ТЕОРИЈА БРОЈЕВА

Припреме за ЈБМО, 11. јун 2004.

Владимир Балтић

1 Дељивост бројева

Још од античких времена људе су занимала нека својства бројева. На пример, у Вавилону, хиљаду година пре Питагоре, математичари су знали како систематски да нађу Питагорине бројеве, тј. целе бројеве који чине странице правоуглог троугла.

Прво ћемо увести основне појмове из теорије бројева као што су дељивост, највећи заједнички делитељ, прости и сложени бројеви, а затим ћемо прећи на конгруенције и њихове особине. Све теореме наводимо без доказа. Основни скупови који се разматрају су скуп природних бројева $\mathbb{N} = \{1, 2, 3, \dots\}$ и скуп целих бројева $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$, а основна релација је дељивост.

Дефиниција 1. Цео број a је дељив целим бројем $b \neq 0$, ако постоји цео број q такав да је $a = bq$.

Ако број b дели број a, то се означава са $b \mid a$ (Руси користе и ознаку $a \vdots b$ за a је дељив бројем b). Тада још кажемо да је b делилац броја a. Ако b не дели a, то се пише $b \nmid a$. Тако, на пример, важи да $3 \mid 15$ и $6 \nmid 15$. Већ на основу ове дефиниције можемо да докажемо неколико особина дељивости целих бројева:

Теорема 1. Нека су n, m, a, b и d произвољни цели бројеви, тада важи

а) $n \mid n$. (особина рефлексије)

б) $d \mid n$ и $n \mid m$ повлачи $d \mid m$. (особина транзитивности)

в) $d \mid n$ и $d \mid m$ повлачи $d \mid (an + bm)$. (особина линеарности)

г) $d \mid n$ повлачи $ad \mid an$. (особина мултипликативности)

д) $ad \mid an$ и $a \neq 0$ повлачи $d \mid n$. (особина скраћивања)

ђ) $1 \mid n$. (1 дели сваки број)

е) $n \mid 0$. (сваки број дели 0)

ж) $d \mid n$ повлачи $-d \mid n$ и $d \mid -n$.

з) $d \mid n$ и $n \neq 0$ повлачи $|d| \leqslant |n|$.

и) $d \mid n$ и $n \mid d$ повлачи $|d| = |n|$, тј. $d = n$ или $d = -n$.

ј) $d \mid n$ повлачи $\dfrac{n}{d} \mid n$.

Пример 1. Сада ћемо дати неке од критеријума дељивости природних бројева са неким од бројева.

- 2: Број n је дељив са 2 (или другачије речено, број n је паран) $\Leftrightarrow$ се завршава парном цифром, односно неком од цифара 0, 2, 4, 6 или 8.
- 3: Број n је дељив са 3 $\Leftrightarrow$ је збир цифара броја n дељив са 3.
- 4: Број n је дељив са 4 $\Leftrightarrow$ се завршава двоцифреним бројем који је дељив са 4.
- 5: Број n је дељив са 5 $\Leftrightarrow$ се завршава неком од цифара 0 или 5.
- 6: Број n је дељив са 6 $\Leftrightarrow$ је дељив и са 2 и са 3.
- 7: Број $n = \overline{a_k a_{k-1} \dots a_3 a_2 a_1}$ је дељив са 7 $\Leftrightarrow$ је и број $m = \overline{a_3 a_2 a_1} - \overline{a_6 a_5 a_4} + \overline{a_9 a_8 a_7} - \dots$ дељив са 7.
- 7: Број n је дељив са 7 $\Leftrightarrow$ је и број m, који се добија тако што избришемо цифру јединица броја n и од тог броја одузмемо двоструку цифру јединица броја n, дељив са 7.
- 8: Број n је дељив са 8 $\Leftrightarrow$ се завршава троцифреним бројем који је дељив са 8.
- 9: Број n је дељив са 9 $\Leftrightarrow$ је збир цифара броја n дељив са 9.
- 10: Број n је дељив са 10 $\Leftrightarrow$ се завршава цифром 0.
- 11: Број $n = \overline{a_k a_{k-1} \dots a_3 a_2 a_1}$ је дељив са 11 $\Leftrightarrow$ је и број $m = a_1 - a_2 + a_3 - a_4 + \dots$ дељив са 7.
- 13: Број $n = \overline{a_k a_{k-1} \dots a_3 a_2 a_1}$ је дељив са 13 $\Leftrightarrow$ је и број $m = \overline{a_3 a_2 a_1} - \overline{a_6 a_5 a_4} + \overline{a_9 a_8 a_7} - \dots$ дељив са 13.
- 25: Број n је дељив са 25 $\Leftrightarrow$ се завршава двоцифреним бројем који је дељив са 25.
- 27: Број $n = \overline{a_k a_{k-1} \dots a_3 a_2 a_1}$ је дељив са 27 $\Leftrightarrow$ је и број $m = \overline{a_3 a_2 a_1} + \overline{a_6 a_5 a_4} + \overline{a_9 a_8 a_7} + \dots$ дељив са 27.
- 37: Број $n = \overline{a_k a_{k-1} \dots a_3 a_2 a_1}$ је дељив са 37 $\Leftrightarrow$ је и број $m = \overline{a_3 a_2 a_1} + \overline{a_6 a_5 a_4} + \overline{a_9 a_8 a_7} + \dots$ дељив са 37.
- 100: Број n је дељив са 100 $\Leftrightarrow$ се завршава са две цифре 0 (тј. са 00).

Следећа теорема говори о томе да ако посматрамо два цела броја a и b и извршимо дељење a/b ($a \neq 0$), онда постоји само један цео број q (*делимични количник*) и само један ненегативан цео број r мањи од $|b|$ (*остатак*) тако да је

$$a = bq + r, \qquad 0 \leqslant r < |b|. \tag{1}$$

Убрзо ћемо видети колико је јединственост овог записа важна.

