Slobodan Vujoševic

Teorija brojeva i kriptografija

Iz nepregledne literature iz teorije brojeva i aritmetike, kao veoma sadržajnu i duhovito napisanu monografiju, koja uglavnom pokriva i delom dopunjava materiju našeg izlaganja, čitaocima preporučujemo knjigu Alana Bejkera *A concise introduction to the theory of numbers,* Cambridge University Press, 1986.

Euklidova teorema

Najčešće se o Euklidovim Elementima govori kao o prvom pokušaju da se na deduktivan način zasnuje geometrija. Manje je poznato da Elementi sadrže i razvijene ideje aritmetike. One se sistematski izlažu u tri, od ukupno trinaest, knjiga Elemenata. Tako je u devetoj knjizi, kao poslednja u oblasti teorije brojeva, dokazana i jedna teorema o savršenim brojevima.

Euklidova teorema. Za svako $n > 1$, ako je $2^n - 1$ prost broj, onda je $2^{n-1}(2^n - 1)$ savršen broj.

Pritom, *savršen broj* jednak je sumi svojih delitelja različitih od njega samog. Kako se veruje, u trećem veku pre Hrista, Euklid je znao nekoliko prvih savršenih brojeva. To su brojevi $p_1 = 6$, $p_2 = 28$, $p_3 = 496$ i $p_4 = 8128$.

U srednjem veku verovalo se da p_n ima n cifara. To nije tačno, budući da je francuski matematičar, Pjer Ferma (1601. – 1665.), izračunao da je $p_5 = 33550336$.

Takodje, verovalo se da savršeni brojevi alternativno završavaju ciframa 6, odnosno 8, ali ni to nije tačno, budući da je $p_6 = 8585896056$.

Medjutim, tačno je da decimalni zapis svakog parnog savršenog broja završava ili cifrom 6 ili cifrom 8. To sledi iz konverzije Euklidove teoreme koju je dokazao Leonard Ojler (1707. – 1783.)

Ojlerova teorema. Svaki paran savršen broj ima oblik $2^{n-1}(2^n - 1)$, za neki prost broj $2^n - 1$ i neko $n > 1$.

Ako pretpostavimo Ojlerovu teoremu, nju ćemo dokazati nešto kasnije, onda svaki paran savršen broj ima oblik $2^{n-1}(2^n - 1)$, gde je $2^n - 1$ prost broj. Ali, ako je $2^n - 1$ prost broj, onda je i n prost broj, pa n može biti oblika ili $4k + 1$ ili $4k + 3$. Ako je $n = 4k + 1$, cifra 6 je poslednja cifra broja 2^{4k}, a cifra 1 broja $2^{4k+1} - 1$, pa poslednja cifra njihovog proizvoda mora biti 6. Ako je $n = 4k + 3$, cifra 4 je poslednja cifra broja 2^{4k+2}, a cifra 7 broja $2^{4k+3} - 1$, pa je poslednja cifra broja $2^{4k+2}(2^{4k+3} - 1)$ jednaka 8.

Veruje se da savršenih brojeva ima beskonačno mnogo, ali dokaz za tu tvrdnju nemamo. Ne zna se da li uopšte postoji neparan savršen broj?

Kako smo već napomenuli, ako je $2^p - 1$ prost broj, onda je i p prost broj, ali obratno ne važi. Brojevi oblika $m_p = 2^p - 1$, gde je p prost broj, su *Mersenovi brojevi.* Ime su dobili po francuskom matematičaru Marenu Mersenu (1588. – 1648.). Broj $m_{44\,497}$ je dvadesetsedmi Mersenov prost broj. U dekadnom zapisu ima 13 395 cifara. Ne zna se da li ima beskonačno mnogo prostih, a takođe ni da li ima beskonačno mnogo složenih Mersenovih brojeva?

Postupak deljenja

Prirodni brojevi su $1, 2, 3, \ldots$. Neki matematičari, naročito logičari, kao prirodan broj podrazumevaju i nulu. Nećemo se upuštati u raspravu o opravdanosti takvog shvatanja, niti ćemo otvarati filosofska pitanja koja se odnose na egzistenciju skupa prirodnih brojeva. Biće dovoljno da pretpostavimo Peanove akiome sa definicijom sabiranja, množenja i standardnog poretka u kome svaki neprazan skup ima najmanji element.

Celi brojevi su $\ldots - 2, -1, 0, 1, 2, \ldots$, sa standardno definisanim operacijama sabiranja i množenja, koje su saglasne navedenom poretku.

Ako su a i b prirodni brojevi, b *deli* a ako postoji prirodan broj c za koji je $a = bc$. Deljivost broja a brojem b označavamo sa $b|a$.

Relacija $b|a$ je refleksivna, $a|a$, tranzitivna, iz $a|b$ i $b|c$ sledi $a|c$ i antisimetrična, odnosno, ako $b|a$ i $a|b$, onda $a = b$. Ako $b|a$, onda $b \leq a$, pa svaki prirodan broj ima konačno mnogo delitelja.

Pojam deljivosti se prirodno proširuje na cele brojeve, uz pretpostavku da je $b \neq 0$.

Prirodni broj različit od 1 je *prost* ako su njegovi jedini delitelji 1 i on sam. Prvih nekoliko prostih brojeva su $2, 3, 5, 7, 11, \ldots$.

Teorema. Za proizvoljne cele brojeve a i $b > 0$, postoje celi brojevi q i r za koje je $a = bq + r$, $0 \leq r < b$.

Dokaz. Ako je bq najveći umnožak od b koji ne prevazilazi a, broj $r = a - bq$ nije negativan, a kako je $b(q + 1) > a$, to mora biti $r < b$.

Isto važi i za svaki ceo broj $b \neq 0$, uz prirodno ograničenje $r < |b|$. Broj q je količnik, a r ostatak u postupku deljenja broja a sa b.

Najveći delitelj

Prirodan broj d je *najveći delitelj* prirodnih brojeva a i b ako svaki delitelj brojeva a i b deli d.

Teorema. Za svaka dva prirodna broja, postoji njihov najveći delitelj.

Dokaz. Ukoliko uopšte postoji, najveći delitelj brojeva a i b je jedinstven. Naime, ako su d_1 i d_2 najveći delitelji, onda $d_1|d_2$ i $d_2|d_1$, pa dakle $d_1 = d_2$. Razmotrimo skup prirodnih brojeva oblika $ax + by \geq 1$, gde su x i y celi brojevi. Kako sadrži brojeve a i b, taj skup nije prazan, pa ima najmanji element d. Svaki delitelj brojeva a i b takodje deli d, budući da je $d = ax + by$, za neke cele brojeve x i y. Kako je $a = dq + r$, $0 \leq r < d$, gde su q i r celi brojevi, dobija se da je $r = a(1 - qx) + b(-qy)$. Kako je d minimalan, mora biti $r = 0$, pa $d|a$ i slično $d|b$.

Najveći delitelj prirodnih brojeva a i b označavamo sa (a, b). Ako je $(a, b) = 1$, brojevi a i b su *uzajamno prosti.*

Teorema. Za svako $n \geq 1$, jednačina $ax + by = n$ ima celobrojna rešenja ako i samo ako $(a, b)|n$.

Otuda sledi da, ako su brojevi a i b uzajamno prosti, jednačina $ax+by = n$ ima rešenje, za svako $n \geq 1$.

Pojam najvećeg delitelja se prirodno proširuje na više od dva broja. Lako se pokazuje da proizvoljni brojevi $a_1, \ldots, a_n$ imaju najveći delitelj $d = (a_1, \ldots, a_n)$ takav da je $d = a_1x_1 + \ldots + a_nx_n$ za neke cele brojeve $x_1, \ldots, x_n$.

Teorema. Ako su brojevi $a_1, \ldots, a_n$, $n \geq 2$, uzajamno prosti, jednačina $a_1x_1 + \ldots + a_nx_n = k$ ima rešenje, za svaki prirodan broj k

Euklidov algoritam

Euklid je definisao i metod za odredjivanje najvećeg delitelja. Prema postupku deljenja, ako su a i b prirodni brojevi, postoje q_0 i r_1 takvi da

$$a = bq_0 + r_1, \ 0 \leq r_1 < b.$$

Ako $r_1 \neq 0$, postoje q_1, r_2 takvi da

$$b = r_1q_1 + r_2, \ 0 \leq r_2 < r_1.$$

Takodje, ako $r_2 \neq 0$, postoje q_2, r_3 takvi da

$$r_1 = r_2q_2 + r_3, \ 0 \leq r_3 < r_2.$$

Nastavljajući ovaj postupak, dobija se strogo opadajući niz prirodnih brojeva $r_1, r_2, \ldots$, pa, za neki prirodan broj $k \geq 1$, mora biti $r_{k+1} = 0$, odnosno, mora biti $r_{k-1} = r_kq_k$.

Vraćajući se unazad, lako se proverava da svaki delitelj brojeva a i b takodje deli $r_1, \ldots, r_k$, odnosno da je $(a, b) = r_k$.

Izloženi postupak je *Euklidov algoritam.* On potvrdjuje postojanje celih brojeva x i y koji zadovoljavaju jednačinu $(a, b) = ax + by$ i omogućava da se takvi brojevi eksplicitno odrede.

Teorema. Mersenovi brojevi su uzajamno prosti.

Dokaz. Neka je $S_n = 2^n - 1$, za svaki prirodan broj n. Tvrdimo da je $(S_m, S_m) = S_{(m,n)}$, za sve prirodne brojeve m i n. Ako je $r_{i-1} = r_iq_{i+1} + r_{i+1}$ korak Euklidovog algoritma za najveći delitelj (m, n), neposredno se proverava da postoji prirodan broj Q_{i+2} takav da važi jednakost $S_{r_{i-1}} = S_{r_i}Q_{i+1} +$

$S_{r_{i+1}}$, što je odgovarajući korak Euklidovog algoritma za najveći delitelj (S_m, S_n). Dakle, ako je $r_{k-1} = r_k q_{k+1}$, onda je $r_k = (m, n)$, što znači da je $S_{r_k} = (S_m, S_n)$, odnosno, $(S_m, S_n) = S_{(m,n)}$. Otuda sledi da su Mersenovi brojevi uzajamno prosti.

Osnovna teorema aritmetike

Teorema. Svaki prirodan broj $n > 1$ ima jedinstvenu reprezentaciju

$$n = p_1^{a_1} \dots p_k^{a_k},$$

za neke $a_1, \dots, a_k > 0$ i proste $p_1 < \dots < p_k$.

Dokaz. Ako je $n > 1$, njegov najmanji delitelj $q_1 > 1$ je sigurno prost. Slično, ako je $n \neq q_1$, postoji najmanji prost $q_2 > 1$ koji deli n/q_1, a ako je $n \neq q_1 q_2$, onda postoji najmanji prost $q_3 > 1$ koji deli $n/q_1 q_2$, itd. Posle konačnog broja koraka dobija se $n = q_1 \dots q_m$, pa se grupisanjem dobija $n = p_1^{a_1} \dots p_k^{a_k}$, za neke $a_1, \dots, a_k > 0$ i proste brojeve $p_1 < \dots < p_k$.

Jedinstvenost ove reprezentacije podrazumeva da ako je $n = q_1^{b_1} \dots q_m^{b_m}$, za neke $b_1, \dots, b_m > 0$ i proste brojeve $q_1 < \dots < q_m$, onda je $k = m$, $p_i = q_i$ i $a_i = b_i$, za sve $i = 1, \dots, k$. Ona neposredno sledi iz sledećih osobina prirodnih brojeva a, b i c.

Ako $(a, c) = 1$ i $(b, c) = 1$ onda $(ab, c) = 1$.

Ako $c|ab$ i $(a, c) = 1$, onda $c|b$.

Otuda sledi da ako prost broj p deli $a_1 \cdots a_n$, onda p deli bar jedan od brojeva $a_1, \dots, a_n$. To znači da ako osim navedene reprezentacije postoji i neka druga $n = q_1^{b_1} \dots q_m^{b_m}$, onda je $p_1 = q_1$ itd, tj. $k = m$, $p_i = q_i$ i $a_i = b_i$.

Dokaz Euklidove teoreme. Svoju tvrdnju Euklid obrazlaže na sledeći način. Prema osnovnoj teoremi aritmetike, ako je $2^n - 1$ prost broj, svi delitelji broja $2^{n-1}(2^n - 1)$ različiti od njega samog su oblika 2^k, gde je $k = 0, \dots, n-1$, ili oblika $2^k(2^n - 1)$, gde je $k = 0, \dots, n-2$, pa kada se oni saberu dobija se taj isti broj.

Dokaz Ojlerove teoreme. Treba dokazati da svaki paran savršen broj ima oblik $2^{n-1}(2^n - 1)$, za neki prost broj oblika $2^n - 1$. Neka je m paran savršen broj, onda je $m = 2^{n-1}p$, za neko $n > 1$ i neki neparan broj p. Neka je σ suma pozitivnih delitelja broja p. Kako pozitivni delitelji broja m uključuju sve pozitivne delitelje broja p i njihove umnoške redom sa $2, \dots 2^{n-1}$ i kako je m savršen broj

$$m = 2^{n-1}p = (1 + 2 + \dots + 2^{n-1})\sigma - m.$$

Otuda sledi da je $\sigma = p + p/(2^n - 1)$, pa kako je σ ceo broj, to $(2^n - 1)|p$, a jedini delitelji broja p su $p/(2^n-1)$ i sam p. Dakle, p je prost i $p/(2^n-1) = 1$, odnosno, $p = 2^n - 1$.

Teorema. Jednačina $x^2 - 2y^2 = 0$ nema celobrojno rešenje različito od trivijalnog $x = 0$ i $y = 0$.

Dokaz. Prema osnovnoj teoremi, broj $x^2 \neq 0$ ima paran, a broj $2y^2 \neq 0$ neparan broj prostih faktora.

Prosti brojevi

Pred kraj drugog milenijuma, madjarski matematičar Pal Erdeš (1913.–1996.) pokušao je da sastavi neku vrstu matematičkog jevandjelja, koje obuhvata božanske matematičke rezultate u koje se veruje i koji se poštuju jednako kao u Sveto Pismo. Kako je sam Erdeš napisao, takva knjiga mora početi Euklidovim dokazom o beskonačnosti skupa prostih brojeva.

Teorema. Ima beskonačno mnogo prostih brojeva.

Euklidov Dokaz. Zaista, ako je $p_1, \ldots, p_n$ bilo koji konačan skup prostih brojeva, onda je broj $p_1 \cdots p_n + 1$ deljiv prostim brojem različitim od svih prostih brojeva $p_1, \ldots, p_n$.

Dokaz sredstvima matematičke analize. Neka je $\pi(x)$ broj prostih brojeva koji nisu veći od realnog broja x. Dokazaćemo da je $\ln x \leq \pi(x) + 1$, za svaki realan broj $x \geq 2$. Kako funkcija $\ln x$ nije ograničena, to će značiti da ima beskonačno mnogo prostih brojeva.

Prvi prost broj je $p_1 = 2$, a sa p_{n+1} označavamo najmanji prost broj veći od p_n, $n \geq 1$.

Neka je $n \leq x < n + 1$. Gornja integralna suma funkcije $f(t) = 1/t$, za podelu intervala $[1, x]$ određenu tačkama $1, 2, \ldots, n, x$, veća je od integrala $\int_1^x 1/t dt = \ln x$, pa važi nejednakost

$$\ln x \leq 1 + \tfrac{1}{2} + \cdots \tfrac{1}{n} \leq \sum \tfrac{1}{m}.$$

Pritom, u sumi $\sum 1/m$ sumiramo po svim prirodnim brojevima m koji sadrže prost faktor $p \leq x$. Kako se svaki takav m može jedinstveno predstaviti u obliku $\prod\limits_{p \leq x} p^{a_p}$, to važi jednakost

$$\sum \tfrac{1}{m} = \prod_{p \leq x} \left(\sum_{k \geq 0} \tfrac{1}{p^k} \right).$$

Unutrašnja suma u poslednjem proizvodu je geometrijska progresija sa količnikom $1/p$, pa važi sledeća nejednakost

$$\ln x \leq \prod_{p \leq x} \tfrac{p}{p-1} = \prod_{k=1}^{\pi(x)} \tfrac{p_k}{p_k - 1}.$$

Kako je $p_k \geq k+1$, mora biti

$$\tfrac{p_k}{p_k-1} = 1 + \tfrac{1}{p_k-1} \leq 1 + \tfrac{1}{k} = \tfrac{k+1}{k},$$

pa se otuda konačno dobija

$$\ln x \leq \prod_{k=1}^{\pi(x)} \tfrac{k+1}{k} = \pi(x) + 1.$$

Euklidov dokaz sugeriše prvu ocenu broja p_n, za koju je verovatno znao i sam Euklid.

Teorema. Za svaki prirodan broj n, $p_{n+1} < 2^{2^n}$.

Dokaz. Indukcijom po $n \geq 1$. Kako je $p_2 < 3 < 2^2$, pretpostavimo da teorema važi za sve brojeve manje od n. Kako broj p_{n+1} nije veći od $p_1 \cdots p_n + 1$, to je

$$p_{n+1} \leq p_1 p_2 \cdots p_n + 1 < 2^{1+2+\cdots+2^{n-1}} + 1 < 2^{2^n}.$$

Eratostenovo sito

Prvi metod za pronalaženje prostih brojeva manjih od datog prirodnog broja definisao je grčki matematičar Eratosten, za koga se veruje da je živeo između 276. i 194. godine pre Hrista. Iako jednostavna, ideja *Eratostenovog sita* prisutna je u najdubljim rezultatima matematike.

Prirodni brojevi $\leq n$ seju se Eratostenovim sitom sve dok u situ ne ostanu samo prosti brojevi. U spisku prirodnih brojeva $2, 3, \ldots, n$, prvi broj je $p_1 = 2$, on je prost i precrtajmo sve parne složene brojeve. U preostalom spisku, prvi neprecrtani broj je $p_2 = 3$, on je prost i precrtajmo sve složene brojeve koji su deljivi sa 3. U preostalom spisku, prvi neprecrtani broj je $p_3 = 5$, on je prost itd. u preostalom spisku, prvi neprecrtani broj posle p_k je prost broj p_{k+1}.

Kako svaki prost delitelj prirodnog broja n nije veći od $\sqrt{n}$, postupak se završava kada se odredi prvi $p_k \geq \sqrt{n}$. Svi preostali neprecrtani brojevi u spisku su prosti.

Pre nego što ilustujemo primenu Eratostenovog sita u proceni broja $\pi(x)$ prostih brojeva manjih od realnog broja x, dokazaćemo *Ojlerovu nejednakost.*

Ako je x realan broj, sa $[x]$ označavamo najveći ceo broj $\leq x$, a sa $\{x\}$ razliku $x - [x]$.

Ojlerova nejednakost. Za svaki realan broj $x \geq 2$,

$$\ln x < \prod_{p \leq x} \left(1 - \tfrac{1}{p}\right)^{-1}.$$

Dokaz. Neka je $p(x) = \prod\limits_{p \leq x} \left(1 - \frac{1}{p}\right)^{-1}$, za svaki realan broj $x \geq 2$.

Za svako $m \geq 1$, ako je $0 < t < 1$, važi nejednakost

$$\tfrac{1}{1-t} = \sum_{k=0}^{\infty} t^k > \sum_{k=0}^{m} t^k,$$

pa ako je $t = 1/p$, dobijamo nejednakost

$$\left(1 - \tfrac{1}{p}\right)^{-1} > 1 + \tfrac{1}{p} + \cdots + \tfrac{1}{p^m}.$$

Dakle, za svako $m \geq 1$,

$$p(x) > \prod_{p \leq x} \left(1 + \tfrac{1}{p} + \cdots + \tfrac{1}{p^m}\right),$$

pa se posle množenja na desnoj strani dobija suma oblika $\sum\limits_k 1/k$. Ako biramo m tako da je $2^{m+1} > x$, prema osnovnoj teoremi aritmetike, u tu sumu ulaze svi sabirci za koje je $1 \leq k \leq [x]$ i moguće neki drugi pozitivni sabirci. Otuda sledi da je

$$p(x) > \sum_{k=1}^{[x]} \tfrac{1}{k}.$$

Koristeći nejednakost $\ln(1+t) < t$, $0 < t \leq 1$, za $t = 1/k$, dobijamo da je $\ln(k+1) - \ln k = \ln(1 + 1/k) < 1/k$, za sve $k \geq 1$. Otuda se konačno dobija da je

$$p(x) > \sum_{k=1}^{[x]} \tfrac{1}{k} > \ln([x] + 1) > \ln x.$$

Ojlerova teorema. $\pi(x)/x \to 0$ *kada* $x \to \infty$.

