Дјељивост. Еуклидов алгоритам. Прости бројеви

Владимир Божовић

vladobozovic@gmail.com

Новембар 2014.

Текст који слиједи је колекција основних теоријских резултата из Теорије бројева и пратећих задатака. Неки од доказа датих тврђења су прескочени, дијелом због комплексности и техника које превазилазе ниво знања ученика, а дијелом и због тога што садржај појединих доказа не доноси нове идеје битне за рад задатака.

Пар тема из елементарне теорије бројева: **Дјељивост** и **Прости бројеви** су обрађени на начин да ученика уведу у теме, уз коришћење примјера и задатака чија је сложеност знатно испод нивоа такмичења на међународном нивоу. Ипак, ти задаци могу бити корисни за загријавање за рад задатака вишег нивоа, оних каквих се могу очекивати, на примјер на Балканској математичкој олимпијади.

Пошто су дате теме обрађене и за прва два разреда, корисно је погледати и тај материјал који садржи неке задатке који нису уврштени овдје.

Глава 1

Дјељивост

У Теорији бројева, од посебног интереса су својства скупа природних бројева

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

као и скупа цијелих бројева

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

Појам дјељивости је основни и један од најважнијих у теорији бројева.

Дефиниција 1.1. *Нека су a и b цијели бројеви, при чему је $a \neq 0$. Уколико постоји цио број m такав да*

$$b = am,$$

*онда кажемо да је b **дјељив са** a. То записујемо са $a \mid b$, а читамо a **дијели** b. Ако b није дјељив са a, онда пишемо $a \nmid b$ и читамо a **не дијели** b.*

Лако се уочавају нека основна својства дјељивости.

Лема 1.1. *Нека су a, b, c, m, n цијели бројеви такви да је $c \mid a$ и $c \mid b$. Онда*

$$c \mid am + bn.$$

Доказ. Пошто је $a = ck_1$ и $b = ck_2$ за $k_1, k_2 \in \mathbb{Z}$, то је онда

$$am + bn = ck_1m + ck_2n = c(k_1m + k_2n),$$

што значи да $c \mid am + bn$. □

Лема 1.2. *Нека су a, b, c цијели бројеви.*

1. *Ако $a \mid b$ и $b \mid c$, онда*
$$a \mid c.$$
2. *Ако $a \mid b$ и $b \mid a$, онда*
$$a = b \text{ или } a = -b.$$

Доказ.

1. Из $a \mid b$ слиједи $b = ak_1$, за $k_1 \in \mathbb{Z}$, а из $b \mid c$, слиједи $c = bk_2$, за $k_2 \in \mathbb{Z}$. Дакле,
$$c = bk_2 = (ak_1)k_2 = a(k_1k_2),$$
што значи да $a \mid c$.
2. Из $a \mid b$ и $b \mid a$, онда
$$a = bk_1 \text{ и } b = ak_2,$$
за $k_1, k_2 \in \mathbb{Z}$, одакле је $a = a(k_1k_2)$, што значи да су $k_1k_2 = 1$, односно
$$k_1 = k_2 = 1 \text{ или } k_1 = k_2 = -1,$$
чиме је тврђење доказано.

□

Задатак 1.1. *Нека су $a, b, m \in \mathbb{Z}$.*

(а) Ако је $m \neq 0$, онда $a \mid b$ ако и само ако $ma \mid mb$.

(б) Ако $a \mid b$ и $b \neq 0$, онда $|a| \leq |b|$.

Рјешење. *Тврђење под (а) слиједи директно из*
$$b = ka \text{ ако и само ако } mb = mka, \text{ за } m \neq 0.$$

У тврђењу под (б), слиједи да су и a и b ненулти цијели борјеви за које вриједи да је $b = ka$, за неко $k \in \mathbb{Z}$ које је такође различито од нуле. Како је $|ka| = |k||a| \geq |a|$, тиме је и доказано тврђење.

Следећа теорема је једна од кључних у Теорији бројева, па се препоручује наставнику да са пажњом и детаљно изведе њен доказ.

Теорема 1.1. *(Теорема о дијељењу са остатком). Нека су a и b цијели бројеви, при чему је $b > 0$. Онда постоје јединствени цијели бројеви,* ***количник*** *q и* ***остатак*** *r, такви да је*

$$a = qb + r \quad и \quad 0 \leq r < b.$$

Доказ. Једна могућност је да је a дјељиво са b, па је у том случају $a = bq$, из чега слиједи да је $r = 0$. Претпоставимо да то није случај, односно да a није дјељиво са b. Посматрајмо скуп

$$S = \{a - bm \, : m \in \mathbb{Z}\} = \{a, a \pm b, a \pm 2b, \ldots\}.$$

Ако је $m = -|a| - 1$, онда је израз $a - bm = a + |a|b + b$ природан број, па скуп S садржи и природне бројеве. По принципу доброг уређења скупа природних бројева (сваки непразан подскуп у $\mathbb{N}$ садржи минималан елемент), скуп $S \cap \mathbb{N}$ садржи најмањи елемент, који је облика $r = a - bq$, за неки цијели број q, одакле је

$$a = bq + r, \quad \text{уз услов} \quad r > 0.$$

Доказујемо да је $r < b$. Претпоставимо супротно, да је $r \geq b$. Случај $r = b$ искључујемо, јер би тада a било дјељиво са b. Онда је $r > b$. Међутим, у том случају је $r - b < r$ и $r - b \in S \cap \mathbb{N}$, што би било у супротности са претпоставком о минималности елемента r. Дакле, $r < b$.

Докажимо јединственост пара бројева q, r. Претпоставимо супротно, да постоји q_1, r_1 који задовољава исте услове као q, r. Нека је, не умањујући општост да је $r_1 > r$. Из

$$qb + r = q_1 b + r_1,$$

слиједи

$$b(q - q_1) = r_1 - r.$$

Како је лијева страна претходне једнакости већа од нуле, а b је природан број, то је онда $q - q_1 \in \mathbb{N}$ такође природан број. Међутим, то повлачи да је $r_1 - r > b$, односно да је $r_1 > b$. Ово је контрадикција у односу на чињеницу да је r_1 мањи од b.