Теорема 2. (Алгоритам дељења) Ако је $a \in \mathbb{Z}$ и $b \in \mathbb{N}$, онда a може на јединствен начин да се представи као

$$a = bq + r, \qquad (q, r \in \mathbb{Z}, 0 \leqslant r < b).$$

Дефиниција 2. Цео број d за који важи $d \mid a$ и $d \mid b$ назива се *заједнички делилац* бројева a и b. Цео број s за који важи $a \mid s$ и $b \mid s$ назива се *заједнички садржалац* бројева a и b.

Како делилац бројева не може бити већи од апсолутне вредности тог броја, видимо да међу заједничким делиоцима бројева a и b постоји највећи. Слично међу садржаоцима постоји најмањи.

Дефиниција 3. Највећи број у скупу делилаца бројева a и b се назива највећи заједнички делилац та два броја и обележава се са НЗД(a, b) или (a, b). Најмањи (позитиван) број у скупу садржалаца бројева a и b се назива најмањи заједнички садржалац та два броја и обележава се са НЗС(a, b) или $[a, b]$.

Ако су два броја узајамно проста, тј. ако немају заједничких фактора, онда им је највећи заједнички делилац 1, тј. $(a, b) = 1$. Због тога се чињеница да су a и b узајамно прости симболички пише баш тако, $(a, b) = 1$.

Теорема 3. Постоје цели бројеви x_0 и y_0 тако да је

$$(a, b) = ax_0 + by_0,$$

ако барем један од бројева a и b није нула.

Уствари лако се види да је (a, b) најмања позитивна вредност функције $ax + by$ кад x и y пролазе скупом $\mathbb{Z}$.

Теорема 4. а) $(ma, mb) = m(a, b)$, за $m \in \mathbb{N}$.
б) Ако $d \mid a, d \mid b$ и $d > 0$, онда је $(\frac{a}{d}, \frac{b}{d}) = \frac{1}{d}(a, b)$.
в) $(\frac{a}{(a,b)}, \frac{b}{(a,b)}) = 1$.
г) Ако је $(a, m) = (b, m) = 1$, онда је $(ab, m) = 1$.
д) Ако $c \mid ab$ и $(b, c) = 1$, онда $c \mid a$.

Везу између највећег заједничког делиоца и најмањег заједничког садржаоца бројева a и b даје нам следећа теорема:

Теорема 5. а) Ако $a_1 \mid b, a_2 \mid b, \ldots, a_n \mid b$, онда $[a_1, \ldots, a_n] \mid b$.
б) Ако је $m \leqslant 1$, онда је $[ma, mb] = m[a, b]$.
в) $(a, b) \cdot [a, b] = |a \cdot b|$.

2 Прости бројеви и основни став аритметике

Дефиниција 4. (Прости и сложени бројеви) Природни бројеви $p \in \mathbb{N}$ који имају тачно два делиоца називају се *прости бројеви*. Природни бројеви ($\neq 1$) који нису прости су *сложени бројеви*.

Наравно та два делиоца су 1 и p. Напоменимо да број 1 није прост број.

Низ простих бројева почиње овако: $2, 3, 5, 7, 11, 13, 17, 19, \ldots$ Најлакши начин да се овај низ настави јесте метод познат као *Ератостеново сито*: ако желимо да нађемо све просте бројеве мање од n, прво треба да испишемо све природне бројеве од 2 до $n-1$ и да редом из списка елиминишемо све парне бројеве изузев броја 2, затим све дељиве са 3, изузев самог броја 3, затим слично за 5, 7 итд. све до последњег природног броја мањег од $\sqrt{n}$. Приметимо да после елиминације парних бројева није више потребно тражити бројеве дељиве са 4, 6 итд. јер су ти сви бројеви парни, па су већ избачени. Слично, после елиминације бројева дељивих

са 3, више није потребно тражити бројеве дељиве са 6, 9 итд. Дакле, да би одредили просте бројеве $< n$. користимо просте бројеве мање од $\sqrt{n}$.

Пример 2. Да бисмо помоћу Ератостеновог сита одредили све просте бројеве < 100, треба редом да елиминишемо све бројеве дељиве са 2, 3, 5 и 7 (то су прости бројеви мањи од $\sqrt{100} = 10$). На тај начин добијамо:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97.$$

Укупно има 25 простих бројева мањих од 100.

Теорема 6. Сваки природан број $n > 1$ је или прост или је производ простих бројева.

Теорема 7. Ако прост број $p \nmid a$ онда је $(a, p) = 1$.

Теорема 8. Ако $p \mid ab$, онда $p \mid a$ или $p \mid b$. Општије, ако $p \mid a_1 a_2 \dots a_n$, тада p дели барем један од бројева $a_1, a_2, \dots, a_n$.

Теорема 9. (Основни став аритметике) Сваки природан број $n > 1$ може се представити као производ простих бројева на јединствен начин (са тачно71у до њиховог поретка).

Ова теорема је кључни став тзв. мултипликативне теорије бројева. У факторизацији броја n неки прост број се може појавити као фактор више пута, рецимо $24 = 2 \cdot 2 \cdot 2 \cdot 3$. Ако су $p_1, \dots, p_k$ сви различити прости фактори броја n, онда се n може представити као

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_k^{\alpha_k} = \prod_{j=1}^{k} p_j^{\alpha_j},$$

где су $\alpha_1, \alpha_2, \dots, \alpha_k$ једнозначно одређени природни бројеви. Ово се назива *канонска репрезентација* или (*каноничко разлагање*) природног броја n. Она се врло често користи у теорији бројева.

