Глава 1

Елементи теорије бројева

1.1 Увод

Теорија бројева је једна од најстаријих грана математике чијем су развоју значајан допринос дали антички математичари Диофант и Еуклид, а касније и неки од најзначајнијих математичара у историји, као што су Ојлер[1] и Гаус[2]. Теорија бројева је углавном током историје посматрана као област тзв. чисте, односно теоријске математике, која нема значајну практичну примену. Међутим, од средине 70-тих година 20. века долази до битне промене оваквог гледишта, да би данас ова математичка дисциплина постала једна од најзначајнијих у области криптографије и безбедне размене информација.

1.2 Дељивост

Теорија бројева се углавном бави проучавањем особина целих бројева. У овом поглављу, користићемо, без доказивања, нека својства скупа $\mathbb{N} = \{1, 2, \ldots\}$ природних бројева, као и скупа $\mathbb{Z} = \{\ldots, -2, -1, 0,$
$1, 2, \ldots\}$ целих бројева. Осим тога, скуп $\mathbb{N} \cup \{0\}$ означаваћемо са $\mathbb{N}_0$.

Појам дељивости је један од најједноставнијих, али истовремено и најважнијих појмова у теорији бројева. Скуп $\mathbb{Z}$ је затворен за операције сабирања, одузимања и множења, тј. збир, разлика или производ два цела броја је такође цео број. Међутим, са операцијом дељења то није случај. Питање дељивости у скупу $\mathbb{Z}$ је веома значајно у теорији бројева.

Дефиниција 1.1. *Цео број a **дељив** је целим бројем b ($b \neq 0$) ако постоји цео број q такав да је $a = bq$.*

Ако је број a дељив бројем b, пишемо $b \mid a$ (b дели a) и кажемо да је број

[1] Leonhard Euler (1707–1783), швајцарски математичар
[2] Johann Carl Friedrich Gauss (1777–1855), немачки математичар

b **делилац** броја a, односно да је број a **садржалац** броја b. Ако број a није дељив бројем b, пишемо $b \nmid a$ (b не дели a).

Основна својства релације дељивости изложена су у следећој теореми.

Теорема 1.1. *(i)* $a \mid a$, *за свако* $a \in \mathbb{Z} \setminus \{0\}$.

(ii) Ако $b \mid a$, *тада* $b \mid ac$ *за свако* $c \in \mathbb{Z}$.

(iii) Ако $b \mid a$ *и* $b \mid c$, *тада* $b \mid ax + cy$ *за све* $x, y \in \mathbb{Z}$.

(iv) Ако $b \mid a$ *и* $a \mid b$, *тада је* $a = b$ *или* $a = -b$.

(v) Ако $b \mid a$ *и* $a \mid c$, *тада* $b \mid c$.

(vi) Ако $b \mid a$ *и* $a \neq 0$, *тада је* $|b| \leqslant |a|$.

Уочимо да је релација дељивости релација парцијалног уређења на скупу $\mathbb{N}$, али не и на скупу $\mathbb{Z}$ (теорема 1.1(*iv*)).

Теорема 1.2. *Ако су у једнакости* $a_1 + a_2 + \cdots + a_n = 0$ *сви сабирци осим једног дељиви целим бројем* b, *онда је и тај сабирак дељив са* b.

Доказ. Нека су у датој једнакости сви сабирци осим a_i, $1 \leqslant i \leqslant n$, дељиви целим бројем b. Тада, према дефиницији 1.1, постоје цели бројеви $q_1, q_2, \ldots, q_{i-1}$, $q_{i+1}, \ldots, q_n$ такви да је

$$a_1 = bq_1,\ a_2 = bq_2,\ \ldots,\ a_{i-1} = bq_{i-1},\ a_{i+1} = bq_{i+1},\ \ldots,\ a_n = bq_n.$$

Сада из дате једнакости добијамо

$$a_i = -b(q_1 + q_2 + \cdots + q_{i-1} + q_{i+1} + \cdots + q_n) = bq_i,$$

где је $q_i = -(q_1 + q_2 + \cdots + q_{i-1} + q_{i+1} + \cdots + q_n) \in \mathbb{Z}$. Дакле, $b \mid a_i$. □

У скупу $\mathbb{Z}$ операција дељења није увек изводљива. Међутим, увек је могуће тзв. „дељење са остатком“, тј. важи следећа теорема.

