)$, pentru $j \neq k$. Deci, $\{a, 2a, \ldots, (p-1)a\}$ reprezintă un sistem complet de resturi modulo p din care a fost exclus 0. Astfel, $a \cdot 2a \cdot \ldots \cdot (p-1)a \equiv 1 \cdot 2 \cdot \ldots \cdot (p-1) \ (mod\ p)$. De aici, $a^{p-1}(p-1)! \equiv (p-1)! \ (mod\ p)$. Cum $((p-1)!, p) = 1$, rezultă în final $a^{p-1} \equiv 1 \ (mod\ p)$. □

Teoremă 3.4.4 *Pentru $p \geq 2$, număr prim şi pentru orice a, număr întreg, are loc relaţia:*

$$a^p \equiv a \ (mod\ p).$$

Demonstraţie. Dacă $p \nmid a$, din mica teoremă a lui Fermat, rezultă că $a^{p-1} \equiv 1 \ (mod\ p)$, de unde, $a^p \equiv a \ (mod\ p)$.
Dacă $p \mid a$, atunci $a^p \equiv a \equiv 0 \ (mod\ p)$. □

O primă aplicaţie a micii teoreme a lui Fermat constă în determinarea unor resturi modulo p pentru puteri. De exemplu, dacă dorim să calculăm restul lui 8^{110} modulo 13, folosind teorema, obţinem că $8^{110} = \left(8^{12}\right)^9 \cdot 8^2 \equiv 64 \equiv 12 \ (mod\ 13)$.

O altă aplicaţie folositoare a acestei teoreme este următoarea:

Corolar 3.4.1 *Dacă $p \geq 2$ este un număr prim, $a \in \mathbf{Z}$ cu $p \nmid a$, atunci a^{p-2} este inversul modulo p al lui a.*

Teorema 3.4.3 oferă astfel o nouă metodă de rezolvare a congruenţelor liniare.

Corolar 3.4.2 *Dacă a, b sunt numere întregi, $p \geq 2$ număr prim cu $p \nmid a$, soluţia congruenţei liniare $ax \equiv b \ (mod\ p)$ este*

$$x \equiv a^{p-2}b \ (mod\ p).$$

3.4.3 Teorema lui Euler

Definiţie 3.4.1 *Funcţia $\phi : \mathbf{N} \to \mathbf{N}$, definită prin $\phi(n)$ este numărul numerelor naturale mai mici decât n şi prime cu n, poartă numele de funcţia lui Euler.*

Definiţie 3.4.2 *Un sistem redus de resturi modulo n este o mulţime de $\phi(n)$ numere întregi, toate prime cu n şi două câte două necongruente modulo n.*

De exemplu, $\{1, 3, 7, 9\}$ este un sistem redus de resturi modulo 10.

Pornind de la un sistem redus de resturi modulo n, asemănător cu rezultatul propoziţiei 3.1.6, putem construi un nou sistem redus de resturi modulo n.

Propoziţie 3.4.1 *Fie $\{r_1, r_2, \ldots, r_{\phi(n)}\}$ un sistem redus de resturi modulo n şi $a \in \mathbf{Z}$, prim cu n. Atunci, $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ este tot un sistem redus de resturi modulo n.*

O generalizare a micii teoreme a lui Fermat este dată de Euler:

Teoremă 3.4.5 (Euler) *Fie $a \in \mathbf{Z}$, $n \in \mathbf{N}$ cu $(a, n) = 1$. Atunci,*

$$a^{\phi(n)} \equiv 1 \ (mod\ n).$$

Demonstraţie. Fie $\{r_1, r_2, \ldots, r_{\phi(n)}\}$ un sistem redus de resturi modulo n. Conform propoziţiei anterioare, $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ este un sistem redus de resturi modulo n.
Deci, resturile modulo n ale numerelor $ar_1, ar_2, \ldots, ar_{\phi(n)}$ sunt $r_1, r_2, \ldots, r_{\phi(n)}$, eventual în altă ordine.
Atunci, $a^{\phi(n)} r_1 r_2 \ldots r_{\phi(n)} \equiv r_1 r_2 \ldots r_{\phi(n)} \ (mod\ n)$.
Aplicând corolarul 3.1.1, obţinem $a^{\phi(n)} \equiv 1 \ (mod\ n)$. □

La fel ca în cazul micii teoreme a lui Fermat, următoarele corolare sunt imediate:

Corolar 3.4.3 *Dacă $n \geq 2$ este un număr natural, $a \in \mathbf{Z}$ cu $(a, n) = 1$, atunci $a^{\phi(n)-1}$ este inversul modulo n al lui a.*

Corolar 3.4.4 *Dacă a, b sunt numere întregi, $n \geq 2$ număr natural cu $(a, n) = 1$, soluţia congruenţei liniare $ax \equiv b \ (mod\ n)$ este*

$$x \equiv a^{\phi(n)-1} b \ (mod\ n).$$

Exerciţii propuse

1. Determinaţi, folosind metoda ridicării repetate la pătrat: $2^{321} \pmod{47}$ şi $3^{22} \pmod{23}$.

2. Rezolvaţi următoarele congruenţe liniare:

i) $3x \equiv 4 \pmod{7}$,

ii) $4x \equiv 3 \pmod{12}$,

iii) $9x \equiv 12 \pmod{21}$,

iv) $27x \equiv 25 \pmod{256}$,

v) $17x \equiv 14 \pmod{21}$,

vi) $15x \equiv 9 \pmod{25}$,

vii) $103x \equiv 612 \pmod{676}$,

viii) $987x \equiv 610 \pmod{1597}$,

ix) $27x \equiv 72 \pmod{900}$.

3. Fie p număr prim impar şi k număr natural nenul. Arătaţi că $x^2 \equiv 1 \pmod{p^k}$ are exact două soluţii necongruente, $x \equiv \pm 1 \pmod{p^k}$.

4. Fie congruenţa $x^2 \equiv 1 \pmod{2^k}$, cu $k \geq 1$. Arătaţi că această congruenţă are soluţie unică pentru $k = 1$ iar pentru $k = 2$, are două soluţii necongruente.
Pentru $k > 2$, demonstraţi că toate soluţiile congruenţei sunt:
$x \equiv \pm 1 \pmod{2^k}$ şi $x \equiv \pm(1 + 2^{k-1}) \pmod{2^k}$.

5. Rezolvaţi următoarele sistemele:

$$\begin{cases} x \equiv 1 \pmod{5} \\ x \equiv 3 \pmod{6} \\ x \equiv 11 \pmod{17} \end{cases} \qquad \begin{cases} x \equiv 6 \pmod{7} \\ x \equiv 2 \pmod{6} \end{cases}$$

$$\begin{cases} x \equiv 2 \pmod{11} \\ x \equiv 6 \pmod{13} \\ x \equiv 5 \pmod{12} \\ x \equiv 4 \pmod{7} \end{cases} \qquad \begin{cases} x \equiv 3 \pmod{15} \\ x \equiv 4 \pmod{11} \\ x \equiv 1 \pmod{14} \end{cases} .$$

6. Determinaţi cea mai mică soluţie pozitivă a sistemelor:

$$\begin{cases} x \equiv 12 \ (mod\ 31) \\ x \equiv 87 \ (mod\ 127) \\ x \equiv 91 \ (mod\ 225) \end{cases} \qquad \begin{cases} 3x \equiv 4 \ (mod\ 17) \\ 2x \equiv 7 \ (mod\ 9) \end{cases}$$

7. Găsiţi un număr care este multiplu de 11 şi împărţit la fiecare dintre numerele $2, 3, 5$, şi 7, dă restul 1.

8. Fie sistemul de congruenţe liniare:

$$\begin{cases} x \equiv a_1 \ (mod\ m_1) \\ x \equiv a_2 \ (mod\ m_2) \end{cases} .$$

Arătaţi că sistemul are soluţie dacă şi numai dacă

$$(m_1, m_2) \mid a_1 - a_2.$$

În cazul în care sistemul are soluţie, arătaţi că ea este unică modulo $[m_1, m_2]$.

Folosind acest rezultat, rezolvaţi sistemele:

$$\begin{cases} x \equiv 4 \ (mod\ 6) \\ x \equiv 13 \ (mod\ 15) \end{cases} \qquad \begin{cases} x \equiv 7 \ (mod\ 10) \\ x \equiv 4 \ (mod\ 15) \end{cases} .$$

9. Rezolvaţi următoarele sisteme de congruenţe liniare:

$$\begin{cases} x + 2y + z \equiv 3 \ (mod\ 6) \\ 3y + 4z \equiv 3 \ (mod\ 6) \\ 2x + 2y + z \equiv 4 \ (mod\ 6) \end{cases} \qquad \begin{cases} 17x + 11y \equiv 7 \ (mod\ 29) \\ 13x + 10y \equiv 8 \ (mod\ 29.) \end{cases}$$

10. Determinaţi $2^{326} \ (mod\ 17)$, folosind mica teoremă a lui Fermat.

11. Găsiţi ultima cifră a numărului 3^{100}, scris în baza 7.

12. Fie p, q două numere prime distincte. Arătaţi că

$$p^{q-1} + q^{p-1} \equiv 1 \ (mod\ pq).$$

13. Pentru $a \in \boldsymbol{Z}$ şi p, număr prim, arătaţi că:

$$p \mid a^p + (p-1)!a.$$

CAPITOLUL 4

Funcţii multiplicative

4.1 Funcţia Euler

Definiţie 4.1.1 *O funcţie aritmetică este o funcţie al cărei domeniu de definiţie este mulţimea numerelor naturale.*

Definiţie 4.1.2 *Fie f o funcţie aritmetică. Dacă $f(mn) = f(m)f(n)$, pentru orice două numere naturale m, n, relativ prime, spunem că f este funcţie multiplicativă.*
Dacă $f(mn) = f(m)f(n)$, pentru orice $m, n \in \mathbf{N}$, atunci f se numeşte complet multiplicativă.

Teoremă 4.1.1 *Fie f o funcţie multiplicativă şi*

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$$

cu p_j numere prime distincte, $\alpha_j \geq 1$, pentru fiecare $1 \leq j \leq k$. Atunci, $f(n) = f\left(p_1^{\alpha_1}\right) \cdot f\left(p_2^{\alpha_2}\right) \cdot \ldots f\left(p_k^{\alpha_k}\right)$.

Teoremă 4.1.2 *Dacă f este o funcţie multiplicativă, atunci funcţia F definită prin $F(n) = \sum\limits_{d|n} f(d)$ este o funcţie multiplicativă.*

Demonstraţie. Fie m, n numere naturale cu $(m, n) = 1$.
$F(mn) = \sum\limits_{d|mn} f(d)$. Dacă $d \mid mn$ şi $(m, n) = 1$, atunci există numerele

naturale d_1 şi d_2, relativ prime, astfel încât $d_1 \mid m$, $d_2 \mid n$, $d = d_1 d_2$. Obţinem:

$$\begin{aligned} F(mn) &= \sum_{\substack{d_1 \mid m \\ d_2 \mid n}} f(d_1 d_2) = \sum_{\substack{d_1 \mid m \\ d_2 \mid n}} f(d_1) f(d_2) \\ &= \sum_{d_1 \mid m} f(d_1) \sum_{d_2 \mid n} f(d_2) = F(m)F(n) \end{aligned}$$

deoarece f este multiplicativă şi d_1, d_2 sunt relativ prime. □

Propoziţie 4.1.1 *Dacă p este număr prim, atunci $\phi(p) = p - 1$. Reciproc, dacă $\phi(n) = n - 1$, atunci n este număr prim.*

Demonstraţie. Prima parte a afirmaţiei este evidentă. Considerăm acum că $\phi(n) = n - 1$ şi presupunem că n este compus. Atunci, există $1 < d < n$ un divizor netrivial al lui n. Astfel, există cel mult $n - 2$ numere mai mici decât n şi prime cu n, de unde $\phi(n) \leq n - 2$, fals. □

Propoziţie 4.1.2 *Fie p număr prim şi k număr natural nenul. Atunci, $\phi(p^k) = p^k - p^{k-1}$.*

Demonstraţie. Pentru $a < p^k$ observăm imediat că $(a, p^k) \neq 1$ dacă şi numai dacă $p \mid a$. Astfel, numerele a care nu sunt prime cu p^k sunt toate de forma jp cu $1 \leq j \leq p^{k-1}$. Deci, sunt p^{k-1} numere mai mici decât p^k care nu sunt prime cu acesta. Relaţia cerută rezultă acum imediat. □

Teoremă 4.1.3 *Funcţia Euler este o funcţie multiplicativă.*

Demonstraţie. Fie $m, n \in \boldsymbol{N}$, relativ prime.
Aşezăm numerele $1, 2, \ldots, mn$ sub forma următoare:

$$\begin{array}{ccccc} 1 & m+1 & 2m+1 & \ldots & (n-1)m+1 \\ 2 & m+2 & 2m+2 & \ldots & (n-1)m+2 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ r & m+r & 2m+r & \ldots & (n-1)m+r \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ m & 2m & 3m & \ldots & nm \end{array}$$

Presupunem $(m, r) = d > 1$. Atunci, din $d \mid m$ şi $d \mid r$, obţinem că pe linia r nu există numere relativ prime cu mn. Astfel, pentru a număra numerele relativ prime cu mn din şir trebuie să alegem doar liniile r cu

$(r, m) = 1$. Sunt exact $\phi(m)$ astfel de linii. Vedem acum câte numere de pe o astfel de linie sunt prime cu mn. Ţinând cont de forma lor, este evident că toate sunt prime cu m. Din propoziţia 3.1.6, rezultă că numerele de pe linie formează un sistem complet de resturi modulo n. Deci, numai $\phi(n)$ dintre ele sunt prime cu n. Cum toate sunt prime cu m şi m, n sunt relativ prime, pe linie sunt $\phi(n)$ numere prime cu mn. În final, am obţinut că sunt $\phi(n) \cdot \phi(m)$ numere mai mici decât mn şi prime cu mn, adică funcţia ϕ este multiplicativă. □

Însumând toate aceste rezultate, şi aplicând teorema 4.1.3, rezultă:

Teoremă 4.1.4 *Dacă* $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ *unde* p_i *sunt numere prime distincte şi* $\alpha_i \geq 1$, *pentru* $1 \leq i \leq k$, *atunci*

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_1}\right)\dots\left(1 - \frac{1}{p_k}\right).$$

Teoremă 4.1.5 *Pentru* n, *un număr natural nenul, are loc relaţia:*

$$\sum_{d|n} \phi(d) = n. \tag{4.1}$$

Demonstraţie. Vom împărţi numerele de la 1 la n în clase. Definim clasa $C_d = \{m \mid (m, n) = d\}$. Observăm că orice două astfel de clase sunt disjuncte. De asemenea, $m \in C_d$ este echivalent cu $\left(\frac{m}{d}, \frac{n}{d}\right) = 1$. Deci, numărul de elemente din clasa C_d este egal cu numărul numerelor naturale mai mici decât $\frac{n}{d}$ şi relativ prime cu $\frac{n}{d}$. Astfel, $\mid C_d \mid = \phi\left(\frac{n}{d}\right)$. Aceste clase C_d realizează o partiţie a mulţimii $\{1, 2, \dots, n\}$. De aici, $n = \sum\limits_{d|n} \mid C_d \mid = \sum\limits_{d|n} \phi\left(\frac{n}{d}\right)$. Dar, când d parcurge toţi divizorii lui n, $\frac{n}{d}$ face acelaşi lucru. Putem scrie atunci, $n = \sum\limits_{d|n} \phi(d)$. □

Să considerăm un exemplu pentru a vedea cum se formează aceste clase. Alegem $n = 12$.
Formăm clasele $C_d = \{m \mid (m, 12) = d\}$ unde $d \in \{1, 2, 3, 4, 6, 12\}$.

$$C_1 = \{1,5,7,11\} \quad |\, C_1 \,| = \phi\left(\frac{12}{1}\right) = 4$$
$$C_2 = \{2,10\} \quad |\, C_2 \,| = \phi\left(\frac{12}{2}\right) = 2$$
$$C_3 = \{3,9\} \quad |\, C_3 \,| = \phi\left(\frac{12}{3}\right) = 2$$
$$C_4 = \{4,8\} \quad |\, C_4 \,| = \phi\left(\frac{12}{4}\right) = 2$$
$$C_6 = \{6\} \quad |\, C_6 \,| = \phi\left(\frac{12}{6}\right) = 1$$
$$C_{12} = \{12\} \quad |\, C_{12} \,| = \phi\left(\frac{12}{12}\right) = 1$$

Obţinem $4+2+2+2+1+1=12$.

4.2 Funcţiile σ şi τ

Definiţie 4.2.1 *Funcţia aritmetică σ este definită prin $\sigma(n)$ este egal cu suma divizorilor naturali ai lui n, adică $\sigma(n) = \sum_{d|n} d$.*

De asemenea, definim funcţia τ prin $\tau(n) = \sum_{d|n} 1$, adică $\tau(n)$ este egal cu numărul divizorilor naturali ai lui n.

Folosind teorema 4.1.2, obţinem că funcţiile σ şi τ sunt funcţii multiplicative.

Lemă 4.2.1 *Dacă $p > 1$ este număr prim şi $k \in \mathbf{N}^*$, atunci:*

$$\sigma(p^k) = \frac{p^{k+1}-1}{p-1},\ \tau(p^k) = k+1.$$

Teoremă 4.2.1 *Fie n un număr natural a cărui descompunere canonică în factori primi este $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$. Atunci,*

$$\sigma(n) = \prod_{j=1}^{k} \frac{p_j^{\alpha_j+1}-1}{p_j-1},\ \tau(n) = \prod_{j=1}^{k}(\alpha_j+1).$$

4.3 Numere perfecte

În antichitate, un interes deosebit îl prezenta relaţia dintre un număr natural şi suma divizorilor săi, relaţie care căpăta chiar valenţe mistice.

Definiţie 4.3.1 *Un număr natural n pentru care $\sigma(n) = 2n$ se numeşte număr perfect.*

De exemplu, cum $\sigma(6) = 12$ şi $\sigma(28) = 56$, numerele 6 şi 28 sunt numere perfecte.

Teoremă 4.3.1 *Un număr natural par n este perfect dacă şi numai dacă $n = 2^{m-1}(2^m - 1)$ unde $m \geq 2$ şi $2^m - 1$ este număr prim.*

Demonstraţie. Presupunem n un număr par perfect.
Atunci, $n = 2^s t$, unde $s \geq 1$ şi t impar. Astfel,

$$\sigma(n) = \sigma(2^s)\sigma(t) = \left(2^{s+1} - 1\right)\sigma(t) \tag{4.2}$$

şi cum

$$\sigma(n) = 2n = 2^{s+1}t, \tag{4.3}$$

din cele două relaţii, obţinem că:

$$2^{s+1}t = \left(2^{s+1} - 1\right)\sigma(t). \tag{4.4}$$

Dar, $\left(2^{s+1}, 2^{s+1} - 1\right) = 1$. Atunci, $2^{s+1} \mid \sigma(t)$, adică $\sigma(t) = 2^{s+1}q$ pentru un număr natural q. Rezultă

$$2^{s+1}t = \left(2^{s+1} - 1\right)2^{s+1}q \tag{4.5}$$

adică $t = \left(2^{s+1} - 1\right)q$. Deci, $q \mid t$ şi $q \neq t$. Avem:

$$t + q = \left(2^{s+1} - 1\right)q + q = 2^{s+1}q = \sigma(t). \tag{4.6}$$

Dacă $q \neq 1$, atunci există cel puţin trei divizori naturali ai lui t, şi anume $1, q, t$. De aici rezultă:

$$\sigma(t) \geq t + q + 1, \tag{4.7}$$

ceea ce contrazice (4.6). Deci, $q = 1$ şi atunci, $t = 2^{s+1} - 1$. Rezultă $\sigma(t) = t + 1$, de unde t este prim. Obţinem $n = 2^s\left(2^{s+1} - 1\right)$ unde $2^{s+1} - 1$ este prim.

Reciproc, presupunem că $n = 2^{m-1}(2^m - 1)$ unde $2^m - 1$ este prim. Atunci, $\sigma(n) = \sigma\left(2^{m-1}\right)\sigma(2^m - 1) = (2^m - 1) \cdot 2^m = 2n$. Astfel, n este număr perfect. □

Pentru a determina numerele pare perfecte avem nevoie de numere prime de forma $2^n - 1$.

Propoziţie 4.3.1 *Dacă $2^n - 1$ este număr prim, atunci n este prim.*

Demonstraţie. Dacă presupunem că n nu este prim, atunci $n = ab$ cu $1 < a, b < n$. Obţinem atunci

$$2^n - 1 = (2^a - 1)\left(2^{a(b-1)} + \ldots + 2^a + 1\right)$$

unde $1 < 2^a - 1 < 2^n - 1$. Astfel, obţinem că $2^n - 1$ este număr compus ceea ce contrazice ipoteza. □

4.4 Numere Mersenne

La început, numerele de forma $2^n - 1$ erau considerate prime, pentru n număr prim. Începând cu anul 1536, diverşi matematicieni au arătat că această afirmaţie nu este corectă, dând contraexemple.

Definiţie 4.4.1 *Fie $n \in \mathbf{N}$. Un număr de forma $M_n = 2^n - 1$ se numeşte număr Mersenne. Dacă p este un număr prim şi M_p este prim, el poartă numele de număr prim Mersenne.*

Mersenne,[1] în lucrarea sa *Cogitata Physica-Mathematica*, din anul 1644 a afirmat, fără demonstraţie, că:
M_p este prim, pentru $p \in \{2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257\}$ iar pentru celelalte valori $n < 257$, numerele M_n erau compuse.

300 de ani au fost necesari pentru a verifica complet această afirmaţie. În anul 1947, când a fost finalizat studiul, s-a remarcat că Mersenne făcuse 5 erori şi anume: M_{61}, M_{89}, M_{107} sunt prime iar M_{67}, M_{257} compuse.

[1] Marin Mersenne (1588-1648) a fost călugăr franciscan, trăind aproape toată viaţa în mânăstirile Parisului. Chilia sa era locul unde mari matematicieni precum Fermat şi Pascal se întâlneau pentru a discuta. Prin vasta sa corespondenţă cu alţi matematicieni, el a jucat un rol important în comunicarea rezultatelor matematice obţinute în acea perioadă, când nu existau publicaţii ştiinţifice.

Pentru a vedea dacă un număr Mersenne este prim, de obicei verificăm dacă are divizori primi mici. Următoarea teoremă a lui Euler şi Fermat este folositoare în această privinţă.

Teoremă 4.4.1 *Fie p şi q numere prime impare. Dacă $q \mid M_p$, atunci $q \equiv \pm 1 \ (mod\ 8)$. Mai mult, $q = 2kp + 1$, pentru un k natural.*

Cu toate că în finalul demonstraţiei se foloseşte un rezultat obţinut în capitolul 7, anume teorema 7.1.3, prezentăm demonstraţia teoremei acum, pentru a nu o separa de enunţ.
Demonstraţie. Din teorema 3.4.3, cum q este prim impar, obţinem $q \mid 2^{q-1} - 1$. Din ipoteză, $q \mid 2^p - 1$. Deci,

$$q \mid \left(2^p - 1, 2^{q-1} - 1\right) = 2^{(p,q-1)} - 1. \tag{4.8}$$

Rezultă că $2^{(p,q-1)} - 1 > 1$, adică $(p, q-1) > 1$. Dar p este număr prim, de unde $(p, q-1) = p$. Astfel, $p \mid q-1$ adică există m natural astfel încât $q = mp + 1$. Din q impar, rezultă că m trebuie să fie număr par. Astfel, există k natural cu $q = 2kp + 1$.
Relaţia $2^{\frac{q-1}{2}} = (2^p)^k \equiv 1 \ (mod\ q)$, arată că 2 este rest pătratic modulo q. Folosind teorema 7.1.3, $q \equiv \pm 1 \ (mod\ 8)$. □.

Să vedem pe câteva exemple cum funcţionează această teoremă.

1) Pentru a vedea dacă $M_{13} = 2^{13} - 1 = 8191$ este prim, vedem dacă are divizori primi de forma $26k + 1$. Singurele numere prime de această formă $\leq \sqrt{8191}$ sunt 53 şi 79. Prin calcul direct, se obţine că ei nu sunt divizori pentru M_{13}. Deci, M_{13} este număr prim Mersenne.

2) Pentru $M_{23} = 8388607$ căutăm divizori primi de forma $46k + 1 \leq \sqrt{M_{23}} = 2896, \ldots$. Se obţine $M_{23} = 47 \cdot 178481$, deci M_{23} este compus.

3) În 1772, Euler a folosit teorema pentru a arăta că M_{31} este prim. Astfel, el a căutat divizori de forma $62k + 1$ care verifică $q = 62k + 1 \equiv \pm 1 \ (mod\ 8)$. Rezolvând congruenţele, rezultă $k \equiv 1 \ (mod\ 4)$ sau k este multiplu de 4. De aici, $q \equiv 1 \ (mod\ 248)$ sau $q \equiv 63 \ (mod\ 248)$. Cum dintre aceste numere, nici unul nu e divizor pentru M_{31}, el este prim.

Se presupune că există o infinitate de numere prime Mersenne, deci o infinitate de numere pare perfecte.

Un rezultat interesant este oferit de Euler în teorema:

Teoremă 4.4.2 *Fie p număr prim, $p \equiv 3 \ (mod\ 4)$. Atunci, $2p+1$ este prim dacă şi numai dacă $2^p \equiv 1 \ (mod\ 2p+1)$.*

Cu alte cuvinte, dacă $p \equiv 3 \ (mod\ 4)$ este număr prim şi $2p+1$ este tot număr prim, atunci M_p este număr compus.

Găsirea de numere prime Mersene este extrem de laborioasă din punct de vedere computaţional. G. Woltman a organizat un program distribuit pe Internet, *Great Internet Mersenne Prime Search,* în care sute de voluntari folosesc computerele pentru a realiza etape din căutare. În cadrul acestui program, pe 17 noiembrie 2003 s-a descoperit al 40-lea număr prim Mersenne iar după şase luni, al 41- lea. Ultimul număr prim Mersenne cunoscut până în prezent a fost determinat în februarie 2005.

Dacă veţi consulta Anexa A, veţi găsi cele 42 de numere prime Mersenne cunoscute până în prezent. Semnele de întrebare care apar în dreptul ultimelor numere din tabel arată că cercetarea primalităţii numerelor Mersenne nu este completă încă în acest interval. Cum căutarea nu a fost făcută pentru toţi exponenţii, trebuie verificat dacă ultimele numere sunt numere prime Mersenne consecutive, adică nu există alte numere prime Mersenne între ultimele 4.

Exerciţii propuse

1. Calculaţi $\phi(n)$ pentru $n \in \{24, 52, 84, 99, 100, 256\}$.

2. Determinaţi suma divizorilor pozitivi ai lui $n \in \{35, 1000, 2^{37}\}$.

3. Pentru $n \in \{36, 99, 144, 10!\}$ determinaţi numărul de divizori pozitivi.

4. Precizaţi care sunt toate numerele naturale cu exact $2, 3$, respectiv 4 divizori pozitivi.

5. Folosind rezultatul teoremei 4.4.1, stabiliţi care dintre numerele Mersene M_7, M_{11}, M_{17} sunt numere prime Mersenne.

6. Fie n număr natural astfel încât $2n+1$ este număr prim. Atunci, $2n+1 \mid M_n$ sau $2n+1 \mid M_n + 2$.

CAPITOLUL 5

Prime aplicaţii ale congruenţelor

5.1 Factorizarea unor numere de formă particulară

Propoziţie 5.1.1 *Fie b şi n două numere relativ prime iar a şi c numere naturale. Dacă $b^a \equiv 1 \pmod n$ şi $b^c \equiv 1 \pmod n$, atunci $b^d \equiv 1 \pmod n$ unde $d = (a, c)$.*

Demonstraţie. Folosind algoritmul lui Euclid, există $u, v \in \boldsymbol{Z}$ astfel ca $d = ua + vc$.
Cum unul din cele două numere u, v este pozitiv iar celălalt negativ sau zero, putem presupune că $u > 0,\ v \leq 0$. Obţinem $b^{au} \equiv 1 \pmod n$ şi $b^{c(-v)} \equiv 1 \pmod n$, de unde, $b^{au-c(-v)} \equiv 1 \pmod n$.
Astfel, $b^d \equiv 1 \pmod n$. □

Propoziţie 5.1.2 *Dacă p este un număr prim cu $p \mid b^n - 1$, atunci $p \mid b^d - 1$ pentru d, un divizor propriu al lui n sau $p \equiv 1 \pmod n$. Dacă $p > 2$, şi n este impar, a doua condiţie devine $p \equiv 1 \pmod{2n}$.*

Demonstraţie. Din ipoteză, $b^n \equiv 1 \pmod p$ iar din mica teoremă a lui Fermat, $b^{p-1} \equiv 1 \pmod p$. Din propoziţia anterioară, $b^d \equiv 1 \pmod p$, unde $d = (n, p-1)$. Dacă $d < n$, obţinem prima relaţie. Pentru cazul

$d = n$, cum $d \mid p-1$, avem $p \equiv 1 \ (mod\ n)$. În situaţia în care p şi n sunt amândoi impari şi $n \mid p-1$, atunci este evident că $2n \mid p-1$. □

Vom exemplifica cum această propoziţie poate fi folosită pentru a descompune în factori anumite numere mari.

1. Pentru $2^{11} - 1 = 2047$ căutăm divizori primi $p \equiv 1 \ (mod\ 22)$. Verificăm dacă $p = 23, 67, 89, \ldots$ sunt divizori ai numărului (de fapt, nu trebuie să depăşim $\sqrt{2047} = 45, \ldots$). Obţinem astfel descompunerea $2047 = 23 \cdot 89$. În mod analog, se arată că $2^{13} - 1 = 8191$ este prim.

2. Pentru a descompune în factori primi $3^{12} - 1 = 531440$, încercăm mai întâi cu divizorii numerelor mai mici $3^1 - 1, 3^2 - 1, 3^3 - 1, 3^4 - 1$ şi cu ai lui $3^6 - 1 = (3^3 - 1)(3^3 + 1)$ care nu apar deja în $3^3 - 1$. Obţinem astfel, $2^4, 5, 7, 13$. Cum $\dfrac{531440}{2^4 \cdot 5 \cdot 7 \cdot 13} = 73$ este prim, am încheiat descompunerea. Trebuie remarcat că, aşa cum era de aşteptat, orice număr prim care nu apare în descompunerea lui $3^d - 1$ pentru d divizor propriu al lui 12 (73, de exemplu) trebuie să fie $\equiv 1 \ (mod\ 12)$.

3. Pentru $2^{35} - 1 = 34359738367$ considerăm la început divizorii $2^d - 1$ pentru $d = 1, 5, 7$ care furnizează divizorii primi 31 şi 127. Obţinem $2^{35} - 1 = 31 \cdot 127 \cdot 8727391$. Propoziţia ne asigură că divizorii primi rămaşi trebuie să fie $\equiv 1 \ (mod\ 70)$. Verificăm pentru $71, 211, 281, \ldots$. Nu trebuie să verificăm toţi divizorii de această formă până la $\sqrt{8727391} = 2954, \ldots$, pentru că găsim imediat $8727391 = 71 \cdot 122921$ şi astfel, rămâne să cercetăm doar până la $\sqrt{122921} = 350, \ldots$. Găsim 122921 număr prim şi astfel, descompunerea în factori primi cerută este $2^{35} - 1 = 31 \cdot 71 \cdot 127 \cdot 122921$.

Ca o remarcă, să vedem cum s-ar face această descompunere folosind un calculator care presupunem că face operaţii aritmetice doar cu numere de maxim 8 cifre zecimale. Vom sparge numărul în părţi. În cazul nostru, atingem limita impusă pentru $2^{26} = 67108864$. Pentru a face înmulţirea cu $2^9 = 512$, scriem $2^{35} = 512 \cdot (67108 \cdot 1000 + 864) = 34359296 \cdot 1000 + 442368 = 34359738368$. Apoi, când trebuie să împărţim $2^{35} - 1$ la $31 \cdot 127 = 3937$, luăm partea întreagă $\left[\dfrac{34359738}{3937}\right] = 8727$ şi scriem $34359738 = 3937 \cdot 8727 + 1539$. Atunci, $\dfrac{34359738367}{3937} = \dfrac{(3937 \cdot 8727 + 1539) \cdot 1000 + 367}{3937} = 8727000 + \dfrac{1539367}{3937} = 8727391$.

5.2 Teste de divizibilitate

Folosind congruenţele, putem realiza teste de divizibilitate pentru întregi ţinând cont de dezvoltarea lor relativ la diferite baze.

Pentru început, discutăm cele mai cunoscute teste care folosesc scrierea zecimală.

Considerăm numărul natural $n = (a_k a_{k-1} \dots a_1 a_0)_{10}$. Deci,

$$n = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \dots + a_1 \cdot 10 + a_0, \text{ cu } 0 \leq a_j \leq 9. \quad (5.1)$$

Test de divizibilitate cu puteri ale lui 2.

Cum $10 \equiv 0 \ (mod\ 2)$, obţinem că $10^j \equiv 0 \ (mod\ 2^j)$, pentru orice $j \leq k$. Astfel,

$$n \equiv (a_{j-1} a_{j-2} \dots a_1 a_0)_{10} \ (mod\ 2^j).$$

Deci, rezultă că:

Test 5.2.1 *n este divizibil cu 2^j dacă şi numai dacă numărul format cu ultimele sale j cifre este divizibil cu 2^j.*

De exemplu, pentru $n = 2114480$, cum $2^5 \nmid 14480$ şi $2^4 \mid 4480$, obţinem că $2^5 \nmid n$ iar pentru $j \leq 4$, $2^j \mid n$.

După un raţionament asemănător, obţinem un ***test de divizibilitate cu puteri ale lui 5***:

Test 5.2.2 *n este divizibil cu 5^j dacă şi numai dacă numărul format cu ultimele sale j cifre este divizibil cu 5^j.*

Spre exemplu, putem verifica imediat că $n = 23752875$ este divizibil cu 5^j pentru $j \leq 3$ iar $5^4 \nmid n$ cum $625 \nmid 2875$.

Teste de divizibilitate cu 3 şi 9.

Din $10 \equiv 1 \ (mod\ 3)$ şi $10 \equiv 1 \ (mod\ 9)$, rezultă:
$10^j \equiv 1 \ (mod\ 3)$ respectiv $10^j \equiv 1 \ (mod\ 9)$.
Din (5.1), obţinem $n \equiv a_k + a_{k-1} + \dots + a_1 + a_0 \ (mod\ 3)$ şi aceeaşi relaţie modulo 9.

Test 5.2.3 *n este divizibil cu 3 sau cu 9 dacă şi numai dacă suma cifrelor sale este divizibilă cu respectiv 3 sau 9.*

Pentru $n = 26453097$, observăm că $2 + 6 + 4 + 5 + 3 + 9 + 7 = 36$, de unde n este divizibil cu 9.

Test de divizibilitate cu 11.

Dacă ţinem cont de faptul că $10 \equiv -1 \ (mod\ 11)$, obţinem:
$10^2 \equiv 1 \ (mod\ 11)$, $10^3 \equiv -1 \ (mod\ 11)$, etc. Astfel, (5.1) implică
$n \equiv a_0 - a_1 + \ldots + (-1)^{k-1} a_{k-1} + (-1)^k a_k \ (mod\ 11)$.

Test 5.2.4 *n este divizibil cu 11 dacă şi numai dacă suma alternată a cifrelor sale este divizibilă cu 11.*

Dacă alegem $n = 291575295$, cum $5-9+2-5+7-5+1-9+2 = -11$, rezultă $11 \mid n$.

Test de divizibilitate cu 7,11 şi 13.

Trebuie remarcat că $7 \cdot 11 \cdot 13 = 1001$, de unde

$$10^3 \equiv -1 \ (mod\ 1001).$$

Atunci,
$n \equiv (a_0 + 10a_1 + 100a_2) + 1000(a_3 + 10a_4 + 100a_5) + 1000^2(a_6 + 10a_7 + 100a_8) + \ldots \equiv (a_2a_1a_0)_{10} - (a_5a_4a_3)_{10} + (a_8a_7a_6)_{10} \ldots \ (mod\ 1001)$.

Test 5.2.5 *n este divizibil cu 7, 11 sau 13 dacă şi numai dacă suma alternată a numerelor formate din blocuri de trei cifre, pornind de la ultimele, este divizibilă cu, respectiv 7, 11 sau 13.*

Să generalizăm acum testele prezentate considerând numărul n scris într-un sistem de numeraţie de bază oarecare b. Fie

$$n = (a_k a_{k-1} \ldots a_1 a_0)_b.$$

Urmând aceeaşi cale de demonstraţie ca pentru cazul scrierii zecimale, obţinem următoarele teste:

Test 5.2.6 *Dacă $d \mid b$ şi $0 \leq j < k$, n este divizibil cu d^j dacă şi numai dacă $(a_{j-1}a_{j-2} \ldots a_1a_0)_b$ este divizibil cu d^j.*

Test 5.2.7 *Dacă $d \mid b - 1$, n este divizibil cu d dacă şi numai dacă $a_k + \ldots a_1 + a_0$ este divizibil cu d.*

Test 5.2.8 *Dacă $d \mid b+1$, n este divizibil cu d dacă şi numai dacă suma $(-1)^k a_k + \ldots + a_2 - a_1 + a_0$ este divizibilă cu d.*

Spre exemplu, dacă considerăm numărul $n = (7F28A6)_{16}$ scris în baza 16, vom obţine:

$2 \mid n$ pentru că $2 \mid 6$ dar $4 \nmid n$ cum $4 \nmid (A6)_{16} = 166$;
$3 \mid n$ deoarece $3 \mid 7 + F + 2 + 8 + A + 6 = 48$ şi din
$5 \nmid 7 + F + 2 + 8 + A + 6$, rezultă $5 \nmid n$;
$17 \nmid n$ se obţine din $17 \nmid 6 - A + 8 - 2 + F - 7 = 10$.

Observaţie 5.2.1 *Dacă dorim, putem face o conversie simplă din sistemul hexagesimal în cel binar şi invers, conform tabelului:*

Hex	0	1	2	3	4	5	6	7
Binar	0000	0001	0010	0011	0100	0101	0110	0111
Hex	8	9	A	B	C	D	E	F
Binar	1000	1001	1010	1011	1100	1101	1110	1111

Spre exemplu, $(2FB3)_{16} = (10111110110011)_2$ unde se observă că am omis cele două zerouri din scrierea lui 2 aflate în faţa numărului. Pentru $(11110111101001)_2$, dacă dorim să-l scriem în baza 16, se formează grupe de câte 4 cifre, pornind de la ultimele, pe care le înlocuim conform tabelului. Obţinem astfel, $(3DE9)_{16}$.

În acelaşi fel se poate face conversia numerelor scrise în bazele b şi b^k.

5.3 Calendarul

Calendarul[1] este un sistem de organizare a unităţilor de timp pentru a calcula timpul pe perioade foarte extinse. Prin convenţie, ziua este cea mai mică unitate calendaristică de timp. Calendarul, indiferent de tipul său, reprezintă o legătură între omenire şi cosmos. El a stat la baza planificării agriculturii, vânătorii, ciclurilor de migraţie, menţinerii ciclurilor de evenimente civile şi religioase.

[1] Kalaendae reprezenta prima zi din fiecare lună în calendarul roman antic.

Conform unor date recente, în lume se folosesc aproximativ 40 de calendare. Ciclurile astronomice fundamentale sunt *ziua* (bazată pe rotaţia Pământului în jurul axei sale), *luna* (bazată pe revoluţia Lunii în jurul Pământului) şi *anul* (bazat pe revoluţia Pământului în jurul Soarelui). Complexitatea calendarelor apare datorită faptului că ciclurile de revoluţie nu cuprind un număr întreg de zile, precum şi datorită faptului că ciclii astronomici nu sunt constanţi şi nici perfect comparabili unii cu ceilalţi.

Fără a dori să prezentăm pe larg *istoria calendarului,* punctăm doar două momente importante în evoluţia sa. La egipteni, fiecare an avea 365 de zile. În anul 45 î.e.n., Iulius Cezar[2] a iniţiat modificarea calendarului, cerând sprijinul astronomului Sosigenes din Alexandria. Acesta a stabilit lungimea anului ca fiind de 365,25 zile. El a creat un *calendar solar*[3] cu 3 ani formaţi din 365 de zile şi cu ani bisecţi la fiecare 4 ani pentru a reflecta mai bine lungimea adevărată a anului. Deci, lungimea anului era de 365,25 de zile.

Cele mai recente calcule arată că un an are un număr de aproximativ 365,2422 de zile. Astfel, cu trecerea secolelor, diferenţa de 0,0078 zile pe an s-a adunat şi calendarul a devenit din ce în ce mai mult incompatibil cu anotimpurile. În secolul XVI, echinocţiul de primăvară, care determina data Paştelui, se mutase cu 10 zile faţă de data exactă.

În anul 1582, Papa Gregoriu al XIII-lea a dat un decret prin care s-au exclus 10 zile din calendar. Data de 5 octombrie a devenit data de 15 octombrie, iar zilele de 6-14 octombrie au fost omise. Ca ani bisecţi, au fost consideraţi cei divizibili cu 4, iar dintre cei divizibili cu 100, bisecţi au fost aleşi doar cei care sunt divizibili şi cu 400. De exemplu, 1900 nu este an bisect, dar 2000, da. Astfel, anul are 365,2425 zile. Eroarea de 0,0003 zile înseamnă 3 zile la 10000 ani. Şi acest calendar încă necesită modificări. Calendarul Gregorian[4] a stabilit ca primă zi

[2]Calendarul Iulian a fost calendarul standard pentru majoritatea ţărilor europene şi pentru America, până în 1582 când a apărut calendarul Gregorian. Ianuarie a devenit prima lună din an, până atunci, anul începând cu luna martie.

[3]Un calendar solar este un calendar care intercalează zile, formând ani bisecţi, pentru a creşte lungimea anului calendaristic.

[4]Trecerea la calendarul Gregorian a fost adoptată de Anglia şi SUA în 1752, printr-un salt de 11 zile, de URSS în 1917, de Grecia în 1923. El este cunoscut sub numele de *calendarul nou*, pe când cel Iulian de *calendarul vechi.* Luând în considerare acest fapt, există algoritmi de conversie a zilelor după calendarul Iulian în zile după calendarul Gregorian.

a anului, data de 1 Ianuarie. Scopul său iniţial a fost ecleziastic, şi anume de a stabili data sărbătoririi Paştelui conform regulilor impuse de biserică. Calcularea datei zilei de Paşte se bazează pe congruenţe şi, un astfel de algoritm a fost dat de Oudin în 1940.

Ne propunem să aplicăm congruenţele în scopul determinării zilei din săptămână corespunzătoare unei date calendaristice. Pentru a simplifica problema, vom considera datele ca fiind date conform calendarului Gregorian. Dacă nu, trebuie să facem apel şi la un algoritm de conversie.

Cum zilele săptămânii se repetă din 7 în 7, vom folosi congruenţa modulo 7. Facem următoarele convenţii:

- Zilele săptămânii, începând cu duminică se notează cu cifre de la 0 la 6.
- Considerăm că anul începe la 1 Martie. Atunci, lunile vor fi numerotate, pornind cu Martie şi terminând cu Februarie, de la 1 la 12. Astfel, pentru anii bisecţi, ziua care se ataşează va fi ultima din an.
- Notăm cu k ziua din lună, cu m luna şi anul va fi notat cu $N = 100C + Y$ unde C marchează secolul iar $Y \leq 99$.

De exemplu, dacă considerăm data de 17 Ianuarie 1990, $k = 17$, $m = 11$, $N = 1989$ de unde $C = 19$, $Y = 89$.

Ca bază de plecare folosim ziua de 1 Martie a fiecărui an. Notăm cu d_N ziua din săptămână corespunzătoare lui 1 Martie din anul N. Începem cu anul 1600, pentru uşurinţa calculului, şi calculăm mai întâi d_N pentru fiecare N.

Între 1 Martie din anul $N-1$ şi 1 Martie din anul N, sunt 365 de zile dacă N nu este an bisect. Astfel,

$$d_N \equiv d_{N-1} + 1 \ (mod\ 7), \tag{5.2}$$

cum $365 \equiv 1 \ (mod\ 7)$. Dacă N este an bisect, avem

$$d_N \equiv d_{N-1} + 2 \ (mod\ 7). \tag{5.3}$$

Calculăm acum câţi ani bisecţi au fost între anii 1600 şi N. Conform calendarului Gregorian, vom avea

$$x = \left[\frac{N-1600}{4}\right] - \left[\frac{N-1600}{100}\right] + \left[\frac{N-1600}{400}\right] = \left[\frac{N}{4}\right] - 400 - \left[\frac{N}{100}\right] + 16 + \left[\frac{N}{400}\right] - 4 = \left[\frac{N}{4}\right] - \left[\frac{N}{100}\right] + \left[\frac{N}{400}\right] - 388.$$

Dacă înlocuim $N = 100C + Y$, obţinem

$$x = 25C + \left[\frac{Y}{4}\right] - C - \left[\frac{Y}{100}\right] + \left[\frac{C}{4}\right] - 388,$$

de unde

$$x \equiv 3C + \left[\frac{C}{4}\right] + \left[\frac{Y}{4}\right] - 3 \ (mod\ 7). \tag{5.4}$$

Din (5.2) şi (5.3), obţinem $d_N \equiv d_{1600} + N - 1600 + x \ (mod\ 7)$ şi, folosind (5.4), rezultă în final,

$$d_N \equiv d_{1600} - 2C + Y + \left[\frac{C}{4}\right] + \left[\frac{Y}{4}\right] \ (mod\ 7). \tag{5.5}$$

Ştim că $d_{2005} \equiv 2 \ (mod\ 7)$, ziua de 1 Martie 2005 fiind într-o zi de marţi. Atunci, $2 \equiv d_{1600} - 2 \cdot 20 + 5 + \left[\frac{20}{4}\right] + \left[\frac{5}{4}\right] \ (mod\ 7)$ de unde $d_{1600} \equiv 31 \equiv 3 \ (mod\ 7)$. Am găsit că 1 Martie 1600 a fost într-o zi de miercuri. Înlocuind în (5.5), rezultă:

$$d_N \equiv 3 - 2C + Y + \left[\frac{C}{4}\right] + \left[\frac{Y}{4}\right] \ (mod\ 7). \tag{5.6}$$

Pasul următor este de a stabili ziua din săptămână corespunzătoare primei zile din fiecare lună a anului N. Observăm că lunile cu 30 de zile deplasează la dreapta ziua de 1 a lunii următoare cu 2 zile, iar lunile cu 31 de zile, cu 3 zile la dreapta. Cum, în cazul nostru, februarie are 28 de zile, ea nu aduce nici o modificare. În total, pe parcursul unui an, se obţine o deplasare de 29 zile.

Rezultatele sunt prezentate în următorul tabel:

Perioada	zile adăugate
1 Martie - 1 Aprilie	3
1 Aprilie - 1 Mai	2
1 Mai - 1 Iunie	3
1 Iunie - 1 Iulie	2
1 Iulie - 1 August	3
1 August - 1 Septembrie	3
1 Septembrie - 1 Octombrie	2
1 Octombrie - 1 Noiembrie	3
1 Noiembrie - 1 Decembrie	2
1 Decembrie - 1 Ianuarie	3
1 Ianuarie - 1 Februarie	3

Pentru $1 \leq m \leq 12$, obţinem că $[2, 6m - 0, 2] - 2$ are aceleaşi valori cu numărul de zile adăugate, corespunzătoare lunii m. Observăm că, pentru $m = 1$, valoarea ei este zero.

Deci, ziua din săptămână corespunzătoare primei zile din luna m a anului N este restul modulo 7 al lui $d_N + [2, 6m - 0, 2] - 2$.

În final, pentru stabilirea zilei W din săptămână corespunzătoare datei k din luna m a anului N, adunăm $k - 1$ în ultima relaţie. Formula care se obţine este:

$$W \equiv k + [2, 6m - 0, 2] - 2C + Y + \left[\frac{C}{4}\right] + \left[\frac{Y}{4}\right] \ (mod\ 7).$$

Ca exemplu, să determinăm ziua din săptămână corespunzătoare datei de 15 Februarie 2005. Atunci,
$k = 15$, $m = 12$, $N = 2004 = 100 \cdot 20 + 4$, de unde $C = 20$, $Y = 4$.
$W \equiv 15 + [2, 6 \cdot 12 - 0, 2] - 2 \cdot 20 + 4 + \left[\frac{20}{4}\right] + \left[\frac{4}{4}\right]$
$\equiv 15 + 31 - 40 + 4 + 5 + 1 \equiv 2\ (mod\ 7)$. Dacă verificăm în calendar, ziua luată ca exemplu a fost într-adevăr într-o zi de marţi.

5.4 Programarea unui turneu

Să vedem cum putem aplica congruenţele în programarea unui turneu.

Presupunem că există N echipe diferite care joacă într-un turneu astfel încât fiecare echipă joacă cu fiecare altă echipă o singură dată. Dacă N este impar, la fiecare etapă o echipă trebuie să nu joace. Atunci, în acest caz introducem o echipă *fictivă*, şi echipa care este programată să joace cu aceasta, de fapt, în runda aceea, stă.

Putem presupune astfel că numărul de echipe participante la turneu este mereu par. Notăm aceste echipe cu $1, 2, \ldots, N-1, N$.

Realizăm următoarea programare:
Fie echipa i cu $i \neq N$. Ea joacă cu echipa j unde $j \notin \{i, N\}$ în turul k dacă $i + j \equiv k \ (mod\ N-1)$. Am programat astfel toate jocurile din turul k mai puţin echipa N şi echipa i pentru care $2i \equiv k \ (mod\ N-1)$. Cum $N-1$ este impar, ultima congruenţă are soluţie unică x unde $1 \leq x \leq N-1$. Punem în joc, în turul k această echipă cu echipa N.

Arătăm că această programare este cea dorită. Pentru aceasta, considerăm iniţial primele $N-1$ echipe.
Pentru $1 \leq i \leq N-1$, echipa i joacă cu echipa N în turul k dacă $2i \equiv k \ (mod\ N-1)$. În alte runde, i nu joacă cu aceleaşi echipe, pentru că dacă $i + j \equiv k \ (mod\ N-1)$ şi $i + j \equiv k' \ (mod\ N-1)$, rezultă $k = k'$, ceea ce este fals.

Cum fiecare echipă din primele $N-1$ joacă $N-1$ jocuri şi nu joacă cu fiecare echipă mai mult decât o dată, obţinem că ele joacă fiecare o singură dată. Echipa N joacă $N-1$ jocuri şi orice altă echipă joacă cu N o singură dată. Deci, echipa N joacă cu fiecare echipă o singură dată.

Spre exemplu, să considerăm că în turneu participă 5 echipe. Atunci, $N = 6$ şi fiecare echipă care este programată să joace cu echipa 6 în fiecare tur, de fapt nu joacă în acel tur. Rezultatul programării este prezentat în tabelul următor:

*Tur**Echipă*	1	2	3	4	5
1	5	4	*stă*	2	1
2	*stă*	5	4	3	2
3	2	1	5	*stă*	3
4	3	*stă*	1	5	4
5	4	3	2	1	*stă*

Exerciţii propuse

1. Fie b şi $n > 2$, două numere prime între ele iar a, c numere naturale cu $d = (a, c)$. Dacă $b^a \equiv -1 \ (mod \ n)$ şi $b^c \equiv \pm 1 \ (mod \ n)$, atunci $b^d \equiv -1 \ (mod \ n)$ şi $\frac{n}{d}$ este număr impar.