Dokaz. Napravićemo Eratostenovo sito. Za svaki realan broj x i svako $k \geq 0$, neka je $s(x,r)$ broj prirodnih brojeva $\leq x$ koji nisu deljivi brojevima $p_1, \ldots, p_r$. Pritom, $s(x,0)$ je broj prirodnih brojeva $\leq x$.

Svi prirodni brojevi $\leq x$ koji nisu deljivi brojevima $p_1, \ldots, p_{r-1}$ dele se u dve klase: na brojeve koji nisu deljivi sa p_r i brojeve koji jesu deljivi sa p_r. Brojeva iz prve klase ima $s(x,r)$, a svaki broj iz druge klase predstavljiv je u obliku $n = p_r m$, gde je $m \leq x/p_r$ i p_i ne deli m, za sve $i = 1, \ldots, r-1$. To znači da druga klasa sadrži $s(x/p_r, r-1)$ brojeva i pritom, $s(x, r-1) = s(x,r) + s(x/p_r, r-1)$, odnosno

$$s(x,r) = s(x,r-1) - s(x/p_r, r-1).$$

Poslednja jednakost važi i za $r = 1$, pa se indukcijom dobija

$$\begin{aligned} s(x,r) &= s(x,0) - \sum_i s(\tfrac{x}{p_i}, 0) + \sum_{i<j} s(\tfrac{x}{p_i p_j}, 0) \\ &- \sum_{i<j<k} s(\tfrac{x}{p_i p_j p_k}, 0) + \cdots + (-1)^r s(\tfrac{x}{p_1 \cdots p_r}, 0). \end{aligned}$$

Kako je $s(x,0) = [x]$, prethodna jednakost ima oblik

$$\begin{aligned} s(x,r) &= [x] - \sum_i \left[\frac{x}{p_i}\right] + \sum_{i<j} \left[\frac{x}{p_i p_j}\right] \\ &- \sum_{i<j<k} \left[\frac{x}{p_i p_j p_k}\right] + \cdots + (-1)^r \left[\frac{x}{p_1 \cdots p_r}\right]. \end{aligned}$$

Ako se u izrazu za $s(x,r)$ zanemare celobrojne vrednosti, pravi se greška manja od jedan u svakom sabirku, pa kako tih sabiraka ima 2^r, ukupna greška pri takvom zanemarivanju je upravo 2^r, pa dakle važi nejednakost

$$\begin{aligned} s(x,r) &< 2^r + x - \sum_i \frac{x}{p_i} + \sum_{i<j} \frac{x}{p_i p_j} \\ &- \sum_{i<j<k} \frac{x}{p_i p_j p_k} + \cdots + (-1)^r \frac{x}{p_1 \cdots p_r}. \end{aligned}$$

Neka je $2 < y < x$ i $r \geq 1$ takvo da $p_r \leq y < p_{r+1}$. Kako je svaki prost broj ili neki od prvih r prostih brojeva ili pripada skupu prirodnih brojeva koji nisu deljivi sa prvih r prostih brojeva, to važi nejednakost

$$\pi(x) \leq r + s(x,r).$$

Imajući u vidu nejednakost $r + 2^r < 2^{r+1} < 2^{y+1}$, otuda sledi

$$\begin{aligned}\pi(x) &< 2^{y+1} + x - \sum_i \tfrac{x}{p_i} + \sum_{i<j} \tfrac{x}{p_i p_j} - \cdots \\ &< 2^{y+1} + x \prod_{p \le y} \left(1 - \tfrac{1}{p}\right) \\ &< 2^{y+1} + \tfrac{x}{\ln y},\end{aligned}$$

gde smo, u poslednjem koraku, koristili Ojlerovu nejednakost. Otuda sada sledi da je

$$\frac{\pi(x)}{x} < \frac{2^{y+1}}{x} + \frac{1}{\ln y}.$$

Sada biramo y, kao funkciju od x, tako da desna strana nejednakosti teži nuli, kad x teži beskonačnosti, odnosno, ako $y(x)$ biramo tako da $y(x) \to \infty$ i $2^{y(x)+1}/x \to 0$, kada $x \to \infty$, onda $\pi(x)/x \to 0$ kad $x \to \infty$.

Na primer, funkcija $y(x) = \gamma \ln x$, gde je $0 < \gamma < 1/\ln 2$, ima takve osobine.

Raspodela prostih brojeva

Prosti brojevi su sasvim neregularno raspoređeni u skupu prirodnih brojeva. Postoje proizvoljno veliki intervali u kojima uopšte nema prostih brojeva. Na primer, za $k > 1$, između $k!+2$ i $k!+k$ nema prostih brojeva, pa stoga ne postoji jednostavna formula za funkciju $\pi(x)$. Sa druge strane, Euklidov dokaz o beskonačnosti skupa prostih brojeva pokazuje da n-ti prost broj p_n nije veći od $p_1 \cdots p_{n-1} + 1$. Posle Euklida, prvo sistematsko izučavanje raspodele prostih brojeva obavio je Pafnutij Ljvovič Čebišev (1821. – 1894.).

Teorema Čebiševa. Postoje pozitivni realni brojevi a i b takvi da važi nejednakost $a\frac{x}{\ln x} < \pi(x) < b\frac{x}{\ln x}$, za svaki realan broj $x > 2$.

Kako prostih brojeva ima beskonačno mnogo, nema smisla reći da ima više prirodnih nego prostih brojeva. Međutim, kako količnik $\pi(n)/n$ određuje "gustinu" prostih u prvih n brojeva i kako $\pi(n)/n < b/\ln n$ teži nuli kada n raste, može se reći da su prosti brojevi veoma retki među prirodnim brojevima. To ilustruje i sledeća ocena veličine n-tog prostog broja.

Teorema. Postoje pozitivni realni brojevi c i d takvi da važi nejednakost $cn \ln n < p_n < dn \ln n$, za svako $n \ge 2$.

Dokaz. Kako je $p_n \ge n$, mora biti $n = \pi(p_n) < b(p_n/\ln p_n)$, pa se dobija da je $p_n > (n \ln p_n)/b \ge n \ln n/b$.

Sa druge strane $n = \pi(p_n) > ap_n/\ln p_n$. Ako je n veliko i p_n je veliki broj, pa postoji konstanta k takva da za $n > k$, $\ln p_n/\sqrt{p_n} < a$. Otuda, ako je $n > k$,

$$n\frac{\ln p_n}{p_n} > a > \frac{\ln p_n}{\sqrt{p_n}},$$

pa je $n > \sqrt{p_n}$, odnosno, $\ln p_n < 2\ln n$, što znači da je $ap_n < n\ln p_n < 2n\ln n$.

Ako je $d = \max\left\{\frac{2}{a}, \frac{p_2}{2\ln 2}, \ldots, \frac{p_{n-1}}{(n-1)\ln(n-1)}\right\}$, onda je $p_n < dn\ln n$, za $n \geq 2$.

Teorema. Ima beskonačno mnogo prostih brojeva.

Ojlerov Dokaz. Ojler je pokazao da red $\sum\limits_{n=1}^{\infty} 1/p_n$ divergira. Naime, $1/p_n > 1/(dn\ln n)$, za $n > 1$, a iz elementarne analize je poznato da red $\sum\limits_{r=2}^{\infty} 1/(n\ln n)$ divergira.

Dirišleova teorema

Euklidov dokaz o beskonačnosti skupa prostih brojeva se često koristi, sa odgovarajućom modifikacijom, u dokazima beskonačnosti skupova prostih brojeva određenog tipa.

Teorema. Prostih brojeva oblika $4n+3$, gde je n prirodan broj, ima beskonačno mnogo.

Euklidov dokaz. Naime, ako su $p_1 = 3$, $p_2 = 7, \ldots, p_r$ svi takvi brojevi, onda je $s = 4p_1 \cdots p_r - 1$ neparan broj oblika $4n+3$. Kako je proizvod brojeva oblika $4n+1$ takođe broj istog oblika, mora postojati prost delitelj p broja s koji ima oblik $4n+3$. Kako ni jedan od brojeva $p_1, p_2, \ldots, p_r$ ne deli s, broj p je novi prost broj.

U dokazu beskonačnosti skupa prostih brojeva oblika $4n+1$, gde je n prirodan broj, Euklidov argument ne prolazi tako jednostavno. Zasniva se na sledećoj činjenici.

Teorema. Ako su a i b uzajamno prosti prirodni brojevi, svaki neparan prost delitelj broja a^2+b^2 je oblika $4n+1$.

Za dokaz teoreme neophodna je *mala Fermatova teorema.* Ona tvrdi da za svaki ceo broj $a \neq 0$ i prost p koji ne deli a, $a^{p-1} = 1 \pmod p$.

Dokaz. Ako je p neparan prost delitelj broja a^2+b^2, onda je $a^2 = -b^2 \pmod p$. Otuda, ako $p|a$, onda $p|b$, što protivreči pretpostavci da je $(a,b) = 1$. Dakle $(a,p) = 1$ i slično $(b,p) = 1$.

Stepenovanjem jednakosti $a^2 = -b^2 \pmod p$ sa $(p-1)/2$ i primenom male Fermatove teoreme dobija se da je $(-1)^{(p-1)/2} = 1 \pmod p$. Međutim,

kako je $p > 2$ i kako je $\left|1 - (-1)^{(p-1)/2}\right| \leq 2$, iz prethodne jednakosti sledi da je $(-1)^{(p-1)/2} = 1$, što zapravo znači da je $(p-1)/2 = 2n$, odnosno, $p = 4n + 1$, za neko $n \geq 1$.

Teorema. Prostih brojeva oblika $4n + 1$, gde je n prirodan broj, ima beskonačno mnogo.

Fermatov dokaz. Pretpostavimo da su svi prosti brojevi oblika $4n + 1$ redom brojevi $p_1 = 5, p_2 = 13, \ldots p_r$ i neka je $s = (2p_1 \cdots p_r)^2 + 1$. Ako je p prost neparan delitelj broja s, on je različit od $p_1, p_2, \ldots p_r$, a prema prethodnoj teoremi, mora biti oblika $4k + 1$, što nije moguće.

Kako kvadrat neparnog broja pri deljenju sa 8 ima ostatak 1, broj oblika $s = (p_1, \ldots, p_n)^2 + 1$ ima ostatak 5, pri deljenju sa 8. Otuda sledi da prostih brojeva oblika $8n + 5$ ima beskonačno mnogo.

Dirišleova Teorema. Ako su a i b uzajamno prosti brojevi, progresija $an + b$ sadrži beskonačno mnogo prostih brojeva.

Teoremu je dokazao nemački matematičar Peter Gustav Ležen Dirišle (1805. – 1859.), ali ne postoji dokaz Dirišleove teoreme koji bi se zasnivao na modifikacijama Euklidovog argumenta poput prethodnih. Njegova priroda je potpuno drugačija i predstavlja repliku ideje Ojlerovog dokaza beskonačnosti skupa prostih brojeva. Iako nije sasvim jasno šta je u matematici elementarno, Dirišleov dokaz se smatra prvim neelementarnim dokazom u aritmetici. Za ovu priliku, na primerima progresija oblika $4n \pm 1$, demonstriraćemo njegove osnovne ideje, ali ga nećemo u celosti izložiti.

Koristeći poznate teoreme matematičke analize, razmotrićemo opšta svojstva redova

$$f_0(s) = \sum_{k=0}^{\infty} \frac{1}{(2k+1)^s}, f_1(s) = \sum_{k=0}^{\infty} \frac{(-1)^k}{(2k+1)^s},$$

gde je s realan broj.

Dirišleov kriterijum: Red $\sum f_n(x) g_n(x)$ ravnomerno konvergira na skupu A realnih brojeva ako zadovoljava sledeće uslove:

(i) red $\sum g_n(x)$ ima ravnomerno ograničene parcijalne sume na skupu A, tj. postoji realan broj K takav da za sve $n \geq 1$ i svako $x \in A$, $\left|\sum_{k=1}^{n} g_k(x)\right| \leq K$,

(ii) za svako $x \in A$, $f_n(x)$ je monoton niz i $f_n(x) \to 0$ ravnomerno na skupu A.

Oba reda konvergiraju za $s > 1$, a red $f_1(s)$ i za sve $s > 0$. Iz Dirišleovog kriterijuma ravnomerne konvergencije sledi da red $f_1(s)$ ravnomerno konvergira u oblasti $s > \delta$, za svako $\delta > 0$. Kako su članovi tog reda neprekidni u oblasti $s > \delta$, prema teoremi o neprekidnosti sume funkcionalnog reda, funkcija $f_1(s)$ je neprekidna u oblasti $s > \delta$, a kako je $\delta > 0$ proizvoljno, funkcija je neprekidna u oblasti $s > 0$.

Lajbnicov kriterijum: Ako $\lim c_n = 0$ i za svako $n \geq 0$, $c_{n+1} \leq c_n$, onda alternativni red $\sum\limits_{n=0}^{\infty} (-1)^n c_n$ konvergira.

Budući da apsolutna vrednost sume alternativnog reda, koji zadovoljava Lajbnicov kriterijum konvergencije, ne prevazilazi vrednost njegovog prvog člana, to je

$$f_1(1) = 1 - \tfrac{1}{3} + \tfrac{1}{5} - \cdots = 1 - \left(\tfrac{1}{3} - \tfrac{1}{5} + \cdots\right) > \tfrac{2}{3}.$$

Za svako $s > 1$, funkcija $1/(2x+1)^s$ je opadajuća i njen nesvojstveni integral u granicama od 0 do ∞ konvergira, pa je

$$f_0(s) = \sum_{k=0}^{\infty} \tfrac{1}{(2k+1)^s} \geq \int_0^{\infty} \tfrac{dx}{(2x+1)^s} = \tfrac{1}{2(s-1)},$$

što znači da je $\lim\limits_{s \to +1} f_0(s) = \infty$.

Predstavićemo funkcije $f_0(s)$ i $f_1(s)$ u formi Ojlerovih proizvoda, odnosno, kao beskonačne proizvode po prostim brojevima. U tom cilju, neka su funkcije $\chi_0(n)$ i $\chi_1(n)$ definisane na skupu prirodnih brojeva sa realnim vrednostima tako da

$$\chi_0(n) = \begin{cases} 0 & \text{ako je } n = 2k, \\ 1 & \text{inače,} \end{cases}$$

$$\chi_1(n) = \begin{cases} 0 & \text{ako je } n = 2k, \\ (-1)^{(n-1)/2} & \text{inače.} \end{cases}$$

Funkcije $\chi_0(n)$ i $\chi_1(n)$ su *multiplikativne*, tj. za sve prirodne brojeve m i n, $\chi(mn) = \chi(m)\chi(n)$. Koristeći multiplikativnost funkcija $\chi_0(n)$ i $\chi_1(n)$, u proizvod po prostim brojevima razložićemo sledeće funkcije:

$$f_0(s) = \sum_{n=1}^{\infty} \tfrac{\chi_0(n)}{n^s}, \quad f_1(s) = \sum_{n=1}^{\infty} \tfrac{\chi_1(n)}{n^s}.$$

Teorema o Ojlerovom proizvodu. Ako je funkcija $f(x)$ multiplikativna i red $S = \sum\limits_{n=1}^{\infty} f(n)$ apsolutno konvergira, onda je

$$S = \prod_p (1 - f(p))^- 1.$$

Dokaz. Zbog pretpostavljene apsolutne konvergencije reda $S = \sum\limits_{n=1}^{\infty} f(n)$, za svako $n > 1$, mora biti $|f(n)| < 1$. U suprotnom bi smo imali $|f(n^m)| = |f(n)|^m \geq 1$, za svako $m > 1$, što nije moguće. Otuda sledi da red

$$\sum_{k=0}^{\infty} f(p^k) = \sum_{k=0}^{\infty} f(p)^k$$

apsolutno konvergira za svaki prost broj p, a njegova suma, kao suma geometrijskog reda sa količnikom manjim od jedan, jednaka je $(1 - f(p))^{-1}$. Množenjem konačnog broja takvih redova i koristeći činjenicu da je $f(n)$ multuplikativna funkcija, dobijamo da je

$$S(x) = \prod_{p \leq x} (1 - f(p))^{-1} = \prod_{p \leq x} \sum_{k=0}^{\infty} f(p^k) = \sum_{i=1}^{\infty} f(n_i),$$

gde se u sabircima $f(n_i)$ javljaju tačno oni prirodni brojevi n_i čiji svi prosti delitelji nisu veći od x. Otuda sledi da se u razlici

$$S - S(x) = \sum_{i=1}^{\infty} f(m_i)$$

javljaju samo sabirci $f(m_i)$ u kojima broj m_i ima bar jedan prost faktor $p > x$. Otuda sledi da je

$$|S - S(x)| \leq \sum_{n > x} |f(n)|,$$

pa kako red $S = \sum\limits_{n=1}^{\infty} f(n)$ apsolutno konvergira, konačno dobijamo da je

$$\lim_{x \to \infty} S(x) = S.$$

Primenom teoreme o Ojlerovom proizvodu na funkcije $\chi_0(n)/n^s$ i $\chi_1(n)/n^s$, za $s > 1$, funkcije $f_0(s)$ i $f_1(s)$ možemo predstaviti kao proizvode po prostim brojevima

$$f_0(s) = \prod_p \left(1 - \frac{\chi_0(p)}{p^s}\right)^{-1}, \ f_1(s) = \prod_p \left(1 - \frac{\chi_1(p)}{p^s}\right)^{-1}.$$

Otuda sledi da je

$$\ln f_0(s) = -\sum_p \ln\left(1 - \tfrac{\chi_0(p)}{p^s}\right),$$
$$\ln f_1(s) = -\sum_p \ln\left(1 - \tfrac{\chi_1(p)}{p^s}\right),$$

pa se na osnovu Tejlorovog razvoja

$$-\ln(1-t) = \sum_{k=1}^{\infty} \tfrac{t^k}{k},$$

gde je $|t| < 1$, dobija da je

$$\ln f_i(s) = \sum_p \sum_{k=1}^{\infty} \tfrac{\chi_i(p)^k}{k \cdot p^{ks}} = \sum_p \tfrac{\chi_i(p)}{p^s} + \sum_p \sum_{k=2}^{\infty} \tfrac{\chi_i(p)^k}{k \cdot p^{ks}},$$

za $i = 0, 1$ i svako $s > 1$.

Ocenićemo sumu $S = \sum_p \sum_{k=2}^{\infty} \frac{\chi_i(p)^k}{k \cdot p^{ks}}$ sa gornje strane. Kako je $|\chi_i(p)| \leq 1$, za sve $s \geq 1$ imamo

$$\begin{aligned} \left|\sum_{k=2}^{\infty} \frac{\chi_i(p)^k}{k \cdot p^{ks}}\right| &\leq \sum_{k=2}^{\infty} \frac{1}{k \cdot p^{ks}} \\ &< \frac{1}{2} \sum_{k=2}^{\infty} \frac{1}{p^{ks}} \\ &= \frac{1}{2(p^{2s} - p^s)} \leq \frac{1}{p^{2s}}. \end{aligned}$$

Koristeći nejednakost $\sum_{n=2}^{\infty} \frac{1}{n^{2s}} \leq \sum_{n=2}^{\infty} \frac{1}{n^2}$ dobijamo sledeću ocenu dvojne sume S:

$$|S| \leq \sum_p \left|\sum_{k=2}^{\infty} \tfrac{\chi_i(p)^k}{k \cdot p^{ks}}\right| \leq \sum_p \tfrac{1}{p^{2s}} \leq \sum_{n=2}^{\infty} \tfrac{1}{n^{2s}} \leq \sum_{n=2}^{\infty} \tfrac{1}{n^2}.$$

To znači da, kada $s \to 1 + 0$, suma S ostaje ograničena, pa dakle

$$\ln f_i(s) = \sum_p \tfrac{\chi_i(p)}{p^s} + O(1),$$

odakle se dobija da je

$$\sum_p \tfrac{\chi_i(p)}{p^s} = \ln f_i(s) + O(1),$$

kada $s \to 1 + 0$, za $i = 0, 1$.