Теорема 1.3. (**Теорема о остатку**) *За сваки цео број* a *и природан број* b *постоје јединствени цели бројеви* q *и* r *такви да је*

$$a = bq + r, \quad 0 \leqslant r < b.$$

При том се број q *назива* ***количник***, *а* r ***остатак*** *при дељењу броја* a *бројем* b.

Доказ. Посматрајмо скуп целих бројева $\{a - kb \mid k \in \mathbb{Z}\}$ и изаберимо у њему најмањи број који припада скупу $\mathbb{N}_0$ (егзистенција таквог броја следи из чињенице да је скуп природних бројева добро уређен). Нека је то број $a - qb$ и обележимо га са r. Тада је

$$a = bq + r, \quad 0 \leqslant r < b, \tag{1.1}$$

јер би у случају $r \geqslant b$ и број $a-(q+1)b = r-b < r$ припадао скупу $\mathbb{N}_0$, што је у контрадикцији са избором броја r. Тиме је доказана егзистенција бројева q и r. Докажимо још њихову јединственост. Претпоставимо да постоје и бројеви q_1 и r_1 такви да је

$$a = bq_1 + r_1, \quad 0 \leqslant r_1 < b. \tag{1.2}$$

Одузимањем (1.2) од (1.1) добијамо

$$0 = b(q - q_1) + (r - r_1),$$

одакле, на основу теореме 1.2, следи да $b \mid r - r_1$. Како је $\mid r - r_1 \mid < b$, мора бити $r - r_1 = 0$, тј. $r = r_1$, па је и $q = q_1$. □

Претпоставка да је b природан број у претходној теореми може се заменити захтевом да је b цео број различит од 0 и условом $0 \leqslant r < \mid b \mid$.

Пример 1.1. Одредити највећи природан број који подељен са 31 даје количник 17.

Решење. Тражени број a, чији је количник при дељењу са 31 једнак 17, према претходној теореми може се написати у облику $a = 31 \cdot 17 + r$, при чему је $0 \leqslant r < 31$. Највећи природан број описаног облика је $a = 31 \cdot 17 + 30 = 557$. △

Дефиниција 1.2. *Цео број d је **заједнички делилац** бројева a и b ако $d \mid a$ и $d \mid b$.*

Сваки цео број различит од 0 има коначно много делилаца, па је скуп заједничких делилаца два цела броја, од којих је бар један различит од 0, коначан и у њему постоји највећи број.

Дефиниција 1.3. *Највећи међу заједничким делиоцима бројева a и b, од којих је бар један различит од 0, је **највећи заједнички делилац** бројева a и b. Обележавамо га са (a, b), $NZD(a, b)$ или $D(a, b)$.*

У књизи ће, осим ако не назначимо другачије, бити коришћена ознака (a, b) за највећи заједнички делилац бројева a и b.

Дефиниција 1.4. *За бројеве a и b кажемо да су **узајамно** (**релативно**) **прости** ако је $(a, b) = 1$.*

Теорема 1.4. *Ако је d највећи заједнички делилац целих бројева a и b, онда постоје цели бројеви α и β такви да је $\alpha a + \beta b = d$. При томе важи да је највећи заједнички делилац целих бројева a и b најмањи позитиван број облика $\alpha a + \beta b$, $\alpha, \beta \in \mathbb{Z}$.*

Теорема 1.5. *Ако се цели број d може приказати у облику $d = \alpha a + \beta b$, $\alpha, \beta \in \mathbb{Z}$, онда $(a, b) \mid d$. Специјално, ако је $\alpha a + \beta b = 1$, онда су бројеви a и b узајамно прости.*

Доказ. Нека је $D = (a, b)$. Тада постоје цели бројеви q_1 и q_2 такви да је $a = Dq_1$ и $b = Dq_2$, па је $d = \alpha a + \beta b = \alpha D q_1 + \beta D q_2 = D(\alpha q_1 + \beta q_2)$, одакле следи да $D = (a, b) \mid d$.

Ако је $\alpha a + \beta b = 1$, тада $(a, b) \mid 1$, одакле следи да је $(a, b) = 1$, тј. бројеви a и b су узајамно прости. □

Неке значајне особине највећег заједничког делиоца су исказане у следећој теореми.