2. Arătaţi că, dacă $p \mid b^n + 1$, cu p număr prim, atunci:

i) $p \mid b^d + 1$, pentru d, un divizor propriu al lui n cu $\frac{n}{d}$ număr impar sau

ii) $p \equiv 1 \ (mod \ 2n)$.

3. Fie $n = 2^{24} + 1 = 16777217$.

i) Găsiţi un număr prim Fermat care divide n.

ii) Arătaţi că orice alt divizor prim p al lui n verifică $p \equiv 1 \ (mod \ 48)$.

iii) Găsiţi descompunerea canonică în factori primi a lui n.

4. Descompuneţi în factori primi numerele următoare:

i) $3^{15} - 1, 3^{24} - 1$,

ii) $10^5 - 1, 10^8 - 1$,

iii) $2^{33} - 1, 2^{21} - 1$.

5. Fie $n = 111 \ldots 1$ un număr de k cifre. Stabiliţi ce condiţii trebuie impuse pentru ca:

i) n să fie divizibil cu 3, respectiv cu 9.

ii) n să fie divizibil cu 11.

iii) n să fie divizibil cu 1001.

iv) n să fie număr prim, dacă $k < 10$.

6. Stabiliţi un test de divizibilitate cu 37.

7. Fie n un număr scris în baza b. Stabiliţi un test de divizibilitate al lui n cu divizori ai lui $b^2 + 1$. Folosind testul găsit, verificaţi dacă $(12100122)_3$ este divizibil cu 2 sau cu 5.

8. Determinaţi ziua din săptămână în care v-aţi născut.

9. Realizaţi, după modelul prezentat, programarea unui turneu la care participă 9 echipe.

CAPITOLUL 6

Rădăcini primitive

6.1 Ordinul unui număr întreg

Fie n număr natural nenul şi $a \in \boldsymbol{Z}$, prim cu n. Din teorema lui Euler ştim că $a^{\phi(n)} \equiv 1 \ (mod \ n)$. Mulţimea numerelor naturale fiind bine ordonată, va exista un cel mai mic număr natural nenul k care să verifice relaţia $a^k \equiv 1 \ (mod \ n)$.

Definiţie 6.1.1 *Fie n număr natural şi $a \in \mathbf{Z}$, prim cu n. Cel mai mic număr natural nenul k pentru care $a^k \equiv 1 \ (mod \ n)$ se numeşte ordinul lui a modulo n şi îl vom nota $ord_n a$.*

De exemplu, din $4^2 \equiv 2 \ (mod \ 7)$, $4^3 \equiv 1 \ (mod \ 7)$, rezultă

$$ord_7 4 = 3.$$

În continuare, vom prezenta câteva proprietăţi de bază ale ordinului unui întreg. Cum majoritatea demonstraţiilor sunt simple, le vom lăsa ca exerciţiu pentru cititor.

Propoziţie 6.1.1 *Dacă a şi n sunt relativ prime, cu $n > 0$, atunci $k \in \mathbf{N}$ este soluţie a congruenţei $a^k \equiv 1 \ (mod \ n)$ dacă şi numai dacă $ord_n a \mid k$.*

De aici, obţinem un rezultat important care uşurează determinarea lui $ord_n a$.

Corolar 6.1.1 *Dacă n este număr natural nenul şi a este un întreg, prim cu n, atunci $ord_n a \mid \phi(n)$.*

Astfel, dacă dorim să determinăm $ord_7 3$, cum $\phi(7) = 6$, calculăm doar 3^k pentru $k \in \{1, 2, 3, 6\}$. Astfel:

$$3^1 \equiv 3 \ (mod\ 7) \quad 3^3 \equiv 6 \ (mod\ 7)$$
$$3^2 \equiv 2 \ (mod\ 7) \quad 3^6 \equiv 1 \ (mod\ 7)$$

Un rezultat des folosit în continuare este dat de următoarea propoziţie:

Propoziţie 6.1.2 *Fie n număr natural nenul şi $a \in \mathbf{Z}$, $(a, n) = 1$. Atunci, $a^i \equiv a^j \ (mod\ n)$ dacă şi numai dacă $i \equiv j \ (mod\ ord_n a)$.*

În continuare prezentăm un algoritm de determinare a ordinului unui număr natural a modulo n. Acesta presupune însă un inconvenient: pentru a putea să aplicăm algoritmul, trebuie să cunoaştem descompunerea în factori primi a lui $\phi(n)$.

Algoritm 6.1.1 (Ordinul unui număr natural)
INPUT: numerele naturale relativ prime a, n cu $\phi(n) = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$.
OUTPUT: $ord_n a = t$

1. *Pune $t \leftarrow \phi(n)$.*
2. *Pentru $i = 1, \dots, k$ execută:*
   - 2.1. *Pune $t \leftarrow t/p_i^{\alpha_i}$.*
   - 2.2. *Calculează $a_1 \leftarrow a^t \ mod\ n$*
   - 2.3. *Cât timp $a_1 \neq 1 \ mod\ n$, execută:*
     - 2.3.1. *Calculează $a_1 \leftarrow a_1^{p_i} \ mod\ n$*
     - 2.3.2. *Pune $t \leftarrow t \cdot p_i$*
3. *Returnează t.*

Un interes deosebit îl prezintă numerele cu ordinul modulo n egal cu $\phi(n)$.

Definiţie 6.1.2 *Dacă $(r, n) = 1$, cu $n > 0$, şi $ord_n r = \phi(n)$, atunci r se numeşte rădăcină primitivă modulo n.*

Spre exemplu, am arătat că 3 este rădăcină primitivă modulo 7.

Dar, trebuie să remarcăm că nu pentru toate numere n există rădăcini primitive. De exemplu, pentru $n = 8$, obţinem $3^2 \equiv 5^2 \equiv 7^2 \equiv 1 \ (mod\, 8)$. Astfel, $ord_8 3 = ord_8 5 = ord_8 7 = 2 \neq 4$.

Propoziţie 6.1.3 *Dacă r este rădăcină primitivă modulo n, atunci $r, r^2, \ldots, r^{\phi(n)}$ formează un sistem redus de resturi modulo n.*

Presupunem că un număr natural nenul n are o rădăcină primitivă. Pentru a stabili numărul total al acestora, avem nevoie de următoarea propoziţie:

Propoziţie 6.1.4 *Dacă $ord_n a = k$ şi $l > 0$ este un număr natural, atunci, $ord_n a^l = \dfrac{k}{(k,l)}$.*

Corolar 6.1.2 *Fie r o rădăcină primitivă modulo n. Atunci, r^k este rădăcină primitivă modulo n dacă şi numai dacă $(k, \phi(n)) = 1$.*

Teoremă 6.1.1 *Dacă n are o rădăcină primitivă, atunci are exact $\phi(\phi(n))$ rădăcini primitive.*

Demonstraţie. Fie r o rădăcină primitivă modulo n. Din propoziţia 6.1.3, $r, r^2, \ldots, r^{\phi(n)}$ este sistem redus de resturi modulo n. Conform corolarului 6.1.2, r^k este rădăcină primitivă modulo n dacă şi numai dacă $(k, \phi(n)) = 1$. Atunci, există $\phi(\phi(n))$ astfel de numere, deci tot atâtea rădăcini primitive modulo n. □

6.2 Existenţa rădăcinilor primitive

Definiţie 6.2.1 *Fie $f \in \mathbf{Z}[X]$, un polinom de grad ≥ 1. Spunem că x este o rădăcină a lui f modulo n, dacă $f(x) \equiv 0 \ (mod\ n)$.*

De exemplu, $f = X^2 + 2$ are două rădăcini necongruente modulo 3, pe $x \equiv 1 \ (mod\ 3)$ şi $x \equiv 2 \ (mod\ 3)$.

Teoremă 6.2.1 (Lagrange) *Fie $f = a_n X^n + a_{n-1} X^{n-1} + \ldots + a_1 X + a_0$, un polinom de grad $n \geq 1$ cu coeficienţi întregi şi p un număr prim cu $p \nmid a_n$. Atunci, f are cel mult n rădăcini necongruente modulo p.*

Demonstraţie[1]. Procedăm prin inducţie matematică după n. Pentru $n = 1$, $f = a_1X + a_0$. Cum $p \nmid a_1$, congruenţa $a_1x \equiv -a_0 \ (mod\ p)$ are o singură soluţie, care va fi şi rădăcina modulo p a lui f.

Presupunem afirmaţia adevărată pentru polinoame de grad $n-1$ şi arătăm că ea rămâne adevărată pentru polinoame de grad n.
Considerăm că un polinom f de grad n are $n+1$ rădăcini necongruente modulo p pe care le notăm $x_0, x_1, \ldots, x_n$. Atunci, pentru $0 \leq k \leq n$, $f(x_k) \equiv 0 \ (mod\ p)$.
Din $f(x)-f(x_0) = a_n\left(x^n - x_0^n\right)+a_{n-1}\left(x^{n-1} - x_0^{n-1}\right)+\ldots+a_1(x-x_0)$, obţinem că $f(x) = f(x_0)+(x-x_0)g(x)$, unde g este un polinom de grad $n-1$. Pentru $1 \leq k \leq n$, obţinem:

$$f(x_k) - f(x_0) \equiv (x_k - x_0)g(x_k) \equiv 0 \ (mod\ p).$$

De aici, cum fiecare $x_k - x_0 \neq 0 \ (mod\ p)$, rezultă $g(x_k) \equiv 0 \ (mod\ p)$. Deci, polinomul g care are gradul $n-1$, are n rădăcini necongruente modulo p. Cum acest rezultat contrazice ipoteza de inducţie, rezultă că presupunerea făcută este falsă. Deci, f are cel mult n rădăcini necongruente modulo p. □

Teoremă 6.2.2 *Fie p un număr prim şi $d \mid p-1$. Atunci, $X^d - 1$ are exact d rădăcini necongruente modulo p.*

Demonstraţie. Fie $p - 1 = de$. Atunci,

$$\begin{aligned} X^{p-1} - 1 &= \left(X^d - 1\right)\left(X^{d(e-1)} + X^{d(e-2)} + \ldots + X^d + 1\right) \\ &= \left(X^d - 1\right) g(X). \end{aligned}$$

Din mica teoremă a lui Fermat, $X^{p-1} - 1$ are $p-1$ rădăcini necongruente modulo p şi orice astfel de rădăcină este rădăcină pentru $X^d - 1$ sau pentru g. Conform teoremei Lagrange, g are cel mult $d(e-1) = p - d - 1$ rădăcini necongruente modulo p. Astfel, $X^d - 1$ are cel puţin

[1] Joseph-Louis Lagrange (1736-1813) a fost un autodidact, el neavând avantajul de a beneficia de sprijinul unor matematicieni contemporani lui. A obţinut rezultate importante în calculul variaţional, pe care l-a aplicat în mecanică, în calculul probabilităţilor, ecuaţiilor diferenţiale, astronomie, dinamică, mecanica fluidelor, în fundamentarea calculului în teoria numerelor. În anul 1770 a arătat că orice număr natural este o sumă de patru pătrate, în 1771 a demonstrat teorema lui Wilson. Se consideră că el a făcut primul pas în dezvoltarea teoriei grupurilor. Expresia sa favorită era *je ne sais pas*, fapt ce dovedeşte marea sa modestie.

$(p-1)-(p-d-1)=d$ rădăcini necongruente modulo p. Dacă aplicăm încă o dată teorema 6.2.1 pentru polinomul X^d-1, obţinem că el are cel mult d soluţii necongruente modulo p. Astfel, X^d-1 are exact d soluţii necongruente modulo p. □

Folosind acest rezultat, putem determina câte numere naturale necongruente au un ordin dat modulo p.

Teoremă 6.2.3 *Fie p un număr prim şi $d \mid p-1$. Atunci, numărul numerelor naturale de ordin d modulo p este egal cu $\phi(d)$.*

Demonstraţie. Pentru $d \mid p-1$, notăm cu $F(d)$ numărul numerelor naturale de ordin d modulo p, mai mici decât p.
Cum ordinul modulo p al unui număr care nu este multiplu de p divide $p-1$, obţinem $p-1=\sum_{d|p-1} F(d)$.
Din teorema 4.1.5, $p-1=\sum_{d|p-1}\phi(d)$.
Dacă arătăm că $F(d)\leq\phi(d)$, din $\sum_{d|p-1}\phi(d)=\sum_{d|p-1}F(d)$, va rezulta egalitatea $F(d)=\phi(d)$, pentru $d\mid p-1$.
Pentru aceasta, fie $d \mid p-1$. Dacă $F(d)=0$, atunci $F(d)\leq\phi(d)$. Presupunem că există a cu $ord_p a = d$. Atunci, $a, a^2, \ldots, a^d$ nu sunt congruente modulo p.
Din $(a^k)^d \equiv a^{kd} \equiv 1 \ (mod\ p)$, pentru $1\leq k\leq d$, rezultă că acestea sunt rădăcini modulo p ale polinomului X^d-1. Folosind propoziţia 6.1.4, $ord_p a^k = d$ dacă şi numai dacă $(k,d)=1$.
Deci, dacă există rădăcini de ordin d modulo p, ele sunt exact în număr de $\phi(d)$. Astfel $F(d)\leq\phi(d)$. □

Corolar 6.2.1 *Orice număr prim are rădăcini primitive.*

Demonstraţie. Fie p număr prim. Din teorema anterioară, există $\phi(p-1)$ numere necongruente modulo p, de ordin $p-1$. Cum fiecare dintre acestea este o rădăcină primitivă modulo p, obţinem că p are $\phi(p-1)$ rădăcini primitive. □

Teoremă 6.2.4 *Dacă p este un număr prim impar cu rădăcina primitivă r, atunci r sau $r+p$ este rădăcină primitivă modulo p^2.*

Demonstraţie. $ord_p r = \phi(p) = p-1$. Notăm $ord_{p^2} r = m$.
Din $r^m \equiv 1 \ (mod\ p^2)$, rezultă $r^m \equiv 1 \ (mod\ p)$, adică

$$p-1 \mid m. \tag{6.1}$$

Din corolarul 6.1.1, avem

$$m \mid \phi(p^2) = p(p-1). \tag{6.2}$$

Astfel, din (6.1) şi (6.2), rezultă $m = p-1$ sau $m = p(p-1)$.
Dacă $m = p(p-1)$, r este rădăcină primitivă modulo p^2.
Pentru $m = p-1$ arătăm că $t = r+p$ este rădăcină primitivă modulo p^2.
Pentru aceasta, observăm mai întâi că t este şi ea rădăcină primitivă modulo p, cum $t \equiv r \ (mod\ p)$. Din calculele făcute anterior, rezultă că $ord_{p^2} t = p-1$ sau $ord_{p^2} t = p(p-1)$. Pentru a încheia demonstraţia, arătăm că $ord_{p^2} t \neq p-1$.

$t^{p-1} = (r+p)^{p-1} = r^{p-1} + \sum_{j=1}^{p-2} C_{p-1}^{j} r^{p-j-1} p^j + p^{p-1}$
$\equiv r^{p-1} + (p-1)p \cdot r^{p-2} \equiv 1 + p(p-1)r^{p-2} \equiv 1 - p \cdot r^{p-2} \ (mod\ p^2)$.
Dacă $t^{p-1} \equiv 1 \ (mod\ p^2)$, atunci, $p \cdot r^{p-2} \equiv 0 \ (mod\ p^2)$, de unde
$r^{p-2} \equiv 0 \ (mod\ p)$, ceea ce este fals ($p \nmid r$). □

De exemplu, pentru $p = 7$, ştim că 3 este rădăcină primitivă. Cum $3^6 \equiv 43 \neq 1 \ (mod\ 49)$, 3 este rădăcină primitivă modulo 49.

Dacă considerăm acum $p = 487$, o rădăcină primitivă este 10. Din $10^{486} \equiv 1 \ (mod\ 487^2)$, rezultă că $10 + 487 = 497$ este rădăcină primitivă modulo 487^2.

Teoremă 6.2.5 *Fie p un număr prim impar. Atunci, există rădăcini primitive modulo p^k, pentru orice k număr natural.*

Mai mult, dacă r este o rădăcină primitivă modulo p^2, r este rădăcină primitivă modulo p^k, pentru orice $k \geq 2$.

Demonstraţie. Fie r o rădăcină primitivă modulo p, care este şi rădăcină primitivă modulo p^2. Atunci, din teorema 6.2.4, $r^{p-1} \neq 1 \ (mod\ p^2)$.

Arătăm, prin inducţie matematică, că, pentru orice $k \geq 2$:

$$r^{p^{k-2}(p-1)} \neq 1 \ (mod\ p^k). \tag{6.3}$$

Pentru $k = 2$, relaţia se verifică. Presupunem că ea este adevărată pentru $k > 2$ şi arătăm că ea rămâne adevărată pentru $k+1$.
Din $(r, p) = 1$, avem $(r, p^{k-1}) = 1$.
Aplicând teorema lui Euler, $r^{\phi(p^{k-1})} = r^{p^{k-2}(p-1)} \equiv 1 \ (mod\ p^{k-1})$.

Există astfel d, număr natural pentru care:

$$r^{p^{k-2}(p-1)} = 1 + d \cdot p^{k-1}. \tag{6.4}$$

Din, ipoteza de inducţie, $r^{p^{k-2}(p-1)} \neq 1 \ (mod\ p^k)$. De aici, rezultă că $p \nmid d$.

Ridicăm la puterea p în relaţia (6.4) şi obţinem

$$r^{p^{k-1}(p-1)} = (1 + d \cdot p^{k-1})^p \equiv 1 + d \cdot p^k \ (mod\ p^{k+1}). \tag{6.5}$$

Cum $p \nmid d$, rezultă $r^{p^{k-1}(p-1)} \neq 1 \ (mod\ p^{k+1})$.

Deci, pentru orice $k \geq 2$, $r^{p^{k-2}(p-1)} \neq 1 \ (mod\ p^k)$.

Notăm $m = ord_{p^k} r$. Atunci, $m \mid \phi(p^k) = p^{k-1}(p-1)$.
Din $r^m \equiv 1 \ (mod\ p^k)$, rezultă $r^m \equiv 1 \ (mod\ p)$. Deci, $p-1 \mid m$. Obţinem astfel $m = p^t(p-1)$ unde $0 \leq t \leq k-1$. Dacă $t \leq k-2$, atunci $r^{p^{k-2}(p-1)} = \left(r^{p^t(p-1)}\right)^{p^{k-2-t}} \equiv 1 \ (mod\ p^k)$. Această relaţie contrazice însă (6.3). Deci, $t = k-1$, de unde $m = \phi(p^k)$. □

Ca exemplu, 3 este rădăcină primitivă modulo 7^k, cu $k \geq 1$.

Să vedem ce putem preciza despre puterile lui 2. Se observă imediat că 1 este rădăcină primitivă modulo 2 iar 3 este rădăcină primitivă pentru 4.

Teoremă 6.2.6 *Dacă a este impar şi $k \geq 3$, atunci,*

$$a^{\frac{\phi(2^k)}{2}} = a^{2^{k-2}} \equiv 1 \ (mod\ 2^k).$$

Demonstraţie. Arătăm, prin inducţie, că afirmaţia se verifică pentru fiecare $k \geq 3$. Cum a este impar, putem scrie $a = 2m+1$, $m \in \boldsymbol{N}$.
Pentru $k = 3$, rezultă $a^2 = (2m+1)^2 = 4m(m+1) + 1 \equiv 1 \ (mod\ 8)$.
Presupunem că $a^{2^{k-2}} \equiv 1 \ (mod\ 2^k)$. Atunci, $a^{2^{k-2}} = 1 + 2^k \cdot d$, pentru un număr natural d.
De aici,
$a^{2^{k-1}} = \left(1 + 2^k \cdot d\right)^2 = 1 + d \cdot 2^{k+1} + 2^{2k} d^2 \equiv 1 \ (mod\ 2^{k+1})$. □

De fapt, teorema arată că, 2 şi 4 sunt singurele puteri ale lui 2 pentru care există rădăcini primitive.

Teoremă 6.2.7 *Fie $k \geq 3$. Atunci, $ord_{2^k} 5 = \frac{\phi(2^k)}{2} = 2^{k-2}$.*

Demonstraţie. Din teorema anterioară, $5^{2^{k-2}} \equiv 1 \ (mod\ 2^k)$, pentru $k \geq 3$. Astfel, $ord_{2^k} 5 \mid 2^{k-2}$. Rămâne să demonstrăm prin inducţie că, pentru $k \geq 3$, $5^{2^{k-3}} \equiv 1 + 2^{k-1} \neq 1 \ (mod\ 2^k)$, adică $ord_{2^k} 5 \nmid 2^{k-3}$.
Pentru $k = 3$, relaţia se verifică imediat.
Presupunem că $5^{2^{k-3}} \equiv 1 + 2^{k-1} \ (mod\ 2^k)$. Relaţia se poate scrie sub forma $5^{2^{k-3}} = (1 + 2^{k-1}) + d \cdot 2^k$. Ridicând la pătrat, rezultă:

$$\begin{aligned} 5^{2^{k-2}} &= \left((1 + 2^{k-1}) + d \cdot 2^k\right)^2 \\ &= (1 + 2^{k-1})^2 + (1 + 2^{k-1}) \cdot d \cdot 2^{k+1} + d^2 \cdot 2^{2k} \\ &\equiv (1 + 2^{k-1})^2 \equiv 1 + 2^k \ (mod\ 2^{k+1}). \quad \square \end{aligned}$$

Teoremă 6.2.8 *Fie n un număr natural care nu este de forma $n = p^k$ sau $n = 2p^k$, unde p este număr prim impar şi k natural. Atunci, nu există rădăcini primitive modulo n.*

Demonstraţie. Fie $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_m^{\alpha_m}$. Presupunem că există r rădăcină primitivă modulo n. Atunci, $(r, n) = 1$ şi $ord_n r = \phi(n)$.
Cum, pentru fiecare $1 \leq j \leq m$, $(r, p_j^{\alpha_j}) = 1$, din teorema lui Euler, avem $r^{\phi(p_j^{\alpha_j})} \equiv 1 \ (mod\ p_j^{\alpha_j})$. Notăm

$$U = \left[\phi(p_1^{\alpha_1}), \phi(p_2^{\alpha_2}), \dots, \phi(p_m^{\alpha_m})\right]. \tag{6.6}$$

De aici, $r^U \equiv 1 \ (mod\ p_j^{\alpha_j})$, pentru orice $1 \leq j \leq m$. Rezultă astfel,

$$ord_n r = \phi(n) = \phi(p_1^{\alpha_1}) \cdot \phi(p_2^{\alpha_2}) \cdot \ldots \cdot \phi(p_m^{\alpha_m}) \leq U. \tag{6.7}$$

Pentru ca produsul unor numere să fie mai mic decât cel mai mic multiplu comun al acestora, numerele trebuie să fie două câte două relativ prime. Deci, pentru $1 \leq i < j \leq m$,

$$\left(\phi(p_i^{\alpha_i}), \phi(p_j^{\alpha_j})\right) = 1. \tag{6.8}$$

Pentru un număr prim p, $\phi(p^t) = p^{t-1}(p-1)$. Acest număr este par dacă p este impar sau dacă $p = 2$ şi $t \geq 2$.
De aici, pentru a se verifica (6.8), în descompunerea lui n trebuie să existe un singur factor prim impar şi, eventual, un 2. Deci $n = p^t$ sau $n = 2p^t$ cu p prim impar şi t natural. $\square$

Teoremă 6.2.9 *Fie p un număr prim impar şi k un număr natural. Atunci, există rădăcini primitive modulo $2p^k$. Mai mult, dacă r este o rădăcină primitivă modulo p^k, atunci r este rădăcină primitivă modulo $2p^k$ dacă r este număr impar. În caz contrar, $r + p^k$ va fi o rădăcină primitivă modulo $2p^k$.*

Demonstraţie. Fie r o rădăcină primitivă modulo p^k.
Atunci, din $r^{\phi(p^k)} \equiv 1 \ (mod\ p^k)$ şi $\phi(2p^k) = \phi(p^k)$, obţinem

$$r^{\phi(2p^k)} \equiv 1 \ (mod\ p^k). \tag{6.9}$$

Dacă r este impar,

$$r^{\phi(2p^k)} \equiv 1 \ (mod\ 2). \tag{6.10}$$

Din (6.9) şi (6.10), rezultă

$$r^{\phi(2p^k)} \equiv 1 \ (mod\ 2p^k). \tag{6.11}$$

Pentru $t < \phi(2p^k)$, $r^t \neq 1 \ (mod\ 2p^k)$ şi obţinem astfel:

$$ord_{2p^k} r = \phi(2p^k).$$

Dacă r este par, $r + p^k$ este număr impar. Astfel,

$$(r + p^k)^{\phi(2p^k)} \equiv 1 \ (mod\ 2). \tag{6.12}$$

Din $r \equiv r + p^k \ (mod\ p^k)$, avem

$$(r + p^k)^{\phi(2p^k)} \equiv 1 \ (mod\ p^k). \tag{6.13}$$

Ultimele două relaţii, arată că

$$(r + p^k)^{\phi(2p^k)} \equiv 1 \ (mod\ 2p^k). \tag{6.14}$$

Cum $\phi(2p^k)$ este cea mai mică putere pentru care (6.14) se verifică, rezultă că $r + p^k$ este, în acest caz, rădăcină primitivă modulo $2p^k$. □

De exemplu, ştim că $r = 3$ este rădăcină primitivă modulo 7^k, pentru k natural. Atunci, cum r este impar, 3 rămâne rădăcină primitivă modulo $2 \cdot 7^k$.

La fel, 2 este rădăcină primitivă modulo 5. $2^4 \equiv 16 \neq 1 \ (mod\ 25)$. Deci, 2 este rădăcină primitivă pentru 25. Fiind număr par, $2 + 5^k$ este o rădăcină primitivă modulo $2 \cdot 5^k$.

Toate rezultatele oferite în acest subcapitol pot fi reunite într-unul singur care să stabilească exact modulele pentru care există rădăcini primitive:

Teoremă 6.2.10 *Există rădăcini primitive modulo n dacă şi numai dacă $n \in \{2, 4, p^k, 2p^k\}$ unde p este prim impar şi k număr natural.*

Observaţie 6.2.1 *Dacă ţinem cont că $U(\mathbf{Z}_n)$, grupul unităţilor lui $\mathbf{Z}_n$, are ordinul $\phi(n)$, existenţa unei rădăcini primitive modulo n este echivalentă cu cea a unui generator pentru grupul $U(\mathbf{Z}_n)$. Deci, există rădăcini primitive modulo n dacă şi numai dacă $U(\mathbf{Z}_n)$ este grup ciclic.*

Prezentăm în final un algoritm de determinare a unui generator pentru un grup ciclic de ordin $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$.

Algoritm 6.2.1 (Generatorul unui grup ciclic)
INPUT: $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, *ordinul grupului.*
OUTPUT: a, *generatorul grupului.*

1. *Alege aleator a un element al grupului.*
2. *Pentru $i = 1, \dots, k$ execută:*
   - 2.1. *Calculează $b \leftarrow a^{n/p_i}$.*
   - 2.2. *Dacă $b = 1$, mergi la pasul 1.*
3. *Returnează a.*

6.3 Index aritmetic

Fie r o rădăcină primitivă modulo n.
Conform propoziţiei 6.1.3, $r, r^2, \dots, r^{\phi(n)}$ este un sistem redus de resturi modulo n.
Atunci, pentru orice întreg a, prim cu n, există un unic $1 \leq x \leq \phi(n)$ astfel încât $a \equiv r^x \ (mod\ n)$.

Definiţie 6.3.1 *Fie r o rădăcină primitivă modulo n şi a, număr natural prim cu n.*
Numărul natural $1 \leq x \leq \phi(n)$ pentru care $a \equiv r^x \ (mod\ n)$ se numeşte indexul lui a în baza r modulo n şi îl vom nota $ind_r a$.

Deci,

$$a \equiv r^{ind_r a} \ (mod\ n) \tag{6.15}$$

Mai observăm că pentru $a \equiv b\ (mod\ n)$, obţinem $ind_r a = ind_r b$.

De exemplu, pentru $r = 3$ rădăcină primitivă modulo $n = 7$, avem:

$3^1 \equiv 3\ (mod\ 7)$ $\quad 3^4 \equiv 4\ (mod\ 7)$
$3^2 \equiv 2\ (mod\ 7)$ $\quad 3^5 \equiv 5\ (mod\ 7)$
$3^3 \equiv 6\ (mod\ 7)$ $\quad 3^6 \equiv 1\ (mod\ 7)$

Obţinem:

a	1	2	3	4	5	6
$ind_3 a$	6	2	1	4	5	3

Mai trebuie remarcat faptul că o schimbare a rădăcinii primitive conduce la modificarea valorii indexului. Astfel, cum 5 este cealaltă rădăcină primitivă modulo 7, tabela de index modulo 7 devine:

a	1	2	3	4	5	6
$ind_5 a$	6	4	5	2	1	3

Propoziţie 6.3.1 *Fie r o rădăcină primitivă modulo n şi a, b două numere naturale, prime cu n. Atunci, următoarele afirmaţii sunt adevărate:*

1) $ind_r 1 \equiv 0\ (mod\ \phi(n))$.

2) $ind_r(ab) \equiv ind_r a + ind_r b\ (mod\ \phi(n))$.

3) $ind_r a^k \equiv k \cdot ind_r a\ (mod\ \phi(n))$.

Demonstraţie. 1) r fiind rădăcină primitivă modulo n, $ord_n r = \phi(n)$. Astfel, $r^{\phi(n)} \equiv 1\ (mod\ n)$ şi $\phi(n)$ este cea mai mică putere pentru care se verifică congruenţa. Deci, $ind_r 1 = \phi(n) \equiv 0\ (mod\ \phi(n))$.
2) Din (6.15), $ab \equiv (r)^{ind_r(ab)}\ (mod\ n)$. Dar,

$$r^{ind_r a + ind_r b} = r^{ind_r a} \cdot r^{ind_r b} \equiv ab\ (mod\ n).$$

Rezultă astfel, $r^{ind_r(ab)} \equiv r^{ind_r a + ind_r b}\ (mod\ n)$ şi, aplicând propoziţia 6.1.2, $ind_r(ab) \equiv ind_r a + ind_r b\ (mod\ \phi(n))$.
3) se demonstrează asemănător cu subpunctul 2). □

O primă aplicaţie a indexului constă în rezolvarea unor tipuri de congruenţe. De exemplu, să considerăm pentru început congruenţa:

$$3x^{14} \equiv 2 \ (mod\ 23).$$

23 este număr prim, deci există rădăcini primitive modulo 23. Cum $5^{11} \equiv -1 \ (mod\ 23)$, $ord_{23}5 = 22$. Deci, 5 este rădăcină primitivă modulo 23.
Scriem tabela de index modulo 23 relativ la această rădăcină primitivă:

a	1	2	3	4	5	6	7	8	9	10	11
$ind_5 a$	22	2	16	4	1	18	19	6	10	3	9

a	12	13	14	15	16	17	18	19	20	21	22
$ind_5 a$	20	14	21	17	8	7	12	15	5	13	11

Congruenţa devine $ind_5(3 \cdot x^{14}) \equiv ind_5 2 \ (mod\ 22)$.
Folosind propoziţia 6.3.1, rezultă $ind_5 3 + 14 \cdot ind_5 x \equiv 2 \ (mod\ 22)$. Deci, $16 + 14 \cdot ind_5 x \equiv 2 \ (mod\ 22)$. Obţinem $14 \cdot ind_5 x \equiv 8 \ (mod\ 22)$, de unde $7 \cdot ind_5 x \equiv 4 \ (mod\ 11)$. Înmulţim congruenţa cu $\bar{7} \equiv 8 \ (mod\ 11)$ şi rezultă $ind_5 x \equiv 10 \ (mod\ 11)$. Deci, $ind_5 x = 10$ sau $ind_5 x = 21$. Atunci, din tabela de index rezultă direct $x \equiv 9 \ (mod\ 23)$ şi $x \equiv 14 \ (mod\ 23)$.

Să rezolvăm acum o congruenţă de forma:

$$3^x \equiv 2 \ (mod\ 23).$$

Congruenţa este echivalentă cu $ind_5(3^x) \equiv ind_5 2 \ (mod\ 22)$, adică $x \cdot ind_5 3 \equiv 2 \ (mod\ 22)$. Din $16 \cdot x \equiv 2 \ (mod\ 22)$ obţinem:
$8 \cdot x \equiv 1 \ (mod\ 11)$, deci $x \equiv 7 \ (mod\ 11)$. Putem scrie această soluţie şi sub forma $x \equiv 7 \ (mod\ 23)$, $x \equiv 18 \ (mod\ 23)$.

Să studiem acum congruenţele de forma

$$x^k \equiv a \ (mod\ n) \tag{6.16}$$

unde a, n, k sunt numere naturale, există rădăcini primitive modulo n iar a şi n sunt relativ prime.

Definiţie 6.3.2 *Cu notaţiile anterioare, spunem că a este $k-$putere reziduală a lui n dacă congruenţa (6.16) are soluţii.*

Teoremă 6.3.1 *Congruenţa (6.16) are soluţii dacă şi numai dacă*

$$a^{\frac{\phi(n)}{d}} \equiv 1 \ (mod\ n),$$

unde $d = (k, \phi(n))$. *Mai mult, dacă congruenţa are soluţii, există exact* d *soluţii necongruente modulo* n.

Demonstraţie. Fie r o rădăcină primitivă modulo n. Congruenţa (6.16) este echivalentă cu

$$k \cdot ind_r x \equiv ind_r a \ (mod\ \phi(n)). \tag{6.17}$$

Din teorema 3.2.1, această congruenţă are soluţii dacă şi numai dacă $d \mid ind_r a$ unde $d = (k, \phi(n))$ şi, în acest caz, sunt d soluţii necongruente. Dar,
$d \mid ind_r a \Leftrightarrow \phi(n) \cdot \frac{ind_r a}{d} = \frac{\phi(n)}{d} \cdot ind_r a \equiv 0 \ (mod\ \phi(n)) \Leftrightarrow a^{\frac{\phi(n)}{d}} \equiv$
$\left(r^{ind_r a}\right)^{\frac{\phi(n)}{d}} \equiv \left(r^{\phi(n)}\right)^{\frac{ind_r a}{d}} \equiv 1 \ (mod\ n).$ □

Observaţie 6.3.1 *Teorema arată că, pentru* p *număr prim,* k *natural şi* a *prim cu* p, a *este* $k-$*putere reziduală a lui* p *dacă şi numai dacă*

$$a^{\frac{p-1}{d}} \equiv 1 \ (mod\ p),$$

unde $d = (k, p-1)$.

6.4 Exponenţi universali

Dacă revedem demonstraţia teoremei 6.2.8, observăm că, pentru un număr natural n şi pentru orice a prim cu n,

$$a^U \equiv 1 \ (mod\ n),$$

unde U este cel definit în relaţia (6.6).

La fel, din teorema lui Euler, $a^{\phi(n)} \equiv 1 \ (mod\ n)$, pentru orice a cu $(a, n) = 1$.

Definiţie 6.4.1 *Un exponent universal al lui* n *este un număr natural* e *cu proprietatea că* $a^e \equiv 1 \ (mod\ n)$, *pentru orice* a *prim cu* n.

Deci, U şi $\phi(n)$ sunt exponenţi universali ai lui n.

Definiţie 6.4.2 *Cel mai mic exponent universal al lui n poartă numele de exponent universal minimal şi îl notăm* $\lambda(n)$.

Folosind descompunerea în factori primi a lui n, să căutăm o formulă pentru a determina $\lambda(n)$.

Este evident că, dacă n are o rădăcină primitivă, atunci $\lambda(n) = \phi(n)$.

Astfel, teorema 6.2.10 precizează că:
$\lambda(2 \cdot p^k) = \lambda(p^k) = \phi(p^k)$, pentru p prim impar şi k natural,
$\lambda(2) = \phi(2) = 1$,
$\lambda(4) = \phi(4) = 2$.

Din teoremele 6.2.6 şi 6.2.7 ştim că $a^{2^{k-2}} \equiv 1 \ (mod\ 2^k)$, pentru $k \geq 3$, a impar şi $ord_{2^k} 5 = 2^{k-2}$. Astfel, $\lambda(2^k) = 2^{k-2}$, pentru $k \geq 3$.

Teoremă 6.4.1 *Fie* $n = 2^{k_0} p_1^{k_1} \dots p_m^{k_m}$, *unde* p_i *sunt numere prime impare distincte şi* $k_i \geq 1$. *Atunci,*

$$\lambda(n) = \left[\lambda(2^{k_0}), \phi(p_1^{k_1}), \dots \phi(p_m^{k_m})\right].$$

În plus, există a, *prim cu* n, *al cărui ordin să fie egal cu* $\lambda(n)$, *cel mai mare ordin posibil modulo* n.

Demonstraţie. Fie a prim cu n. Din teorema 6.2.6, $a^{\lambda(2^{k_0})} \equiv 1 \ (mod\ 2^{k_0})$.
Cum $(a, p_i^{k_i}) = 1$, $a^{\phi(p_i^{k_i})} \equiv 1 \ (mod\ p_i^{k_i})$, pentru fiecare i.

Notăm $M = \left[\lambda(2^{k_0}), \phi(p_1^{k_1}), \dots \phi(p_m^{k_m})\right]$.
Din $\lambda(2^{k_0}) \mid M$ şi $\phi(p_i^{k_i}) = \lambda(p_i^{k_i}) \mid M$, pentru $1 \leq i \leq m$, rezultă

$$a^M \equiv 1 \ (mod\ n).$$

Am arătat astfel că M este exponent universal. Să arătăm că el este şi minimal.
Pentru aceasta, găsim un număr a cu proprietatea că $a^t \neq 1 \ (mod\ n)$, pentru $t < M$. Acest a va fi elementul de ordin maxim modulo n.
Notăm cu r_i o rădăcina primitivă modulo $p_i^{k_i}$, $1 \leq i \leq m$ şi considerăm sistemul de congruenţe:

$$\begin{cases} x \equiv 3 \ (mod\ 2^{k_0}) \\ x \equiv r_1 \ (mod\ p_1^{k_1}) \\ \vdots \\ x \equiv r_m \ (mod\ p_m^{k_m}) \end{cases}$$

Folosind teorema chinezească a resturilor, există o soluţie unică a, modulo $2^{k_0}p_1^{k_1}\dots p_m^{k_m} = n$. Arătăm că $ord_n a = M$.
Fie t pentru care $a^t \equiv 1 \ (mod\ n)$. Atunci, $a^t \equiv 1 \ (mod\ 2^{k_0})$ şi, pentru fiecare i, $a^t \equiv 1 \ (mod\ p_i^{k_i})$. Dar, a este soluţie a sistemului.
Obţinem $ord_{2^{k_0}} a = \lambda(2^{k_0})$, $ord_{p_i^{k_i}} a = \lambda(p_i^{k_i})$, cu $1 \leq i \leq m$. Deci, $\lambda(2^{k_0}) \mid t$ şi fiecare $\phi(p_i^{k_i}) \mid t$. Atunci, $M \mid t$. De aici, $ord_n a = M$. □

Să aplicăm această teoremă pentru $n = 100$.
$\lambda(100) = \left[\lambda(2^2), \lambda(5^2)\right] = [2, 20] = 20$. Pentru a determina elementul de ordin 20 modulo 100, rezolvăm sistemul:

$$\begin{cases} x \equiv 3 \ (mod\ 4) \\ x \equiv 2 \ (mod\ 25) \end{cases}$$

folosind teorema chinezească a resturilor. Rezultă $a \equiv 27 \ (mod\ 100)$.

Algoritm 6.4.1 (Element de ordin maxim modulo $n = pq$)
INPUT: p, q *numere prime impare.*
OUTPUT: a, *cu* $ord_n a = [p-1, q-1]$.

1. Foloseşte algoritmul 6.2.1 pentru a găsi α o rădăcină primitivă mod p.
2. Foloseşte algoritmul 6.2.1 pentru a găsi β o rădăcină primitivă mod q.
3. Aplică algoritmul 3.3.1 pentru a găsi $1 \leq a \leq n$ soluţia sistemului $x \equiv \alpha \ (mod\ p)$, $x \equiv \beta \ (mod\ q)$.
4. Returnează a.

Observaţie 6.4.1 *Exponentul universal minimal, $\lambda(n)$, îşi găseşte aplicaţii în unele metode de generare a numerelor pseudo-aleatoare. Aceste metode creează un şir de numere, pornind de la un număr ales iniţial, numit generator. Şirurile obţinute astfel, nu sunt aleatoare, ele fiind obţinute în mod metodic, după o anumită regulă (de exemplu, metoda congruenţei liniare, metoda celor mai mici pătrate). De aceea ele se numesc pseudo-aleatoare. Cel mai mare dezavantaj în generarea de numere pseudo-aleatoare prin aceste metode, este că, în funcţie de alegerea*

generatorului, pot rezulta şiruri cu un număr redus de numere, care se repetă mereu. Din acest motiv se urmăreşte ca lungimea maximă a şirului fără repetiţie, numită lungimea perioadei, să fie cât mai mare. Ea este dată de $\lambda(n)$.

Definiţie 6.4.3 *Fie* $n > 0$, *natural şi* a, *prim cu* n. *Cel mai mic număr natural* x *pentru care* $a^x \equiv \pm 1 \ (mod\ n)$, *se numeşte* $\pm 1-$*exponentul lui* a *modulo* n.

Vrem să determinăm, pentru fiecare n, cel mai mare $\pm 1-$exponent posibil, pe care îl vom nota $\lambda_0(n)$ şi îl numim $\pm 1-$*exponent maximal* al lui n. Din definiţie, toţi $\pm 1-$exponenţii modulo n sunt $\leq \lambda(n)$.

Începem, ca şi înainte, cu situaţia în care există o rădăcină primitivă modulo n.

Teoremă 6.4.2 *Pentru* $n > 2$, *cu proprietatea că există rădăcini primitive modulo* n,

$$\lambda_0(n) = \frac{\phi(n)}{2} = \frac{\lambda(n)}{2}.$$

Demonstraţie. Fie r o rădăcină primitivă modulo n.
Atunci, $\lambda(n) = \phi(n)$. Cum, în acest cax, $\phi(n)$ este număr par, $\frac{\lambda(n)}{2} \in \boldsymbol{N}$.
Folosind teorema lui Euler, $a^{\phi(n)} = \left(a^{\frac{\phi(n)}{2}}\right)^2 \equiv 1 \ (mod\ n)$, pentru $(a, n) = 1$. De aici, $a^{\frac{\phi(n)}{2}} \equiv \pm 1 \ (mod\ n)$, adică $\lambda_0(n) \leq \frac{\phi(n)}{2}$.
Notăm cu e_1 $\pm 1-$exponentul lui r modulo n. Atunci, $r^{e_1} \equiv \pm 1 \ (mod\ n)$, de unde $r^{2e_1} \equiv 1 \ (mod\ n)$. Astfel, $ord_n r = \phi(n) \mid 2e_1$, sau $\frac{\phi(n)}{2} \mid e_1$.
$\lambda_0(n)$ este cel mai mare $\pm 1-$exponent modulo n, deci $e_1 \leq \lambda_0(n)$. Rezultă astfel că $\frac{\phi(n)}{2} \leq \lambda_0(n)$, de unde obţinem, în final, egalitatea dorită. □

Lemă 6.4.1 *Fie* n *cu proprietatea că nu există rădăcini primitive modulo* n *şi fie* a, *un număr natural prim cu* n, *cu* $ord_n a = \lambda(n)$.
Presupunem că a *verifică* $a^{\frac{\lambda(n)}{2}} \neq -1 \ (mod\ n)$. *Atunci,* $\pm 1-$*exponentul lui* a *modulo* n *este egal cu* $\lambda(n)$.

Demonstraţie. Notăm $\pm 1-$exponentul lui a modulo n cu e_a. Astfel, $a^{e_a} \equiv \pm 1 \ (mod\ n)$. Cum $ord_n a = \lambda(n)$ şi $a^{2e_a} \equiv 1 \ (mod\ n)$, avem $\lambda(n) \mid 2e_a$. Din $e_a \leq \lambda(n)$, obţinem $e_a = \dfrac{\lambda(n)}{2}$ sau $e_a = \lambda(n)$.

Pentru $e_a = \dfrac{\lambda(n)}{2}$, avem $a^{\frac{\lambda(n)}{2}} \equiv \pm 1 \ (mod\ n)$. Din ipoteză, $a^{\frac{\lambda(n)}{2}} \neq -1 \ (mod\ n)$. $ord_n a = \lambda(n)$ implică $a^{\frac{\lambda(n)}{2}} \neq 1 \ (mod\ n)$. Deci, acest caz nu este posibil şi obţinem $e_a = \lambda(n)$. □

Teoremă 6.4.3 *Dacă nu există rădăcini primitive modulo n, atunci,*

$$\lambda_0(n) = \lambda(n).$$

Demonstraţie. Folosind rezultatul lemei anterioare, pentru a demonstra teorema trebuie doar să găsim un număr a care verifică condiţiile acestei leme.
Fie $n = 2^{k_0} p_1^{k_1} \dots p_m^{k_m}$. Considerăm mai multe cazuri:

1) n are cel puţin doi factori primi impari diferiţi.
Descompunem în factori primi $\phi(p_i^{k_i})$ pentru $1 \leq i \leq m$. Vom nota cu j, indicele pentru care exponentul lui 2 în aceste descompuneri este minim. Fie r_i o rădăcină primitivă modulo $p_i^{k_i}$, $1 \leq i \leq m$. Fie a soluţia sistemului:

$$\begin{cases} x \equiv 3 \ (mod\ 2^{k_0}) \\ x \equiv r_i \ (mod\ p_i^{k_i}) \quad \forall i \neq j \\ x \equiv r_j^2 \ (mod\ p_j^{k_j}) \end{cases}$$

Din teorema 6.4.1,

$$ord_n a = \left[\lambda(2^{k_0}), \phi(p_1^{k_1}), \dots, \frac{\phi(p_j^{k_j})}{2}, \dots, \phi(p_m^{k_m}) \right].$$

Din alegerea lui j, $\left[\lambda(2^{k_0}), \phi(p_1^{k_1}), \dots, \dfrac{\phi(p_j^{k_j})}{2}, \dots, \phi(p_m^{k_m}) \right] = \lambda(n)$.

Din $a \equiv r_j^2 \ (mod\ p_j^{k_j})$, obţinem $a^{\frac{\phi(p_j^{k_j})}{2}} \equiv r_j^{\phi(p_j^{k_j})} \equiv 1 \ (mod\ p_j^{k_j})$. Dar, $\dfrac{\phi(p_j^{k_j})}{2} \mid \dfrac{\lambda(n)}{2}$. Astfel, $a^{\frac{\lambda(n)}{2}} \equiv 1 \neq -1 \ (mod\ n)$. Deci, am găsit a care verifică condiţiile lemei 6.4.1.

2) $n = 2^{k_0} p^k$ cu p prim impar, $k > 0$, $k_0 \geq 2$.
Dacă $k_0 = 2$ sau 3, $\lambda(n) = \left[2, \phi(p^k)\right] = \phi(p^k)$. Fie a soluţia sistemului

$$\begin{cases} x \equiv 1 \ (mod\ 4) \\ x \equiv r \ (mod\ p^k) \end{cases}$$

unde r este rădăcină primitivă modulo p^k. Rezultă $ord_n a = \lambda(n)$. Din $a \equiv 1 \ (mod\ 4)$, $a^{\frac{\lambda(n)}{2}} \equiv 1 \ (mod\ 4)$ şi rezultă că $a^{\frac{\lambda(n)}{2}} \neq -1 \ (mod\ n)$. Astfel, $\pm 1-$exponentul lui a modulo n este $\lambda(n)$.
Dacă $k_0 \geq 4$, alegem a ca fiind soluţia sistemului

$$\begin{cases} x \equiv 3 \ (mod\ 2^{k_0}) \\ x \equiv r \ (mod\ p^k) \end{cases} .$$

Obţinem $ord_n a = \lambda(n)$. Din $4 \mid \lambda(2^{k_0})$, rezultă $4 \mid \lambda(n)$.
Atunci,
$a^{\frac{\lambda(n)}{2}} \equiv 3^{\frac{\lambda(n)}{2}} \equiv (3^2)^{\frac{\lambda(n)}{4}} \equiv 1 \ (mod\ 8)$ şi astfel, $a^{\frac{\lambda(n)}{2}} \neq -1 \ (mod\ n)$. Folosind lema 6.4.1, rezultă $e_a = \lambda(n)$.

3) $n = 2^{k_0}$, $k_0 \geq 3$.
Din teorema 6.2.7, $ord_n 5 = \lambda(n)$. Din $5^{\frac{\lambda(n)}{2}} \equiv (5^2)^{\frac{\lambda(n)}{4}} \equiv 1 \ (mod\ 8)$, rezultă $5^{\frac{\lambda(n)}{2}} \neq -1 \ (mod\ n)$, deci $a = 5$ verifică condiţiile lemei. □

Să vedem cum se utilizează $\pm 1-$exponentul maximal $\lambda_0(n)$ în procesul de îmbinare a cablurilor telefonice.

Cablurile telefonice sunt formate din mai multe straturi concentrice de fire izolate din cupru. Liniile telefonice se construiesc prin îmbinarea secţiunilor de cablu. Dacă două fire din acelaşi strat devin adiacente în mai multe secţiuni, apar probleme de interferenţă şi de suprapuneri de convorbiri. Din acest motiv, două fire adiacente din acelaşi strat într-o secţiune, nu trebuie să fie adiacente, în acelaşi strat, în orice secţiune apropiată. De asemenea, modalitatea de a realiza acest lucru trebuie să fie simplă, ţinând cont de mediul în care se realizează aceste îmbinări.

Pentru îmbinarea cablurilor, vom aplica următoarea regulă:
Firele dintr-un strat concentric sunt îmbinate cu fire din stratul corespunzător al secţiunii următoare, folosind aceeaşi direcţie de îmbinare la fiecare joncţiune. Presupunem că stratul are n fire şi conectăm firul aflat pe poziţia j, $1 \leq j \leq n$, dintr-o secţiune cu cel de pe poziţia $S(j)$ din secţiunea următoare. $S(j)$ se defineşte ca fiind restul modulo n al lui $1 + (j-1)s$, unde s poartă numele de *întinderea* sistemului de îmbinare. Astfel, de fapt, se îmbină firul j cu cel care se află cu s modulo n poziţii mai departe (în sensul convenit) din secţiunea următoare.

Corespondenţa definită trebuie să fie bijectivă, adică:
dacă $S(j) \equiv S(k) \ (mod\ n)$, atunci $j = k$, $1 \leq j, k \leq n$. Înlocuind, rezultă congruenţa $js \equiv ks \ (mod\ n)$ care trebuie să implice $j = k$. Deci, $(s, n) = 1$.

Notăm cu $S_t(j)$ firul cu care este îmbinat în secţiunea t firul iniţial j, din prima secţiune.
Aplicând metoda inducţiei matematice, se obţine uşor că

$$S_t(j) \equiv 1 + (j-1)s^{t-1} \ (mod\ n).$$

Pentru a fi îndeplinită regula precizată iniţial, trebuie ca firele adiacente să fie separate în cât mai multe secţiuni posibile. Presupunem că firele j şi $j+1$ sunt adiacente în a $t-$a secţiune făcută. Atunci,
$S_t(j) - S_t(j+1) \equiv \pm 1 \ (mod\ n)$, adică $s^{t-1} \equiv \pm 1 \ (mod\ n)$.