□

Сада можемо обрадити и случај $b < 0$, јер је у том случају $-b > 0$, па према претходној теореми постоје јединствени q^* и r, тако да је

$$a = -bq^* + r \; 0 \leq r < -b.$$

За $q = -q^*$, имамо $a = bq + r$. Комбинујући ово и резултат претходне теореме, слиједи:

Последица 1.1. *Нека су a и b цијели бројеви, при чему је $b \neq 0$. Онда постоје јединствени цијели бројеви, q и r, такви да је*

$$a = qb + r \;\; u \;\; 0 \leq r < |b|.$$

Задатак 1.2. *Доказати да је број $m^5 - m$, $m \in \mathbb{N}$, дјељив са 30.*

Рјешење. *Како је $m^5 - m = m(m-1)(m+1)(m^2+1)$, видимо да на десној страни имамо производ три узастопна природна броја, па је онда дати израз дјељив са 6. Остало је још да се покаже да је број дјељив са 5.*

Произвољан цијели број m има облик $5k$, $5k+1$, $5k+2$, $5k+3$, или $5k+4$. ААко је m облика $5k$, $5k+1$ или $5k+4$, онда је јасно да је m, $m-1$, односно $m+1$ дјељиво са 5. У преосталим случајевима, ако је m једнако $5k+2$ или $5k+3$, израз m^2+1 је дјељив са 5.

Задатак 1.3. *Наћи три последње цифре броја 7^{9999}.*

Рјешење. *Најприје, примјетимо да је*

$$7^{9999} = 7^{4 \cdot 2499 + 3} = 7^{4 \cdot 2499} \cdot 7^3,$$

што истиче важност израза облика 7^{4n} у датом контексту. Пошто је $7^4 = 2401$, онда је

$$7^{4n} = (1 + 2400)^n = 1 + n \cdot 2400 + \binom{n}{2} 2400^2 + \cdots .$$

Из претходне суме уочавамо да се сви сабирци почевши од трећег члана завршавају са најмање четири нуле, што значи да не утичу на последње три цифре посматраног броја. Дакле, да би одредили последње три цифре броја 7^{4n} довољно је посматрати израз $1 + n \cdot 2400$. Пошто је

$$1 + n \cdot 2400 = 24n \cdot 100 + 1 = (\ldots m) \cdot 100 + 1 = \ldots m01,$$

гдје је са $(\dots m)$ *заправо представљен број* $24n$*, а* m *његова последња цифра. У нашем, конкретном случају, за посматрано* $n = 2499$*, слиједи* $24n = 59976$*, па је* $m = 6$*. Значи, број* 7^{4n} *се завршава са* 601*. На крају,*

$$7^{9999} = 7^{4\cdot 2499} \cdot 7^3 = (\dots 601)(343) = (\dots 143),$$

што значи да се тражени број завршава са 143*.*

1.1 Највећи заједнички дјелилац

Дефиниција 1.2. *Нека су* a *и* b *цијели бројеви од којих је бар један различит од нуле. Цијели број* d *зовемо заједнички дјелилац од* a *и* b *ако* $d|a$ *и* $d|b$*. Највећи међу њима се зове* ***највећи заједнички дјелилац*** *и означава се са* $\mathbf{нзд}(a, b)$ *или* (a, b)*.*
Слично дефинишемо и највећи заједнички дјелилац цијелих бројева $b_1, b_2, \dots, b_n$*, од којих је бар један различит од нуле, а означавамо са*

$$\mathbf{нзд}(b_1, b_2, \dots, b_n) \text{ или } (b_1, b_2, \dots, b_n).$$

Бројеви $b_1, b_2, \dots, b_n$ *су* ***релативно прости*** *ако је*

$$\mathbf{нзд}(b_1, b_2, \dots, b_n) = 1.$$

Бројеви $b_1, b_2, \dots, b_n$ *су* ***релативно прости у паровима*** *ако је* $\mathbf{нзд}(b_i, b_j) = 1$ *за свако* i, j *за које је* $1 \leq i < j \leq n$*.*

Примјер 1.1. *Бројеви* $12, 8, 15$ *су релативно прости, али нису релативно прости у паровима, јер на примјер,* $\mathbf{нзд}(12, 8) = 4$*.*

Напомена Убудуће, кад год напишемо $\mathbf{нзд}(a, b)$, подразумијеваћемо да је услов из претходне дефиниције, да је бар један од бројева a и b различит од нуле испуњен.

Теорема 1.2. *Највећи заједнички дјелилац бројева* a *и* b *је минималнi елемент скупа*

$$\{ax + by \,:\, x, y \in \mathbb{Z}\} \cap \mathbb{N}.$$

Доказ. Нека је $g = \mathbf{нзд}(a, b)$, те нека је l најмањи позитивни члан скупа $S = \{ax + by \ : \ x, y \in \mathbb{Z}\} \cap \mathbb{N}$. То значи да постоје цијели бројеви x_0 y_0 такви да је $l = ax_0 + by_0$. Покажимо да $l \mid a$ и $l \mid b$. Претпоставимо, на примјер да $l \nmid a$. Тада на основу Теореме 1.1 постоје q и r такви да је $a = lq + r$ и $0 < r < l$. Сада је

$$r = a - lq = a - q(ax_0 + by_0) = a(1 - qx_0) + b(-qy_0) \in S,$$

што је у супротности са минималношћу броја l. Дакле, $l \mid a$, а на исти начин се показује $l \mid b$. То значи да је $l \leq g$, јер је $g = \mathbf{нзд}(a, b)$ највећи заједнички дјелилац a и b.