Теорема 1.6. *(i) Ако је $k > 0$, тада је $(ka, kb) = k(a, b)$.*

(ii) Ако је $a = bq$ и $b \geqslant 0$, онда је $(a, b) = b$.

(iii) Ако $c \mid ab$ и при томе је $(c, a) = 1$, тада $c \mid b$.

(iv) $(ab, c) = 1$ ако и само ако је $(a, c) = 1$ и $(b, c) = 1$.

(v) Ако је $a = bq + r$, тада је $(a, b) = (b, r)$.

(vi) Ако је d произвољан заједнички делилац бројева a и b, тада $d \mid (a, b)$.

(vii) Важи да је $\left(\dfrac{a}{(a,b)}, \dfrac{b}{(a,b)}\right) = 1$, тј. бројеви $a_1 = \dfrac{a}{(a,b)}$ и $b_1 = \dfrac{b}{(a,b)}$ су узајамно прости.

Доказ. Доказаћемо нека од ових тврђења, која су једноставнија или пак значајна за доказ Еуклидовог алгоритма о коме ће касније бити речи.

(ii) Како $b \mid a$ (јер је $a = bq$) и $b \mid b$ (због рефлексивности релације дељивости), следи да је b заједнички делилац бројева a и b. Број $b \geqslant 0$ не може имати ниједан делилац $c > b$, одакле следи да је $(a, b) = b$.

(iii) Како је $(c, a) = 1$, према теореми 1.4 следи да постоје цели бројеви γ и α такви да је $\gamma c + \alpha a = 1$, па је $\gamma cb + \alpha ab = b$. Како по претпоставци $c \mid ab$ и важи да $c \mid cb$, следи, према теореми 1.2, да $c \mid b$.

(v) Нека је $d_1 = (a, b)$ и $d_2 = (b, r)$. Тада из услова $a = bq + r$ следи да $d_1 \mid r$ (јер $d_1 \mid a$ и $d_1 \mid b$, па $d_1 \mid (a - bq) = r$), тј. d_1 је заједнички делилац бројева b и r, па је $d_1 \leqslant d_2$.

Осим тога, из услова $a = bq + r$ следи да $d_2 \mid a$ (јер $d_2 \mid b$ и $d_2 \mid r$, па $d_2 \mid (bq + r) = a$), тј. d_2 је заједнички делилац бројева a и b, па је $d_2 \leqslant d_1$. Како је $d_1 \leqslant d_2$ и $d_2 \leqslant d_1$, то је $d_1 = d_2$, тј. $(a, b) = (b, r)$. □

Нагласимо да из услова $c \mid ab$, без додатне претпоставке $(c, a) = 1$, не следи да $c \mid b$ (тврђење *(iii)*). На пример, $10 \mid 4 \cdot 15$, али $10 \nmid 4$ и $10 \nmid 15$.

Питање дељивости целих бројева не зависи од њиховог знака, па се можемо ограничити на дељивост природних бројева. У наставку ћемо изложити поступак за одређивање највећег заједничког делиоца два природна броја, познат као **Еуклидов алгоритам**. На основу теореме 1.3 можемо записати следећи низ

једнакости

$$
\begin{aligned}
a &= bq_1 + r_1, && 0 \leqslant r_1 < b,\\
b &= r_1q_2 + r_2, && 0 \leqslant r_2 < r_1,\\
r_1 &= r_2q_3 + r_3, && 0 \leqslant r_3 < r_2,\\
&\vdots\\
r_{n-2} &= r_{n-1}q_n + r_n, && 0 \leqslant r_n < r_{n-1},\\
r_{n-1} &= r_nq_{n+1}.
\end{aligned}
\tag{1.3}
$$

Како бројеви r_n чине строго опадајући низ природних бројева, након коначно много корака долазимо до $r_{n+1} = 0$, тј. до једнакости $r_{n-1} = r_nq_{n+1}$, која говори о дељивости два узастопна остатка.