Deci, pornind de la două fire adiacente în prima secţiune, pentru a le păstra cât mai mult separate, trebuie să alegem întinderea s care are $\pm 1-$ exponentul maximal $\lambda_0(n)$.

De exemplu, dacă $n = 100$, $\lambda_0(100) = \lambda(100) = 20$ iar $s = 27$ a fost calculat anterior.

Exerciţii propuse

1. Determinaţi $ord_{10}3, ord_{13}10, ord_{17}9$.

2. Determinaţi toate rădăcinile primitive modulo 13.

3. Fie $n \in \{4, 8, 10, 18, 19, 25, 98, 100, 343, 1001\}$. Precizaţi pentru ce valori ale lui n există rădăcini primitive modulo n.

4. Determinaţi o rădăcină primitivă modulo n, dacă

$$n \in \{22, 26, 121, 169\}.$$

5. Fie n un număr natural pentru care există r, o rădăcină primitivă. Folosind această rădăcină, arătaţi că produsul numerelor mai mici decât n şi relativ prime cu n este congruent cu -1 modulo n.

6. Determinaţi toate soluţiile următoarelor congruenţe:

i) $3x^5 \equiv 1 \ (mod\ 23)$.

ii) $13^x \equiv 5 \ (mod\ 23)$.

7. Pentru ce numere naturale a congruenţa $ax^4 \equiv 2 \ (mod\ 13)$ are soluţii?

8. Fie congruenţa $8x^7 \equiv a \ (mod\ 29)$. Stabiliţi toate valorile lui a pentru ca această congruenţă să aibă soluţie.

9. Fie r o rădăcină primitivă modulo p, cu p număr prim impar. Arătaţi că $ind_r(p-1) = \frac{p-1}{2}$.

10. Calculaţi $\lambda(n)$ şi $\pm 1-$exponentul maximal pentru

$$n \in \{11, 17, 22, 36, 38, 120, 144, 222\}.$$

11. Fie $n \in \{12, 15, 36, 47\}$. Determinaţi un număr al cărui ordin modulo n este cel mai mare posibil.

12. Fie $n \in \{13, 14, 15, 25, 30\}$. Determinaţi un număr a al cărui $\pm 1-$exponent modulo n este egal cu $\lambda_0(n)$.

CAPITOLUL 7

Reciprocitate pătratică

Diofante, în *Arithmetica*, a făcut următoarea afirmaţie care a fost punctul de plecare pentru obţinerea rezultatului cunoscut sub numele de *legea reciprocităţii pătratice*:

65 se scrie în mod natural ca sumă de două pătrate, adică $7^2 + 4^2$ *şi* $8^2 + 1^2$*, datorită faptului că* $65 = 13 \cdot 5$ *iar fiecare dintre factori este sumă de două pătrate.*

Evident, Diofante cunoştea formula

$$(a^2 + b^2)(c^2 + d^2) = (ac \pm bd)^2 + (bc \mp ad)^2$$

care arată că un produs de sume de două pătrate este la rândul ei o sumă de două pătrate.

De aici, Fermat a dedus că pentru a cunoaşte care numere se scriu ca sumă de două pătrate, trebuie să fie cunoscute numerele prime cu această proprietate. Este uşor de arătat că numerele prime de forma $4k + 3$ nu sunt sumă de două pătrate. Dificil este de arătat că toate numerele prime de forma $4k + 1$ sunt sume de două pătrate.[1] Fermat a găsit forme liniare şi pentru numere prime de forma $a^2 + 2b^2$ şi $a^2 + 3b^2$. Primele sunt numere prime de forma $8k + 1$ sau $8k + 3$ iar ultimele sunt exact cele de forma $3k + 1$.

[1] Această teoremă a fost enunţată de Fermat în 1640, dar prima demonstraţie cunoscută este datorată lui Euler, în anul 1755.

La mijlocul secolului al XVIII-lea, Euler observă că aflarea numerelor prime de forma a^2+b^2, a^2+2b^2 sau a^2+3b^2 depinde dacă p este pătrat $(mod\ q)$ pentru anumiţi întregi p şi q. Astfel, pentru p şi q numere prime impare, el a obţinut următorul rezultat:

1. Când p, q sunt amândoi de forma $4k+3$, atunci p este pătrat modulo q dacă şi numai dacă q nu este pătrat modulo p.

2. Altfel, p este pătrat modulo q dacă şi numai dacă q este pătrat modulo p.

Datorită relaţiei reciproce între p şi q, această afirmaţie se numeşte *legea reciprocităţii pătratice*.[2]

7.1 Simbolul Legendre

Definiţie 7.1.1 *Fie m un număr natural şi a un întreg, relativ prim cu m. a se numeşte rest pătratic modulo m dacă congruenţa $x^2 \equiv a\ (mod\ m)$ are soluţii. În caz contrar, spunem că a nu este rest pătratic modulo m.*

Spre exemplu, din congruenţele:

$$\begin{array}{ll} 1^2 \equiv 10^2 \equiv 1\ (mod\ 11) & 2^2 \equiv 9^2 \equiv 4\ (mod\ 11) \\ 3^2 \equiv 8^2 \equiv 9\ (mod\ 11) & 4^2 \equiv 7^2 \equiv 5\ (mod\ 11) \\ 5^2 \equiv 6^2 \equiv 3\ (mod\ 11) & \end{array}$$

rezultă că $1, 3, 4, 5, 9$ sunt resturi pătratice modulo 11 iar $2, 6, 7, 8, 10$ nu sunt.

Lemă 7.1.1 *Fie p număr prim impar şi $a \in \mathbf{Z}$, cu $p \nmid a$. Congruenţa*

$$x^2 \equiv a\ (mod\ p) \tag{7.1}$$

are 2 soluţii necongruente modulo p, sau nu are soluţie.

[2]Euler nu a putut demonstra acest rezultat, decât pe câteva cazuri particulare, prima demonstraţie fiind dată de Gauss. Există aproape 200 de demonstraţii diferite pentru legea reciprocităţii pătratice. Astfel, aceasta a devenit a doua teoremă cu cele mai multe demonstraţii, după teorema lui Pitagora.

Demonstraţie. Presupunem că congruenţa (7.1) are o soluţie, pe x_0. Atunci, şi $-x_0$ este soluţie pentru (7.1). Dacă $x_0 \equiv -x_0 \ (mod\ p)$, atunci, $p \mid 2x_0$. Cum p este impar, $p \mid x_0$, de unde $p \mid a$, ceea ce este fals. Deci, x_0 şi $-x_0$ sunt soluţii necongruente modulo p. Rămâne să arătăm că orice altă soluţie y a lui (7.1) este congruentă modulo p cu una din acestea două. Din $y^2 \equiv a \equiv x_0^2 \ (mod\ p)$, obţinem $p \mid y^2 - x_0^2$. Cum p este prim, $p \mid y - x_0$ sau $p \mid y + x_0$ de unde obţinem rezultatul dorit. □

Propoziţie 7.1.1 *Pentru p număr prim impar, există exact $\frac{p-1}{2}$ resturi pătratice modulo p şi $\frac{p-1}{2}$ non-resturi pătratice modulo p între numerele $1, 2, \ldots, p-1$.*

Demonstraţie. Pentru a determina resturile pătratice modulo p dintre numerele $1, 2, \ldots, p-1$, procedăm ca în exemplul anterior. Calculăm resturile modulo p ale pătratelor celor $p-1$ numere. Sunt $p-1$ pătrate care trebuie considerate. Ştim că fiecare congruenţă (7.1) are 2 soluţii necongruente modulo p sau niciuna. Deci, sunt exact $\frac{p-1}{2}$ resturi pătratice modulo p. Cele rămase, în număr de $p - 1 - \frac{p-1}{2} = \frac{p-1}{2}$ sunt non-resturi pătratice modulo p. □

Definiţie 7.1.2 *Fie p număr prim impar şi a un întreg relativ prim cu p. Definim simbolul lui Legendre*[3]*, $\left(\frac{a}{p}\right)$ prin:*

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{dacă } a \text{ este rest pătratic mod } p; \\ -1, & \text{dacă } a \text{ nu este rest pătratic mod } p. \end{cases}$$

Observaţie 7.1.1 *În unele lucrări de specialitate, simbolul lui Legendre este definit şi pentru cazul când $p \mid a$, luând valoarea 0 în această situaţie. Dar, acest caz nu ne interesează în studiul nostru.*

Spre exemplu, $\left(\frac{3}{11}\right) = \left(\frac{4}{11}\right) = 1$ iar $\left(\frac{2}{11}\right) = \left(\frac{6}{11}\right) = -1$.

[3]Adrien-Marie Legendre (1752-1833), în lucrarea sa de teoria numerelor din anul 1785, a prezentat multe rezultate importante legate de legea reciprocităţii pătratice şi a numerelor prime aflate într-o progresie aritmetică.

Pentru p număr prim şi $p \nmid a \ (mod\ p)$, din teorema 3.4.3 obţinem $a^{p-1} \equiv 1 \ (mod\ p)$. Euler a folosit acest rezultat pentru a obţine un criteriu care să stabilească dacă un număr este rest pătratic modulo p sau nu.

Teoremă 7.1.1 (Criteriul Euler) *Fie p număr prim impar, $a \in \mathbf{Z}$ cu $p \nmid a$. Atunci,*

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \ (mod\ p). \tag{7.2}$$

Demonstraţie. Presupunem mai întâi că $\left(\frac{a}{p}\right) = 1$. Atunci, congruenţa (7.1) are soluţie pe care o notăm x_0. Din teorema 3.4.3,

$$a^{\frac{p-1}{2}} = \left(x_0^2\right)^{\frac{p-1}{2}} \equiv x_0^{p-1} \equiv 1 \ (mod\ p).$$

Considerăm acum $\left(\frac{a}{p}\right) = -1$. Deci, congruenţa (7.1) nu are soluţie. Din teorema 3.2.1, pentru orice $1 \leq i \leq p-1$ există $1 \leq j \leq p-1$ astfel încât $ij \equiv a \ (mod\ p)$. În acest caz, i şi j trebuie să fie diferite. Putem grupa numerele $1, 2, \ldots, p-1$ în $\frac{p-1}{2}$ perechi, fiecare cu produsul egal cu a. Atunci, $(p-1)! \equiv a^{\frac{p-1}{2}} \ (mod\ p)$. Aplicând acum teorema Wilson, rezultă $a^{\frac{p-1}{2}} \equiv -1 \ (mod\ p)$. □

Propoziţie 7.1.2 *Fie p număr prim impar şi $a, b \in \mathbf{Z}$ cu $p \nmid a$ şi $p \nmid b$. Atunci,*

1. *Dacă $a \equiv b \ (mod\ p)$, atunci $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.*
2. $\left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$.
3. $\left(\frac{a^2}{p}\right) = 1$.

Demonstraţie. 1) $a \equiv b \ (mod\ p)$. Atunci, $x^2 \equiv a \ (mod\ p)$ are soluţii dacă şi numai dacă $x^2 \equiv b \ (mod\ p)$ are soluţii.
2) Folosind criteriul lui Euler, $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \ (mod\, p)$, $\left(\frac{b}{p}\right) \equiv b^{\frac{p-1}{2}} \ (mod\, p)$

şi $\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} \pmod p$. Atunci, $\left(\frac{a}{p}\right)\cdot\left(\frac{b}{p}\right) \equiv \left(\frac{ab}{p}\right) \pmod p$. Cum valorile simbolului lui Legendre sunt ± 1, obţinem egalitatea cerută.

3) Folosind 2), din $\left(\frac{a}{p}\right) = \pm 1$, rezultă ultima afirmaţie. □

Observăm că punctul 2) al propoziţiei afirmă că produsul a două resturi pătratice sau a două non-resturi pătratice modulo p este rest pătratic, pe când produsul dintre un rest pătratic şi un non-rest pătratic modulo p este un non-rest pătratic modulo p.

Folosind criteriul lui Euler, vedem uşor care numere prime impare au pe -1 rest pătratic. Obţinem astfel:

Teoremă 7.1.2 *Dacă p este număr prim impar,*

$$\left(\frac{-1}{p}\right) = \begin{cases} 1, & \text{dacă } p \equiv 1 \pmod 4; \\ -1, & \text{dacă } p \equiv -1 \pmod 4. \end{cases}$$

Un alt criteriu care stabileşte dacă un număr este rest pătratic modulo p a fost enunţat de Gauss.

Lemă 7.1.2 (Lema lui Gauss) *Fie $p > 2$ număr prim şi $a \in \mathbf{Z}$, prim cu p. Dacă dintre resturile modulo p ale numerelor $a, 2a, 3a, \ldots, \frac{p-1}{2}a$, doar s sunt mai mari decât $\frac{p}{2}$, atunci $\left(\frac{a}{p}\right) = (-1)^s$.*

Demonstraţie. Fie $u_1, u_2, \ldots, u_s$ resturile modulo p mai mari decât $\frac{p}{2}$ şi notăm $v_1, v_2, \ldots, v_t$ celelalte resturi. Din $(j \cdot a, p) = 1$ pentru orice $1 \le j \le \frac{p-1}{2}$, toate resturile se află în mulţimea $\{1, 2, \ldots, p-1\}$.

Arătăm că $p - u_1, p - u_2, \ldots, p - u_s, v_1, v_2, \ldots, v_t$ acoperă mulţimea $\{1, 2, \ldots, \frac{p-1}{2}\}$ într-o anumită ordine.

Dacă avem $u_j \equiv u_i \pmod p$ sau $v_i \equiv v_i \pmod p$, ar exista $m, n \le \frac{p-1}{2}$ astfel încât $ma \equiv na \pmod p$. De aici, cum $m \ne n \pmod p$, rezultă $p \mid a$, ceea ce contrazice ipoteza. Deci, pentru $i \ne j$, $u_i \ne u_j \pmod p$ şi $v_i \ne v_j \pmod p$.

Dacă $p - u_i \equiv v_j \pmod p$, pentru $i \ne j$, atunci există $1 \le m, n \le \frac{p-1}{2}$

pentru care $ma \equiv p - na \ (mod\, p)$. Obţinem atunci, $m \equiv -n \ (mod\, p)$, ceea ce este imposibil ţinând cont de alegerea numerelor m, n. Deci, pentru $i \neq j$, $p - u_i \neq v_j \ (mod\ p)$.

Am demonstrat astfel că $p - u_1, p - u_2, \ldots, p - u_s, v_1, v_2, \ldots, v_t$ sunt numerele $1, 2, \ldots, \dfrac{p-1}{2}$, într-o anumită ordine. Atunci,

$$(p - u_1)(p - u_2) \ldots (p - u_s)v_1v_2 \ldots v_t \equiv \left(\frac{p-1}{2}\right)! \ (mod\ p) \tag{7.3}$$

adică

$$(-1)^s u_1u_2 \ldots u_sv_1v_2 \ldots v_t \equiv \left(\frac{p-1}{2}\right)! \ (mod\ p) \tag{7.4}$$

Dar, $u_1u_2 \ldots u_sv_1v_2 \ldots v_t \equiv a \cdot 2a \cdot \ldots \cdot \left(\dfrac{p-1}{2}\right) \cdot a \ (mod\ p)$ de unde

$$u_1u_2 \ldots u_sv_1v_2 \ldots v_t \equiv a^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \ (mod\ p) \tag{7.5}$$

Din (7.4) şi (7.5), obţinem

$$(-1)^s a^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \equiv \left(\frac{p-1}{2}\right)! \ (mod\ p). \tag{7.6}$$

De aici, cum p şi $\left(\dfrac{p-1}{2}\right)!$ sunt relativ prime, rezultă

$$(-1)^s a^{\frac{p-1}{2}} \equiv 1 \ (mod\ p). \tag{7.7}$$

Prin înmulţire cu $(-1)^s$, obţinem $\left(\dfrac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \equiv (-1)^s \ (mod\ p)$ ceea ce finalizează demonstraţia. □

De exemplu, pentru $p = 11$ şi $a = 6$, obţinem $\dfrac{p-1}{2} = 5$. Rezultă

$$\begin{aligned}
1 \cdot 6 &\equiv 6 \ (mod\ 11)\\
2 \cdot 6 &\equiv 1 \ (mod\ 11)\\
3 \cdot 6 &\equiv 7 \ (mod\ 11)\\
4 \cdot 6 &\equiv 9 \ (mod\ 11)\\
5 \cdot 6 &\equiv 8 \ (mod\ 11)
\end{aligned}$$

Cum sunt 4 resturi mai mari decât 5, $\left(\frac{6}{11}\right) = (-1)^4 = 1$.

Folosind lema lui Gauss, caracterizăm numerele prime impare care au pe 2 rest pătratic.

Teoremă 7.1.3 *Dacă p este număr prim impar,*

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & \text{dacă } p \equiv \pm 1 \ (mod\ 8); \\ -1 & \text{dacă } p \equiv \pm 3 \ (mod\ 8). \end{cases}$$

Demonstraţie. Păstăm notaţiile din demonstraţia lemei lui Gauss.
Fie $1 \leq j \leq \frac{p-1}{2}$. Din $2 \cdot j \leq \frac{p}{2}$ pentru $j \leq \frac{p}{4}$ rezultă că există $\left[\frac{p}{4}\right]$ numere strict mai mici decât $\frac{p}{2}$. Atunci, există $s = \frac{p-1}{2} - \left[\frac{p}{4}\right]$ resturi mai mari decât $\frac{p}{2}$.

Rămâne să arătăm că $\frac{p-1}{2} - \left[\frac{p}{4}\right] \equiv \frac{p^2-1}{8} \ (mod\ 2)$.
Pentru aceasta, cum p este prim impar, avem situaţiile:
$p \equiv \pm 1 \ (mod\ 8)$ sau $p \equiv \pm 3 \ (mod\ 8)$.
Pentru primul caz, $p = 8k \pm 1$, pentru k natural. Obţinem

$$\frac{p^2-1}{8} = 8k^2 \pm 2k \equiv 0 \ (mod\ 2),$$

$$\frac{p-1}{2} - \left[\frac{p}{4}\right] = \begin{cases} 2k \equiv 0 \ (mod\ 2), & \text{dacă } p = 8k+1; \\ 2k+2 \equiv 0 \ (mod\ 2), & \text{dacă } p = 8k+7. \end{cases}$$

Rezultă astfel, $\frac{p-1}{2} - \left[\frac{p}{4}\right] \equiv \frac{p^2-1}{8} \ (mod\ 2)$.
Pentru $p = 8k \pm 3$, $\frac{p^2-1}{8} = 8k^2 \pm 6k + 1 \equiv 1 \ (mod\ 2)$. Pe de altă parte,

$$\frac{p-1}{2} - \left[\frac{p}{4}\right] = \begin{cases} 2k+1 \equiv 1 \ (mod\ 2), & \text{dacă } p = 8k+3; \\ 2k+1 \equiv 1 \ (mod\ 2), & \text{dacă } p = 8k+5. \end{cases}$$

Obţinem şi în această situaţie congruenţa dorită. □

De exemplu, să calculăm următoarele simboluri Legendre:

1. $\left(\frac{317}{11}\right)$. Pentru aceasta, cum $317 \equiv 9 \ (mod\ 11)$, obţinem:

$$\left(\frac{317}{11}\right) = \left(\frac{9}{11}\right) = \left(\frac{3}{11}\right)^2 = 1.$$

2. $\left(\frac{89}{13}\right)$. Din $89 \equiv -2 \ (mod\ 13)$ rezultă:
$\left(\frac{89}{13}\right) = \left(\frac{-2}{13}\right) = \left(\frac{-1}{13}\right) \cdot \left(\frac{2}{13}\right) = -1$, pentru că:
din $13 \equiv 1 \ (mod\, 4)$ rezultă $\left(\frac{-1}{13}\right) = 1$ şi, deoarece $13 \equiv -3 \ (mod\, 8)$,
$\left(\frac{2}{13}\right) = -1$.

7.2 Legea reciprocităţii pătratice

Teorema elegantă, datorată lui Gauss, leagă $\left(\frac{p}{q}\right)$ de $\left(\frac{q}{p}\right)$ unde p, q sunt numere prime impare diferite. Cunoscută sub numele de *legea reciprocităţii pătratice,* ea precizează dacă congruenţa $x^2 \equiv p \ (mod\ q)$ are soluţii, ştiind dacă congruenţa $x^2 \equiv q \ (mod\ p)$ are soluţii.

Înainte de a o enunţa, să vedem cum funcţionează următoarea lemă, necesară în demonstraţia teoremei.

Lemă 7.2.1 *Fie p număr prim impar şi $a \in \mathbf{Z}$, impar, cu $p \nmid a$. Atunci,*

$$\left(\frac{a}{p}\right) = (-1)^{T(a,p)} \tag{7.8}$$

unde

$$T(a,p) = \sum_{j=1}^{\frac{p-1}{2}} \left[\frac{ja}{p}\right]. \tag{7.9}$$

Demonstraţie. Considerăm resturile modulo p ale numerelor $a, 2a, \ldots, \frac{p-1}{2}a$. Notăm cu $u_1, u_2, \ldots, u_s$ pe cele $> \frac{p}{2}$ iar cu $v_1, v_2, \ldots, v_t$ pe cele $< \frac{p}{2}$. Teorema împărţirii cu rest arată că

$$ja = p\left[\frac{ja}{p}\right] + r$$

unde r este restul împărţirii care nu poate fi decât un u_k sau un v_l.

Adunând cele $\frac{p-1}{2}$ astfel de ecuaţii, obţinem:

$$\sum_{j=1}^{\frac{p-1}{2}} ja = \sum_{j=1}^{\frac{p-1}{2}} p\left[\frac{ja}{p}\right] + \sum_{k=1}^{s} u_k + \sum_{l=1}^{t} v_l. \tag{7.10}$$

Din lema 7.1.2, $p-u_1, \ldots, p-u_s, v_1, \ldots, v_t$ sunt exact resturile $1, 2, \ldots, \frac{p-1}{2}$, eventual în altă ordine.

Calculând suma lor, rezultă

$$\sum_{k=1}^{\frac{p-1}{2}} k = \sum_{j=1}^{s}(p-u_j) + \sum_{j=1}^{t} v_j = ps - \sum_{j=1}^{s} u_j + \sum_{j=1}^{t} v_j. \tag{7.11}$$

De aici, scăzând din (7.10) relaţia (7.11), rezultă

$$\sum_{j=1}^{\frac{p-1}{2}} ja - \sum_{j=1}^{\frac{p-1}{2}} j = \sum_{j=1}^{\frac{p-1}{2}} p\left[\frac{ja}{p}\right] - ps + 2\sum_{j=1}^{s} u_j \tag{7.12}$$

$$(a-1)\sum_{j=1}^{\frac{p-1}{2}} j = pT(a,p) - ps + 2\sum_{j=1}^{s} u_j. \tag{7.13}$$

Cum a şi p sunt impare, $0 \equiv T(a,p) - s \ (mod\ 2)$, de unde $T(a,p) \equiv s \ (mod\ 2)$.

Aplicând încă o dată lema lui Gauss, obţinem

$$\left(\frac{a}{p}\right) = (-1)^s = (-1)^{T(a,p)}. \quad \square \tag{7.14}$$

Să calculăm simbolul lui Legendre pentru $a = 7$, $p = 11$.

$\sum_{j=1}^{5} \left[\frac{7j}{11}\right] = \left[\frac{7}{11}\right] + \left[\frac{14}{11}\right] + \left[\frac{21}{11}\right] + \left[\frac{28}{11}\right] + \left[\frac{35}{11}\right] = 0+1+1+2+3 = 7.$

De aici, $\left(\frac{7}{11}\right) = (-1)^7 = -1$.

În mod analog,

$\sum_{j=1}^{3} \left[\frac{11j}{7}\right] = \left[\frac{11}{7}\right] + \left[\frac{22}{7}\right] + \left[\frac{33}{7}\right] = 1+3+4 = 8,$

de unde, $\left(\frac{11}{7}\right) = (-1)^8 = 1$.

Teoremă 7.2.1 (Legea reciprocităţii pătratice) *Fie p, q numere prime impare. Atunci,*

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} \tag{7.15}$$

Să vedem cum am aplica lema anterioară pentru a demonstra teorema pe cazul numeric tratat anterior. Considerăm $p = 7$ şi $q = 11$.

Formăm perechi (x, y) cu $1 \leq x \leq \frac{7-1}{2} = 3$, $1 \leq y \leq \frac{11-1}{2} = 5$. Sunt în total 15 astfel de perechi pentru care nu se verifică egalitatea $11x = 7y$. Dacă egalitatea ar fi verificată pentru o pereche (x, y), atunci $11 \mid 7y$, de unde $11 \mid y$, fals. Împărţim aceste perechi în două grupe după cum urmează:

Prima grupă este formată din perechile (x, y) cu $1 \leq x \leq 3$, $1 \leq y \leq 5$ şi $11x > 7y$. Atunci, $1 \leq x \leq 3$, $1 \leq y \leq \frac{11x}{7}$. Pentru o valoare fixată a lui x sunt $\left[\frac{11x}{7}\right]$ valori posibile pentru y.

Astfel, prima grupă este formată din $\sum_{j=1}^{3} \left[\frac{11j}{7}\right] = 8$ perechi care sunt:

$$(1,1), (2,1), (2,2), (2,3), (3,1), (3,2), (3,3), (3,4).$$

Cea de-a doua grupă cuprinde celelalte perechi, adică:
(x, y) cu $1 \leq x \leq 3$, $1 \leq y \leq 5$ şi $11x < 7y$. Atunci, $1 \leq y \leq 5$ şi $1 \leq x \leq \frac{7y}{11}$. Pentru o valoare fixată a lui y sunt $\left[\frac{7y}{11}\right]$ valori posibile

pentru x.

Grupa este formată din $\sum_{j=1}^{5}\left[\frac{7j}{11}\right] = 7$ perechi care sunt:

$$(1,2),(1,3),(1,4),(1,5),(2,4),(2,5),(3,5).$$

Astfel,

$$\frac{11-1}{2}\cdot\frac{7-1}{2} = 5\cdot 3 = 15 = \sum_{j=1}^{3}\left[\frac{11j}{7}\right] + \sum_{j=1}^{5}\left[\frac{7j}{11}\right] = 8+7.$$

Rezultă, în final,

$$(-1)^{\frac{11-1}{2}\cdot\frac{7-1}{2}} = (-1)^{\sum_{j=1}^{3}\left[\frac{11j}{7}\right]}\cdot(-1)^{\sum_{j=1}^{5}\left[\frac{7j}{11}\right]} = \left(\frac{11}{7}\right)\cdot\left(\frac{7}{11}\right).$$

Să ne întoarcem acum la demonstraţia teoremei.

Demonstraţie. Formăm perechi

$$(x,y),\ 1\le x\le\frac{p-1}{2},\ 1\le y\le\frac{q-1}{2}.$$

Sunt în total $\frac{p-1}{2}\cdot\frac{q-1}{2}$ astfel de perechi. Dacă $qx = py$, atunci $q \mid py$, de unde $q \mid y$, ceea ce este fals. Astfel, pentru fiecare pereche (x,y), $qx \neq py$. Împărţim aceste perechi în două grupe ca mai sus.

Astfel, prima grupă este formată din perechile

$$(x,y),\ 1\le x\le\frac{p-1}{2},\ 1\le y\le\frac{q-1}{2},\ qx > py.$$

Atunci, perechile căutate sunt exact cele pentru care $1\le x\le\frac{p-1}{2}$, $1\le y\le\frac{qx}{p}$. Pentru o valoare fixată a lui x sunt $\left[\frac{qx}{p}\right]$ valori posibile pentru y. Deci, prima grupă este formată din $\sum_{j=1}^{\frac{p-1}{2}}\left[\frac{qj}{p}\right]$ perechi.

A doua grupă cuprinde perechile pentru care

$$1 \leq x \leq \frac{p-1}{2},\ 1 \leq y \leq \frac{q-1}{2},\ qx < py.$$

Atunci, $1 \leq y \leq \frac{q-1}{2}$, $1 \leq x \leq \frac{py}{q}$. Pentru o valoare fixată a lui y sunt $\left[\frac{py}{q}\right]$ valori posibile pentru x. Deci, această grupă este formată din $\sum_{j=1}^{\frac{q-1}{2}} \left[\frac{pj}{q}\right]$ perechi.

Numărul total de perechi (x, y) este egal cu:

$$\frac{p-1}{2} \cdot \frac{q-1}{2} = \sum_{j=1}^{\frac{p-1}{2}} \left[\frac{qj}{p}\right] + \sum_{j=1}^{\frac{q-1}{2}} \left[\frac{pj}{q}\right].$$

Folosind notaţiile lemei 7.2.1, putem scrie: $\frac{p-1}{2} \cdot \frac{q-1}{2} = T(q,p) + T(p,q)$.

Rezultă,

$$(-1)^{T(q,p)+T(p,q)} = (-1)^{T(q,p)} \cdot (-1)^{T(p,q)} = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}.$$

Din lema 7.2.1, $(-1)^{T(q,p)} = \left(\frac{q}{p}\right)$ şi $(-1)^{T(p,q)} = \left(\frac{p}{q}\right)$. Obţinem astfel relaţia dorită. □

Să observăm că $\frac{p-1}{2}$ este număr par dacă $p \equiv 1\ (mod\ 4)$ iar, în caz contrar, este număr impar. Astfel,

$$(-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} = \begin{cases} 1, & \text{dacă } p \equiv 1\ (mod\ 4) \text{ sau } q \equiv 1\ (mod\ 4); \\ -1, & \text{dacă } p \equiv q \equiv 3\ (mod\ 4). \end{cases}$$

Obţinem:

$$\left(\frac{p}{q}\right) = \begin{cases} \left(\frac{q}{p}\right), & \text{dacă } p \equiv 1\ (mod\ 4) \text{ sau } q \equiv 1\ (mod\ 4); \\ -\left(\frac{q}{p}\right), & \text{dacă } p \equiv q \equiv 3\ (mod\ 4). \end{cases}$$

Spre exemplu, considerăm $p = 11$, $q = 19$. Din $11 \equiv 19 \equiv 3 \ (mod\ 4)$, rezultă:
$\left(\frac{11}{19}\right) = -\left(\frac{19}{11}\right) = -\left(\frac{2}{11}\right)^3 = -(-1)^3 = 1$, pentru că $11 \equiv 3 \ (mod\ 8)$.

Folosind teorema 7.2.1, putem calcula acum anumite simboluri Legendre. Pentru $\left(\frac{217}{1009}\right)$, din $217 = 31 \cdot 7$, rezultă:
$\left(\frac{217}{1009}\right) = \left(\frac{31}{1009}\right) \cdot \left(\frac{7}{1009}\right)$
$1009 \equiv 1 \ (mod\ 4)$, de unde:
$\left(\frac{31}{1009}\right) = \left(\frac{1009}{31}\right) = \left(\frac{17}{31}\right) = \left(\frac{31}{17}\right) = \left(\frac{14}{17}\right) = \left(\frac{2}{17}\right) \cdot \left(\frac{7}{17}\right)$.
Din $17 \equiv 1 \ (mod\ 8)$, $\left(\frac{2}{17}\right) = 1$.
Obţinem, $\left(\frac{31}{1009}\right) = \left(\frac{7}{17}\right) = \left(\frac{17}{7}\right) = \left(\frac{3}{7}\right) = -\left(\frac{7}{3}\right) = -\left(\frac{4}{3}\right) = -\left(\frac{2}{3}\right)^2 = -1$.
Procedăm analog pentru $\left(\frac{7}{1009}\right)$ şi obţinem
$\left(\frac{7}{1009}\right) = \left(\frac{1009}{7}\right) = \left(\frac{8}{7}\right) = \left(\frac{2}{7}\right)^3 = 1^3 = 1$.
Deci, $\left(\frac{217}{1009}\right) = (-1) \cdot 1 = -1$.

7.3 Simbolul Jacobi

Simbolul Jacobi[4] este o generalizare a simbolului Legendre. El este folositor în evaluarea acestuia şi apare în definirea unui tip de numere pseudoprime (vezi capitolul 10.6).

Definiţie 7.3.1 *Fie $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_m^{\alpha_m}$ un număr compus impar, unde p_i sunt numere prime distincte, $\alpha_i \geq 1$, pentru fiecare $1 \leq i \leq m$.*

[4]Carl Gustav Jacob Jacobi (1804-1851) are contribuţii importante în teoria numerelor, legate de resturi cubice, în studiul funcţiilor eliptice cât şi al ecuaţiilor cu diferenţiale parţiale.

Considerăm $a \in \mathbf{Z}$ *cu* $(a, n) = 1$. *Definim simbolul Jacobi* $\left(\frac{a}{n}\right)$ *prin:*

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{\alpha_1} \cdot \left(\frac{a}{p_2}\right)^{\alpha_2} \cdot \ldots \cdot \left(\frac{a}{p_m}\right)^{\alpha_m}.$$

Deoarece pentru n număr prim, simbolul coincide cu simbolul Legendre, se foloseşte aceeaşi notaţie.

De exemplu, $\left(\frac{2}{1001}\right) = \left(\frac{2}{7}\right) \cdot \left(\frac{2}{11}\right) \cdot \left(\frac{2}{13}\right) = 1 \cdot (-1) \cdot (-1) = 1.$

Trebuie să remarcăm faptul că, pentru n număr compus, valoarea simbolului Jacobi nu precizează dacă congruenţa $x^2 \equiv a \ (mod \ n)$ are soluţii.

Dacă congruenţa are soluţii, atunci, pentru fiecare $1 \leq i \leq m$, congruenţa $x^2 \equiv a \ (mod \ p_i)$ are soluţii. Astfel, $\left(\frac{a}{p_i}\right) = 1$, pentru toţi divizorii primi p_i ai lui n. Din modul de definire al simbolului Jacobi, obţinem $\left(\frac{a}{n}\right) = 1$.

Dar, dacă $\left(\frac{a}{n}\right) = 1$, este posibil ca $x^2 \equiv a \ (mod \ n)$ să nu aibă soluţii. Spre exemplu, congruenţa $x^2 \equiv 2 \ (mod \ 55)$ este echivalentă cu sistemul de congruenţe:

$$\begin{cases} x^2 \equiv 2 \ (mod \ 5) \\ x^2 \equiv 2 \ (mod \ 11) \end{cases}$$

Cele două congruenţe care formează sistemul nu au soluţii pentru că $\left(\frac{2}{5}\right) = \left(\frac{2}{11}\right) = -1$. Deci, congruenţa iniţială nu are soluţii, cu toate că $\left(\frac{2}{55}\right) = (-1)(-1) = 1$.

Teoremă 7.3.1 *Fie* n *număr natural impar şi* $a, b \in \mathbf{Z}$, *cu* $(a, n) = 1$, $(b, n) = 1$. *Atunci:*

1) Dacă $a \equiv b \ (mod \ n)$ *atunci,* $\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$.

2) $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right) \cdot \left(\frac{b}{n}\right)$.

3) $\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}}$.

4) $\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}$.

Demonstraţie. 1) Fie $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_m^{\alpha_m}$ descompunerea în factori primi a lui n. Din $a \equiv b \ (mod\ n)$, rezultă $a \equiv b \ (mod\ p_i)$, pentru fiecare $1 \leq i \leq m$. Astfel,
$\left(\frac{a}{p_i}\right) = \left(\frac{b}{p_i}\right)$, pentru fiecare i.
Rezultă $\left(\frac{a}{n}\right) = \prod_{i=1}^{m} \left(\frac{a}{p_i}\right)^{\alpha_i} = \prod_{i=1}^{m} \left(\frac{b}{p_i}\right)^{\alpha_i} = \left(\frac{b}{n}\right)$.
2) $\left(\frac{ab}{n}\right) = \prod_{i=1}^{m} \left(\frac{ab}{p_i}\right)^{\alpha_i} = \prod_{i=1}^{m} \left(\frac{a}{p_i}\right)^{\alpha_i} \cdot \prod_{i=1}^{m} \left(\frac{b}{p_i}\right)^{\alpha_i} = \left(\frac{a}{n}\right) \cdot \left(\frac{b}{n}\right)$.
3) Din criteriul lui Euler obţinem că, pentru fiecare $1 \leq i \leq m$,

$$\left(\frac{-1}{p_i}\right) = (-1)^{\frac{p_i-1}{2}}. \tag{7.16}$$

Astfel,

$$\left(\frac{-1}{n}\right) = \prod_{i=1}^{m} \left(\frac{-1}{p_i}\right)^{\alpha_i} = (-1)^{\alpha_1 \frac{p_1-1}{2} + \dots + \alpha_m \frac{p_m-1}{2}}. \tag{7.17}$$

Din descompunerea lui n, obţinem

$$n = (1 + (p_1 - 1))^{\alpha_1} (1 + (p_2 - 1))^{\alpha_2} \dots (1 + (p_m - 1))^{\alpha_m}.$$

Fiecare $p_i - 1$ fiind un număr par, rezultă:

$$(1 + (p_i - 1))^{\alpha_i} \equiv 1 + \alpha_i (p_i - 1) \ (mod\ 4),$$

$$(1 + \alpha_i (p_i - 1)) \cdot (1 + \alpha_j (p_j - 1)) \equiv 1 + \alpha_i (p_i - 1) + \alpha_j (p_j - 1) \ (mod\ 4).$$

Deci,

$$n \equiv 1 + \alpha_1 (p_1 - 1) + \alpha_2 (p_2 - 1) + \dots + \alpha_m (p_m - 1) \ (mod\ 4).$$

Atunci,

$$\frac{n-1}{2} \equiv \frac{\alpha_1(p_1-1)}{2} + \frac{\alpha_2(p_2-1)}{2} + \ldots + \frac{\alpha_m(p_m-1)}{2} \ (mod\ 2) \quad (7.18)$$

şi astfel, $\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}}$.

4) Conform lemei lui Gauss, $\left(\frac{2}{p_i}\right) = (-1)^{\frac{p_i^2-1}{8}}$, pentru fiecare $1 \leq i \leq m$.

Atunci,

$$\left(\frac{2}{n}\right) = \prod_{i=1}^{m} \left(\frac{2}{p_i}\right)^{\alpha_i} = (-1)^{\alpha_1 \frac{p_1^2-1}{8} + \ldots + \alpha_m \frac{p_m^2-1}{8}}. \quad (7.19)$$

Ca la subpunctul precedent,

$$n^2 = (1+(p_1^2-1))^{\alpha_1}(1+(p_2^2-1))^{\alpha_2}\ldots(1+(p_m^2-1))^{\alpha_m}.$$

Cum fiecare $p_i^2 - 1 \equiv 0\ (mod\ 8)$, obţinem

$$(1+(p_i^2-1))^{\alpha_i} \equiv 1 + \alpha_i(p_i^2-1)\ (mod\ 64),$$

de unde:

$$n^2 \equiv 1 + \alpha_1(p_1^2-1) + \alpha_2(p_2^2-1) + \ldots + \alpha_m(p_m^2-1)\ (mod\ 64).$$

De aici,

$$\frac{n^2-1}{8} \equiv \frac{\alpha_1(p_1^2-1)}{8} + \frac{\alpha_2(p_2^2-1)}{8} + \ldots + \frac{\alpha_m(p_m^2-1)}{8}\ (mod\ 8). \quad (7.20)$$

Din relaţiile (7.19) şi (7.20), obţinem relaţia cerută. □

Teoremă 7.3.2 (Legea de reciprocitate pentru simbolul Jacobi) *Fie m, n două numere naturale impare, relativ prime. Atunci,*

$$\left(\frac{n}{m}\right) \cdot \left(\frac{m}{n}\right) = (-1)^{\frac{n-1}{2}\cdot\frac{m-1}{2}}.$$

Demonstraţie. Considerăm descompunerile canonice:
$n = p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_s^{\alpha_s}$ şi $m = q_1^{\beta_1}q_2^{\beta_2}\ldots q_r^{\beta_r}$.
Atunci,

$$\left(\frac{n}{m}\right) = \prod_{i=1}^{r}\left(\frac{n}{q_i}\right)^{\beta_i} = \prod_{i=1}^{r}\prod_{j=1}^{s}\left(\frac{p_j}{q_i}\right)^{\alpha_j\beta_i} \quad (7.21)$$

şi

$$\left(\frac{m}{n}\right)=\prod_{j=1}^{s}\left(\frac{m}{p_j}\right)^{\alpha_j}=\prod_{j=1}^{s}\prod_{i=1}^{r}\left(\frac{q_i}{p_j}\right)^{\alpha_j\beta_i} \tag{7.22}$$

Astfel,

$$\left(\frac{n}{m}\right)\cdot\left(\frac{m}{n}\right)=\prod_{i=1}^{r}\prod_{j=1}^{s}\left[\left(\frac{p_j}{q_i}\right)\cdot\left(\frac{q_i}{p_j}\right)\right]^{\alpha_j\beta_i} \tag{7.23}$$

Dar, din teorema 7.2.1,

$$\left(\frac{p_j}{q_i}\right)\cdot\left(\frac{q_i}{p_j}\right)=(-1)^{\frac{p_j-1}{2}\cdot\left(\frac{q_i-1}{2}\right)}. \tag{7.24}$$

Deci,

$$\left(\frac{n}{m}\right)\cdot\left(\frac{m}{n}\right)=\prod_{i=1}^{r}\prod_{j=1}^{s}(-1)^{\alpha_j\ \frac{p_j-1}{2}\ \beta_i\left(\frac{q_i-1}{2}\right)}=$$

$$=(-1)^{\sum_{i=1}^{r}\sum_{j=1}^{s}\alpha_j\ \frac{p_j-1}{2}\ \beta_i\left(\frac{q_i-1}{2}\right)}. \tag{7.25}$$

Din relaţia (7.18), obţinem:

$$\sum_{j=1}^{s}\alpha_j\left(\frac{p_j-1}{2}\right)\equiv\frac{n-1}{2}\ (mod\ 2) \tag{7.26}$$

$$\sum_{i=1}^{r}\beta_i\left(\frac{q_i-1}{2}\right)\equiv\frac{m-1}{2}\ (mod\ 2). \tag{7.27}$$

Astfel,

$$\sum_{i=1}^{r}\sum_{j=1}^{s}\alpha_j\left(\frac{p_j-1}{2}\right)\beta_i\left(\frac{q_i-1}{2}\right)=\sum_{j=1}^{s}\alpha_j\left(\frac{p_j-1}{2}\right)\cdot\sum_{i=1}^{r}\beta_i\left(\frac{q_i-1}{2}\right)$$

$$\equiv\frac{n-1}{2}\cdot\frac{m-1}{2}\ (mod\ 2). \tag{7.28}$$

Înlocuind această ultimă relaţie în (7.25), rezultă:

$$\left(\frac{n}{m}\right)\cdot\left(\frac{m}{n}\right)=(-1)^{\frac{n-1}{2}\cdot\frac{m-1}{2}}.\quad\square$$

Stabilim, în final un algoritm eficient de determinare a simbolurilor Jacobi.

Fie a, n numere naturale, relativ prime. Presupunem $a > n$. Notăm $r_0 = a$, $r_1 = n$. Aplicăm algoritmul lui Euclid, punând în evidenţă puterea maximă a lui 2 din fiecare rest. Obţinem astfel,

$$r_0 = r_1 q_2 + 2^{s_1} r_2 \tag{7.29}$$
$$r_1 = r_2 q_3 + 2^{s_2} r_3 \tag{7.30}$$
$$r_2 = r_3 q_4 + 2^{s_3} r_4 \tag{7.31}$$
$$\cdots \tag{7.32}$$
$$r_{n-3} = r_{n-2} q_{n-1} + 2^{s_{n-2}} r_{n-1} \tag{7.33}$$
$$r_{n-2} = r_{n-1} q_n + 2^{s_{n-1}} \cdot 1 \tag{7.34}$$

unde pentru $1 \leq j \leq n-1$, toţi $s_j \in \boldsymbol{N}$, r_j impari şi $r_j < r_{j-1}$.

De exemplu, dacă alegem $a = 3027$, $n = 407$, obţinem relaţiile:

$$\begin{aligned} 3027 &= 407 \cdot 7 + 2 \cdot 89 \\ 407 &= 89 \cdot 4 + 2^0 \cdot 51 \\ 89 &= 51 \cdot 1 + 2 \cdot 19 \\ 51 &= 19 \cdot 2 + 2^0 \cdot 13 \\ 19 &= 13 \cdot 1 + 2 \cdot 3 \\ 13 &= 3 \cdot 4 + 2^0 \cdot 1. \end{aligned}$$

Teoremă 7.3.3 *Fie $a > n$ numere naturale relativ prime. Atunci, simbolul Jacobi $\left(\frac{a}{n}\right)$ este egal cu:*

$$(-1)^{s_1 \frac{r_1^2-1}{8} + \ldots + s_{n-1} \frac{r_{n-1}^2-1}{8} + \frac{r_1-1}{2} \cdot \frac{r_2-1}{2} + \ldots + \frac{r_{n-2}-1}{2} \cdot \frac{r_{n-1}-1}{2}}.$$

Demonstraţie. Folosind rezultatele teoremei 7.3.1, obţinem
$\left(\frac{a}{n}\right) = \left(\frac{r_0}{r_1}\right) = \left(\frac{2^{s_1} r_2}{r_1}\right) = \left(\frac{2}{r_1}\right)^{s_1} \cdot \left(\frac{r_2}{r_1}\right) = (-1)^{s_1 \frac{r_1^2-1}{8}} \cdot \left(\frac{r_2}{r_1}\right)$.
Din teorema 7.3.2,
$\left(\frac{r_2}{r_1}\right) = (-1)^{\frac{r_1-1}{2} \cdot \frac{r_2-1}{2}} \cdot \left(\frac{r_1}{r_2}\right)$.

Deci,

$$\left(\frac{a}{n}\right) = (-1)^{s_1 \frac{r_1^2-1}{8} + \frac{r_1-1}{2}\cdot\frac{r_2-1}{2}} \cdot \left(\frac{r_1}{r_2}\right). \tag{7.35}$$

În mod analog, folosind celelalte relaţii din algoritmul lui Euclid pentru $2 \leq j \leq n-2$, rezultă:

$$\left(\frac{r_{j-1}}{r_j}\right) = (-1)^{s_j \frac{r_j^2-1}{8} + \frac{r_j-1}{2}\cdot\frac{r_{j+1}-1}{2}} \cdot \left(\frac{r_j}{r_{j+1}}\right). \tag{7.36}$$

Înlocuind relaţiile (7.36) în (7.35) vom obţine rezultatul dorit. □

Pentru exemplul anterior, vom obţine exponentul lui -1 egal cu:

$$1 \cdot \frac{407^2-1}{8} + 0 \cdot \frac{89^2-1}{8} + 1 \cdot \frac{51^2-1}{8} + 0 \cdot \frac{19^2-1}{8} + 1 \cdot \frac{13^2-1}{8} +$$
$$0 \cdot \frac{3^2-1}{8} + \frac{407-1}{2} \cdot \frac{89-1}{2} + \frac{89-1}{2} \cdot \frac{51-1}{2} + \frac{51-1}{2} \cdot \frac{19-1}{2} +$$
$$\frac{19-1}{2} \cdot \frac{13-1}{2} + \frac{13-1}{2} \cdot \frac{3-1}{2} = 31369.$$

Atunci, $\left(\frac{3027}{407}\right) = (-1)^{31369} = -1$.

Algoritm 7.3.1 (Simbolul Jacobi)
INPUT: numerele naturale a, n.
OUTPUT: $\left(\frac{a}{n}\right)$

1. $u \leftarrow a \bmod n,\ v \leftarrow n,\ k \leftarrow 1$.
2. *Cât timp* $u > 1$ *calculează:*
   - 2.1. *Dacă* u *este par, atunci* $u \leftarrow u/2, k \leftarrow k \cdot (-1)^{(v^2-1)/8}$
     - 2.1.1. *Dacă* $u = v$, *atunci returnează* $(a, n) \neq 1$ *şi se opreşte.*
   - 2.2. *Dacă* $u > v$ *atunci* $u \leftarrow (u-v)/2, k \leftarrow k \cdot (-1)^{(v^2-1)/8}$
     - 2.2.1. $u \leftarrow (v-u)/2,\ v \leftarrow u,$
       $k \leftarrow k \cdot (-1)^{(u-1)\cdot(v-1)/4},$
       $k \leftarrow k \cdot (-1)^{(v^2-1)/8}$
3. *Returnează* k.

Algoritmul poate fi propus şi sub forma:

Algoritm 7.3.2
$J(a,n)$
INPUT: numerele naturale $a < n$, *cu* $n \geq 3$ *impar.*
OUTPUT: $\left(\frac{a}{n}\right)$
1. Dacă $a = 0$, *atunci returnează* 0 *şi se opreşte.*
2.Dacă $a = 1$, *returnează* 1 *şi se opreşte.*
3. Scrie $a = 2^e a_1$, *unde* a_1 *este impar.*
4. Dacă e *este par, pune* $s \leftarrow 1$. *Altfel, dacă* $n \equiv \pm 1 \ (mod\ 8)$
pune $s \leftarrow 1$ *şi dacă* $n \equiv \pm 3 \ (mod\ 8)$ *pune* $s \leftarrow -1$.
5. Dacă $n \equiv 3 \ (mod\ 4)$ *şi* $a_1 \equiv 3 \ (mod\ 4)$, *pune* $s \leftarrow -s$.
6. Pune $n_1 \leftarrow n \ mod\ a_1$
7. Dacă $a_1 = 1$, *atunci returnează* s *şi se opreşte;*
altfel, returnează $s \cdot J(n_1, a_1)$

Exerciţii propuse

1. Calculaţi următoarele simboluri Legendre:

$$\left(\frac{11}{37}\right), \left(\frac{97}{101}\right), \left(\frac{31}{167}\right), \left(\frac{1801}{8191}\right)$$

şi simbolurile Jacobi:

$$\left(\frac{5}{21}\right), \left(\frac{27}{101}\right), \left(\frac{111}{1001}\right).$$

2. Arătaţi că:

i) -3 este rest pătratic modulo p, cu p număr prim impar, dacă şi numai dacă $p \equiv 1 \ (mod\ 3)$.

ii) 3 este non-rest pătratic modulo orice număr prim Mersenne > 3.

3. Arătaţi că 5 este rest pătratic modulo p, un număr prim impar, dacă şi numai dacă $p \equiv \pm 1 \ (mod\ 20)$ sau $p \equiv \pm 9 \ (mod\ 20)$.

4. Stabiliţi pentru ce valori ale numărului prim impar p, -5 nu este rest pătratic modulo p.

5. Calculaţi $\left(\frac{5}{F_n}\right)$ şi $\left(\frac{7}{F_n}\right)$, unde F_n este un număr prim Fermat.

CAPITOLUL 8

Criptografie cu cheie secretă

Criptografia[1] este studiul principiilor şi tehnicilor prin care informaţia poate fi ascunsă în texte cifrate şi mai târziu este dezvăluită de persoane avizate folosind chei secrete (pentru persoane neautorizate este imposibil sau computaţional imposibil).

Criptanaliza[2] studiază redobândirea informaţiei din textul cifrat, fără a cunoaşte cheia.

Criptologia[3] este ştiinţa ce înglobează cele două domenii mai sus definite.

Istoria criptografiei începe încă de acum 4000 de ani (la egipteni). De cele mai multe ori, rezultatele acesteia erau folosite în domeniul militar, diplomatic şi guvernamental. Criptografia a fost folosită ca un instrument important în protejarea secretelor şi strategiilor naţionale.

