4 Teorija števil

Teorija števil se ukvarja s *celimi števili*. Množico celih števil zapišemo kot

$$\mathbb{Z} = \{0, 1, -1, 2, -2, 3, -3, \ldots\}$$

in jo razdelimo na množico naravnih števil

$$\mathbb{N} = \{1, 2, 3, \ldots, \},$$

množico negativnih celih števil

$$\mathbb{N}^- = \{-1, -2, -3, \ldots\}$$

in množico, ki vsebuje le število 0.

4.1 Delitelji in večkratniki

Med najosnovnejše pojme teorije števil sodi pojem deljivosti.

DEFINICIJA 4.1 Celo število m deli celo število n, če in samo če obstaja takšno celo število k, da je $n = km$. V tem primeru pišemo $m \mid n$ in rečemo, da je m delitelj števila n, da je n deljiv s številom m in da je n večkratnik števila m.

Opazimo, da je 0 večkratnik vsakega celega števila (saj je $0 = 0 \cdot m$ za vsak $m \in \mathbb{Z}$) in da je edino število, ki ga 0 deli, število 0 (saj je $k \cdot 0 = 0$ za vsak $k \in \mathbb{Z}$). Po drugi stran pa števili 1 in -1 delita prav vsa cela števila (saj je $n = n \cdot 1$ in $n = (-n) \cdot (-1)$ za vsak $n \in \mathbb{Z}$) in poleg števil 1 in -1 nimata prav nobenih drugih deliteljev.

Naj bosta m in n poljubni števili. Tedaj največje naravno število, ki deli tako m kot n označimo z $\gcd(m, n)$ in ga imenujemo *največji skupni delitelj* števil m in n. (Oznaka gcd izvira iz angleškega poimenovanja *greatest common divisor*). Najmanjše naravno število, ki je deljivo tako z m kot z n, pa imenujemo *najmanjši skupni večkratnik* števil m in n in ga označimo z $\mathrm{lcm}(m, n)$ (angl. *least common multiple*). Celi števili m in n sta *tuji*, če velja $\gcd(m, n) = 1$.

Omenimo še, da je relacija deljivosti tranzitivna relacije. Natančneje, velja naslednje:

TRDITEV 4.2 *Če $r \mid m$ in $m \mid n$, tedaj $r \mid n$.*

DOKAZ: Iz definicije deljivosti sledi, da obstajata celi števili k in ℓ, za kateri je $m = kr$ in $n = \ell m$. Tedaj pa je $n = \ell kr$, od koder sledi, da je n deljiv z r. ∎

Funkciji div in mod

Naj bo n poljubno celo število in m poljubno neničelno celo število. Kot smo že opazili, kvocient n/m tedaj ni nujno celo število, kar pomeni, da v množici celih števil običajna operacija deljenje ni dobro definirana. Namesto običajnega deljenja zato vpeljemo operacijo celoštevilskega deljenja, ki številoma n in m priredi *celoštevilski količnik* $k = n \operatorname{div} m$ ter *ostanek* $r = n \bmod m$. Celoštevilski količnik k in ostanek r sta natanko določena s pogojem:

$$n = km + r; \quad k, r \in \mathbb{Z},\ 0 \leq r \leq |m| - 1.$$

4.2 Praštevila

DEFINICIJA 4.3 Od 1 različno naravno število je praštevilo, če poleg samega sebe in 1 ne premore nobenega drugega naravnega delitelja.

TRDITEV 4.4 *Vsako od* 1 *različno naravno število je deljivo z vsaj enim praštevilom.*

DOKAZ: Dokaz bo potekal z indukcijo na naravno število n. Za $n = 1$ trditev ne trdi ničesar, za $n = 2$ pa je pravilna, saj je 2 res deljiv s praštevilom, namreč kar z 2. Privzemimo torej, da je $n \geq 3$ in da je vsako naravno število, ki je manjše od n, deljivo s kakim praštevilom. Dokazati moramo, da tedaj isto velja tudi za število n.

Če je n praštevilo, tedaj je deljivo s praštevilom n. Če n ni praštevilo, tedaj je deljivo s kakim naravnim številom m, $2 \leq m \leq n-1$. Po indukcijski predpostavki je m deljiv z nekim praštevilom p. Tedaj pa iz Trditve 4.2 sledi, da p deli n. ∎

TRDITEV 4.5 *Praštevil je neskončno mnogo.*

DOKAZ: Pa recimo, da jih je le končno mnogo; označimo jih s p_1, $p_2, \ldots, p_n$. Oglejmo si število $m = p_1 p_2 \ldots p_m + 1$. Očitno je m večji od vsakega od praštevil p_i, zato ni praštevilo. Iz Trditve 4.4 tedaj sledi, da je p deljiv s kakim praštevilom; denimo s p_i. Tedaj je

$$m = p_1 \ldots p_{i-1} p_i p_{i+1} \ldots p_m + 1 = kp_i$$

za kak $k \in \mathbb{Z}$, in zato $1 = p_i(k - p_1 \ldots p_{i-1} p_{i+1} \ldots p_m)$. To pa je nemogoče, saj 1 ni deljiv z nobenim praštevilom, torej tudi ne s p_i. ∎

DEFINICIJA 4.6 Naj bodo $p_1, p_2, \ldots, p_k$ poljubna, paroma različna praštevila in $\alpha_1, \ldots, \alpha_k$ poljubna naravna števila. Tedaj zapisu

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

pravimo razcep števila n na prafaktorje.