Теорема 1.7. *Последњи остатак r_n који је различит од нуле у једнакостима* (1.3) *представља највећи заједнички делилац бројева a и b.*

Доказ. На основу теореме 1.6(v) важе следеће једнакости

$$(a, b) = (b, r_1) = (r_1, r_2) = \cdots = (r_{n-2}, r_{n-1}) = (r_{n-1}, r_n).$$

Како је $r_{n-1} = r_nq_{n+1}$, то према теореми 1.6(ii) важи да је $(r_{n-1}, r_n) = r_n$, па је $(a, b) = r_n$. □

Пример 1.2. Применом Еуклидовог алгоритма одредити $(252, 198)$.

Решење. Како је

$$
\begin{aligned}
252 &= 198 \cdot 1 + 54\\
198 &= 54 \cdot 3 + 36\\
54 &= 36 \cdot 1 + 18\\
36 &= 18 \cdot 2,
\end{aligned}
$$

следи да је $(252, 198) = 18$. △

Према теореми 1.4 највећи заједнички делилац целих бројева a и b може се приказати као њихова линеарна комбинација, тј. у облику $\alpha a + \beta b$, $\alpha, \beta \in \mathbb{Z}$. Бројеве α и β можемо ефективно одредити применом Еуклидовог алгоритма, што ће бити показано у следећем примеру.

Пример 1.3. Одредити целе бројеве α и β такве да је $\alpha \cdot 252 + \beta \cdot 198 = (252, 198)$.

Решење. На основу претходног примера важи да је $(252, 198) = 18$, као и

$$
\begin{aligned}
18 &= 54 - 36 \cdot 1 = 54 - (198 - 54 \cdot 3) \cdot 1 = 4 \cdot 54 - 1 \cdot 198\\
&= 4 \cdot (252 - 198 \cdot 1) - 1 \cdot 198 = 4 \cdot 252 - 5 \cdot 198.
\end{aligned}
$$

△

Представљање највећег заједничког делиоца бројева a и b у облику њихове целобројне линеарне комбинације биће нам веома значајно код решавања тзв. линеарних Диофантових једначина о чему ће бити речи касније.

Дефиницију највећег заједничког делиоца можемо проширити и на скуп од n произвољних целих бројева.

Дефиниција 1.5. *Највећи заједнички делилац n целих бројева $a_1, a_2, \ldots, a_n$, од којих је бар један различит од нуле, је највећи од заједничких делилаца ових бројева и обележавамо га са $(a_1, a_2, \ldots, a_n)$. Ако је $(a_1, a_2, \ldots, a_n) = 1$, бројеви $a_1, a_2, \ldots, a_n$ су* ***узајамно*** *(****релативно****)* ***прости.***

Бројеви $a_1, a_2, \ldots, a_n$ су ***узајамно*** *(****релативно****)* ***прости у паровима*** *ако је $(a_i, a_j) = 1$ за $i, j = 1, 2, \ldots, n$, $i \neq j$.*

Пример 1.4. Бројеви $5, 11, 15$ су узајамно прости, тј. $(5, 11, 15) = 1$, али нису узајамно прости у паровима, јер је $(5, 15) = 5$.

Дефиниција 1.6. *Заједнички садржалац целих бројева a и b, различитих од нуле, је број који је дељив сваким од њих. Најмањи међу позитивним заједничким садржаоцима бројева a и b зове се најмањи заједнички садржалац ових бројева и обележава са $[a, b]$ или $NZS(a, b)$ или $S(a, b)$.*

Ми ћемо надаље користити ознаку $[a, b]$ за најмањи заједнички садржалац бројева a и b.

Дефиниција најмањег заједничког садржаоца се такође може проширити на скуп од n произвољних целих бројева различитих од нуле.

1.3 Прости бројеви

Дефиниција 1.7. *Цео број $p > 1$ је* ***прост*** *ако нема ниједан делилац d такав да је $1 < d < p$. Цео број $m > 1$ који није прост је* ***сложен*** *број.*

Прости бројеви су $2, 3, 5, 7, 11, 17, \ldots$, а сложени $4, 6, 8, 10, \ldots$

Теорема 1.8. *Природан број $n > 1$ је сложен ако и само ако има прост фактор p, такав да је $p \leqslant \sqrt{n}$.*