Na osnovu definicije funkcija $\chi_i(p)$ i apsolutne konvergencije redova $\sum_p \frac{\chi_i(p)}{p^s}$, za $s > 1$, $i = 0, 1$, dobijamo sledeće jednakosti:

$$\sum_{p=1 \pmod 4} \frac{1}{p^s} - \sum_{p=3 \pmod 4} \frac{1}{p^s} = \ln f_1(s) + O(1),$$
$$\sum_{p=1 \pmod 4} \frac{1}{p^s} + \sum_{p=3 \pmod 4} \frac{1}{p^s} = \ln f_0(s) + O(1),$$

a otuda sledi da je

$$\sum_{p=1 \pmod 4} \frac{1}{p^s} = \frac{1}{2}(\ln f_0(s) + \ln f_1(s)) + O(1),$$
$$\sum_{p=3 \pmod 4} \frac{1}{p^s} = \frac{1}{2}(\ln f_0(s) - \ln f_1(s)) + O(1).$$

Kako je funkcija $f_1(s)$ neprekidna u tački $s = 1$ i kako smo ranije pokazali da je $f_1(1) > \frac{2}{3} > 0$, funkcija $\ln f_1(s)$ je ograničena u okolini tačke $s = 1$. Ali, kako funkcija $f_0(s)$ teži beskonačnosti kada $s \to 1 + 0$, to znači da je

$$\lim_{s \to 1+0} \sum_{p=1 \pmod 4} \frac{1}{p^s} = \infty,$$
$$\lim_{s \to 1+0} \sum_{p=3 \pmod 4} \frac{1}{p^s} = \infty.$$

Otuda sledi da svaka od progresija $4k + 1$ i $4k + 3$, gde je k prirodan broj, sadrži beskonačno mnogo prostih brojeva.

Aritmetička funkcija

Razmotrićemo svojstva nekoliko najvažnijih aritmetičkih funkcija. Pre svega to je funkcija $\phi(n)$, broj prirodnih brojeva koji su uzajamno prosti sa n i manji od n, a zatim, broj delitelja $\tau(n)$ i suma delitelja $\sigma(n)$ prirodnog broja n. Radi se o aritmetičkim funkcijama u sasvim strogom smislu. Naime, realna funkcija f definisana na skupu prirodnih brojeva je *aritmetička* ako je $f(m)f(n) = f(mn)$, za sve uzajamno proste prirodne brojeve m i n.

Ako aritmetička funkcija f nije identički jednaka nuli, onda je $f(1) = 1$.

Ako je $n = p_1^{a_1} \cdots p_k^{a_k}$ i f aritmetička funkcija, onda je

$$f(n) = f(p_1^{a_1}) \cdots f(p_k^{a_k}),$$

što znači da je za određivanje vrednosti funkcije f dovoljno poznavanje njenih vrednosti na stepenima prostih brojeva.

Teorema. Ako je f aritmetička funkcija, onda je i funkcija $g(n) = \sum_{d|n} f(d)$ takođe aritmetička. Pritom, sumira se po svim deliteljima broja n.

Dokaz. Zaista, ako je $(m, n) = 1$ onda

$$g(mn) = \sum_{d|m} \sum_{d'|n} f(dd') = \sum_{d|m} f(d) \sum_{d'|n} f(d') = g(m)g(n).$$

Račun ostataka

U prethodnim razmatranjima, sa $a = b \pmod{n}$ označavali smo činjenicu da prirodan broj n deli razliku $a - b$ celih brojeva a i b. U tom slučaju celi brojevi a i b su *kongruentni* $\pmod{n}$, a ako je $0 \leq b < n$, broj b je *ostatak* od $a \pmod{n}$. Sasvim jednostavno se proverava da je $a = b \pmod{n}$ relacija ekvivalencije. Njene klase ekvivalencije nazivamo *klasama ostataka*, a skup koji sadrži po jednog predstavnika svake od klasa je *kompletan skup ostataka* $\pmod{n}$.

Relacija $a = b \pmod{n}$ je *kongruencija* u odnosu na operacije sabiranja i množenje celih brojeva, tj. ako $a = b \pmod{n}$ i $c = d \pmod{n}$ onda $a + c = b + d \pmod{n}$ i $ac = bd \pmod{n}$.

Opštije, ako $a = b \pmod{n}$ i ako je $f(x)$ polinom sa celim koeficijentima, onda je $f(a) = f(b) \pmod{n}$.

Ako su k i n uzajamno prosti i $ka = kb \pmod{n}$, onda $a = b \pmod{n}$. To znači da ako je $a_1, \ldots, a_n$ kompletan skup ostataka $\pmod{n}$, onda je takav i skup $ka_1, \ldots, ka_n$.

Ojlerova funkcija

Ako je n prirodan broj, *Ojlerova funkcija* $\phi(n)$ je broj svih brojeva uzajamno prostih sa n, koji su manji od n. Na primer, $\phi(4) = 2$, $\phi(12) = 4$, $\phi(p) = p - 1$, ako je p prost broj.

Za svaki prirodan broj n, *redukovani skup ostataka* $\pmod{n}$ je skup od $\phi(n)$ brojeva uzajamno prostih sa n koji su predstavnici različitih klasa ostataka $\pmod{n}$. Specijalno, brojevi a takvi da $(a, n) = 1$ i $1 \leq a \leq n$ čine redukovani skup ostataka $\pmod{n}$.

Teorema. Funkcija ϕ je aritmetička.

Dokaz. Pretpostavimo da su $n, n' \geq 1$ uzajamno prosti brojevi. Neka a prolazi redukovani skup ostataka $\pmod{n}$ i a' redukovani skup ostataka $\pmod{n'}$. Dovoljno je dokazati da tada $an' + a'n$ prolazi redukovani skup ostataka $\pmod{nn'}$.

Treba dakle dokazati da za svako $b \geq 1$, ako $(b, nn') = 1$, onda $b = an' + a'n$, za neko a iz redukovanog skupa ostataka $\pmod{n}$ i neko a' iz redukovanog skupa ostataka $\pmod{n'}$.

Kako je $(n, n') = 1$, postoje celi brojevi m, m' koji zadovoljavaju jednačinu $mn' + m'n = 1$. Kako je $(bm, n) = 1$, postoji a takvo da $a = bm \pmod n$ i slično, kako je $(bm', n') = 1$, postoji a' takvo da $a' = bm' \pmod{n'}$. Otuda se neposredno dobija da je $b = an' + a'n \pmod{nn'}$.

Ojlerova teorema. Za svaki prirodan broj n,

$$\phi(n) = n \prod_{p|n} (1 - \tfrac{1}{p}).$$

Dokaz. Neka je $n = p_1^{k_1} \dots p_m^{k_m}$. Zbog multiplikativnosti funkcije ϕ, izračunavanje vrednosti $\phi(n)$ svodi se na izračunavanje vrednosti $\phi(p^k)$, gde je p prost broj, a ona iznosi $\phi(p^k) = p^k - p^{k-1}$.

Na osnovu Ojlerove teoreme, dobija se još jedan dokaz beskonačnosti skupa prostih brojeva. Naime, ako je $m = 2 \cdot 3 \cdot 5 \cdots p_n$ i kada ne bi bilo prostih brojeva manjih od m različitih od $p_1, \dots, p_n$, to bi značilo da je $\phi(m) = 1$, što nije moguće, budući da je

$$\phi(m) = m \left(1 - \tfrac{1}{p_1}\right) \cdots \left(1 - \tfrac{1}{p_n}\right) > 1.$$

Pod istim uslovima, na osnovu Ojlerove teoreme, dobija se i ocena $\pi(m) \leq \phi(m) + n$.

Neposredna posledica aritmetičke prirode funkcije ϕ je i sledeća relacija:

Gausova teorema. Za svako $n \geq 1$, $\sum_{d|n} \phi(d) = n$.

Dokaz. Funkcija na levoj strani jednakosti je aritmetička, a kada je $n = p^k$, njena vrednost je $\phi(1) + \phi(p) + \dots + \phi(p^k) = p^k$.

Mebijusova funkcija

Dokazali smo da je suma vrednosti aritmetičke funkcije, po deliteljima prirodnog broja n, takođe aritmetička funkcija. Između tih funkcija postoji još tešnja veza; one su u izvesnom smislu međusobno inverzne. Takva veza uspostavlja se pomoću funkcije koju je definisao Avgust Ferdinand Mebijus (1790. – 1868.).

Neka je $\nu(1) = 1$ i $\nu(n) = 0$, za svako $n > 1$. *Mebijusova funkcija* $\nu(n)$ je aritmetička funkcija koja zadovoljava rekurentnu relaciju $\mu(n) = \sum_{d|n} \mu(d)$.

Ako je p prost broj i $k > 0$, $\nu(p^k) = \mu(1) + \mu(p) = 0$, pa zbog multiplikativnosti funkcije μ, $\mu(1) = 1$ i

$$\mu(n) = \begin{cases} (-1)^k & \text{ako } n = p_1 \dots p_k, \\ 0 & \text{ako } m^2 | n, \text{ za neko } m > 1, \end{cases}$$

za svaki prirodan broj $n > 1$.

Svojstva funkcija μ i ν omogućavaju na da dokažemo *formulu inverzije* za aritmetičke funkcije.

Teorema. Ako su f i g aritmetičke funkcije,

$$g(n) = \sum_{d|n} f(d) \Leftrightarrow f(n) = \sum_{d|n} \mu(d) g(n/d).$$

Dokaz. Ako je $g(n) = \sum_{d|n} f(d)$,

$$\begin{aligned} \sum_{d|n} \mu(d) g(n/d) &= \sum_{d|n} \sum_{d'|n/d} \mu(d) f(d') \\ &= \sum_{d'|n} f(d') \nu(n/d'). \end{aligned}$$

Kako je $\nu(n/d') = 0$, osim u slučaju $d' = n$, to mora biti

$$f(n) = \sum_{d|n} \mu(d) g(n/d).$$

Obratno, ako se pretpostavi da važi upravo dobijenu jednakost onda $f(n) = \sum_{d'|n} \mu(n/d') g(d')$, pa je

$$\begin{aligned} \sum_{d|n} f(d) &= \sum_{d|n} f(n/d) \\ &= \sum_{d|n} \sum_{d'|n/d} \mu(n/dd') g(d') \\ &= \sum_{d'|n} g(d') \nu(n/d'). \end{aligned}$$

Kako je $\nu(n/d') = 0$, osim u slučaju $d' = n$, to mora biti $g(n) = \sum_{d|n} f(d)$.

Teorema. Ojlerova i Mebijusova funkcija zadovoljavaju relaciju $\phi(n) = n \sum_{d|n} \mu(d)/d$.

Dokaz. Neposredno sledi iz formule $\sum_{d|n} \phi(d) = n$.

Rimanova hipoteza

Sredinom devetnaestog veka, Georg Fridrih Bernhard Riman (1826. – 1866.) uočio je blisku povezanost raspodele prostih brojeva sa svojstvima zeta-funkcije

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

gde je s kompleksan broj. Jasno je da red $\sum_{n=1}^{\infty} 1/n^s$ apsolutno konvergira za $\sigma > 1$, gde je $s = \sigma + it$, a konvergira uniformno za $\sigma > 1 + \delta$, za sve $\delta > 0$. Pritom, σ i t su realni brojevi.

Riman je dokazao da zeta-funkcija $\zeta(s)$ ima analitičko produženje na kompleksnu ravan. To produženje je regularno, osim u prostom polu $s = 1$, sa reziduumom 1.

Fundamentalna veza zeta-funkcije sa raspodelom prostih brojeva određena je Ojlerovim proizvodom

$$\zeta(s) = \prod_p \left(1 - \frac{1}{p^s}\right)^{-1},$$

za sve $\sigma > 1$. Ona se dobija primenom Teoreme o Ojlerovom proizvodu na funkciju $f(n) = 1/n^s$.

Ojlerov proizvod pokazuje da $\zeta(s)$ nema nulu za $\sigma > 1$. Njeno analitičko produženje, za $\sigma < 0$, ima samo "trivijalne nule" u tačkama $s = -2, -4, \ldots$ Sve druge nule zeta-funkcije leže u zoni $0 \leq \sigma \leq 1$. Riman je postavio hipotezu da one zapravo leže na pravoj $\sigma = \frac{1}{2}$, za koju ima mnogo potvrda, ali njen dokaz nemamo. Ako je Rimanova hipoteza tačna, razlika susednih prostih brojeva zadovoljava relaciju $p_{n+1} - p_n = O(p_n^{\frac{1}{2}+\epsilon})$.

Linearna kongruencija

Ako je $f(x)$ polinom sa celobrojnim koeficijentima, ceo broj a takav da $f(a) = 0 \pmod n$ je rešenje kongruencije $f(x) = 0 \pmod n$.

U opštem slučaju, ako ima bar jedno rešenje a, kongruencija $f(x) = 0 \pmod n$ ima beskonačno mnogo rešenja oblika $b = a \pmod n$. Stoga, različita rešenja kongruencije $f(x) = 0 \pmod n$ računamo $\pmod n$, odnosno, u kompletnom skupu ostataka $\pmod n$. Pritom, broj rešenja kongruencije ne zavisi od izbora kompletnog skupa ostataka.

Ako $d > 0$ deli n, $d > 0$ i ako je a rešenje kongruencije $f(x) = 0 \pmod n$, broj a je rešenje kongruencije $f(x) = 0 \pmod d$

Teorema. Ako su a i n prirodni brojevi i b ceo broj, kongruencija $ax = b \pmod n$ ima rešenje ako i samo ako $(a, n)|b$.

Dokaz. Ako kongruencija $ax = b \pmod n$ ima rešenje, onda jasno $(a, n)|b$. Pretpostavimo da $d = (a, n)$ deli b i neka je $a' = a/d$, $b' = b/d$

i $n' = n/d$. Sada je dovoljno rešiti kongruenciju $a'x = b' \pmod{n'}$. Kako su a' i n' uzajamno prosti, kada x prođe kompletnim skupom ostataka $\pmod{n'}$, $a'x$ prođe isti skup. Ako je x' rešenje kongruencije $a'x' = b' \pmod{n'}$, onda je kompletan skup rešenja kongruencije $ax = b \pmod{n}$ određen sa $x = x' + mn'$, gde je $1 \leq m < d$.

Dakle, kada $d|b$, kongruencija $ax = b \pmod{n}$ ima tačno d rešenja $\pmod{n}$. Ako je p prost broj i a nije deljiv sa p onda kongruencija $ax = b \pmod{p}$ uvek ima tačno jedno rešenje.

Kineska teorema o ostacima

Raspravićemo egzistenciju rešenja sistema linearnih kongruencija. Ključni argument u toj raspravi je *Kineska teorema o ostacima.* Nebitno preformulisana na jezik savremene aritmetike, njena originalna verzija izgledala je ovako:

Svaki ostatak $\pmod{mn}$ ima jedinstveno određene ostatke $\pmod{m}$ i $\pmod{n}$. Ako su m i n uzajamno prosti, važi i obratno, tj. na osnovu ostataka $\pmod{m}$ i $\pmod{n}$, može se jednoznačno odrediti ostatak $\pmod{mn}$. Pritom, uvek postoji ceo broj koji ima zadate ostatke $\pmod{m}$ i $\pmod{n}$.

Zanimljiv je originalni dokaz teoreme. Neka su m i n uzajamno prosti. Ako brojevi a i b daju iste ostatke $\pmod{m}$ i $\pmod{n}$, onda je broj $a - b$ deljiv sa mn, pa a i b daju isti ostatak $\pmod{mn}$. Kako različitih parova ostataka $\pmod{m}$ i $\pmod{n}$ ima mn, svakom takvom paru odgovara tačno jedan ostatak $\pmod{mn}$.

Prirodni brojevi $n_1, \ldots, n_k$ su uzajamno prosti u parovima, ako za sve $i \neq j$, $(n_i, n_j) = 1$.

Kineska teorema o ostacima. Ako su prirodni brojevi $n_1, \ldots, n_k$ uzajamno prosti u parovima, postoji ceo broj x takav da $x = c_i \pmod{n_i}$, $i = 1, \ldots, k$, za proizvoljne cele brojeve $c_1, \ldots, c_k$.

Dokaz. Postoji jedinstveno rešenje sistema x modulo $n = n_1 \cdots n_k$. Da to dokažemo, neka je $m_i = n/n_i$, za $1 \leq i \leq k$. Kako je $(m_i, n_i) = 1$ postoji ceo broj x_i takav da $m_i x_i = c_i \pmod{n_i}$. Ako je $x = m_1 x_1 + \cdots m_k x_k$ onda očigledno $x = c_i \pmod{n_i}$. Ako su x i y rešenja sistema $x = c_i \pmod{n_i}$, ondaje $x = y \pmod{n_i}$, za $0 \leq i \leq k$, pa kako su n_i uzajamno prosti u parovima, mora biti $x = y \pmod{n}$.

Na osnovu teoreme o linearnoj kongruenciji i Kineske teoreme o ostacima dobijamo opšti stav o egzistenciji rešenja sistema linearnih kongruencija.

Teorema. Ako su prirodni brojevi $n_1, \ldots, n_k$ uzajamno prosti u parovima, sistem kongruencija $a_i x = b_i \pmod{n_i}$, $1 \leq i \leq k$, ima rešenje ako i samo ako (a_i, n_i) deli b_i, za sve $1 \leq i \leq k$.

Na primer, sistem kongruencija

$$\begin{aligned} x &= 2 \pmod 5, \\ x &= 3 \pmod 7, \\ x &= 4 \pmod{11}, \end{aligned}$$

ima rešenje $x = 77x_1 + 55x_2 + 35x_3$, gde su x_1, x_2, x_3 rešenja kongruencija

$$\begin{aligned} 2x_1 &= 2 \pmod 5, \\ 6x_2 &= 3 \pmod 7, \\ 2x_3 &= 4 \pmod{11}. \end{aligned}$$

Dakle, može se uzeti da je $x_1 = 1$, $x_2 = 4$, $x_3 = 2$ što daje rešenje $x = 367$. Konačno, kompletno rešenje je $x = -18 \pmod{385}$.

Rešavanje kongruencije

Ne postoji opšti metod za rešavanje kongruencija. Najčešće, prvi korak je svođenje problema na kongruencije po prostom modulu. Takvo svođenje omogućava kineska teorema o ostacima.

Teorema. Ako je $n = p_1^{e_1} \cdots p_k^{e_k}$ prirodan broj, kongruencija $f(x) = 0 \pmod n$ je ekvivalentna sistemu kongruencija $f(x) = 0 \pmod{p_i^{e_i}}$, $i = 1, \ldots, k$.

Broj a je rešenje kongruencije $f(x) = 0 \pmod n$ ako i samo ako $a = a_i \pmod{p^{e_i}}$, gde je a_i neko od rešenja kongruencije $f(x) = 0 \pmod{p^{e_i}}$, $0 \leq i \leq k$.

Dokaz. Kako su moduli p^{e_i} uzajamno prosti u parovima, ispunjeni su uslovi za primenu kineske teoreme o ostacima. Ako su a_i rešenja redom kongruencija $f(x) = 0 \pmod{p^{e_i}}$, odredimo cele brojeve x_i tako da $np_i^{-e_i} x_i = 1 \pmod n$, pa je

$$a = \sum_{i=1}^{k} \tfrac{n}{p^{e_i}} a_i x_i \pmod n$$

rešenje kongruencije $f(x) = 0 \pmod n$. Ako svaka od kongruencija $f(x) = 0 \pmod{p^{e_i}}$ ima s_i rešenja, kongruencija $f(x) = 0 \pmod n$ ima $s_1 \cdots s_k$ različitih rešenja $\pmod n$.

Tako se rešavanje kongruencije $f(x) = 0 \pmod{n}$ svodi na rešavanje kongruencije $f(x) = 0 \pmod{p^k}$, gde je p prost broj.

Ako je a rešenje $f(x) = 0 \pmod{p^k}$ i b rešenje kongruencije $f(x) = 0 \pmod{p^{k-1}}$ takvo da $a = b \pmod{p^{k-1}}$, onda je $a = b + qp^{k-1} \pmod{p^k}$, za neki ceo broj q.

Kako polinom $f(x)$ ima Tejlorov razvoj, to je

$$\begin{aligned} f(a) &= f(b + qp^{k-1}) \\ &= \sum_{i=0}^{m} \tfrac{1}{i!} f^{(i)}(b) q^i p^{i(k-1)} \\ &= 0 \pmod{p^k}, \end{aligned}$$

gde je $m \geq 1$ stepen polinoma $f(x)$. Otuda je

$$f(b) + f'(b)qp^{k-1} = 0 \pmod{p^k},$$

pa kako je $f(b) = 0 \pmod{p^{k-1}}$, mora biti

$$f(b) + f'(b)qp^{k-1} = 0 \pmod{p}.$$

Ako je b rešenje kongruencije $f(x) = 0 \pmod{p^{k-1}}$ i q rešenje kongruencije $f(b) + f'(b)qp^{k-1} = 0 \pmod{p}$, onda je ceo broj $a = b + qp^{k-1}$ rešenje polazne kongruencije $f(x) = 0 \pmod{p^k}$.