Пример 3. *Број делилаца* броја n се означава са $\tau(n)$. Ако број n има канонску репрезентацију онда је сваки делилац броја n облика

$$n = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \dots \cdot p_k^{\beta_k},$$

где су бројеви $\beta_i (i = 1, 2, \dots, k)$ такви да важи $0 \leqslant \beta_i \leqslant \alpha_i (i = 1, 2, \dots, k)$. Због јединствености факторизације, која се односи и на d, сваки делилац броја n је на јединствен начин одређен избором експонената $\beta_i (i = 1, 2, \dots, k)$. Како β_i можемо да изаберемо на $\alpha_i + 1$ начина, видимо да је укупан број избора, односно укупан број делилаца броја n једнак

$$\tau(n) = (\alpha_1 + 1) \cdot (\alpha_2 + 1) \cdot \dots \cdot (\alpha_k + 1).$$

У теорији бројева је веома битна и *Ојлерова фи–функција*, $\varphi(n)$ која представља број природних бројева мањих од n и узајамно простих са n:

$$\varphi(n) = n \cdot (1 - \frac{1}{p_1}) \cdot (1 - \frac{1}{p_2}) \cdot \dots \cdot (1 - \frac{1}{p_k}).$$

Функције $\tau(n)$ и $\varphi(n)$ су мултипликативне функције, тј. важи: ако су бројеви m и n узајамно прости, $(m, n) = 1$, тада је

$$\tau(m \cdot n) = \tau(m) \cdot \tau(n) \qquad \varphi(m \cdot n) = \varphi(m) \cdot \varphi(n).$$

Ова особина се може искористи за рачунање Ојлерове функције јер је за прост број p и $k \in \mathbb{N}_0$ испуњено

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

Тако број $24 = 2^3 \cdot 3$ има $\tau(24) = (3+1) \cdot (1+1) = 8$ делилаца и то су: 1, 2, 4, 8, 3, 6, 12 и 24. Природни бројеви < 24 и узајамно прости са 24 су: 1, 5, 7, 11, 13, 17, 19 и 23 и њих има $\varphi(24) = 24 \cdot (1 - \frac{1}{2}) \cdot (1 - \frac{1}{3}) = 8$. Сада још да проверимо мултипликативност ових функција. $\tau(8) = (3 + 1) = 4$ (делиоци су 1,2,4,8), $\tau(3) = (1 + 1) = 2$ (делиоци су 1,3) и $\tau(24) = \tau(8) \cdot \tau(3) = 4 \cdot 2 = 8$. $\varphi(8) = \varphi(2^3) = 2^3 - 2^2 = 8 - 4 = 4$ (узајамно прости су 1,3,5,7), $\varphi(3) = \varphi(3^1) = 3^1 - 3^0 = 3 - 1 = 2$ (узајамно прости су 1,2), $\varphi(24) = \varphi(8) \cdot \varphi(3) = 4 \cdot 2 = 8$.

Одговор на питање колико има простих бројева знали су још старогрчки математичари. Еуклид у IX књизи својих "Елемената" даје следећи доказ чињенице да је скуп простих бројева бесконачан:

Теорема 10. (Еуклидова теорема) Не постоји највећи прост број.

3 Конгруенције

Бројеви који дају исти остатак при дељењу бројем m имају много заједничких особина. Због тога се и уводе следећа дефиниција и ознака:

Дефиниција 5. (Конгруентност) За целе бројеве a и b који при дељењу са $m \neq 0$ дају исте остатке (тј. ако цео број m дели $a-b$; ова два исказа су еквивалентна због Теореме 2) каже се да су *конгруентни по модулу* m. Симболички се то пише

$$a \equiv b \pmod{m}.$$

Ако m не дели $a-b$, каже се да a *није конгруентно* b *по модулу* m и пише се

$$a \not\equiv b \pmod{m}.$$

Ову нотацију увео је Гаус у књизи "Disquisitiones arithmeticae", која је била објављена 1801. године, када је Гаусу било свега 24 године.

Како је $a-b$ дељиво са m ако и само ако је дељиво са $-m$, можемо без ограничења општости у конгруенцијама претпоставити да су модули m природни бројеви. Стога ћемо од сад па надаље претпостављати да је m природан број.

Конгруенције имају многе заједничке особине са једнакостима. Неке од тих особина следе непосредно из дефиниције конгруенције и садржи их следећа теорема.

Теорема 11. Нека су a, b, c, d, x и y произвољни цели бројеви, тада важи
а) $a \equiv a \pmod{m}$. (особина рефлексивности)
б) $a \equiv b \pmod{m}$, $b \equiv a \pmod{m}$ и $a - b \equiv 0 \pmod{m}$ су еквивалентна тврђења. (особина симетричности)
в) Ако је $a \equiv b \pmod{m}$ и $b \equiv c \pmod{m}$ онда је и $a \equiv c \pmod{m}$. (особина транзитивности)
г) Ако је $a \equiv b \pmod{m}$ и $c \equiv d \pmod{m}$ онда је и $ax + cy \equiv bx + dy \pmod{m}$. (особина линеарности)
д) Ако је $a \equiv b \pmod{m}$, онда постоји цео број q такав да је $a = mq + b$.
ђ) Ако је $a \equiv b \pmod{m}$ и $c \equiv d \pmod{m}$ онда је и $ac \equiv bd \pmod{m}$. (особина мултипликативности)
е) Ако је $a \equiv b \pmod{m}$ и $f(x)$ полином са целим коефицијентима, онда је $f(a) \equiv f(b)$.
ж) Ако је $a \equiv b \pmod{m}$ и $d \mid m$, онда је $a \equiv b \pmod{d}$.

За реалне бројеве важи особина скраћивања: ако је $ax = ay$ и $a \neq 0$, онда је $x = y$. Код скраћивања конгруенција потребно је више опреза, као што показује следећа теорема.

Теорема 12. а) $ax \equiv ay \pmod{m}$ ако и само ако је $x \equiv y \pmod{\dfrac{m}{(a,m)}}$ $\quad (a \neq 0)$.
б) Ако је $ax \equiv ay \pmod{m}$ и $(a, m) = 1$, онда је $a \equiv b \pmod{m}$.
в) $a \equiv b \pmod{m_i}$ за $i = 1, 2 \ldots, k$ ако и само ако је $a \equiv b \pmod{[m_1, m_2, \ldots, m_k]}$. $[m_1, \ldots, m_k]$ представља највећи заједнички садржалац свих бројева $m_1, \ldots, m_k$.