Са друге стране, будући да је $g = \mathbf{нзд}(a, b)$, то постоје $\beta, \gamma \in \mathbb{Z}$, такви да је $a = g\beta$, $b = g\gamma$, па је $l = ax_0 + by_0 = g(\beta x_0 + \gamma y_0)$. Одавде слиједи да је $g \leq l$, чиме је доказано да је $g = l$. □

Претходна теорема установљава јединственост приказа за $\mathbf{нзд}(a, b)$ у облику цјелобројне линеарне комбинације

$$\mathbf{нзд}(a, b) = a\alpha + b\beta,$$

која се у литератури назива **Безуов идентитет**.

Примјетимо да је, за произвољна два цијела броја a и b, од којих је бар један различит од нуле $\mathbf{нзд}(a, b) \geq 1$. Такође, елементарном анализом закључујемо да је

$$\mathbf{нзд}(a, b) = \mathbf{нзд}(b, a) = \mathbf{нзд}(\pm b, \pm a).$$

Значи, можемо подразумијевати да су бројеви чији **нзд** ненегативни, при чему је бар један већи од нуле.

Задатак 1.4. *Доказати да се разломци*

$$\frac{12n + 1}{30n + 2} \ \textit{и} \ \frac{21n + 4}{14n + 3}$$

не могу скратити ни за један природан број.

Рјешење. *Претпоставимо да d дијели бројеве $12n + 1$ и $30n + 2$. Тада d дијели и сваку линеарну комбинацију ова два броја, па специјално*

$$d \mid 5(12n + 1) - 2(30n + 2) = 1,$$

одакле слиједи да је $d = 1$*, чиме је доказано да се дати разломак не може даље скратити.*

Слично се доказује и за други разломак, јер је

$$d \mid 3(14n + 3) - 2(21n + 4) = 1.$$

Лема 1.3. *Нека* a*,* b*,* q *и* r *цијели бројеви за које вриједи* $a = bq + r$*. Онда је*

$$\textbf{нзд}(a, b) = \textbf{нзд}(b, r).$$

Доказ. Ако цијели број d дијели бројеве a и b, онда, на основу Леме 1.1, слиједи да d дијели и $a - bq$ односно r. Дакле, d дијели b и r. То значи да

$$\textbf{нзд}(a, b) \leq \textbf{нзд}(b, r). \tag{1}$$

Обрнуто, ако d дијели b и r, слиједи да d дијели a, из чега закључујемо да d дијели и a и b. Тиме смо показали да је

$$\textbf{нзд}(b, r) \leq \textbf{нзд}(a, b). \tag{2}$$

Из (1) и (2), слиједи тврђење

$$\textbf{нзд}(a, b) = \textbf{нзд}(b, r).$$

□

Лема 1.4. *Нека су* a*,* b *і* h *цијели бројеви, такви да*

$$h \mid a \text{ и } h \mid b.$$

Онда $h \mid \textbf{нзд}(a, b)$*.*

Доказ. Како је d највећи заједнички дјелилац a и b, онда је

$$d = ax_0 + by_0,$$

за неке $x_0, y_0 \in \mathbb{Z}$. Пошто h дијели a и b, онда дијели сваку њихову линеарну комбинацију, па дијели лијеву страну претходне једнакости. Тиме дијели и десну, односно d. □

Својство дато у претходној леми може бити веома корисно, јер истиче да су заједнички дјелиоци неких бројева a и b истовремено и дјелиоци њиховог највећег зајендичког дјелиоца.

Дефиниција 1.3. *За цијеле бројеве $a_1, a_2, \ldots, a_n$, за $n \geq 2$, кажемо да су узајамно или релативно прости ако је*

$$\textbf{нзд}(a_1, a_2, \ldots, a_n) = 1,$$

а да су у паровима релативно прости ако је

$$\textbf{нзд}(a_i, a_j) = 1, \text{ за све } 1 \leq i, j \leq n,\ i \neq j.$$

Лема 1.5. *Нека су a, b цијели бројеви такви да* $\textbf{нзд}(a, b) = d$. *Тада је*

$$\textbf{нзд}(\frac{a}{d}, \frac{b}{d}) = 1,$$

односно $\frac{a}{d}, \frac{b}{d}$ су узајамно прости. Такође, вриједи

$$\textbf{нзд}(ma, mb) = md,$$

за сваки цио број $m > 0$.

Доказ. Претпоставимо да је $\textbf{нзд}(\frac{a}{d}, \frac{b}{d}) = k$ и $k > 1$. Слиједи да је

$$a = kmd, \ \ b = knd,$$

па је $\textbf{нзд}(a, b) \geq kd > d$, што је контрадикција у односу на претпоставку. На основу Теореме 1.2 $\textbf{нзд}(ma, mb)$ је најмањи позитивни број облика

$$max + mby = m(ax + by),$$

гдје су $x, y \in \mathbb{Z}$. Како је d најмањи природан број облика $ax + by$, слиједи да је $\textbf{нзд}(ma, mb) = md$. □

Последица 1.2. *Нека је $d = \textbf{нзд}(a_1, a_2, \ldots, a_n)$, гдје су $a_1, a_2, \ldots, a_n$ цијели бројеви. Онда је*

$$\textbf{нзд}\left(\frac{a_1}{d}, \frac{a_2}{d}, \ldots, \frac{a_n}{d}\right) = 1.$$

Лема 1.6. *Нека су a, b, m цијели бројеви такви да* $\textbf{нзд}(a, m) = \textbf{нзд}(b, m) = 1$. *Тада је* $\textbf{нзд}(ab, m) = 1$.