TRDITEV 4.7 *Vsako od* 1 *različno naravno število premore razcep na prafaktorje. Razcep je do vrstnega reda faktorjev en sam.*

Včasih je priročno v razcep naravnega števila n vrini še kako praštevilo, s katerim n ni deljiv; tako praštevilo mora seveda v razcepu nastopati z eksponentom 0. Na ta način omogočimo, da poljubni dve naravni števili $a, b \in \mathbb{N}$ zapišemo z naborom istih praštevil: $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, $b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$, $\alpha_i, \beta_i \geq 0$. S pomočjo razcepa na prafaktorje lahko dokažemo več zanimivih trditev:

TRDITEV 4.8 *Naravno število m deli naravno število n, če in samo če za njuna razcepa na prafaktorje velja naslednje:*

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k},\ m = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k},\ b_i \leq a_i \text{ za vsak } i \in \{1, \ldots, k\}.$$

TRDITEV 4.9 *Naj bodo a, b in c poljubna cela števila. Če sta a in b tuji števili in če a deli bc, tedaj a deli c.*

TRDITEV 4.10 *Naj bosta a in b poljubni celi števili in c njun skupni delitelj. Tedaj je* $\gcd(\frac{a}{c}, \frac{b}{c}) = \frac{\gcd(a,b)}{c}$.

Iz zgornje trditeve neposredno sledi, da sta za poljubni celi števili a in b števili $\frac{a}{\gcd(a,b)}$ in $\frac{b}{\gcd(a,b)}$ tuji.

Računanje gcd **in** lcm **s pomočjo razcepa na prafaktorje**

Vzemimo naravni števili m in n. Če je katero od njih enako 1 (denimo $n = 1$), potem je očitno

$$\gcd(m, 1) = 1 \quad \text{in} \quad \operatorname{lcm}(m, 1) = m.$$

Predpostavimo sedaj, da je $m, n \geq 2$. Naj bodo $p_1, \ldots, p_n$ tista praštevila, ki delijo tako m kot n. Tedaj imata razcepa števili m in n na prafaktorje obliko

$$\begin{aligned} m &= p_1^{\alpha_1} \cdots p_n^{\alpha_n} \cdot q_1^{\delta_1} \cdots q_k^{\delta_k}, \\ n &= p_1^{\beta_1} \cdots p_n^{\beta_n} \cdot r_1^{\gamma_1} \cdots r_\ell^{\gamma_\ell}, \end{aligned}$$

pri čemer je $q_i \neq r_j$ za vsak par indeksov i, j. V tem primeru velja:

$$\begin{aligned} \gcd(m,n) &= p_1^{\min\{\alpha_1,\beta_1\}} \cdots p_n^{\min\{\alpha_n,\beta_n\}} \\ \operatorname{lcm}(m,n) &= p_1^{\max\{\alpha_1,\beta_1\}} \cdots p_n^{\max\{\alpha_n,\beta_n\}} \cdot q_1^{\delta_1} \cdots q_k^{\delta_k} \cdot r_1^{\gamma_1} \cdots r_\ell^{\gamma_\ell} \end{aligned}$$

Od tod neposredno sledi naslednje:

TRDITEV 4.11 *Za poljubni naravni števili m in n velja enakost*

$$\gcd(m,n) \cdot \operatorname{lcm}(m,n) = mn.$$

4.3 Diofantske enačbe

Enačbe, pri katerih iščemo zgolj celoštevilske rešitve, se imenujejo *diofantske enačbe*. Oglejmo si nekoliko podrobneje linearne diofantske enačbe, torej enačbe oblike

$$a_1x_1 + a_2x_2 + \ldots + a_nx_n = c, \qquad (*)$$

kjer so a_i, $i = 1, \ldots, n$, in c poljubna cela števila, x_i, $i = 1, \ldots, n$, pa neznanke. Rešitev enačbe $(*)$ je vsaka n-terica $(x_1, \ldots, x_n)$ celih števil, ki zadošča $(*)$.

Oglejmo si najprej primer, ko imamo eno samo neznanko:

$$ax = c, \;\; a \neq 0. \qquad (+)$$

Če bi dopuščali tudi racionalne rešitve, bi zgornja enačba imela natanko eno rešitev, namreč $x = c/a$. Ker pa nas pri diofantskih enačbah zanimajo le celoštevilske rešitve, bo imela diofantska enačba $(+)$ rešitev tedaj in le tedaj, ko bo a delil c (in bo zato c/a celo število).

Nekoliko bolj zanimiva je linearna diofantska enačba z dvema neznankama:

$$ax + by = c, \;\; a, b \neq 0. \qquad (\times).$$

Premislimo najprej, kako je z racionalnimi rešitvami. Ker je $a \neq 0$, lahko zgornjo enakost preoblikujemo v $x = (c - by)/a$. To pomeni, da lahko za poljuben y najdemo ustrezen x, tako da bo par (x, y) rešil enačbo $(\times)$. Racionalnih rešitev enačbe $(\times)$ je torej neskončno mnogo pri poljubnih koeficientih a, b in c.