Odată cu dezvoltarea în anii 60 a sistemelor de comunicaţie şi a computerelor, apare cerinţa de a oferi sectorului privat mijloace de protejare a informaţiei în formă digitală şi de asigurare a serviciilor de securitate. Principiile criptografiei, concepută iniţial pentru a secretiza mesaje scrise, se aplică la fel de bine pentru securizarea fluxului de date între

[1] Provine din cuvintele greceşti *kryptos*-a ascunde şi *graphein*-a scrie.
[2] Provine din cuvintele greceşti *kryptos*-a ascunde şi *analyein*-a dezlega.
[3] Provine din cuvintele greceşti *krypos*-a ascunde şi *logos*-cuvânt.

computere, a comunicaţiilor de voce digitale cât şi la cifrarea de facsimile şi a semnalelor de televiziune. De exemplu, majoritatea sateliţilor cifrează în mod curent fluxul de date către şi de la staţiile terestre pentru a furniza securitate şi confidenţialitate abonaţilor.

Câteva dintre principalele scopuri urmărite în criptografie sunt:

1. *Confidenţialitatea*, care presupune păstrarea secretă a informaţiei faţă de toţi cei care nu sunt autorizaţi să o cunoască.

2. *Integritatea datelor*, realizează protejarea datelor la alterare sau manipulare de către persoane neautorizate.
   Prin manipularea datelor înţelegem procese cum ar fi inserţii, întârzieri sau substituiri.

3. *Autentificarea*, care presupune posibilitatea de identificare a informaţiei şi a entităţii (o persoană, un terminal de computer, o carte de credit).

4. *Non-repudierea*, care previne negarea unor angajamente sau acţiuni anterioare.

Criptografia trebuie să acopere, în mod corespunzător, aceste patru direcţii, atât în teorie, cât şi în practică. Ea trebuie să prevină şi să detecteze furtul şi alte acţiuni ilegale, fiind doar una dintre tehnicile de asigurare a securităţii informaţiei.

Pentru început, definim următoarele noţiuni:

1. *Alfabet de definiţie* $\mathcal{A}$ care este o mulţime finită. De exemplu, $\mathcal{A} = \{0, 1\}$ se numeşte *alfabet binar*. Trebuie să remarcăm că orice alfabet, spre exemplu alfabetul englezesc, poate fi scris în funcţie de alfabetul binar. Literele vor deveni şiruri de câte cinci cifre binare.

2. *Spaţiul de mesaje* $\mathcal{M}$ este format din şiruri de simboluri ale unui alfabet de definiţie. Un element al lui $\mathcal{M}$ se numeşte *text de bază*. De exemplu, $\mathcal{M}$ poate fi format din şiruri binare, un text în engleză sau în altă limbă, codul unui computer, etc.

3. *Spaţiul de text cifrat* $\mathcal{C}$ este alcătuit din şiruri de simboluri ale unui alfabet de definiţie, care poate fi diferit de $\mathcal{A}$. Un element al lui $\mathcal{C}$ se numeşte *text cifrat*.

4. *Spaţiul cheilor* $\mathcal{K}$ este o mulţime de şiruri (*chei*) peste un alfabet. Pentru fiecare $e \in \mathcal{K}$, aplicaţia bijectivă $E_e : \mathcal{M} \to \mathcal{C}$, determinată de e, se numeşte *funcţie* sau *transformare de criptare.*
   În mod analog, funcţia bijectivă $D_d : \mathcal{C} \to \mathcal{M}$, determinată de $d \in \mathcal{K}$, poartă numele de *funcţie* sau *transformare de decriptare.*

5. *Procesul (algoritmul) de criptare* E este procesul de aplicare a transformării E_e lui $\mathcal{M}$. Deci, $E_e(\mathcal{M}) = \mathcal{C}$.

6. *Procesul (algoritmul) de decriptare* D este procesul de aplicare a transformării D_d lui $\mathcal{C}$. Astfel, $D_d(\mathcal{C}) = \mathcal{M}$. Subliniem faptul că algoritmii D şi E trebuie să aibă proprietatea $D_d(\mathcal{C}) = D_d(E_e(\mathcal{M})) = \mathcal{M}$.

7. O *schemă de criptare*, sau un *cifru,* este formată dintr-o mulţime de transformări de criptare $\{E_e\}$ şi din mulţimea corespunzătoare $\{D_d\}$, de transformări de decriptare cu proprietatea că, pentru fiecare $e \in \mathcal{K}$, există un unic $d \in \mathcal{K}$ astfel încât $D_d = E_e^{-1}$. Cheile e şi d cu această proprietate se numesc *pereche de chei* şi de multe ori se notează (e, d). Pentru a construi o schemă de criptare avem nevoie de toate noţiunile definite anterior.

Criptosistemele pot fi clasificate în:

1. *Sisteme criptografice cu cheie secretă,* numite şi criptosisteme simetrice.

2. *Sisteme criptografice cu cheie publică,* numite şi criptosisteme asimetrice.

Criptografia cu cheie secretă se ocupă de primul tip de criptosisteme.

Un sistem de criptare se numeşte *simetric*[4] dacă, din punct de vedere computaţional, pentru fiecare pereche de chei (e, d) se poate determina uşor d cunoscând doar pe e şi invers.

De cele mai multe ori, într-un sistem cu cheie secretă, cheile e şi d coincid. Cheia comună k, numită *cheie secretă,* este folosită atât la criptare cât şi la decriptare. De aceea aceste sisteme poartă numele de *sisteme simetrice.*

[4] Alţi termeni folosiţi în literatura de specialitate pentru aceste sisteme sunt: criptare tradiţională, cu cheie unică, cu cheie secretă.

Vom studia cum se pot transmite mesaje între două persoane: expeditorul A, de cele mai multe ori numit *Alice* şi destinatarul B, numit uzual *Bob*.

Astfel, Alice aplică funcţia bijectivă E_k pentru a realiza un text cifrat prin $C = E_k(M)$, pentru fiecare $M \in \mathcal{M}$, pe care îl trimite lui Bob printr-un canal nesigur (persoane neautorizate pot citi, schimba, şterge informaţia). Cheia k trebuie şi ea trimisă lui Bob, dar printr-un canal sigur. Bob decriptează textul cifrat prin transformarea inversă, D_k, şi obţine $D_k(C) = D_k(E_k(M)) = M$, pentru $C \in \mathcal{C}$, adică reconstituie textul iniţial.

8.1 Cifrări flux (binar)

În cifrările flux, unităţile de mesaj sunt cifre binare şi cheia este produsă de obicei de un generator aleator binar. Textul de bază este criptat bit cu bit. Cheia este încărcată într-un generator aleator de biţi pentru a crea un şir lung de semnale binare. Cheia şir k este aplicată apoi textului de bază M, (de obicei se face adunare modulo 2) pentru a obţine textul cifrat C. De exemplu:

M	0	1	1	0	0	0	1	1	1	1	1	1	1	...
k	1	0	0	1	1	0	0	1	0	0	0	1	0	...
C	1	1	1	1	1	0	1	0	1	1	1	0	1	...

Pentru decriptare, se foloseşte aceeaşi cheie.

8.2 Criptosisteme caracter

Primele sisteme de criptare erau bazate pe transformarea fiecărei litere din textul iniţial într-o literă diferită pentru a obţine textul cifrat. Astfel de cifrări, în care unitatea de mesaj este formată dintr-o singură literă, poartă numele de *sisteme de criptare caracter, substituţie* sau *monografice.*

Vom considera în toate exemplele că $\mathcal{A}$ este alfabetul limbii engleze. Cum acesta este format din 26 de litere, vom atribui fiecăreia un echiva-

lent numeric de la 0 la 25 după cum urmează:

A	B	C	D	E	F	G	H	I	J	K	L	M
↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕
13	14	15	16	17	18	19	20	21	22	23	24	25

Din considerente istorice, alegem ca prim sistem caracter, un sistem de criptare care se presupune că a fost inventat şi folosit de Iulius Cezar.

Aici, cheia este $k = 3$ şi transformarea de criptare este

$$C = E_3(M) \equiv M + 3 \ (mod\ 26),\ 0 \leq M \leq 25.$$

Cu alte cuvinte, fiecare literă este deplasată la dreapta cu trei poziţii faţă de poziţia iniţială din alfabet. De exemplu, A devine D, X se transformă în A, Y în B, Z în C.

Presupunem că textul iniţial este:

$$THIS\ MESSAGE\ IS\ TOP\ SECRET$$

Pentru început, el este împărţit în blocuri de 5 litere pentru a preveni recunoaşterea unor cuvinte particulare

$$THISM\ ESSAG\ EISTO\ PSECR\ ET$$

şi fiecare literă este înlocuită cu echivalentul său numeric

19 7 8 18 12 4 18 18 0 6 4 8 18 19 14 15 18 4 2 17 4 19.

Fiecare echivalent numeric este transformat după regula precizată:

22 10 11 21 15 7 21 21 3 9 7 11 21 22 17 18 21 7 5 20 7 22

şi apoi se înlocuieşte cu litera corespunzătoare. Textul cifrat rezultat este:

$$WKLVP\ HVVDJ\ HLVWR\ SVHFU\ HW.$$

Pentru decifrare, se foloseşte transformarea

$$M = D_3(C) \equiv C - 3 \ (mod\ 26),\ 0 \leq C \leq 25.$$

Acest cifru face parte din categoria *criptosistemelor de deplasare*. În acest caz, cheia este $0 \leq k \leq 25$, funcţia de criptare este

$$E_k(M) \equiv M + k \ (mod\ 26),\ 0 \leq M \leq 25,$$

iar transformarea de decriptare este dată de

$$D_k(C) \equiv C - k \ (mod\ 26),\ 0 \leq C \leq 25.$$

Dacă vom generaliza, obţinem *criptosistemele afine* unde cheia este perechea (a, b) cu $0 \leq a, b \leq 25$ iar a este relativ prim cu 26. Observăm că putem construi $12 \cdot 26 = 312$ astfel de chei. Transformarea de criptare este dată de funcţia

$$E_{(a,b)}(M) \equiv aM + b \ (mod\ 26), 0 \leq M \leq 25$$

iar cea de decriptare este

$$D_{(a,b)}(C) \equiv \overline{a}(C - b) \ (mod\ 26),\ 0 \leq C \leq 25.$$

De exemplu, dacă aplicăm o transformare afină textului $SECURITY$ folosind cheia $(7, 10)$ obţinem: $GMYUZONW$ după cum se remarcă mai jos:

S	E	C	U	R	I	T	Y
18	4	2	20	17	8	19	24
6	12	24	20	25	14	13	22
G	M	Y	U	Z	O	N	W

Pentru criptanaliza sistemelor caracter trebuie făcută o analiză a frecvenţei de apariţie a literelor în textul cifrat. Aceasta este comparată cu frecvenţa literelor dintr-un text obişnuit. În limba engleză, cele mai frecvente litere dintr-un text sunt E, T, R, N, I, O, A (pentru limba română, ele ar fi I, E, A, B). Astfel, punând în corespondenţă cea

mai des întâlnită literă din textul cifrat (de preferinţă mai lung, pentru a realiza o cât mai corectă corespondenţă între literele cu frecvenţă maximă) cu litera care apare de cele mai multe ori într-un text arbitrar, se pot dobândi informaţii legate de cheia de criptare.

De exemplu, considerăm două situaţii:

1. Presupunem că un text, scris în limba engleză, a fost criptat printr-un sistem de deplasare. Observăm că litera care apare cel mai des în textul cifrat este P. Atunci, putem presupune că ea corespunde literei E, litera cu cea mai mare frecvenţă într-un text scris în limba engleză. Ţinând cont de echivalenţii numerici corespunzători acestor litere, obţinem relaţia $15 \equiv 4 + k \ (mod\ 26)$, de unde $k = 11$ este o posibilă cheie de cifrare.

Cum există doar 26 de transformări de deplasare, inclusiv cea identică, determinarea cheii nu presupune un volum foarte mare de muncă. În concluzie, acest sistem este uşor de criptanalizat.

2. Presupunem acum că un text, scris în limba engleză, a fost criptat printr-o transformare afină. Analizând frecvenţa literelor din textul cifrat, vedem că cele mai des folosite litere sunt L şi U. Atunci, putem presupune că L este în corespondenţă cu E iar U corespunde lui T. Rezultă relaţiile $11 \equiv 4a + b \ (mod\ 26)$ şi $20 \equiv 19a + b \ (mod\ 26)$. Rezolvând sistemul de congruenţe, o posibilă cheie este $(11, 19)$. Deci, transformarea de criptare ar fi $E_{(11,19)}(M) \equiv 11M + 19 \ (mod\ 26)$. Pentru decriptare, se foloseşte $D_{(11,19)}(C) \equiv 19(C - 19) \equiv 19C + 3 \ (mod\ 26)$ unde am ţinut cont că $\overline{a} \equiv 19 \ (mod\ 26)$.

8.3 Criptosisteme bloc

Pentru a evita faptul că primele criptosisteme prezentate sunt mult prea vulnerabile, s-a preferat împărţirea textului de bază în blocuri de o anumită lungime şi transformarea acestora în blocuri cu aceeaşi lungime. Aceste sisteme se numesc *sisteme bloc*[5] sau *poligrafice.*

Studiem mai întâi cazul *cifrului diagrafic* pe un exemplu concret. Aici blocurile sunt formate din două cifre. Considerăm textul iniţial

THE GOLD IS BURIED IN ORONO.

[5] Au fost prezentate de Hill, în anul 1930.

Mai întâi, textul iniţial se împarte în blocuri de 2 litere. Dacă numărul de litere este impar, se completează ultimul bloc cu o literă, de exemplu, X. Obţinem pentru exemplul nostru,

$$TH\ EG\ OL\ DI\ SB\ UR\ IE\ DI\ NO\ RO\ NO.$$

Fiecare literă din bloc este înlocuită cu echivalentul său numeric:

19 7 4 6 14 11 3 8 18 1 20 17 8 4 3 8 13 14 17 14 13 14.

Fiecare bloc de numere M_1M_2 din textul iniţial este înlocuit cu blocul C_1C_2 după transformarea:

$$C_1 \equiv 5M_1 + 17M_2 \ (mod\ 26)$$
$$C_2 \equiv 4M_1 + 15M_2 \ (mod\ 26).$$

Acest criptosistem este mult mai uşor de descris matriceal, şi anume:

$$\begin{pmatrix} C_1 \\ C_2 \end{pmatrix} \equiv \begin{pmatrix} 5 & 17 \\ 4 & 15 \end{pmatrix} \cdot \begin{pmatrix} M_1 \\ M_2 \end{pmatrix} \ (mod\ 26).$$

Se observă că matricea care intervine are invers modulo 26, matricea inversă intervenind în procesul de decriptare.

Trecem acum la cazul general, în care blocurile în care este împărţit textul iniţial conţin n litere. Procesul de cifrare se realizează la fel cu cazul anterior, numai că, aici, unitatea este un bloc $M = \begin{pmatrix} M_1 \\ \vdots \\ M_n \end{pmatrix}$ cu $0 \leq M_i \leq 25$, pentru $0 \leq i \leq n$. În acest caz cheia este $A \in M_n(\boldsymbol{Z})$, cu $(\det A, 26) = 1$, deci matricea A are invers modulo 26. Transformarea de criptare este $E_A(M) \equiv AM \ (mod\ 26)$ iar pentru decriptare se foloseşte funcţia $D_A(C) \equiv \overline{A}C \ (mod\ 26)$, $C = \begin{pmatrix} C_1 \\ \vdots \\ C_n \end{pmatrix}$, $0 \leq C_i \leq 25$.

De exemplu, să vedem cum criptăm mesajul

$$STOP\ PAYMENT$$

folosind un astfel de algoritm.

Alegem $n = 3$ iar cheia $A = \begin{pmatrix} 11 & 2 & 19 \\ 5 & 23 & 25 \\ 20 & 7 & 1 \end{pmatrix}$. A este corect aleasă pentru că, din $\det A \equiv 5 \ (mod\ 26)$, matricea este inversabilă modulo 26.

Textul iniţial este împărţit în blocuri de trei litere, adăugând pentru blocul final un X pentru ca şi acest bloc să aibă numărul corespunzător de litere:

$$STO\ PPA\ YME\ NTX.$$

Înlocuim literele cu echivalenţii lor numerici

$$18\ 19\ 14 \quad 15\ 15\ 0 \quad 24\ 12\ 4 \quad 13\ 19\ 23$$

şi aplicăm fiecărei unităţi de mesaj transformarea de criptare. De exemplu, pentru primul bloc, calculăm

$$\begin{pmatrix} C_1 \\ C_2 \\ C_3 \end{pmatrix} \equiv \begin{pmatrix} 11 & 2 & 19 \\ 5 & 23 & 25 \\ 20 & 7 & 1 \end{pmatrix} \cdot \begin{pmatrix} 18 \\ 19 \\ 14 \end{pmatrix} \equiv \begin{pmatrix} 8 \\ 19 \\ 13 \end{pmatrix} \ (mod\ 26).$$

Pentru obţinerea textului cifrat, în şirul rezultat

$$8\ 19\ 13 \quad 13\ 4\ 15 \quad 0\ 2\ 22 \quad 20\ 11\ 0$$

înlocuim echivalenţii numerici cu litere corespunzătoare:

$$ITN\ NEP\ ACW\ ULA.$$

La decriptare, vom folosi matricea inversă modulo 26 a lui A,
$\overline{A} = \begin{pmatrix} 6 & -5 & 11 \\ -5 & -1 & -10 \\ -7 & 3 & 7 \end{pmatrix}$.

Acest tip de criptosistem este şi el vulnerabil la frecvenţa blocurilor de litere. De exemplu, în limba engleză, cele mai frecvente perechi de litere dintr-un text sunt TH şi HE iar THE, AND şi THA sunt cele mai des întâlnite blocuri de trei litere. Făcând analiza corespunzătoare, putem găsi cheia.

De exemplu, dacă într-un text cifrat, scris în limba engleză cele mai frecvente grupe de două litere sunt KX şi VZ, presupunând că algoritmul folosit este de tipul celui prezentat, putem pune în corespondenţă KX cu TH iar VZ cu HE. Înlocuind literele cu echivalenţii lor numerici, din relaţia $\begin{pmatrix} 10 & 21 \\ 23 & 25 \end{pmatrix} \equiv A \cdot \begin{pmatrix} 19 & 7 \\ 7 & 4 \end{pmatrix} \ (mod\ 26)$ rezultă $A = \begin{pmatrix} 10 & 21 \\ 23 & 25 \end{pmatrix} \cdot \begin{pmatrix} 4 & 19 \\ 19 & 19 \end{pmatrix} \equiv \begin{pmatrix} 23 & 17 \\ 21 & 2 \end{pmatrix} \ (mod\ 26)$ ca posibilă cheie.

8.4 Criptare exponenţială

Acest criptosistem a fost inventat de Pohlig şi Helmann în anul 1976.

Se alege p un număr prim, şi un număr natural e, prim cu $p-1$, care este cheia de criptare. Fiecare unitate de mesaj, în cazul nostru o literă, se înlocuieşte cu echivalenţi numerici alcătuiţi toţi din două cifre. Astfel, de exemplu echivalentul lui A este 00, C va avea echivalentul numeric egal cu 02, etc.

Mesajul se împarte în blocuri de $2m$ cifre zecimale unde $2m$ este cel mai mare număr par cu proprietatea că toate numerele de $2m$ cifre alcătuite din echivalenţii numerici ai celor m litere sunt mai mici decât p. Astfel, dacă $p = 2633$, din $2525 < p < 252525$ rezultă $m = 2$.

Fiecărui bloc M cu $2m$ cifre zecimale i se aplică transformarea de criptare $C = E_e(M) \equiv M^e \ (mod\ p)$, deci fiecare bloc din textul cifrat va fi un număr mai mic decât p. De exemplu, considerăm mesajul

THIS IS AN EXAMPLE OF AN EXPONENTIATION CIPHER

pe care vrem să-l criptăm folosind un algoritm exponenţial.
Alegem $p = 2633$ şi $e = 29$. Transformăm literele în echivalenţi numerici şi formăm blocuri de câte 4 cifre:

1907 0818 0818 0013 0423 0012 1511 0414 0500 1304

2315 1413 0413 1908 0019 0814 1302 0815 0704 1723

În acest caz, am adăugat la finalul ultimului bloc un X pentru a avea aceeaşi dimensiune.

Aplicăm transformarea $C \equiv M^{29} \ (mod\ 2633)$ pentru fiecare bloc în parte, de exemplu $C \equiv 1907^{29} \equiv 2199 \ (mod\ 2633)$, şi obţinem:

2199 1745 1745 1206 2437 2425 1729 1619 0935 0960

1072 1541 1701 1553 0735 2064 1351 1704 1841 1459

care constituie mesajul criptat. Remarcăm că, faţă de celelalte criptosisteme prezentate, în forma criptată mesajul nu mai poate fi transformat în litere.

Pentru decriptare, se foloseşte cheia d, unde d este inversul modulo $p-1$ al cheii e. Din $e \cdot d \equiv 1 \ (mod\ p-1)$, rezultă $e \cdot d = k(p-1)+1$, cu k, număr natural. Pentru a verifica dacă cheia d este cea corectă, să arătăm că transformarea D_d este inversa transformării E_e. Pentru un bloc C, arbitrar ales, folosind mica teoremă a lui Fermat, obţinem: $D_d(C) \equiv C^d \equiv D_d(E_e(M)) \equiv M^{e \cdot d} \equiv M^{k(p-1)+1} \equiv M \cdot \left(M^{p-1}\right)^k \equiv M \ (mod\ p)$.

Pentru exemplul anterior, obţinem $d \equiv -363 \equiv 2269 \ (mod\ 2632)$ rezolvând ecuaţia $29d - 2632k = 1$ cu ajutorul algoritmului extins al lui Euclid. Pentru a decripta mesajul secret, vom calcula pentru fiecare bloc $0 \leq C \leq 2633$, $M \equiv C^{2269} \ (mod\ 2633)$ şi, apoi, fiecare echivalent numeric de două cifre va fi înlocuit cu litera corespunzătoare, regăsind mesajul iniţial.

Procesul de criptare şi cel de decriptare pentru criptosistemul de exponenţiere modulară se face rapid, folosind algoritmul de ridicare repetată la pătrat şi reducere modulo p, respectiv algoritmul lui Euclid extins.

În general, criptanaliza nu mai poate fi făcută rapid. Presupunem că se ştie numărul prim p folosit şi s-a stabilit că blocul C_0 corespunde blocului M_0, adică $C_0 \equiv M_0^e \ (mod\ p)$. Atunci, avem de rezolvat această congruenţă pentru a afla cheia e (conform teoremei 6.3.1, congruenţa are soluţie unică). e este atunci logaritmul lui C_0 în baza M_0 modulo p. Vom discuta despre algoritmii folosiţi pentru calculul logaritmului discret în capitolul 12. Oricum, aceşti algoritmi, pentru p convenabil ales, sunt foarte lenţi. De obicei, se aleg numere prime p cu proprietatea că $p-1$ nu are numai factori primi mici: de exemplu, $p = 2q+1$, număr prim unde q este şi el un număr prim mare.

Criptosistemele exponenţiale pot fi utilizate şi pentru a stabili chei comune, chei ce pot fi folosite de două sau mai multe persoane. Pentru aceasta, se alege p, un număr prim mare şi un întreg a cu $(a, p) = 1$. Considerăm cazul a două persoane.
Fiecare alege o cheie e_i, cu $(e_i, p-1) = 1$, $i \in \{1, 2\}$. Pentru a determina cheia comună, Alice trimite lui Bob $x \equiv a^{e_1} \pmod p$, $1 \leq x \leq p-1$. Bob găseşte cheia comună k calculând $k \equiv x^{e_2} \equiv a^{e_1 e_2} \pmod p$, $k < p$. Analog, Bob trimite $y \equiv a^{e_2} \pmod p$, $y < p$ lui Alice care află cheia comună prin $k \equiv y^{e_1} \equiv a^{e_1 e_2} \pmod p$.

8.5 DES

Fără a intra în amănunte, prezentăm câteva informaţii generale despre *Data Encryption Standard (DES).* El este cel mai răspândit sistem criptografic cu cheie secretă folosit în prezent, atât de guverne cât şi de companii particulare. *DES* a fost proiectat de IBM şi aprobat în anul 1977 de *U.S. National Bureau of Standards (NBS)* care acum se numeşte *U.S. National Institute of Standards and Technology (NIST).* Acest standard (algoritm) a fost publicat prima dată în anul 1977 (*FIPS 46- Federal Information Proccesing Standard 46*) şi este revăzut la fiecare 5 ani.

Standardul este public şi toate caracteristicile sale sunt fixate. Algoritmul foloseşte transformări de transpoziţie, substituţie şi operaţii neliniare. Ele se aplică în 16 iteraţii fiecărui bloc al unui mesaj. Mesajul se împarte în blocuri de 64 biţi. Cheia secretă folosită este formată din 56 biţi aleşi dintr-o cheie cu 64 biţi. Fiecare unitate de mesaj M de 64 biţi este transformată într-o unitate de aceeaşi dimensiune C a textului cifrat, după cum urmează:

Se aplică la început o permutare de biţi, M devenind M'. Această permutare nu are o semnificaţie criptografică aparentă.

Apoi, *DES* împarte M' în jumătate obţinând L_0, (jumătatea din stânga) şi R_0, cealaltă jumătate. Fiecare au deci, 32 de biţi.

În a treia etapă, *DES* execută operaţiile următoare de 16 ori, pentru $i \in \{1, 2, \ldots, 16\}$:

$$\begin{cases} L_i = R_{i-1}, \\ R_i = L_{i-1} \oplus f(R_{i-1}, k_i), \end{cases}$$

unde $\oplus$ este operatorul *sau exhaustiv*, iar f este o funcţie care transformă o jumătate dreaptă de 32 biţi cu ajutorul unei chei k_i, de fiecare dată diferită, pentru a rezulta tot un bloc de 32 biţi.

În final, textul pre-cifrat $C' = (R_{16}, L_{16})$ este permutat cu inversa permutării iniţiale pentru a obţine textul cifrat C.

Pentru decriptare, algoritmul este parcurs în sens invers.

Toate aceste vaste acţiuni binare pot fi încorporate într-un singur microcip construit special în acest scop. Astfel, *DES* se poate implementa într-un mod foarte eficient.

Deoarece s-a arătat că o criptanaliză a acestui sistem poate fi realizată relativ uşor, se preferă sistemul *Triple DES (TDES)* care presupune criptare multiplă. Astfel, mesajului i se aplică de trei ori câte un *DES* diferit. Dacă E_k, D_k reprezintă transformările de criptare şi decriptare pentru un *DES* cu cheia k, pentru criptarea mesajului M cu ajutorul lui *TDES,* transformarea este dată de $C = E_{k_3}(D_{k_2}(E_{k_1}(M)))$. Pentru decriptare, aplicăm $M = D_{k_1}(E_{k_2}(D_{k_3}(C)))$.

Pentru mai multe informaţii, cei interesaţi pot consulta [25].

Exerciţii propuse

Considerăm că, pentru toate exerciţiile următoare, alfabetul este cel al limbii engleze, format din 26 de litere.

1. Decriptaţi textul cifrat $RTOLK\ TOIK$, ştiind că a fost criptat folosind transformarea afină $C \equiv 3M + 24\ (mod\ 26)$.

2. Dacă cea mai des folosită literă dintr-un text lung cifrat este Q şi presupunem că pentru criptarea mesajului iniţial s-a folosit o transformare de deplasare, aflaţi valoarea plauzibilă a cheii de criptare.

3. Folosind o transformare afină şi cheia de criptare $(a, b) = (13, 9)$, criptaţi textul $HELP\ ME$.

4. Presupunem că studiem un text lung cifrat, criptat cu ajutorul unei transformări afine. Dacă literele Y şi V, în această ordine, prezintă cea mai mare frecvenţă în text, găsiţi o posibilă valoare a cheii de criptare.

5. Presupunem că un text a fost criptat folosind un cifru diagrafic. Perechile de litere care apar cel mai des în textul cifrat sunt KH şi XW. Stabiliţi o posibilă matrice de criptare, folosită în această situaţie.

6. Determinaţi cifrul produs, obţinut prin folosirea transformării $C \equiv 17M+3 \ (mod\ 26)$ urmată apoi de transformarea $C \equiv 5M+13 \ (mod\ 26)$.

7. Câte perechi de litere rămân neschimbate dacă criptarea mesajului se face folosind transformarea:

$$\begin{cases} C_1 \equiv 7M_1 + 17M_2 \ (mod\ 26) \\ C_2 \equiv M_1 + 6M_2 \ (mod\ 26) \end{cases} \quad ?$$

8. Presupunem că realizăm produsul unui cifru de tip Hill cu blocuri de lungime n cu un cifru de acelaşi tip, dar pentru blocuri de lungime m. Arătaţi că cifrul produs este tot un cifru Hill cu blocuri de lungime $[m, n]$.

9. Folosind o criptare exponenţială cu $p = 101$, $e = 3$ criptaţi mesajul $WE\ ARE\ THE\ CHAMPIONS$.

10. Textul 1213 0902 0539 1208 1234 1103 1374 este obţinut printr-o criptare exponenţială unde $p = 31$ şi $e = 11$. Determinaţi textul iniţial.

11. Mesajul 04 19 19 11 04 24 09 15 15 este obţinut printr-o criptare exponenţială. Se presupune că se cunoaşte $p = 29$ şi faptul că blocul 24 corespunde literei U din mesajul de bază. Stabiliţi care este mesajul iniţial.

CAPITOLUL 9

Criptografie cu cheie publică

În criptarea tradiţională, cheile de criptare şi decriptare trebuie păstrate secrete. Cum în trecut criptografia era folosită cel mai des în scopuri militare sau diplomatice, exista de fiecare dată un grup restrâns, bine definit, de utilizatori care puteau uşor împărţi şi distribui periodic cheile. Generarea, transmiterea şi stocarea acestor chei se numeşte *managementul cheilor*. Criptarea cu cheie secretă are deseori probleme în a oferi o gestionare securizată de chei, mai ales pentru sisteme deschise, cu un mare număr de utilizatori.

În prezent, aplicaţiile criptografiei s-au extins şi includ multe alte domenii în care sistemele de comunicaţii joacă un rol esenţial (colectarea şi stocarea de informaţii confidenţiale, tranzacţii financiare electronice). De multe ori există o reţea mare de utilizatori în care un grup restrâns trebuie să păstreze secretul comunicaţiei atât faţă de ceilalţi din reţea, cât şi faţă de persoane din afară. La fel, este posibil ca în urma unei comunicări avute, unul dintre parteneri trebuie să transmită o parte a informaţiei secrete unei terţe persoane.

În loc să rezolve problema managementului de chei, Whitfield Diffie şi Martin Hellman au introdus conceptul de criptografie cu cheie publică în anul 1976 în lucrarea *New Directions in Cryptography*. Astfel, ei furnizează o metodă nouă, ingenioasă, pentru schimbul de chei la care

securitatea se bazează pe imposibilitatea de a rezolva problema logaritmilor discreţi. Chiar dacă cei doi nu au realizat la acel moment, în mod practic, un criptosistem cu cheie publică, ideea a generat un interes deosebit şi o activitate intensă în domeniu. În anul 1977, Rivest, Shamir şi Adleman au descoperit prima schemă practică de criptare cu cheie publică şi de semnătură, *RSA*, bazată tot pe o problemă dificilă din punct de vedere computaţional, problema *factorizării numerelor mari*. Cu toate că anii 80 au adus noi metode de factorizare, acestea nu au slăbit securitatea criptosistemului *RSA*. O altă clasă de scheme practice cu cheie publică, bazată pe problema logaritmului discret, este găsită de ElGamal în anul 1985.

Criptosistemele cu cheie publică au două utilizări principale: *criptarea* şi *autentificarea* (semnătura digitală). Fiecare persoană primeşte o pereche de chei formată dintr-o cheie publică care este făcută cunoscută şi o cheie privată care este păstrată secretă. Astfel, necesitatea împărţirii informaţiei secrete de către două persoane care comunică este eliminată. Toate comunicaţiile implică doar cheile publice; nici o cheie privată nu se transmite sau se împarte cu cineva. Deci, nu mai este nevoie să folosim un canal sigur de comunicaţie. Singura cerinţă este ca aceste chei publice să fie asociate cu utilizatorii lor într-un mod autentificat (de încredere). Oricine poate trimite un mesaj confidenţial, dar mesajul poate fi decriptat cu o cheie privată, care este în posesia unică a destinatarului dorit. Astfel, cu ajutorul criptării cu cheie publică, este posibil să se realizeze o comunicaţie secretă între două persoane fără ca acestea să aibă un contact iniţial, fără să stabilească dacă au încredere unul în celălalt.

În criptosistemele cu cheie publică, cheia privată este mereu legată matematic de cheia publică. De aceea, este întotdeauna posibil să ataci un sistem cu cheie publică dobândind cheia privată din cheia publică. În mod natural, pentru a putea să apărăm sistemul, trebuie să facem ca problema obţinerii cheii private să fie cât mai dificilă posibil. Astfel, criptosistemele cu cheie publică se bazează pe probleme care, din anumite puncte de vedere sunt greu de rezolvat. Dificultatea se referă mai mult la cerinţele computaţionale necesare găsirii unei soluţii, decât la conceperea problemei. Aceste probleme se numesc ***probleme dificile.***

Procesul de criptare se realizează sub următoarea formă, indiferent de criptosistemul folosit: Alice trimite lui Bob un mesaj secret, criptându-l cu cheia publică a lui Bob. Acesta foloseşte cheia sa privată pentru a decripta mesajul primit şi îl citeşte.

Pentru a semna un mesaj, Alice realizează un calcul ce foloseşte cheia ei privată şi mesajul. Rezultatul este numit *semnătură digitală* şi se ataşează mesajului. Bob, pentru a verifica semnătura, efectuează un calcul ce implică mesajul, semnătura şi cheia publică a lui Alice. Dacă rezultatul este corect conform cu o relaţie matematică simplă, prescrisă, semnătura este cea originală. În caz contrar, semnătura este falsă sau mesajul a fost alterat.

Cele mai mari avantaje ale criptării cu cheie publică sunt creşterea securităţii şi posibilitatea de a furniza semnături digitale care nu pot fi repudiate. Un mare dezavantaj al ei este viteza, multe sisteme cu cheie secretă fiind mult mai rapide decât cele cu cheie publică. Oricum, criptarea cu cheie publică nu are rolul de a înlocui criptarea cu cheie secretă, ci de a mări securitatea acesteia. Ele pot fi folosite şi împreună, un astfel de protocol numindu-se *criptosistem hibrid.* În unele cazuri, criptarea cu cheie publică nu este necesară, fiind suficientă criptarea cu cheie secretă. De exemplu, sunt situaţii în care utilizatorii se întâlnesc în particular sau o singură autoritate cunoaşte şi administrează toate cheile, ca de exemplu un sistem bancar închis. Cum acesta cunoaşte deja toate cheile, nu mai are rost ca unele să fie publice şi altele secrete. Dar, acest ultim caz poate deveni impracticabil dacă numărul utilizatorilor creşte; astfel de limitări nu sunt necesare în criptarea cu cheie publică, care se potriveşte cel mai bine unui mediu deschis, cu un mare număr de utilizatori.

Găsirea de noi criptosisteme cu cheie publică şi îmbunătăţirea mecanismelor criptografice existente continuă într-un ritm alert.

9.1 RSA

Criptosistemul RSA a fost realizat de Ronald Rivest[1], Adi Shamir[2] şi Leonard Adleman[3], în anul 1977. El este un criptosistem cu cheie publică care realizează atât criptare de mesaje, cât şi autentificare (semnătură digitală).

Algoritmul RSA funcţionează astfel: se aleg două numere prime mari, p şi q şi se calculează $n = pq$, numit modul. Se alege e, $e < n$ şi prim cu $(p-1)(q-1) = \phi(n)$. Atunci e are invers modulo $\phi(n)$. Fie d acesta. e poartă numele de exponent public iar d se numeşte exponent privat. Cheia publică este perechea (n, e) iar cheia privată este (n, d). Factorii p şi q pot fi distruşi sau păstraţi cu cheia secretă.

Numerele folosite ca modul $n = pq$ se numesc numere RSA. Ele sunt listate în *Factoring Challenge of RSA Security*[4] şi sunt alese pentru proprietarea de a fi greu de factorizat. Aceste numere au fost denumite la început după numărul de cifre zecimale pe care le au. De exemplu, $RSA-100$ este un număr RSA cu 100 de cifre zecimale. Mai târziu, s-a trecut la indicarea numerelor în funcţie de scrierea lor binară. De exemplu, $RSA-576$ are 576 de cifre binare, adică 174 de cifre zecimale.

De obicei, numerele prime p şi q sunt alese astfel încât $p \pm 1$ şi $q \pm 1$ sunt divizibile cu numere prime mari, altfel există metode rapide de factorizare, ca de exemplu, metoda Pollard rho (vezi 11.4). Ele se pot genera aleator. De exemplu, se poate porni de la un număr aleator mare m. Dacă el este par, se alege $m + 1$. Cu ajutorul testului probabilistic

---

[1]Profesor de inginerie electronică şi informatică la Institutul de Tehnologie Massachussets (MIT), conducătorul laboratorului Cryptography and Information Security Group. A fondat RSA Data Security.

[2]Profesor la Departamentul de Matematici Aplicate şi Informatică la Institutul de Ştiinte Weizmann, Israel. A studiat diferite tipuri de atacuri pe criptosisteme diferite, cum ar fi criptosistemul rucsac, scheme şi tehnici criptografice, criptanaliză diferenţială.

[3]Coleg cu Rivest la MIT. El a reuşit să spargă primele 42 de criptosisteme realizate de Rivest şi Shamir. Doar al 43-lea a rezistat şi a fost considerat optim. Acum este profesor la Departamentul de Informatică al Universităţii California de Sud. Activitatea sa principală se desfăşoară în domeniul informaticii teoretice.

[4]RSA Security Data a început să sponsorizeze în martie 1991 *RSA Factoring Challenge* pentru a încuraja cercetarea în teoria computaţională a numerelor şi în studierea dificultăţilor practice a factorizării numerelor mari. Acest lucru este folositor utilizatorilor algoritmului RSA în alegerea unei chei de lungime corespunzătoare cu nivelul de securitate dorit.

Miller-Rabin (vezi 10.7) vedem dacă numărul convine. Dacă nu, repetăm pentru $m+2, m+4, \ldots$ până găsim primul număr prim $\geq m$.

Mărimea unei chei în algoritmul RSA se referă la mărimea lui n. Cele două numere prime p, q trebuie alese astfel încât să aibă o mărime aproximativ egală. Mărimea modulului depinde de cerinţele de securitate. Cu cât modulul este mai mare, cu atât securitatea este mai mare, dar, în acelaşi timp, scade viteza de operare. Lungimea modulului trebuie aleasă în funcţie de valoarea datelor ce trebuie protejate, de timpul necesar de protecţie, de cât de puternice pot fi posibilele ameninţări.

În anul 1999, un grup condus de Herman te Riele, utilizând 300 de staţii de lucru şi PC-uri, a factorizat după şapte luni numărul $RSA-155$ în două numere prime cu 78 cifre binare. Până în prezent s-au mai factorizat $RSA-160$, $RSA-200$, $RSA-576$. De aceea Laboratoarele RSA recomandă chei de mărime de 1024 de biţi pentru corporaţii şi chei de 2048 de biţi pentru chei de valoare deosebită, cum ar fi cheia pentru autentificare.

Este normal să ne asigurăm că o cheie a unui utilizator expiră după o anumită dată, să zicem doi ani. Aceasta oferă posibilitatea de a schimba chei în mod regulat şi de a asigura nivelul dorit de securitate, folosind datele furnizate de Laboratoarele RSA.

Criptosistemul RSA este folosit în mod curent peste tot în lume. El se regăseşte în multe produse comerciale software, este construit în sisteme operaţionale curente de către Microsoft, Apple, Sun, Novell. În hardware, algoritmul RSA se regăseşte în securizarea telefoanelor, în reţeaua de carduri Ethernet. Algoritmul este inclus în toate protocoalele importante pentru asigurarea securităţii comunicaţiilor Internet, este utilizat în interiorul unor instituţii cum ar fi guvernul U.S.A., marile corporaţii, laboratoare naţionale şi universităţi.

Să vedem acum cum funcţionează acest algoritm pentru criptarea mesajelor.

Presupunem că mesajul este deja transformat ca în cazul criptării exponenţiale, doar că de această dată p este înlocuit cu n. Fiecare unitate de mesaj M este transformată după regula $C \equiv M^e \pmod{n}$ pentru a rezulta mesajul cifrat.

De exemplu, dacă alegem $n = 43 \cdot 59 = 2537$ şi $e = 13$, pentru a cripta mesajul

PUBLIC KEY CRYPTOGRAPHY

grupăm în blocuri de două litere pe care le transformăm în echivalenţi numerici de două cifre. Obţinem astfel,

1520 0111 0802 1004 2402 1724 1519 1406 1700 1507 2423.

Fiecare bloc este transformat prin $C \equiv M^{13} \ (mod\ 2537)$ şi vom obţine textul cifrat, format din

0095 1648 1410 1289 0811 2333 2132 0370 1185 1457 1084.

Pentru decifrare, este nevoie de d, care în acest caz este $d = 937$.

În practică, sistemul RSA este des folosit împreună cu DES. Atunci când Alice doreşte să trimită un mesaj lui Bob, mai întâi criptează mesajul cu DES, folosind o cheie aleasă aleator, apoi foloseşte cheia publică a lui Bob pentru a cripta cheia DES. Mesajul criptat DES şi cheia DES criptată RSA formează un criptosistem hibrid, care este transmis lui Bob. Acesta decriptează cheia DES cu cheia sa privată şi apoi utilizează cheia DES pentru a decripta mesajul. În acest fel se combină viteza ridicată a DES-ului cu managementul de chei al sistemului RSA.

Atât criptarea cât şi autentificarea au loc fără a împărţi chei private; sunt folosite doar cheile publice ale unei alte persoane şi cheile private ale persoanei în discuţie.

În final, prezentăm câteva din variantele de a încerca criptanaliza acestui sistem.

1. O variantă este aceea de a încerca factorizarea lui n prin diverse metode.

2. De asemenea, cum problema factorizării lui n în acest caz este echivalentă cu cea a cunoaşterii lui $\phi(n)$, putem încerca să aflăm valoarea lui $\phi(n)$. Dacă aceasta este cunoscută, din relaţiile:

$$\begin{aligned} p + q &= n - \phi(n) + 1 \\ p - q &= (p+q)^2 - 4n, \end{aligned}$$

rezultă

$$p = \frac{1}{2}\left[(p+q) + (p-q)\right], \ q = \frac{1}{2}\left[(p+q) - (p-q)\right].$$

3. Presupunem acum că putem determina d astfel ca $a^{de} \equiv a \ (mod\ n)$, pentru toţi a primi cu n. Acest lucru înseamnă că $de - 1$ este multiplu

al celui mai mic multiplu comun al numerelor $p-1, q-1$. A cunoaşte $m = de - 1$ este un rezultat mai slab decât dacă l-am cunoaşte pe $\phi(n)$. Cu toate acestea, şi în acest caz, există o metodă prin care n poate fi factorizat, cu o mare probabilitate.

Deci, presupunem $n = pq$, produsul a două numere prime mari, m, un număr natural cu proprietatea că $a^m \equiv 1 \ (mod\ n)$, pentru orice a, prim cu n. Observăm că m trebuie să fie număr par deoarece relaţia trebuie să se verifice şi pentru $a = -1$. Mai întâi verificăm dacă $\frac{m}{2}$ are aceeaşi proprietate cu m, caz în care înlocuim m cu $\frac{m}{2}$. Dacă nu, congruenţa $a^{\frac{m}{2}} \equiv 1 \ (mod\ n)$ nu este verificată pentru cel puţin jumătate din valorile lui a modulo $\phi(n)$. Astfel, dacă pentru o mulţime suficient de mare de valori ale lui a, alese aleator, congruenţa se verifică, putem presupune (cu probabilitate mare) că m poate fi înlocuit cu $\frac{m}{2}$. Continuăm acest procedeu, până când congruenţa nu se mai verifică pentru $\frac{m}{2}$ de la acel pas.

Acum apar două posibilităţi:

(i) $\frac{m}{2}$ este multiplu de unul din numerele $p-1, q-1$, dar nu de ambele. Presupunem că $\frac{m}{2}$ este multiplu de $p-1$. Atunci, $a^{\frac{m}{2}} \equiv 1 \ (mod\ p)$ este adevărată pentru orice a, dar, pentru exact jumătate din valorile lui a, $a^{\frac{m}{2}} \equiv -1 \ (mod\ q)$ (vezi teorema 7.1.1).

(ii) $\frac{m}{2}$ nu este multiplu nici de $p-1$, nici de $q-1$. Atunci, $a^{\frac{m}{2}} \equiv 1 \ (mod\ n)$ se verifică pentru exact un sfert din valorile lui a, $a^{\frac{m}{2}} \equiv -1 \ (mod\ n)$ pentru acelaşi număr de valori. Pentru cealaltă jumătate de valori a lui a, $a^{\frac{m}{2}} \equiv 1 \ (mod\ p)$ şi $a^{\frac{m}{2}} \equiv -1 \ (mod\ q)$, sau invers.

Astfel, alegând aleator valori pentru a, vom găsi cu mare probabilitate un a pentru care $a^{\frac{m}{2}} - 1$ este multiplu de p dar nu de q, sau invers. Când am aflat un astfel de a, din $(n, a^{\frac{m}{2}} - 1) = p$ rezultă un factor al lui n.

Până în prezent, nu s-au găsit metode de a criptanaliza un astfel de sistem fără a factoriza numărul n.

9.2 Criptosisteme bazate pe DLP

Problema logaritmului discret, cunoscută şi sub forma *DLP*, este o altă ***problemă dificilă.*** Dacă lucrăm cu numere reale, exponenţierea a^x nu este mult mai uşoară decât operaţia inversă. Dacă presupunem că lucrăm însă într-un grup finit, cum ar fi $U(\boldsymbol{Z}_n)$, cu ajutorul metodei de ridicare repetată la pătrat, se poate calcula rapid a^x pentru valori mari ale lui x. Problema inversă, poartă numele de problema logaritmului discret: cunoscând b, care ştim că este de forma a^x, cum determinăm $x = log_a b$? Cuvântul *discret* face distincţia dintre cazul grupurilor finite şi situaţia clasică. Această problemă va fi tratată pe larg în capitolul 12.

Sistemul de schimbare de chei Diffie-Hellman-Merkle

Datorită faptului că criptosistemele cu cheie publică sunt relativ mai încete decât criptosistemele clasice (cel puţin în stadiul actual de cunoaştere tehnologică şi teoretică), este bine să le folosim împreună cu acestea. De exemplu, dacă două persoane trebuie să se pună de acord asupra unei chei comune secrete, printr-o reţea publică, pentru a fi folosită apoi în schimbul de mesaje realizate cu criptosisteme clasice, se poate folosi criptarea cu cheie publică pentru secretizarea cheii şi criptosistemul *DES* pentru transmiterea mesajelor.

Primul astfel de protocol a fost realizat de Whitfield Diffie[5], Martin Hellman[6] şi Ralph Merkle[7]. El funcţionează astfel:

1. Se aleg q, un număr prim şi g, un generator al grupului finit $\boldsymbol{Z}_q^*$. Acestea sunt făcute publice.

2. Alice alege aleator un a, $1 \leq a \leq q-1$, calculează $g^a \ (mod\ q)$ şi îl trimite lui Bob. a este păstrat secret.

3. Bob alege şi el, în mod aleator b, $1 \leq b \leq q-1$, calculează $g^b \ (mod\ q)$ şi transmite valoarea aceasta lui Alice. b este păstrat şi el

[5]Inginer la *Sun Microsystems* în Palo Alto, California. Este cunoscut în special pentru că a descoperit în anul 1975 conceptul de criptare cu cheie publică pentru care i s-a decernat titlul de *Doctor Honoris Causa* de către *Swiss Federal Institute of Technology,* în 1992.

[6]Este considerat *tatăl* criptografiei (cu cheie publică) moderne.

[7]Teza sa de doctorat a avut tema *Secrecy, Authentification and Public Key Systems,* profesorul îndrumător fiind Hellman. Alături de Adleman, Diffie, Helmann, Rivest şi Shamir a primit premiul *ACM Kenellakis Award* în anul 1977. În 1998 i s-a decernat premiul *Feyman* în nanotehnologie iar în anul 2000, premiul *RSA* în matematică.

secret.

4. Alice şi Bob calculează amândoi $g^{ab} \ (mod\ q)$ care va fi cheia secretă pe care o vor folosi în următoarele comunicaţii.

O a treia persoană cunoaşte $g, q, g^a \ (mod\ q), g^b \ (mod\ q)$ şi trebuie să determine $g^{ab} \ (mod\ q)$. Securitatea sistemului se bazează pe următoarea presupunere:

Presupunerea Diffie-Helman-Merkle. Este imposibil din punct de vedere computaţional să se calculeze g^{ab} din g^a şi g^b.

Până în prezent nu s-a determinat o metodă prin care să se afle g^{ab} fără a calcula a şi b, cu ajutorul logaritmului discret. Teoretic, o altă cale ar exista, dar ea nu a fost găsită încă.

Criptosistemul ElGamal

În anul 1985, ElGamal[8] a propus un criptosistem cu cheie publică, bazat pe logaritmi discreţi, pentru a asigura securizarea comunicaţiilor:

1. Se aleg q, un număr prim mare şi un generator g pentru $\boldsymbol{Z}_q^*$, care sunt făcute publice.

2. Alice alege un a, $1 \leq a \leq q-1$, care este cheia secretă de decriptare, şi calculează $g^a \ (mod\ q)$, care este cheia publică de criptare.

3. Presupunem că Bob doreşte să-i trimită lui Alice un mesaj M format cu echivalenţi numerici $mod\ q$. El alege aleator b, $1 \leq b \leq q-1$ şi trimite lui Alice perechea de elemente

$$\left(g^b \ (mod\ q), Mg^{ab} \ (mod\ q)\right).$$

4. Cum Alice cunoaşte a, ea poate regăsi M, calculând $g^{ab} \ (mod\ q)$ şi apoi împărţind al doilea element din pereche la acesta.

Oricine poate rezolva problema logaritmului discret în corpul finit cu q elemente, poate găsi cheia secretă a din cheia publică g^a. Securitatea sistemului se bazează pe presupunerea Diffie-Helman-Merkle. Astfel, criptosistemul ElGamal este echivalent cu sistemul de schimbare de chei Diffie-Hellman.

[8] Ahmed ElGamal este profesor conducător al Departamentului de Inginerie Structurată al Universităţii California, San-Diego. Activitatea sa de cercetare se desfăşoară în domenii ca tehnologie informatică, inginerie structurată, studiu seismologic.

Criptosistemul Massey-Omura

Acest criptosistem este un alt sistem foarte cunoscut, folosit pentru transmiterea mesajelor.

1. Se alege q, o putere a unui număr prim, deci vom lucra într-un corp finit cu q elemente.

2. Fiecare utilizator îşi alege, în mod aleator, o cheie e, $1 \leq e \leq q-1$ astfel încât $(e, q-1) = 1$ şi calculează $d \equiv \overline{e}\ (mod\ q-1)$, folosind algoritmul lui Euclid extins.