Ako kongruencija $f(b) + f'(b)qp^{k-1} = 0 \pmod{p}$ nema rešenja, kongruencija $f(x) = 0 \pmod{p^k}$ nema rešenje koje proishodi iz rešenja b.

Na taj način, kongruenciju $f(x) = 0 \pmod{p^k}$ rešavamo, korak po korak, na osnovu rešenja kongruencije $f(x) = 0 \pmod{p}$.

Fermatova teorema

Sredinom sedamnaestog veka, izučavajući osobine Mersenovih brojeva, Fermat je formulisao sledeće dve teoreme:

Prva Teorema. Ako je $p > 0$, svaki prost delitelj Mersenovog broja m_p ima oblik $2kp + 1$, za neko $k \geq 1$.

Druga Teorema. Za svaki prost broj p, $2^p = 2 \pmod{p}$.

Nije jasno da li je Ferma znao dokaz bilo koje od ovih teorema, ali je uočio njihovu blisku povezanost.

Teorema. Prva i druga teorema su ekvivalentne.

Fermatov Dokaz. Verujemo da je Fermatova argumentacija izgledala ovako: Kako proizvod brojeva oblika $2kp+1$ i sam ima isti oblik, $m_p = 2kp+1$,

za neko $k \geq 1$ i kako je $m_p = 2^p - 1$, dobijamo $2^p - 2 = kp$, tj. važi druga teorema. Obratno, pretpostavimo drugu teoremu i neka je $q > 2$ prost delitelj Mersenovog broja m_p. To znači da broj q deli brojeve $2^p - 1$ i $2^{q-1} - 1$, pa je

$$(2^p - 1, 2^{q-1} - 1) = 2^{(p,q-1)} - 1.$$

Kako je $q > 1$, mora biti $(p, q-1) > 1$, a kako je p prost broj, to znači da $p|(q-1)$. tj. $q = sp + 1$, za neki prirodan broj s. Pritom, s mora biti oblika $2k$ jer, u suprotnom i prost broj q bi bio paran broj, pa dakle $q = 2kp + 1$.

Mala Fermatova teorema. Za svako $a > 1$ i svaki prost broj p, $a^p = a \pmod p$. Pritom, ako su a i p uzajamno prosti brojevi, $a^{p-1} = 1 \pmod n$.

Na ovu teoremu se u matematici često poziva kao na malu Fermatovu teoremu. Verovatno zbog velike Fermatove hipoteze. U nešto opštijoj formi i sto godina kasnije, teoremu je dokazao Ojler.

Teorema. Ako su ceo broj a i prirodan broj n uzajamno prosti, $a^{\phi(n)} = 1 \pmod n$.

Dokaz. Kako su a i n uzajamno prosti brojevi, kada x prolazi redukovani skup ostataka $(\bmod n)$, onda ax prolazi isti skup $(\bmod n)$, pa je

$$\prod_{(x,n)=1} x = \prod_{(x,n)=1} ax = a^{\phi(n)} \prod_{(x,n)=1} x \pmod n.$$

Skraćivanjem sa $\prod_{(x,n)=1} x$, dobija se $a^{\phi(n)} = 1 \pmod n$.

Neka su a i n uzajamno prosti prirodni brojevi. Najmanji prirodan broj d za koji je $a^d = 1 \pmod n$ je *red* prirodnog broja $a \pmod n$ ili, kako se to najčešće kaže, broj a *pripada* stepenu $d \pmod n$.

Teorema. Ako su a i n uzajamno prosti prirodni brojevi, red d broja $a \pmod n$ postoji i deli $\phi(n)$.

Dokaz. Važi i nešto više, d deli svaki broj k za koji je $a^k = 1 \pmod n$ jer, u suprotnom, ako bi bilo $k = dq + r$ i $0 \leq r < d$, onda bi smo imali $a^r = 1 \pmod n$, što protivreči definiciji reda d.

Teorema. Ima beskonačno mnogo prostih brojeva.

Dokaz. Neka je p najveći prost broj. Tvrdimo da je svaki prost broj q koji deli Mersenov broj $2^p - 1$ veći od p. Naime, ako q deli $2^p - 1$, onda je $2^p = 1 \pmod q$, pa prema prethodnoj teoremi, p deli $q - 1$, tj. $p < q$.

Vilsonova teorema

Dokazaćemo jedan od najstarijih kriterijuma za proste brojeve. Zasniva se na teoremi Džona Vilsona (1741. – 1739.).

Teorema. Za svaki prost broj p, $(p-1)! = -1 \ (mod\, p)$.

Dokaz. Možemo pretpostaviti da je $p > 2$. Za svaki prirodan broj $a < p$, postoji jedinstven prirodan broj $a' < p$ takav da je $aa' = 1 \pmod p$. Ako je $a = a'$, onda je $a^2 = 1 \pmod p$, pa dakle $a = 1$ ili $a = p-1$. Dakle, skup $2, 3, \ldots, p-2$ se može podeliti na $\frac{1}{2}(p-3)$ parova a, a' za koje je $aa' = 1 \pmod p$. Otuda je $2 \cdot 3 \cdots (p-2) = 1 \pmod p$, pa množenjem sa $p-1$ dobijamo $(p-1)! = p-1 = -1 \pmod p$.

Teorema. Kongruencija $x^2 = -1 \ (mod\, p)$ ima rešenje ako i samo ako $p = 1 \ (mod\, 4)$, za svaki prost broj $p > 2$.

Dokaz. Vilsonovu teoremu možemo izraziti u obliku $\prod_{k=1}^{(p-1)/2} k(p-k) = -1 \pmod p$, pa se dobija da je

$$(-1)^{(p-1)/2} \left(\prod_{k=1}^{(p-1)/2} k \right)^2 = -1 \pmod p.$$

Ako je $p = 1 \pmod 4$, onda $(-1)^{(p-1)/2} = 1$, pa jednačina $x^2 = -1 \pmod p$ ima rešenje

$$x = \prod_{k=1}^{(p-1)/2} k.$$

Ako je $p = 3 \pmod 4$ i ako bi x bilo rešenje kongruencije $x^2 = -1 \pmod p$, ondabi smo imali

$$x^{p-1} = (x^2)^{(p-1)/2} = (-1)^{(p-1)/2} = -1 \pmod p,$$

što protivreči maloj Fermatovoj teoremi.

Vilsonova teorema dopušta i konverziju, pa se tako dobija jedan test složenosti prirodnih brojeva.

Kriterijum sa proste brojeve: prirodan broj n je prost ako i samo ako $(n-1)! = -1 \ (mod\, n)$.

Dokaz. Ako je n složeni broj, svaki njegov delitelj, različit od njega samog, deli $(n-1)!$.

Vilsonov kriterijum ipak nema praktični značaj, budući da broj operacija u njegovoj primeni nekontrolisano raste. Mnogo značajnija je netačna

konverzija Fermatove teoreme. Naime, iako iz relacije $2^n = 2 \pmod{n}$ ne sledi da je n prost broj, skoro svi takvi brojevi su prosti.

Ako je a ceo broj i $a^n = a \pmod{n}$, broj n je *pseudoprost za osnovu* a. Pseudoprosti brojevi se relativno lako generišu, pa u praksi zamenjuju proste brojeve. Najmanji pseudo prost broj za bazu 2, koji nije prost je $341 = 11 \cdot 31$.

Lagranžova teorema

U slučaju kongruencije, osnovna teorema algebre ima specifičan oblik koji je formulisao i dokazao francuski matematičar Žozef Luj Lagranž (1736. – 1813.).

Teorema. Neka je $f(x) = a_n x^n + \ldots + a_0$ polinom stepena $n \geq 1$ sa celobrojnim koeficijentima. Ako je p prost broj i ako $(a_n, p) = 1$, kongruencija $f(x) = 0 \pmod{p}$ ima najviše n rešenja $\pmod{p}$.

Dokaz. Pretpostavimo da $f(x) = 0 \pmod{p}$ ima n rešenja $x_1, \ldots, x_n$. Ako podelimo $f(x)$ sa $x - x_1$, dobija se $f(x) = f_1(x)(x - x_1) + c_1$. Kako je $f(x_1) = 0 \pmod{p}$, to mora biti $c_1 = 0 \pmod{p}$, pa je $f(x) = f_1(x)(x - x_1) + kp$. Ako se isti postupak primeni na $f_1(x)$, a zatim na $f_2(x)$ itd. dobija se

$$f(x) = a_n(x - x_1) \cdots (x - x_n) + pg(x),$$

za neki polinom $g(x)$. Ako bi postojalo rešenje x_{n+1} koje nije kongruentno prethodnim, imali bi smo da je

$$f(x) = a_n(x_{n+1} - x_1) \cdots (x_{n+1} - x_n) = 0 \pmod{p},$$

što protivreči pretpostavci $(a_n, p) = 1$.

Teorema. Ako je vodeći koeficijent polinoma $f(x)$ jednak 1, kongruencija $f(x) = 0 \pmod{p}$ ima tačno n rešeja ako i samo ako $f(x)$ deli polinom $x^p - x \pmod{p}$.

Dokaz. Ako kongruencija $f(x) = 0 \pmod{p}$ ima n rešenja onda $n \leq p$. Neka je $x^p - x = f(x)q(x) + r(x)$, gde je $r(x)$ nula ili polinom stepena manjeg od n. Za svako rešenje a kongruencije $f(x) = 0 \pmod{p}$, $a^p - a = 0 \pmod{p}$, pa je $r(a) = 0 \pmod{p}$. To znači da polinom $r(x)$ stepena $< n$ ima n rešenja $\pmod{p}$, a to je moguće ako je $r(x)$ nula polinom ili ima oblik $ps(x)$. Dakle $f(x)$ deli $x^p - x \pmod{p}$.

Obratno, ako $x^p - x = f(x)q(x) + ps(x)$, onda za svaki ceo broj a, $f(a)q(a) = 0 \pmod p$, pa polinom $f(x)q(x)$ ima tačno p rešenja. Po Lagranžovoj teoremi, polinom $q(x)$ ima $k \leq p - n$ rešenja. Ako broj $a \pmod p$ nije rešenje polinoma $q(x)$, onda$(q(a), p) = 1$, pa zbog $f(a)q(a) = 0 \pmod p$ mora biti $f(a) = 0 \pmod p$, pa $f(x)$ ima bar n različitih korena.

Ograničenje na vodeći koeficijent je neophodno da bi se moglo izvršiti deljenje polinoma $x^p - x$ sa $f(x)$ u skupu celih brojeva. Ono ipak nije esencijalno, budući da, ako je a vodeći koeficijent polinoma $f(x)$, postoji a' takvo da $aa' = 1 \pmod p$. Pritom, kongruencije $a'f(x) = 0 \pmod p$ i $f(x) = 0 \pmod p$ imaju ista rešenja.

Na osnovu prethodne teoreme,

$$x^{p-1} - 1 = (x-1)\cdots(x-p+1) \pmod p,$$

pa se upoređivanjem konstantnih koeficijenata dobija još jedan dokaz Vilsonove teoreme.

Ako je $n \geq 1$ složeni broj, Lagranžova teorema ne važi za kongruencije po modulu n. Na primer, kongruencija $x^2 = 1 \pmod 8$ ima četiri rešenja.

Primitivni koreni

Ako je n prirodan broj, na skupu ostataka $\pmod n$ može se definisati i logaritamska funkcija $\pmod n$. To znači da postoji ceo broj g takav da se svaki ostatak $\pmod n$ može predstaviti kao stepen broja $g \pmod n$. Odredićemo sve prirodne brojeve n sa takvim svojstvom.

Neka su a i n uzajamno prosti prirodni brojevi. Kako smo ranije napomenuli, najmanji prirodan broj d za koji je $a^d = 1 \pmod n$ je red prirodnog broja $a \pmod n$, odnosno, kažemo da broj a *pripada* stepenu $d \pmod n$. Podsetimo se da d deli svaki broj k za koji je $a^k = 1 \pmod n$.

Ako a pripada eksponentu $\phi(n) \pmod n$, broj a nazivamo *primitivnim korenom* $\pmod n$.

Gausova teorema. Svaki prost broj $p > 2$ ima $\phi(p-1)$ primitivnih korena $\pmod p$.

Dokaz. Svaki broj a, gde je $1 \leq a \leq p-1$, pripada nekom eksponentu $d \pmod p$ tako da $d|(p-1)$. To znači da su brojevi $1, a, a^2, \ldots, a^{d-1}$ različiti $\pmod p$. Na osnovu Lagranžove teoreme, ti brojevi su sva rešenja kongruencije $x^d = 1 \pmod p$.

Tvrdimo da su svi brojevi koji pripadaju $d \pmod p$ oblika a^m, za neko m, za koje je $(m, d) = 1$.

Svaki takav broj je reda d jer, ako $a^{md'} = 1 \pmod p$ onda $d|d'$. Ako b pripada $d \pmod p$, onda je $b = a^m$ za neko m takvo da $1 \leq m \leq d$. Kako je $b^{\frac{d}{(m,d)}} = (a^d)^{\frac{m}{(m,d)}} = 1 \pmod p$, to mora biti $(m, d) = 1$. Dakle, ako $d|p-1$, broj ostataka $a \pmod p$ koji pripadaju $d \pmod p$, u oznaci $\psi(d)$, je ili $\phi(d)$ ili nula, odnosno, $\psi(d) \leq \phi(d)$. Kako svaki broj a pripada nekom $d \pmod p$ koji deli $p-1$, mora biti

$$\sum_{d|(p-1)} \psi(d) = p - 1.$$

Kako je $\sum_{d|(p-1)} \phi(d) = p - 1$, otuda sledi da je

$$\sum_{d|(p-1)} (\psi(d) - \phi(d)) = 0,$$

što znači da je $\psi(d) - \phi(d) = 0$, za svaki broj d koji deli $p-1$, pa dakle $\psi(p-1) = \phi(p-1)$.

Teorema. Neka je $(a, p) = 1$ i $d = (n, p-1)$, gde je a ceo broj, p prost i $n \geq 1$. Ako je $a^{(p-1)/d} = 1 \pmod p$, kongruencija $x^n = a$, $\pmod p$ ima tačno d rešenja $\pmod p$, a uopšte nema rešenja ako je $a^{(p-1)/d} \neq 1 \pmod p$.

Dokaz. Ako je u rešenje kongruencije $x^n = a \pmod p$,

$$a^{(p-1)/d} = u^{n(p-1)/d} = u^{(p-1)(n/d)} = 1 \pmod p,$$

pa kongruencija $x^n = a$, $\pmod p$ nema rešenja ako je $a^{(p-1)/d} \neq 1 \pmod p$.

Pretpostavimo da je $a^{(p-1)/d} = 1 \pmod p$. Prema prethodnoj teoremi, postoji primitivan koren $g \pmod p$ i eksponent k takav da $g^k = a \pmod p$. Otuda sledi da je

$$g^{k(p-1)/d} = a^{(p-1)/d} = 1 \pmod p,$$

što znači da je $k(p-1)/d = 0 \pmod{(p-1)}$, pa dakle d deli k. Ako uopšte postoji, svako rešenje kongruencije $x^n = a \pmod p$ je stepen primitivnog korena g, odnosno, ima oblik $g^y \pmod p$. Dakle, rešenja kongruencije $x^n = a \pmod p$ odgovaraju rešenjima kongruencije $g^{yn} = g^k \pmod p$, koja ima rešenje ako i samo ako $yn = k \pmod{(p-1)}$. Kako d deli k, prema teoremi o linearnoj kongruenciji, kongruencija $yn = k \pmod{(p-1)}$ ima tačno d rešenja.

Teorema. Kongruencija $x^2 = a \pmod p$, gde su prost broj p i ceo broj a uzajamno prosti, ima dva rešenja ako $a^{(p-1)/2} = 1 \pmod p$, a uopšte nema rešenje ako $a^{(p-1)/2} \neq 1 \pmod p$.

Teorema. Ako je g primitivni koren $(\mathrm{mod}\, p)$, postoji ceo broj x takav da za svako $k \geq 1$, $g' = g + xp$ je primitivni koren $(\mathrm{mod}\, p^k)$.

Dokaz. Kako je $g^{p-1} = 1 + yp$, za neki ceo broj y, po binomnoj formuli imamo da je $g'^{p-1} = 1 + zp$, gde je $z = y + (p-1)g^{p-2}x \pmod p$. Koeficijent uz x nije deljiv sa p, pa se x može izabrati tako da $(z, p) = 1$.

Tvrdimo da je g' primitivni koren $(\mathrm{mod}\, p^k)$.

Pretpostavimo da g' pripada $d \pmod{p^k}$. Onda d deli $\phi(p^k) = p^{k-1}(p-1)$. Kako je g' primitivni koren $(\mathrm{mod}\, p)$, $p-1$ deli d. Otuda sledi da je $d = p^i(p-1)$, za neko $i < k$. Dalje, kako je p neparan,

$$(1 + pz)^{p^i} = 1 + p^{i+1} z_i,$$

gde je $(z_i, p) = 1$. Sada zbog $g'^d = 1 (\mathrm{mod}\, p^k)$ mora biti $k = i + 1$, što znači da je $d = \phi(p^k)$.

Teorema. Primitivni koren $(\mathrm{mod}\, n)$ postoji ako i samo ako prirodan broj n ima oblik 2, 4, p^k ili $2p^k$, gde je p neparan prost broj.

Dokaz Jasno je da su 1 i 3 primitivni koreni $(\mathrm{mod}\, 2)$, odnosno, $(\mathrm{mod}\, 4)$. Ako je g primitivni koren $(\mathrm{mod}\, p^k)$, jedan od brojeva g ili $g + p^k$ je neparan, pa je on primitivni koren $(\mathrm{mod}\, 2p^k)$, jer $\phi(2p^k) = \phi(p^k)$. Obratno, ako je $n = n_1 n_2$, gde je $(n_1, n_2) = 1$ i $n_1, n_2 > 2$, onda ne postoje primitivni koreni $(\mathrm{mod}\, n)$ jer, $\phi(n_1)$ i $\phi(n_2)$ su parni, pa

$$a^{\frac{1}{2}\phi(n)} = \left(a^{\phi(n_1)}\right)^{\frac{1}{2}\phi(n_2)} = 1 \pmod{n_1},$$

za svaki prirodan broj a. Slično, $a^{\frac{1}{2}\phi(n)} = 1 \pmod{n_2}$, pa dakle $a^{\frac{1}{2}\phi(n)} = 1 \pmod n$. Takođe, za $k > 2$, indukcijom se dokazuje da je $a^{2^{k-2}} = 1 \pmod{2^k}$, za svaki neparan broj a, pa ne postoje primitivni koreni $(\mathrm{mod}\, 2^k)$, za $k > 2$.

Za dati prost broj p, u konačno mnogo koraka, može se odrediti primitivni koren $(\mathrm{mod}\, p)$. Pritom znamo da za $p > 2$, ostaci oblika $a^2 \pmod p$, (ili kvadratni ostaci), nisu primitivni koreni, a za $p > 3$, ni -1 nije primitivni koren $(\mathrm{mod}\, p)$. Ali, osim ovih jednostavnih izuzetaka i bez neke dublje teorije, ostale moguće vrednosti primitivnih korena moraju se neposredno proveravati. Iako je Gaus razvio čitav niz tehnika za njihovo izračunavanje, kao u slučaju testa prostih brojeva, ne postoji efikasan test za određivanje primitivnih korena.

Konverzija ovog problema je mnogo teža: za dati ceo broj a, odrediti proste brojeve p za koje je broj a primitivni koren $(\mathrm{mod}\, p)$. Veruje se da je svaki ceo broj, različit od -1 i kvadrata celog broja, primitivni koren za beskonačno mnogo prostih brojeva.

Celobrojni logaritam

Ukoliko postoji, primitivni koren $(\bmod n)$ generiše redukovani skup ostataka $(\bmod n)$, pa služi kao baza logaritma $(\bmod n)$. Naime, ako je g primitivni koren $(\bmod n)$, stepeni g^k, $k = 0, 1, \ldots, \phi(n) - 1$ čine redukovani skup ostataka $(\bmod n)$, pa ako je broj a uzajamno prost sa n, postoji jedinstven k takav da $g^k = a \pmod n$. Eksponent k naziva se *indeksom* broja a s obzirom na g i označava sa $\operatorname{ind} a$.