Če pa zahtevamo, da so rešitve celoštevilske, pa se pojavi težava, saj število $x = (c - by)/a$ niti pri celoštevilskih y ni nujno celo. Velja pa naslednje:

IZREK 4.12 *Diofantska enačba*

$$ax + by = c,\ \ a, b \neq 0, \qquad (\times)$$

je rešljiva, če in samo če je število c deljivo z največjim skupnim deliteljem števil a in b. V tem primeru je rešitev neskončno mnogo. Če je (x_0, y_0) neka rešitev enačbe $(\times)$, so ostale rešitve enačbe $(\times)$ oblike

$$x = x_0 - kb',\ \ y = y_0 + ka', \qquad k \in \mathbb{Z},$$

kjer je $a' = a/\gcd(a, b)$ in $b' = b/\gcd(a, b)$.

DOKAZ: Obstoj rešitve, v primeru, da $\gcd(a, b)$ deli c, bomo pokazali v nadaljevanju, ko bomo predstavili postopek za iskanje rešitve. Osredotočimo se torej na preostale trditve iz izreka.

Denimo, da je enačba $(\times)$ rešljiva. Tedaj obstajata takšni števili $x_0, y_0 \in \mathbb{Z}$, da je $ax_0 + bx_0 = c$. Če je m poljuben skupni delitelj števil a in b, tedaj je $a = rm$ in $b = tm$ za neki celi števili r in t, in zato

$$c \ = \ ax_0 + by_0 \ = \ rmx_0 + tmy_0 \ = \ (rx_0 + ty_0)m.$$

Od tod sledi, da vsak skupni delitelj števil a in b (tudi $\gcd(a, b)$) deli c.

Naj bo (x_0, y_0) poljubna rešitev enačbe $(\times)$ in $x = x_0 - kb'$, $y = y_0 + ka'$ za neko celo število k. Tedaj je

$$ax + by = a(x_0 - kb') + b(y_0 + ka') = ax_0 + by_0 = c,$$

kar dokazuje, da je tudi (x, y) rešitev enačbe.

Dokazati moramo le še, da je res vsaka rešitev enačbe $(\times)$ oblike $x = x_0 + kb'$, $y = y_0 - ka'$. Pa naj bo (x_1, y_1) še neka rešitev enačbe $(\times)$. Tedaj je $(ax_0 + by_0) - (ax_1 + by_1) = 0$, in zato $a(x_0 - x_1) = b(y_1 - y_0)$. Če iz slednje enakosti pokrajšamo največji skupni večkratnik števil a in b, dobimo

$$a'(x_0 - x_1) = b'(y_1 - y_0).$$

Iz trditve 4.10 sledi, da sta števili a' in b' tuji. Tedaj pa iz trditve 4.9 sledi, da je $k = (y_1 - y_0)/a'$ celo število. Pri tem velja

$$x_0 - kb' = x_0 - \frac{(y_1 - y_0)b'}{a'} = x_0 - (x_0 - x_1) = x_1, \quad y_0 + ka' = y_0 + (y_1 - y_0) = y_1,$$

in rešitev (x_1, y_1) je res zahtevane oblike. ∎

4.4 Razširjeni Evklidov algoritem

Razširjeni Evklidov algoritem uporabljamo za računanje največjega skupnega delitelja danih celih števil in za reševanje linearnih diofantskih enačb z dvema neznankama. Sam postopek lahko opišemo takole:

VHODNI PODATEK: Par (a, b) neničelnih celih števil.

$(r_0, x_0, y_0) := (a, 1, 0)$;
$(r_1, x_1, y_1) := (b, 0, 1)$;
$i := 1$;
dokler $r_i \neq 0$ izvajaj
    $i := i + 1$;
    $k_i := r_{i-2}$ div r_{i-1};
    $(r_i, x_i, y_i) := (r_{i-2}, x_{i-2}, y_{i-2}) - k_i(r_{i-1}, x_{i-1}, y_{i-1})$;
konec zanke

VRNI: $(r_{i-1}, x_{i-1}, y_{i-i})$.

TRDITEV 4.13 *Naj bosta a in b neničelni celi števili. Tedaj trojica (d, x, y), ki jo vrne razširjeni Evklidov algoritem z vhodnim podatkom (a, b), zadošča pogoju*

$$ax + by = d, \quad d = \gcd(a, b).$$

DOKAZ: Za števila r_i, a_i in b_i iz opisa razširjenega evklidovega algoritma za vsak $i \geq 0$ z indukcijo dokažimo enakost

$$ax_i + by_i = r_i. \qquad (*)$$

Ta enakost očitno velja za $i = 0$ in $i = 1$, saj je $ax_0+by_0 = a\cdot 1+b\cdot 0 = a = r_0$ in $ax_1+by_1 = a\cdot 0+b\cdot 1 = b = r_1$. Denimo sedaj, da je $i \geq 2$, in privzemimo, da enakost $(*)$ velja za vse indekse manjše od izbranega i. Tedaj

$$ax_i+by_i = a(x_{i-2}-k_ix_{i-1})+b(y_{i-2}-k_iy_{i-1}) = ax_{i-2}+by_{i-2}-k(ax_{i-1}+by_{i-1}).$$

Po indukcijski predpostavki je slednje enako $r_{i-2} - kr_{i-1} = r_i$. S tem smo dokazali enakost $(*)$, in zato tudi $ax + by = d$.