Доказ. Из претпоставки, а на основу Теореме 1.2, слиједи

$$1 = ax_0 + my_0$$
$$1 = bx_1 + my_1$$

Из претходне двије једнакости добијамо

$$abx_0x_1 = (1 - my_0)(1 - my_1) = 1 - mt,$$

гдје је $t = y_0 + y_1 - my_0y_1$. Сада, из

$$abx_0x_1 + mt = 1$$

закључујемо да је $\textbf{нзд}(ab, m) = 1$. □

Лема 1.7. *Нека су a и b узајамно прости цијели бројеви.*

(а) Ако $a \mid c$ и $b \mid c$, онда $ab \mid c$.

(б) Ако $a \mid bc$, онда $a \mid c$.

Доказ.

(а) Како је $1 = ax+by$ за неке цијеле бројеве, онда је $c = cax+cby$. Међутим, $c = as$ и $c = bt$, па је $c = abtx + absy = ab(tx + sy)$.

(б) Као и под (а), имамо да је $c = cax + cby$. Пошто $a \mid a$ и $a \mid bc$, онда из дате једнакости слиједи $a \mid c$.

□

1.2 Еуклидов алгоритам

У следећој теореми је описана конструктивна, практична процедура за тражење највећег заједничког дјелиоца два цијела бројева.

Теорема 1.3. *(Еуклидов алгоритам). Нека су a и $b > 0$ цијели бројеви. Претпоставимо да је узастопном примјеном Теореме 1.1 добијен низ једнакости*

$$\begin{array}{rcll} b & = & aq_1 + r_1, & 0 < r_1 < a \\ a & = & r_1q_2 + r_2, & 0 < r_2 < r_1 \\ r_1 & = & r_2q_3 + r_3, & 0 < r_3 < r_2 \\ & \dots & & \\ r_{j-2} & = & r_{j-1}q_j + r_j, & 0 < r_j < r_{j-1} \\ r_{j-1} & = & r_jq_{j+1}. & \end{array}$$

Тада је $\mathbf{нзд}(a, b)$ *једнак* r_j*, односно последњем ненултом остатку.*

Доказ. Уочавамо да у општем случају, ред у Еуклидовом алгоритму изгледа

$$r_i = r_{i+1}q_{i+2} + r_{i+2},\ 0 \leq r_{i+2} < r_{i+1},\ \text{за } i \geq -1,$$

уколико дефинишемо да је $r_{-1} = b$, а $r_0 = a$. Како је низ остатака r_i строго опадајући, онда је извјесно да ће за неки природан број j бити r_j последњи ненулти остатак, односно $r_{j+1} = 0$. На основу Леме 1.3 закључујемо да је

$$\mathbf{нзд}(r_i, r_{i+1}) = \mathbf{нзд}(r_{i+1}, r_{i+2}),$$

из чега произилази низ једнакости

$$\mathbf{нзд}(r_{-1}, r_0) = \ldots = \mathbf{нзд}(r_j, r_{j+1}) = \mathbf{нзд}(r_{j+1}, 0) = r_j.$$

□

Algorithm 1 Еуклидов алгоритам

```
1: procedure EUCLID(a, b)                          ▷ нзд(a, b)
2:     r ← a mod b
3:     while r ≠ 0 do          ▷ Имамо одговор ако је r једнако 0
4:         a ← b
5:         b ← r
6:         r ← a mod b
7:     end while
8:     return b                                    ▷ нзд је b
9: end procedure
```

Лема 1.8. *За остатке у Еуклидовом алгоритму важи релација*

$$r_{i+2} < \frac{1}{2} r_i \;\; i = -1, 0, 1, 2, \ldots .$$

За број корака j у Еуклидовом алгоритму вриједи $j < 2 \log_2 a$.

Доказ. Могућа су два случаја:

I $r_{i+1} \leq 1/2 r_i$
Како је $r_{i+2} < r_{i+1}$, онда је $r_{i+2} < 1/2 r_i$.

II $r_{i+1} > 1/2 r_i$
Ово значи да је у кораку дијељења r_i са r_{i+1}, количник једнак 1, односно

$$r_i = 1 \cdot r_{i+1} + r_{i+2}.$$

Одавде је

$$r_{i+2} = r_i - r_{i+1} < r_i - 1/2 r_i = 1/2 r_i.$$

На основу претходног, закључујемо

$$1 \leq r_j < \frac{r_{j-2}}{2} < \frac{r_{j-4}}{4} < \cdots < \frac{r_0}{2^{j/2}},$$

ако је j парно, а

$$2 \leq r_{j-1} < \frac{r_{j-3}}{2} < \frac{r_{j-5}}{4} < \cdots < \frac{r_0}{2^{(j-1)/2}},$$

ако је j непарно. Дакле, у сваком случају је $a = r_0 > 2^{j/2}$, па је $j < 2 \log_2 a$. □

Користећи Еуклидов алгоритам, могуће је највећи заједнички дјелилац два броја изразити као њихову линеарну комбинацију. У следећем примјеру је дат поступак како је то могуће урадити.

Проширени Еуклидов алгоритам. Рјешења једначине

$$ax + by = \mathbf{нзд}(a, b)$$

могу се ефикасно добити у следећем поступку. Ако је

$$\begin{array}{lll} r_{-1}=a, & r_0=b; & r_i=r_{i-2}-q_i r_{i-1}; \\ x_{-1}=1, & x_0=0; & x_i=x_{i-2}-q_i x_{i-1}; \\ y_{-1}=1, & y_0=0; & y_i=y_{i-2}-q_i y_{i-1}; \end{array}$$

онда је

$$ax_i+by_i=r_i, \quad i=-1,0,1,\ldots,j+1,$$

гдје је j индекс везан за Еуклидов алгоритам, представљен у Теореми 1.3.