На основу особина а, б и в Теореме 11 следи да је конгруенција по модулу m релација *еквиваленције*. Класе еквиваленције су бројеви који при дељењу са m дају исти остатак. У раду са бројевима по модулу m у суштини вршимо уобичајене операције аритметике $+$ и $\cdot$, али занемарујемо умношке броја m. За свако $a \geqslant 1$ нека је

$$a = qm + r \qquad (0 \leqslant r < m)$$

по алгоритму дељења (Теорема 2). Тада је $a \equiv r \pmod{m}$, и види се да је сваки цео број конгруентан по модулу m неком од бројева $0, 1, \ldots, m-1$. Такође је јасно да међу последњим бројевима никоја два нису конгруентна по модулу m. Каже се да тих m бројева образује *потпуни систем остатака по модулу* m. У општем случају бројеви $x_1, x_2, \ldots x_m$ образују потпуни систем остатака по модулу m ако $x_i \not\equiv x_j \pmod{m}$ за $i \neq j$. Тада је опет сваки број a конгруентан једном (и само једном) од бројева x_i по модулу m. Јасно је да потпуних система остатака има бесконачно много, јер се рецимо додавањем истог броја сваком елементу из потпуног система остатака добијају бројеви који опет чине потпуни систем остатака.

Теорема 13. а) Ако је $a \equiv b \pmod{m}$, $a \equiv b \pmod{n}$ и $(m, n) = 1$ онда је $a \equiv b \pmod{mn}$.
б) Ако је $a \equiv b \pmod{m}$, онда је $(a, m) = (b, m)$.

Каже се да бројеви $r_1, r_2, \ldots, t_t$ образују *редуковани* (или *сведени*) *систем остатака по модулу* m ако је $(r_i, m) = 1$ за $i = 1, 2, \ldots, t$ и $r_i \not\equiv r_j$ за $i \neq j$, и ако свако x за које је (x, m)1 задовољава $x \equiv r_i \pmod{m}$ за неко i. Јасно је да се редуковани систем остатака по модулу m може добити ако се из потпуног система остатака по модулу m одстране сви они бројеви x_i за које је $(x_i, m) > 1$, тј. задрже они бројеви x_i за које је $(x_i, m) = 1$.

Једнозначно одређени број t представља Ојлерову функцију, тј. $t = \varphi(m)$. Јасно је да је $\varphi(1) = 1$. Ако је p прост број и $k \geqslant 1$, онда је

$$\varphi(p^k) = p^k - p^{k-1},$$

јер су бројеви $n \leqslant p$ за које је $(n, p^k) > 1$ бројеви $p, 2p, 3p, \ldots, p^k$, а њих је укупно p^{k-1}.

Пример 4. Ако посматрамо остатке по модулу 8 (тј. $m = 8$), тада бројеви $0, 1, 2, 3, 4, 5, 6, 7$ чине потпуни, а $1, 3, 5, 7$ редуковани систем остатака по модулу 8. Сваки цео број је конгруентан по модулу 8 неком од бројева из потпуног система остатака по модулу 8, а сваки број узајамно прост са 8 је конгруентан по модулу 8 неком од бројева из редукованог система остатака по модулу 8, тј. неком од бројева 1, 3, 5 или 7. $t = 4 = \varphi(8) = 8 \cdot (1 - \frac{1}{2})$.

4 Питагорини бројеви

Дефиниција 5. *Питагорину тројку* (x, y, z) чине природни бројеви $x, y, z \in \mathbb{N}$ који задовољавају једначину $x^2 + y^2 = z^2$. Уколико су они узајамно прости тада кажемо да они чине *основну Питагорину тројку*. Правоугли троугао који има катете x и y и хипотенузу z назива се *Питагорин троугао*.

Још су Египћани користили правоугли троугао са страницама $(3, 4, 5)$ за мерење правих углова. Сваки непаран број је део неке Питагорине тројке: $x = 2\alpha + 1$, $y = 2\alpha^2 + 2\alpha$ и $z = y + 1 = 2\alpha^2 + 2\alpha + 1$. Ова решења је нашао још Питагора. Платон је узео да му разлика $z - y$ буде једнака 2 (уместо 1 као код Питагоре) и добио је решења: $x = 2\beta$, $y = \beta^2 - 1$ и $z = \beta^2 + 1$. Такође су и Индуси, независно од Грка, нашли неке Питагорине тројке: $(3, 4, 5)$, $(5, 12, 13)$, $(7, 24, 25)$, који су специјални случајеви Питагориног решења и $(8, 15, 17)$, $(12, 35, 37)$, који су специјални случајеви Платоновог решења. Диофант и Индијац Брамегупта (независно један од другог) дошли су до решења $x = 2mn$, $y = m^2 - n^2$ и $z = m^2 + n^2$.

Следеће две теореме дају нека од основних својстава Питагориних тројки:

Теорема 14. а) Уколико је (x, y, z) Питагорина тројка, тада је и (y, x, z) Питагорина тројка.
б) Уколико је (x, y, z) Питагорина тројка, тада је и (kx, ky, kz) Питагорина тројка $(k \in \mathbb{N})$.

Теорема 15. Ако је (x, y, z) основна Питагорина тројка, онда постоје узајмно прости природни бројеви m и n, $(m, n) = 1$, $m > n$, такви да је $x = 2mn$, $y = m^2 - n^2$ и $z = m^2 + n^2$ или $x = m^2 - n^2$, $y = 2mn$ и $z = m^2 + n^2$.

5 Основне теореме теорије бројева

У овом поглављу ћемо само навести (без доказа) основне теореме теорије бројева.