Dokazati moramo še, da je $\gcd(a, b) = d$. V izreku 4.12 smo že dokazali, da iz enakosti $ax + by = d$ sledi, da $\gcd(a, b)$ deli d. Dokazati moramo še, da d deli tako a kot b (in zato tudi $\gcd(a, b)$).

Razširjeni Evklidov algoritem se ustavi takrat, ko vrednost ostanka r_i pade na nič, število d, ki ga algoritem vrne, pa je zadnji neničelni ostanek

(označimo njegov indeks z n). Ker je $0 = r_{n+1} = r_{n-1} - kr_n = r_{n-1} - kd$, vidimo, da d deli r_{n-1}. Dokažimo, da d deli r_i za vsak $i \in \{0, \ldots, n\}$. Pa denimo, da temu ni tako, in vzemimo največji indeks j, za katerega r_n ne deli r_j (seveda $j \leq n-2$). Ker je $r_{j+2} = r_j - kr_{j+1}$, je $r_j = r_{j+2} + kr_{j+1}$. Iz definicije indeksa j sledi, da sta števili r_{j+1} in r_{j+2} deljivi z d, in zato tudi število r_j. To pa je v protislovju z našo predpostavko. S tem smo dokazali, da d res deli r_i za vsak $i \geq 0$, torej tudi $r_0 = a$ in $r_1 = b$. S tem je izrek dokazan. ∎

Trditev 4.13 nam pove, kako poiskati rešitev diofantske enačbe $ax + by = c$ kadar je $c = \gcd(a, b)$. Kaj pa, če je c nek pravi večkratnik števila $\gcd(a, b)$, na primer $c = t \gcd(a, b)$. Tedaj najprej z razširjenim evklidovim algoritmom poiščemo rešitev (x', y') enačbe $ax' + by' = \gcd(a, b)$. Če to enakost pomnožimo s številom t, vidimo, da je $x_0 = tx'$, $y_0 = ty'$ res rešitev prvotne diofantske enačbe.

ZGLED. *Poišči vse rešitve diofantske enačbe*

$$4333x + 623y = 21. \qquad (*)$$

Izvedimo razširjeni Evklidov algoritem z vhodnim podatkom $(a, b) = (4333, 623)$.

i	r_i	x_i	y_i	k_i
0	4333	1	0	
1	623	0	1	
2	595	1	−6	6
3	28	−1	7	1
4	7	22	−153	21
5	0	−89	619	4

Algoritem torej vrne trojico $(7, 22, -153)$. Trditev 4.13 tedaj pravi, da je $\gcd(4333, 623) = 7$ in

$$4333 \cdot 22 + 623 \cdot (-153) = 7.$$

Enakost pomnožimo s 3 in dobimo:

$$4333 \cdot 66 + 623 \cdot (-459) = 21.$$

Od tod razberemo, da je $x_0 = 66$ in $y_0 = -459$ rešitev enačbe $(*)$. Iz Izreka 4.12 sledi, da je poljubna rešitev enačbe $(*)$ enaka $x_k = 66 - \frac{623}{7}k = 66 + 89k$, $y_k = -459 + \frac{4333}{7}k = -459 + 619k$, za kak $k \in \mathbb{Z}$. ∎

4.5 Modularna aritmetika

DEFINICIJA 4.14 Naj bo m poljubno naravno število. Pravimo, da sta celi števili x in y *kongruentni po modulu* m, če in samo če m deli $y - x$. Pri tem pišemo

$$x \equiv y \pmod{m} \text{ ali tudi } x \equiv_m y.$$

Relacija kongruence je v tesni zvezi z operacijo celoštevilskega ostanka mod . Velja namreč naslednje:

TRDITEV 4.15 *Za poljubna števila* $x, y \in \mathbb{Z}$ *in* $m \in \mathbb{N}$ *velja*

$$x \equiv y \pmod{m} \;\Leftrightarrow\; x \bmod m = y \bmod m.$$

DOKAZ: Zapišimo $x = km + r$ in $y = \ell m + s$, kjer je $r = x \bmod m$ in $s = y \bmod m$. Če je $r = s$, tedaj očitno m deli število $y - x = m(\ell - k)$.

Denimo sedaj, da je $x \equiv y \pmod{m}$. Dokazati moramo, da od tod sledi $r = s$. Ker m deli število $y - x = (\ell - k)m + s - r$, je $(\ell - k) + s - r = tm$ za neki $t \in \mathbb{Z}$, in zato $s - r = m(t + k - \ell)$. Vendar števili s in r obe ležita na intervalu med 0 in $m - 1$, zato tudi njuna razlika po absolutni vrednosti ne presega števila $m - 1$. Iz zgornje enakosti tedaj sledi, da je $t + k - \ell = 0$, in zato $s = r$, kot je bilo potrebno dokazati. ∎

Kot kaže naslednji izrek, je relacija kongruence lepo uglašena z operacijama seštevanja in množenja.

IZREK 4.16 *Naj velja* $x_1 \equiv y_1 \pmod{m}$ *in* $x_2 \equiv y_2 \pmod{m}$. *Tedaj velja tudi*

$$x_1 + x_2 \equiv y_1 + y_2 \pmod{m} \;\text{ in }\; x_1 x_2 \equiv y_1 y_2 \pmod{m}.$$

DOKAZ: Pišimo $y_1 - x_1 = k_1 m$ in $y_2 - x_2 = k_2 m$. Tedaj je $(y_1 + y_2) - (x_1 + x_2) = (k_1 + k_2)m$, in zato $x_1 + x_2 \equiv y_1 + y_2 \pmod{m}$.