Funkcija $\operatorname{ind} a$ ima sve osobine logaritamske funkcije. Naime, ako su a i b uzajamno prosti sa n,

$$\begin{gathered}\operatorname{ind} a + \operatorname{ind} b = \operatorname{ind} ab \pmod{\phi(n)},\\ \operatorname{ind} a^k = k \operatorname{ind} a \pmod{\phi(n)},\end{gathered}$$

za svako $k \geq 1$. Takođe, $\operatorname{ind} 1 = 0$ i $\operatorname{ind} g = 1$.

Kako je $g^{2 \operatorname{ind}(-1)} = 1 \pmod n$ i $2 \operatorname{ind}(-1) < 2\phi(n)$, to mora biti $\operatorname{ind}(-1) = \phi(n)/2$, za svako $n > 2$.

Ispitaćemo rešenja kongruencije $ax^n = b \pmod p$, gde je $n \geq 1$ i p prost broj.

Kako je $n \operatorname{ind} x = \operatorname{ind} b - \operatorname{ind} a \pmod{(p-1)}$, ako pretpostavimo $(n, p - 1) = 1$ onda

$$\operatorname{ind} x = n^{-1}(\operatorname{ind} b - \operatorname{ind} a) \pmod{(p-1)},$$

pa kongruencija $ax^n = b \pmod p$ ima tačno jedno rešenje $g^{\operatorname{ind} x}$, gde je g primitivni koren $(\bmod p)$.

Ako je $(n, p-1) = d$ i d deli $(\operatorname{ind} b - \operatorname{ind} a)$, kongruencija $ax^n = b \pmod p$ ima tačno d rešenja čiji su indeksi $y_i = y + i(p-1)/d$, gde je $i = 0, \ldots, d-1$ i

$$y = (n/d)^{-1}(\operatorname{ind} b - \operatorname{ind} a)/d \pmod{(p-1)/d}.$$

Konačno, ako broj d ne deli $(\operatorname{ind} b - \operatorname{ind} a)$, kongruencija $ax^n = b \pmod p$ nema rešenje.

Na primer, rešićemo kongruenciju $x^5 = 2 \pmod 7$.

Lako se dobija da je 3 primitivni koren $(\bmod 7)$. Kako je $3^2 = 2 \pmod 7$, imamo da je $\operatorname{ind} 2 = 2$, pa se zbog $5 \operatorname{ind} x = 2 \pmod 7$, dobija da je $\operatorname{ind} x = 4$, što konačno znači da je $x = 3^4 = 4 \pmod 7$ rešenje kongruencije $x^5 = 2 \pmod 7$.

Neka je x redukovani ostatak $(\bmod pq)$, gde su p i q prosti brojevi. Ako je g primitivni koren $(\bmod p)$ i h primitivni koren $(\bmod q)$, onda je

$x = g^m h^n \pmod{pq}$, za neko $m = 0, \ldots, p-1$ i neko $n = 0, \ldots, q-1$. Kako su brojevi m i n jedinstveno određeni, vektor $\operatorname{ind} x = (i, j)$ možemo shvatiti kao *vektorski indeks* broja $x \pmod{pq}$. On ima sva svojstva standardno definisanog indeksa.

Na primer, iako za $k > 2$ ne postoje primitivni koreni $\pmod{2^k}$, broj 5 pripada $2^{k-2} \pmod{2^k}$, pa je svaki neparan broj a kongruentan $(-1)^m 5^n \pmod{2^k}$, za neko $m = 0, 1$ i neko $n = 0, 1, \ldots, 2^{k-2} - 1$. Saglasno prethodnoj oznaci, to znači da je $\operatorname{ind} a = (m, n) \pmod{2^k}$.

Ležandrov simbol

Bavićemo se egzistencijom rešenja kvadratne jednačine $x^2 = a \pmod{n}$, gde je a ceo broj, ali će time biti obuhvaćena i opšta kvadratna kongruencija

$$ax^2 + bx + c = 0 \pmod{n},$$

budući da se ona, smenom $y = 2ax + b$, svodi na kongruenciju $y^2 = d \pmod{4an}$, gde je $d = b^2 - 4ac$.

Neka je $(a, n) = 1$, gde je a ceo broj i $n \geq 1$. Ako kongruencija $x^2 = a \pmod{n}$ ima rešenje, broj a je *kvadratni ostatak* $\pmod{n}$.

Ako je p prost broj i $(a, p) = 1$, *Ležandrov simbol* definišemo tako da

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{ako je a kvadratni ostatak } \pmod{p}, \\ -1 & \text{inače.} \end{cases}$$

Ako je $a = b \pmod{p}$, Ležandrovi simboli celih brojeva a i b su jednaki.

Ojlerov kriterijum. Ako je $p > 2$ prost broj,

$$\left(\frac{a}{p}\right) = a^{\frac{1}{2}(p-1)} \ (mod\, p).$$

Dokaz. Neka je $r = (p-1)/2$. Ako je a kvadratni ostatak $\pmod{p}$, onda postoji $x \geq 1$ takvo da $x^2 = a \pmod{p}$, pa prema Fermatovoj teoremi $a^r = x^{p-1} = 1 \pmod{p}$. Ako a nije kvadratni ostatak, $\pmod{p}$, treba dokazati da je $a^r = -1 \pmod{p}$. Primetimo da redukovani skup ostataka $\pmod{p}$ ima r kvadratnih ostataka $\pmod{p}$, a svaki kvadratni ostatak $\pmod{p}$ je rešenje kongruencije $a^r = 1 \pmod{p}$ koja, prema Lagranžovoj teoremi nema drugih rešenja. Otuda sledi da broj a, koji nije kvadratni ostatak, ne može biti rešenje kongruencije $a^r = 1 \pmod{p}$. Ali, prema Fermatovoj teoremi, $a^{p-1} = 1 \pmod{p}$, pa je $a^r = \pm 1 \pmod{p}$.

Prva posledica Ojlerovog kriterijuma je svojstvo multiplikativnosti Ležandrovog simbola,

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right),$$

za sve a i b koji nisu deljivi prostim brojem p.

Ojlerov kriterijuma daje i karakterizaciju broja -1 kao kvadratnog ostatka $(\bmod p)$

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{1}{2}(p-1)} \pmod p.$$

Dakle, -1 je kvadratni ostatak $(\bmod p)$ ako i samo ako $p = 1 \pmod 4$, za svaki prost broj p. Na osnovu Vilsonove teoreme, ako je $r = (p-1)/2$ i $p = 1 \pmod 4$, rešenja kongruencije $x^2 = -1 \pmod p$ su $x = r!$ i $x = -(r!)$.

Zakon kvadratnog reciprociteta

Do sada smo kompletan ili redukovan sistem klasa ostataka $(\bmod n)$ najčešće izražavali predstavnicima $0, 1, \ldots, n-1$. U narednim razmatranjima, kao predstavnika klase celog broja $a \pmod n$ biramo broj $a' = a \pmod n$ takav da $-n/2 < a' \leq n/2$.

Gausova lema. Ako su prost broj $p > 2$ i ceo broj a uzajamno prosti, $a, 2a, \ldots, (p-1)a/2$ ostaci $(\bmod p)$ i n broj tih ostataka manjih od nule, onda je $\left(\frac{a}{p}\right) = (-1)^n$.

Dokaz. Neka je $r = (p-1)/2$. Kako predstavnike klasa $(\bmod p)$ biramo iz skupa celih brojeva između $-p/2$ i $p/2$, to je $1 \leq |ak| \leq r$, za sve $k = 1, \ldots, r$, pa je svaki broj $|ak|$, neki od brojeva $1, 2, \ldots, r$. Pritom, svi $|ak|$ su različiti $(\bmod p)$ jer, ako $ai = -aj \pmod p$, onda $0 < i + j < p$, što nije moguće zbog $(a, p) = 1$, a ako je $ai = aj \pmod p$, onda $i = j$. Otuda sledi da je $a \cdot 2a \cdots ra = (-1)^n r!$, odnosno, $a^r r! = (-1)^n r! \pmod p$, što konačno znači da je $a^r = (-1)^n \pmod p$.

Nekada se smatralo da je zakon kvadratnog reciprociteta centralni rezultat aritmetike. Formulisao ga je Ojler, a dokazao Gaus u svom glavnom delu Disquisitiones arithmeticae. Zapravo, Gaus je taj zakon dokazao na osam različitih načina.

Zakon kvadratnog reciprociteta: Ako su p i q različiti neparni prosti brojevi,

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{1}{4}(p-1)(q-1)}.$$

Drugačije rečeno, ako je bar jedan od brojeva p i q nije kongruentan 3 $(\bmod 4)$,

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right),$$

a u ostalim slučajevima

$$\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right).$$

Gausov dokaz. Koristimo pretpostavke Gausove leme. Za svaki ceo broj x, ako je $0 < x < q/2$, postoje celi brojevi y i r takvi da je $px = qy + r$. Prema Gausovoj lemi, $\left(\frac{p}{q}\right) = (-1)^k$, gde je k broj ostataka $r = px - qy$ takvih da je $r < 0$. To znači da je k broj tačaka (x, y) koje zadovoljavaju uslove: $0 < x < \frac{1}{2}q$ i $-\frac{1}{2}q < px - qy < 0$. Otuda sledi da je $y < px/q + 1/2 < (p+1)/2$, pa kako je y ceo broj, to znači da je $0 < y < p/2$.

Dakle, sve tačke (x, y) pripadaju pravougaoniku $P = \{(x, y) : 0 < x < q/2,\ 0 < y < p/2\}$, a k je broj elemenata skupa $P_1 \subseteq P$, koji se sastoji od tačaka (x, y) takvih da važi uslov $-q/2 < px - qy < 0$. Slično, $\left(\frac{q}{p}\right) = (-1)^m$, gde je m broj elemenata skupa $P_2 \subseteq P$, koji se sastoji od tačaka (x, y) takvih da važi uslov $-p/2 < qy - px < 0$.

Treba još dokazati da je broj $s = (p-1)(q-1)/2 - (k+m)$ paran. Međutim, s je broj tačaka pravougaonika P koje nisu u P_1 ili nisu u P_2, odnosno, koje pripadaju $P_1^c \cup P_2^c$. Kako skupu P_1^c pripadaju tačke koje zadovoljavaju uslov $px - qy \leq -q/2$, a skupu P_2^c tačke za koje važi uslov $qy - px \leq -p/2$, skupovi P_1^c i P_2^c su disjunktni. Međutim, kako je transformacija $x = (q+1)/2 - x'$, $y = (p+1)/2 - y'$ obostrano jednoznačna i prevodi skupove P_1^c i P_2^c jedan u drugi, broj s mora biti paran.

Zakon kvadratnog reciprociteta sasvim pojednostavljuje račun sa Ležandrovim simbolima.

Na primer

$$\left(\tfrac{15}{71}\right) = -\left(\tfrac{71}{3}\right)\left(\tfrac{71}{5}\right) = -\left(\tfrac{2}{3}\right)\left(\tfrac{1}{5}\right) = 1.$$

Slično, za svaki prost broj $p > 2$,

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = (-1)^{(p-1)/2}\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right),$$

što znači da je -3 kvadratni ostatak za sve proste brojeve $p = 6n + 1$, a nije kvadratni ostatak ako je $p = 6n + 5$.

Jakobijev simbol

Jedno od mogućih uopštenja Ležandrovog simbola na pozitivne neparne brojeve definisao je Karl Gustav Jakov Jakobi (1804. – 1851.).

Ako je $n = p_1 \cdots p_k$ pozitivni neparan broj i $(a, n) = 1$, *Jakobijev simbol* definisan je tako da

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right) \cdots \left(\frac{a}{p_k}\right),$$

gde su faktori na desnoj strani Ležandrovi simboli. Pritom za $n = 1$, Jakobijev simbol je 1, a po definiciji nula, za $(a, n) > 1$.

Teorema. Ako je $a = a'$ $(\mathrm{mod}\, n)$, Jakobijevi simboli celih brojeva a i a' su jednaki.

Primetimo da $\left(\frac{a}{n}\right) = 1$ ne znači da je broj a kvadratni ostatak $(\mathrm{mod}\, n)$. Na primer $\left(\frac{2}{9}\right) = 1$, ali kongruencija $x^2 = 2 \pmod 9$ nema rešenja.

Teorema. Celi broj a je kvadratni ostatak $(\mathrm{mod}\, n)$ ako i samo ako a je kvadratni ostatak $(\mathrm{mod}\, p)$, za svaki prost delitelj broja n.

Teorema. Ako je $\left(\frac{a}{n}\right) = -1$, ceo broj a nije kvadratni ostatak $(\mathrm{mod}\, n)$.

Teorema. Ako su m i n pozitivni neparni brojevi, a p i q celi brojevi i $(pq, mn) = 1$, ondaje redom

$$\left(\frac{p}{m}\right)\left(\frac{p}{n}\right) = \left(\frac{p}{mn}\right), \ \left(\frac{p}{m}\right)\left(\frac{q}{m}\right) = \left(\frac{pq}{m}\right).$$

Teorema. Ako je $q > 0$ neparan broj,

$$\left(\frac{-1}{q}\right) = (-1)^{(q-1)/2}, \ \left(\frac{2}{q}\right) = (-1)^{(q^2-1)/8}.$$

Dokaz. Prema definiciji i svojstvima Jakobijevog simbola,

$$\left(\frac{-1}{q}\right) = \prod_{i=1}^{s} \left(\frac{-1}{q_i}\right) = \prod_{i=1}^{s} (-1)^{(q_i-1)/2} = (-1)^{\sum (q_i-1)/2}.$$

Otuda, višestrukom primenom kongruencije

$$(a-1)/2 + (b-1)/2 = (ab-1)/2 \pmod 2,$$

gde su a i b celi brojevi, dobija se

$$\sum_{i=1}^{s} \frac{(q_i-1)}{2} = \frac{1}{2}\left(\prod_{i-1}^{s} q_i - 1\right) = \frac{q-1}{2} \pmod 2.$$

Takođe, višestrukom primenom kongruencije

$$(a^2-1)/8 + (b^2-1)/8 = (a^2b^2-1)/8 \pmod 2$$

i primenom osobina Jakobijevih i Ležandrovih simbola, dobija se da važi relacija $\left(\frac{2}{q}\right) = (-1)^{(q^2-1)/8}$.

Zakon kvadratnog reciprociteta: Ako su p i q pozitivni neparni brojevi i $(p, q) = 1$,

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{1}{4}(p-1)(q-1)}.$$

Dokaz. Dokaz se svodi na višestruku primenu kongruencija navedenih u dokazu prethodne teoreme.

Prethodna definicija Jakobijevog simbola motivisana je zakonom kvadratnog reciprociteta. Naime, moglo bi se reći da bi prirodnije proširenje Ležandrovog simbola bio simbol $\left(\frac{a}{n}\right)$ koji ima vrednost 1 ako je a kvadratni ostatak, odnosno, (-1) ako a nije kvadratni ostatak $(\bmod n)$. Ali u tom slučaju ne bi važio zakon kvadratnog reciprociteta. Na primer, za $p = 5$ i $q = 9$. Veza sa kvadratnim ostacima napuštena je u korist zakona kvadratnog reciprociteta.

Linearna permutacija

Definicija Jakobijevog simbola ima svoje opravdanje i u njegovoj vezi sa linearnim permutacijama skupa ostataka $(\bmod n)$. Taj pristup omogućava da se zakon kvadratnog reciprociteta dokaže postupkom koji se bitno razlikuje od Gausovog. Dokaz je veoma zanimljiv, a dugujemo ga ruskom matematičaru Jegoru Ivanoviču Zalatarjevu (1847. – 1878.).

Ako je m neparan prirodan broj i a ceo broj uzajamno prost sa n, preslikavanje $\pi(x) = ax \pmod m$ je *linearna permutacija* kompletnog skupa ostataka $(\bmod m)$. Ako je $\operatorname{sgn}(\pi)$ znak permutacije π, Jakobijev simbol je

$$\left(\frac{a}{m}\right) = \operatorname{sgn}(\pi).$$

Pritom, znak permutacije $\pi(x) = ax + b \pmod m$ je takođe $\left(\frac{a}{m}\right)$, budući da se u tom slučaju permutacija π svodi na b-ti stepen parne permutacije $(0, 1, \ldots, m-1)$.

Teorema. Jakobijev simbol, u smislu prethod ne definicije, zadovoljava zakon kvadratnog reciprociteta

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{\frac{1}{4}(m-1)(n-1)},$$

gde su m i n neparni uzajamno prosti prirodni brojevi.

Dokaz. Definišimo preslikavanje $*$ skupa P ostataka $(\bmod mn)$ i skupa $Q = \{(x,y) : 0 \leq x < m, 0 \leq y < n\}$ tako da za svako $x \in P$, $x^* = (x \bmod m, x \bmod n)$.

S obzirom na Kinesku teoremu o ostacima, $*$ je uzajamno jednoznačno preslikavanje skupa P na skup Q.

Razmotrićemo permutacije μ i ν skupa Q koje su zadate sledećim relacijama $\mu(x,y) = (x+my)^*$ i $\nu(x,y) = (nx+y)^*$.

Kako je $\nu(x,y) = (nx + y \bmod m, y)$, za fiksirano y, permutacija ν svodi se na linearnu permutaciju kompletnog skupa ostataka $(\bmod m)$, pa je $\operatorname{sgn}(\nu) = \left(\frac{n}{m}\right)^n = \left(\frac{n}{m}\right)$. Na isti način, μ je permutacija skupa Q čiji je znak $\left(\frac{m}{n}\right)$, pa je

$$\operatorname{sgn}(\nu^{-1}\mu) = \left(\tfrac{n}{m}\right)\left(\tfrac{m}{n}\right).$$

Sa druge strane, $\nu^{-1}\mu$ je permutacija

$$(nx+y)^* \longmapsto (x+my)^*,$$

pa budući da je $*$ bijekcija, znak permutacije $\nu^{-1}\mu$ je $(-1)^k$, gde je k broj parova (x,y) i (x',y') skupa Q za koje važe nejednakosti

$$nx + y > nx' + y' \text{ i } x + my < x' + my'.$$

Budući da je $|x - x'| < m$ i $|y - y'| < n$, dobijamo da je k broj parova (x,y) i (x',y') skupa Q za koje važe nejednakosti $x > x'$ i $y < y'$.

Takvih parova ima $\binom{m}{2}\binom{n}{2}$, pa se konačno dobija da je $k = \frac{1}{4}(m-1)(n-1) \pmod 2$.

Teorema. Jakobijev simbol je multiplikativan.

Dokaz. Neka su a i b celi brojevi uzajamno prosti sa neparnim prirodnim brojem n. Ako je $\pi_c(x) = ax \pmod n$, gde je c ceo broj uzajamno prost sa n, neposredno se dobija da je $\operatorname{sgn}(\pi_a b) = \operatorname{sgn}(\pi_a)\operatorname{sgn}(\pi_b)$. što znači da je $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$.

Teorema. Ako je prirodan broj m neparan,

$$\left(\tfrac{2}{m}\right) = (-1)^{(m^2-1)/8}.$$

Dokaz. Ako je prirodan broj m neparan, primenom zakona o kvadratnom reciprocitetu i koristeći multiplikativnost, redom imamo da je $\left(\frac{2}{m}\right) = \left(\frac{-1}{m}\right)\left(\frac{m-2}{m}\right) = \left(\frac{-1}{m}\right)\left(\frac{m}{m-2}\right) = (-1)^{(m-1)/2}\left(\frac{2}{m-2}\right)$. Otuda se indukcijom dobija da je $\left(\frac{2}{m}\right) = (-1)^{(m^2-1)/8}$.

Teorema. Jakobijev simbol je multiplikativan i po donjem argumentu, tj. zadovoljava jednakost

$$\left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right)\left(\frac{b}{n}\right),$$

gde su m i n neparni prirodni brojevi i a ceo broj takav da je $(a, m) = (a, n) = 1$.

Dokaz. Izaberimo broj $r > 0$ oblika $4k + 1$ takav da je $r = a \pmod{mn}$. Taj izbor je moguć budući da je $(a, mn) = 1$. Sada, na osnovu zakona o kvadratnom reciprocitetu redom imamo: $\left(\frac{a}{mn}\right) = \left(\frac{r}{mn}\right) = \left(\frac{mn}{r}\right) = \left(\frac{m}{r}\right)\left(\frac{n}{r}\right) = \left(\frac{r}{m}\right)\left(\frac{r}{n}\right) = \left(\frac{a}{m}\right)\left(\frac{a}{n}\right)$.

Na osnovu prethodnog pravila sledi jednakost prvobitno definisanog standardnog Jakobijevog simbola i Jakobijevog simbola definisanog preko linearnih permutacija, uz uslov da se ovaj drugi, za neparan prost broj, svodi na Ležandrov simbol.