Примјер 1.2. *Одредити највећи заједнички дјелитељ за бројеве* 4056 *и* 1848 *и приказати га као њихову линеарну комбинацију.*

Рјешење

$$\begin{aligned} 4056 &= 1848\cdot 2+360 \\ 1848 &= 360\cdot 5+48 \\ 360 &= 48\cdot 7+24 \\ 48 &= 24\cdot 2+0 \end{aligned}$$

i	q_i	x_i	y_i
-1		1	0
0		0	1
1	2	1	-2
2	5	-5	11
3	7	36	-79

Дакле, имамо да је

$$36\cdot 4056-79\cdot 1848=24.$$

□

Задатак 1.5. *Доказати да је* $a^{2^n}+1$ *дјелилац броја* $a^{2^m}-1$ *за* $m>n$, *а да је за* $a,m,n\in\mathbb{N}$, $m\neq n$

$$\textbf{нзд}\left(a^{2^m}+1, a^{2^n}+1\right)=\begin{cases} 2, & \text{ако је } a \text{ непаран,} \\ 1, & \text{ако је } a \text{ паран.} \end{cases}$$

Рјешење. *Прво тврђење у задатку се доказује индукцијом по* $m>n$. *Како је* $(a^{2^n}+1)(a^{2^n}-1)=a^{2^{n+1}}-1$, *слиједи да* $a^{2^n}+1 \mid a^{2^{n+1}}-1$. *Дакле, ако* $a^{2^n}+1 \mid a^{2^k}-1$, *онда*

$$a^{2^n}+1 \mid \left(a^{2^k}-1\right)\left(a^{2^k}+1\right)=a^{2^{k+1}}-1,$$

чиме је први дио тврђења доказан.

Ако је $m \neq n$, онда је један од бројева m, n већи. Нека је то, на примјер, број m. Користећи претходну тврдњу, имамо да је

$$a^{2^m} - 1 = k(a^{2^n} + 1),$$

што значи да је

$$a^{2^m} + 1 = k(a^{2^n} + 1) + 2,$$

одакле слиједи да је $\textbf{нзд}\left(a^{2^m} + 1, a^{2^n} + 1\right)$ *дјелилац броја* 2*. То значи да су једине двије могућности* 1 *или* 2*. У случају, да је a паран, онда су бројеви $a^{2^m} + 1, a^{2^n} + 1$ непарни, па највећи заједнички дјелилац мора бити* 1*. У случају да је a непаран, онда су посматрани бројеви парни, па је највећи заједнички дјелилац* 2*.*

Напомињемо да се у доказу ништа суштински не би промијенило ни да смо претпоставили да је n већи, сем што би m и n у претходном поступку замијенили мјеста.

1.3 Најмањи заједнички садржалац

Дефиниција 1.4. ***Заједнички садржалац*** *два ненулта броја, a и b, је цио број c, такав да $a \mid c$ и $b \mid c$. Ако су оба броја, a и b, ненулта, онда увијек постоји позитивни заједнички садржалац, као на примјер $|ab|$. Сагласно томе, постоји и* ***најмањи заједнички садржалац****,* $\textbf{нзс}(a, b)$*, односно најмањи позитивни број l који задовољава два услова*

(1) Ако $a \mid l$ и $b \mid l$.

(2) Ако $a \mid c$ и $b \mid c$, при чему је $l > 0$, онда $l \leq c$.

Често се умјесто $\textbf{нзс}(a, b)$ *користи и ознака $[a, b]$.*

Слично, дефинишемо најмањи заједнички садржалац ненултих бројева $a_1, a_2, \ldots a_n$ и означавамо са $[a_1, a_2, \ldots, a_n]$.

Својства најмањег заједничког садржаоца су у одређеном смислу везана за својства највећег заједничког дјелиоца, што се потврђује и следећом теоремом. Пошто је $\textbf{нзд}(a, b) = \textbf{нзд}(|a|, |b|)$, а $\textbf{нзс}(a, b) = \textbf{нзс}(|a|, |b|)$, онда без умањења општости можемо сматрати да су a и b природни бројеви.

Теорема 1.4. *Ако су a и b природни бројеви, онда је*

$$\textbf{нзд}(a,b)\,\textbf{нзс}(a,b) = ab.$$

Доказ. Нека је $d = \textbf{нзд}(a,b)$ и $l = \textbf{нзс}(a,b)$. Доказујемо да је $\dfrac{ab}{d}$ најмањи заједнички садржалац бројева a и b. Ако је $e = a/d$ и $f = b/d$, онда

$$\frac{ab}{d} = \frac{(de)(df)}{d} = def.$$

Очигледно, добијени број def је позитиван, па је потребно доказати да је то заправо најмањи заједнички садржалац датих бројева. Прво,

$$def = (de)f = af \text{ и } def = (df)e = be,$$

што значи да је $a \mid def$ и $b \mid def$, па је def заједнички садржалац бројева a и b. Доказујемо да је то заправо најмањи заједнички садржалац.

Претпоставимо да $a \mid c$ и $b \mid c$, за $c > 0$. Потребно је показати да је $def \leq c$. На основу Теореме 1.2 имамо да је $d = au + bv$, за цијеле бројеве u и v. На основу тога имамо

$$\frac{c}{def} = \frac{cd}{(de)(df)} = \frac{cd}{ab} = \frac{c(au+bv)}{ab} = \frac{c}{b}u + \frac{c}{a}v,$$

што је цио број, па закључујемо да је $def \mid c$, односно $def \leq c$. □

Лема 1.9. *Сваки заједнички садржалац бројева $a_1, a_2, \ldots, a_n$ је дјељив са* $\textbf{нзс}(a_1, a_2, \ldots, a_n)$.