Pri dokazu druge kongruence moramo biti nekoli zviti. Računajmo:

$$y_1 y_2 - x_1 x_2 = y_1(y_2 - x_2) + (y_1 - x_1)x_2 = (y_1 k_2 + k_1 x_2)m.$$

Torej m deli razliko $y_1 y_2 - x_1 x_2$, in zato $x_1 x_2 \equiv y_1 y_2 \pmod{m}$. ∎

Od tod lahko z uporabo indukcije izpeljemo naslednji sklep.

TRDITEV 4.17 *Če je* $x \equiv y \pmod{m}$ *in* $r \in \mathbb{N}$, *tedaj je tudi* $x^r \equiv y^r \pmod{m}$.

Naslednji izrek pa nam pove, na kakšen način lahko iz kongruence krajšamo multiplikativne faktorje.

IZREK 4.18 *Naj bodo a, x, y poljubna cela števila, $a \neq 0$, in m poljubno naravno število. Tedaj velja naslednji sklep:*

$$ax \equiv ay \pmod{m} \;\Rightarrow\; x \equiv y \pmod{\frac{m}{\gcd(a,m)}}.$$

DOKAZ: Naj velja $ax \equiv ay \pmod{m}$. Tedaj obstaja $k \in \mathbb{Z}$, tako da je $ay - ax = km$. Na levi izpostavimo a in enakost delimo z $\gcd(a, m)$. Dobimo:

$$\frac{a}{\gcd(a,m)}(y - x) = k\frac{m}{\gcd(a,m)}.$$

Iz trditve 4.9 sledi, da sta števili $\frac{a}{\gcd(a,m)}$ in $\frac{m}{\gcd(a,m)}$ tuji. Trditev 4.10 pa tedaj pravi, da $\frac{m}{\gcd(a,m)}$ deli $y - x$, kot smo želeli pokazati. ∎

Zgornjo trditev največkrat uporabimo v dveh skrajnih primerih: ko je a tuj m in ko a deli m. Sklepa, ki ju dobimo v teh dveh primerih, zapišimo posebej:

POSLEDICA 4.19 *Naj velja $ax \equiv ay \pmod{m}$.*

(i) *Če je $\gcd(a, m) = 1$, tedaj je $x \equiv y \pmod{m}$.*

(ii) *Če a deli m, tedaj je $x \equiv y \pmod{\frac{m}{a}}$.*

4.6 Kolobar ostankov

Skozi ves razdelek naj m predstavlja poljubno fiksno naravno število, večje ali enako 2. Množico vseh možnih ostankov pri deljenju s številom m označimo takole:

$$\mathbb{Z}_m = \{0, 1, \ldots, m - 1\}.$$

Na množici ostankov $\mathbb{Z}_m$ definirajmo operaciji, ki ju bomo imenovali *seštevanje in množenje po modulu m* in označevali z $\oplus$ in $\odot$. Za $a, b \in \mathbb{Z}_m$ naj bo

$$a \oplus b = (a + b) \bmod m \;\text{ in }\; a \odot b = (ab) \bmod m.$$

Kot bomo videli, se ti dve operaciji v mnogočem obnašata podobno kot navadno seštevanje in množenje, zato bomo, kadar ne bo nevarnosti za pomoto, krožec okoli znakov $+$ in $\cdot$ izpuščali. Ni se težko prepričati, da operaciji $\oplus$ in $\odot$ zadoščata mnogim običajnim pravilom, ki veljajo za običajno seštevanje in množenje v množici celih števil. Na primer, za poljubne $x, y, z \in \mathbb{Z}_n$ velja naslednje:

1. $x \oplus y = y \oplus x$ in $x \odot y = y \odot x$ (komutativnost);
2. $(x \oplus y) \oplus z = x \oplus (y \oplus z)$ in $(x \odot y) \odot z = x \odot (y \odot z)$ (asociativnost);
3. $(x \oplus y) \odot z = (x \odot z) \oplus (y \odot z)$ (distributivnost);
4. $x \oplus 0 = x$, $x \odot 0 = 0$, $x \odot 1 = x$;
5. Za vsak $a \in \mathbb{Z}_n$ obstaja neki $b \in \mathbb{Z}_n$, za katerega je $a \oplus b = 0$ (namreč, za b lahko vzamemo element $n - a$).

V kolobarju $\mathbb{Z}_m$ se lahko nekateri elementi obnašajo nekoliko nenavadno. Oglejmo si na primer elementa 6 in 4 v $\mathbb{Z}_8$. Njun običajni produkt je enak 24, kar je deljivo z 8. Zato v $\mathbb{Z}_8$ velja enakost $6 \odot 4 = 0$. V kolobarju ostankov je torej produkt dveh neničelni Števil lahko enak 0. Takšna števila si zaslužijo ime: imenujemo jih *delitelji niča*. Ni težko razmisliti, da je neničelni element x kolobarja $\mathbb{Z}_m$ delitelj niča, če in samo če x ni tuj m.

4.7 Obrnljivi elementi v $\mathbb{Z}_n$

Naj bo n poljubno naravno število, večje ali enako 2. Zaradi enostavnejšega zapisa bomo v tem razdelku operaciji $\oplus$ in $\odot$ v kolobarju $\mathbb{Z}_n$ pisali kar kot običajna "plus" in "krat". Kadar bo obstajala nevarnosti za nesporazum, bomo posebej poudarili, ali imamo v mislih običajne operacije v $\mathbb{Z}$ ali pa gre za operacije v $\mathbb{Z}_n$.