Teorema Zalatarjeva. Ako je $p > 2$ prost broj, a ceo broj uzajamno prost sa p i π linearna permutacija određena brojem a, onda je $\operatorname{sgn}(\pi) = \left(\frac{a}{p}\right)$, gde je $\left(\frac{a}{p}\right)$ Ležandrov simbol.

Dokaz. Neka je $f(x_1, \ldots, x_p) = \prod_{i<j}(x_i - x_j)$. Neparna permutacija promenljivih menja znak polinoma f, a parna ne menja, pa je znak permutacije π jednak količniku $f(x_{\pi(1)}, \ldots, x_{\pi(p)})$ i $f(x_1, \ldots, x_p)$.

Ako je $x_1 = 1, \ldots, x_p = p$ onda

$$\begin{aligned} \operatorname{sgn}(\pi) &= \prod_{i<j} \frac{\pi(i)-\pi(j)}{i-j} = \prod_{i<j} \frac{ai-aj}{i-j} \\ &= \prod_{i<j} a = a^{p(p-1)/2} \pmod{p}. \end{aligned}$$

Otuda, prema maloj Fermatovoj teoremi i Ojlerovom kriterijumu, $\operatorname{sgn}(\pi) = a^{(p-1)/2} = \left(\frac{a}{p}\right) \pmod{p}$, što dokazuje tvrđenje.

Test primalnosti

U mnogim okolnostima neophodno je utvrditi da li je dati prirodan broj prost. Na primer, u kriptosistemima sa javnim ključem potrebno je odrediti veliki slučajan prost broj. To može da znači da treba izabrati veliki neparan slučajan broj n_0, koristeći generator slučajnih cifara, a zatimi testirati primalnost brojeva n_0, $n_0+2, \ldots$ sve dok se ne dobije prvi prost broj veći od n_0. Druga okolnost u kojoj se takva potreba javlja jeste kada treba proveriti, za neki veliki prost broj p, da li je Mersenov broj $2^p - 1$ prost.

Test primalnosti je zapravo kriterijum da prirodan broj nije prost. Ako prođe test primalnosti, prirodan broj je moguće prost, a ako ne prođe, on

je definitivno složen broj. Ovo poslednje otvara veoma teško pitanje utvrđivanja prostih faktora: u opštem slučaju znatno je teže faktoristati prirodan broj određenog reda veličine, nego pronaći prost broj istog reda veličine. (Ovo je empirijsko tvrđenje, a ne teorema – bar za sada.)

Eratostenovo sito: Svakako, najstariji test primalnosti je Eratostenovo sito. Prirodan broj n je prost ako posle svih $[\sqrt{n}]$ prosejavanja ostane u situ. Intuitivno, posle svakog prosejavanja, ako preostane u situ, verovatnoća da je n prost broj raste. Kako koristi mnogo prostora i vremena računara, ovaj test nije praktičan i uglavnom se ne koristi, ali ipak nije sasvim napušten. U poslednje vreme, ideja sita i njena uopštenja koriste se za prosejavanje prirodnih brojeva koji zadovoljavaju neke dodatne uslove koji sito čine znatno efikasniji. Razvijeni su specijalni mikroprocesori koji prilično brzo prosejavaju prirodne brojeve.

Vilsonov kriterijum: Podsetimo se, po Vilsonovoj teoremi, prirodan broj n je prost ako i samo ako zadovoljava relaciju $(n-1)! = -1 \pmod{n}$. U teoriji brojeva ovaj kriterijum ima veliki značaj, ali je njegova primena u proveri primalnosti prirodnih brojeva zanemarljiva.

Test na osnovu Fermatove teoreme: Ako je n prost broj, za svako $a \in \{1, 2, \ldots, n-1\}$, $a^{n-1} = 1 \pmod{n}$, ali ne obratno, tj. postoje složeni brojevi za koje je $a^{n-1} = 1 \pmod{n}$, za pojedine ili čak sve $a \in \{1, 2, \ldots, n-1\}$.

Zapravo, kao test ne koristimo Fermatovu teoremu, već njenu kontrapoziciju: ako postoji $a \in \{1, 2, \ldots, n-1\}$ za koje je $a^{n-1} \neq 1 \pmod{n}$, onda je n složen broj. Ona daje sledeći verovatnosni test primalnosti:

1. Na slučaj biramo broj a iz skupa $\{1, 2, \ldots, n-1\}$.
2. Euklidovim algoritmom izračunavamo (a, n).
3. Ako je $(a, n) \neq 1$, broj n je složen i test je završen.
4. Ako je $(a, n) = 1$, proveravamo relaciju $a^{n-1} = 1 \pmod{n}$.
5. Ako je $a^{n-1} \neq 1 \pmod{n}$, broj n je složen i test je završen.
6. Ako je $a^{n-1} = 1 \pmod{n}$, rezultat nije izvestan i test se može ponoviti.

Ako prirodan broj n zadovoljava relaciju $a^{n-1} = 1 \pmod{n}$, kažemo da je *n pseudoprost za osnovu a*. Na primer, u sledećim parovima (a, n), prirodan broj n je pseudoprost za osnovu a: $(2, 341)$, $(3, 91)$, $(5, 217)$ i $(7, 25)$. Pritom, navedeni su najmanji pseudoprosti brojevi redom za osnove $2, 3, 5$ i 7.

Primetimo da postoji beskonačno mnogo parova (a, n), gde je n složen broj i pseudoprost za osnovu a.

Na primer, ako par $(2, n)$ zadovoljava relaciju $2^{n-1} = 1 \pmod{n}$, onda par $(2, 2^n - 1)$ takođe zadovoljava istu relaciju.

Naime, ako je $2^{n-1} = 1 \pmod n$, onda $2^n - 2 = 2(2^{n-1} - 1) = 2qn$, za neki prirodan broj q, pa je

$$2^{2^n-2} - 1 = 2^{2nq} - 1 = (2^n - 1)(2^{n(2q-1)} + \cdots + 1) = 0 \pmod{(2^n - 1)}.$$

Pritom, ako je n složen broj, onda je broj $2^n - 1$ takođe složen, pa dakle ima beskonačno mnogo pseudoprostih brojeva za osnovu 2.

Za $a > 2$, koristimo sledeći rezultat: za svaki prost broj $p > 2$ i svaki ceo broj a, ako je $(a^2 - 1, p) = 1$, broj $\frac{a^{2p}-1}{a^2-1}$ je pseudoprost za osnovu a.

Iako ih ima beskonačno mnogo, pseudoprosti brojevi su veoma retki u skupu prirodnih brojeva. Na primer, poznato je da u prvih 25 milijardi prirodnih brojeva ima 1 091 987 405 prostih i svega 21 853 pseudoprostih brojeva za osnovu 2.

Tvrđenje 1. Neka n neparan prirodan broj, $Z_n = \{0, 1, \ldots, n-1\}$ prsten ostataka $(\bmod n)$ i $Z_n^* = \{1, \ldots, n-1\}$ multiplikativna grupa prstena Z_n.

(i) Broj n je pseudoprost za osnovu a ako i samo ako $(a, n) = 1$ i red elementa a deli $n - 1$.

(ii) Ako je n pseudoprost po osnovama $a, b \in Z_n^*$, onda je n pseudoprost po osnovama ab i ab^{-1}.

(iii) Skup $G_n = \{a \in Z_n : a^{n-1} = 1 \pmod n\}$ je podgrupa grupe Z_n^*.

(iv) Ako postoji bar jedno $a \in Z_n^*$ takvo da broj n nije pseudoprost za osnovu a, onda je $|G_n| \leq \frac{1}{2}|Z_n^*|$.

Dokaz: Tvrđenja (i), (ii) i (iii) su očigledna. Ako broj n nije pseudoprost za osnovu a, grupa G_n je prava podgrupa grupe Z_n^*, pa indeks grupe Z_n^* po podgrupi G_n nije manji od 2. $\lhd$

Iz prethodnog tvrđenja sledi da ako postoji bar jedno $a \in Z_n^*$ takvo da broj n nije pseudoprost za osnovu a, onda postoji bar $(n-1)/2$ brojeva $b \in Z_n^*$ takvih da n nije pseudoprost za osnovu b.

Prirodan broj n je *pseudoprost* broj ili *Karmajklov* broj ako za svako $a \in Z$, $(a, n) = 1$, zadovoljava relaciju $a^{n-1} = 1 \pmod n$.

Sada možemo zaključiti da se u svakom koraku izloženog testa primalnosti mogu pojaviti sledće tri okolnosti:

– ako je n prost broj, test uvek daje odgovor "nije izvesno,"

– ako je n složen i nije pseudoprost broj, sa verovatnoćom koja nije manja od 1/2, test daje odgovor "n je složen broj,"

– ako je n složen pseudoprost broj, test uvek daje odgovor "nije izvesno."

Jasno je da treća mogućnost nije dobro svojstvo ovog testa, odnosno, u primenama su neophodni testovi u kojima se takva mogućnost ne pojavljuqje. Pre nego što izložimo jedan takav test, razmotrićemo neka svojstva pseudoprostih brojeva.

Teorema 1. Neka je n složen neparan prirodan broj. Ako $p^2|n$, gde je $p > 2$ prost broj, broj n nije pseudoprost.

Dokaz: Pretpostavimo da $p^2|n$ i neka je g primitivni koren $(\bmod p^2)$. Kako je $\varphi(p^2) = p(p-1)$, to znači da je $p(p-1)$ red broja g $(\bmod p^2)$. Neka je n' proizvod svih prostih faktora broja n različitih od p. Prema kineskoj teoremi, postoji b takvo da $b = g$ $(\bmod p^2)$ i $b = 1$ $(\bmod n')$. Pritom, kao i g, broj b je primitivni koren $(\bmod p^2)$ i zadovoljava uslov $(b, n) = 1$ jer nije deljiv sa p, niti bilo kojim drugim porostim faktorom broja n.

Tvrdimo da broj n nije pseudoprost za osnovu b. Naime, ako važi relacija $b^{n-1} = 1$ $(\bmod n)$, kako $p^2|n$, imamo da je $b^{n-1} = 1$ $(\bmod p^2)$, što znači da $p(p-1)|(n-1)$, jer $p(p-1)$ je red broja b $(\bmod p^2)$. Međutim, kako $p|n$, $n - 1 = -1$ $(\bmod p)$, a to znači da broj $n - 1$ nije deljiv sa $p(p-1)$. Dakle, postoji osnova za koju broj n nije pseudoprost. $\lhd$

Teorema 2. Neka je $n = p_1 p_2 \cdots p_k$, $p_i \neq p_j$, neparan broj. Broj n je pseudoprost ako i samo ako $(p_i - 1)|(n-1)$, za svako $i = 1, \ldots, k$.

Dokaz: Neka je $n = p_1 p_2 \cdots p_k$, $p_i \neq p_j$, neparan broj i $(p_i - 1)|(n-1)$, za svako $i = 1, \ldots, k$. To znači da postoji m_i takvo da $n - 1 = (p_i - 1)m_i$, za svako $i = 1, \ldots, k$. Otuda, za svaku osnovu a imamo da je $a^{n-1} = a^{(p_i-1)m_i} = 1$ $(\bmod p_i)$, pa prema Kineskoj teoremi imamo da je $a^{n-1} = 1$ $(\bmod n)$, tj. broj n je pseudoprost.

Obratno, pretpostavimo da je n pseudoprost broj. Za svako $i = 1, \ldots, k$, neka je a_i primtivni koren $(\bmod p_i)$. Onda iz uslova $a_i^{n-1} = 1$ $(\bmod n)$ sledi da $(p_i - 1)|(n-1)$, za sve $i = 1, \ldots, k$. $\lhd$

Teorema 3. Svaki složen pseudoprost broj je proizvod najmanje tri različita prosta broja.

Dokaz: Ako je $n = p\,q$, gde su $p < q$ različiti neparni prosti brojevi, onda je $n - 1 = p(q - 1 + 1) - 1 = p - 1$ $(\bmod (q-1))$, pa kako je $0 < p - 1 < q - 1$, to protivreči uslovu $(q-1)|(n-1)$ iz prethodne teoreme. $\lhd$

Pseudoprosti brojevi su sasvim retki. U prvih 25 milijardi prirodnih brojeva ima svega 2136 psedudoprostih. Najmanji takav broj je $561 = 3 \cdot 11 \cdot 17$. Tek nedavno, 1992. godine, ustanovljeno je da ima beskonačno mnogo pseudoprostih brojeva (Alford, Granville, Pomerance).

Teorema 4. Pretpostavimo da je n neparan prirodan broj. Broj n je prost ako i samo ako za svaki ceo broj a, $(a,n)=1$,

$$a^{\frac{n-1}{2}} = \left(\frac{a}{n}\right) \pmod{n}.$$

Dokaz: Ako je n prost broj, tvrđenje važi na osnovu Ojlerovog kriterijuma. Pretpostavimo da važi relacija $a^{\frac{n-1}{2}} = \left(\frac{a}{n}\right) \pmod{n}$, gde je $(a,n)=1$, ali da n nije prost broj. Onda je

$$a^{n-1} = \left(a^{\frac{n-1}{2}}\right)^2 = \left(\frac{a}{n}\right)^2 = 1 \pmod{n},$$

pa je n pseudoprost broj i mora imati oblik $n = p_1 p_2 \cdots p_k$, $p_i \neq p_j$. Neka je b ceo broj koji nije kvadratni ostatak $(\operatorname{mod} p_1)$. Po Kineskoj teoremi, postoji ceo broj a takav da je

$$\begin{aligned} a &= b \pmod{p_1}, \\ a &= 1 \pmod{p_2}, \\ &\cdots \\ a &= 1 \pmod{p_k}. \end{aligned}$$

Na osnovu svojstava Jakobijevog simbola, broj a zadovoljava jednakost

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\cdots\left(\frac{a}{p_k}\right) = \left(\frac{a}{p_1}\right) = \left(\frac{b}{p_1}\right) = -1,$$

pa kako, po pretpostavci $a^{\frac{n-1}{2}} = \left(\frac{a}{n}\right) \pmod{n}$, to mora biti $a^{\frac{n-1}{2}} = \left(\frac{a}{n}\right) = -1 \pmod{p_2}$, a to protivreči izboru broja a, koji zadovoljava uslov $a = 1 \pmod{p_2}$. $\lhd$

Neka je n prirodan broj. Ako $a^{\frac{n-1}{2}} = \left(\frac{a}{n}\right) \pmod{n}$, za neki ceo broj a takav da $(a,n)=1$, onda je n *Ojlerov pseudoprost broj za osnovu* a. Na osnovu prethodne teoreme, analogon pseudoprostih ili Karmajklovih brojeva u Ojlerovom smislu ne postoji, tj. ne postoji broj koji je Ojlerov pseudoprost i koji je takav za svaku osnovu.

Solovej-Štrasenov test: Koristeći prethodnu teoremu, 1977. godine, Solovej i Štrasen formulisali su sledeći test primalnosti:

1. Na slučaj biramo broj a iz skupa $\{1, 2, \ldots, n-1\}$.
2. Euklidovim algoritmom izračunavamo (a,n).
3. Ako je $(a,n) \neq 1$, broj n je složen i test je završen.
4. Ako je $(a,n)=1$, proveravamo relaciju $a^{\frac{n-1}{2}} = \left(\frac{a}{n}\right) \pmod{n}$.
5. Ako je $a^{\frac{n-1}{2}} \neq \left(\frac{a}{n}\right) \pmod{n}$, broj n je složen i test je završen.

6. Ako je $a^{\frac{n-1}{2}} = \left(\frac{a}{n}\right) \pmod{n}$, rezultat nije izvestan i test se može ponoviti.

Iako u svemu slični (složenost im je ista) prednost ovog testa u odnosu na test zasnovan na maloj Fermatovoj teoremi jeste u tome što se sada u svakom njegovom koraku mogu javiti samo dve okolnosti:

– ako je n prost broj, test uvek daje odgovor "nije izvesno,"

– ako je n složen, sa verovatnoćom koja nije manja od $1/2$, test daje odgovor "n je složen broj."

Posle k koraka Solovej-Štrasenovog testa, verovatnoća da test propusti složen broj nije veća od $1/2^k$. Dokaz ove ocene sledi neposredno iz sledećeg tvrđenja, koje je analogno tvrđenju datom u slučaju testa primalnosti zasnovanog na maloj Fermatovoj teoremi.

Tvrđenje 2. Neka su a i b celi brojevi takvi da je $(a, n) = (b, n) = 1$, gde je n neparan prirodan broj. Sa Z_n označavamo (prsten) skup ostataka $\pmod{n}$, a sa Z_n^* multiplikativnu grupu prstena Z_n.

(i) Ako je n Ojlerov pseudoprost broj za osnovu a onda je n pseudoprost broj za osnovu a.

(ii) Ako je n Ojlerov pseudoprost broj po osnovama a i b, onda n Ojlerov pseudoprost broj po osnovama ab i ab^{-1}.

(iii) Skup $E_n = \{a \in Z_n : a^{\frac{n-1}{2}} = \left(\frac{a}{n}\right) \pmod{n}\}$ je podgrupa grupe Z_n^*.

(iv) Ako postoji bar jedno $a \in Z_n^*$ takvo da broj n nije pseudoprost za osnovu a, onda je $|E_n| \leq \frac{1}{2}|Z_n^*|$.

Dokaz: Ako je prirodan broj n Ojlerov pseudoprost broj za osnovu a, onda je $a^{\frac{n-1}{2}} = \left(\frac{a}{n}\right) \pmod{n}$, pa se kvadriranjem obe strane te relacije dobija da je $a^{n-1} = 1 \pmod{n}$, tj. n je pseudoprost broj za osnovu a, pa važi tvrđenj (i). Sva preostala tvrđenja su očigledna. $\triangleleft$

Uvod u kriptografiju

Kriptografija se bavi izučavanjem metoda sigurne razmene poruka. Manje nadobudno rečeno, to je veština pisanja i čitanja skrivenih poruka. Pritom, piše se standardnim slovima i simbolima čije je značenje izmenjeno, tako da se sadržaj zapisa ne može lako, ili ne može uopšte, pročitati bez odgovarajućeg ključa. Ključ obezbeđuje sigurnost razmene poruka, odnosno, onemogućava neovlašćene subjekte da u toj razmeni učestvuju. Centralno pitanje u kriptografiji jeste: do kog stepena je takva sigurnost ostvariva.

Do nedavno, usluge kriptografa (koji stvaraju kriptografske protokole) i kriptoanalitičara (koji nastoje da pronađu slabosti tih protokola) naručivala je uglavnom država, ali se sa razvojem interneta krug korisnika takvih usluga jako proširio. Pojavili su se novi kriptografski protokoli i suštinski se promenio klasični pristup sigurnoj razmeni poruka.

Kriptografski sistem

U opisu kriptografskog sistema nužno pretpostavljamo sasvim apstraktan, idealizovan model za koji verujemo da je dovoljno sveobuhvatan da pokrije sve okolnosti koje se mogu javiti u stvarnosti. Da bi smo pojednostavili izražavanje i lakše formulisali različite scenarije koji se javljaju u kriptografiji, uvešćemo jedan broj likova (to nisu karakteri) sa određenom ulogom u procesu razmene poruka.

Glavni likovi u kriptografskom scenariju su Alisa, Bob i Eva. Alisa i Bob razmenjuju tajne poruke. Najčešće, Alisa šalje poruku. Eva je analitičar koji posmatra razmenu poruka (ne može neposredno da utiče na njihov sadržaj) i nastoji da ih pročita. Ako drugačije ne naglasimo, isti scenario podrazumevaćemo u svim kriptografskim protokolima.

Svakako, postoje i drugi scenariji, sa drugim likovima i, kako se internet

razvija i širi njegova upotreba, biće ih sve više. Na primer, da bi se uverio u njenu autentičnost, Bob može da zahteva da poruka bude potpisana tako da Alisa ne može da osporava da je poruka zaista njena. Takođe, može se zamisliti da Eva nastoji da falsifikuje Alisin potpis ili da nastoji da izmeni sadržaj poruka. Postoje i scenariji u kojima se javlja centralni administrativni autoritet koji može da ima različite uloge, na primer, da izdaje digitalne sertifikate za identifikaciju itd.

Alisa *kriptuje* poruku M tako što, koristeći *kriptujuću funkciju* e, konstruiše *kriptogram* $C = e(M)$. Kriptogram C dostavlja Bobu koji, koristeći *dekriptujuću funkciju* d, rekonstruiše poruku $M = d(C)$. Eva u principu zna funkcije e i d i dostupni su joj kriptogrami, ali joj nije dostupan *ključ* K, bez koga dekripcija nije jednostavna ili nije uopšte moguća.