3. Pentru ca Alice să trimită un mesaj M lui Bob, ea calculează $M^{e_A}\ (mod\ q)$ şi îl trimite acestuia. Când primeşte mesajul, Bob nu îl poate citi încă. El returnează lui Alice $M^{e_A e_B}\ (mod\ q)$ care îi trimite înapoi $M^{e_A e_B d_A} \equiv M^{e_B}\ (mod\ q)$. Bob descifrează mesajul prin $M \equiv M^{e_B d_B}\ (mod\ q)$.

9.3 Criptosisteme knapsack

Criptosistemul rucsac (knapsack) Merkle-Hellman a fost publicat în anul 1978. El se bazează pe *problema sumei unei submulţimi* din combinatorică, sau *problema rucsacului*, cum mai este întâlnită.
Această problemă presupune alegerea unui număr de obiecte cu greutate cunoscută dintr-o mulţime mare de astfel de obiecte aşa încât suma greutăţilor lor să fie egală cu o valoare stabilită iniţial. Tratată pe caz general, ea este inclusă în categoria ***problemelor dificile.***
Sub formă matematică, problema s-ar putea transcrie astfel:
Fie $\{a_1, a_2, \ldots, a_n\}$ o mulţime de numere naturale şi S, un număr natural. Să se determine dacă există $x_i \in \{0, 1\}$, $1 \leq i \leq n$, pentru care $\sum_{i=1}^{n} x_i a_i = S$.

În anumite situaţii, problema se poate rezolva uşor. De exemplu, dacă $a_i = 2^{i-1}$, $1 \leq i \leq n$, atunci problema se reduce la scrierea lui S în baza 2.

Un caz particular al problemei rucsacului este *problema rucsac supercrescătoare.*

Spunem că şirul de numere naturale $(a_i)_{i \geq 1}$ este *supercrescător* dacă $\sum_{i=1}^{j-1} a_i < a_j$, pentru $j \geq 2$.

De exemplu, $2, 3, 6, 12, 25, 51$ este o secvenţă supercrescătoare. Să rezolvăm problema:

$$2x_1 + 3x_2 + 6x_3 + 12x_4 + 25x_5 + 51x_6 = 68.$$

Pentru aceasta, cum $2 + 3 + 6 + 12 + 25 < 51$, $x_6 = 1$, altfel suma este mai mică decât 51. Rezultă $2x_1 + 3x_2 + 6x_3 + 12x_4 + 25x_5 = 17$ şi reluăm procedeul. Din $25 > 17$, obţinem $x_5 = 0$. Astfel, $2x_1 + 3x_2 + 6x_3 + 12x_4 = 17$, de unde $x_4 = 1$ (altfel, suma ar fi < 12). În final, din $2x_1 + 3x_2 + 6x_3 = 5$ rezultă $x_3 = 0, x_2 = 1, x_1 = 1$.

Pe caz general, problema rucsacului pentru şiruri supercrescătoare, $\sum_{i=1}^{n} x_i a_i = S$ unde $\{a_1, a_2, \ldots, a_n\}$ formează un şir supercrescător, se rezolvă astfel:

1. Determinăm x_n prin:

$$x_n = \begin{cases} 1, & S \geq a_n; \\ 0, & S < a_n. \end{cases}$$

2. Determinăm $x_{n-1}, x_{n-2}, \ldots, x_1$ folosind relaţiile:

$$x_j = \begin{cases} 1, & S - \sum_{i=j+1}^{n} x_i a_i \geq a_j; \\ 0, & S - \sum_{i=j+1}^{n} x_i a_i < a_j, \end{cases}$$

pentru $j \in \{n-1, n-2, \ldots, 1\}$. Trebuie remarcat faptul că, dacă această problemă are soluţie, ea este unică.

Să vedem acum cum funcţionează criptosistemul Merkle-Hellman.

1. Mai întâi, mesajul este transformat înlocuind fiecare literă cu echivalentul său numeric binar. Dacă presupunem, ca şi până acum, că alfabetul este format din 26 de litere, cum $25 = (11001)_2$, fiecare literă va avea un echivalent numeric format din 5 cifre binare:
$A - (00000)_2, B - (00001)_2, \ldots, Z - (11001)_2$.

2. Se alege un $n-$uplu supercrescător $a_1, a_2, \ldots, a_n$ (n este 5 sau un multiplu de 5, ţinând cont că fiecare literă este substituită cu un bloc de 5 cifre), un modul $m > 2a_n$ şi un număr natural w, prim cu m, numit multiplu. Aceste alegeri se fac prin procese aleatoare. De exemplu,

se poate considera o secvenţă arbitrară $l_1, l_2, \ldots, l_{n+1}$, de numere mai mici decât o anumită valoare convenabil aleasă, pe baza căruia se poate construi $a_1 = l_1$, $a_j = l_j + a_{j-1} + a_{j-2} + \ldots + a_1$, $2 \leq j \leq n$. m poate fi ales de forma $m = l_{n+1} + \sum_{i=1}^{n} a_i$. Pentru w, alegem aleator un $w_0 < m$ iar w va fi primul număr mai mare decât w_0, prim cu m.

3. Determinăm $n-$uplul $b_i \equiv wa_i \ (mod\ m)$, $0 < b_i < m$ pentru $1 \leq i \leq n$. Acesta este făcut public, el reprezentând cheia de criptare. Cheia de decriptare, care trebuie păstrată secretă, este $(\overline{w}, m)$. Cu ajutorul ei, se obţine uşor din $b_1, b_2, \ldots, b_n$ $n-$uplul iniţial.

4. Alice, pentru a trimite mesajul lui Bob, împarte mesajul format din echivalenţii numerici binari ai literelor în blocuri de n cifre binare $x_1x_2 \ldots x_n$ (dacă este nevoie, se completează ultimul bloc cu cifre de 1 pentru a obţine acelaşi număr de cifre). Pentru fiecare astfel de unitate de mesaj, se calculează suma $S = \sum_{i=1}^{n} x_i b_i$. Şirul format cu aceste sume formează mesajul cifrat.

5. Pentru a decripta mesajul, Bob calculează pentru fiecare sumă: $S_0 \equiv \overline{w}S \equiv \sum_{i=1}^{n} \overline{w} b_i x_i \equiv \sum_{i=1}^{n} x_i a_i \ (mod\ m)$, $0 < S_0 < m$.
Din $\sum_{i=1}^{n} x_i a_i < m$, rezultă $S_0 = \sum_{i=1}^{n} x_i a_i$. Această ecuaţie se poate rezolva uşor pentru că şirul $\{a_1, a_2, \ldots, a_n\}$ este supercrescător. Rezultă astfel $M = x_1x_2 \ldots x_n$. Întreg mesajul este regăsit înlocuind echivalenţii binari cu literele corespunzătoare.

De exemplu, folosim un $10-$uplu supercrescător:

$$(2, 11, 14, 29, 58, 119, 241, 480, 959, 1917),$$

$m = 3837$ $(m > 2a_{10})$, $w = 1001$, pentru a aplica sistemul la criptarea mesajului:

REPLY IMMEDIATELY

Formăm unităţi de mesaj alcătuite din 10 cifre binare (echivalenţii a două litere):

1000100100 0111101011 1100001000 0110001100

0010000011 0100000000 1001100100 0101111000

Formăm 10−uplul $b_i \equiv 1001a_i \ (mod\ 3837)$, $1 \leq i \leq 10$ şi obţinem $(2002, 3337, 2503, 2170, 503, 172, 3347, 855, 709, 417)$. Pentru fiecare bloc determinat anterior calculăm sumele $\sum_{i=1}^{10} x_i b_i$. Astfel, pentru primul bloc obţinem $S = b_1 + b_5 + b_8 = 3360$.

Mesajul cifrat este

3360 12986 8686 10042 3629 3337 5530 9729

Pentru decriptare, din congruenţa $1001\overline{w} \equiv 1 \ (mod\ 3837)$ rezultă $\overline{w} = 23$. Pentru fiecare bloc rezolvăm $23S \equiv \sum_{i=1}^{10} x_i a_i \ (mod\ 3837)$. Verificăm tot pentru primul bloc: $3360 \cdot 23 \equiv 540 \ (mod\ 3837)$. Din $540 = 480 + 58 + 2$, rezultă $x_1 = x_5 = x_8 = 1$ iar restul nuli, adică 1000100100.

Pentru un timp, acest sistem a fost considerat sigur. Dar, tipul de problemă rucsac pe care se bazează acest sistem este tot un caz particular: se obţine din problema supercrescătoare prin transformări simple (multiplicarea şi reducerea modulo m a fiecărui element din şir). În anul 1982, Shamir a spart acest criptosistem rucsac (într-o singură iteraţie), găsind un algoritm de rezolvare a acestuia. Chiar dacă Merkle a dezvoltat un alt astfel de criptosistem cu multiple iteraţii, nici acesta nu s-a dovedit imposibil de criptanalizat, Brickell fiind cel care a oferit un algoritm pentru acest caz.

Astfel, criptosistemul Merkle-Hellman nu mai este astăzi considerat sigur, el fiind vulnerabil la o criptanaliză eficientă.

Un criptosistem rucsac, care nu se bazează pe exponenţiere modulară, este sistemul Chor-Rivest. El utilizează polinoame cu coeficienţi într-un corp finit. Prima dată, a fost publicat în anul 1984 şi a fost revizuit în 1988. În prezent, acesta este singurul criptosistem rucsac care încă nu a fost spart. Pentru mai multe informaţii, se poate studia [12], [15].

9.4 Semnătură digitală

Presupunem că Alice îi trimite un mesaj criptat lui Bob. De obicei, pentru a fi mai sigur, unul din blocurile mesajului este *blocul de semnătură*. Bob poate identifica acest bloc deoarece, la decriptare, acesta nu are înţeles.

Prezentăm în continuare câteva scheme de semnătură:

Schemă bazată pe criptosistemul RSA

1. Presupunem că (n_A, e_A) este cheia publică a lui Alice iar (n_B, e_B) cea a lui Bob. Cheile secrete de decriptare sunt d_A, respectiv, d_B. Pentru ca Alice să-i trimită lui Bob semnătura sa, ea calculează: $S_A \equiv \left(M^{d_A} \ (mod\ n_A)\right)^{e_B} \ (mod\ n_B)$, dacă $n_A < n_B$ sau
$S_A \equiv (M^{e_B} \ (mod\ n_B))^{d_A} \ (mod\ n_A)$, pentru cazul $n_A > n_B$.

Ea trimite apoi S_A ca unitate de mesaj cifrat lui Bob. În ambele situaţii, inegalitatea precizată ne asigură că expresia din paranteză nu este mai mare decât cheia care reprezintă modulul în raport cu care se face calculul.

2. În primul caz, Bob poate verifica autenticitatea mesajului ridicând la puterea d_B modulo n_B şi apoi la puterea e_A modulo n_A. Pentru celălalt caz, el va face acelaşi calcul, dar în ordine inversă.

Schemă bazată pe criptosistemul ElGamal

1. Alice alege un număr prim p şi două numere naturale aleatoare $g, x < p$. Ea calculează $y \equiv g^x \ (mod\ p)$, face public (y, g, p) şi păstrează secret x.

2. Apoi, Alice alege aleator k, prim cu $p-1$ şi calculează:

$$a \equiv g^k \ (mod\ p),\ b \equiv \overline{k}(M - xa) \ (mod\ p-1).$$

Acum Alice a generat semnătura (a, b). Ea trebuie să păstreze secret şi pe k.

3. Pentru a verifica semnătura, Bob vede dacă $y^a a^b \equiv g^M \ (mod\, p)$ este adevărată.

Semnătura digitală standard

În anul 1991, Institutul Naţional de Standarde şi Tehnologie al guvernului U.S.A., *NIST*, a propus un algoritm pentru semnături digitale. Algoritmul este cunoscut sub numele *DSA*, *Digital Signature Algorithm*. *DSA* a devenit *Standard pentru semnături digitale, DSS*, fiind prima schemă de semnătură recunoscută de orice guvern. El este destinat a fi folosit în poşta electronică, transferări electronice de bani, schimb electronic de date, distribuţie software, stocare de date şi alte aplicaţii care necesită asigurarea integrităţii datelor şi autentificarea acestora.

Rolul lui DSS este asemănător lui DES, adică trebuie să furnizeze o metodă standard de semnătură care să fie folosită atât de guvern cât şi de organizaţii comerciale. Deoarece, pentru a construi semnături digitale, este necesară criptarea cu cheie publică, $NIST$ a ales ca schema de semnătură digitală să se bazeze pe problema logaritmului discret.

DSA/DSS constă în două procese principale: generarea semnăturii, folosind o cheie privată, şi verificarea acesteia cu ajutorul unei chei publice. Algoritmul funcţionează astfel:

1. *Generarea cheii DSA*

1.1. Fiecare expeditor, Alice, alege un număr prim q de aproximativ 160 biţi, folosind un generator aleator de numere şi un test de primalitate.

1.2. Ea alege un al doilea număr prim p, $p \equiv 1 \ (mod\ q)$, de aproximativ 512 biţi.

1.3. Alice alege un generator al unicului subgrup ciclic de ordin q al grupului $\boldsymbol{Z}_p^*$. Pentru a realiza aceasta, verifică dacă pentru un g, ales aleator, $g^{\frac{p-1}{q}} \neq 1 \ (mod\ p)$. Dacă da, g este generator.

1.4. Alice alege aleator x, $0 < x < q$, care este cheia ei secretă şi îşi calculează cheia publică $y \equiv g^x \ (mod\ p)$.

2. *Generarea semnăturii DSA*

Pentru a realiza această etapă, Alice trebuie să folosească o funcţie $hash$. O funcţie hash este o aplicaţie uşor de calculat, $f : x \to h$ care transformă şiruri binare de lungime arbitrară foarte mare în şiruri binare de lungime fixată, mult mai scurtă, numită valoare hash. De exemplu, şiruri de 10^6 biţi pot fi transformate în şiruri de 150 biţi. Funcţia trebuie să mai verifice proprietatea că, pentru x, x' diferiţi, nu se poate obţine $f(x) = f(x')$.

2.1. Ea aplică o funcţie hash mesajului pentru a obţine $h < q$.

2.2. Alice alege aleator k, $0 < k < q$. Cu ajutorul acestuia îşi construieşte semnătura (r, s) prin:

$$r \equiv \left(g^k \ (mod\ p)\right) \ (mod\ q)$$
$$s \equiv \overline{k}(h + xr) \ (mod\ q).$$

Pentru a verifica semnătura:

Bob calculează $u_1 \equiv \overline{s}h \ (mod\ q)$ şi $u_2 \equiv \overline{s}r \ (mod\ q)$.

Să observăm mai întâi că, $g^{u_1}y^{u_2} = g^{\overline{s}(h+xr)} \equiv g^k \ (mod\ p)$. Dacă $r \equiv (g^{u_1}y^{u_2} \ (mod\ p)) \ (mod\ q)$, atunci semnătura este corectă. Dacă congruenţa nu se verifică, atunci mesajul a fost semnat incorect sau a fost semnat de un impostor. În acest caz, mesajul nu este considerat valid.

Această schemă de semnătură are avantajul că semnăturile sunt destul de scurte, fiind formate din două numere de 160 biţi. Pe de altă parte, securitatea sistemului depinde de imposibilitatea de a rezolva problema logaritmului discret în grupul multiplicativ $\boldsymbol{Z}_p^*$, cu p suficient de mare.

9.5 Împărţirea secretelor

Schemele de împărţire a secretelor au fost descoperite, independent, de Blakley şi Shamir. Principalul scop al acestora este gestionarea securizată a cheilor. În unele situaţii există o singură cheie secretă care permite accesul la mai multe fişiere importante. Dacă o astfel de cheie este pierdută (de exemplu, persoana care cunoaşte cheia nu este disponibilă sau computerul care depozitează cheia este distrus), atunci toate fişierele sunt inaccesibile. Ideea de bază în împărţirea de secrete este de a diviza cheia secretă în mai multe părţi, numite *umbre* care sunt distribuite la persoane diferite aşa încât cheia secretă să poată fi regăsită dintr-o submulţime de umbre.

O schemă generală de împărţire a secretelor specifică numărul minim de umbre necesare la reconstituirea cheii secrete.

Un exemplu clasic de împărţire a secretelor este schema k *din* n sau schema $(k,n)-$*threshold* cu $1 < k < n$. Într-o astfel de schemă, există un expeditor, sau dealer şi n participanţi. Dealer-ul împarte secretul în n părţi şi dă fiecărui participant câte o parte astfel încât orice k părţi pot reconstitui secretul, dar orice $k-1$ părţi nu sunt suficiente pentru a-l determina. O astfel de schemă se numeşte *perfectă* dacă orice grup de cel mult $k-1$ participanţi nu poate afla mai multe informaţii despre secret decât o persoană din exteriorul grupului.

Cea mai simplă schemă *threshold* este bazată pe teoria congruenţelor şi pe teorema chinezească a resturilor. Pentru a construi o astfel de

schemă $(k,n)-$*threshold* putem folosi următorul algoritm, format din două etape principale: construirea umbrelor şi reconstituirea secretului din k umbre.

1. Notăm cu S secretul (este un număr) şi cu $s_1, s_2, \ldots, s_n$ umbrele care trebuie create.

Alegem secvenţa $m_1, m_2, \ldots, m_n$ de numere naturale care verifică condiţiile:
$(m_i, m_j) = 1$, pentru $i \neq j$,
$m_1 m_2 \ldots m_k > m_n m_{n-1} \ldots m_{n-k+2}$.

Determinăm secretul S astfel încât

$$m_n m_{n-1} \ldots m_{n-k+2} < S < m_1 m_2 \ldots m_k,$$

unde $m_n m_{n-1} \ldots m_{n-k+2}$ este cea mai mare valoare obţinută calculând produsul a $k-1$ numere din şir, iar $m_1 m_2 \ldots m_k$ reprezintă cea mai mică valoare obţinută dintre produsele de k numere.

Construim umbrele prin

$$s_i \equiv S \ (mod\ m_i),\ 1 \leq i \leq n.$$

Fiecare participant P_i va primi (s_i, m_i, M), unde $M = m_1 m_2 \ldots m_n$.

2. Să vedem acum dacă am definit o schemă $(k,n)-$*threshold.* Considerăm umbrele $s_{j_1}, s_{j_2}, \ldots, s_{j_k}$ cunoscute. Fiecare persoană P_{j_i}, folosind cheia sa secretă (s_{j_i}, m_{j_i}, M), calculează:
$M_{j_i} = \dfrac{M}{m_{j_i}}$, $N_{j_i} \equiv \overline{M}_{j_i}\ (mod\ m_{j_i})$ şi, în final $I_{j_i} = s_{j_i} M_{j_i} N_{j_i}$.

Folosind teorema chinezească a resturilor, găsim $s \equiv \sum_{i=1}^{k} I_{j_i}\ (mod\ M_j)$, unde $M_j = m_{j_1} m_{j_2} \ldots m_{j_k}$. Dar, din $0 < S < M_j$, rezultă $S = s$ şi, astfel, am reconstituit secretul.

Spre exemplu, să construim o schemă $(3,5)-$*threshold.*

Administratorul schemei alege şirul de numere:
$m_1 = 11, m_2 = 12, m_3 = 17, m_4 = 19, m_5 = 25$.
El calculează $M = 1065900$, $m_1 m_2 m_3 = 2244$, $m_4 m_5 = 475$ şi defineşte secretul $S = 1011$. Se observă că $475 < S < 2244$.
În final, calculează umbrele $s_i \equiv S\ (mod\ m_i)$, obţinând:
$s_1 = 21, s_2 = 3, s_3 = 8, s_4 = 4, s_5 = 11$. Fiecare persoană P_i va primi

(s_i, m_i, M). Să vedem cum obţin persoanele P_1, P_3, P_4 secretul S.
P_1 calculează $M_1 = \dfrac{M}{m_1} = 96900$, $N_1 \equiv \overline{M}_1 \ (mod\ 11)$, de unde $N_1 = 1$ şi $I_1 = 2034900$.
P_3 calculează $M_3 = \dfrac{M}{m_3} = 62700$, $N_3 \equiv \overline{M}_3 \ (mod\ 17)$, de unde $N_3 = 13$ şi $I_3 = 6520800$.
P_4 calculează $M_4 = \dfrac{M}{m_4} = 56100$, $N_4 \equiv \overline{M}_4 \ (mod\ 19)$, de unde $N_4 = 8$ şi $I_4 = 1795200$.

În final, rezultă $S \equiv I_1 + I_3 + I_4 = 10350900 \equiv 1011 \ (mod\ 3553)$ unde $m_1 m_3 m_4 = 3553$.

Dacă încercăm să regăsim secretul folosind doar umbrele s_1, s_3, obţinem $S \equiv I_1 + I_3 = 8555700 \equiv 76 \ (mod\ 187)$, ceea ce nu este corect.

Încheiem acest subcapitol cu prezentare schemei de împărţire a secretelor a lui Shamir. Aceasta este o schemă perfectă care se bazează pe interpolarea polinomială şi pe faptul că un polinom de gradul $k-1$ este unic determinat de cei k coeficienţi ai săi.

1. Construirea umbrelor.

Administratorul alege un număr prim p, cu $p > \max\{S, n\}$ unde S este secretul iar n, numărul de participanţi. Apoi, defineşte $a_0 = S$ şi alege în mod aleator $k-1$ coeficienţi independenţi $a_1, \ldots, a_{k-1}$ astfel încât $1 \leq a_i \leq p-1$, $1 \leq i \leq k-1$. Dealer-ul defineşte polinomul $f = \sum_{i=0}^{k-1} a_i X^i$, care este de fapt un polinom cu coeficienţi într-un corp finit cu p elemente. Umbrele secretului S vor fi create prin $s_j \equiv f(j) \ (mod\ p)$, pentru n valori diferite j, $1 \leq j \leq p-1$. Fiecare participant P_j primeşte (s_j, j), printr-un canal sigur.

2. Reconstituirea secretului.

Considerăm că un grup de k sau mai mulţi participanţi vor să determine secretul. Fiecare pereche (j, s_j) este considerată ca fiind un punct (x_j, y_j), unde $y_j = f(x_j)$. Pentru a determina funcţia polinomială al cărei grafic trece prin aceste puncte, folosim formula de interpolare Lagrange:

$$f(x) = \sum_{j=1}^{k} y_j \prod_{\substack{1 \leq l \leq k \\ l \neq j}} \frac{x - x_l}{x_j - x_l}.$$

Cum $S = a_0 = f(0)$, putem scrie $S = \sum_{j=1}^{k} c_j y_j$, unde $c_j = \prod_{\substack{1 \le l \le k \\ l \ne j}} \frac{x_l}{x_l - x_j}$.

Deci, fiecare grup de k participanţi va determina secretul calculând o combinaţie liniară a umbrelor, coeficienţii c_j nefiind secreţi.

Un caz simplu de vizualizat este pentru $k = 2$. Graficul funcţiei polinomiale este o dreaptă. Punctul A, în care dreapta intersectează axa Oy, are coordonatele $(0, f(0))$. Din $S = f(0)$, rezultă că secretul este ordonata punctului A. Fiecare umbră este de fapt un punct pe dreaptă.

Dacă considerăm orice două puncte, acestea determină în mod unic dreapta, deci găsim secretul. Dacă considerăm un singur punct, prin acesta pot trece o infinitate de drepte. În acest caz, secretul poate fi orice punct de pe axa Oy, deci nu îl putem afla.

Exerciţii propuse

1. Fie $n > 1$ un număr liber de pătrate, iar d şi e numere naturale astfel încât $p - 1 \mid de - 1$, pentru orice divizor prim p al lui n (de exemplu, acesta poate fi cazul când $de \equiv 1 \ (mod\ \phi(n))$). Arătaţi că $a^{de} \equiv a \ (mod\ n)$, pentru orice întreg a.

2. Determinaţi numerele prime p şi q dacă $n = pq = 14647$ iar $\phi(n) = 14400$.

3. Precizaţi care dintre următoarele $5-$upluri sunt supercrescătoare:

i) $(3, 5, 9, 19, 40)$

ii) $(2, 6, 10, 15, 36)$.

4. Fie $A = \{2, 3, 4, 7, 11, 13, 16\}$. Determinaţi toate submulţimile B ale mulţimii A cu proprietatea că suma tuturor elementelor din B este egală cu 18.

5. Fie

i) $(2, 3, 7, 20, 35, 69)$ şi $S = 45$

ii) $(1, 2, 5, 9, 20, 49)$ şi $S = 73$

iii) $(1, 3, 7, 12, 22, 45)$ şi $S = 67$.

Pentru fiecare dintre aceste 6−upluri şi S, stabiliţi care dintre problemele rucsac sunt supercrescătoare. Găsiţi, pentru fiecare problemă rucsac, toate soluţiile, dacă acestea există.

6. Arătaţi că:

i) Pentru un $n-$uplu supercrescător, $(a_1, a_2, \ldots, a_n)$ se verifică $a_j \geq 2^{j-1}$, pentru $1 \leq j \leq n$.

ii) Orice $n-$uplu $(a_1, a_2, \ldots, a_n)$ care verifică $a_{j+1} \geq 2a_j$, pentru $1 < j < n$, este supercrescător.

7. Determinaţi secvenţa ce se obţine din $7-$uplul $(1, 3, 5, 10, 20, 41, 80)$ pentru multiplul $w = 17$ şi modulul $m = 162$.

8. Presupunem că un mesaj a fost criptat folosind un sistem rucsac cu cheia publică $(57, 14, 3, 24, 8)$. Cunoscând şi cheia privată $b = 23$, $m = 61$, reconstituiţi mesajul ştiind că mesajul cifrat are unităţile

14 25 89 3 65 24 3 49 89 24 41 25 68 41 71.

CAPITOLUL 10

Teste de primalitate

Încă din antichitate, matematicienii au fost fascinaţi de probleme ce implicau numere prime.

O problemă de bază ce se referă la numerele prime este aceea de a stabili dacă un anumit număr este prim sau nu. Un test care realizează acest lucru poartă numele de test de primalitate. Ele sunt importante şi în prezent, mai ales din punct de vedere practic, ţinând cont de utilizarea acestor numere în criptografie.

Testele de primalitate pot fi *deterministice* sau *probabilistice*.

Cele deterministice stabilesc cu certitudine dacă un număr este prim pe când testele probabilistice pot identifica în mod fals (cu o mică probabilitate) un număr compus ca fiind prim (invers nu este posibil). Aceste teste sunt mult mai rapide decât cele deterministice. Numerele care trec un test de primalitate probabilistic vor fi numite *probabil prime* până când primalitatea lor este demonstrată în mod deterministic. Testele probabilistice de primalitate folosesc pe lângă numărul n care este testat şi alte numere alese aleator dintr-o mulţime de probe. Orice astfel de test trebuie să dea răspunsul corect cu o mare probabilitate (de exemplu, mai mare decât $\frac{2}{3}$). Probabilitatea erorii poate fi micşorată repetând testul pentru mai multe valori probă independente.

Un test probabilistic de primalitate are următoarea structură de bază:

1. Aleg la întâmplare un număr b.

2. Verific o egalitate ce implică numerele b şi n, numărul testat. Dacă egalitatea nu este adevărată, n este compus şi b poartă numele de *martor* al lui n, testul oprindu-se.

3. Repetăm pasul 1 până se obţine certitudinea dorită. Dacă, după mai multe iteraţii, numărul n nu se dovedeşte compus, el este declarat *probabil prim*.

10.1 Ciurul lui Eratostene

Acesta este cel mai vechi test de primalitate cunoscut, apărut în jurul anului 240 î.e.n.[1] El funcţionează corect pentru orice numere prime. Considerat un număr n, pentru a testa dacă este prim, întocmim o listă cu toate numerele naturale pornind de la 2 până la n. Din ea se înlătură toate numerele care sunt multiplii de numerele prime $\leq \sqrt{n}$. Cele care rămân în listă sunt toate numere prime.

De exemplu, pentru a găsi numerele prime impare, mai mici decât 100, listăm întâi numerele impare de la 3 la 100. Primul număr din listă este 3, astfel el este primul număr prim impar. Înlăturăm din şir toţi multiplii lui 3 şi primul număr rămas este 5, care este deci, prim. Pentru el aplicăm acelaşi procedeu. Cum $11 > \sqrt{100}$, mai rămâne să aplicăm procedeul doar pentru 7. Toate numerele rămase în listă sunt numere prime.

10.2 Căutare de divizori prin încercări

Testul de căutare de divizori prin încercări, *trial division*, stabileşte dacă numărul n este prim, verificând dacă el are divizori primi $\leq \sqrt{n}$ conform teoremei 1.1.1.

De exemplu, pentru a testa dacă 211 este număr prim, vedem dacă unul dintre numerele 2,3,5,7,11 sau 13 este divizor al său.

[1] Eratostene (276-194 î.e.n,) a studiat la şcoala lui Platon în Atena. El a scris multe lucrări în domeniul matematicii, geografiei, astronomiei, istoriei, filozofiei, criticii literare. El este cunoscut pentru măsurătorile sale geografice printre care se numără şi faimoasa măsurare a circumferinţei pământului.

Pentru a îmbunătăţi aplicarea practică a acestei metode, facem observaţia următoare: toate numerele prime, mai puţin 2 şi 3 sunt de forma $6k \pm 1$.

Astfel, e mai practic să facem împărţirile pentru 2,3,5 iar apoi să vedem dacă numere congruente cu 1,7,11,13,17,19,23,29 modulo 30, mai mici decât $\sqrt{n}$, sunt divizori pentru n. Acest fel de factorizare e uneori numită *factorizare circulară.* Ea necesită mai multe împărţiri (unii divizori vor fi numere compuse), dar are avantajul că nu trebuie să avem la dispoziţie o listă de numere prime.

Oricum, cele două teste prezentate nu se aplică decât pentru numere mici; dacă n are mai mult de 25 cifre, avem nevoie de teste mai rapide.

10.3 Teste n-1. Testul Pepin

Dacă vom studia cu atenţie o listă formată din cele mai mari numere prime cunoscute, p, vom observa uşor că majoritatea acestora au o formă particulară, anume, $p-1$ sau $p+1$ se pot descompune foarte repede. Acest rezultat nu este neaşteptat pentru că există teste deterministice care verifică primalitatea numerelor de această formă.

În 1891, Lucas[2] a transformat mica teoremă a lui Fermat într-un test practic de primalitate, îmbunătăţit de Kraitchik şi Lehmer[3]:

Teoremă 10.3.1 *Fie $n > 1$. Dacă pentru orice factor prim p al lui $n-1$ există un întreg a astfel încât:*

1. $a^{n-1} \equiv 1 \ (mod\ n)$ *şi*
2. $a^{\frac{n-1}{p}} \neq 1 \ (mod\ n)$,

atunci, n este prim.

[2]François Edouard Anatole Lucas (1842-1891) este cunoscut în special pentru studiul făcut asupra şirului Fibonacci şi a şirurilor Lucas pe care le-a asociat acestuia. El a inventat metode de testare a primalităţii numerelor cu ajutorul cărora, în 1876 a arătat că M_{127} este prim. Acest număr este cel mai mare număr prim descoperit fără ajutorul computerelor.

[3]Derrick Norman Lehmer (1905-1991), profesor la Berkeley, a obţinut rezultate importante referitoare la funcţiile Lucas, teste de primalitate, fracţii continue, ecuaţii diofantice, tehnici computaţionale. El este considerat un pionier în aplicarea metodelor mecanice, incluzând şi computerul, pentru rezolvarea unor probleme de teoria numerelor.

Demonstraţie. Pentru a arăta că n este prim, demonstrăm că $\phi(n) = n-1$. De fapt, pentru a simplifica, arătăm că $n-1 \mid \phi(n)$.
Dacă presupunem contrariul, există p număr prim, $r > 0$ astfel încât $p^r \mid n-1$ şi $p^r \nmid \phi(n)$. Pentru acest p există a care verifică cele două condiţii din enunţul teoremei. Fie $m = ord_n(a)$. Atunci, $m \mid n-1$ dar $m \nmid \frac{n-1}{p}$. Astfel, $p^r \mid m$ şi din $m \mid \phi(n)$ ajungem la o contradicţie. □

De fapt, în această demonstraţie, se arată că grupul $U(\boldsymbol{Z}_n)$ are ordinul $n-1$, deci n este număr prim. Acest procedeu stă la baza tuturor testelor moderne de primalitate indiferent dacă acestea sunt simple, ca testul în discuţie, sau mai complicate, cum ar fi teste ce folosesc curbele eliptice sau corpuri de numere.

Teorema are un inconvenient: necesită factorizarea completă a lui $n-1$. Din acest motiv, Poklington a stabilit un rezultat care întăreşte teorema anterioară, fiind necesară doar factorizarea unui divizor al lui $n-1$.

Teoremă 10.3.2 (Teorema Poklington) *Fie $n-1 = p^k R$ unde p este număr prim, $p \nmid R$. Dacă există un întreg a astfel încât:*

1. $a^{n-1} \equiv 1 \pmod{n}$ *şi*
2. $(a^{\frac{n-1}{p}} - 1, n) = 1$,

atunci fiecare factor prim al lui n are forma $p^k r + 1$.

Demonstraţie. Fie q un divizor al lui n şi $m = ord_q(a)$. Din prima condiţie, $m \mid n-1$ iar din a doua, $m \nmid \frac{n-1}{p}$. Atunci, $p^k \mid m$. Astfel, $m = p^k l$. Din $m \mid q-1$ rezultă q de forma cerută. □

Putem generaliza teorema Poklington, obţinând testul:

Teoremă 10.3.3 *Fie $n-1 = F \cdot R$ unde $F > R$, $R < \sqrt{n}$,*
$F = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$. Dacă pentru fiecare $i = 1, \dots, k$ există b_i astfel încât:

1. $b_i^{n-1} \equiv 1 \pmod{n}$,
2. $\left(b_i^{\frac{n-1}{p_i}} - 1,\ n\right) = 1$,

atunci n este prim.

Dintre cazurile clasice ale teoremei 10.3.3, prezentăm următoarele două:

Teoremă 10.3.4 (Testul Pepin (1877)) *Fie $F_n = 2^{2^n} + 1$ al $n-$lea număr Fermat cu $n > 1$.*
F_n este prim dacă şi numai dacă $3^{\frac{F_n-1}{2}} \equiv -1 \ (mod\ F_n)$.

Demonstraţie. Dacă $3^{\frac{F_n-1}{2}} \equiv -1 \ (mod\ F_n)$, din teorema 10.3.3, luând $b = 3$, obţinem F_n număr prim. Reciproc, dacă considerăm F_n prim, Atunci, $\left(\frac{3}{F_n}\right) \equiv 3^{\frac{F_n-1}{2}} \ (mod\ F_n)$.
Dar, $\left(\frac{3}{F_n}\right) = \left(\frac{F_n}{3}\right) = \left(\frac{2}{3}\right) = -1$. □

Teoremă 10.3.5 (Teorema Proth (1878)) *Fie $n = h \cdot 2^k + 1$ cu $2^k > h$. Dacă există a, număr întreg, astfel încât $a^{\frac{n-1}{2}} \equiv -1 \ (mod\ n)$, atunci n este prim.*

10.4 Teste n+1. Testul Lucas-Lehmer

Pentru început, definim şirurile Lucas.

Fie p şi q numere întregi astfel încât $d = p^2 - 4q > 0$. Atunci, polinomul $X^2 - pX + q$ are rădăcini distincte:

$$a = \frac{1}{2}\left(p + \sqrt{d}\right),\ b = \frac{1}{2}\left(p - \sqrt{d}\right).$$

Prin inducţie, se arată că:

Lemă 10.4.1 $a^m = \frac{V_m + U_m\sqrt{d}}{2}$ *unde şirurile U_m, V_m sunt definite recursiv prin:*

$$U_0 = 0,\ U_1 = 1,\ U_m = pU_{m-1} - qU_{m-2},\ m \geq 2, \tag{10.1}$$

$$V_0 = 2,\ V_1 = p,\ V_m = pV_{m-1} - qV_{m-2},\ m \geq 2. \tag{10.2}$$

Obţinem, de fapt, pentru $n \geq 0$:

$$U_n = \frac{a^n - b^n}{a - b},\ V_n = a^n + b^n.$$

Aceste şiruri se numesc *şirurile Lucas asociate numerelor p şi q.* Un caz particular cunoscut se obţine pentru $p = 1,\ q = -1$. Atunci, U_n este şirul numerelor Fibonacci.

Lemă 10.4.2 *Şirurile Lucas verifică următoarele relaţii:*

$$V_{2n+2} = (p^2 - 2q)V_{2n} - q^2V_{2n-2}, \tag{10.3}$$
$$U_{2n+2} = (p^2 - 2q)U_{2n} - q^2U_{2n-2}, \tag{10.4}$$

pentru orice $n \geq 1$.

Demonstraţie. Aplicăm relaţia (10.1) şi obţinem:

$$\begin{aligned} U_{2n+2} &= pU_{2n+1} - qU_{2n} = p\left(pU_{2n} - qU_{2n-1}\right) - qU_{2n} \\ &= (p^2 - q)U_{2n} - pqU_{2n-1} = (p^2 - 2q)U_{2n} + q\left(U_{2n} - pU_{2n-1}\right) \\ &= (p^2 - 2q)U_{2n} - q^2U_{2n-2}. \end{aligned}$$

Cealaltă relaţie se obţine în acelaşi mod. □

Lemă 10.4.3 *Fie m un număr natural, relativ prim cu p şi cu q. Notăm* $p' \equiv \bar{q}(p^2 - 2q)\ (mod\ m)$. *Atunci, şirurile* $(U'_n)_{n\geq 0}$, $(V'_n)_{n\geq 0}$ *definite prin*

$$U'_n = \bar{p}q^{1-n}U_{2n}\ (mod\ m), \tag{10.5}$$
$$V'_n = \bar{q}^nV_{2n}\ (mod\ m), \tag{10.6}$$

pentru orice $n \geq 0$, *sunt şirurile Lucas, calculate modulo m, asociate numerelor* p' *şi* 1.

Demonstraţie. Arătăm că şirul $(U'_n)_{n\geq 0}$ verifică relaţia (10.1). Pentru aceasta,

$$U'_0 \equiv \bar{p}qU_0 = 0\ (mod\ m),\ U'_1 \equiv \bar{p}U_2 \equiv \bar{p}p \equiv 1\ (mod\ m).$$

Folosind lema 10.4.2, pentru $n \geq 1$ obţinem:

$$\begin{aligned} U'_{n+1} &\equiv \bar{p}\bar{q}^nU_{2n+2} \equiv \bar{p}\bar{q}^n(p^2 - 2q)U_{2n} - \bar{p}q^{2-n}U_{2n-2} \\ &\equiv \bar{p}q^{1-n}U_{2n}\bar{q}(p^2 - 2q) - \bar{p}q^{2-n}U_{2(n-1)} \equiv p'U'_n - 1 \cdot U'_{n-1}. \end{aligned}$$

În mod analog, se arată că

$$V'_0 \equiv 2\ (mod\ m), V'_1 \equiv p'\ (mod\ m), V'_{n+1} = p'V'_n - V'_{n-1}.\quad \square$$

Se poate stabili uşor că şirurile Lucas verifică următoarele identităţi:

$$U_{2n} = U_n V_n \tag{10.7}$$
$$U_{2n+1} = U_{n+1} V_n - q^n \tag{10.8}$$
$$V_{2n} = V_n^2 - 2q^n,\ n \geq 1 \tag{10.9}$$
$$V_n^2 = dU_n^2 + 4q^n \tag{10.10}$$
$$V_{2n+1} = V_{n+1} V_n - pq^n. \tag{10.11}$$

Aceste formule permit calculul elementelor din şir pentru valori mari ale lui n, mai ales dacă în descompunerea lui n apar mulţi factori pari.

Lemă 10.4.4 *Pentru p, q, a, definiţi anterior şi d care nu este pătrat modulo n, fie $2a \equiv s + t\sqrt{d}\ (mod\ n)$ pentru s, t numere întregi cu aceeaşi paritate. Dacă n este prim, atunci $2a^n \equiv s - t\sqrt{d}\ (mod\ n)$.*

Să reformulăm această lemă folosind şirul U_n. Observăm că lema afirmă cu necesitate că a^n este conjugatul complex al lui a modulo n. Din acest motiv, le înmulţim şi rezultă:

Lemă 10.4.5 *Cu p, q ca mai sus, dacă n este prim, atunci*

$$U_{n+1} \equiv 0\ (mod\ n).$$

Folosind aceste rezultate putem enunţa teorema corespunzătoare teoremei 10.3.1:

Teoremă 10.4.1 *Fie $n > 1$ un număr impar. Dacă există un şir Lucas astfel încât sunt verificate condiţiile:*

1. $\left(\frac{d}{n}\right) = -1,\ (n, dp) = 1,\ U_{n+1} \equiv 0\ (mod\ n)$
2. *Pentru orice factor prim r al lui $n+1$,* $\left(U_{\frac{n+1}{r}}, n\right) = 1,$

atunci n este prim.

De menţionat că putem folosi valori diferite pentru p, q cât timp valoarea lui d nu se modifică.

Un caz particular al acestui test este următorul, specific numerelor Mersenne:

Teoremă 10.4.2 (Testul Lucas-Lehmer(1930)) *Fie* $M_n = 2^n - 1$, *al* $n-$ *lea număr Mersenne. Considerăm şirul* s_k *definit recurent:*

$$s_0 = 4,\ s_{k+1} \equiv s_k^2 - 2\ (mod\ M_n),\ k \geq 1.$$

Pentru $n \geq 3$ *număr prim,* M_n *este număr prim Mersenne dacă şi numai dacă* $s_{n-2} \equiv 0\ (mod\ M_n)$.

Demonstraţie. Vom aplica testul corespunzător şirurilor Lucas enunţat în teorema 10.4.1.

Alegem $p = 2, q = -2$. Atunci, $d = 12$.

Calculăm mai întâi simbolul $\left(\frac{3}{M_n}\right)$. Folosind legea reciprocităţii pătratice şi lema lui Gauss, obţinem:

$$\left(\frac{3}{M_n}\right) = -\left(\frac{M_n}{3}\right) = \left(\frac{2}{3}\right) = -1.$$

Obţinem $\left(\frac{d}{M_n}\right) = \left(\frac{3}{M_n}\right) = -1$.

În cazul în care, în teorema 10.4.1, alegem pentru n numărul Mersenne M_n, cele două condiţii din enunţul teoremei devin:

1. $U_{M_n+1} \equiv 0\ (mod\ M_n)$
2. $\left(U_{\frac{M_n+1}{2}}, M_n\right) = 1$.

Arătăm că acestea sunt echivalente cu condiţia

$$V_{\frac{M_n+1}{2}} \equiv 0\ (mod\ M_n). \tag{10.12}$$

Presupunem că cele două condiţii ale testului se verifică. Atunci, din a doua relaţie, rezultă că $U_{\frac{M_n+1}{2}}$ are invers modulo M_n.
Din (10.7), ştim că $U_{M_n+1} = U_{\frac{M_n+1}{2}} V_{\frac{M_n+1}{2}}$. Prima condiţie implică atunci, $V_{\frac{M_n+1}{2}} \equiv 0\ (mod\ M_n)$.

Reciproc, dacă (10.12) se verifică, prima condiţie este imediată.
Fie t un divizor al lui M_n. Atunci, t este număr impar. Să presupunem

că $t \mid U_{\frac{M_n+1}{2}}$.
În cazul nostru, relaţia (10.10) arată că

$$V^2_{\frac{M_n+1}{2}} = dU^2_{\frac{M_n+1}{2}} + 4q^{\frac{M_n+1}{2}}.$$

Obţinem $V^2_{\frac{M_n+1}{2}} - 12U^2_{\frac{M_n+1}{2}} = 4(-2)^{\frac{M_n+1}{2}}$.
Aplicăm (10.12) şi astfel, $M_n \mid 12U^2_{\frac{M_n+1}{2}} + 4(-2)^{\frac{M_n+1}{2}}$.
În final rezultă $t \mid 4(-2)^{\frac{M_n+1}{2}}$, adică t este număr par.
Această contradicţie arată că M_n şi $U_{\frac{M_n+1}{2}}$ sunt prime între ele.

Pentru a încheia demonstraţia acestui test, aplicăm lema 10.4.3 pentru $p = 2, q = -2, m = M_n$. Atunci, $p' = -4$ şi $(-2)^n V'_n \equiv V_{2n} \ (mod\ M_n)$.

Astfel, folosind (10.9),

$$V'_{2n} = (-2)^{-2n} V_{4n} \equiv (-2)^{-2n} \left(V^2_{2n} - 2(-2)^{2n}\right) \equiv V'^2_n - 2 \ (mod\ M_n).$$

Deci, $V'_{2n} = V'^2_n - 2$, pentru $n > 0$.
Dacă notăm $s_j = V'_{2^j}$, pentru $j \geq 0$, obţinem şirul:
$s_0 = V'_1 = p' = -4$, $s_{j+1} = V'_{2^{j+1}} = V'_{2\cdot 2^j} = \left(V'_{2^j}\right)^2 - 2 = s_j^2 - 2$, $j > 0$.

De aici, relaţia (10.12) este echivalentă cu

$$V_{2^{n-1}} = V_{2\cdot 2^{n-2}} = (-2)^{2^{n-2}} V'_{2^{n-2}} = (-2)^{2^{n-2}} s_{n-2}.$$

Astfel, cele două condiţii din testul de primalitate 10.4.1 sunt echivalente cu $s_{n-2} \equiv 0 \ (mod\ M_n)$. □

Valoarea s_{n-2} poartă numele de *reziduu Lucas-Lehmer al lui n.*
Acest test este deosebit de rapid deoarece nu foloseşte împărţiri.

Spre exenplu, pentru $n = 7$, $M_7 = 2^7 - 1 = 127$. Şirul este dat de $s_0 = 4,\ s_1 \equiv 14 \ (mod\ 127),\ s_2 \equiv 67 \ (mod\ 127),\ s_3 \equiv 42 \ (mod\ 127),$ $s_4 \equiv 111 \ (mod\ 127),\ s_5 \equiv 0 \ (mod\ 127)$. Astfel, M_7 este prim.

Algoritm 10.4.1 (Algoritmul Lucas-Lehmer)
INPUT: un număr Mersenne $M_n = 2^n - 1$ cu $n \geq 3$.
OUTPUT: un răspuns referitor la primalitatea lui M_n.
1. Se verifică prin metoda obişnuită dacă n are un divizor d cu $2 \leq d \leq \sqrt{n}$. Dacă există, se returnează număr compus *şi se opreşte.*
2. $s \leftarrow 4$.

3. Pentru k de la 1 la $n-2$ calculează:
3.1. $s \leftarrow (s^2-2) \ mod \ M_n$.
4. Dacă $s=0$ returnează număr prim. *Altfel, returnează* număr compus.

10.5 Testul Fermat

Din teorema 3.4.4 ştim că, dacă n este număr prim şi $b \in \boldsymbol{Z}$, atunci $b^n \equiv b \ (mod \ n)$. Cu alte cuvinte, dacă există un întreg b pentru care $b^n \neq b \ (mod \ n)$, atunci n este număr compus.

De exemplu, pentru $n=129$ şi $b=2$ obţinem $2^{129} = \left(2^7\right)^{18} \cdot 8 = 128^{18} \cdot 8 \equiv (-1)^{18} 8 \equiv 8 \ (mod \ 129)$.

În China antică numerele n pentru care $2^n \equiv 2 \ (mod \ n)$ se considerau prime. Dar, reciproca micii teoreme a lui Fermat nu este adevărată. De exemplu, pentru numărul compus $n = 341 = 11 \cdot 31$ obţinem:

$$2^{10} \equiv 1 \ (mod \ 11) \tag{10.13}$$

$$2^{340} = \left(2^{10}\right)^{34} \equiv 1 \ (mod \ 11) \tag{10.14}$$

$$2^{340} = \left(2^5\right)^{68} = 32^{68} \equiv 1 \ (mod \ 31) \tag{10.15}$$

Din (10.14) şi (10.15) rezultă că $2^{340} \equiv 1 \ (mod \ 341)$. Astfel, chiar dacă 341 este compus, $2^{341} \equiv 2 \ (mod \ 341)$.

Definiţie 10.5.1 *Fie $b \geq 2$ un număr natural. Un numărul natural compus n care verifică relaţia:*

$$b^n \equiv b \ (mod \ n) \tag{10.16}$$

se numeşte pseudoprim cu baza b.

Tabelul B.1 (vezi Anexa B) prezintă cele mai mici numere pseudoprime cu primele 100 de baze.

Observaţie 10.5.1 *Dacă $(b,n)=1$, congruenţa (10.16) este echivalentă cu*

$$b^{n-1} \equiv 1 \ (mod \ n) \tag{10.17}$$

Lemă 10.5.1 *Fie d, n numere naturale astfel încât $d \mid n$. Atunci,*

$$2^d - 1 \mid 2^n - 1.$$

Teoremă 10.5.1 *Există o infinitate de numere pseudoprime cu baza* 2.

Demonstraţie. Arătăm că pentru n, număr pseudoprim impar cu baza 2, obţinem $m = 2^n - 1$ număr pseudoprim cu baza 2. Dacă demonstrăm această afirmaţie, cum 341 este pseudoprim cu baza 2, putem construi o infinitate de numere pseudoprime impare cu baza 2 formând şirul de numere $n_0 = 341$, $n_k = 2^{n_{k-1}} - 1$ pentru $k \geq 1$. Şirul fiind strict crescător, toate numerele găsite sunt diferite între ele.
Dacă n este pseudoprim impar, atunci n este compus şi verifică (10.17). Considerăm d un divizor netrivial al lui n. Din lema anterioară rezultă că $2^d - 1$ este divizor al lui m şi se observă că el este diferit de 1 şi m. Deci, m este compus.
Din $2^n \equiv 2 \ (mod\ n)$ obţinem $2^n - 2 = kn$ pentru un k natural. Atunci, $2^{m-1} = 2^{2^n - 2} = 2^{kn}$. Aplicăm din nou lema şi obţinem $2^n - 1 \mid 2^{kn} - 1$ adică $m \mid 2^{m-1} - 1$. Astfel, $2^{m-1} \equiv 1 \ (mod\ m)$. □

Presupunem că relaţia $2^{n-1} \equiv 1 \ (mod\ n)$ este verificată pentru numărul impar n. Atunci, n poate fi număr prim sau pseudoprim cu baza 2. Pentru a stabili cu exactitate natura sa, trebuie testat n în raport cu alte baze. Dacă găsim un b, prim cu n, pentru care $b^{n-1} \neq 1 \ (mod\ n)$, atunci n este compus.

De exemplu, pentru 341 care este pseudoprim cu baza 2, testăm dacă relaţia (10.17) este verificată pentru $b = 7$. Observăm că:

$$7^3 = 343 \equiv 2 \ (mod\ 341) \tag{10.18}$$

$$2^{10} = 1024 \equiv 1 \ (mod\ 341) \tag{10.19}$$

Din aceste relaţii,

$$7^{340} = \left(7^3\right)^{113} 7 \equiv 2^{113} \cdot 7 = \left(2^{10}\right)^{11} \cdot 2^3 \cdot 7 \equiv 8 \cdot 7 \equiv 56 \neq 1 \ (mod\ 341).$$

Deci, 341 este compus.