Теорема 16. (Ојлерова теорема) Ако је $(a, m) = 1$, онда је

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

У посебном случају Ојлерова теорема, када је $m = p$ прост број (тада је $\varphi(p) = p - 1$), је

$$a^{p-1} \equiv 1 \pmod{p} \qquad (a, p) = 1,$$

а множењем са a добија се следећи резултат, који је у литератури познат као *мала Фермаова теорема* из 1640. (*велика Фермаова теорема* је тврђење да једначина $x^n + y^n = z^n$ нема решења у скупу природних бројева ако је $n \geqslant 3$ и она је била вековима изазов за математичаре, а решена је 1997. године).

Теорема 17. (мала Фермаова теорема) Ако је p прост број и a цео број који није дељив са p, онда је

$$a^{p-1} \equiv 1 \pmod{p}.$$

Ова теорема се често задаје и у облику $a^p \equiv a \pmod{p}$, где је p прост број, а a произвољан број.

Мала Фермаова теорема налази практичну примену у рачунарству: за потребе кодирања потребно је одредити велике просте бројеве (једини 100% ефикасан начин за установљавање сложености неког броја n је Ератостеново сито, односно потебно је испитати да ли је дељив са неким простим бројем мањим или једнаким од $\sqrt{n}$, али тај поступак тражи веома много времена) и тада ако нам неки "псеудопрост" број да резултат мале Фермаове теореме за неколико (што више то боље — већа је вероватноћа да је тај број заиста прост) различитих вредности a онда га можемо сматрати као прост за генерисање неког кода.

Пример 5. Помоћу Ојлерове теореме можемо да решимо конгруенцију

$$ax \equiv b \pmod{m} \qquad ((a,m)=1), \tag{2}$$

где је x непозната, а величине a, b и m су дате. Ова једначина не може да има више од једног решења по модулу m. Наиме, ако x_1 и x_2 задовољавају (2), онда следи

$$ax_1 \equiv ax_2 \pmod{m},$$

а по Теореми 12 б) добија се да је $x_1 \equiv x_2 \pmod{m}$. С друге стране

$$x_1 = a^{\varphi(m)-1}b$$

је очигледно решење једначине (2), јер је

$$ax_1 = a^{\varphi(m)}b \equiv 1 \cdot b \pmod{m}$$

по Ојлеровој теореми. Другим речима једначина (2) има јединствено решење по модулу m.

По аналогији са проблемима решавања алгебарских једначина поставља се природно и проблем решавања конгруенција. У општем случају се решава конгруенција

$$f(x) \equiv 0 \pmod{m},$$

где је f полином n–тог степена (због тога је потребно да је $a_n \not\equiv 0 \pmod{m}$ јер се у противном добија конгруенција са полиномом степена мањим од n) $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ чији су коефицијенти a_j цели бројеви. Ако је скуп $\{x_1, x_2, \ldots, x_m\}$ потпуни систем остатака по модулу m, број решења конгруенције $f(x) \equiv 0 \pmod{m}$ се дефинише као број оних x_i за које је $f(x_i) \equiv 0 \pmod{m}$. По Теореми 11 е) јасно је да је број решења $f(x) \equiv 0 \pmod{m}$ независтан од избора потпуног система остатака по модулу m, као и да тај број решења никада не прелази m. На пример
$x^3 - x \equiv 0 \pmod{3}$ има три, тј. максималан број решења,
$x^2 + 1 \equiv 0 \pmod{7}$ нема решења,
$x^2 + 1 \equiv 0 \pmod{5}$ има два решења,
$x^2 - 1 \equiv 0 \pmod{8}$ има четири решења.

Теорема 18. (Лагранжова теорема) Нека је p прост број и $p \nmid a_n$ и нека је $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ дати полином са целим коефицијентима. Тада конгруенција

$$f(x) \equiv 0 \pmod{p}$$

има највише n решења по модулу p.

Тврђење не мора бити тачно ако p није прост број, као што рецимо показује пример конгруенције $x^2 - 1 \equiv 0 \pmod{8}$, која има четири решења: 1, 3, 5 и 7.

Последица. Нека је p прост број и нека је $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ дати полином са целим коефицијентима. Ако конгруенција

$$f(x) \equiv 0 \pmod{p}$$

има више од n решења по модулу p, онда је сваки коефицијент полинома $f(x)$ дељив са p.

Имајући у виду Лагранжову теорему и њену последицу, сада можемо лако да докажемо један од класичних ставова елементарне теорије бројева, који је у литератури познат као Вилсонова теорема. Следећа теорема је занимљива, јер даје формулу која важи за све просте бројеве и ни за један други број. На жалост, коришћење те формуле за испитивање сложености бројева, односно одређивање простих бројева, није нимало практично. Ову теорему је први открио Лајбниц 1682. године, али данас носи Вилсоново име. $(p-1)!$ представља производ првих $p-1$ природних бројева, тј. $(p-1)! = 1 \cdot 2 \cdot \ldots \cdot (p-1)$.

Теорема 19. (Вилсонова теорема) Конгруенција

$$(p-1)! \equiv -1 \pmod{p}$$

важи ако и само ако је p прост број.

Систем од две или више конгруенција не мора да има решења, премда свака појединачна конгруенција има решења. Рецимо не постоји x које истовремено задовољава $x \equiv 1 \pmod{2}$ и $x \equiv 0 \pmod{4}$, мада свака

од појединачних конгруенција има решења. Разлог томе је што модули конгруенција 2 и 4 нису узајамно прости. Следећа теорема, позната у литератури као *Кинеска теорема о остацима* даје услове под којима више линеарних конгруенција има заједничко решење ако су модули конгруенција узајамно прости у паровима. Мада је прво опште решење за проблеме овог типа дао Ојлер, следећа теорема се назива кинеском јер је кинески математичар Сун-Це у I веку решио задатак који се своди на налажење целих бројева x који при дељењу са 3, 5 и 7 дају редом остатке 2, 3 и 2. Тај проблем је еквивалентан следећем систему конгруенција:

$$\left.\begin{array}{rcl} x & \equiv & 2 \pmod 3 \\ x & \equiv & 3 \pmod 5 \\ x & \equiv & 2 \pmod 7 \end{array}\right\} \quad \Rightarrow \quad x \equiv 23 \pmod{105}.$$

105 је једнако $105 = 3 \cdot 5 \cdot 7$.