Доказ. Нека је $N = \textbf{нзс}(a_1, a_2, \ldots, a_n)$. Претпоставимо да постоји заједнички садржалац M датих бројева који није дјељив са N. Онда је

$$M = qN + r,$$

гдје је r природан број и $r < N$. Дакле, $r = M - qN$. Нека је i произвољан број из скупа $1, 2, \ldots, n$. Пошто су M и N садржаоци броја a_i, онда је $M = x_i a_i$ и $N = y_i a_i$. Одатле је

$$r = M - qN = (x_i - qy_i)a_i,$$

одакле закључујемо да $a_i \mid r$ за $i = 1, 2, \ldots, n$. Слиједи да је r заједнички садржалац за бројеве $a_1, a_2, \ldots, a_n$, мањи од N. То је супротно претпоставвци да је N најмањи заједнички садржалац бројева $a_1, a_2, \ldots, a_n$. Значи, $M \mid N$. □

Лема 1.10. *Сваки заједнички дјелилац бројева $a_1, a_2, \ldots, a_n$ дијели* **нзд**$(a_1, a_2, \ldots, a_n)$.

Доказ. Нека је $d = \mathbf{нзд}(a_1, a_2, \ldots, a_n)$, а s произвољан дјелилац датих бројева. Нека је $N = \mathbf{нзс}(d, s)$. За произвољно a_i вриједи

$$d \mid a_i \text{ и } s \mid a_i,$$

па на основу претходне леме имамо $N \mid a_i$, за $i = 1, 2, \ldots, n$. Дакле, N је заједнички дјелилац $a_1, a_2, \ldots, a_n$. Како је d највећи заједнички дјелилац тих бројева, то је $N \leq d$. Са друге стране, $N = \mathbf{нзс}(d, s)$, па је $N \geq d$. Тиме је показано да је $N = d$, из чега слиједи да $s \mid d$. □

Лема 1.11. *За природне бројеве $a_1, a_2, \ldots, a_n$ вриједи*

$$\mathbf{нзд}(a_1, a_2, \ldots, a_n) = \mathbf{нзд}(\mathbf{нзд}(a_1, a_2, \ldots, a_{n-1}), a_n)$$

Доказ. Нека је $t = \mathbf{нзд}(a_1, a_2, \ldots, a_{n-1})$, а

$$s = \mathbf{нзд}(\mathbf{нзд}(a_1, a_2, \ldots, a_{n-1}), a_n) = \mathbf{нзд}(t, a_n).$$

Пошто је s дјелитељ t и a_n, а t дјелитељ сваког од посматраних бројева $a_1, a_2, \ldots, a_{n-1}$, онда је s заједнички дјелитељ $a_1, a_2, \ldots, a_n$. Нека је s' произвољан дјелитељ бројева $a_1, a_2, \ldots, a_n$. На основу претходне леме, слиједи да $s' \mid t$. Како $s' \mid a_n$, онда $s' \mid \mathbf{нзд}(t, a_n)$, односно $s' \mid s$. То значи да је s заједнички дјелитељ бројева $a_1, a_2, \ldots, a_n$ са особином да је дјељив са произвољним заједничким дјелиоцем посматраних бројева. То управо значи да је $s = \mathbf{нзд}(a_1, a_2, \ldots, a_n)$. □

Лема 1.12. *За природне бројеве $a_1, a_2, \ldots, a_n$ вриједи*

$$\mathbf{нзс}(a_1, a_2, \ldots, a_n) = \mathbf{нзс}(\mathbf{нзс}(a_1, a_2, \ldots, a_{n-1}), a_n)$$

Доказ. Нека је $N = \mathbf{нзс}(\mathbf{нзс}(a_1, a_2, \ldots, a_{n-1}), a_n)$. Очигледно, N је садржалац бројева $a_1, a_2, \ldots, a_n$. Нека је M произвољан садржалац бројева $a_1, a_2, \ldots, a_n$. Пошто

$$\mathbf{нзс}(a_1, a_2, \ldots, a_{n-1}) \mid M \text{ и } a_n \mid M,$$

онда на основу Леме 1.9 слиједи да

$$\mathbf{нзс}(\mathbf{нзс}(a_1, a_2, \ldots, a_{n-1}), a_n) \mid M,$$

односно $N \mid M$. Дакле, N је заједнички садржалац $a_1, a_2, \ldots, a_n$ такав да дијели сваки други заједнички садржалац датих бројева. Слиједи, по дефиницији, да је $N = \mathbf{нзс}(a_1, a_2, \ldots, a_n)$. □

1.4 Представљање цијелих бројева у одређеној бази

Подразумијеван облик представљања бројева је у *децималном* облику, што значи да запис неког броја користимо *основу* или *базу* 10, па запис одређеног броја, на примјер 3567, значи:

$$3 \cdot 10^3 + 5 \cdot 10^2 + 6 \cdot 10^1 + 7 \cdot 10^0.$$

Не постоји јасан разлог због чега би за представљање бројева користили основу 10, изузев то што имамо 10 прстију на рукама. Познато је да су Вавилонци користили основу 60, док су Маје користиле основу 20. У свијету рачунара, користимо основу 2.

Следећа теорема указује да сваки природан број већи од 1 може бити база представљања.

Теорема 1.5. *Нека је b природан број већи од 1. Сваки природан број n се може написати у облику*

$$n = a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b + a_0,$$

гдје су a_j цијели бројеви такви да $0 \leq a_j \leq b-1$ за $j = 0, 1, \ldots, k$ и $a_k \neq 0$.

Последица 1.3. *Сваки природан број је могуће, на јединствен начин, представити као суму степена броја 2.*

Задатак 1.6. *Наћи све природне бројеве a такве да је $a^{10} + 1$ дјељиво са 10.*

Рјешење. *Нека је r остатак при дијељењу природног броја са 10. Лако је видјети да је $a^{10} + 1$ дјељиво са 10 ако и само ако је $r^{10} + 1$ дјељиво са 10. Пошто су могућности за r из скупа $0, 1, \ldots, 9$ онда директном провјером закључујемо да су само*

$$3^{10} + 1 \text{ и } 7^{10} + 1$$

дјељиви са 10. Дакле, сви бројеви a облика $10k + 3$ и $10k + 7$, за $k = 0, 1, 2, \ldots$ су они за које вриједи да је $a^{10} + 1$ дјељиво са 10.