Доказ. Ако број $n > 1$ има прост фактор $p \leqslant \sqrt{n}$, онда је он према дефиницији 1.7 сложен број. Обрнуто, нека је p најмањи прост фактор сложеног броја n. Тада постоји природан број m такав да је $n = pm$, при чему је $m \geqslant p$. Одавде је $n = pm \geqslant p^2$, тј. $p \leqslant \sqrt{n}$. □

Претходну теорему можемо искористити при налажењу свих простих бројева мањих од датог природног броја n поступком који је познат као **Ератостеново сито**. Најпре исписујемо све природне бројеве од 1 до n.

$$\not{1}, 2, 3, \not{4}, 5, \not{6}, 7, \not{8}, \not{9}, \not{10}, 11, \not{12}, 13, \not{14}, \not{15}, \not{16}, 17, \not{18}, 19, \ldots, n.$$

Затим, прецртамо број 1. Како је 2 први прост број, прецртамо све бројеве дељиве са 2 и веће од 2 (они су сложени). Следећи прост број је 3. Прецртамо све бројеве веће од 3 који су дељиви са 3. Следећи непрецртан број је 5, па је дакле он прост, јер би у супротном већбио прецртан. Први непрецртани садржалац броја 5 је $25 = 5^2$. Настављајући описани поступак издвојићемо („кроз сито ће проћи“) све просте бројеве мање од n. Имајући у виду теорему 1.8 закључујемо да се поступак прекида када прецртамо све сложене бројеве који су садржаоци простих бројева не већих од $\sqrt{n}$.

Теорема 1.9. (**Еуклид**) *Од сваког простог броја постоји већи прост број, тј. постоји бесконачно много простих бројева.*

Доказ. Претпоставимо супротно, тј. да постоји коначно много простих бројева. Нека су то бројеви $p_1, p_2, \ldots, p_k$, а сви остали природни бројеви већи од 1 су сложени. Број

$$n = p_1 p_2 \cdots p_k + 1$$

је сложен према претпоставци, па мора бити дељив неким простим бројем. Међутим, то је немогуће, јер при дељењу било којим од простих бројева $p_1, p_2, \ldots, p_k$ даје остатак 1, одакле следи да је тврђење теореме истинито. □

Теорема 1.10. (**Еуклидова лема**) *Ако је p прост број и $p \mid ab$, тада $p \mid a$ или $p \mid b$. Важи и општије, ако $p \mid a_1 a_2 \cdots a_n$, тада $p \mid a_i$, за неко $i = 1, 2, \ldots, n$.*

Доказ. Нека $p \mid ab$ и претпоставимо да $p \nmid a$. Како су једини делиоци простог броја p бројеви 1 и p, следи да је $(p, a) = 1$, па према теореми 1.6(iii) важи да $p \mid b$.

Општије тврђење доказујемо индукцијом по броју чинилаца n. □

Користећи претходну теорему доказаћемо следећу, веома важну теорему теорије бројева.

Теорема 1.11. (**Основни став аритметике**) *Сваки природан број $n > 1$ може се на јединствен начин представити у облику производа простих чинилаца (са тачношћу до њиховог поретка), тј. за сваки природан број $n > 1$ постоје јединствени прости бројеви $p_1, p_2, \ldots, p_k$, такви да је $p_1 < p_2 < \cdots < p_k$, и јединствени цели бројеви $\alpha_1, \alpha_2, \ldots, \alpha_k$, тако да је*

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

Доказ. Ако је n прост број, тврђење очигледно важи. Претпоставимо да тврђење важи за сваки сложен број мањи од n. Ако је n сложен број, тада се n може написати у облику $n = n_1 n_2$, при чему $1 < n_1, n_2 < n$. Бројеви n_1 и n_2 су или прости или се по индуктивној претпоставци могу приказати као производ простих чинилаца, одакле следи да и број n има то својство. Групишући једнаке просте факторе броја n, закључујемо да се сваки природан број $n > 1$ може представити у облику

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}, \tag{1.4}$$

где су $p_1 < p_2 < \cdots < p_k$ прости бројеви и $\alpha_1, \alpha_2, \ldots, \alpha_k$ природни бројеви.

Представљање броја $n > 1$ у облику (1.4) познато је као **канонска факторизација** броја n.