Теорема 20. (Кинеска теорема о остацима) Нека су $m_1, m_2, \ldots, m_r$ природни бројеви који задовољавају $(m_i, m_j) = 1$ за $i \neq j$, и нека су $b_1, b_2, \ldots, b_r$ произвољни цели бројеви. Тада систем конгруенција

$$\left.\begin{array}{rcl} x & \equiv & b_1 \pmod{m_1} \\ x & \equiv & b_2 \pmod{m_2} \\ & \vdots & \\ x & \equiv & b_r \pmod{m_r} \end{array}\right\}$$

има тачно једно решење x_0 по модулу $m = m_1 \cdot m_2 \cdot \ldots \cdot m_r$.

Важи и следеће поопштење претходне теореме.

Теорема 21. Нека су $m_1, m_2, \ldots, m_r$ природни бројеви који су узајамно прости у паровима ($(m_i, m_j) = 1$ за $i \neq j$) и нека су $a_1, a_2, \ldots, a_r$ и $b_1, b_2, \ldots, b_r$ произвољни цели бројеви. Тада систем конгруенција

$$\left.\begin{array}{rcl} a_1 x & \equiv & b_1 \pmod{m_1} \\ a_2 x & \equiv & b_2 \pmod{m_2} \\ & \vdots & \\ a_r x & \equiv & b_r \pmod{m_r} \end{array}\right\}$$

има тачно једно решење x_0 по модулу $m = m_1 \cdot m_2 \cdot \ldots \cdot m_r$.

Пример 6. Сада ћемо на примеру Сун-Цеовог задатка да илуструјемо како се користи Кинеска теорема о остацима. Из система

$$\left.\begin{array}{rcl} x & \equiv & 2 \pmod 3 \\ x & \equiv & 3 \pmod 5 \\ x & \equiv & 2 \pmod 7 \end{array}\right\}$$

налазимо да је $m_1 = 3$, $m_2 = 5$, $m_3 = 7$, $m = m_1 \cdot m_2 \cdot m_3 = 105$ и $\dfrac{m}{m_1} = 35$, $\dfrac{m}{m_2} = 21$, $\dfrac{m}{m_3} = 15$ и $b_1 = 2$, $b_2 = 3$, $b_3 = 2$. Сада треба да решимо три конгруенције (сваку понаособ) по непознатим c_1, c_2 и c_3:

$$\begin{array}{rcl} 35c_1 & \equiv & 1 \pmod 3 \\ 21c_2 & \equiv & 1 \pmod 5 \\ 15c_3 & \equiv & 1 \pmod 7 \end{array} \quad \Rightarrow \quad \begin{array}{rcl} -c_1 & \equiv & 1 \pmod 3 \\ c_2 & \equiv & 1 \pmod 5 \\ c_3 & \equiv & 1 \pmod 7 \end{array}.$$

Одмах добијамо решења $c_1 = 2$, $c_2 = 1$ и $c_3 = 1$, што нам даје основно решење

$$x_0 = 35 \cdot 2 \cdot 2 + 21 \cdot 1 \cdot 3 + 15 \cdot 1 \cdot 2 = 233 \equiv 23 \pmod{105},$$

а одатле налазимо и коначно решење

$$x = 105k + 23, \quad k \in \mathbb{Z}.$$

Помоћу Кинеске теореме о остацима може се показати да се решавање полиномне конгруенције $f(x) \equiv 0 \pmod m$ може свести на решавање једноставније конгруенције $f(x) \equiv 0 \pmod{p^k}$, а затим се може ићи и даље и показати да је довољно ограничити се на конгруенције типа $f(x) \equiv 0 \pmod p$.

Као што смо видели конгруенције играју веома битну улогу у теорији бројева. Неке од најзначајнијих теорема у општој теорији бројева се показују помоћу апарата који користи конгруенције. Даље у изучавању опште теорије бројева следе квадратни остаци које је увео Лежандр ради решавања квадратне конгруенције, а основни став је дао Гаус и по њему се зове Гаусов закон квадратног реципроцитета.

6 Задаци

1. Да ли је број $\underbrace{77\ldots7}_{27}$ дељив са: **а)** 189; **б)** 333; **в)** 777; **г)** 567?

2. Доказати да су следећи бројеви сложени: **а)** $2^{33}+1$; **б)** $(3299^5+6)^{18}-1$; **в)** $3^{105}+4^{105}$; **г)** $5\cdot 2^{298}+3^{299}$; **д)** $5^{501}+4^{502}+3^{503}$; **ђ)** $2222^{5555}+5555^{2222}$; **е)** 15^4+4^{15}; **ж)** $972^2+235^2=1000009$; .

3. Доказати да је за сваки природан број n број $\dfrac{n}{3}+\dfrac{n^2}{2}+\dfrac{n^3}{6}$ природан.

4. Доказати да за сваки природан број n важи **а)** $27 \mid 10^n+18n-1$; **б)** $9 \mid 4^n+15n-1$; **в)** $64 \mid 3^{2n+3}+40n-27$.

5. Нека је p прост број и $p \geq 5$. Доказати $24 \mid p^2-1$.

6. Наћи све природне бројеве p за које су бројеви $p+1$, $p+2$ и $p+4$ прости.

7. Наћи све природне бројеве p за које су бројеви p, $p+10$ и $p+14$ прости.

8. Бројеви p и $8p^2+1$ су прости. Доказати да је број $8p^2+2p+1$ такође прост.

9. Доказати да не постоји прост број p, такав да су и бројеви $p+5$ и $p+10$ прости.

10. Да ли је број $1^{2000}+2^{2000}+3^{2000}+4^{2000}$ дељив са 5?

11. Наћи све природне бројеве n за које важи: **а)** $7 \mid 2^n-1$; **б)** $7 \mid 2^n+1$.