Dar, există numere compuse n care verifică relaţia (10.17), pentru orice baze b prime cu n. Spre exemplu, dacă alegem $n = 561 = 3 \cdot 11 \cdot 17$

şi o bază b unde $(b,n)=1$, obţinem că $(b,3)=1$, $(b,11)=1$, $(b,17)=1$. Aplicând teorema 3.4.3, obţinem:

$$b^{560}=\left(b^2\right)^{280}\equiv 1\ (mod\ 3) \tag{10.20}$$

$$b^{560}=\left(b^{10}\right)^{56}\equiv 1\ (mod\ 11) \tag{10.21}$$

$$b^{560}=\left(b^{16}\right)^{35}\equiv 1\ (mod\ 17) \tag{10.22}$$

de unde $b^{560}\equiv 1\ (mod\ 561)$.

Definiţie 10.5.2 *Un număr natural compus n care verifică relaţia (10.17) pentru orice b număr relativ prim cu n, se numeşte număr Carmichael.*

În tabelul B.2, din cadrul Anexei B, alături de numerele pseudoprime cu baza 2 mai mici decât 41041, sunt menţionate şi numerele Carmichael existente până la această limită.

Propoziţie 10.5.1 *Fie n un număr natural impar.*

1) *Dacă n se divide cu pătratul unui număr natural >1, atunci n nu este un număr Carmichael.*

2) *Dacă n este liber de pătrate, atunci n este număr Carmichael dacă şi numai dacă $p-1\mid n-1$ pentru fiecare divizor prim p al lui n.*

Demonstraţie. 1) Presupunem că $p^2\mid n$, unde p este un număr prim. Fie r o rădăcină primitiv modulo p^2. Atunci, $ord_{p^2}r=p(p-1)$. Notăm cu n_1 produsul tuturor numerelor prime diferite de p care divid n. Aplicând teorema chinezească a resturilor, sistemul

$$\begin{cases} x\equiv r\ (mod\ p^2)\\ x\equiv 1\ (mod\ n_1)\end{cases}$$

are soluţie unică pe b. Atunci, b este rădăcină primitivă modulo p^2 şi este prim cu n deoarece nu este divizibil cu p sau cu alt factor prim care divide n_1.

Vom arăta că n nu este pseudoprim cu baza b, deci nu va fi număr Carmichael.
Pentru aceasta, presupunem contrariul, adică $b^{n-1}\equiv 1\ (mod\ n)$. Atunci, din $p^2\mid n$, rezultă $b^{n-1}\equiv 1\ (mod\ p^2)$. Dar, $ord_{p^2}b=p(p-1)$ implică

$p(p-1) \mid n-1$ de unde obţinem $p \mid n-1$. Din $p \mid n$ rezultă $p = 1$ ce contrazice faptul că p este prim.
2) În acest caz, $n = p_1 p_2 \dots p_k$ unde p_i sunt numere prime distincte. Presupunem mai întâi că $p_i - 1 \mid n-1$ pentru fiecare $1 \leq i \leq k$. Atunci, pentru fiecare i există t_i astfel încât $n-1 = t_i(p_i-1)$. Fie b un întreg prim cu n. Aplicăm teorema 3.4.3 şi obţinem $b^{n-1} = \left(b^{p_i-1}\right)^{t_i} \equiv 1 \ (mod\ p_i)$. Din corolarul 3.1.2, rezultă $b^{n-1} \equiv 1 \ (mod\ n)$.
Reciproc, presupunem că n este număr Carmichael dar există un p_j pentru care $p_j - 1 \nmid n-1$. Atunci, fie r o rădăcină primitivă modulo p_j. Ca în demonstraţia primului punct, găsim un întreg b, prim cu n, care verifică

$$\begin{cases} b \equiv r \ (mod\ p_j) \\ b \equiv 1 \ \left(mod\ \dfrac{n}{p_j}\right) \end{cases}$$

Atunci, ca şi înainte, $(b, n) = 1$ şi $b^{n-1} \equiv r^{n-1} \ (mod\, p_j)$. Dar, $p_j - 1 \nmid n-1$ de unde, $r^{n-1} \neq 1 \ (mod\ p_j)$. Astfel, $b^{n-1} \neq 1 \ (mod\ p_j)$ ceea ce arată că $b^{n-1} \neq 1 \ (mod\ n)$, fals. □

Propoziţie 10.5.2 *Un număr Carmichael trebuie să fie produsul a cel puţin trei factori primi distincţi.*

Demonstraţie. Propoziţia anterioară a stabilit că orice număr Carmichael este liber de pătrate. Arătăm că un astfel de număr nu poate fi un produs de două numere prime distincte. Pentru aceasta, fie $n = pq$ unde p, q sunt prime, distincte. Alegem $p < q$. Dacă n este un număr Carmichael, atunci, conform propoziţiei anterioare, $q - 1 \mid n - 1$. Deci, $n - 1 \equiv 0 \ (mod\ q-1)$. Pe de altă parte, din $n - 1 = p(q - 1 + 1) - 1$, obţinem $n - 1 \equiv p - 1 \ (mod\ q-1)$.
Dar, din $0 < p - 1 < q - 1$ rezultă $n - 1 \neq 0 \ (mod\ q-1)$. Această contradicţie încheie demonstraţia. □

Observaţie 10.5.2 *În anul 1992, deci suficient de recent, Alford, Granville şi Pomerance au demonstrat că există o infinitate de numere Carmichael (vezi [1]).*

Mica teoremă a lui Fermat afirmă că pentru un număr prim n şi a un întreg , $1 \leq a \leq n-1$, atunci $a^{n-1} \equiv 1 \ (mod\ n)$. După cum am văzut, reciproca teoremei lui Fermat nu este adevărată.

Ideea testului Fermat este următoarea:

Pentru numărul n, a cărui primalitate o cercetăm, alegem $b > 1$ şi calculăm $b^{n-1} \pmod n$. Dacă rezultatul nu este 1, atunci numărul este compus şi b se numeşte martor Fermat al faptului că n este compus. Dacă este egal cu 1, atunci n este prim sau pseudoprim cu baza b.

Acest test stă la baza testelor probabilistice de primalitate. El nu este cu adevărat un test probabilistic deoarece el nu poate distinge între numerele prime şi numerele Carmichael.

Algoritm 10.5.1 (Algoritm Fermat)
INPUT: un număr $n > 2$ impar, un parametru de securitate $t > 1$.
OUTPUT: un răspuns referitor la primalitatea lui n.

1. *Pentru i de la 1 la t :*
   - *1.1. Alege aleator un întreg b cu $2 \leq b \leq n-2$.*
   - *1.2. Calculează $r = b^{n-1} \bmod n$ folosind algoritmul 3.1.1.*
   - *1.3. Dacă $r \neq 1$, atunci returnează* număr compus *şi se opreşte*
2. *Returnează* număr prim.

10.6 Testul Solovay-Strassen

Fie p număr prim impar şi $b \in \boldsymbol{Z}$, cu $p \nmid b$.

Conform criteriului lui Euler, $b^{\frac{p-1}{2}} \equiv \left(\frac{b}{p}\right) \pmod p$.

Deci, dacă dorim să testăm dacă un număr natural n este prim, putem alege un b, prim cu n şi verificăm dacă $b^{\frac{n-1}{2}} \equiv \left(\frac{b}{n}\right) \pmod n$.

Dacă congruenţa nu se verifică, atunci n este compus.

De exemplu, pentru $n = 341$ şi $b = 2$, obţinem $2^{170} \equiv 1 \pmod{341}$.

Din $341 \equiv -3 \pmod 8$, rezultă $\left(\frac{2}{341}\right) = -1$.

Deci, $2^{170} \neq \left(\frac{2}{341}\right) \pmod{341}$, de unde, 341 este compus.

Definiţie 10.6.1 *Un număr natural compus n, care verifică congruenţa*

$$b^{\frac{n-1}{2}} \equiv \left(\frac{b}{n}\right) \pmod n, \tag{10.23}$$

pentru $b \in \mathbf{Z}$, $(b, n) = 1$, *se numeşte număr Euler pseudoprim cu baza* b.

De exemplu, $n = 1105$ este Euler pseudoprim cu baza $b = 2$ deoarece $2^{552} \equiv 1 \ (mod\ 1105)$ şi, din $1105 \equiv 1 \ (mod\ 8)$, rezultă $\left(\frac{2}{1105}\right) = 1$.

Teoremă 10.6.1 *Dacă* n *este Euler pseudoprim cu baza* b, *atunci* n *este pseudoprim cu baza* b.

Demonstraţie. Cum n este Euler pseudoprim cu baza b, congruenţa

$$b^{\frac{n-1}{2}} \equiv \left(\frac{b}{n}\right) \ (mod\ n)$$

este verificată. Astfel, $b^{n-1} \equiv \left(\frac{b}{n}\right)^2 \ (mod\ n)$. Dar, $\left(\frac{b}{n}\right) = \pm 1$, de unde $b^{n-1} \equiv 1 \ (mod\ n)$. □

Observaţie 10.6.1 *Trebuie să remarcăm faptul că nu orice număr pseudoprim este Euler pseudoprim. Astfel, din exemplul anterior,* 341, *despre care ştim că este pseudoprim cu baza* 2, *nu este Euler pseudoprim cu baza* 2.

Lemă 10.6.1 *Fie* n *număr impar care nu este pătrat perfect. Atunci există cel puţin un număr natural* b, $1 < b < n$, *relativ prim cu* n, *pentru care* $\left(\frac{b}{n}\right) = -1$.

Demonstraţie. Dacă n este număr prim, propoziţia 7.1.1 ne asigură de existenţa unui astfel de b.
Considerăm acum că n este compus. Ţinând cont de condiţia impusă lui n, aceea că n nu este pătrat perfect, putem scrie $n = r \cdot s$, unde $(r, s) = 1$ şi $r = p^a$, cu p prim impar, a număr impar. Fie t un nonrest pătratic modulo p (existenţa lui este asigurată de propoziţia 7.1.1). Folosind teorema chinezească a resturilor, există $1 < b < n$, prim cu n care verifică

$$\begin{cases} b \equiv t \ (mod\ r) \\ b \equiv 1 \ (mod\ s) \end{cases}$$

Atunci, $\left(\frac{b}{r}\right) = \left(\frac{b}{p^a}\right) = \left(\frac{b}{p}\right)^a = (-1)^a = -1$ şi $\left(\frac{b}{s}\right) = 1$. De aici, $\left(\frac{b}{n}\right) = \left(\frac{b}{r}\right) \cdot \left(\frac{b}{s}\right) = -1$. □

Lemă 10.6.2 *Fie n număr compus impar. Atunci, există cel puţin un $1 < b < n$, prim cu n, pentru care $b^{\frac{n-1}{2}} \neq \left(\frac{b}{n}\right) \ (mod\ n)$.*

Demonstraţie. Vom presupune că nu există un astfel de b, adică, pentru toate numerele b mai mici decât n şi prime cu n, avem $b^{\frac{n-1}{2}} \equiv \left(\frac{b}{n}\right) \ (mod\ n)$. Atunci, pentru fiecare astfel de b, obţinem:

$$b^{n-1} \equiv \left(\frac{b}{n}\right)^2 = (\pm 1)^2 = 1 \ (mod\ n).$$

De aici, rezultă că n este număr Carmichael. Astfel, $n = p_1 p_2 \dots p_k$, unde p_i sunt numere prime distincte.

Vom arăta că $b^{\frac{n-1}{2}} \equiv 1 \ (mod\ n)$, pentru orice $1 < b < n$, prim cu n. Pentru aceasta, reducem la absurd şi presupunem că există un $1 < b < n$, prim cu n, pentru care $b^{\frac{n-1}{2}} \neq 1 \ (mod\ n)$. Aplicăm teorema chinezească a resturilor pentru a obţine un număr $1 < a < n$, prim cu n, care verifică sistemul:

$$\begin{cases} a \equiv b \ (mod\ p_1) \\ a \equiv 1 \ (mod\ p_2 \dots p_k) \end{cases}$$

Rezultă $a^{\frac{n-1}{2}} \equiv b^{\frac{n-1}{2}} \equiv -1 \ (mod\ p_1)$ şi $a^{\frac{n-1}{2}} \equiv 1 \ (mod\ p_2 \dots p_k)$. Deci, $a^{\frac{n-1}{2}} \neq \pm 1 \ (mod\ n)$, rezultat ce contrazice presupunerea făcută la începutul demonstraţiei.

Astfel, $b^{\frac{n-1}{2}} \equiv 1 \ (mod\ n)$, pentru orice $1 < b < n$, prim cu n. De aici, ţinând cont de ipoteza de lucru, obţinem $b^{\frac{n-1}{2}} \equiv \left(\frac{b}{n}\right) = 1 \ (mod\ n)$, pentru orice $1 < b < n$, prim cu n.
Acest rezultat contrazice afirmaţia făcută în lema 10.6.1, deci presupunerea făcută la începutul demonstraţiei este falsă. □

Teoremă 10.6.2 (Solovay) *Fie n număr compus impar. Numărul numerelor mai mici decât n, prime cu n, în raport cu care n este Euler pseudoprim este mai mic decât $\frac{\phi(n)}{2}$.*

Demonstraţie. Din lema 10.6.2, există un $1 < b < n$, prim cu n, pentru care $b^{\frac{n-1}{2}} \neq \left(\frac{b}{n}\right) \ (mod\ n)$. Fie $a_1, a_2, \ldots, a_m$ toate numerele mai mici dacât n, prime cu n pentru care

$$a_j^{\frac{n-1}{2}} \equiv \left(\frac{a_j}{n}\right) \ (mod\ n) \tag{10.24}$$

pentru $1 \leq j \leq m$. Fie $r_1, r_2, \ldots, r_m$ resturile modulo n ale numerelor $ba_1, ba_2, \ldots, ba_m$. Se verifică uşor că r_j sunt distincţi şi primi cu n, pentru $1 \leq j \leq m$.

Dacă pentru un j ar avea loc congruenţa $r_j^{\frac{n-1}{2}} \equiv \left(\frac{r_j}{n}\right) \ (mod\ n)$, atunci $(ba_j)^{\frac{n-1}{2}} \equiv \left(\frac{ba_j}{n}\right) \ (mod\ n)$. Astfel, $b^{\frac{n-1}{2}} \cdot a_j^{\frac{n-1}{2}} \equiv \left(\frac{b}{n}\right) \cdot \left(\frac{a_j}{n}\right) \ (mod\ n)$. Din relaţia (10.24), obţinem $b^{\frac{n-1}{2}} \equiv \left(\frac{b}{n}\right) \ (mod\ n)$, ceea ce contrazice alegerea lui b.

Deci, pentru orice $1 \leq j \leq m$, $r_j^{\frac{n-1}{2}} \neq \left(\frac{r_j}{n}\right) \ (mod\ n)$.

Cum pentru fiecare j, numerele a_j verifică congruenţele (10.24), în timp ce r_j nu le verifică, cele două mulţimi formate cu aceste elemente sunt disjuncte. Am obţinut astfel $2m$ numere mai mici decât n şi prime cu n. Deci, $2m \leq \phi(n)$, de unde $m \leq \frac{\phi(n)}{2}$. □

Observaţie 10.6.2 *Dacă n este număr compus şi se alege aleator un număr $1 < b < n$, prim cu n, probabilitatea ca n să fie Euler pseudoprim cu baza b este mai mică decât $\frac{1}{2}$.*

Testul probabilistic de primalitate Solovay[4]-Strassen[5] a fost primul test popularizat la apariţia criptografiei cu cheie publică, în particular, a criptosistemului RSA. El nu mai este folosit, deoarece testul Miller-Rabin este o alternativă mai eficientă şi cel puţin la fel de corectă.

[4]Robert Solovay, profesor la Berkeley, are multe contribuţii remarcabile în matematică, găsind soluţii decisive pentru probleme dificile de interes general, cum ar fi testarea primalităţii.

[5]Volker Strassen, matematician german, care, pentru munca sa în studiul testării primalităţii, a primit în anul 2003 premiul Paris Kanellakis al ACM, Association for Computing Machinery.

Criteriul lui Euler, teorema 7.1.1, precizează că, pentru un număr prim n, avem $a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \ (mod\ n)$, pentru orice întreg a relativ prim cu n.

Testul de faţă se bazează pe acest criteriu. Astfel, dacă pentru un a obţinem $(a,n) \neq 1$ sau $a^{\frac{n-1}{2}} \neq \left(\frac{a}{n}\right) \ (mod\ n)$, numărul este compus iar a se numeşte *martor Euler* (pentru faptul că numărul este compus) *pentru n.* În caz contrar, n este prim sau Euler pseudoprim cu baza a.

Teoremă 10.6.3 *Fie n un număr compus impar. Probabilitatea ca testul Solovay-Strassen, aplicat pentru t baze diferite, să declare numărul n ca fiind prim este mai mică decât* $\left(\frac{1}{2}\right)^t$.

Algoritm 10.6.1 (Test Solovay-Strassen)
INPUT: un număr $n > 2$ impar, un parametru de securitate $t > 1$.
OUTPUT: un răspuns referitor la primalitatea lui n.

1. *Pentru i de la 1 la t :*
   - *1.1. Alege aleator un întreg a cu $2 \leq a \leq n-2$.*
   - *1.2. Calculează $r = a^{\frac{n-1}{2}} mod\ n$ folosind algoritmul 3.1.1.*
   - *1.3. Dacă $r \neq 1$, şi $r \neq n-1$, atunci returnează* număr compus *şi se opreşte.*
   - *1.4. Calculează simbolul Jacobi $s = \left(\frac{a}{n}\right)$ folosind algoritmul 7.3.1*
   - *1.5. Dacă $r \neq s\ mod\ n$, returnează* număr compus *şi se opreşte.*
2. *Returnează* număr prim.

Observăm că, dacă $d = (a,n) > 1$, atunci, $d \mid a^{\frac{n-1}{2}} \ (mod\ n)$. Astfel, testând la pasul 1.3. dacă $r \neq 1$, eliminăm necesitatea de a verifica dacă $(a,n) \neq 1$.

10.7 Testul Miller-Rabin

Să presupunem că n verifică congruenţa (10.17) pentru b prim cu n. Putem lua în considerare restul lui $b^{\frac{n-1}{2}}$ modulo n. Astfel, dacă $x = b^{\frac{n-1}{2}}$, atunci congruenţa devine $x^2 \equiv 1 \ (mod\ n)$. În cazul în care n este prim, $x \equiv \pm 1 \ (mod\ n)$.

Deci, dacă congruenţa (10.17) este verificată, putem vedea dacă $b^{\frac{n-1}{2}} \equiv \pm 1 \ (mod\ n)$. În situaţia în care această relaţie nu se verifică, atunci n este compus.

Spre exemplu, dacă alegem cel mai mic număr Carmichael $n = 561$, pentru $b = 5$ obţinem $5^{\frac{561-1}{2}} = 5^{280} \equiv 67 \ (mod\ 561)$, deci 561 este compus.

Definiţie 10.7.1 *Fie $n > 2$ număr natural impar cu $n - 1 = 2^s t$ unde s, t sunt numere naturale cu t impar. Spunem că n trece testul Miller pentru baza b, un număr natural, prim cu n, dacă este verificată una dintre următoarele condiţii:*

$$b^t \equiv 1 \ (mod\ n) \tag{10.25}$$

$$\exists\ 0 \leq j \leq s-1,\ b^{2^j t} \equiv -1 \ (mod\ n). \tag{10.26}$$

Teoremă 10.7.1 *Fie n un număr prim şi b un număr natural, prim cu n. Atunci, n trece testul Miller pentru baza b.*

Demonstraţie. Fie $n - 1 = 2^s t$ cu t impar. Pentru fiecare $0 \leq k \leq s$ considerăm

$$x_k = b^{\frac{n-1}{2^k}} = b^{2^{s-k} t}.$$

Din teorema 3.4.3, cum n este prim, $x_0 = b^{n-1} \equiv 1 \ (mod\ n)$. Atunci, $x_1^2 = \left(b^{\frac{n-1}{2}}\right)^2 = x_0 \equiv 1 \ (mod\ n)$, de unde $x_1 \equiv \pm 1 \ (mod\ n)$.
Dacă $x_1 \equiv 1 \ (mod\ n)$, atunci $x_2^2 = x_1 \equiv 1 \ (mod\ n)$, de unde $x_2 \equiv \pm 1 \ (mod\ n)$. Pe caz general, dacă am găsit

$$x_0 \equiv x_1 \equiv x_2 \equiv \ldots \equiv x_k \equiv 1 \ (mod\ n),\ k < s,$$

atunci $x_{k+1}^2 \equiv 1 \ (mod\ n)$ şi obţinem $x_{k+1} \equiv \pm 1 \ (mod\ n)$.
Continuând procedeul, obţinem $x_k \equiv 1 \ (mod\ n)$ pentru orice k sau există un j pentru care $x_j \equiv -1 \ (mod\ n)$. Deci, n trece testul Miller pentru baza b. □

Propoziţie 10.7.1 *Dacă n trece testul Miller pentru baza b, el este pseudoprim cu baza b.*

Demonstraţie. Presupunem aceleaşi notaţii. Dacă n verifică condiţia (10.25), atunci $b^{n-1} = (b^t)^{2^s} \equiv 1 \ (mod\ n)$. În cazul în care este verificată condiţia (10.26), $b^{n-1} = \left(b^{2^j t}\right)^{2^{s-j}} \equiv (-1)^{2^{s-j}} \equiv 1 \ (mod\ n)$. □

Definiţie 10.7.2 *Spunem că un număr compus n este tare pseudoprim cu baza b unde $(b, n) = 1$ dacă el trece testul Miller pentru baza b.*

Spre exemplu, dacă considerăm $n = 2047 = 23 \cdot 89$, $n - 1 = 2 \cdot 1023$. Observăm că

$$2^{\frac{2046}{2}} = 2^{1023} = (2^{11})^{93} \equiv 1 \ (mod\ 2047).$$

Deci, 2047 este tare pseudoprim cu baza 2.

Teoremă 10.7.2 *Există o infinitate de numere tari pseudoprime cu baza 2.*

Demonstraţie. Arătăm că dacă n este pseudoprim impar cu baza 2, atunci $m = 2^n - 1$ este tare pseudoprim cu baza 2.
Fie n număr compus impar şi $2^{n-1} \equiv 1 \ (mod\ n)$. Atunci, $2^{n-1} - 1 = kn$, cu k impar.

$$m - 1 = 2^n - 2 = 2(2^{n-1} - 1) = 2kn.$$

Deci, în acest caz, $s = 1$, $t = kn$ impar.

$$2^{\frac{m-1}{2}} = 2^{nk} = (2^n)^k = (m+1)^k \equiv 1 \ (mod\ m).$$

Astfel, m trece testul Miller pentru baza 2. Din teorema 10.5.1, există o infinitate de numere pseudoprime cu baza 2, şi astfel obţinem o infinitate de numere tari pseudoprime cu baza 2. □

Teoremă 10.7.3 *Dacă n este tare pseudoprim cu baza b, atunci el este Euler pseudoprim cu baza b.*

Demonstraţie. Fie $n - 1 = 2^s \cdot t$, cu t impar şi s natural nenul.
Fie $n = \prod_{i=1}^{m} p_i^{\alpha_i}$, descompunerea sa canonică în factori primi.

Presupunem întâi cazul când $b^t \equiv 1 \ (mod\ n)$.
Fie p un divizor prim al lui n. Atunci, $b^t \equiv 1 \ (mod\ p)$, de unde $ord_p b \mid t$.
Cum t este impar, rezultă $ord_p b$ număr impar.
Dar, $ord_p b \mid \phi(p) = p-1$, de unde $ord_p b \mid \frac{p-1}{2}$.
Astfel, $b^{\frac{p-1}{2}} \equiv 1 \ (mod\ p)$ şi, aplicând criteriul lui Euler, $\left(\frac{b}{p}\right) = 1$, pentru orice divizor prim p al lui n. Atunci, $\left(\frac{b}{n}\right) = \prod_{i=1}^{m} \left(\frac{b}{p_i}\right)^{\alpha_i} = 1$.
Din $b^t \equiv 1 \ (mod\ n)$ rezultă $b^{\frac{n-1}{2}} = \left(b^t\right)^{2^{s-1}} \equiv 1 \ (mod\ n)$.

Pentru cazul în care există $0 \leq j \leq s-1$ astfel ca $b^{2^j t} \equiv -1 \ (mod\ n)$, obţinem că $b^{2^j t} \equiv -1 \ (mod\ p)$, pentru orice divizor prim p al lui n. Ridicând la pătrat, rezultă $b^{2^{j+1} t} \equiv 1 \ (mod\ p)$, de unde $ord_p b \mid 2^{j+1} t$.
Din $ord_p b \nmid 2^j t$, avem $ord_p b = 2^{j+1} c$, cu c număr impar.
$2^{j+1} \mid ord_p b$ şi $ord_p b \mid p-1$, implică $2^{j+1} \mid p-1$. Deci, există $d \in \boldsymbol{Z}$, astfel încât $p = 2^{j+1} d + 1$.
Din $b^{\frac{ord_p b}{2}} \equiv -1 \ (mod\ p)$, rezultă

$$\left(\frac{b}{p}\right) \equiv b^{\frac{p-1}{2}} = \left(b^{\frac{ord_p b}{2}}\right)^{\frac{p-1}{ord_p b}} \equiv (-1)^{\frac{p-1}{2^{j+1} c}} \ (mod\ p).$$

Cum c este impar, $(-1)^c \equiv -1 \ (mod\ p)$, de unde
$\left(\frac{b}{p}\right) \equiv (-1)^{\frac{p-1}{2^{j+1}}} \equiv (-1)^d \ (mod\ p)$.

Am arătat că, pentru fiecare $1 \leq i \leq m$, există $d_i \in \boldsymbol{Z}$, astfel ca divizorii p_i să fie de forma $p_i = 2^{j+1} d_i + 1$. Atunci,

$$\begin{aligned} n &= \prod_{i=1}^{m} p_i^{\alpha_i} = \prod_{i=1}^{m} \left(2^{j+1} d_i + 1\right)^{\alpha_i} \equiv \prod_{i=1}^{m} \left(1 + 2^{j+1} \alpha_i \cdot d_i\right) \\ &\equiv 1 + 2^{j+1} \sum_{i=1}^{m} d_i \alpha_i \ (mod\ 2^{j+2}). \end{aligned}$$

Deci, $2^{s-1} t = \frac{n-1}{2} \equiv 2^j \sum_{i=1}^{m} d_i \alpha_i \ (mod\ 2^{j+1})$.

Astfel, obţinem $t \cdot 2^{s-j-1} \equiv \sum_{i=1}^{m} d_i\alpha_i \ (mod\ 2)$. De aici,

$$b^{\frac{n-1}{2}} = \left(b^{2^j t}\right)^{2^{s-j-1}} \equiv (-1)^{2^{s-j-1}} = (-1)^{\sum_{i=1}^{m} d_i\alpha_i} \ (mod\ n).$$

Pe de altă parte,

$$\left(\frac{b}{n}\right) = \prod_{i=1}^{m}\left(\frac{b}{p_i}\right)^{\alpha_i} = \prod_{i=1}^{m}\left((-1)^{d_i}\right)^{\alpha_i} = \prod_{i=1}^{m}(-1)^{\alpha_i d_i} = (-1)^{\sum_{i=1}^{m}\alpha_i d_i}.$$

Deci, şi în acest caz, n este Euler pseudoprim cu baza b. □

Observaţie 10.7.1 *Nu orice număr Euler pseudoprim cu baza b este tare pseudoprim cu baza b. De exemplu, am văzut că 1105 este Euler pseudoprim cu baza* 2.
$1104 = 2^4 \cdot 69$. *Calculând, obţinem:*

$$2^{69} \equiv 138 \neq \pm 1 \ (mod\ 1105), \qquad 2^{276} \equiv 781 \ (mod\ 1105),$$
$$2^{138} \equiv 259 \ (mod\ 1105), \qquad 2^{552} \equiv 1 \neq -1 \ (mod\ 1105).$$

De aici, 1105 nu este tare pseudoprim cu baza 2.

Cu toate acestea, în anumite cazuri particulare, cele două tipuri de numere coincid.

Propoziţie 10.7.2 *Dacă $n \equiv 3 \ (mod\ 4)$ şi n este Euler pseudoprim cu baza b, atunci el este tare pseudoprim cu baza b.*

Demonstraţie. Din $n \equiv 3 \ (mod\ 4)$, putem scrie $n - 1 = 2 \cdot t$, unde t este impar. n este Euler pseudoprim, deci $b^t = b^{\frac{n-1}{2}} \equiv \left(\frac{b}{n}\right) \ (mod\ n)$. Cum $\left(\frac{b}{n}\right) = \pm 1$, rezultă $b^t \equiv \pm 1 \ (mod\ n)$, adică n este tare pseudoprim cu baza b. □

Propoziţie 10.7.3 *Dacă n este Euler pseudoprim cu baza b şi $\left(\frac{b}{n}\right) = -1$, atunci n este tare pseudoprim cu baza b.*

Demonstraţie. Fie $n-1 = 2^s t$, unde t este impar şi s natural. Din ipoteză, obţinem $b^{2^{s-1}t} = b^{\frac{n-1}{2}} \equiv \left(\frac{b}{n}\right) \equiv -1 \ (mod\ n)$. Deci, n este tare pseudoprim cu baza b. □

Notăm cu Ψ_k cel mai mic număr tare pseudoprim cu primele k numere prime alese ca baze.

În anul 1993, Jaeschke a calculat Ψ_k, pentru $5 \leq k \leq 8$ şi a dat margini superioare pentru $9 \leq k \leq 11$. Astfel,

$\Psi_1 = 2047$
$\Psi_2 = 1373653$
$\Psi_3 = 25326001$
$\Psi_4 = 3215031751$
$\Psi_5 = 2152302898747$
$\Psi_6 = 3474749660383$
$\Psi_7 = 341550071728321$
$\Psi_8 = 341550071728321$
$\Psi_9 \leq 41234316135705689041$
$\Psi_{10} \leq 155336056607314320554100 2401$
$\Psi_{11} \leq 56897193526942024370326972321$

De asemenea, el a arătat că există 101 numere tari pseudoprime cu bazele 2,3 şi 5 mai mici decât 10^{12}. Dacă adăugăm şi baza 7 sunt 9 iar în cazul în care şi 11 este ales drept bază, nu există nici unul.

Observăm că primul număr tare pseudoprim cu bazele $2, 3, 5, 7$ este 3215031751. Putem concluziona acum că, dacă aplicăm testul Miller pentru un număr $\leq 2,5 \cdot 10^{10}$, diferit de 3215031751, şi acesta trece testul pentru bazele $2, 3, 5, 7$, el este prim.

La fel, dacă aplicăm un test în şapte paşi, rezultatele anterioare permit verificarea primalităţii tuturor numerelor $\leq 3,4 \cdot 10^{14}$.

Testul Miller-Rabin se bazează pe noţiunea de număr tare pseudoprim, prezentată anterior.

Pentru a verifica dacă un număr impar n este prim sau nu, folosind acest test, scriem întâi $n-1 = 2^s t$ unde t este impar şi alegem la întâmplare o bază b, $1 < b < n$. Dacă n nu trece testul Miller pentru această bază, atunci el este compus. Altfel, n este prim sau tare pseudoprim cu baza b.

Teoremă 10.7.4 (Rabin) *Dacă n este nu număr impar compus, acesta trece testul Miller-Rabin pentru cel mult $\frac{n-1}{4}$ baze b cu $1 \leq b \leq n-1$.*

Pentru a demonstra teorema, avem nevoie de următorul rezultat care este un caz particular al teoremei 6.3.1:

Lemă 10.7.1 *Fie p un număr prim impar şi k, t numere naturale. Congruenţa $x^t \equiv 1 (mod\ p^k)$ are exact $(t, p^{k-1}(p-1))$ soluţii necongruente modulo p^k.*

Demonstraţia teoremei. Fie $n = p_1^{k_1} p_2^{k_2} \dots p_m^{k_m}$ un număr compus care trece testul Miller pentru baza b. Fie $n-1 = 2^s \cdot t$, cu t impar. Atunci, $b^{n-1} \equiv 1\ (mod\ n)$, indiferent de condiţia din definiţia testului Miller care se verifică. Conform lemei anterioare, pentru $1 \leq i \leq m$, congruenţa $x^{n-1} \equiv 1\ (mod\ p_i^{k_i})$ are $(n-1, p_i^{k_i-1}(p_i-1)) = (n-1, p_i-1)$ soluţii necongruente.
Astfel, folosind teorema chinezească a resturilor, obţinem că există $\prod_{i=1}^{m} (n-1, p_i-1)$ soluţii necongruente ale congruenţei $x^{n-1} \equiv 1\ (mod\ n)$.

Considerăm două cazuri:

1. Mai întâi, presupunem că există j, cu $1 \leq j \leq m$, pentru care $k_j \geq 2$.

Observăm că $\frac{p_j - 1}{p_j^{k_j}} = \frac{1}{p_j^{k_j-1}} - \frac{1}{p_j^{k_j}} \leq \frac{2}{9}$ pentru că, valorile cele mai mari ale expresiei se obţin când $p_j = 3$ şi $k_j = 2$. Atunci,

$$\prod_{i=1}^{m} (n-1, p_i-1) \leq \prod_{i=1}^{m} (p_i - 1) \leq \left(\prod_{i \neq j} p_i \right) \cdot \left(\frac{2}{9} \cdot p_j^{k_j} \right) \leq \frac{2}{9} \cdot n.$$

Deci, numărul de soluţii necongruente modulo n ale congruenţei $x^{n-1} \equiv 1\ (mod\ n)$ este $\leq \frac{2}{9} \cdot n$.

Observăm că pentru $n \geq 9$, $\frac{2}{9} \cdot n \leq \frac{1}{4} \cdot (n-1)$. Astfel, există cel mult $\frac{n-1}{4}$ baze $1 \leq b \leq n$, în raport cu care n este tare pseudoprim.

2. Presupunem acun $n = p_1 p_2 \dots p_m$.
Pentru fiecare i, fie $p_i - 1 = 2^{s_i} \cdot t_i$, cu toţi t_i impari. După o eventuală

renumerotare, vom avea $s_1 \leq s_2 \leq \ldots \leq s_m$.
Cu notaţiile făcute, pentru $1 \leq i \leq m$,

$$(n-1, p_i - 1) = 2^{\min(s,s_i)}(t, t_i).$$

Conform lemei, fiecare congruenţă $x^t \equiv 1 \ (mod\ p_i)$ are $T_i = (t, t_i)$ soluţii necongruente.

Considerăm acum congruenţele

$$x^{2^j \cdot t} \equiv -1 \ (mod\ p_i),\ 1 \leq i \leq m.$$

Folosind teorema 6.3.1, stabilim în ce condiţii aceste congruenţe au soluţii.
Dacă $0 \leq j \leq s_i - 1$, pentru fiecare i, congruenţa are $2^j \cdot T_i$ soluţii necongruente.
Dacă $j \geq s_i$, atunci $(2^j \cdot t, p_i - 1) = 2^{s_i} \cdot T_i$ şi $\frac{p_i - 1}{2^{s_i} \cdot T_i} = \frac{t_i}{T_i}$ este impar.
Rezultă $(-1)^{\frac{t_i}{T_i}} \equiv -1 \ (mod\ p_i)$ şi astfel, în acest caz, nu există soluţii.

Am obţinut următorul rezultat:
pentru congruenţa $x^t \equiv 1 \ (mod\ n)$ există $T = T_1 T_2 \ldots T_m$ soluţii necongruente şi
pentru $x^{2^j \cdot t} \equiv -1 \ (mod\ n)$, cu $0 \leq j \leq s_1 - 1$ există $2^{jm} \cdot T_1 T_2 \ldots T_m$ soluţii necongruente.

În total, vor exista

$$T\left(1 + \sum_{j=0}^{s_1 - 1} 2^{jm}\right) = T\left(1 + \frac{2^{ms_1} - 1}{2^m - 1}\right)$$

baze $b \leq n - 1$ în raport cu care n este tare pseudoprim.
În acest caz,

$$\phi(n) = (p_1 - 1)(p_2 - 1)\ldots(p_m - 1) = t_1 t_2 \ldots t_m \cdot 2^{s_1 + s_2 + \ldots + s_m}.$$

Arătăm că $T\left(1 + \frac{2^{ms_1} - 1}{2^m - 1}\right) \leq \frac{\phi(n)}{4}$.
Pentru aceasta, cum $T = T_1 T_2 \ldots T_m \leq t_1 t_2 \ldots t_m$, rămâne de demonstrat că

$$\left(1 + \frac{2^{ms_1} - 1}{2^m - 1}\right) \cdot \frac{1}{2^{s_1 + s_2 + \ldots + s_m}} \leq \frac{1}{4}. \tag{10.27}$$

Din $s_1 \leq s_2 \leq \ldots \leq s_m$, rezultă

$$\left(1+\frac{2^{ms_1}-1}{2^m-1}\right)\cdot\frac{1}{2^{s_1+s_2+\ldots+s_m}} \leq \left(1+\frac{2^{ms_1}-1}{2^m-1}\right)\cdot\frac{1}{2^{ms_1}} =$$
$$= \frac{1}{2^{ms_1}} + \frac{2^{ms_1}-1}{2^{ms_1}(2^m-1)} = \frac{1}{2^{ms_1}} + \frac{1}{2^m-1} - \frac{1}{2^{ms_1}(2^m-1)} =$$
$$= \frac{1}{2^m-1} + \frac{2^m-2}{2^{ms_1}(2^m-1)} \leq \frac{1}{2^m-1} + \frac{2^m-2}{2^m(2^m-1)} =$$
$$= \frac{1}{2^m-1} + \frac{2}{2^m} - \frac{1}{2^m-1} = \frac{1}{2^{m-1}}. \quad (10.28)$$

Dacă $m \geq 3$, din (10.28) rezultă (10.27).
Pentru $m = 2$, obţinem $n = p_1p_2$. Dacă $s_1 < s_2$,

$$\left(1+\frac{2^{2s_1}-1}{3}\right)\cdot\frac{1}{2^{s_1+s_2}} = \left(1+\frac{2^{2s_1}-1}{3}\right)\cdot\frac{1}{2^{2s_1}\cdot 2^{s_2-s_1}} =$$
$$= \left(\frac{1}{3}+\frac{1}{3\cdot 2^{2s_1-1}}\right)\cdot\frac{1}{2^{s_2-s_1}} \leq \frac{1}{2}\cdot\left(\frac{1}{3}+\frac{1}{6}\right) = \frac{1}{4}. \quad (10.29)$$

Astfel, (10.27) se verifică şi în acest caz.

Rămâne cazul în care $s_1 = s_2$.
Presupunem $p_1 > p_2$. Dacă $T_1 = t_1$, atunci $p_1 - 1 \mid n - 1$.
Din $n \equiv 1 \ (mod\ p_1 - 1)$ şi $n = p_1p_2 \equiv p_2 \ (mod\ p_1 - 1)$, rezultă
$p_2 \equiv 1 \ (mod\ p_1 - 1)$. Deci, $p_2 > p_1$, ceea ce contrazice alegerea noastră.
Astfel, $T_1 \neq t_1$. Pentru că $T_1 = (t, t_1)$, rezultă $t_1 = T_1 \cdot d$, unde $d > 1$.
Dar, t_1, T_1 fiind impari, rezultă $d \geq 3$. Astfel, $T_1 \leq \frac{t_1}{3}$.
Dacă presupunem $p_1 < p_2$ şi refacem raţionamentul anterior, obţinem $T_2 \neq t_2$, de fapt, $T_2 \leq \frac{t_2}{3}$.

Deci, indiferent de presupunerea făcută, $T_1T_2 \leq \frac{t_1t_2}{3}$. Cum $s_1 \geq 1$, rezultă $\left(1+\frac{2^{2s_1}-1}{3}\right)\cdot\frac{1}{2^{2s_1}} \leq \frac{1}{2}$.
Astfel, obţinem:
$T_1T_2\left(1+\frac{2^{2s_1}-1}{3}\right) \leq \frac{t_1t_2\cdot 2^{2s_1}}{6} = \frac{\phi(n)}{6} \leq \frac{n-1}{6} < \frac{n-1}{4}$. □

Teoremă 10.7.5 (Rabin (1980)) *Dacă n este nu număr impar compus, probabilitatea ca acesta să treacă testul Miller-Rabin pentru k baze b cu $1 \leq b \leq n-1$ este mai mică decât $\frac{1}{4^k}$.*

Astfel, dacă alegem 25 de iteraţii pentru testul Miller aplicat unui număr, probabilitatea ca acesta să nu fie compus este mai mică decât 2^{-50}.
Cu aceeaşi probabilitate, calculatorul poate da erori datorate hardware-ului, viruşilor, utilizatorul poate muri de inimă în timpul rulării programului. Acest lucru subliniază, încă o dată, avantajul folosirii testului.

În practică, nu avem de ales un număr mare de baze b pentru a fi aproape siguri că n este prim. De exemplu, cum am stabilit deja, singurul număr tare pseudoprim cu bazele 2,3,5,7, mai mic decât $2,5 \cdot 10^{10}$ este 3215031751. Astfel, dacă n trece testul pentru bazele menţionate şi este diferit de acesta, el este prim.

Dacă considerăm un număr impar de 1024 cifre binare şi s-ar folosi 44 de valori diferite ale bazei b, am declara, cu o probabilitate mai mică decât 2^{-80}, că numărul este prim. Această probabilitate arată că n poate fi folosit sigur în scopuri criptografice. Oricum, de obicei, se testează în general 6 valori diferite pentru bază pentru a garanta această probabilitate, spre deosebire de 90 de iteraţii necesare testului Solovay-Strassen pentru a asigura aceeaşi probalilitate.

Din păcate, nu este total sigur să ne sprijinim pe un test probabilistic, chiar dacă acesta este rapid şi probabilitatea ca el să eşueze este foarte mică.

O afirmaţie făcută de Émile Borel, cred că merită să fie menţionată în acest cadru:

Un fenomen a cărui probabilitate de a nu se întâmpla este de 10^{-50}, nu se va produce de loc sau, cel puţin, nu va fi observat.

(*Les Probabilitée et la vie)*

Dacă am presupune că există un număr destul de mic B (depinde de mărimea lui n) astfel încât, dacă n este compus, există o bază $b < B$ pentru care n nu trece testul Miller, am spune cu siguranţă că numărul n este compus. Astfel, pentru a verifica în mod sigur dacă numărul este prim, ar trebui să aplicăm testul pentru primele B baze. O astfel de

afirmaţie există, dar se bazează pe *Ipoteza generalizată Rieman* (GRH),[6] o *problemă de un milion de dolari* a Institutului de Matematică Clay. [7]

În forma sa iniţială, testul Miller era un test deterministic, bazat pe GRH, şi anume:

Teoremă 10.7.6 (Miller) *Dacă GRH este adevărată şi n este număr compus impar, atunci n nu trece testul Miller pentru o bază $b < 2\lg^2 n$.*

Modificarea făcută de Rabin a transformat testul într-un test probabilistic, dar care nu este condiţionat de nici o afirmaţie nedemonstrată.

Algoritm 10.7.1 (Miller-Rabin)
INPUT: un număr $n > 2$ impar, un parametru de securitate $r > 1$.
OUTPUT: un răspuns referitor la primalitatea lui n.

1. *Determină s şi t astfel încât $n - 1 = 2^s t$ cu t impar.*
2. *Pentru i de la 1 la r:*
   - *2.1. Alege aleator un întreg b cu $2 \leq b \leq n - 2$.*
   - *2.2. Calculează $y = b^t \bmod n$ folosind algoritmul 3.1.1.*
   - *2.3. Dacă $y \neq 1$ şi $y \neq n - 1$, atunci:*
     - *2.3.1. $j \leftarrow 1$.*
     - *2.3.2. Cât timp $j \leq s - 1$ şi $y \neq n - 1$ execută:*
       - *2.3.2.1. $y \leftarrow y^2 \bmod n$.*
       - *2.3.2.2. Dacă $y = 1$, atunci returnează* număr compus *şi se opreşte.*
       - *2.3.2.3. $j \leftarrow j + 1$*
     - *2.3.3. Dacă $y \neq n - 1$, returnează* număr compus *şi se opreşte.*
3. *Returnează* număr prim.

În a 5-a linie a pasului 2.3., dacă $y = 1$, atunci $b^{2^j r} \equiv 1 \ (mod\ n)$. Cum acesta este cazul când $b^{2^{j-1} r} \neq \pm 1 \ (mod\ n)$, n este compus. De fapt,

[6] Ipoteza Riemann este o conjectură care a fost enunţată prima dată în 1859 de Bernhard Riemann în lucrarea sa *On the Number of Primes Less Than a Given Magnitude* De fapt, sub o formă echivalentă, ea spune că numerele prime sunt distribuite cât de regulat posibil, ţinând cont de apariţia lor, ce pare aleatoare în şirul numerelor naturale.

[7] Pentru a sărbători matematicienii acestui mileniu, Institutul de Matematică Clay din Cambridge, Massachusetts, a nominalizat şapte probleme importante care nu au putut fi demonstrate până acum. Găsirea unei demonstraţii este răsplătită cu câte un milion de dolari, fiecare. În iunie 2004, Louis DeBranges de Bourcia a afirmat că a demonstrat GRH, fapt care încă nu este confirmat.

$\left(b^{2^{j-1}r}-1, n\right)$ este un divizor propriu al lui n. În ultima linie a pasului 2.3., dacă $y \neq n-1$, atunci b este un *martor al faptului că n este compus.*

Testul Solovay-Strassen foloseşte, spre deosebire de testul Miller-Rabin, şi calculul unui simbol Jacobi, fiind mai dificil de implementat şi necesitând mai multe calcule. Din acest motiv, ţinând cont şi de faptul că probabilitatea în acest caz este mai mică, putem renunţa la testul Solovay-Strassen în favoarea lui Miller-Rabin.

10.8 Primalitate folosind curbele eliptice

În anii 70 s-a încercat îmbunătăţirea testele $n+1$ şi $n-1$. Adleman, Pomerance şi Rumely au fost cei care au introdus testul de primalitate APR, în 1979. Acesta este considerat ca fiind începutul erei moderne a testelor de primalitate. Cohen şi Lenstra au îmbunătăţit acest test care lucrează cu numere de 100 cifre în câteva secunde.

Pornind de la ideea de bază a testului Fermat, aceea de a determina ordinul grupului $U(\mathbf{Z}_n)$ şi de a vedea dacă acesta este $n-1$, pasul următor făcut în vederea obţinerii de noi teste de primalitate a fost de a modifica grupul iniţial.

Astfel, în 1986, Goldwasser şi Kilian au propus un algoritm bazat pe curbele eliptice.

Teoria curbelor eliptice, studiată în teoria nunerelor cât şi în geometria algebrică, nu se va regăsi în conţinutul acestei cărţi. Pentru mai multe informaţii legate de această teorie, se poate studia [12]. În continuare, va fi prezentată doar ideea de bază a acestui algoritm.

O curbă eliptică este o mulţime de puncte (x, y) care verifică ecuaţia $E(a,b): \ y^2 = x^3 + ax + b$ unde $4a^3 + 27b^2 \neq 0$ şi un singur punct O, numit *punctul de la infinit.* Punctele raţionale de pe o astfel de curbă formează un grup în care adunarea este definită prin metoda *tangentei şi a coardei.* Astfel, dacă două puncte P_1, P_2 sunt raţionale (au coordonatele raţionale), dreapta determinată de acestea intersectează curba tot într-un punct raţional pe care îl vom nota $-(P_1 + P_2)$ (Semnul negativ este necesar pentru ca operaţia să fie asociativă). Dacă punctele nu sunt distincte, folosim tangenta în P_1 la curbă. Dacă unul dintre puncte este O, de exemplu $P_1 = O$, atunci $P_1 + P_2 = P_2$.

Conform unei teoreme datorate lui Mordell, acest grup este finit generat.

Pentru a aplica algoritmul, se reduce acest grup modulo un număr prim p şi obţinem un grup al cărui ordin va fi folosit aproape la fel ca în teorema Poklington. S-a înlocuit astfel un grup de ordin $n-1$ sau $n+1$ cu un altul al cărui ordin se află în intervalul $\left(p+1-2\sqrt{p},\ p+1+2\sqrt{p}\right)$ (teorema Hasse).

10.9 Algoritmul AKS

În anul 2002, Agrawal, Kayal şi Saxena au găsit un algoritm deterministic, relativ simplu, care nu se bazează pe nici o presupunere nedemonstrată.

Ideea pentru AKS rezultă dintr-o altă versiune simplă a micii teoreme a lui Fermat:

Teoremă 10.9.1 *Fie $p > 1$ şi a un întreg, relativ prim cu p. Atunci, p este prim dacă şi numai dacă $(x-a)^p \equiv (x^p - a)\ (mod\ p)$.*

Demonstraţie. Dacă p este prim, $p \mid C_p^k$, pentru $k \in \{1, \ldots, p-1\}$. Atunci, $(x-a)^p \equiv (x^p - a^p)\ (mod\ n)$ după care nu mai avem decât să aplicăm mica teoremă a lui Fermat pentru a obţine congruenţa finală.
Reciproc, dacă presupunem că p este compus, el are un divizor prim q. Fie k astfel încât q^k este cea mai mare putere a lui q care divide p. Atunci, $q^k \nmid C_p^q$. Dacă $(q^k, a^{p-q}) \neq 1$, rezultă $q \mid a$ şi astfel $(a,p) \neq 1$, fals. Deci, $(q^k, a^{p-q}) = 1$. În final, obţinem că x^q are în membrul stâng al congruenţei coeficientul nenul, ceea ce este fals. □

În această formă este dificil să folosim algoritmul, fiind prea mulţi coeficienţi pe care trebuie să-i verificăm. Următor pas făcut a fost acela de a găsi o condiţie mai simplă şi anume:

$$(x-a)^p \equiv (x^p - a)\ (mod\ x^k - 1, p)$$

unde $a \equiv b\ (mod\ n, m)$ înseamnă că $a - b$ este suma dintre un multiplu de n şi un multiplu de m.
Congruenţa trebuie să se verifice dacă p este prim.

O afirmaţie, fără demonstraţie până acum, precizează următoarele: dacă $k > 1$ nu divide p şi congruenţa este adevărată, atunci p este prim

sau $p^2 \equiv 1 \ (mod\ k)$. Odată rezolvată această problemă, se va putea da o versiune mai eficientă acestui test.

Algoritm 10.9.1 (AKS)
INPUT: un număr $n > 2$.
OUTPUT: un răspuns referitor la primalitatea lui n.

1. Dacă n *este de forma* a^b *cu* $b > 1$, *returnează* număr compus *şi se opreşte.*
2. $r \leftarrow 2$
3. Cât timp $r < n$, *execută:*
  3.1. Dacă $(n, r) \neq 1$, *returnează* număr compus *şi se opreşte.*
  3.2. Dacă $r \geq 2$ *este prim, execută:*
    Fie q *cel mai mare factor al lui* $r - 1$.
    Dacă $q > 4\sqrt{r}\lg n$ *şi* $n^{\frac{r-1}{q}} \neq 1 \ (mod\ r)$, *atunci salt la 4.*
  3.3. $r \leftarrow r + 1$
4. Pentru a *de la 1 la* $2\sqrt{r}\lg n$ *execută:*
  4.1. Dacă $(x - a)^n \neq (x^n - a) \ (mod\ x^r - 1, n)$, *atunci returnează* număr compus *şi se opreşte.*
5. Returnează număr prim.