Definicija 4.20 Naj bo x poljuben element kolobarja ostankov $\mathbb{Z}_n$. Če v $\mathbb{Z}_n$ obstaja element $\bar{x}$, za katerega v kolobarju $\mathbb{Z}_n$ velja $x\bar{x} = 1$, rečemo, da je element x obrnljiv v $\mathbb{Z}_n$, element $\bar{x}$ pa imenujemo *inverz* elementa x in ga označimo z x^{-1}.

Za zgled si oglejmo element 2 v $\mathbb{Z}_7$. Ker je $2 \cdot 4 = 8 \equiv 1 \pmod 7$, je 2 obrnljiv element v $\mathbb{Z}_7$ in $2^{-1} = 4$. Če si ogledamo spodnjo tabelico množenja v kolobarju $\mathbb{Z}_7$, se hitro prepričamo, da je v $\mathbb{Z}_7$ obrnljiv prav vsak neničelni element.

	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

Inverze lahko prečitamo iz spodnje tabele.

x	1	2	3	4	5	6
x^{-1}	1	4	5	2	3	6

Precej drugačna je situacija v kolobarju $\mathbb{Z}_6$. Oglejmo si tabelico množenja.

	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Vidimo, da sta edina obrnljiva elementa kolobarja $\mathbb{Z}_6$ števili 1 in 5. Pri tem, kot vedno, velja $1^{-1} = 1$. Nekoliko nenavadna pa je enakost $5^{-1} = 5$.

Vprašajmo se torej, ali znamo za dano naravno število n ugotoviti, kateri elementi kolobarja $\mathbb{Z}_n$ so obrnljivi, ne da bi izračunali celotno tabelico množenja. Odgovor se skriva v naslednjem izreku.

IZREK 4.21 *Neničelni element a kolobrja $\mathbb{Z}_n$ je obrnljiv, če in samo če je tuj proti številu n.*

DOKAZ: Problem prevedimo na običajne operacije med celimi števili. Element $a \in \mathbb{Z}_n$ je obrnljiv v $\mathbb{Z}_n$, če in samo če obstaja število x, za katerega je $ax \equiv 1 \pmod{n}$, oziroma, če in samo če obstajata celi števili x in y, za kateri je $ax - 1 = ny$. Takšni števili pa obstajata, če in samo če je rešljiva naslednja diofantska enačba

$$ax - ny = 1. \qquad (*)$$

Kot vemo, pa ima zgornja enačba rešitev, če in samo če sta števili a in n tuji. S tem je izrek dokazan. ∎

Dokaz pa nam je povedal tudi, kako inverz danega elementa dejansko izračunati. Potrebno je rešiti diofantsko enačbo $(*)$ in po potrebi poiskati tisto rešitev, za katero je x na intervalu med 0 in $n - 1$. (Premisli, da lahko takšno rešitev vedno najdemo.)

ZGLED. *Izračunaj* 31^{-1} *v* $\mathbb{Z}_{365}$

Rešiti moramo difantsko enačbo $31x - 365y = 1$. To lahko storimo z razširjenim Evklidovim algoritmom. ∎

Koliko obrnljivih elementov pa premore kolobar $\mathbb{Z}_n$? Kot pravi izrek 4.21, natanko toliko, kot je naravnih števil med 1 in $n-1$, ki so tuja številu n. Število takšnih števil je tako pomembno, da nosi svoje ime.

4.8 Eulerjeva funkcija

DEFINICIJA 4.22 Naj bo n poljubno naravno število, večje ali enako 2. Število tistih naravnih števil med 1 in $n-1$, ki so tuja n, označimo z $\varphi(n)$. Dodatno definiramo še $\varphi(1) = 1$. Tako definirani funkciji $\varphi\colon \mathbb{N} \to \mathbb{N}$ rečemo *Eulerjeva funkcija.*

TRDITEV 4.23 *Če je p praštevilo in r poljubno naravno število, je*

$$\varphi(p^r) = p^r - p^{r-1} = p^{r-1}(p-1) = p^r(1 - \frac{1}{p}).$$

Če sta a in b tuji naravni števili, je

$$\varphi(ab) = \varphi(a)\varphi(b).$$

Zgornja trditev nam omogoča, da izračunamo Eulerjevo funkcijo $\varphi(n)$ za vsako naravno število n, če ga le znamo razcepiti na prafaktorje. Namreč, če je

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

razcep števila n na prafaktorje, tedaj je

$$\varphi(n) = \varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2}) \cdots \varphi(p_k^{\alpha_k}) = p_1^{\alpha_1}(1 - \frac{1}{p_1})p_2^{\alpha_2}(1 - \frac{1}{p_2}) \cdots p_k^{\alpha_k}(1 - \frac{1}{p_k}) =$$

$$= n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \cdots (1 - \frac{1}{p_k}).$$

4.9 Mali Fermatov izrek in Eulerjev izrek

IZREK 4.24 (**Fermat**) *Naj bo p praštevilo in a naravno število, tuje p. Tedaj je $a^{p-1} \equiv 1 \bmod p$.*

Opomba. Zgornji izrek lahko povemo tudi v jeziku kolobarjev ostankov. Izrek namreč pravi, da za vsako praštevilo p in element $a \in \mathbb{Z}_p \setminus \{0\}$ velja $a^{p-1} = 1$.