12. Нека је дат број $n=144!$. Са колико нула се завршава n?

13. Доказати да збир квадрата три цела броја при дељењу са 8 не даје остатак 7.

14. Доказати да квадрат природног броја не може да се завршава са 4 једнаке цифре различите од нуле.

15. Наћи све $x, y \in \mathbb{Z}$ за које важи: **а)** $x+y=xy$; **б)** $x^2-3xy+2y^2=3$; **в)** $\dfrac{1}{x}+\dfrac{1}{y}+\dfrac{1}{xy}=1$; **г)** $3^x-y^3=1$.

16. Који се природни бројеви могу представити у облику разлике квадрата 2 природна броја?

17. Колико треба употребити цифара 5 и 2 да би број $5252\ldots$ био дељив са 99.

18. Колико делилаца имају бројеви **а)** 1984; **б)** 2000; **в)** 2004?

19. Ако природан број има непаран број делилаца онда је он потпун квадрат. Доказати.

20. Одредити природан број који је дељив са 12 и има 14 делилаца.

21. Ако је $(16a+17b)(17a+16b)$ дељиво са 11 онда је дељиво и са 121.

22. Доказати да једначина $x^2+1999x+2001=0$ нема целобројних решења.

23. Колико је n, ако је $n-1$ дељиво са 15, а $n+1$ садржано у 1001?

24. Ако је $6x+11y$ дељиво са 31 онда је и $x+7y$ дељиво са 31. Доказати.

25. Наћи највећи и најмањи природан број који је дељив са 225 и збир цифара му је 225.

26. Првих 2000 цифара неког броја су двојке, других 2000 цифара су јединице, а остало су нуле. Доказати да тај број није тачан куб.

27. Наћи све тројке узастопних простих бројева, тако да је збир њихових квадрата исто прост број.

28. Ако је $\overline{11\ldots1}$ прост онда је и збир цифара тог броја прост.

29. Доказати да 2^n-1 и 2^n+1 не могу бити истовремено прости.

30. Решити у целим бројевима: $xy-z^2=1, x+y=2$.

31. Доказати да број $n^2+9n+12$ није дељив са 121 ни за један природан број n.

32. Наћи остатак при дељењу 2^{p^2} са 13, где је p прост број.

33. Наћи све природне бројеве k за које је број $k^{3k-1}+k+1$ прост.

34. Наћи све природне бројеве n за које је број $2^8+2^{11}+2^n$ квадрат природног броја.

35. Ако је број x облика $x=3n+1$, $n \in \mathbb{N}_0$ доказати да је израз $P=1+3^x+9^x$ дељив са 13.

36. Одредити остатак при дељењу броја: **а)** 3^{21} са 11; **б)** 11^{35} са 13; **в)** 8^{130} са 131; **г)** 3^{100} са 13.

37. Која је последња цифра броја $\left(9^9\right)^9$, а која 9^{9^9}?

38. Које су последње две цифре броја $((7^9)^9)^9$?

39. Решити једначину $1!+2!+3!+\ldots+x!=y^2$ у $\mathbb{N}$.

40. Узета су два произвољна природна броја, па су састављени њихов збир, разлика и производ. Доказати да је бар један од њих дељив са 3.

41. Који је најмањи природан број који помножен са 8316 даје тачан квадрат?

42. За које вредности n је 3^n+1 дељиво са 8?

43. Доказати да је $10!+1$ дељив са 11.

44. Одредити остатак при дељењу броја: **а)** 2^{30} са 13; **б)** 317^{259} са 15.

45. Којом цифром се завршава број: **а)** 7^{2003}; **б)** 777^{777}; **в)** $((7^7)^7)^7$; **г)** $7^{7^{7^7}}$?

46. Доказати да је број $3^{105}+4^{105}$ дељив са 91, а није дељив са 11.

47. Доказати да је за сваки природан број n, број $7^{2n}-4^{2n}$ дељив са 33.

48. Доказати да једначина $15x^2-7y^2=9$ нема целобројних решења.

49. Колико има правоуглих троуглова чије су све странице целобројне, а једна катета 6?

50. Одредити природне бројеве x и y тако да је $p(x+y)=xy$ где је p дати прост број.

51. Одредити природан број n и прост број p тако да је $n^4+4=p$.

52. Постоји ли прост број p који се може приказати у облику $8n^2+10n+3$, где је $n\in\mathbb{Z}$? Ако је одговор потврдан колико има таквих бројева?

53. Одредити целе бројеве који задовољавају једначине: **а)** $x^2-7=2xy$; **б)** $xyz-xy=x+xz+3$; **в)** $x^4-y^4=15$.

54. Ако је $n\in\mathbb{N}$ и p прост решити следеће једначине: **а)** $3p+1=n^3$; **б)** $n^4+n^2+1=p$; **в)** $n^3-3n=p-2$.

55. Ако су $x,y,z\in\mathbb{Z}$ решити једначину $(x-y)^3+(y-z)^3+(z-x)^3=6$.

56. Решити у $\mathbb{Z}$ једначине: **а)** $x^2y=y^3+10$; **б)** $xy-7x=2y-4$; **в)** $y^4+x=xy+9$.

57. Одредити целе бројеве x и y тако да је $x^2+5y=98765432$.

58. Доказати да једначина $x^4+y^4=\underbrace{333\ldots33}_{100}$ нема решења у $\mathbb{Z}$.

59. Решити у $\mathbb{Z}$ једначину $x!+8y=5555$.

60. Одредити све природне n и просте бројеве p тако да је $n!+2=p^2$.

61. Доказати да једначина $x^2+y^2+z^2=2007$ нема решења у $\mathbb{Z}$.

62. Решити у $\mathbb{Z}$ једначину $x!+y^2=987654$.

63. Решити у $\mathbb{Z}$ једначине: **а)** $x^2-5y=10z+3$; **б)** $2x^2+5y=1001$; **в)** $2x^4+y^4=10032$.