Exerciţii propuse

1. Folosind testul Pepin, arătaţi că următoarele numere Fermat sunt prime: $F_1 = 5, F_3 = 257, F_4 = 65537$.

2. Cu ajutorul testului Pepin, arătaţi că 3 este rădăcină primitivă pentru orice număr prim Fermat.

3. Folosind testul Lucas-Lehmer, stabiliţi care dintre numerele Mersenne M_3, M_5, M_{11}, M_{13} sunt prime.

4. Explicaţi de ce nu trebuie verificat cu ajutorul testului Fermat dacă un număr Fermat sau un număr Mersenne este prim.

5. Arătaţi că 91 este pseudoprim cu baza 3 iar 45 este pseudoprim cu bazele 17 şi 19.

6. Fie n un număr impar compus şi $(b, n) = 1$. Dacă p este un divizor prim al lui n, fie $n' = \frac{n}{p}$. Arătaţi că n este pseudoprim cu baza b dacă şi numai dacă $b^{n'-1} \equiv 1 \ (mod\ p)$. Folosind acest rezultat, arătaţi că nu există un număr pseudoprim cu baza $2, 5$, sau 7 care să fie de forma $n = 3p$ cu p număr prim > 3.

7. Găsiţi toate bazele b pentru care 15, respectiv 21 este pseudoprim.

8. Determinaţi cel mai mic pseudoprim cu baza 5.

9. Fie $n = pq$ cu p, q numere prime impare.
Fie $d = (p - 1, q - 1)$. Arătaţi că n este pseudoprim cu baza b dacă şi numai dacă $b^d \equiv 1 \ (mod\ n)$.

10. Fie m număr natural astfel încât $6m + 1, 12m + 1, 18m + 1$ sunt toate numere prime. Arătaţi că $n = (6m + 1)(12m + 1)(18m + 1)$ este număr Carmichael.

11. Arătaţi că următoarele numere

$$1105 = 5 \cdot 13 \cdot 17,\ 1729 = 7 \cdot 13 \cdot 19,\ 2465 = 5 \cdot 17 \cdot 29$$

sunt numere Carmichael.

12. Arătaţi că 561 este cel mai mic număr Carmichael.

13. Fie n Euler pseudoprim cu bazele b_1 şi b_2. Arătaţi că n este Euler pseudoprim cu bazele $b_1 b_2$.

14. Fie $n \equiv 5 \ (mod\ 8)$ un număr Euler pseudoprim cu baza 2. Arătaţi că n este tare pseudoprim cu baza 2.

15. Arătaţi că:

i) 561 este tare pseudoprim cu baza 101.

ii) 65 este tare pseudoprim cu bazele 8 şi 18.

iii) 1387 este pseudoprim cu baza 2 dar nu este tare pseudoprim cu baza 2.

16. Arătaţi că dacă găsim b astfel încât n este pseudoprim dar nu tare pseudoprim cu baza b, atunci putem factoriza rapid n. Explicaţi cum se poate proteja criptosistemul RSA, prin alegerea lui n, de această situaţie.

CAPITOLUL 11

Problema factorizării

Problema factorizării este cea mai cunoscută ***problemă dificilă***. Am văzut că ea este ideea ce stă la baza criptosistemului RSA. Factorizarea presupune determinarea tuturor divizorilor primi ai unui număr întreg compus. Problema factorizării reprezintă un domeniu de cercetare foarte activ, atât pentru matematicieni, cât şi pentru informaticieni. Algoritmii de factorizare pot fi împărţiţi în două categorii:

1) algoritmi cu *scop special*, care sunt eficienţi în factorizarea numerelor cu divizori mici. Astfel de algoritmi sunt: *metoda Pollard rho*, *metoda Pollard p-1*, *metoda curbelor eliptice.*

2) algoritmi cu *scop general*, a căror eficienţă depinde de numărul care se factorizează. Ele sunt cele mai importante în domeniul sistemelor criptografice şi al securităţii acestora. Dintre ele putem menţiona *filtrul corpului numerelor* (NFS), cel mai des folosit algoritm de factorizare la acest moment, *filtrul pătratic polinomial multiplu* (MPQS).

Un *număr general* este un număr care nu are o formă particulară ce ar putea conduce uşor la determinarea divizorilor săi. Astfel de numere sunt folosite la crearea modulului în criptosistemul RSA. Dacă un număr are o formă uşoară de reprezentare, el se numeşte număr *cu formă specială*. De exemplu, numerele Fermat sunt astfel de numere.

Problema factorizării a devenit mai uşoară în ultimii 15 ani datorită faptului că numărul computerelor, puterea de procesare şi performanţele

acestora au crescut foarte mult şi au fost găsiţi algoritmi superiori de factorizare.

11.1 Factorizare prin căutare directă

Metoda de căutare a divizorilor prin încercări, prezentată în 10.2, este cea mai simplă metodă de determinare a divizorilor primi ai unui număr şi mai poate fi întâlnită sub denumirea de *trial division*.

La informaţiile furnizate anterior, în 10.2, mai facem doar o scurtă observaţie care poate simplifica testul:
Dacă cel mai mic factor prim p al lui n este $> \sqrt[3]{n}$, atunci $\frac{n}{p}$ este număr prim. Pentru a arăta că această afirmaţie este adevărată, să presupunem că $m = \frac{n}{p}$ este compus. Atunci, $m = a \cdot b$. Putem presupune că $a, b \geq p$. Astfel, ajungem la o contradicţie, şi anume $n = pm = pab \geq p^3 > n$. Deci, m este prim.

11.2 Metoda Fermat

De obicei, metoda este recomandată în cazul în care n are doi factori de mărime similară. Pentru un număr natural n, se caută întregi x, y astfel încât $n = x^2 - y^2$. Atunci $n = (x - y)(x + y)$ şi se obţine o primă descompunere a lui n, în care un factor este foarte mic. La baza acestui rezultat stă următoarea propoziţie, uşor de demonstrat:

Propoziţie 11.2.1 *Fie n un număr natural impar. Există o corespondenţă bijectivă între descompunerile lui n de forma $n = ab$ cu $a \geq b > 0$ şi reprezentările lui n de forma $n = x^2 - y^2$ unde x, y sunt numere naturale. Corespondenţa este dată de relaţiile:*

$$x = \frac{a+b}{2},\ y = \frac{a-b}{2},\ a = x + y,\ b = x - y.$$

Dacă $n = ab$, cu a şi b de valori apropiate, y va fi un număr mic iar x puţin mai mare decât $\sqrt{n}$. În acest caz, căutăm pătrate perfecte de forma $x^2 - n$, pornind cu $x_1 = [\sqrt{n}] + 1$. Testăm dacă $x_1^2 - n$ este pătrat perfect. Cum există doar 22 de combinaţii pentru ultimele două cifre ale unui număr pătrat perfect, multe cazuri pot fi eliminate.

Dacă $x_1^2 - n$ nu este pătrat perfect, alegem $x_2 = x_1 + 1$ şi refacem raţionamentul.
Procesul se opreşte pentru că descompunerea trivială $n = n \cdot 1$ conduce la $n = \left(\frac{n+1}{2}\right)^2 - \left(\frac{n-1}{2}\right)^2$.

Spre exemplu, să aplicăm metoda pentru $n = 4429$.

Din $66 < \sqrt{4429} < 67$, pornim cu $x_1 = 67$. Obţinem:

$x_1 = 67$, $67^2 - n = 60$ - nu este pătrat perfect,
$x_2 = 68$, $68^2 - n = 195$ - nu este pătrat perfect,
$x_3 = 69$, $69^2 - n = 332$ - nu este pătrat perfect,
$x_4 = 70$, $70^2 - n = 471$ - nu este pătrat perfect,
$x_5 = 71$, $71^2 - n = 612$ - nu este pătrat perfect,
$x_6 = 72$, $72^2 - n = 755$ - nu este pătrat perfect,
$x_7 = 73$, $73^2 - n = 900$ - este pătrat perfect.

Deci, $4429 = (73 - 30)(73 + 30) = 43 \cdot 103$. Apoi, reluăm procesul pentru factorii găsiţi. La noi, aceştia sunt primi.

Această factorizare poate fi ineficientă dacă cei doi factori a şi b nu au valori apropiate: este posibil să fie necesare $\frac{n+1}{2} - \sqrt{n}$ verificări pentru a testa dacă numerele generate sunt pătrate perfecte.

În această situaţie se poate folosi o *metodă Fermat generalizată* care acţionează mai bine în astfel de cazuri. Pentru aceasta, se alege k număr mic şi x va lua succesiv valorile $\left[\sqrt{kn}\right] + 1$, $\left[\sqrt{kn}\right] + 2, \ldots$. Ne vom opri când $x^2 - kn$ este pătrat perfect. Presupunem $x^2 - kn = y^2$. Atunci, din $(x + y)(x - y) = kn$, $(x + y, n)$ este un divizor propriu al lui n.

De exemplu, ca să factorizăm uşor $n = 68987$ folosind metoda Fermat generalizată, alegem $k = 3$.
Atunci $454 < \sqrt{3n} < 455$. Chiar la prima iteraţie obţinem:
$455^2 - 3 \cdot 68987 = 64$, adică $3n = 455^2 - 8^2$.
Calculând $(455 + 8,\ 68987) = 463$, rezultă $68987 = 463 \cdot 149$.

Algoritm 11.2.1 (Fermat generalizată)
INPUT: un număr n, impar compus şi k, factor de apropiere.
OUTPUT: doi factori a, b cu $n = ab$.

1. $N \leftarrow [\sqrt{kn}]$, $i \leftarrow 1$, $t \leftarrow 0$.

2. Cât timp $i \leq N$ *şi* $t = 0$, *efectuează:*
2.1. $y \leftarrow \sqrt{(N+i)^2 - kn}$.
2.2. Dacă $y = [y]$, *atunci* $x \leftarrow N + i$, $t \leftarrow 1$.
2.3. $i \leftarrow i + 1$.
3. Dacă $t = 1$, *atunci returnează* $a = (x + y, n)$, $b = n/a$ *şi se opreşte.*
4. Returnează mesaj de eşec.

11.3 Metoda Euler

Metoda Euler de factorizare se poate aplica pentru numere n impare care se pot scrie ca sumă de două pătrate în două feluri diferite. Astfel,

$$n = a^2 + b^2 = c^2 + d^2$$

unde a şi c sunt pare iar b şi d impare. Obţinem că $a^2 - c^2 = d^2 - b^2$, sau $(a - c)(a + c) = (d - b)(d + b)$.

Notăm $k = (a - c, d - b)$. Deci, k este par şi $a - c = kl$, $d - b = km$, cu $(l, m) = 1$. Înlocuind, obţinem $l(a + c) = m(b + d)$. De aici, $m \mid a + c$. Fie $a + c = mr$. Atunci, $b + d = lr$ unde $r = (a + c, b + d)$ este număr par. Ţinând cont de toate aceste rezultate, obţinem:

$$\left[\left(\frac{k}{2}\right)^2 + \left(\frac{r}{2}\right)^2\right]\left(l^2 + m^2\right) = \frac{1}{4}\left(k^2 + r^2\right)\left(l^2 + m^2\right) =$$
$$= \frac{1}{4}\left[(km)^2 + (kl)^2 + (mr)^2 + (lr)^2\right] =$$
$$= \frac{1}{4}\left[(d - b)^2 + (a - c)^2 + (a + c)^2 + (b + d)^2\right] =$$
$$= \frac{1}{4}\left(2a^2 + 2b^2 + 2c^2 + 2d^2\right) = \frac{1}{4}(2n + 2n) = n.$$

11.4 Metoda Pollard-rho

Presupunem că un număr mare n este compus; de exemplu, nu a trecut un test de primalitate prezentat în capitolul anterior. Cel mai simplu test, mult mai rapid decât metoda împărţirilor, este datorat lui J. M. Pollard. El poartă numele de *metoda rho*, sau *metoda Monte Carlo.* Acest test este un test cu scop special folosit pentru a găsi factori primi mici pentru un număr compus.

Algoritmul Pollard-rho prezintă două aspecte care trebuie subliniate.

Primul constă în ideea de a itera o formulă până se cade într-un ciclu. Fie S o mulţime finită şi $f : S \to S$ o funcţie oarecare. Fie $x_0 \in S$ punctul de plecare. Definim $x_{k+1} = f(x_k)$ pentru $k \geq 0$. Cum S este finită, există o pereche (p, q) pentru care $x_{p+q} = x_p$. Aplicând în mod repetat pe f în ambii membri, obţinem $x_{r+q} = x_r$, pentru toţi $r \geq p$. Cel mai mic p pentru care x_p se repetă se numeşte *pre-perioada* M. Cel mai mic q se numeşte *perioada* T. Ele depind de alegerea lui x_0, de f şi S. Punctele $x_0, \ldots, x_M$ se numesc *coada* şi punctele x_{M+r} cu $r \geq 0$ poartă numele de *ciclul* lui ρ. Numele algoritmului provine din forma pe care o are şirul de numere.

Considerăm că mulţimea S are n elemente (se poate alege, $S = \boldsymbol{Z}_n$). Funcţia f trebuie să fie aleasă astfel încât valorile ei să poată fi uşor calculate. Astfel, f este de obicei o funcţie polinomială; de exemplu $f(x) = x^2 + a$ unde $a \notin \{0, -2\}$.

Fie $n = \alpha\beta$ unde α, β sunt divizori relativi primi necunoscuţi ai lui n. Iterând $x_{k+1} \equiv x_k^2 + a \ (mod\ n)$ (sau orice altă formulă polinomială), pentru orice valoare iniţială x_0, se obţine un şir de numere care va intra într-un ciclu. Timpul până când x_i vor intra într-un ciclu, cât şi lungimea ciclului sunt proporţionale cu $\sqrt{n}$.

Din teorema chinezească a resturilor, fiecare $x \ (mod\ n)$ corespunde perechii $(x \ (mod\ \alpha), x \ (mod\ \beta))$.
Din $x_{k+1} \equiv x_k^2 + a \ (mod\ \alpha)$ şi $x_{k+1} \equiv x_k^2 + a \ (mod\ \beta)$, rezultă că şirul modulo α intră într-un ciclu de lungime mai mică.

Comparăm diferiţi x_i pentru a obţine doi care sunt resturi diferite modulo n, dar sunt congruenţi modulo un divizor al lui n. Fie x_i şi x_j două astfel de elemente. În acest caz, spunem că avem o *coliziune*. Atunci, $(x_i - x_j, n)$ este egal cu un divizor propriu al lui n.

De exemplu, pentru factorizarea lui $n = 91$ alegem $f(x) = x^2 + 1$ şi $x_0 = 1$. Atunci, $x_1 = 2$, $x_2 = 5$, $x_3 = 26$. Nu mai continuăm pentru că am găsit un divizor propriu $(26 - 5, 91) = 7$.

Al doilea aspect constă în detectarea faptului că şirul de numere devine periodic. Cantitatea mare de stocare a numerelor x_i necesară obţinerii unei coliziuni, a fost eliminată de Pollard care a folosit algoritmul lui Floyd de găsire a unui ciclu. În această metodă se porneşte cu $y_0 = x_0$ şi se calculează $y_{k+1} = f(f(y_k))$. Se obţine rapid, folosind

inducţia matematică, $y_k = x_{2k}$. Astfel, dacă k este multiplu de T, obţinem $y_k = x_k$. Verificând la fiecare pas dacă se obţine identitatea vom găsi un multiplu de T. Dacă M şi T sunt de mărime comparabilă, atunci vom găsi chiar un multiplu mic al lui T.

Algoritm 11.4.1 (Pollard-rho)
INPUT: un număr $n > 2$ compus, care nu este putere a unui număr prim.
OUTPUT: un divizor propriu al lui n.

1. *Pune $a \leftarrow 2$, $b \leftarrow 2$.*
2. *Pentru $i = 1, 2, \ldots$ execută:*
   - *2.1. Calculează $a \leftarrow a^2 + 1 \ mod \ n$, $b \leftarrow b^2 + 1 \ mod \ n$, $b \leftarrow b^2 + 1 \ mod \ n$.*
   - *2.2. Calculează $d = (a - b, n)$.*
   - *2.3. Dacă $1 < d < n$, atunci returnează d şi se opreşte.*
   - *2.4. Dacă $d = n$, atunci returnează mesaj de eşec (trebuie aleasă o altă funcţie polinomială).*

De exemplu, pentru $n = 455459$ şi $x_0 = 2$ obţinem:

$x_1 = 5,$	$y_1 = f(f(x_1)) \equiv 26 \ (mod \ 455459),$	$(y_1 - x_1, n) = 1;$
$x_2 = 26,$	$y_2 \equiv 2871 \ (mod \ 455459),$	$(y_2 - x_2, n) = 1;$
$x_3 = 677,$	$y_3 \equiv 179685 \ (mod \ 455459),$	$(y_3 - x_3, n) = 1;$
$x_4 = 2871,$	$y_4 \equiv 155260 \ (mod \ 455459),$	$(y_4 - x_4, n) = 1;$
$x_5 = 44380,$	$y_5 \equiv 416250 \ (mod \ 455459),$	$(y_5 - x_5, n) = 1;$
$x_6 = 179685,$	$y_6 \equiv 43670 \ (mod \ 455459),$	$(y_6 - x_6, n) = 1;$
$x_7 = 121634,$	$y_7 \equiv 164403 \ (mod \ 455459),$	$(y_7 - x_7, n) = 1;$
$x_8 = 155260,$	$y_8 \equiv 247944 \ (mod \ 455459),$	$(y_8 - x_8, n) = 1;$
$x_9 = 44567,$	$y_9 \equiv 68343 \ (mod \ 455459),$	$(y_9 - x_9, n) = 743.$

Deci, 743 este un divizor netrivial al lui 455459.
Obţinem $455459 = 743 \cdot 613$.

Pentru că în această situaţie, la fiecare pas este necesar să aplicăm de trei ori funcţia, putem pierde mult timp. De aceea, ultima parte a algoritmului a fost modificată de către Brent care a înlocuit algoritmul lui Floyd cu un altul.

Mai întâi să presupunem că M şi T au m cifre binare. Atunci, ar trebui să găsim o repetiţie pentru $k = 2^m - 1$. Deoarece $T \leq 2^m - 1$,

$k + T = 2^m + T - 1$ este mai mic decât $2^{m+1} - 2$. Astfel vom stoca $y_m = x_{2^m-1}$ şi îl vom compara cu x_k pentru $2^m \leq k \leq 2^{m+1} - 2$. La fiecare pas, se aplică f o singură dată. Pe de altă parte, M este aproape dublat, deci facem aproape un număr dublu de testări faţă de cazul iniţial Pollard. Este evident că alegerea între cele două versiuni se va face ţinând cont de care dintre următoarele două procese este mai mare consumatoare de timp: calcularea funcţiei sau compararea.

11.5 Metoda Pollard p-1

Această metodă este o metodă cu scop special, fiind folosită pentru factorizarea numerelor n care au un factor prim p cu proprietatea că $p - 1$ este produs de factori primi mai mici dacât un număr relativ mic B.

Ideea este următoarea:

Fie m cel mai mic multiplu comun al tuturor puterilor de numere prime $\leq B$ care sunt $\leq n$. Dacă $q^l \leq n$, atunci $l \ln q \leq \ln n$ şi, deci $l \leq \left[\frac{\ln n}{\ln q}\right]$.

Astfel, $m = \prod_{q \leq B} q^{\left[\frac{\ln n}{\ln q}\right]}$ unde produsul se face după toate numerele prime $q \leq B$.

Dacă p este un factor prim al lui n astfel încât $p-1$ are toţi factorii primi $\leq B$, atunci $p-1 \mid m$. Astfel, din mica teoremă a lui Fermat, pentru orice $(a, p) = 1$ avem $a^m \equiv 1 \ (mod\ p)$. De aici, dacă notăm $d = (a^m - 1, n)$, obţinem $p \mid d$. Este posibil ca $d = n$, caz în care algoritmul eşuează. Oricum, această situaţie este puţin probabil să apară dacă n are doi factori primi mari distincţi.

Algoritm 11.5.1 (Pollard p-1)
INPUT: un număr $n > 2$ compus, care nu este putere a unui număr prim.
OUTPUT: un divizor propriu al lui n.

1. *Alege o margine B.*
2. *Alege, aleator, un a, $2 \leq a \leq n - 1$ şi calculează $d = (a, n)$. Dacă $d \geq 2$, returnează d şi se opreşte.*
3. *Pentru fiecare număr prim $q \leq B$, execută:*
   - 3.1. *Calculează $l = [\ln n / \ln q]$.*
   - 3.2. *Calculează $a \leftarrow a^{q^l} \ mod\ n$.*

4. Calculează $d = (a - 1, n)$.
5. Dacă $d = 1$ *sau* $d = n$, *returnează mesaj de eşec; altfel, returnează* d.

De exemplu, pentru $n = 19048567$, $B = 19$, $a = 3$ obţinem:

$q = 2,\ l = 24,\ a \equiv 2293244\ (mod\ 19048567);$
$q = 3,\ l = 15,\ a \equiv 13555889\ (mod\ 19048567);$
$q = 5,\ l = 10,\ a \equiv 16937223\ (mod\ 19048567);$
$q = 7,\ l = 8,\ a \equiv 15214586\ (mod\ 19048567);$
$q = 11,\ l = 6,\ a \equiv 9685355\ (mod\ 19048567);$
$q = 13,\ l = 6,\ a \equiv 13271154\ (mod\ 19048567);$
$q = 17,\ l = 5,\ a \equiv 11406961\ (mod\ 19048567);$
$q = 19,\ l = 5,\ a \equiv 554506\ (mod\ 19048567).$

În acest caz, $(554506 - 1, 19048567) = 5281$.
Se obţine $19048567 = 5281 \cdot 3607$, care este chiar descompunerea în factori primi a lui n. Trebuie remarcat că:

$$5280 = 5281 - 1 = 2^5 \cdot 3 \cdot 5 \cdot 11, \quad 3606 = 3607 - 1 = 2 \cdot 3 \cdot 601.$$

Deci, 5280 are factorii primi mai mici decât 19, în timp ce celălalt număr nu are această proprietate.

11.6 Factorizare folosind curbele eliptice

Ca şi în cazul testului de primalitate ce utilizează teoria curbelor eliptice, şi aici vom prezenta doar ideea ce stă la baza acestui algoritm. Algoritmul generalizează algoritmul Pollard $p-1$ în sensul că grupul $\boldsymbol{Z}_p^*$, al cărui ordin este $p - 1$ (p este prim) este înlocuit cu grupul unei curbe eliptice aleatoare peste $\boldsymbol{Z}_p$. Dacă ordinul grupului ales are toţi factorii primi mai mici decât un număr iniţial considerat, atunci algoritmul furnizează un divizor propriu al lui n. În caz contrar, trebuie ales un alt grup.

În practică, acest algoritm este folosit pentru a determina factori primi cu mai puţin de 40 cifre zecimale pentru numere mari compuse. Astfel, el este considerat un algoritm cu scop special.

11.7 Metoda bazei factor

Ideea ce se află la baza acestei metode de factorizare este de fapt comună tuturor metodelor de factorizare cu pătrate aleatoare, şi anume:

Dacă găsim întregi x, y astfel încât $x^2 \equiv y^2 \ (mod\ n)$ şi $x \neq \pm y \ (mod\ n)$, atunci am aflat de fapt un divizor netrivial al lui n, anume $(x+y, n)$ sau $(x-y, n)$. Aceasta se obţine ţinând cont că $n \nmid x \pm y$ şi $n \mid (x-y)(x+y)$.

Pentru un modul n, şi a un număr întreg, vom spune că a_0 *este cel mai mic rest în valoare absolută* al lui a dacă $a \equiv a_0 \ (mod\ n)$ şi $-\frac{n}{2} \leq a_0 \leq \frac{n}{2}$.

Definiţie 11.7.1 *O bază factor este o mulţime $B = \{p_1, p_2, \ldots, p_k\}$ de numere prime distincte, mai puţin, eventual, p_1 care poate fi -1.*

Spunem că pătratul unui număr întreg b este $B-$ număr, relativ la numărul n, dacă cel mai mic rest în valoare absolută al lui $b^2 \ (mod\ n)$ se poate scrie ca un produs de numere din B.

De exemplu, pentru $n = 2701$ şi $B = \{-1, 2, 3\}$:
Din $52^2 \equiv 3 \ (mod\ 2701)$, $53^2 \equiv 108 \equiv 2^2 \cdot 3^3 \ (mod\ 2701)$, obţinem că 52^2 şi 53^2 sunt $B-$numere.

Considerăm n natural şi B o bază factor formată din k numere. Fiecărui $B-$număr b^2 îi vom pune în corespondenţă un vector

$$e = (e_1, e_2, \ldots, e_k)$$

unde $e_i \in \{0, 1\}$, pentru fiecare i, după cum urmează:
Scriem cel mai mic rest în valoare absolută $b^2 \ (mod\ n)$ sub forma $\prod_{i=1}^{k} p_i^{\alpha_i}$ şi definim $e_i \equiv \alpha_i \ (mod\ 2)$. Astfel, $e_i = 0$, dacă α_i este par şi $e_i = 1$, pentru α_i impar.

În exemplul nostru, lui 52^2 îi corespunde vectorul $(0, 0, 1)$ iar lui 53^2, acelaşi vector.

Fie $e_j = (e_{j1}, e_{j2}, \ldots, e_{jk})$ vectorul corespunzător lui a_j, cel mai mic rest în valoare absolută al $B-$ numărului $b_j^2 \ (mod\ n)$, pentru $1 \leq j \leq s$. Dacă suma vectorilor este vectorul nul (suma se calculează modulo 2), atunci produsul tuturor a_j este un produs de puteri pare ale numerelor

prime din B. Astfel,

$$\prod_{j=1}^{s} a_j = \prod_{i=1}^{k} p_i^{\sum\limits_{j=1,s} \alpha_{ji}} = \left(\prod_{i=1}^{k} p_i^{\frac{1}{2} \sum\limits_{j=1,s} \alpha_{ji}} \right)^2 .$$

Am găsit astfel x, y cele mai mici resturi în valoare absolută pentru numerele

$$\prod_{j=1}^{s} b_j \ (mod\ n), \quad \prod_{i=1}^{k} p_i^{\frac{1}{2} \sum\limits_{j=1,s} \alpha_{ji}} \ (mod\ n)$$

ale căror pătrate sunt congruente modulo n. Trebuie să observăm faptul că fiecare număr este construit altfel, unul ca produs de b_j, celălalt ca produs de p_i.

Dacă $x \equiv \pm y \ (mod\ n)$, trebuie să reluăm raţionamentul pentru altă mulţime de $B-$ numere pentru care suma vectorilor este vectorul nul.

Cum n este compus, probabilitatea să întâlnim o astfel de situaţie este de $\frac{1}{2}$. Va trebui continuat până când găsim o pereche (x, y) care ne furnizează un divizor propriu al lui n.

În exemplul considerat, $(0,0,1) + (0,0,1) = (0,0,0)$. Obţinem:
$52^2 \cdot 53^2 \equiv 3 \cdot 108 \equiv (2 \cdot 3^2)^2 \ (mod\ 2701)$.
Atunci, $x \equiv 52 \cdot 53 \equiv 55 \ (mod\ 2701)$, $y \equiv 18 \ (mod\ 2701)$.
Calculăm $(55 + 18, 2701) = 73$ şi rezultă $2701 = 73 \cdot 37$.

În practică, baza factor şi numerele b_j se aleg prin diverse metode. O alegere este de a porni cu B formată din primele k sau $k-1$ numere prime, după cum alegem $p_1 = -1$ sau nu. Numerele b_j se aleg aleator până se găsesc câteva ale căror pătrate sunt $B-$numere.

O altă cale de lucru constă în a începe cu alegerea unor b_j pentru care cel mai mic rest în valoare absolută $b_j^2 \ (mod\ n)$ este mic (în valoare absolută); de exemplu, alegem b_j apropiaţi de $\sqrt{hn}$, pentru multiplii mici hn. Atunci, B va fi formată din numerele prime mici, eventual şi -1, care apar în descompunerea în factori primi a mai multor $b_j^2 \ (mod\ n)$.

Să rezumăm acum modul de factorizare a unui număr mare n prin alegerea aleatoare a numerelor b_j.

Se alege un număr c de mărime intermediară; de exemplu, dacă n are 50 de cifre în scrierea zecimală, putem alege c un număr cu 5 sau 6 cifre zecimale. B este formată din -1 şi din toate numerele prime $\leq c$,

deci va avea $\pi(c)+1$ elemente. Se caută aleator mai multe numere b_j şi se calculează cel mai mic rest în valoare absolută pentru $b_j^2 \pmod n$. Se verifică dacă acesta se poate scrie ca produs de primi din B. Căutarea se opreşte când am găsit suficiente $B-$ numere $b_j^2 \pmod n$ ($\pi(c)+2$ sunt de ajuns). Pentru fiecare dintre ele se scrie vectorul corespunzător şi se formează o submulţime de numere b_j care au proprietatea că suma vectorilor este zero. Apoi se calculează $x = \prod_j b_j \pmod n$, $y = \prod_j p_j^{\beta_j} \pmod n$ care ştim că verifică $x^2 \equiv y^2 \pmod n$. Dacă $x \neq \pm y \pmod n$, am găsit un divizor propriu al lui n, calculând $(x+y, n)$.

11.8 Metoda fracţiilor continue

Am văzut că metoda bazei factor se aplică cel mai bine dacă există o metodă avantajoasă de a găsi întregi b astfel încât cel mai mic rest în valoare absolută al lui $b^2 \pmod n$ să fie produs de numere prime mici. Această situaţie apare în mod sigur dacă valoarea absolută a lui $b^2 \pmod n$ este mică. Prezentăm în cele ce urmează o metodă de a găsi întregi b pentru care $\mid b^2 \pmod n \mid < 2\sqrt{n}$. Pentru aceasta, este necesar să reprezentăm numărul $\sqrt{n}$ sub forma unei fracţii continue.

Propoziţie 11.8.1 *Fie $\alpha > 1$ un număr real a cărui fracţie continuă are convergentele $\frac{p_k}{q_k}$. Atunci, pentru orice $k \geq 0$,*

$$\left|p_k^2 - \alpha^2 q_k^2\right| < 2\alpha.$$

Demonstraţie. Ştim că $\frac{p_k}{q_k} < \alpha < \frac{p_{k+1}}{q_{k+1}}$ şi, din corolarul 2.1.2, $\left|\frac{p_k}{q_k} - \frac{p_{k+1}}{q_{k+1}}\right| = \frac{1}{q_k q_{k+1}}$. De aici,

$$\left|p_k^2 - \alpha^2 q_k^2\right| = q_k^2 \left|\alpha - \frac{p_k}{q_k}\right| \left|\alpha + \frac{p_k}{q_k}\right| < q_k^2 \frac{1}{q_k q_{k+1}} \left(\alpha + \left(\alpha + \frac{1}{q_k q_{k+1}}\right)\right).$$

Astfel,

$$\left|p_k^2 - \alpha^2 q_k^2\right| - 2\alpha < 2\alpha \left(-1 + \frac{q_k}{q_{k+1}} + \frac{1}{2\alpha q_{k+1}^2}\right) <$$

$$< 2\alpha \left(-1 + \frac{q_k}{q_{k+1}} + \frac{1}{q_{k+1}}\right) < 2\alpha \left(-1 + \frac{q_{k+1}}{q_{k+1}}\right) = 0. \qquad \square$$

Această propoziţie conduce la următorul rezultat:

Propoziţie 11.8.2 *Fie n număr natural, care nu este pătrat perfect. Fie $\frac{p_k}{q_k}$ convergentele fracţiei continue simple a lui $\sqrt{n}$. Atunci, pentru orice $k \geq 0$, cel mai mic rest în valoare absolută al lui $p_k^2 \ (mod\ n)$ este mai mic decât $2\sqrt{n}$.*

Demonstraţie. Folosim rezultatul demonstrat anterior pentru $\alpha = \sqrt{n}$. Astfel, $p_k^2 \equiv p_k^2 - nq_k^2 \ (mod\ n)$, de unde $\left|p_k^2 \ (mod\ n)\right| < 2\sqrt{n}$. □

Acest rezultat stă la baza algoritmului fracţiilor continue. Astfel, se precizează că, alegând numărătorii p_k ai convergentelor fracţiei continue a lui $\sqrt{n}$, se poate obţine un şir de numere ale căror pătrate au resturi mici. Pe lângă faptul că ne interesează doar numărătorii acestor fracţii, se operează doar cu resturi modulo n, deci, nu vom lucra cu numere foarte mari.

Vom preciza acum modul de realizare a algoritmul de factorizare folosind fracţiile continue utilizând o bază factor. De această dată, nu mai alegem aleator elementele b_j.

Astfel, începem prin a iniţializa:
$b_{-1} = 1,\ b_0 = [\sqrt{n}] = a_0,\ x_0 = \sqrt{n} - a_0$. Calculăm $b_0^2 \ (mod\ n)$.
Pentru $j = 1, 2, \ldots$ executăm:

1. $a_j = \left[\frac{1}{x_{j-1}}\right]$ şi apoi $x_j = \frac{1}{x_{j-1}} - a_j$.
2. $b_j \equiv a_j b_{j-1} + b_{j-2} \ (mod\ n)$.
3. Calculăm $b_j^2 \ (mod\ n)$.

După ce realizăm aceste calcule pentru mai multe valori ale lui j, vedem care numere de la punctul 3. se scriu ca $\pm$ produse de numere mici prime. Alegem în funcţie de acestea baza B care va fi formată din -1 şi din numerele prime mici ce apar în scrierea mai multor $b_j^2 \ (mod\ n)$. Apoi, procedăm ca în cazul metodei bazei factor.

De exemplu, pentru $n = 9509$,
$b_0 = 97,\ x_0 = 0,514101, b_0^2 \equiv -100 \ (mod\ 9509)$.
Obţinem:
$a_1 = \left[\frac{1}{x_0}\right] = 1,\ b_1 = 1 \cdot 97 + 1 = 98,\ x_1 = \frac{1}{x_0} - a_1 = 0,945143,$

$b_1^2 = 9604 \equiv 95 \ (mod\ 9509)$;
$a_2 = \left[\frac{1}{x_1}\right] = 1,\ b_2 = 1 \cdot 98 + 97 = 195,\ x_2 = \frac{1}{x_1} - a_2 = 0,0580409,$
$b_2^2 = 38025 \equiv -11 \ (mod\ 9509)$;
$a_3 = \left[\frac{1}{x_2}\right] = 17,\ b_3 = 17 \cdot 195 + 98 = 3413,\ x_3 = \frac{1}{x_2} - a_3 = 0,229229,$
$b_3^2 = 11648569 \equiv 44 \ (mod\ 9509)$.

Observăm că $-100 = -1 \cdot 2^2 \cdot 5^2,\ 95 = 5 \cdot 19,\ -11 = -1 \cdot 11,\ 44 = 2^2 \cdot 11$. Alegem $B = \{-1, 2, 5, 11\}$ şi numerele b_0, b_2, b_3. Vectorii corespunzători sunt $(1,0,0),\ (1,0,1),\ (0,0,1)$ a căror sumă vedem că este vectorul nul. Atunci,
$x = 97 \cdot 195 \cdot 3413 = 64556895 \equiv 294 \ (mod\ 9509)$ şi $y = 2^2 \cdot 5 \cdot 11 = 220$.
Calculăm $(294 + 220, 9509) = 257$ şi $(294 - 220, 9509) = 37$.

În final, prezentăm o variantă a metodei de factorizare cu ajutorul fracţiilor continue în care nu folosim o bază factor.

Pentru aceasta, să facem mai întâi următoarea observaţie: în cazul metodei Fermat se căutau numere naturale x, y cu proprietatea că $n = x^2 - y^2$ şi $x - y \neq 1$.

Factorizarea lui n este posibilă şi în cazul în care impunem nişte condiţii mai slabe asupra numerelor x, y şi anume:

$$n = x^2 - y^2, \quad 0 < y < x < n, \quad x + y \neq n.$$

Din aceste relaţii obţinem $n \nmid x \pm y$ şi $n \mid (x-y)(x+y)$. Atunci, $(x-y, n)$ şi $(x+y, n)$ sunt divizori netriviali ai lui n.

Pentru a determina soluţiile congruenţei se poate folosi reprezentarea lui $\sqrt{n}$ sub formă de fracţie continuă.

Propoziţie 11.8.3 *Fie n număr natural, care nu este pătrat perfect. Definim:*
$\alpha_0 = \sqrt{n},\ \alpha_k = \frac{P_k + \sqrt{n}}{Q_k},\ a_k = [\alpha_k],\ P_{k+1} = a_k Q_k - P_k,$
$Q_{k+1} = \frac{n - P_{k+1}^2}{Q_k},\ pentru\ k \geq 0.$

Fie $\frac{p_k}{q_k}$ $k-$convergenta fracţiei continue simple a lui $\sqrt{n}$. Atunci,

$$p_k^2 - nq_k^2 = (-1)^{k-1} Q_{k+1}.$$

Demonstraţie. Fie $\sqrt{n} = \alpha_0 = [a_0; a_1, a_2, \ldots, \alpha_k]$.
Astfel, $\sqrt{n} = \dfrac{\alpha_{k+1}p_k + p_{k-1}}{\alpha_{k+1}q_k + q_{k-1}}$. Cum $\alpha_{k+1} = \dfrac{P_{k+1} + \sqrt{n}}{Q_{k+1}}$, rezultă

$$\sqrt{n} = \frac{\left(P_{k+1} + \sqrt{n}\right) p_k + Q_{k+1}p_{k-1}}{\left(P_{k+1} + \sqrt{n}\right) q_k + Q_{k+1}q_{k-1}}.$$

Obţinem astfel,

$$nq_k + \left(P_{k+1}q_k + Q_{k+1}q_{k-1}\right)\sqrt{n} = \left(P_{k+1}p_k + Q_{k+1}p_{k-1}\right) + p_k\sqrt{n}.$$

De aici,

$$nq_k = P_{k+1}p_k + Q_{k+1}p_{k-1} \tag{11.1}$$
$$p_k = P_{k+1}q_k + Q_{k+1}q_{k-1} \tag{11.2}$$

Înmulţim prima relaţie cu q_k, a doua cu p_k şi scădem. Dacă ţinem cont şi de propoziţia 2.1.1, rezultă:

$$p_k^2 - nq_k^2 = \left(p_kq_{k-1} - p_{k-1}q_k\right) Q_{k+1} = (-1)^{k-1}Q_{k+1}. \quad \square$$

Cu ajutorul acestei propoziţii să vedem cum funcţionează algoritmul, fără a mai alege o bază factor.

Conform propoziţiei, $p_k^2 \equiv (-1)^{k-1}Q_{k+1} \ (mod\ n)$, pentru fiecare k. Presupunem k impar şi $Q_{k+1} \equiv s^2 \ (mod\ n)$, un pătrat perfect. Atunci $p_k^2 \equiv s^2 \ (mod\, n)$. Astfel, vom căuta pătrate perfecte s^2 în şirul Q_j pentru indici j pari. Atunci, pentru fiecare p_{j-1} vedem dacă $(p_{j-1} + s, n)$ este divizor propriu al lui n.

De exemplu, pentru $n = 9509$, obţinem:

$\alpha_0 = \sqrt{9509},\ P_0 = 0,\ Q_0 = 1,\ a_0 = \left[\sqrt{9509}\right] = 97;$

$P_1 = 97 \cdot 1 - 0 = 97,\ Q_1 = \dfrac{9509 - 97^2}{1} = 100,$

$\alpha_1 = \dfrac{\sqrt{9509} + 97}{100},\ a_1 = [\alpha_1] = 1;$

$P_2 = 100 \cdot 1 - 97 = 3,\ Q_2 = \dfrac{9509 - 3^2}{100} = 95,$

$\alpha_2 = \dfrac{\sqrt{9509} + 3}{95},\ a_2 = [\alpha_2] = 1;$

$$P_3 = 95 \cdot 1 - 3 = 92,\ Q_3 = \frac{9509 - 92^2}{95} = 11,$$

$$\alpha_3 = \frac{\sqrt{9509} + 92}{11},\ a_3 = [\alpha_3] = 17;$$

$$P_4 = 17 \cdot 11 - 92 = 95,\ Q_4 = \frac{9509 - 95^2}{11} = 44,$$

$$\alpha_4 = \frac{\sqrt{9509} + 95}{44},\ a_4 = [\alpha_4] = 4;$$

$$P_5 = 44 \cdot 4 - 95 = 81,\ Q_5 = \frac{9509 - 81^2}{44} = 67,$$

$$\alpha_5 = \frac{\sqrt{9509} + 81}{67},\ a_5 = [\alpha_5] = 2;$$

$$P_6 = 67 \cdot 2 - 81 = 53,\ Q_6 = \frac{9509 - 53^2}{67} = 100,$$

$$\alpha_6 = \frac{\sqrt{9509} + 53}{100},\ a_6 = [\alpha_6] = 1.$$

Calculăm acum p_5.

$p_0 = a_0 = 97,\ p_1 = a_0 a_1 + 1 = 98$
$p_2 = 1 \cdot 98 + 97 = 195,$
$p_3 = 17 \cdot 195 + 98 = 3413,$
$p_4 = 4 \cdot 3413 + 195 = 13847,$
$p_5 = 2 \cdot 13847 + 3413 = 31107 \equiv 2580\ (mod\ n).$

Atunci, $2580^2 \equiv 10^2\ (mod\ 9509)$.
Prin calcul, obţinem $(2580 - 10, 9509) = 257$ şi $(2580 + 10, 9509) = 37$.
Deci, $9509 = 257 \cdot 37$.

11.9 Metoda filtrului pătratic

Metoda filtrului pătratic, realizată de Pomerance, la începutul anilor 80, a fost mult timp mai performantă decât alte metode de factorizare de tip general. Ea este folosită pentru a factoriza numere mari n care nu au factori primi de mărime mult mai mică decât $\sqrt{n}$.

Filtrul pătratic este o variantă a metodei bazei factor. Ca bază B, vom alege în acest caz toate numerele prime $p \leq P$ (P este un număr

limită ales într-un fel optim) pentru care $\left(\frac{n}{p}\right) = 1$ pentru p impar. $p = 2$ va fi şi el inclus în bază, în mod automat. Vom nota cu S mulţimea de $B-$ numere pe care le căutăm. Ea va fi aceeaşi mulţime ca cea folosită în metoda Fermat, şi anume:

$$S = \{t^2 - n \mid \lceil\sqrt{n}\rceil \leq t \leq \lceil\sqrt{n}\rceil + A\}$$

cu A, o limită potrivit aleasă.

Ideea principală a acestei metode constă într-o filtrare asemănătoare ciurului lui Eratostene pentru elementele bazei alese iniţial.

Fie n un număr compus impar.

1. Alegem marginile P şi A, ambele de mărime apropiată cu $e^{\sqrt{\ln n \ln\ln n}}$. În general, A este ales mai mare decât P, dar nu mai mare decât o putere mică a lui P. De exemplu, $P < A < P^2$.

2. Pentru fiecare prim $p \leq P$, verificăm mai întâi dacă $\left(\frac{n}{p}\right) = 1$. Dacă relaţia nu se verifică, p este eliminat din bază.

3. Pentru $t = [\sqrt{n}]+1, [\sqrt{n}]+2, \ldots, [\sqrt{n}]+A$, realizăm o coloană de numere $t^2 - n$.

4. Alegem din coloana de la punctul 3. doar numerele $t^2 - n$ care sunt $B-$ numere.

5. Mai departe, se procedează ca în metoda bazei factor.

Pentru a exemplifica această metodă, factorizăm $n = 24961$ folosind cea mai simplă variantă de filtru pătratic.

Considerăm $P = 23$. Pentru simplificarea aplicaţiei, vom alege pentru t valorile $[\sqrt{n}], [\sqrt{n}] \pm 1, [\sqrt{n}] \pm 2, \ldots$.
Calculând $\left(\frac{n}{p}\right)$, pentru numerele prime $p \in \{7, 11, 17, 19\}$, n nu este rest pătratic. Deci, ele se elimină din bază. Obţinem $B = \{-1, 2, 3, 5, 13, 23\}$. Baza având 6 elemente, trebuie să determinăm cel puţin 7 $B-$ numere din care să putem alege pe cele pentru care aplicăm metoda bazei factor. Obţinem:

$a_0 = 157,\ b_0 \equiv a_0^2 - 24961 \equiv -312\ (mod\ 24961)$,
$-312 = -1 \cdot 2^3 \cdot 3 \cdot 13,\ v_0 = (1, 1, 1, 0, 1, 0)$.

$a_1 = 158,\ b_1 \equiv a_1^2 - 24961 \equiv 3\ (mod\ 24961)$,

$v_1 = (0, 0, 1, 0, 0, 0)$.

$a_2 = 156,\ b_2 \equiv a_2^2 - 24961 \equiv -625\ (mod\ 24961)$,
$-625 = -1 \cdot 5^4,\ v_2 = (1, 0, 0, 0, 0, 0)$.

$a_3 = 159,\ b_3 \equiv a_3^2 - 24961 \equiv 320\ (mod\ 24961)$,
$320 = 2^6 \cdot 5,\ v_3 = (0, 0, 0, 1, 0, 0)$.

$a_4 = 155,\ b_4 \equiv a_4^2 - 24961 \equiv -936\ (mod\ 24961)$,
$-936 = -1 \cdot 2^3 \cdot 3^2 \cdot 13,\ v_4 = (1, 1, 0, 0, 1, 0)$.

$a_5 = 161,\ b_5 \equiv a_5^2 - 24961 \equiv 960\ (mod\ 24961)$,
$960 = 2^6 \cdot 3 \cdot 5,\ v_5 = (0, 0, 1, 1, 0, 0)$.

$a_6 = 151,\ b_6 \equiv a_6^2 - 24961 \equiv -2160\ (mod\ 24961)$,
$-2160 = -1 \cdot 2^4 \cdot 3^3 \cdot 5,\ v_6 = (1, 0, 1, 1, 0, 0)$.

Observăm $v_0 + v_1 + v_4 = (0, 0, 0, 0, 0, 0)$. Atunci,

$$x \equiv 157 \cdot 158 \cdot 155 \equiv 936\ (mod\ 24961),$$
$$y \equiv -1 \cdot 2^3 \cdot 3^2 \cdot 13 \equiv 24025\ (mod\ 24961).$$

În această situaţie, $x \equiv -y\ (mod\ 24961)$, deci trebuie să căutăm altă combinaţie.

Din $v_2 + v_5 + v_6 = (0, 0, 0, 0, 0, 0)$, rezultă:

$$x \equiv 23405\ (mod\ 24961),$$
$$y \equiv -1 \cdot 2^5 \cdot 3^2 \cdot 5^3 \equiv 13922\ (mod\ 24961).$$

Acum $23405 \neq \pm 13922\ (mod\ 24961)$, şi calculăm:
$(23405 - 13922, 24961) = (9483, 24962) = 109$.

O situaţie mai complexă de tratare a acestei metode poate fi întâlnită în [12]. De asemenea, alte variante folosesc mai multe polinoame în selectarea $B-$ numerelor (noi am folosit doar $f = X^2 - n$), pentru a asigura o mai mare şansă de factorizare şi un interval de filtrare mai scurt, fiind aplicabil procesării paralele.

11.10 Filtrul corpului de numere

Problema factorizării nu a cunoscut îmbunătăţiri majore până în anul 1990 când Pollard a realizat un algoritm foarte rapid, cu ajutorul căruia a factorizat numărul RSA-130.

În unele privinţe, algoritmul este asemănător cu cele anterioare, el căutând întregi x, y astfel încât $x^2 \equiv y^2 \ (mod\ n)$ şi $x \neq \pm y \ (mod\ n)$. Pentru a realiza acest lucru, se folosesc două baze factor; una este formată din toate numere prime mai mici decât o anumită limită şi cealaltă bază este formată din toate idealele prime de normă mai mică decât o valoare considerată, din inelul de întregi al unui corp de numere algebrice potrivit ales.

Astfel, având la bază tehnica filtrului pătratic, algoritmul foloseşte teoria algebrică a numerelor, fiind considerat cel mai complicat algoritm cunoscut.

O versiune specială a algoritmului este folosită pentru a factoriza numere de forma $n = r^e - s$ pentru valori mici ale lui r şi $|s|$ (vezi [14]).

S-a dovedit că acest algoritm este mult mai rapid decât filtrul pătratic în factorizarea numerelor de aproximativ 115 cifre zecimale. La ora actuală, el deţine locul întâi în ierarhia algoritmilor de factorizare cu scop general.

Exerciţii propuse

1. Factorizaţi numerele: 8633, 200819, 809009 folosind metoda Fermat. Pentru 68987 aplicaţi metoda Fermat generalizată.

2. Arătaţi că numărul 23360947609 nu poate fi folosit într-un criptosistem RSA.

3. Aplicaţi metoda rho pentru a obţine o descompunere în factori primi pentru următoarele situaţii. De fiecare dată, comparaţi x_k numai cu x_j unde $j = 2^h - 1$ şi k este un număr cu $(h + 1)$ cifre binare.

i) $f(x) = x^2 - 1,\ x_0 = 2,\ n = 91$;

ii) $f(x) = x^2 + 1,\ x_0 = 1,\ n = 8051$;

iii) $f(x) = x^2 - 1,\ x_0 = 5,\ n = 7031$.

4. Factorizaţi $n = 4633$. folosind numerele 68, 152, 153 împreună cu o bază factor B potrivit aleasă.

5. Factorizaţi numerele $13561, 8777, 14429, 12403, 197209$ prin metoda fracţiilor continue.

6. Factorizaţi numerele 1046603 şi 998771 folosind metoda filtrului pătratic.

CAPITOLUL 12

Problema logaritmului discret

După cum am văzut în capitolul 9, securitatea multor criptosisteme se bazează pe ***problema logaritmului discret***, o altă ***problemă*** considerată în prezent ca fiind ***dificilă***.

Dacă considerăm un grup ciclic G, de ordin n, cu g un generator al său, atunci $G = \{1, g, g^2, \ldots, g^{n-1}\}$. Pentru $b \in G$, definim $\log_g b$ *logaritmul discret al lui* b *în baza* g ca fiind unicul număr $1 \leq x \leq n-1$ care verifică $b = g^x$.

Un caz particular a fost deja studiat în capitolul 6, şi anume situaţia în care grupul $U(\boldsymbol{Z}_n)$ este ciclic. În acest caz, un generator al grupului este rădăcina primitivă r, iar logaritmul discret a fost numit index aritmetic.

De exemplu, $U(\boldsymbol{Z}_{17})$ este un grup ciclic de ordin 16. Cum $ord_{17}3 = 16$, 3 este un generator sau, rădăcină primitivă modulo 17. Deoarece $3^4 = 81 \equiv 13 \ (mod\ 17)$, obţinem $log_3 13 = 4$.

Problema logaritmului discret, DLP, este formulată astfel:

Dacă considerăm un număr prim p, g un generator al grupului $\boldsymbol{Z}_p^*$ (rădăcină primitivă modulo p) şi un element $b \in \boldsymbol{Z}_p^*$, să se determine $1 \leq x \leq p-1$ pentru care $b \equiv g^x \ (mod\ p)$.

Dacă în locul lui $\boldsymbol{Z}_p^*$ alegem un grup ciclic oarecare, spunem că am enunţat ***problema generalizată a logaritmului discret,*** $GDLP$.