Докажимо да је представљање броја n у облику (1.4) јединствено. Претпоставимо супротно, тј. да број $n > 1$ има две такве факторизације

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}, \quad p_1 < p_2 < \cdots < p_k, \quad \alpha_1, \alpha_2, \ldots, \alpha_k \in \mathbb{N},$$

и

$$n = q_1^{\beta_1} q_2^{\beta_2} \cdots q_s^{\beta_s}, \quad q_1 < p_2 < \cdots < q_s, \quad \beta_1, \beta_2, \ldots, \beta_s \in \mathbb{N}. \tag{1.5}$$

Како $p_i \mid q_1^{\beta_1} q_2^{\beta_2} \cdots q_s^{\beta_s}$, $1 \leqslant i \leqslant k$, према теореми 1.10 постоји индекс j, $1 \leqslant j \leqslant s$, такав да $p_i \mid q_j$, одакле, пошто су p_i и q_j прости бројеви, следи да је $p_i = q_j$. Дакле, $\{p_1, p_2, \ldots, p_k\} \subseteq \{q_1, q_2, \ldots, q_s\}$. Аналогно се показује да је и $\{q_1, q_2, \ldots, q_s\} \subseteq \{p_1, p_2, \ldots, p_k\}$, па је $\{p_1, p_2, \ldots, p_k\} = \{q_1, q_2, \ldots, q_s\}$. Закључујемо да је $k = s$, а како су низови $p_1, p_2, \ldots, p_k$ и $q_1, q_2, \ldots, q_s$ растући, важи да је $p_1 = q_1, p_2 = q_2, \ldots, p_k = q_k$, одакле следи да се једнакост (1.5) може написати у облику

$$n = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}. \tag{1.6}$$

Докажимо још да је $\alpha_i = \beta_i$, $1 \leqslant i \leqslant k$. Претпоставимо да је $\alpha_1 \neq \beta_1$ и нека је, на пример, $\alpha_1 < \beta_1$, тј. $\beta_1 = \alpha_1 + \gamma$, $\gamma > 0$. Ако поделимо израз на десној страни сваке од једнакости (1.4) и (1.6) са $p_1^{\alpha_1}$ добијамо

$$p_2^{\alpha_2} \cdots p_k^{\alpha_k} = p_1^{\gamma} p_2^{\alpha_2} \cdots p_k^{\alpha_k},$$

одакле следи да p_1 дели десну, а не дели леву страну последње једнакости, што је немогуће, па мора бити $\alpha_1 = \beta_1$. Аналогно се доказује да је $\alpha_i = \beta_i$, $i = 2, \ldots, k$, одакле следи јединственост факторизације. □

Помоћу канонске факторизације датих бројева a и b лако се одређује њихов највећи заједнички делилац и најмањи заједнички садржалац.

Теорема 1.12. *Нека су* $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ *и* $b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$, $\alpha_i, \beta_i \geqslant 0$, $i = 1, 2, \ldots, k$, *канонске факторизације природних бројева* a *и* b. *Тада*

(*i*) $b \mid a \Leftrightarrow \beta_i \leqslant \alpha_i, \quad i = 1, 2, \ldots, k.$

(*ii*) $(a, b) = p_1^{\min\{\alpha_1, \beta_1\}} p_2^{\min\{\alpha_2, \beta_2\}} \cdots p_k^{\min\{\alpha_k, \beta_k\}}.$

(*iii*) $[a, b] = p_1^{\max\{\alpha_1, \beta_1\}} p_2^{\max\{\alpha_2, \beta_2\}} \cdots p_k^{\max\{\alpha_k, \beta_k\}}.$

На основу претходне теореме може се закључити да важи следеће тврђење.

Последица 1.1. *За целе бројеве* a *и* b *важи да је*

$$(a, b) \cdot [a, b] = |a\, b|.$$

Коришћењем канонске факторизације природног броја a могуће је одредити укупан број позитивних делилаца тог броја.

Теорема 1.13. *Нека је $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ канонска факторизација природног броја a. Тада укупан број свих позитивних делилаца броја a (укључујући 1 и a), у ознаци $\tau(a)$, одређен је са*

$$\tau(a) = (\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_k + 1).$$

Пример 1.5. За бројеве $a = 2^2 \cdot 5^3 \cdot 11$ и $b = 2 \cdot 3^2 \cdot 5 \cdot 7^4$ важи да је $(a, b) = 2 \cdot 5 = 10$, $[a, b] = 2^2 \cdot 3^2 \cdot 5^3 \cdot 7^4 \cdot 11$ и $\tau(a) = (2 + 1) \cdot (3 + 1) \cdot (1 + 1) = 24$.