Kada, znajući samo funkcije e i d i kriptograme, pokušava da otkrije ključ, Eva izvodi *čisti napad* na kriptografski sistem. Ako je Evi dostupan i izvestan broj poruka i kriptograma, ona vrši *napad na poruku*, odnosno, ako je na neki način uspela da sama odabere poruke i njihove kriptograme koje analizira, Eva vrši *napad na izabranu poruku*.

Bob uvek zna ključ, a do pred kraj dvadesetog veka, u svim kriptografskim sistemima ključ je morala da zna i koristi i Alisa. Kriptografski sistemi sa takvim svojstvom nazivaju se *simetričnim*. Međutim, najveći napredak u kriptografiji jeste otkriće da kriptografski sistem ne mora biti simetričan, a da istovremeno može biti pouzdan i praktično upotrebljiv. Kriptografski sistemi u kojima samo Bob zna ključ poznati su kao *sistemi sa javnim ključem*.

Na prvi pogled, podela kriptografskih sistema na klasične i savremene izgleda sasvim tehnička. Međutim, ona je ipak suštinska i sastoji se u različitim pristupima problemu *sigurnosti* kriptografskog sistema.

Istorisjki, definiciju sigurnosti kriptografskog sistema postavio je Šenon 1949. godine: *sigurnost* kriptografskog sistema određena je količinom informacija koje kriptogram nosi o poruci ili o ključu. Pritom, on je pretpostavio da

Čovekova moć izračunavanja nije ograničena.

U klasičnom kriptografskom sistemu, Alisa i Bob nastoje da ograniče *informaciju* koju Eva, na osnovu uvida u jedan broj parova poruka i kriptograma i sa neograničenom moći izračunavanja, može dobiti o njihovim budućim porukama i ključu. Pod tim pretpostavkama, Šenon je uspeo da dokaže da postoje *savršeno sigurni* kriptografski sistemi, tj. sistemi u kojima kriptogrami ne nose nikakvu informaciju o porukama. Međutim, on je istovremeno dokazao da savršen sistem nužno ima jednu praktičnu manu:

da bi bio savršeno siguran, neophodno je da kriptografski sistem ima ključ koji je duži od poruke.

Sa druge strane, savremeni kruptografski sistemi sigurnost zasnivaju na pretpostavci da

Čovekova moć izračunavanja jeste ograničena.

Informacija koju parovi poruka i kriptograma nose o budućim porukama i ključu postoji, ali Evi nije praktično dostupna zbog apsolutnih ograničenja čovekovih računskih mogućnosti. Zapravo, osnovu moderne kriptografije čini matematička teorija složenosti.

Primer 1. Pretpostavimo da Alisa šalje niz od n poruka, $n \geq 1$, koje se sastoje od jednog znaka iz skupa $\{0, 1\}$. Bacajući novčic, Alisa i Bob su generisali slučajan niz $K \in \{0, 1\}^n$, koji koriste kao ključ kriptografskog sistema. Alisa kriptuje poruke $M_1, M_2, \ldots, M_n$ na sledeći način:

$$C_i = e(M_i) = M_i +_2 K_i,$$

gde je $+_2$ sabiranje po modulu 2. Koristeći isti ključ, Bob lako dekriptuje:

$$M_i = d(C_i) = C_i +_2 K_i.$$

Pretpostavimo da Eva zna svih $n - 1$ parova poruka i kriptograma

$$(M_1, C_1), (M_2, C_2), \ldots, (M_{n-1}, C_{n-1}).$$

Ako zna kriptogram C_n, šta može da zaključi o poruci M_n? Kako je K_n dobijen na slučajan način, jednako su verovatne mogućnosti $M_n = C_n$ i $M_n = C_n +_2 1$. To znači da prethodnih $n - 1$ parova (M_i, C_i), $i < n$, kao i kriptogram C_n, ne nose nikakvu informaciju o poruci C_n.

Zadatak 1. Kako se menja sigurnost prethodnog kriptografskog sistema ako se isti ključ koristi više puta?

Za razliku od Šenona, savremena kriptografija ne pretpostavlja da kriptogram ne nosi nikakvu informaciju o poruci, ved da se ona ne može efektivno ekstrahovati budući da su naši računski resursi ograničeni. Ali, ako su Evini računski resursi ograničeni, onda su takvi i Alisini i Bobovi resursi, od kojih očekujemo da efektivno obave postupke kriptovanja i dekriptovanja. Stoga se savremena kriptografija zasniva na pretpostavci o postojanju takozvanih *one-way* funkcija:

Postoje funkcije koje se *lako* računaju, a *teško* invertuju.

Sa takvom pretpostavkom može se konstruisati kriptografski sistem u kome, sa stanovišta teorije složenosti izračunavanja, postoji bitna razlika između *lakih* procedura kriptovanja i dekriptovanja za Alisu i Boba i *teškog* postupka ekstrakcije informacija iz kriptograma, sa kojim se mora suočiti Eva.

Simetrični kriptografski sistem

Kako smo već rekli, kriptografski sistem u kome Alisa i Bob koriste isti ključ je simetričan. Formalno, takav sistem definišemo kao niz

$$(\mathcal{M}, \mathcal{K}, \mathcal{C}, e, d)$$

u kome je $\mathcal{M}$ skup svih mogućih poruka ili *prostor poruka*, $\mathcal{K}$ skup svih mogućih ključeva ili *prostor ključeva* i $\mathcal{C}$ skup svih mogućih kriptograma ili *prostor kriptograma*. Pritom, *kriptujuća funkcija*

$$e : \mathcal{M} \times \mathcal{K} \longrightarrow \mathcal{C},$$

i *dekriptujuća funkcija*

$$d : \mathcal{C} \times \mathcal{K} \longrightarrow \mathcal{D},$$

zadovoljavaju uslov

$$d(e(M, K), K) = M,$$

za svaku poruku $M \in \mathcal{M}$ i svaki ključ $K \in \mathcal{K}$. On obezbeđuje da se svaki kriptogram može dekriptovati, odnosno, da ima bar onoliko kriptograma koliko i poruka.

Primer 2. Kriptovanje permutovanjem azbuke:

Prostor poruka možemo shvatiti kao skup svi smislenih tekstova Engleskog jezika. Da bi kriptovala poruku M, koja se sastoji od $n \geq 1$ slova, Alisa svako slovo M_i zamenjuje slovom $\pi(M_i)$, gde je π permutacija azbuke odgovarajućeg jezika, pa je kriptogram poruke M niz slova

$$C = e(M, \pi) = \pi(M_1) \cdots \pi(M_n).$$

Da bi dekriptovao, Bob prosto primenjuje inverznu permutaciju na svako od slova kriptograma C.

Mana ovog kriptografskog sistema je što se u njemu svako slovo kriptuje uvek na isti način. On se lako razbija analizom frekvencija pojedinih slova. Na primer, u Engleskom jeziku, slova E i T su česća od slova J i Z.

Primer 3. Cezarov kriptografski sistem:

Veruje se da je prvi kriptografski sistem smislio Gaj Julije Cezar. Slova latinske azbuke, ima ih 26, označio je brojevima od 0 do 25. Kriptujuća funkcija bila je translacija $e(M) = M + K \pmod{26}$, gde je $0 \leq M, K \leq 25$.

Sistem se lako razbija, ako Eva raspolaže dovoljno dugim tekstom. Kako je E najfrekventnije slovo u latinskom jeziku, ako se u kriptogramu najčešće pojavljuje slovo U, to znači da je $e(4) = 20$, tj. ključ je $K = 16$.

Cezar je koristio i nešto komplikovaniji *afini kriptografski sistem* oblika $e(M) = aM + b \pmod{26}$. Za dekripciju treba rešiti linearnu kongruenciju, pa da bi rešenje bilo jednoznačno, neophodno je da važi uslov $(a, 26) = 1$. Ključ ovog sistema je par $K = (a, b)$.

Naravno, kao sistem u kome se slovo kriptuje uvek na isti način, i afini sistem se lako razbija. Ako je u kriptogramu najfrekventnije slovo K, a drugo po frekvenciji slovo D, njihove dekripcije su slova E i T, kao najfrekventnija slova latinskog jezika.

Primer 4. Viženerov (Vigenèr) kriptografski sistem:

Ključ u Viženerovom sistemu je niz od $k \geq 1$ slova. Ponavljajući kluč, tako da pokrije dužinu poruke (iz koje mogu biti uklonjena prazna mesta), pravimo niz koji saberemo sa porukom $\pmod{26}$ i tako dobijamo kriptogram. Na primer, ako je ključ niz `KEY`, poruka

$$M = \texttt{THISISTHEMESSAGE}$$

kriptuje se koristeći niz

$$K = \texttt{KEYKEYKEYKEYKEYK}$$

i dobija kriptogram

$$C = \texttt{DLGCMQDLCWIQCEEO}.$$

Viženerov sistem je znatno otporniji na napad analizom frekvencija od prethodnih jer, u njemu slovo nema jedinstven šifrat. Ipak, kada je dat dovoljno veliki šifrat, sistem se jednostavno razbija. Eva najpre treba da odredi parametar $k \geq 1$. On se dobija analizom frekvencije za različite moguće vrednosti parametra k, jer, za njegovu korektnu vrednost, slova na rastojanju k su kriptovana u fiksiranoj azbuci, sa istim frekvencijama kao u odgovarajućem jeziku poruke. Jasno, što je ključ duži, sistem je sigurniji. Slično, što se manje poruka šifrira po istom ključu, Eva će teže obaviti svoj posao.

Zadatak 2. Kako glasi poruka, čiji je kriptogram

`NZBCKOZLELOTKGSFVMA`,

ako Alisa u Viženerovom sistemu koristi ključ `ALICE`.

Primer 5. Vernamov kriptografski sistem:

U Vernamovom sistemu, poruka M i ključ K su binarni nizovi iste dužine, recimo $n \geq 1$. Pritom, K je slučajan niz. Kriptogram se pravi po formuli

$$C = e(M, K) = M + K \pmod 2,$$

a dekriptuje se po formuli

$$M = d(C, K) = C + K \pmod 2.$$

Ovaj sistem može se shvatiti kao poseban slučaj Viženerovog sistema, u kome ključ ima dužinu poruke i dobija se na slučajan način. On ima osobinu da za svaki kriptogram C i svaku poruku M, postoji tačno jedan ključ K koji u dekripciji kriptograma C, daje poruku M. Naime, $K = M + C \pmod 2$. U svim drugim kriptografskim sistemima, o kojima smo do sada govorili, kada dešifruje kriptogram, Eva je mogla da prepozna da li poruka koju je dobila ima smisla. U Vernamovom sistemu, svaki kriptogram može biti kriptogram bilo koje poruke, tako da Eva nikada nije sigurna da li je uspešno obavila dekripciju.

Vernamov sistem je očigledno siguran, ali ima i značajne nedostatke. Prvo, kod mora biti dugačak bar koliko i poruka, a to je skupo i stvara probleme u praksi. I drugo, svako ponavljanje istog koda značajno smanjuje sigurnost sistema. Istorijski, zbog toga što su Rusi ponavljali isti kod, Američka nacionalna bezbednosna agencija (NSA) je dugo uspevala da dekriptuje komunikaciju u odgovarajućoj službi Rusije (KGB). O tome videti članak Roberta Bensona na sajtu NSA.

Savršena sigurnost

Vratimo se klasičnoj teoriji informacija u kojoj kriptografski sistem može da ima "savršenu sigurnost". To je jedan od njenih najvažnijih pojmova, koji je Klod Šenon definisao kao sistem u kome kriptogram ne nosi nikakvu informaciju o poruci. Da to preciziramo, definisaćemo Šenonov verovatnosni model kriptografskog sistema.

Pretpostavljamo da svaka poruka $M \in \mathcal{M}$ iman verovatnoću $p_M > 0$, gde je

$$\sum_{M \in \mathcal{M}} p_M = 1.$$

Pritom, pretpostavka da su sve verovatnoće p_M različite od nule znači da u prostoru $\mathcal{M}$ nema poruka koje se nikada ne šalju.

Slično, svaki ključ K ima verovatnoću $q_K > 0$ da bude upotrebljen u kriptovanju poruke i opet imamo

$$\sum_{K \in \mathcal{K}} q_K = 1.$$

Smisao pretpostavke $q_K > 0$ jeste da se svaki ključ stvarno koristi. Otuda sledi da verovatnoća r_C kriptograma $C \in \mathcal{C}$ iznosi

$$r_C = \sum_{e(M,K)=C} p_M q_K > 0.$$

U konkretnim okolnostima razmene poruka, verovatnoće p_M mogu biti različite, dok je raspodela verovatnoća p_K najčešće uniformna.

Kriptografski sistem ima savršenu sigurnost ako kriptogram ne nosi nikakvu informaciju o poruci. Preciznije, ako je $P(M/C)$ verovatnoća poruke M kada je primljen kriptogram C, distribucija verovarnoća $P(M/C)$ mora biti jednaka distribuciji verovatnoća p_M.

Kako je

$$\begin{aligned} P(M/C) &= \frac{P(M \cap C)}{r_C} \\ &= \frac{P(C/M)p_M}{r_C} \\ &= \frac{p_M}{r_C} \sum_{e(M,K)=C} q_K, \end{aligned}$$

savršena sigurnost svodi se na uslov

$$p_M = \frac{p_M}{r_C} \sum_{e(M,K)=C} q_K,$$

za sve $M \in \mathcal{M}$ i sve $C \in \mathcal{C}$.

U savršeno sigurnom kriptografskom sistemu broj kriptograma manji je od broja kodova, tj. $|\mathcal{C}| \leq |\mathcal{K}|$. Naime, ako je $p_M > 0$, onda mora biti $\sum q_K > 0$, pa postoji bar jedan ključ $K \in \mathcal{K}$ takav da je $e(M, K) = C$. Dakle, za fiksirano M, svi različiti kriptogrami poruke M moraju biti različiti, pa su i ključevi sa kojima su ti kriptogrami dobijeni takođe različiti. Dakle, savršena sigurnost ima visoku cenu.

Vratićemo se Vernamovom sistemu i pokazati da on jeste savršeno siguran.

U tom slučaju prostor poruka, prostor kriptograma i prostor ključeva je skup $\{0,1\}^n$, tj. skup binarnih nizova dužine $n \geq 1$. Treba dokazati da je $P(M/C) = p_M$, za sve $M, C \in \{0,1\}^n$. Po definiciji,

$$P(M/C) = \frac{P(M \cap C)}{r_C},$$

pa ako je $M = (M_1, \ldots, M_n)$ i $C = (C_1, \ldots, C_n)$, postoji tačno jedan ključ $K \in \mathcal{K}$ takav da je $e(M, K) = C$. Naime, to je ključ

$$K = (M_1 + C_1, \ldots, M_n + C_n),$$

gde je $+$ sabiranje po modulu 2. Kako je svaki ključ slučajan binarni niz, ključ K ima verovatnoću $q_K = 1/2^n$, pa mora biti

$$r_C = \sum_{M \in \mathcal{M}} \frac{p_M}{2^n} = \frac{1}{2^n}.$$

Kako je $P(M \cap C) = P(M \cap K)$ i kako je izbor ključa nezavisan od poruke, to je $P(M \cap C) = p_M/2^n$, pa se konačno dobija da je $P(M/C) = p_M$, što znači da je Vernamov sistem savršeno siguran.

Vernamov kriptografski sistem je klasičan primer takozvanog *strim* (stream) *sistema*, u kome se poruka kriptuje slovo po slovo u jedinici vremena. Formalno, u strim sistemu, poruka $M \in \{0,1\}^n$ se kriptuje, bit po bit u jedinici vremena, pomoću *strim ključa* $K \in \{0,1\}^n$, da bi se dobio kriptogram $C = M +_2 K$. Kada je strim ključ slučajan niz dužine $n \geq 1$, strim sistem se svodi na Vernamov sistem. Međutim, nepraktično je i skupo da Alisa i Bob raspolažu istim ključem velike dužine. Umesto toga, mnogi sistemi emuliraju Vernamov sistem.

Da bi smo definisali strim sistem, dovoljno je odrediti kako se generiše strim ključ: Alisa i Bob raspolažu istim kratkim slučajnim nizom i polazeći od njega, koristeći isti generator, generišu dugačak strim ključ. Zapravo, generišu jedan *pseudo slučajan niz.*

Linearni generator pseudo-slučajnog niza

Izložićemo ukratko kako radi *linearni generator pseudo-slučajnog niza*, odnosno, kako se originalno naziva: *linear feedback shift register machine.* Linearni generator je mašina koja se sastoji od $m \geq 1$ registara $R_{m-1}, \ldots, R_0$, tim redom, od kojih svaki sadrži jedan bit. Mašina je određena karakterističnim nizom $(c_1, \ldots, c_m) \in \{0,1\}^n$.

Ako je $x_i(t)$ sadržaj registra R_i u trenutku $t \geq 1$,

$$x(t) = (x_{n-1}(t), \ldots, x_0(t)),$$

označava *stanje* mašine u trenutku t. U trenutku $t+1$ mašina štampa $Z_{t+1} = x_0(t)$ i prelazi u stanje

$$x_i(t+1) = x_{i+1}(t),$$

za $0 \leq i \leq m-2$ i

$$x_{m-1}(t+1) = c_m x_0(t) +_2 c_{m-1} x_1(t) +_2 \ldots +_2 c_1 x_{m-1}(t).$$

Jednostavnije rečeno, u svakom otkucaju sata, registar R_i prenosi svoj sadržaj u susedni sa desne strane. Sadržaj (krajnjeg desnog) registra R_0 se štampa i to je Z_t, a novi sadržaj (krajnjeg levog) registra R_{m-1} izračunava se na osnovu karakterističnog niza $(c_1, \ldots, c_m)$, po prethodnoj formuli.

Ako je $x(0)$ početno stanje mašine, ona će proizvesti beskonačan niz $(Z_t : t \geq 1)$, gde je $Z_t = x_0(t-1)$. Ako je

$$x(0) = (Z_m, Z_{m-1}, \ldots, Z_1),$$

izlazni niz počinje sa

$$Z_1, Z_2, \ldots, Z_m, \ldots$$

Pritom, ako je $x(0) = \mathbf{0}$, svi Z_t će biti nula.

Ako je u karakterističnom nizu $c_m = 1$, linearni generator je *nesingularan.* Polinom

$$c(x) = 1 + c_1 x + c_2 x^2 + \ldots + c_m x^m,$$

je *karakteristični polinom* linearnog generatora.

Niz $(Z_t : t \geq 1)$ je *periodičan* sa periodom $p \geq 1$ ako za neko početno stanje važi $Z_{t+p} = Z_t$, za svako $t \geq 1$ i ako je p najmanji prirodan broj sa tim svojstvom.

Lako se dokazuje da svaki linearni generator proizvodi periodičan niz $(Z_t : t \geq 1)$, za svako početno stanje. Ako linearni generator ima $m \geq 1$ registara, njegov maksimalni period iznosi $2^m - 1$.

Naime, ako linearni generator ima $m \geq 1$ registara i ako je njegov karakteristični polinom

$$c(x) = 1 + c_1 x + c_2 x^2 + \ldots + c_m x^m, \ c_m = 1,$$

onda za svako $t \geq 0$,

$$x(t+1) = Cx(t),$$

gde je

$$C = \begin{pmatrix} c_1 & c_2 & c_3 & \cdots & c_{m-1} & c_m \\ 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 0 \end{pmatrix}.$$

Pritom, aritmetičke operacije izvode se po modulu 2.

Primetimo da je $\det C = c_m = 1$, tj. matrica C je nesingularna. Ako je $x(0) = \mathbf{0}$, izlazni niz je konstanta nula (ima period jedan), pa možemo pretpostaviti da je $x(0) \neq \mathbf{0}$.

Kako je $x(t) = C^t x(0)$, za svako $t \geq 1$, $X(t) \neq \mathbf{0}$. Ako je $k = 2^m - 1$, u nizu od 2^m binarnih vektora

$$x(0), Cx(0), \ldots, C^k x(0),$$

različitih od $\mathbf{0}$, ima bar dva jednaka (ima samo $2^m - 1$ takvih vektora). Otuda, postoje $1 \leq i < j \leq k$ takvi da je

$$C^i x(0) = C^j x(0),$$

pa kako je C nesingularna matrica

$$x(0) = C^{j-i} x(0) = x(j-i).$$

Ako je $p = j - i$, onda $x(t+p) = x(t)$, za svako $t \geq 0$, pa je izlazni niz periodičan sa periodom najviše $p \leq 2^m - 1$.