Trebuie să subliniem un fapt important. Dacă considerăm g_1 şi g_2 doi generatori diferiţi ai grupului G, ciclic de ordin n, iar $b \in G$ obţinem:

$$b = g_1^{\log_{g_1} b} = g_2^{\log_{g_2} b} = \left(g_1^{\log_{g_1} g_2}\right)^{\log_{g_2} b}.$$

Astfel, $\log_{g_1} b \equiv \log_{g_2} b \cdot \overline{\log_{g_1} g_2} \ (mod\ n)$. De aici rezultă că un algoritm care calculează logaritmi relativ la baza g_1 poate calcula logaritmi în orice bază g, cu g un generator oarecare al grupului. Această observaţie arată că dificultatea problemei logaritmului discret nu depinde de generatorul ales.

Spre deosebire de algoritmii de factorizare care au fost studiaţi timp de sute de ani, algoritmii de calcul a logaritmilor discreţi au o perioadă mult mai scurtă de cercetare, anume începând cu anul 1970. De cele mai multe ori, aceşti algoritmi sunt împărţiţi în două clase:

1. *metode de calculare a indexului*, care sunt asemănătoare cu cele mai rapide metode de factorizare. Există două metode clasice, strâns legate de algoritmii filtrului pătratic şi cel al filtrul corpului numerelor. Ele sunt eficiente numai în anumite grupuri, fiind necesar să se verifice anumite proprietăţi matematice.

2. *metode de găsire de coliziuni*, aplicate în cazuri generale. Cea mai performantă dintre acestea este metoda Pollard-rho.

Vom prezenta în continuare cei mai cunoscuţi algoritmi de rezolvare a *DLP*. Grupul ciclic G va fi grupul multiplicativ al unui corp finit cu p elemente, deci un grup de ordin $p-1$. Generatorul acestui grup va fi notat cu g şi vom avea de calculat $\log_g b$, unde $b \in G$.

12.1 Algoritmul Shanks

Fie $m = \left\lceil \sqrt{p-1} \right\rceil$. Dacă $b = g^x \in G$, atunci putem scrie $x = cm + d$, cu $0 \leq c, d \leq m-1$. Atunci, $b = g^x = g^{cm} g^d$, de unde $bg^{-d} = (g^m)^c$.

Pornind de la această observaţie, Shanks a propus o metodă de căutare succesivă pentru a determina $\log_g b$, numită şi algoritmul ***baby-step giant-step.***

Se creează două liste :

Giant step	Baby step
1	b
g^m	bg^{-1}
g^{2m}	bg^{-2}
$\vdots$	$\vdots$
$g^{(m-1)m}$	$bg^{-(m-1)}$

şi vedem pentru ce valori ale lui c şi d obţinem $g^{cm} = bg^{-d}$. Atunci, $\log_g b = cm + d$.

Algoritm 12.1.1 (Shanks)
INPUT: g, p, b *cu semnificaţiile anterioare.*
OUTPUT: $\log_g b$.

1. $m \leftarrow [\sqrt{p-1}]$
2. *Pentru* $c = 0, \ldots, m-1$, *construieşte un tabel cu* (c, g^{mc}), *care se ordonează după a doua componentă.*
3. *Calculează* g^{-1} *şi pune* $a \leftarrow b$.
4. *Pentru* $d = 0, \ldots, m-1$, *execută:*
   - 4.1. *Verifică dacă* a *este a doua componentă a unui element din tabel.*
   - 4.2. *Dacă* $a = g^{mc}$, *returnează* $x = cm + d$ *şi se opreşte.*
   - 4.3. *Pune* $a \leftarrow ag^{-1}$.

Spre exemplu, dacă alegem grupul ciclic $G = \boldsymbol{Z}_{181}^*$, de ordin 180, un generator al său este $g = 2$. În acest caz, $m = 13$. Vrem să aplicăm algoritmul pentru a determina $\log_2 30$.

Pentru $0 \leq c \leq 12$, $\left(2^{13}\right)^c$ ia valorile înscrise în tabel:

c	0	1	2	3	4	5
2^{13c}	1	47	37	110	102	88

c	6	7	8	9	10	11	12
2^{13c}	154	179	87	107	142	158	5

Din $2^{180} \equiv 1 \ (mod\ 181)$, rezultă $2^{-1} \equiv 2^{179} \equiv 91 \ (mod\ 181)$.
Calculăm $b2^{-d}$, până găsim o valoare egală cu un 2^{13c} anterior calculat.

Pentru $d \leq 7$ valorile obţinute sunt:

d	0	1	2	3	4	5	6	7
$30 \cdot 2^{-d}$	30	15	98	49	115	148	74	37

Am obţinut $\left(2^{13}\right)^2 \equiv 30 \cdot 2^{-7} \ (mod\ 181)$. Astfel, $c = 2$ iar $d = 7$. Rezultă $\log_2 30 = 2 \cdot 13 + 7 = 33$.

12.2 Algoritmul Pohlig-Hellman

Acest algoritm este utilizabil dacă ordinul grupului ciclic are factori primi mici. Presupunem că $p - 1 = \prod_{i=1}^{m} q_i^{k_i}$, cu q_i numere prime distincte. Fie $g^x \equiv b \ (mod\ p)$. Din capitolul 6.3, ştim că această congruenţă este echivalentă cu $x \equiv \log_g b \ (mod\ p-1)$. Folosind teorema chinezească a resturilor, este suficient să determinăm $x_i \equiv x \ (mod\ q_i^{k_i})$, pentru fiecare $1 \leq i \leq m$. Cu aceste valori, vom calcula apoi $x \ (mod\ p-1)$.

Fie q un divizor prim al lui $p-1$ astfel încât $q^k \| p-1$. Pentru a calcula $x_q \equiv x \ (mod\ q^k)$, considerăm $x \equiv a_0 + a_1 q + \ldots + a_{k-1} q^{k-1} \ (mod\ q^k)$, cu $0 \leq a_i \leq q-1$. Vom determina succesiv aceşti coeficienţi.

Pentru aceasta, fie $\alpha \equiv g^{\frac{p-1}{q}} \ (mod\ p)$. Atunci, $\alpha^q \equiv 1 \ (mod\ p)$.

Vom determina toate elementele $r_{q,i} \equiv \alpha^i \ (mod\ p)$ de ordin q, pentru $0 \leq i \leq q-1$, folosind metoda ridicării succesive la pătrat şi le vom păstra într-un tabel. Lucrând în ipoteza că divizorii primi ai lui $p-1$ sunt mici, dimensiunea tabelului este rezonabilă.

Congruenţa $g^x \equiv b \ (mod\ p)$ devine:

$$b^{\frac{p-1}{q}} \equiv (g^x)^{\frac{p-1}{q}} \equiv g^{a_0 \frac{p-1}{q} + a_1 (p-1) + \cdots} \equiv g^{a_0 \frac{p-1}{q}} \equiv \alpha^{a_0} \ (mod\ p).$$

Deci, $r_{q,a_0} = \alpha^{a_0} \equiv b^{\frac{p-1}{q}} \ (mod\ p)$. Astfel, vom compara $b^{\frac{p-1}{q}}$ cu toate elementele $r_{q,j}$ şi a_0 va fi egal cu valoarea j pentru care obţinem egalitate.

Pentru a determina a_1, considerăm $b_1 \equiv b g^{-a_0} \ (mod\ p)$, adică:

$$g^{x-a_0} \equiv b_1 \ (mod\ p).$$

Atunci:

$$b_1^{\frac{p-1}{q^2}} \equiv (g^{x-a_0})^{\frac{p-1}{q^2}} \equiv g^{a_1\frac{p-1}{q}+a_2(p-1)+\ldots} \equiv g^{a_1\frac{p-1}{q}} \equiv \alpha^{a_1} \equiv r_{q,a_1} \ (mod\ p).$$

Vom compara $b_1^{\frac{p-1}{q^2}}$ cu elementele din mulţimea $\{r_{q,j}\}_{0\leq j<q}$ după care identificăm a_1 cu indicele j pentru care se obţine egalitatea.

Procedăm inductiv, pentru a obţine toţi coeficienţii a_i. Vom nota:

$$b_i = bg^{-(a_0+a_1q+\ldots+a_{i-1}q^{i-1})}.$$

Atunci, $b_i^{\frac{p-1}{q^i}} \equiv 1 \ (mod\ p)$ şi $b_i^{\frac{p-1}{q^{i+1}}} \equiv r_{q,a_i}$.

În final, obţinem $x \ (mod\ q^k)$. Aplicând procedeul pentru fiecare divizor $q \mid p-1$ şi folosind teorema chinezească a resturilor, obţinem $x = \log_g b$.

Algoritm 12.2.1 (Pohlig-Hellman)
INPUT: g, p, b *cu semnificaţiile anterioare.*
OUTPUT: $\log_g b$.

1. *Factorizează* $p-1 = \prod_{i=1}^{m} q_i^{k_i}$.
2. *Pentru* i *de la* 1 *la* m *efectuează:*
   - 2.1. $q \leftarrow q_i$, $k \leftarrow k_i$.
   - 2.2. $b_1 \leftarrow 1$, $a_{-1} \leftarrow 0$.
   - 2.3. *Calculează* $\alpha \leftarrow g^{(p-1)/q}$
   - 2.4. *Pentru* j *de la* 0 *la* $k-1$, *efectuează:*
     - 2.4.1. *Calculează* $b_1 \leftarrow b_1 g^{a_{j-1}q^{j-1}}$, $b' \leftarrow (bb_1^{-1})^{(p-1)/q^{j+1}}$.
     - 2.4.2. *Calculează* $a_j \leftarrow \log_\alpha b'$ *folosind algoritmul Shanks.*
   - 2.5. $x_i \leftarrow a_0 + a_1q + \ldots + a_{k-1}q^{k-1}$.
3. *Aplică algoritmul Gauss pentru a rezolva sistemul* $x \equiv x_i \ (mod\ q_i^{k_i})$, $1 \leq i \leq m$.
4. *Returnează* x.

De exemplu, să recalculăm $\log_2 30$ în grupul $G = \boldsymbol{Z}_{181}^*$, de ordin $180 = 2^2 \cdot 3^2 \cdot 5$. Vom avea $p = 181$, $g = 2$, $b = 30$ şi $q \in \{2, 3, 5\}$.

Calculăm pentru fiecare q valorile $r_{q,j}$ pentru $0 \leq j \leq q-1$.

1. $q = 2$. Atunci, $x \equiv a_0 + a_1 \cdot 2 \ (mod\ 4)$, $a_0, a_1 \in \{0, 1\}$.
$\alpha = 2^{\frac{180}{2}} = 2^{90} \equiv 180 \equiv -1 \ (mod\ 181)$.
$r_{2,0} = \alpha^0 = 1$, $r_{2,1} = \alpha = -1$.
$b^{\frac{180}{2}} = 30^{90} \equiv 180 \ (mod\ 181)$, deci $a_0 = 1$.
Fie $b_1 = bg^{-1} \equiv 30 \cdot 91 \equiv 15 \ (mod\ 181)$. Din $b_1^{\frac{180}{2^2}} \equiv 15^{45} \equiv 1 \ (mod\ 181)$, rezultă $b_1^{\frac{180}{2^2}} \equiv r_{2,0} \ (mod\ 181)$, adică $a_1 = 0$. Deci, $x \equiv 1 \ (mod\ 4)$.

2. $q = 3$. Reluăm procedeul anterior, şi, pentru $x \equiv a_0 + a_1 \cdot 3 \ (mod\ 9)$, cu $0 \leq a_0, a_1 \leq 2$, rezultă:
$r_{3,0} \equiv 1 \ (mod\ 181)$, $r_{3,1} \equiv \alpha \equiv 2^{\frac{180}{3}} \equiv 2^{60} \equiv 48 \ (mod\ 181)$,
$r_{3,2} \equiv \alpha^2 \equiv 132 \ (mod\ 181)$.
$30^{\frac{180}{3}} = 30^{60} \equiv 1 \equiv r_{3,0} \ (mod\ 181)$, deci $a_0 = 0$.
Acum, $b_1 = b = 30$. Din $b_1^{\frac{180}{3^2}} \equiv 30^{20} \equiv 132 \equiv r_{3,2} \ (mod\ 181)$, rezultă $a_1 = 2$, deci $x \equiv 6 \ (mod\ 9)$.

3. $q = 5$. În acest caz, $x \equiv a_0 \ (mod\ 5)$, $0 \leq a_0 \leq 4$.
$r_{5,0} \equiv 1 \ (mod\ 181)$, $r_{5,1} \equiv \alpha \equiv 2^{\frac{180}{5}} \equiv 2^{36} \equiv 59 \ (mod\ 181)$,
$r_{5,2} \equiv \alpha^2 \equiv 42 \ (mod\ 181)$, $r_{5,3} \equiv \alpha^3 \equiv 125 \ (mod\ 181)$,
$r_{5,4} \equiv \alpha^4 \equiv 135 \ (mod\ 181)$.
$b^{\frac{180}{5}} \equiv 30^{36} \equiv 125 \equiv r_{5,3} \ (mod\ 181)$. Astfel, $a_0 = 3$ şi $x \equiv 3 \ (mod\ 5)$.

Rezolvăm sistemul:

$$\begin{cases} x \equiv 1 \ (mod\ 4) \\ x \equiv 6 \ (mod\ 9) \\ x \equiv 3 \ (mod\ 5) \end{cases}$$

folosind teorema chinezească a resturilor şi obţinem $x \equiv 33 \ (mod\ 180)$. Deci, $\log_2 30 = 33$.

12.3 Algoritmul Pollard rho

Algoritmul Polard rho pentru calculul logaritmului discret este preferat algoritmului Shanks datorită faptului că acesta necesită o cantitate mai mică de date ce trebuie stocate. Pentru a simplifica prezentarea acestui algoritm vom considera cazul în care grupul ciclic G este $\boldsymbol{Z}_p^*$, cu p număr prim.

Grupul G este partiţionat în trei mulţimi S_1, S_2, S_3, de cardinale aproximativ egale. Alegerea celor trei submulţimi trebuie făcută cu grijă: $1 \notin S_2$ şi criteriul după care se face distribuirea elementelor grupului în fiecare mulţime trebuie să conţină condiţii uşor de verificat. Cele mai simple şi mai des întâlnite moduri de partiţionare sunt următoarele:

$$\begin{aligned} S_1 &= \{x \in G \mid 0 < x < \frac{p}{3}\} \\ S_2 &= \{x \in G \mid \frac{p}{3} < x < \frac{2p}{3}\} \\ S_3 &= \{x \in G \mid \frac{2p}{3} < x < p\} \end{aligned}$$

sau

$$\begin{aligned} S_1 &= \{x \in G \mid x \equiv 1 \ (mod\ 3)\} \\ S_2 &= \{x \in G \mid x \equiv 0 \ (mod\ 3)\} \\ S_3 &= \{x \in G \mid x \equiv 2 \ (mod\ 3)\} \end{aligned}$$

Definim şirul $(x_i)_{i \geq 0}$ de elemente ale grupului G prin $x_0 = 1$ şi, pentru $i > 0$:

$$x_{i+1} = \begin{cases} bx_i, & x_i \in S_1; \\ x_i^2, & x_i \in S_2; \\ gx_i, & x_i \in S_3. \end{cases}$$

Şirul astfel construit determină alte două şiruri de numere naturale $(c_i)_{i \geq 0}$ şi $(d_i)_{i \geq 0}$ care verifică $x_i = g^{c_i} b^{d_i}$. Astfel, $c_0 = 0$, $d_0 = 0$ şi pentru $i > 0$,

$$c_{i+1} = \begin{cases} c_i, & x_i \in S_1; \\ 2c_i \ (mod\ p-1), & x_i \in S_2; \\ c_i + 1 \ (mod\ p-1), & x_i \in S_3. \end{cases}$$

şi

$$d_{i+1} = \begin{cases} d_i + 1 \ (mod\ p-1), & x_i \in S_1; \\ 2d_i \ (mod\ p-1), & x_i \in S_2; \\ d_i, & x_i \in S_3. \end{cases}$$

Algoritmul lui Floyd de ciclare, prezentat în 11.2, este folosit în continuare pentru a determina o coliziune $x_i = x_{2i}$.

Atunci, $g^{c_i} b^{d_i} \equiv g^{c_{2i}} b^{d_{2i}} \ (mod\ p)$, de unde $g^{c_i - c_{2i}} \equiv b^{d_{2i} - d_i} \ (mod\ p)$. Dacă notăm $e \equiv d_{2i} - d_i \ (mod\ p-1)$ şi $f \equiv c_i - c_{2i} \ (mod\ p-1)$, $0 \leq e, f \leq p-2$, obţinem

$$b^e \equiv g^f \ (mod\ p) \tag{12.1}$$

de unde,

$$e \log_g b \equiv f \ (mod\ p-1). \tag{12.2}$$

Această congruenţă oferă o posibilitate de a determina $\log_g b$ dacă $e \neq 0 \ (mod\ p-1)$. În cazul în care $e \equiv 0 \ (mod\ p-1)$, trebuie alese alte valori pentru c_0, d_0 şi repetat procedeul.

Fie $d = (e, p-1)$ şi u, v numerele întregi pentru care $d = eu + (p-1)v$. Din congruenţa (12.1) rezultă $b^{eu} \equiv g^{fu} \ (mod\ p)$. Obţinem:

$$b^d \equiv b^{eu} \left(b^{p-1}\right)^v \equiv b^{eu} \equiv g^{fu} \ (mod\ p).$$

Cum $b \equiv g^{\log_g b} \ (mod\ p)$, deducem

$$g^{d \log_g b} \equiv g^{fu} \ (mod\ p)$$

şi, în final,

$$d \log_g b \equiv fu \ (mod\ p-1).$$

Fie k număr natural pentru care $d \log_g b = fu + k(p-1)$. Din $d \mid p-1$, rezultă $d \mid fu$ şi astfel,

$$\log_g b = \frac{k(p-1) + fu}{d}$$

pentru un k, $0 \leq k \leq d-1$.

Dacă $d = 1$, e are invers modulo $p-1$ şi, din (12.2), obţinem

$$\log_g b \equiv \overline{e} f \ (mod\ p-1).$$

Dacă $d \neq 1$, se calculează $\log_g b$, dând valori lui k, până se verifică congruenţa $g^{log_g b} \equiv b \ (mod\ p)$. Dacă valoarea lui d este foarte mare, atunci trebuie căutată o altă variantă de lucru datorită volumului mare de verificări ce trebuie făcute.

Putem face următoarea observaţie: dacă grupul G are ordinul n, un număr prim şi $e \neq 0 \ (mod\ n)$, atunci, $d = 1$ şi determinarea logaritmului discret se simplifică.

Pentru acest caz, propunem următorul algoritm:

Algoritm 12.3.1 (Polard-rho)
INPUT: g, b *cu semnificaţiile anterioare şi*
n *număr prim, egal cu ordinul grupului* G.
OUTPUT: $\log_g b$.

1. $x_0 \leftarrow 1, c_0 \leftarrow 0, d_0 \leftarrow 0$.
2. *Pentru* $i = 1, 2, \ldots$ *efectuează:*
   - 2.1. *Folosind* $x_{i-1}, c_{i-1}, d_{i-1}$ *şi* $x_{2i-2}, c_{2i-2}, d_{2i-2}$ *calculează* x_i, c_i, d_i *şi* x_{2i}, c_{2i}, d_{2i} *folosind relaţiile anterioare.*
   - 2.2. *Dacă* $x_i = x_{2i}$ *atunci:*
     - 2.2.1. $e \leftarrow d_{2i} - d_i \pmod n$
     - 2.2.2. *Dacă* $e \equiv 0 \pmod n$, *returnează mesaj de eşec şi se opreşte; altfel calculează şi returnează* $\log_g b = \overline{e}(c_i - c_{2i}) \pmod n$.

Să vedem, pe un caz concret, cum funcţionează algoritmul. Calculăm $\log_2 153$ în $\boldsymbol{Z}^*_{181}$. Alegem pentru partiţionare grupului, a doua variantă prezentată. Rezultatele sunt cuprinse în următorul tabel:

i	x_i	c_i	d_i	x_{2i}	c_{2i}	d_{2i}
1	153	0	1	60	0	2
2	60	0	2	141	1	4
3	161	0	4	123	3	8
4	141	1	4	109	6	17
5	152	2	8	24	6	19
6	123	3	8	3	24	76
7	106	6	16	81	96	124
8	109	6	17	34	24	136
9	25	6	18	87	25	137
10	24	6	19	19	50	95
11	33	12	38	22	51	96
12	3	24	76	80	102	14
13	9	48	152	45	103	15
14	81	96	124	134	26	31
15	45	12	68	148	54	62

i	x_i	c_i	d_i	x_{2i}	c_{2i}	d_{2i}
16	34	24	136	11	54	64
17	134	24	137	108	55	65
18	87	25	137	160	111	130
19	148	50	94	34	42	82
17	134	24	137	108	55	65
18	87	25	137	160	111	130
19	148	50	94	34	42	82
20	19	50	95	87	43	83
21	11	50	96	19	86	167
22	**22**	51	96	**22**	87	168

Am găsit o coliziune $x_{22} = x_{44}$. Atunci, avem de rezolvat congruenţa $(168 - 96)y \equiv 51 - 87 \ (mod\ 180)$.
Ea este echivalentă cu $72y \equiv -36 \ (mod\ 180)$, adică $y \equiv 2 \ (mod\ 5)$. Deci, $y = 2 + 5k$, $k < 36$.
Pentru $k = 21$ obţinem $y = 107$ care verifică $2^{107} \equiv 153 \ (mod\ 181)$. Deci, $\log_2 153 = 107$.

12.4 Algoritmul index-calculus

Acest algoritm reprezintă cea mai puternică metodă cunoscută pentru determinarea logaritmului discret. Ea este însă aplicabilă doar unor grupuri, cum ar fi $\boldsymbol{Z}_p^*$ sau pentru grupul multiplicativ al unui corp finit cu p^n elemente, unde p este număr prim. Algoritmul este în multe privinţe asemănător cu metoda bazei factor, prezentată în capitolul 11.7.

Pentru o prezentare cât mai simplificată a acestui algoritm, vom studia doar cazul lui $G = \boldsymbol{Z}_p^*$. Pentru cazul $G = F_{p^n}^*$ unde F_{p^n} este un corp finit cu p^n elemente, trebuie mai întâi studiate proprietăţile corpurilor finite, construcţia acestora, algoritmul Berlekamp de factorizare a polinoamelor cu coeficienţi într-un corp finit (ce pot fi găsite în [9]). Doar după aceea se poate înţelege algoritmul prezentat în [12].

Algoritmul este format din două etape importante:

Pregătirea calculului.

1. Se alege mai întâi o bază $B \subset \boldsymbol{Z}_p^*$. În cazul nostru, de obicei se aleg primele t numere prime având grijă ca majoritatea elementelor grupului să poată fi exprimate în funcţie de acestea.
Fie $B = \{p_1, p_2, \ldots, p_t\}$.

2. Se determină $\log_g p_i$ pentru fiecare element al bazei. Pentru aceasta, se alege aleator k, $0 \leq k \leq p-2$, şi se calculează $g^k \ (mod\ p)$. Vedem dacă

$$g^k \equiv \prod_{i=1}^{t} p_i^{a_i} \ (mod\ p),$$

unde $a_i \geq 0$.

Dacă relaţia nu se verifică, se alege altă valoare pentru k.

Dacă congruenţa are loc, rezultă

$$k \equiv \sum_{i=1}^{t} a_i \log_g p_i \ (mod\ p-1).$$

Se repetă acest procedeu până obţinem un sistem liniar de congruenţe cu soluţie unică, adică determinantul matricei sistemului este număr prim cu $p-1$. În acest moment, rezolvând sistemul obţinem o *bază de date* ce este folosită în etapa următoare.

Ţinând cont de cele prezentate, rezultă că dimensiunea bazei trebuie aleasă cu grijă. Baza trebuie să conţină un număr redus de elemente, pentru ca sistemul de congruenţe ce trebuie rezolvat să nu fie prea mare. În acelaşi timp, dacă t este prea mic, există riscul ca relaţiile ce trebuie aflate să nu se găsească uşor.

Calculul logaritmului discret.

1. Se alege aleator k, cu $0 \leq k \leq p-2$ şi se calculează $bg^k \ (mod\ p)$.

2. Dacă $bg^k \equiv \prod_{i=1}^{t} p_i^{b_i} \ (mod\ p)$, $b_i \geq 0$, aplicăm logaritmul în ambii membri ai congruenţei şi obţinem valoarea dorită

$$\log_g b \equiv \sum_{i=1}^{t} b_i \log_g p_i - k \ (mod\ p-1).$$

În caz contrar, se repetă calculul pentru o altă valoare a lui k.

Spre exemplu, să calculăm $log_2 62$ în $\boldsymbol{Z}_{181}^*$. Alegem baza $B = \{2, 3, 5\}$.
Din $2^{56} \equiv 3 \ (mod\ 181)$ rezultă $\log_2 3 = 56$.
$2^{90} \equiv 180 \equiv 2^2 \cdot 3^2 \cdot 5 \ (mod\ 181)$ conduce la congruenţa
$90 \equiv 2 + \log_2 3 + \log_2 5 \ (mod\ 180)$. Înlocuind, rezultă $\log_2 5 = 156$.
Deci, $\log_2 2 = 1, \log_2 3 = 56, \log_2 5 = 156$.
Din $62 \cdot 2^8 \equiv 5^3 \ (mod\ 181)$, obţinem
$\log_2 62 + 8 \equiv 3 \log_2 5 \ (mod\ 180)$.
Atunci, $\log_2 62 \equiv 468 \equiv 100 \ (mod\ 180)$. Deci, $\log_2 62 = 100$.

Exerciţii propuse

1. Folosind algoritmul Shanks determinaţi:

$$\log_{11} 14 \ (mod\ 23),\ \log_3 57 \ (mod\ 113).$$

2. Cu ajutorul algoritmului Pohlig-Hellman, calculaţi:

$$log_2 28 \ (mod\ 37),\ \log_{11} 8 \ (mod\ 41).$$

3. Aplicaţi algoritmul Pollard-rho pentru a afla

$$log_2 228 \ (mod\ 191)$$

4. Folosind algoritmul index-calculus:

i) rezolvaţi congruenţa $3^x \equiv 76 \ (mod\ 89)$.

ii) aflaţi valoarea lui $\log_6 13 \ (mod\ 229)$.

CAPITOLUL 13

Problema rădăcinilor pătrate modulo n

Folosind algoritmul 7.3.1, putem determina uşor dacă un întreg a cu $1 < a < p$, este rest pătratic modulo p, adică stabilim dacă congruenţa $x^2 \equiv a \ (mod\ p)$ are soluţii.

Dacă considerăm acum un număr compus, n, spre deosebire de cazul precedent($n = p$ prim), aici stabilirea dacă a este rest pătratic modulo n este mult mai complicată.

Dacă simbolul Jacobi $\left(\frac{a}{n}\right) = -1$, atunci este simplu, a este non-rest pătratic modulo n.

Problema apare când $\left(\frac{a}{n}\right) = 1$. În acest caz, stabilirea dacă a este rest pătratic sau nu modulo n este considerată o problemă dificilă. Aceasta poartă numele de ***problema resturilor pătratice*** şi stă la baza securităţii unor scheme criptografice cu cheie publică.

Funcţiile criptografice folosesc frecvent operaţii de ridicare la pătrat modulo n sau de extragere a rădăcinii pătrate modulo n. Din păcate, dacă n este compus şi nu i se cunoaşte descompunerea în factori primi, este foarte dificil să determinăm rădăcini pătrate modulo n. Această problemă este cunoscută sub numele de ***problema rădăcinilor pătrate modulo n***. S-a demonstrat că această problemă este computaţional echivalentă cu problema factorizării (vezi [15]).

13.1 Rădăcini pătrate mod p

Pentru a determina soluţiile congruenţei $x^2 \equiv a \ (mod\ p)$ unde a este un rest pătratic modulo p, ne vom folosi de b, un non-rest pătratic modulo p, pe care îl determinăm prin încercări.

Mai întâi scriem $p-1 = 2^s t$, unde t este impar. Facem notaţiile:

$$c \equiv b^t \ (mod\ p),\ r \equiv a^{\frac{t+1}{2}} \ (mod\ p),$$

cu $c, r < p$.

Arătăm că c are ordinul egal cu 2^s modulo p.
Observăm că $c^{2^s} \equiv b^{2^s t} \equiv b^{p-1} \equiv 1 \ (mod\ p)$. Deci, $ord_p c \mid 2^s$. Presupunem $ord_p c = 2^{s_1}$, unde $s_1 < s$. Fie ξ o rădăcină primitivă modulo p. Atunci, conform propoziţiei 6.1.3, există k cu $1 \leq k \leq \phi(p)$ astfel ca $c = \xi^k$. Din $\xi^{k2^{s_1}} \equiv 1 \ (mod\ p)$, rezultă $2^s t \mid k2^{s_1}$. Din presupunerea făcută, $2^{s-s_1} t \mid k$ deci, k este număr par. Rezultă $c = \xi^{2k_1}$ şi c devine pătrat modulo p. Această afirmaţie nu este însă adevărată, pentru că $\left(\frac{c}{p}\right) = \left(\frac{b}{p}\right)^t = (-1)^t = -1$.

În concluzie, $ord_p c = 2^s$.
Observăm că $\left(r^2 a^{-1}\right)^{2^{s-1}} \equiv a^{2^{s-1}t} = a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \equiv 1 \ (mod\ p)$.

Vom înlocui r cu un element x de ordin 2^s modulo p astfel ca $x^2 a^{-1} \equiv 1 \ (mod\ p)$. Rămâne să găsim o putere convenabilă c^j, cu $0 \leq j < 2^s$, pentru care $x = c^j r$ este rădăcina pătrată modulo p a lui a.
Pentru aceasta, scriem j în baza 2 astfel

$$j = j_0 + 2j_1 + 4j_2 + \ldots + 2^{s-2} j_{s-2}$$

şi să vedem cum determinăm cifrele sale binare. Înainte de a realiza acest lucru, subliniem că putem presupune $j < 2^{s-1}$ deoarece $c^{2^{s-1}} \equiv -1 \ (mod\ p)$. Prin înlocuirea lui j cu 2^{s-1}, obţinem un alt j pentru care $c^j r$ este cealaltă rădăcină pătrată modulo p a lui a.

Procedeul inductiv de determinare a cifrelor binare ale lui j constă în:

1) Calculăm $\left(r^2 a^{-1}\right)^{2^{s-2}} \ (mod\ p)$. Am văzut că pătratul acestei expresii este 1 $(mod\ p)$. Deci, vom obţine $\pm 1 \ (mod\ p)$. Dacă valoarea găsită

este 1, luăm $j_0 = 0$, altfel $j_0 = 1$. Deci, j_0 este ales astfel încât $\left(c^{j_0} r\right)^2 a^{-1}$ să aibă ordinul modulo p egal cu 2^{s-2}.

2) Presupunem că am determinat $j_0, \ldots, j_{k-1}$ astfel ca

$$\left(c^{j_0+2j_1+\ldots+2^{k-1}j_{k-1}} \cdot r\right)^2 \cdot a^{-1}$$

să aibă ordinul 2^{s-k-1} modulo p. Pentru a determina j_k, ridicăm acest număr la o putere egală cu jumătate din ordinul său. Obţinem astfel,

$$\left(\left(c^{j_0+2j_1+\ldots 2^{k-1}j_{k-1}} \cdot r\right)^2 \cdot a^{-1}\right)^{2^{s-k-2}} \equiv \pm 1 \ (mod\ p).$$

Pentru valoarea 1, alegem $j_k = 0$ iar pentru -1, $j_k = 1$.
Astfel,

$$\left(c^{j_0+2j_1+\ldots+2^k j_k} \cdot r\right)^2 \cdot a^{-1}$$

va avea ordinul 2^{s-k-2} modulo p.
Când ajungem la $j = s-2$, vom avea

$$\left(c^{j_0+2j_1+\ldots+2^{s-2}j_{s-2}} \cdot r\right)^2 \cdot a^{-1} \equiv 1 \ (mod\ p),$$

de unde $c^j r$ este cel căutat.

Să găsim o rădăcină pătrată a lui $a = 186$ modulo $p = 401$.

Primul non-rest pătratic găsit este $b = 3$. Avem $p-1 = 2^4 \cdot 25$. Atunci, $c \equiv 3^{25} \equiv 268 \ (mod\ 401)$ şi $r \equiv a^{13} \equiv 103 \ (mod\ 401)$.
Aplicăm algoritmul de determinare al inversului lui a modulo 401 şi obţinem $a^{-1} \equiv 235 \ (mod\ 401)$.
Calculăm $r^2 a^{-1} \equiv 98 \ (mod\ 401)$ cu $ord_{401} 98 = 8$.
Din $98^4 \equiv -1 \ (mod\ 401)$, rezultă $j_0 = 1$.
Calculăm apoi $(cr)^2 a^{-1} \equiv (268 \cdot 103)^2 \cdot 235 \equiv -1 \ (mod\ 401)$. Cum, la pătrat, numărul va fi 1, obţinem $j_1 = 0$ şi $j_2 = 1$. Astfel, $j = 1 + 2 \cdot 0 + 4 \cdot 1 = 5$. Rădăcina pătrată căutată este $c^5 r \equiv 304 \ (mod\ 401)$.

Algoritm 13.1.1 (Rădăcini pătrate mod p prim)
INPUT: numerele naturale $a < p$, cu p prim impar.
OUTPUT: Două rădăcini pătrate ale lui a mod p.

1. *Calculează $\left(\frac{a}{p}\right)$ folosind algoritmul 7.3.1.*
2. *Dacă $\left(\frac{a}{p}\right) = -1$, atunci returnează* a nu are rădăcini pătrate $(\mathrm{mod}\ p)$ *şi se opreşte.*
3. *Caută $1 \leq b \leq p-1$, până când $\left(\frac{b}{p}\right) = -1$.*
4. *Scrie $p - 1 = 2^s t$, unde t este impar.*
5. *Calculează $\bar{a}$ $(mod\ p)$, folosind algoritmul 3.2.1.*
6. *Pune $c \leftarrow b^t$ $(mod\ p)$, $r \leftarrow a^{(t+1)/2}$ $(mod\ p)$ (algoritmul 3.1.1)*
7. *Pentru $i = 1, \ldots, p-1$ execută:*
   - 7.1. *$d \leftarrow (r^2 \cdot \bar{a})^{2^{s-i-1}}$ $(mod\ p)$*
   - 7.2. *Dacă $d \equiv -1$ $(mod\ p)$, atunci $r \leftarrow r \cdot c$ $(mod\ p)$.*
   - 7.3. *$c \leftarrow c^2$ $(mod\ p)$*
8. *Returnează r,-r.*

Cea mai simplă situaţie ce poate apare pentru acest algoritm este cea în care $p \equiv 3\ (mod\ 4)$. Atunci, $s = 1$, de unde $\frac{t+1}{2} = \frac{p+1}{4}$. Atunci, $\left(\pm a^{\frac{p+1}{4}}\right)^2 = a^{\frac{p+1}{2}} = a^{\frac{p-1}{2}} \cdot a \equiv \left(\frac{a}{p}\right) \cdot a \equiv a\ (mod\ p)$, presupunând că a este rest pătratic modulo p.
Deci, $x \equiv \pm r \equiv \pm a^{\frac{p+1}{4}}$ $(mod\ p)$ sunt rădăcinile pătrate pentru a modulo p.

Astfel, algoritmul precedent capătă următoarea formă simplificată:

Algoritm 13.1.2 (Rădăcini pătrate mod p prim, $p \equiv 3\ (mod\ 4)$)
INPUT: numerele naturale $p \equiv 3\ (mod\ 4)$, prim şi a un rest pătratic modulo p.
OUTPUT: Două rădăcini pătrate ale lui a mod p.

1. *Calculează $r \equiv a^{\frac{p+1}{4}}$ $(mod\ p)$ folosind algoritmul 3.1.1.*
2. *Returnează $r, -r$.*

Dacă particularizăm algoritmul 13.1.1 pentru cazul $s = 2$ şi ne folosim de faptul că 2 este non-rest pătratic modulo un număr prim $p \equiv 5 \ (mod\ 8)$, obţinem o formă simplificată, şi anume:

Algoritm 13.1.3 (Rădăcini pătrate mod $p \equiv 5 \ (mod\ 8)$)
INPUT: numerele naturale $p \equiv 5 \ (mod\ 8)$, prim şi a un rest pătratic modulo p.
OUTPUT: Două rădăcini pătrate ale lui a mod p.

1. *Calculează $d \leftarrow a^{\frac{p-1}{4}} \ (mod\ p)$, folosind algoritmul 3.1.1.*
2. *Dacă $d = 1$, calculează $r \leftarrow a^{(p+3)/8} \ (mod\ p)$.*
3. *Dacă $d = p - 1$, calculează $r \leftarrow 2a(4a)^{(p-5)/8} \ (mod\ p)$.*
4. *Returnează $r, -r$.*

Dacă $p - 1 = 2^s t$ cu s mare, este preferabil să se folosească un alt algoritm, în locul celui iniţial. Acesta utilizează polinoame cu coeficienţi întregi modulo p. Cei interesaţi pot găsi mai multe date referitoare la această problemă, consultând [15].

13.2 Rădăcini pătrate mod n

Vom studia doar cazul în care n este produs de două numere prime impare diferite p şi q. Pentru a găsi rădăcinile pătrate ale lui a modulo $n = pq$, aflăm mai întâi rădăcinile pătrate ale lui a modulo p şi modulo q, după care aplicăm teorema chinezească a resturilor pentru a afla rădăcinile pătrate modulo n ale lui a.

Astfel, presupunem că $1 \leq a \leq n - 1$ este un rest pătratic modulo n, adică congruenţa

$$x^2 \equiv a \ (mod\ n) \tag{13.1}$$

are soluţii. Fie x_0 o soluţie a acesteia. Arătăm că ea are exact 4 soluţii necongruente modulo n. Pentru aceasta, fie

$$x_1 \equiv x_0 \ (mod\ p),\ 0 < x_1 < p \tag{13.2}$$

$$x_2 \equiv x_0 \ (mod\ q),\ 0 < x_2 < q \tag{13.3}$$

Atunci, congruenţa

$$x^2 \equiv a \ (mod\ p) \tag{13.4}$$

are exact două soluţii necongruente, pe x_1 şi $p - x_1$ iar

$$x^2 \equiv a \ (mod\ q) \tag{13.5}$$

pe x_2 şi $q - x_2$.

Congruenţa (13.1) este echivalentă cu sistemul format din congruenţele (13.4) şi (13.5).

Astfel, folosind teorema chinezească a resturilor, există exact 4 soluţii necongruente modulo $n = pq$, ce se obţin rezolvând următoarele sisteme:

$$(S_1) \quad \begin{cases} x \equiv x_1 \ (mod\ p) \\ x \equiv x_2 \ (mod\ q) \end{cases} \qquad (S_2) \quad \begin{cases} x \equiv x_1 \ (mod\ p) \\ x \equiv q - x_2 \ (mod\ q) \end{cases}$$

$$(S_3) \quad \begin{cases} x \equiv p - x_1 \ (mod\ p) \\ x \equiv x_2 \ (mod\ q) \end{cases} \qquad (S_4) \quad \begin{cases} x \equiv p - x_1 \ (mod\ p) \\ x \equiv q - x_2 \ (mod\ q) \end{cases}$$

Dacă notăm soluţia sistemului (S_1) cu x şi soluţia lui (S_2) cu y, atunci soluţia sistemului (S_3) este $n - y$ iar cea a ultimului sistem este $n - x$, după cum se poate verifica uşor.

Algoritmul următor realizează cele prezentate:

Algoritm 13.2.1 (Rădăcini pătrate mod $n = pq$)
INPUT: numerele naturale p, q prime impare cu $n = pq$ şi a un rest pătratic modulo n.
OUTPUT: Cele patru rădăcini pătrate ale lui a mod n.

1. *Folosind algoritmul 13.1.1, determină cele două rădăcini pătrate $\pm r$ ale lui a mod p.*
2. *Folosind algoritmul 13.1.1, determină cele două rădăcini pătrate $\pm s$ ale lui a mod q.*
3. *Foloseşte algoritmul 1.2.2 pentru a determina c, d astfel ca $cp + dq = 1$.*
4. *Pune $x \leftarrow rdq + scp \ (mod\ n)$, $y \leftarrow rdq - scp \ (mod\ n)$.*
5. *Returnează $\pm x \ (mod\ n),\ \pm y \ (mod\ n)$.*

Dacă considerăm acum cazul particular

$$n = pq,\ p \equiv q \equiv\ 3 \ (mod\ 4),$$

congruenţa (13.4) are soluţiile $\pm x_1 \equiv \pm a^{\frac{p+1}{4}} \ (mod\ p)$, după cum am văzut mai înainte, când modulul era prim.
La fel, (13.5) va avea soluţiile $\pm x_2 \equiv \pm a^{\frac{q+1}{4}} \ (mod\ q)$.

Pentru a exemplifica cele prezentate, să considerăm un caz numeric unde $a = 860$, $n = 11021 = 103 \cdot 107$.
Să rezolvăm congruenţa $x^2 \equiv 860 \ (mod\ 11021)$. Ea este echivalentă cu sistemul:

$$\begin{cases} x^2 \equiv 860 \equiv 36 \ (mod\ 103) \\ x^2 \equiv 860 \equiv 4 \ (mod\ 107) \end{cases}$$

Soluţiile primei congruenţe din sistem sunt

$$\pm 36^{\frac{103+1}{4}} = \pm 36^{26} \equiv \pm 6 \ (mod\ 103)$$

iar pentru a doua congruenţă, soluţiile sunt

$$\pm 4^{\frac{107+1}{4}} = \pm 4^{27} \equiv \pm 2 \ (mod\ 107).$$

Aplicând acum teorema chinezească a resturilor, obţinem pentru congruenţa iniţială soluţiile:
$x \equiv \pm 212 \ (mod\ 11021)$ şi $x \equiv \pm 109 \ (mod\ 11021)$.

În final, dăm un exemplu de metodă *flip coin*.

Presupunem că Alice şi Bob comunică electronic.

1. Alice alege două numere prime mari p şi q cu $p \equiv q \equiv 3 \ (mod\ 4)$, calculează $n = pq$ şi trimite rezultatul n lui Bob.

2. Bob alege aleator un număr $x < n$, calculează $x^2 \equiv a \ (mod\ n)$ şi trimite numărul $a < n$ lui Alice.

3. Alice găseşte cele 4 soluţii necongruente $x, y, n - y, n - x$ ale congruenţei $x^2 \equiv a \ (mod\ n)$ şi trimite una dintre ele lui Bob.

4. Dacă Bob primeşte y sau $n - y$ el va putea descompune în factori numărul n astfel:
$x + y \equiv 2x_1 \neq 1 \ (mod\ p)$ şi $x + y \equiv 0 \ (mod\ q)$, de unde, $(x + y, n) = q$.
În mod analog, pentru cealaltă situaţie se obţine $(x + (n - y), n) = p$.
Dacă Bob primeşte x sau $n - x$, el nu poate factoriza în timp util pe n.

În consecinţă, Bob câştigă *flip coin* dacă poate factoriza pe n şi pierde, în caz contrar. Ţinând cont de observaţiile anterioare, există şanse egale ca Bob să primească o soluţie a congruenţei care să-l ajute să factorizeze rapid pe n, sau o soluţie care să nu îi fie utilă. Deci, această metodă *flip coin* este corectă.

Exerciţii propuse

1. Fie $p = 2081$. Notăm cu b cel mai mic non-rest pătratic modulo p. Aflaţi b şi, folosind metoda prezentată, determinaţi o rădăcină pătrată a lui 302 modulo p.

2. Determinaţi o rădăcină pătrată a lui 55 modulo 89.

3. Rezolvaţi următoarele congruenţe:

i) $x^2 \equiv 1 \ (mod\ 15)$.

ii) $x^2 \equiv 31 \ (mod\ 75)$.

iii) $x^2 \equiv 16 \ (mod\ 105)$.

ANEXA A

Numere prime Mersene

Tabel A.1: Numerele prime Mersene cunoscute.

nr.	p	$cifre M_p$	*Observaţii*
1	2	1	*antichitate*
2	3	1	*antichitate*
3	5	2	*antichitate*
4	7	3	*antichitate*
5	13	4	*Reguis, Cataldi* (1461)
6	17	6	*Cataldi* (1588)
7	19	6	*Cataldi* (1588)
8	31	10	*Euler* (1750)
9	61	19	*Pervouchine, Seelhoff* (1883)
10	89	27	*Powers* (1911)
11	107	33	*Powers* (1913)
12	127	39	*Lucas* (1876)
13	521	157	*Robinson* (1952)

$nr.$	p	$cifre M_p$	$Observaţii$
14	607	183	*Robinson* (1952)
15	1279	386	*Robinson* (1952)
16	2203	664	*Robinson* (1952)
17	2281	687	*Robinson* (1952)
18	3217	969	*Riesel* (1957)
19	4253	1281	*Hurwitz* (1961)
20	4423	1332	*Hurwitz* (1961)
21	9689	2917	*Gillies* (1963)
22	9941	2993	*Gillies* (1963)
23	11213	3376	*Gillies* (1963)
24	19937	6002	*Tuckerman* (1971)
25	21701	6533	*Noll, Nickel* (1978)
26	23209	6987	*Noll* (1979)
27	44497	13395	*Nelson, Slowinski* (1979)
28	86243	25962	*Slowinski* (1982)
29	110503	33265	*Colquitt, Welsh* (1988)
30	132049	39751	*Slowinski* (1983)
31	216091	65050	*Slowinski* (1985)
32	756839	227832	*Slowinski, Gage* (1992)
33	859433	258716	*Slowinski, Gage* (1994)
34	1257787	378632	*Slowinski, Gage* (1996)
35	1398269	420921	*Armengaud/GIMPS* (1996)
36	2976221	895832	*Spence/GIMPS* (1997)
37	3021377	909526	*Clarkson/GIMPS* (1998)
38	6972593	2098960	*Hajratwala/GIMPS* (1999)
39	13466917	4053946	*Cameron/GIMPS* (2001)
40?	20996011	6320430	*Shafer/GIMPS* (2003)
41?	24036583	7235733	*Findley/GIMPS* (2004)
42?	25964951	7816230	*Nowak/GIMPS* (2005)

ANEXA B

Numere pseudoprime

Tabel B.1: Cele mai mici numere pseudoprime n cu primele 100 de baze b.

b	n	b	n	b	n	b	n	b	n
2	341	15	341	28	45	41	105	54	55
3	91	16	51	29	35	42	205	55	63
4	15	17	45	30	49	43	77	56	57
5	124	18	25	31	49	44	45	57	65
6	35	19	45	32	33	45	76	58	133
7	25	20	21	33	85	46	133	59	87
8	9	21	55	34	35	47	65	60	341
9	28	22	69	35	51	48	49	61	91
10	33	23	33	36	91	49	66	62	63
11	15	24	25	37	45	50	51	63	341
12	65	25	28	38	39	51	65	64	65
13	21	26	27	39	95	52	85	65	112
14	15	27	65	40	91	53	65	66	91

b	n	b	n	b	n	b	n	b	n
67	85	74	75	81	85	88	91	95	141
68	69	75	91	82	91	89	99	96	133
69	85	76	77	83	105	90	91	97	105
70	169	77	247	84	85	91	115	98	99
71	105	78	341	85	129	92	93	99	145
72	85	79	91	86	87	93	301	100	153
73	111	80	81	87	91	94	95		

Tabel B.2: Numerele pseudoprime cu baza 2 şi numerele Carmichael (cele boldate) mai mici dacât 41041.

a	n	a	n	a	n	a	n
1	341	14	4369	27	13741	40	**29341**
2	**561**	15	4371	28	13747	41	30121
3	645	16	4681	29	13981	42	30889
4	**1105**	17	5461	30	14491	43	31417
5	1387	18	**6601**	31	15709	44	31609
6	**1729**	19	7957	32	**15841**	45	31621
7	1905	20	8321	33	16705	46	33153
8	2047	21	8481	34	18705	47	34945
9	**2465**	22	**8911**	35	18721	48	35333
10	2701	23	10261	36	19951	49	39865
11	**2821**	24	**10585**	37	23001	50	**41041**
12	3277	25	11305	38	23377		
13	4033	26	12801	39	25761		

Bibliografie

[1] Alford, W.R., Granville, A., Pomerance, C., *There are Infinitely Many Carmichael Numbers*, Annals Math., 140 (1994), 703-722.

[2] Albu, T., Ion, I.D., *Capitole speciale de teoria numerelor,* Editura Academiei, Bucureşti, 1984.

[3] Albu, T., Ion, I.D., *Itinerar elementar în algebra superioară*, Editura All, 1997.

[4] Bobancu, V., *Caleidoscop matematic*, Editura Albatros, Bucureşti, 1979.

[5] Buşneag, D., Boboc, F., Piciu, D., *Aritmetică şi teoria numerelor*, Editura Universitaria, Craiova, 1999.

[6] Cohen, H., *A Course in Computational Algebric Number Theory*, Springer-Verlag, 1995.

[7] Cucurezeanu, I., *Probleme de aritmetică şi teoria numerelor*, Editura Tehnică, Bucureşti, 1976.

[8] Depman, J., *Din istoria matematicii*, Editura Cartea Rusă, Bucureşti, 1952.

[9] Dincă, Al., *Lecţii de algebră*, Editura Universitaria, Craiova, 2000.

[10] Kiran, K., *Is this number prime?*, Berkeley Math Circle, November, 2002.

[11] Koblitz, N., *Algebric Aspects of Cryptography*, Springer-Verlag, Berlin, 1988.

[12] Koblitz, N., *A Course in Number Theory and Cryptography*, ed. a II-a, Springer-Verlag, Berlin, 1994.

[13] Knuth, D.E., *The Art of Computer Programming*, vol.I, ed. a II-a, Addison-Wesley, 1973.

[14] Lenstra, A.K., Lenstra, H.W. jr., Manasse, M.S., Pollard, J.M., *The Number Field Sieve*, The Developement of the Number Field Sieve, Springer-Verlag, 1993.

[15] Menezes, A., Oorschot, P., Vanstone, S., *Handbook of Applied Cryptography*, CRC Press, Boca Raton, Florida, 1998.

[16] Năstăsescu, C., Niţă, C., Vraciu, C., *Aritmetică şi algebră*, Editura Didactică şi Pedagogică, Bucureşti, 1993.

[17] Pomerance, C., *The Quadratic sieve factoring algorithm*, Advances in Cryptology, Proceedings of Eurocrypt 84, Paris, 1984, Lectures notes in Computer Sci, 209 (1985), 169-182.

[18] Popovici, C.P., *Teoria numerelor*, Editura Didactică şi Pedagogică, Bucureşti, 1973.

[19] Robin, G., *Algorithmique et Criptographie*, Mathematique et Applications, Ellipses, 1991.

[20] Rosen, K.H., *Elementary Number Theory and Cryptography*, Addison-Wesley, 1993.

[21] Sierpinski, W., *Elementary Theory of Numbers*, Polski Academic Nauk, Warsaw, 1964.

[22] Sierpinski. W., *Ce ştim şi ce nu ştim despre numerele prime*, Editura Ştiinţifică, Bucureşti, 1966.

[23] Stillwell, J., *Elements of Number Theory*, Springer-Verlag, New-York, 2003.

[24] Stinson, D.R., *Cryptography: Theory and Practice*, CRC Press, Boca Raton, Florida, 1995.

[25] Yan Song, Y., *Number Theory for Computing*, ed. a II-a, Springer-Verlag, 2002.

Index