1.4 Конгруенције

Дефиниција 1.8. *Нека је $m > 1$ природан број. Цели бројеви a и b су конгруентни по модулу m ако $m \mid a - b$. Пише се $a \equiv b \pmod{m}$.*

Пример 1.6. $17 \equiv 5 \pmod{12}$, $7 \equiv 7 \pmod{12}$ и $36 \equiv 0 \pmod{12}$. Слично, $6 \equiv -14 \pmod{20}$.

Користећи дефиницију релације конгруенције по модулу m лако се закључује да важе следећа тврђења.

Теорема 1.14. *(i) $a \equiv b \pmod{m}$ ако и само ако је $a = mk + b$ за неки цео број k.*

(ii) $a \equiv b \pmod{m}$ ако и само ако бројеви a и b дају исти остатак при дељењу са m.

(iii) Бити конгруентан по датом модулу је релација еквиваленције у скупу $\mathbb{Z}$.

Осим тога, неке особине конгруенција дате су у следећој теореми.

Теорема 1.15. *(i) Ако је $a \equiv b \pmod{m}$ и $c \equiv d \pmod{m}$, тада је $ax + cy \equiv bx + dy \pmod{m}$, за свака два цела броја x и y.*

(ii) Ако је $a \equiv b \pmod{m}$ и $c \equiv d \pmod{m}$, тада је $ac \equiv bd \pmod{m}$.

(iii) Ако је $a \equiv b \pmod{m}$ и $m = kd$, $d > 1$, тада је $a \equiv b \pmod{d}$.

(iv) Ако је $a \equiv b \pmod{m}$, онда је $P(a) \equiv (b) \pmod{m}$, где је $P(x)$ полином са целобројним коефицијентима.

Дефиниција 1.9. *Број природних бројева који нису већи од датог природног броја m и узајамно су прости са њим означава се са $\varphi(m)$. Функција φ зове се* ***Ојлерова функција****.*

Ако је p прост број, тада је $\varphi(p) = p - 1$.

Пример 1.7. Важи да је $\varphi(4) = 2$, $\varphi(6) = 2$, $\varphi(7) = 6$, $\varphi(9) = 6$, итд.

Ојлерова функција неког природног броја се може лако израчунати коришћењем његове канонске факторизације.

Теорема 1.16. *Ако је* $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ *канонска факторизација броја* n*, тада је*

$$\begin{aligned}\varphi(n) &= n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right)\\ &= p_1^{\alpha_1-1}p_2^{\alpha_2-1}\cdots p_k^{\alpha_k-1}(p_1-1)(p_2-1)\cdots(p_k-1).\end{aligned}$$

Ова функција је веома важна, јер се помоћу ње може осказати следећа (Ојлерова) теорема.

Теорема 1.17. (**Ојлер**) *Ако је* $(a,m)=1$*, тада је* $a^{\varphi(m)} \equiv 1 \pmod{m}$.

Специјалан случај Ојлерова теореме је следећа теорема.

Теорема 1.18. (**Мала Фермаова**[3] **теорема**) *Ако је* p *прост број и* $p \nmid a$*, онда је* $a^{p-1} \equiv 1 \pmod{p}$.

Доказ. Ако је p прост број и $p \nmid a$, тада је $(a,p)=1$, па према Ојлеровој теореми важи да је $a^{\varphi(p)} \equiv 1 \pmod{p}$. За прост број p је $\varphi(p) = p-1$, одакле следи тврђење. □

Последица 1.2. *Ако је* p *прост број и* a *произвољан цео број, тада је* $a^p \equiv a \pmod{p}$.

Доказ. Ако $p \nmid a$, тада је према претходној теореми $a^{p-1} \equiv 1 \pmod{p}$, одакле следи да је $a^p \equiv a \pmod{p}$. Ако $p \mid a$, тада $p \mid a^p - a$, тј. $a^p \equiv a \pmod{p}$. □

[3] Pierre de Fermat (1601–1665), француски математичар