Задатак 1.7. *Доказати да постоји бесконачан скуп бројева облика* $t_n = \frac{1}{2}n(n+1)$, $n = 1, 2, \ldots$ *такав да су свака два елемента тог скупа релативно проста.*

Рјешење. *Показаћемо заправо да постоји бесконачан растући низ траженог облика у ком су свака два елемента релативно проста.*

Најприје показујемо да ако постоји m *таквих бројева*

$$t_{k_1} < t_{k_2} < \cdots < t_{k_m},$$

који су релативно прости, онда постоји $t \in \mathbb{N}$, *такође облика* $\frac{1}{2}n(n+1)$ *за неко* $n \in \mathbb{N}$, *такав да је релативно прост са свим бројевима*

$$t_{k_1}, t_{k_2}, \ldots, t_{k_m}.$$

Нека је $s = t_{k_1}t_{k_2}\cdots t_{k_m}$. *Посматрајмо број*

$$t = \frac{(2s+1)(2s+2)}{2} = (s+1)(2s+1).$$

Очигледно, број t *је одговарајућег облика и производ је фактора* $s+1$ *и* $2s+1$ *који су релативно прости са* s, *а тиме и са сваким од бројева* $t_{k_1}, t_{k_2}, \ldots, t_{k_m}$ *који учествују у производу. Тиме смо показали да постојећи скуп од* m *бројева можемо проширити са новим* $t_{k_{m+1}} = t$, *а да остану задовољене све тражене особине. На описани начин, поступак се наставља за* $m+2, m+3, \ldots$

На примјер, ако почнемо са најмањим бројем $t_1 = 1$ *имамо низ*

$$t_1 = 1, t_2 = 3, t_4 = 10, t_{13} = 91, t_{22} = 253, \ldots$$

у ком су свака два броја релативно проста.

Задатак 1.8. *Ако су* a *и* b *два различита цијела броја, онда постоји бесконачно много природних бројева* $n \in \mathbb{N}$ *таквих да су* $a+n$ *и* $b+n$ *релативно прости.*

Рјешење. *Нека су* a *и* b *два различита цијела броја и нека је* $a < b$. *Посматрајмо број*

$$n = (b-a)k + 1 - a.$$

За довољно велико k, n *је природан број. Тиме су и*

$$a + n = (b-a)k + 1,\ b + n = (b-a)(k+1) + 1$$

такође природни броеви. Ако $d \mid a+n$ *и* $d \mid b+n$*, онда* $d \mid b-a$*. Даље, из* $d \mid a+n$ *и* $d \mid b-a$*, слиједи да* $d \mid 1$*, одакле је* $d = 1$*. Дакле,*

$$\textbf{нзд}(a+n, b+n) = 1.$$

Значи, одабиром довољно великог броја k *добијамо одговарајући број* n *за који вриједи да су* $a+n$ *и* $b+n$ *релативно прости.*

Глава 2

Прости бројеви

Вјероватно не постоји у историји математике појам који је привлачио више пажње како лаичке, тако и стручне математичке јавности од простих бројева.

Дефиниција 2.1. *Природан број $p > 1$ је* ***прост*** *ако нема других дјелитеља сем 1 и себе. Ако природан број $m > 1$ није прост, онда је* ***сложен****.*

Задатак 2.1. *Одредити прост број p ако се зна да су $p+10$ и $p+14$ прости бројеви.*

Рјешење. *За $p = 3$ су $p + 10$ и $p + 14$ прости бројеви. Ако је $p \geq 3$ прост број, онда је он или облика $3k + 1$ или облика $3k + 2$, за неко $k \in \mathbb{N}$. У првом случају је $p + 14 = 3(k + 5)$, а у другом је $p + 10 = 3(k + 4)$ сложен број. Дакле, једини такав p је број 3.*

Лема 2.1. *Најмањи дјелилац већи од јединице, произвољног цијелог броја је прост број.*

Доказ. Нека је n цио број и нека је q његов најмањи дјелилац који је већи од 1. Ако би q био сложен, онда би постојао неки дјелилац p за који важи $1 < p < q$. Но, тада би p дјелилац и броја n, па q не би био најмањи међу дјелиоцима броја n који су већи од 1. □

Теорема 2.1. ***(Еуклид)*** *Постоји бесконачно много простих бројева. Другим ријечима, од сваког простог броја постоји већи прост број.*

Доказ. Претпоставимо да тврђење није истинито, односно да постоји коначан скуп простих бројева $p_1, p_2, \ldots, p_k$, а да су сви остали природни бројеви већи од 1 сложени. Број

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

је према томе сложен. На основу претходне леме, слиједи да је најмањи дјелилац, већи од 1, неки прост број. Међутим, то није могуће, јер N приликом дијељења са било којим простим бројем из листе $p_1, p_2, \ldots, p_k$ даје остатак 1. То значи да скуп простих бројева мора бити бесконачан. □

Теорема 2.2. *Сваки природан број $n > 1$ може се приказати (представити) као производ простих бројева. Овај приказ је јединствен, односно два представљања се могу разликовати само у поретку чинилаца.*

Примјетимо да претходна теорема обезбјеђује да се сваки природан број n може приказати у облику

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r},$$

гдје су $p_1, \ldots, p_r$ различити бројеви, а $\alpha_1, \ldots, \alpha_r$ природни бројеви. Овај приказ називамо **канонским растављањем** или **канонском факторизацијом** природног броја на просте чиниоце.