64. Решити у $\mathbb{Z}$ једначине: **а)** $x!+3y=5555$; **б)** $1\cdot1!+2\cdot2!+3\cdot3!+\ldots+x\cdot x!=y^4$; **в)** $x!+y!=10z+9$.

65. Ако су x, y и z различити природни бројеви, решити једначину $\dfrac{1}{x}+\dfrac{1}{y}+\dfrac{1}{z}=1$.

66. Доказати да једначина $x^n+y^n=z^n,\ n\in\mathbb{N}$ нема решења у скупу природних бројева, где је $z\le n$.

67. Доказати да 1999 дели $1997!!+1998!!$.

68. Доказати да је број $a=\underbrace{22\ldots2}_{1980}$ дељив са $1982\cdot1983$.

69. Решити једначину у $\mathbb{Z}$: $a^2+b^2+c^2=a^2b^2$.

70. Наћи најмању вредност броја: **а)** $|12^m-5^n|, m,n\in\mathbb{N}$; **б)** $|36^m-5^n|, m,n\in\mathbb{N}$.

71. Решити у скупу целих бројева: **а)** $x^2+x=y^4+y^3+y^2+y$; **б)** $y^2=1+x+x^2+x^3+x^4$.

72. Приметимо да је $8^3-7^3=(2^2+3^2)^2$ и $105^3-104^3=(9^2+10^2)^2$. Показати да ако је разлика два узастопна куба квадрат, онда је то квадрат суме два узастопна квадрата.

73. Да ли једначина $x! \cdot y! = z!$ има решења већа од 5?

74. Решити $x! + y! = z!$.

75. Не постоји прост број облика $p = 4k + 3$ који је збир два квадрата, али прости бројеви облика $p = 4k + 1$ могу се јединствено представити као збир два квадрата. Доказати.

76. Многи бројеви који се могу записати као алтернативан низ нула и јединица су сложени, нпр. $101010101 = 41 \cdot 271 \cdot 9091$. Да ли поред броја 101 има још простих бројева таквог облика?

77. Решити једначину $(p-1)! + 1 = p^m$, при чему је p прост, а m природан.

78. Решити једначину $x^2 + xy + y^2 = 0$ у $\mathbb{Z}$.

79. Решити једначину $2x^2 + 3y^2 = z^2$ у $\mathbb{Z}$.

80. Решити једначину $x^2 + y^2 = 2z^2$ у $\mathbb{N}$.

81. Доказати да једначина $x^4 + y^4 = z^4$ у $\mathbb{Z}$ нема решења која нису тривијална.

82. Доказати да једначина $x^4 + y^4 = u^2$ у $\mathbb{Z}$ нема решења која нису тривијална.

83. Доказати да $4xy - x - y = z^2$ има само тривијално решење.

84. Одредити све тројке (x, y, z) целих бројева за које важи $x^y - 2^z = 1$.

85. Доказати да постоји бесконачно много простих бројева облика $4n - 1$.

86. Нека су $(a, b) = 1$, $a, b \in \mathbb{N}$. Доказати да ако је $a \cdot b$ тачан квадрат, тада су и a и b квадрати.

87. Које остатке по модулу 19 дају бројеви $7^n + 11^n$, $n \in \mathbb{N}$.

88. Решити конгруенцију $2^n \equiv n \pmod 7$.

89. Наћи остатак при дељењу са 7 броја $2^{2^{\cdot^{\cdot^{\cdot^2}}}}$, где се бројеви 2 јављају n пута.

90. Да ли постоји деветоцифрен природан број чије су све цифре међусобно различите од нуле, који је дељив са 5 и потпун је квадрат?

91. Природни бројеви a, b и c су такви да су бројеви $p = b^c + a$, $q = a^b + c$ и $r = c^a + b$ прости. Доказати да су два од бројева p, q, r међусобно једнаки.

92. Доказати да је број $n^n - n$ дељив са 24 за све непарне природне бројеве n.

93. Наћи све бројеве $b \in \mathbb{N}$ за које постоји $a \in \mathbb{N}$ тако да $b \mid a^2 + 1$ и $b \mid a^3 - 1$.

94. Доказати да је број $\underbrace{1000\ldots001}_{2^{2004}+2^{1000}-1}$ сложен.

95. Колико има тројки природних бројева (a, b, c) таквих да је $2a + 1$ дељиво са b, $2b + 1$ дељиво са c, и $2c + 1$ дељиво са a?

96. Наћи сва решења једначине $x^2 + y^2 + z^2 = 2004 \cdot x \cdot y \cdot z$ у скупу $\mathbb{Z}$.

97. Доказати да једначина $x^3 + y^3 + z^3 = 2003$ нема решења у скупу целих бројева.

98. Нека су m и n различити 14−цифрени природни бројеви чији декадни записи садрже тачно по два пута сваку од цифара 1, 2, 3, 4, 5, 6 и 7. Да ли је могуће да број $\frac{m}{n}$ буде цео?

99. Доказати да се сваки цео број може приказати као збир пет кубова целих бројева.

100. Доказати да број $(n+2)^4 - n^4$ ни за један природан број n није потпун куб природног броја.

101. Доказати да постоји природан број n тако да број 3^n има 2004 узастопних нула.

102. Нека је $p > 3$ прост број. Доказати да се број $4p^2 + 1$ може представити као збир квадрата три различита природна броја (напомена: $0 \notin \mathbb{N}$).

103. Нека је a природан број већи од 1. Доказати да је број $n(2n+1)(3n+1)\ldots(an+1)$ дељив свим простим бројевима мањим од a, за сваки природан број n.

104. Ако је p непаран прост број и a и b из $\mathbb{N}$. Решити једначину: $(p+1)^a - p^b = 1$.

105. Наћи све парове природних бројева (a, b) за које важи: $5a^b - b = 2004$.

106. Ако су a, b, c природни бројеви такви да је и $\frac{a}{b} + \frac{b}{c} + \frac{c}{a}$ природан број, доказати да је abc потпун куб.