Karakteristični polinom linearnog generatora sa $m \geq 1$ registara je *primitivan* ako nije svodljiv i ako ne deli polinom $x^d + 1$, za svako $d < 2^m - 1$. U kriptografiji su takvi polinomi važni jer linearni generator čiji je karakteristični polinom primitivan ima maksimalan period za svaki ulaz. Ovu činjenicu navodimo bez dokaza.

Jedan od mogućih načina (najjednostavniji) da se linearni generator koristi u kriptografskom sistemu jeste da se kao ključ koristi niz $Z_1, Z_2, \ldots$ i kriptuje bit po bit po formuli $C_i = M_i +_2 Z_i$, za sve $i \geq 1$. Sledeća teorema pokazuje da je takav kriptografski sistem beznadežno nesiguran.

Ako je niz $Z_1, Z_2, \ldots$ generisan nesingularnim linearnim generatorom sa $m \geq 1$ registara i ako se taj niz ne može generisati sa $k < m$ registara, onda je karakteristični polinom linearnog generatora determinisan sa $2m$ uzastopnih članova niza $Z_1, Z_2, \ldots$

Ne umanjujući opštost, možemo pretpostaviti da je poznato prvih $2m$ članova niza $Z_1, Z_2, \ldots$ Oni zadovoljavaju sledeći sistem jednačina

$$\begin{pmatrix} Z_{m+1} \\ Z_{m+1} \\ \vdots \\ Z_{2m} \end{pmatrix} = \begin{pmatrix} Z_m & Z_{m-1} & \cdots & Z_1 \\ Z_{m+1} & Z_m & \cdots & Z_2 \\ \vdots & & \ddots & \vdots \\ Z_{2m-1} & Z_{2m-2} & \cdots & Z_m \end{pmatrix} \begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_m \end{pmatrix}.$$

Ako je matrica na desnoj strani invertibilna, parametri linearnog generatora $c_1, \ldots, c_n$ su jedinstveno određeni. Pretpostavimo suprotno, tj. da su redovi matrice linearno zavisni. Kako su to vektori stanja linearnog generatora, postoji linearna zavisnost

$$\sum_{i=0}^{m-1} b_i x(i) = \mathbf{0},$$

gde koeficijenti $b_0, b_1, \ldots, b_{m-1} \in \{0, 1\}$ nisu svi jednaki nuli. Neka je $k = \max\{i : b_i \neq 0\}$. Kako je $k \leq m - 1$ i kako radimo po modulu 2, to imamo da je

$$x(k) = \sum_{i=0}^{k-1} b_i x(i).$$

Ako je C matrica linearnog generatora, za svako $t \geq 1$,

$$x(t + k) = C^t x(k) = \sum_{i=0}^{k-1} b_i C^t x(i) = \sum_{i=0}^{k-1} b_i x(t + i).$$

Dakle, za svako $t \geq 1$,

$$Z_{t+k} = \sum_{i=0}^{k-1} b_i Zt + i,$$

pa je niz $Z_1, Z_2, ...$ generisan linearnim generatorom sa $k < m$ registara, a to protivreči pretpostavci teoreme.

Ovaj rezultat pokazuje da je strim sistem zasnovan samo na linearnom generatoru nije pouzdan. Evi je dovoljno da zna $2m$ uzastopnih poruka M_j, i njihovih $2m$ kriptograma C_j, pa da lako odredi $2m$ uzastopnih vrednosti $Z_j = M_j +_2 C_j$ sa kojima je determinisan linearni generator. Ali, uprkos prethodnoj teoremi, linearni generator je u širokoj upotrebi. Pre svega, zbog jednostavnosti implementacije u hardver, ali i zbog toga što postoje načini da se kombinacijom više linearnih generatora dobiju mnogo sigurniji kriptografski sistemi. Pritom, jedan od kriterijuma sigurnosti može biti period generisanog niza ili, na primer broj registara linearnog generatora. *Linearna složenost* binarnog niza $(Z_n : n \geq 1)$ je najmanji broj $m \geq 1$, za

koji postoji linearni generator sa m stanja koji generiše niz $(Z_n : n \geq 1)$, a ako takav generator ne postoji, onda niz ima beskonačnu linearnu složenost.

Jasno je da bilo kakva kombinacija linearnih generatora ne može dati generator beskonačne složenost, ali se njegova složenost može značajno povećati u odnosu na polazne linearne generatore. Na primer, u takozvanom Geffeovom generatoru iz 1973. godine, koristi se nelinearna kombinacija

$$f(x_1, x_2, x_3) = x_1x_2 + x_2x_3 + x_3.$$

Pritom, ako se kombinuju tri linearna generatora, čiji su karakteristični polinomi primitivni, sa redom a, b i c registara, gde su a, b i c po parovima uzajamno prosti brojevi, Geffe-ov generator ima period $(2^a - 1)(2^b - 1)(2^c - 1)$ i linearnu složenost $ab + bc + c$.

Drugi način da se dobije pouzdaniji generator jeste da se koristi samo jedan linearni generator, ali da se na izlazu javljaju vrednosti neke funkcije (filtera), čija se vrednost izračunava na osnovu $k \geq 1$ uzastopnih vrednosti linearnog generatora. Takvi generatori poznati su kao *nelinearni filter generatori*. O ovoj temi postoji zaista nepregledna literatura.

Blok sistemi i DES

Umesto da se kriptuje bit po bit, kao u strim sistemima, poruka se može kriptovati po blokovima. Takvi sistemi su u širokoj upotrebi i prirodno se nazivaju *blok sistemima*.

Formalno, blok poruke dužine $m \geq 1$ kriptuje se ključem dužine $k \geq 1$ i dobija kriptogram dužine n, pa

$$e : \{0,1\}^m \times \{0,1\}^k \longrightarrow \{0,1\}^m,$$

$$d : \{0,1\}^m \times \{0,1\}^k \longrightarrow \{0,1\}^m,$$

tako da važi uslov $d(e(M, K)) = M$, a ključ K se najčešće bira na slučaj.

Najvažniji i još uvek najčešći blok sistem, uprkos godinam je *Data Encryption Standard* ili DES. To je primer Fejstelovog kriptografskog sistema koji ima blokove dužine $2m$, $m \geq 1$. Blok poruka M se deli na par n-bitnih polublokova i dobija $M = (L_0, R_0)$. Kriptovanje je iterativni proces koji se, u nekom dogovorenom broju iteracija $t \geq 1$, izvodi na sledeći način:

U svakoj iteraciji, iz para polublokova (L_{j-1}, R_{j-1}), formira se novi par polublokova (L_j, R_j) po pravilu

$$L_j = R_{j-1},\ R_j = L_{j-1} +_2 f(R_{j-1}, K_j),$$

gde je K_j podključ za j-tu iteraciju dobijen, na neki prethodno utvrđen način, iz ključa K i gde je f neka zadata funkcija. Kriptogram poruke je $C = (L_t, R_t)$.

Važno svojstvo ovog postupka kriptovanja je ste da je on reverzibilan za svakoga ko taj postupak zna. Ako je dat par (L_j, R_j), onda se par (L_{j-1}, R_{j-1}) dobija tako da $R_{j-1} = L_j$ i

$$L_{j-1} = R_j +_2 f(R_{j-1}, K_j) = R_j +_2 f(L_j, K_j).$$

Otuda sledi da se Fejstelov kriptografski sistem zadaje Fejstelovom funkcijom, koju smo označili sa f, kao i procedurom generisanja podključeva $K_1, \ldots, K_t$, polazeći od originalnog ključa K. Neke od od tih detalja izložićemo u slučaju kriptografskog sistema DES.

DES je Fejstelov kriptografski sistem izveden iz IBM-ovog sistema *Lucifer*, ranih sedamdesetih godina i u Americi je 1977. godine prihvaćen kao standard od strane *Nacional Institute of Standards and Technology.* On operiše na blok porukama dužine 64 bita. Za ključ se takođe rezerviše 64 bita, ali se stvarno ne koristi 8 bita, pa je dužina ključa 56 bita.

DES radi u 16 iteracija. Prvo se primeni fiksirana permutacija na blok od 64 bita (inicijalna permutacija), pa se dobijeni blok deli po pola i dobija (L_0, R_0). Pritom, ne zna se kakav kriptografski značaj ima inicijalna permutacija?

Raspored podključeva, koji se izvode iz datog ključa, jeste sledeći:

Prvo se odredi 56 *bitova ključa* K *i podeli na dva dela po* 28 *bita. U svakoj iteraciji obe polovone se rotiraju na levo za jedan ili dva bita (što zavisi od broja iteracije), a potom ekstrahuje po* 24 *bita iz svake polovine i dobija podključ od* 48 *bita.*

U DES-u se iteracije izvode kao u Fejstelovom kriptografskom sistemu, pa ostaje da definišemo funkciju f. Ona se u j-toj iteraciji primenjuje na polublok R_{j-1} i podključ K_j. Postupa se na sledeći način:

Koristeći takozvanu ekspanzivnu permutaciju *koja duplira neke od bitova, polublok* R_{j-1} *od* 32 *bita, proširuje se do* 48 *bita.*

Podključ K_j*, koji takođe ima* 48 *bita, sabira se sa proširenim polublokom po modulu* 2.

Rezultujući 48*-bitni blok se deli na* 6*-bitne blokove i na njih primenjuje nelinearna operacija. Ona svaki* 6*-bitni blok prevodi u* 4*-bitni blok. Operacija se naziva* S*-boks.*

Na 32*-bitni izlaz primenjuje se permutacija (takozvani* P*-boks) i tako dobija* $f(R_{j-1}, K_j)$.

Konačno, posle šesnaeste iteracije, na blok (L_{15}, R_{15}), primenjuje se inverzna inicijalna permutacija ili *finalna permutacija*.

Najznačajni aspekt kriptovanja u DES-u jeste upotreba S-boksova. Ona u proces uvodi nelinearnost bez koje bi se sistem lako razbio. O tome kako S-boksovi izgledaju mnogo je pisano. Zna se da je u prvobitnoj varijanti DES bio osetljiv na napad koji se naziva *diferencijalna kriptoanaliza*. Iz tog razloga, S-boksovi su nekoliko puta menjani. Ovde nećemo izlagati poznate teorijske napade na DES, koji često koriste kombinaciju diferencijalne i linearne kriptoanalize, budući da svaki od njih zahteva ogroman broj poznatih poruka, te su stoga praktično neupotrebljivi. Najpoznatiji praktični napad je *napad brutalnom silom*, tj. pretragom svih 2^{56} mogućih ključeva, sve dok se pravi ne pronađe. Naime, 1998. godine, računar koji je koštao 250 000 dolara uspeo je da razbije poruku kriptovanu u DES-u posle 56 sati rada. Iako su teorijski napadi na DES sigurno jeftiniji, u praksi se brutalna sila ipak najbolje pokazala.

Zanimljivo je da, iako je bilo poznato da je uspešni brutalni napad na DES izveden, on je u SAD-u potvrđen kao federalni standard 1999. godine. Pritom, preporučena je njegova varijanta koja se naziva *Trostruki DES* ili $3DES$.

Ključ $3DES$-a je trojka $K = (K_1, K_2, K_3)$, gde je svaki od K_i jedan DES ključ. Ako je DES_{K_i} i $DES_{K_i}^{-1}$ kriptovanje, odnosno, dekriptovanje u DES-u po ključu K_i, onda je kriptogram poruke M od 64 bita u $3DES$-su

$$C = DES_{K_3}(DES_{K_2}^{-1}(DES_{K_1}(M))).$$

Prvi teorijski napad na $3DES$ nije bio uspešan. Naime, verovalo se da $\{DES_K : K \in \mathcal{K}\}$ čini grupu, s obzirom na kompoziciju, pa bi se $3DES$ kompozicija svela na DES, ali se ispostavilo da to nije tačno. Izgleda da je $3DES$ znatno sigurniji od DES-a.

Sistemi sa javnim ključem

Pošto smo napravili pregled klasičnih kriptografskih sistema, izložićemo i savremeni pristup kriptografiji, zasnovan na matematičkoj teoriji složenosti, odnosno, na pretpostavci da postoji teorijska razlika u složenosti problema koji rešavaju Alisa i Bob, kada kriptuju i dekriptuju, sa jedne i Eva, kada analizira poruku, sa druge strane. Preciznije, u takvom kriptografskom sistemu se kriptuje i dekriptuje u polinomijalnom vremenu, ali je problem razbijanja njegovog ključa znatno teži. Pritom, svi akteri imaju istu ograničenu računsku moć: mogu da koriste samo algoritme koji rade u (moguće probabilističkom) polinomijalnom vremenu.

Primer 6. Sistem RSA:

Najšire korišćen i dobro poznat sistem sa javnim ključem je *Rivest, Shamir i Adelmanov* ili RSA sistem. Njegova shema objavljena je 1977. godine. U to doba izazvao je ogromnu pažnju i danas je sasvim sigurno najpoznatiji kriptografski sistem. U njemu se radi na sledeći način:

Formiranje ključa: Bob formira ključ sistema tako što bira dva velika prosta broja p i q i formira *javni modulus* $n = pq$. Zatim bira *javni eksponent* e koji je uzajamno prost sa $(p-1)(q-1)$ i zadovoljava uslov $1 < e < (p-1)(q-1)$. Par (n, e) je *javni ključ* sistema i Bob ga javno objavljuje. Njegov *privatni ključ* je jedinstven broj d, $1 < d < (p-1)(q-1)$ takav da

$$ed = 1 \pmod{(p-1)(q-1)}.$$

Privarni ključ Bob drži u tajnosti.

Kriptovanje: Alisa poruku M prvo razloži na niz blokova $M_1, M_2, \ldots, M_t$, tako da svaki blok M_i zadovoljava uslov $0 \leq M_i < n$, pa potom kriptuje blokove

$$C_i = M_i^e \pmod{n}.$$

Dekripcija: Koriseći privatni ključ d, Bob dekriptuje tako što izračunava

$$M_i = C_i^d \pmod{n}.$$

Nije odmah jasno da li dekripcija u RSA stvarno funkcioniše? Da to dokažemo, koristimo relaciju

$$ed = 1 \pmod{(p-1)(q-1)}.$$

To znači da je $ed = 1 + t(p-1)(q-1)$, za neki ceo broj t. Otuda se, na osnovu male Fermatove teoreme, redom dobija

$$C_i^d = M_i^{ed} = M_i^{t(p-1)(q-1)+1} = M_i \pmod{p}.$$

Na isti način, $C_i^d = M_i \pmod{q}$, pa zbog Kineske teoreme o ostacima imamo da je $C_i^d = M_i \pmod{n}$.

Formiranje RSA ključa je jednostavno jer Bob može izabrati dva k-bitna prosta broja tako što bira slučajne brojeve i testira njihovu primalnost. On potom množenjem formira modulus n i određuje javni eksponent e, tako što bira slučajne k-bitne brojeve sve dok ne nađe jedan koji je uzajamno prost sa

$(p-1)(q-1)$. Da odredi privatni ključ d, koristi Euklidov algoritam. Za svaki od tih koraka ima na raspolaganju algoritme koji rade u polinomijalnom vremenu. Kriptovanje i dekripcija se vrše eksponencijacijom po modulu n, pa su ostvarive u polinomijalnom vremenu.

RSA-problem: Problem sa kojim se Eva suočava jeste: Dati su n, e i C, odrediti e-ti koren iz C po modulu n.

To izgleda znatno teže. Najprirodnije što Eva može da učini jeste da pokuša da faktoriše broj n i tako odredi p i q.

Problem faktorizacije: Dat je prirodan broj, odrediti sve njegove faktore.

Ako to reši, Eva dalje sve radi lako, u polinomijalnom veremenu. Koristeći javni ključ e, ona lako izračunava Bobov tajni ključ d i čita sve kriptograme koje on dobija.

Međutim, ne postoji jednostavan i brz algoritam za rešenje problema faktorizacije. Jedan algoritam faktorizacije sastojao bi se u suksesivnom delenju broja n svim prostim brojevima manjim od $\sqrt{n}$. U primeni tog algoritma pojavljuju se dve glavne teškoće. Prvo, neophodno je napraviti spisak svih prostih brojeva manjih od $\sqrt{n}$, što je samo po sebi težak zadatak. Sa druge strane, za veliko n, broj operacija delenja broja n može biti tako veliki da se ne može izvršiti. Asimptotska složenost ovog algoritma faktorizacije iznosi $O(\sqrt{n}\log n)$.

Iako jednostavan, izloženi algoritam implicitno je sadržan u svim savremenim metodima faktorizacije. Asimptotska složenost najboljeg od tih algoritama iznosi $O(n^{0.13})$, što je sa stanovišta moći savremenih računara premnogo. Više od toga, bilo kakav rast moći savremenih računara marginalno doprinosi rešenju zadatka faktorizacije prirodnih brojeva.

Ako uopšte postoji, rešenje tog problema nalazi se u njegovim matematičkim osnovama. Naime, kao što je poznato, faktorizacija je NP-kompletan problem, pa ako je $P \neq NP$, onda faktorizacija nije put za razbijanje RSA sistema. U suprotnom, ako je $P = NP$, sistem RSA nije siguran.

Može li se reći da je sigurnost RSA sistema zasnovana je na činjenici da ne postoji jednostavan i brz algoritam za faktorizaciju prirodnih brojeva? Za sada ne, jer nije dokazano da je problem faktorizacije ekvivalentan zadatku razbijanja RSA sistema.

Primer 7. Elgamalov sistem:

Izložićemo i Elgamalov kriptografski sistem sa javnim ključem. Definisan je 1985. godine, a njegova sigurnost zasniva se na složenosti problema diskretnog logaritma.

Formiranje ključa: Bobov javni ključ je prost broj p, primitivni koren $g \pmod p$ i vrednost $g^x \pmod p$, gde je $x \in Z_p^*$. Njegov privatni ključ je broj x.

Kriptovanje: Pretpstavljamo da je $0 \leq M \leq p-1$. Ako to nije slučaj, poruka se razlaže na blokove. Alisa bira slučajan broj $y \in Z_p^*$ i izračunava brojeve

$$k = g^y \pmod p, \quad d = M(g^x)^y \pmod p.$$

Kriptogram poruke M je par $C = (k, d)$.

Dekripcija: Koristeći privatni ključ, Bob računa

$$M = k^{p-1-x} d \pmod p.$$

Treba ipak dokazati da dekripcija u Elgamalovom sistemu zaista radi: Naime, radeći po modulu p, imamo

$$k^{p-1-x} = k^{-x} = g^{-xy} \pmod p,$$

pa je

$$k^{p-1-x} d = g^{-xy} d = g^{-xy} M (g^x)^y = M \pmod p.$$

Jasno je da se i kriptovanje i dekripcija izvode lako. Nešto manje je jasno kako Bob generiše njegov ključ. On lako bira prost broj, ali ne postoji polinomijalni algoritam za generisanje primitivnih korena po modulu datog prostog broja. Zapravo ne postoji ni efektivan algoritam koji proverava da li broj $h \in Z_p^*$ jeste primitivan koren modulo p. Dakle, u teoriji ne postoji efektivan algoritam za generisanje Elgamalovog javnog ključa, pa se to u praksi prevazilazi na različite načine.

Na primer, koriste se *prosti brojevi Sofije Žermen.* To su prosti brojevi q takvi da broj $p = 2q + 1$ jeste prost (broj p je u tom slučaju *siguran prost broj*). Veruje se da ima beskonačno mnogo prostih brojeva Sofije Žermen i ako se sa $\pi_S(x)$ označi broj takvih prostih brojeva manjih od x, onda

$$\pi_S(x) \sim \frac{cx}{(\log x)^2},$$

gde je $c \simeq 1.3203$. Ako se pretpostavi ta je ova hipoteza tačna, onda postoji verovatnosni algoritam koji generiše Elgamalov ključ u polinomijalnom očekivanom vremenu.

Da bi razbila sistem, Eva treba da reši

Elgamalov problem: Dati su prost broj p, primitivni koren g modulo p, $g^x \pmod p$ i kriptogram (k, d), odrediti poruku M.

To bi bilo moguće ako bi Eva imala brz algoritam za određivanje celobrojnog logaritma:

Problem celobrojnog logaritma: Dati su prost broj p, primitivni koren g modulo p i ceo broj y, odrediti ceo broj x tako da je $g^x = y \pmod{p}$.

Nije poznato da li su Elgamalov problem i Problem celobrojnog logaritma ekvivalentni?