DOKAZ: Oglejmo si elemente $a, 2a, 3a, \ldots, (p-1)a$ of $\mathbb{Z}_p$. Če sta dva izmed njih enaka, denimo $ia = ja$, potem z množenjem z a^{-1} v $\mathbb{Z}_p$ dobimo $i = j$ (spomni se, da je element a v $\mathbb{Z}_p$ obrnljiv, če je tuj proti p. S tem smo dokazali, da so zgoraj našteti elementi paroma različni, in ker jih je ravno $p-1$, tvorijo množico vseh neničelnih elementov v $\mathbb{Z}_p$:

$$\{a, 2a, 3a, \ldots, (p-1)a\} = \{1, 2, 3, \ldots, p-1\}.$$

Če zmnožimo vse elemente množic na levi in desni strani enakosti, dobimo naslednjo enakost v $\mathbb{Z}_p$:

$$(p-1)! = 1 \cdot 2 \cdot 3 \cdots (p-1) = a \cdot 2a \cdot 3a \cdots (p-1)a = (p-1)!a^{p-1}.$$

Vendar $(p-1)!$ je tuj proti p, zato ga smemo iz leve in desne strani enakosti v $\mathbb{Z}_p$ pokrajšati. Od to dobimo enakost $a^{p-1} = 1$ v $\mathbb{Z}_p$. ∎

Zgornji izrek pa lahko nekoliko posplošimo. Najprej opazimo, da je $\varphi(p) = p-1$ za vsako praštevilo p. Zato lahko izraz a^{p-1} interpretiramo tudi kot $a^{\varphi(p)}$. Ob tej interpretaciji se izkaže, da lahko pogoj, da je p praštevilo, izpustimo. Velja namreč naslednji izrek.

IZREK 4.25 (**Euler**) *Naj bo n poljubno naravno število in a število, ki je tuje n. Tedaj je $a^{\varphi(n)} \equiv 1 \bmod n$.*

Opomba. V jeziku kolobarjev ostankov zgornji izrek pravi, da je $a^{\varphi(n)} = 1$ za vsak obrnljiv element $a \in \mathbb{Z}_n^*$.

Dokaz Eulerjevega izreka je na las podoben dokazu malega Fermatovega izreka, le da namesto s števili $a, 2a, \ldots, (p-1)a$ pričnemo z elementi za, kjer z preteče vse obrnljive elemente iz $\mathbb{Z}_n^*$. Podrobnosti dokaza lahko izdela bralec sam.

ZGLED. *S pomočjo Eulerjevega izreka izračunaj* $1840^{1995} \bmod 26$

Najprej izračunamo $1840 \bmod 26 = 20$. Zato $1840^{1995} \equiv 20^{1995} \bmod 26$. Ker 20 ni tuje 26, Eulerjevega izreka ne moremo uporabiti takoj. Zato 20^{1995} pišemo kot $4^{1995} \cdot 5^{1995}$. Za razcep $20 = 4 \cdot 5$ smo se odložili zato, ker je 5 med delitelji števila 20 največji, ki je tuj 26.

Ker je $\gcd(5, 26) = 1$, lahko število $5^{1995} \bmod 26$ izračunamo neposredno s pomočjo Eulerjevega izreka. Ker je $\varphi(26) = 12$, najprej zapišemo $1995 = 12 \cdot 166 + 3$ in od tod dobimo

$$5^{1995} \equiv (5^{12})^{166} \cdot 5^3 \equiv 5^3 \equiv 21 \,(\bmod 26).$$

Pri računanju ostanka $4^{1995} \bmod 26$ moramo biti nekoliko iznajdljivejši. Najprej zapišemo $4^{1995} = 2^{3990}$ in označimo $x = 2^{3990} \bmod 26$. Tedaj je $x = 2^{3990} - 26q$, kjer $q = 2^{3990} \operatorname{div} 26$, in zato $x = 2y$ za neko naravno število y. Od tod dobimo $2y \equiv 2^{3990} \,(\bmod 26)$, od koder sledi $y \equiv 2^{3989} \,(\bmod 13)$, in zato $y = 2^{3989} \bmod 13$. Slednji ostanek pa lahko izračunamo s pomočjo Eulerjevega izreka (oziroma celo s pomočjo Fermatovega malega izreka). Ker je $\varphi(13) = 12$ in $3989 = 332 \cdot 12 + 5$, je

$$2^{3989} \equiv 2^5 \equiv 6 \bmod 13,$$

in torej $y = 6$ in $x = 12$. S tem smo dokazali kongruenco

$$4^{1995} \equiv 12 \,(\bmod 26).$$

Račun zaključimo takole:

$$1840^{1995} \equiv 20^{1995} \equiv 4^{1995} \cdot 5^{1995} \equiv 12 \cdot 5^3 \equiv 60 \cdot 25 \equiv 8 \cdot (-1) \equiv 18 \,(\bmod 26).$$

■

4.10 Kriptografski sistem RSA

Za zgled uporabe modularne aritmetike si oglejmo kriptografsko metodo, imenovano RSA, ki omogoča pošiljanje tajnih sporočil med več udeleženci, pri čemer vsebino tajnega sporočila lahko razbere le tisti, ki mu je bilo sporočilo poslano.

Sistem RSA sodi med kriptografke sisteme z javnim ključem. Posebnost teh sistemov je, da vsak udeleženec komunikacije, ki želi prejemati tajna sporočila od ostalih udeležencev, javno objavi svoj *javni ključ* (geslo), ki ga ostali uporabijo za šifriranje njemu namenjenih sporočil, v tajnosti pa ohrani svoj *privatni ključ*, ki je potreben za dešifriranje sporočil, ki so bila zašifrirana z njegovim javnim ključem. Varnost metode sledi na dejstvu, da je iz posameznikovega javnega ključa zelo težko (praktično neizvedljivo) izračunati njegov privatni ključ.

Opišimo na kratko, kaj mora storiti oseba A, ki bi od osebe B želela prejeti tajno sporočilo.

- Najprej naključno izbere dve praštevili, p in q, ter izračuna

$$n = pq, \quad \varphi = \varphi(n) = (p-1)(q-1).$$

  Za varnost sistema je zelo pomembno, da sta praštevili p in q tako veliki, da števila n nihče, razen osebe A, ne zna razcepiti na produkt praštevil. Danes se v praksi uporabljajo vsaj 100 mestna praštevila, kjer pa je potrebna večja varnost, pa še večja praštevila.

- Izbere poljubno število $e \in \mathbb{Z}_\varphi^*$ (število med 1 in $\varphi - 1$, ki je tuje φ) in s pomočjo razširjenega Evklidovega algoritma izračuna inverz

$$d = e^{-1} \in \mathbb{Z}_\varphi^*.$$

  V praksi število e izbremo tako, da naključno izberemo število med 1 in $\varphi - 1$, nato pa z razširjenim Evklidovim algoritmom testiramo, ali je število e res tuje številu φ; če ni, postopek izbire števila e ponovimo. Kot bomo videli kasneje, nekatere vrednosti števila e niso najbojše (na primer, $e = 1$), zato zavrnemo tudi morebitne takšne naključne izbire.

- Javno objavi števili n in e (javni ključ), sam pa varno shrani število d (privatni ključ). Ostale podatke "pozabi".

Zdaj pa si oglejmo, kaj mora storiti oseba B, ki želi osebi A poslati tajno sporočilo.

- Svoje tekstovno sporočilo najprej pretvori v število $m \in \mathbb{Z}_n$. To stori na javno znan način in tako, da bo vsak, ki bo poznal število m, brez težav rekonstruiral začetno tekstovno sporočilo. Če je tekstovno sporočilo predolgo, ga najprej razbije na manjše dele, jih pretvori v zaporedje števil v $\mathbb{Z}_n$, in izvede spodaj opisani postopek za vsak člen tega zaporedja.

- Prebere javni ključ (n, e) osebe A, izračuna število

$$c = m^e \bmod n$$

  in ga pošlje osebi A.

Ko oseba A prejme število c, uporabi svoj privatni ključ d in izračuna število

$$m' = c^d \bmod n.$$

Izkaže se, da je število m' kar enako originalnemu številu m. Nazadnje oseba A iz števila $m' = m$ rekonstruira tekstovno sporočilo osebe B.

Vidimo, da celotna metoda temelji na naslednji trditvi.

TRDITEV 4.26 *Naj bosta p in q različni praštevili in naj bo $n = pq$ ter $\varphi = (p-1)(q-1)$. Nadalje, naj bo e poljuben obrnljiv element kolobarja $\mathbb{Z}_\varphi$ in $d = e^{-1} \in \mathbb{Z}_\varphi^*$ njegov inverz. Tedaj za vsako celo število m, $1 \leq m \leq n-1$, iz enakosti $c = m^e \bmod n$ sledi enakost $c^d \bmod n = m$.*

DOKAZ: Ker je d inverz elementa e v $\mathbb{Z}_\varphi$, obstaja celo število x, za katerega je $ed - x\varphi = 1$. Tedaj

$$c^d \equiv m^{ed} = m^{1+x\varphi} = m \cdot (m^\varphi)^x \bmod n.$$

Če je $\gcd(m, n) = 1$, potem iz Eulerjevega izreka sledi $m^\varphi \equiv 1 \bmod n$, in zato $c^d \equiv m \bmod n$.

Predpostavimo torej lahko, da m ni tuj n. To se zgodi le, če bodisi p bodisi q deli število m. Brez izgube splošnoti lahko predpostavimo, da je m večkratnik števila p. Tedaj je tudi število $c^d = m^{ed}$ deljivo s p, in zato

$$c^d \equiv m \equiv 0 \bmod p.$$

Ker m ni hkrati deljiv tudi s q (saj bi sicer ne bil manjši od n), smemo uporabiti Fermatov izrek in ugotoviti, da je $m^{q-1} \equiv 1 \bmod q$. Zato velja

$$c^d = m^{ed} = m^{1+x\varphi} = m \cdot \left(m^{(q-1)}\right)^{(p-1)x} \equiv m \bmod q.$$

Od tod sledi, da imata števili $c^d \bmod n$ in m enaka ostanka pri deljenju s p kot tudi pri deljenju s q. Ni težko videti, da imata tedaj enaka ostanka tudi pri deljenju z $n = pq$. Ker sta obe števili manjši ali enaki n, sta zato enaki. ∎