Лема 2.2. *Ако је p прост број и $p \mid ab$, онда $p \mid a$ или $p \mid b$. Општије, ако $p \mid a_1 a_2 \cdots a_n$, онда p дијели бар један чинилац a_i.*

Доказ. Претпоставимо да p не дијели a. Онда су p и a узајамно прости бројеви. У том случају, на основу Леме 1.7, слиједи да $p \mid b$. Општији случај се по истом принципу доказује индукцијом. □

Задатак 2.2. *Доказати да ако је n непаран број, онда је $n^2 - 1$ дјељив са 8, а ако је n прост број већи од 3, онда је $n^2 - 1$ дјељив са 24.*

Рјешење. *Пошто је $n^2 - 1 = (n-1)(n+1)$ производ два узастопна парна броја, онда је бар један од њих дјељив са 4, па је производ дјељив са 8. Уколико је n прост број већи од 3, онда n није дјељив са 3, али зато неки од његових сусједа, $n-1$ или $n+1$ мора бити. Стога је производ дјељив са 8 и 3, односно са 24.*

Задатак 2.3. *Доказати да*

$$M = \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}$$

не може бити цијели број.

Рјешење. *Нека је k највећи цио број за који је $2^k \leq n$ и P производ свих непарних бројева који нису већи од n. Претпоставимо, супротно тврђењу, да је број M цио. Онда је и $2^{k-1}PM$ цијели број. Међутим, тада имамо да су у изразу*

$$2^{k-1}PM = 2^{k-1}P(\frac{1}{2} + \frac{1}{3} + \ldots \frac{1}{2^k} + \ldots + \frac{1}{n})$$

сви сабирци цијели бројеви изузев $2^{k-1}P\frac{1}{2^k} = \frac{P}{2}$. Контрадикција.

Теорема 2.3. *Ако је производ два релативно проста природна броја квадрат цијелог броја*

$$ab = c^2, \ \textbf{нзд}(a, b) = 1,$$

онда су a и b такође квадрати неких цијелих бројева.

Доказ. Да би број био квадрат неопходно је и довољно да су му сви експоненти у факторизацији парни. Како су бројеви a и b узајамно прости, сваки прост дјелилац броја c^2 се јавља или у факторизацији броја a или b, али не у оба. Из тог разлога, експоненти простих бројева који у учествују у факторизацији бројева a и b морају бити парни. □

Задатак 2.4. *Одредити све просте бројеве p и q за које је*

$$p^2 - 2q^2 = 1.$$

Рјешење. *Дата једначина се може написати у облику*

$$(p-1)(p+1) = 2q^2.$$

Очигледно, за $p = 2$ она нема рјешења. Ако је p прост и $p > 2$, онда $(p-1)(p+1)$ мора бити дјељиво са 8, па је q^2 дјељиво са 4, па q није прост, изузев ако је $q = 2$. Но, у том случају, $p = 3$. Дакле, једино рјешење је $p = 3$ и $q = 2$.

Интересантно је, коришћењем факторизације цијелих бројева на просте факторе, опет размотрити највећи заједнички дјелилац и најмањи садржалац. Наиме, лако се закључује да

$$\textbf{нзд}(a,b) = \prod_p p^{\min(\alpha(p),\beta(p))},$$
$$\textbf{нзс}(a,b) = \prod_p p^{\max(\alpha(p),\beta(p))}.$$

Овај облик представљања и чињеница да за произвољне природне бројеве α и β вриједи

$$\min(\alpha,\beta) + \max(\alpha,\beta) = \alpha + \beta,$$

доказује на још један начин Теорему 1.4, односно да је

$$\textbf{нзд}(a,b)\,\textbf{нзс}(a,b) = |ab|,$$

за ненулте цијеле бројеве a и b.

Примјер 2.1. *Доказати да сваки сложен број n има прост чинилац $p \le \sqrt{n}$.*

Доказ. Нека је p најмањи прост број који дијели n. Слиједи да је

$$n = pm, \text{ при чему је } p \le m.$$

Дакле, $n \ge p^2$, што значи да $p \le \sqrt{n}$. □

Примјер 2.2. *Доказати да простих бројева облика $4k+3$ има бесконачно много.*

Доказ. Сви непарни прости бројеви су облика $4r+1$ или $4k+3$. Лако се уочава да се множењем два броја облика $4r+1$ добија број истог облика.

Претпоставимо да су $\{p_1, p_2, \ldots, p_n\}$ сви прости бројеви облика $4k+3$. Посматрајмо број

$$4p_1p_2\cdots p_n - 1.$$

Овај број није облика $4r+1$, што значи да има бар један прост фактор облика $4k+3$. Међутим, то нас доводи до закључка да тај прост фактор мора бити из скупа $\{p_1, p_2, \ldots, p_n\}$, а одатле слиједи да тај прост број дијели 1, што је немогуће. Дакле, претпоставка да имамо коначно много простих бројева облика $4k+3$ је погрешна. □

Примјер 2.3. *Доказати да за сваки природан број n постоји n узастопних сложених бројева.*

Доказ. Посматрајмо бројеве

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

Сваки од датих бројева облика $(n+1)!+j$, гдје је $2 \leq j \leq n+1$ је сложен, јер се фактор j може извући као уаједнички за два сабирка. □

Примјер 2.4. *Доказати да не постоји полином $f(x)$ са цјелобројним коефицијентима степена ≥ 1, такав да је $f(n)$ прост за све $n \in \mathbb{N}$.*

Доказ. Нека је $f(1) = p$. Тада је p прост број. Како увијек $x - y$ дијели $x^m - y^m$, онда је $f(1+kp) - f(1)$ дјељиво са $(1+kp)-1 = kp$. Одавдје слиједи да $p \mid f(1+kp)$ за сваки $k \in \mathbb{N}$. Међутим, $f(1+kp)$ је прост, па мора бити $f(1+kp) = p$ за свако $k \in \mathbb{N}$. Значи, полином $f(x)-p$ има бесконачно много нула, одакле закључујемо да је $f(x) = p$, а што је у супротности са претпоставком да је степен полинома $f(x)$ већи од један. □

Примјер 2.5. *Нека је број 2^n+1 прост. Доказати да је тада $n = 0$ или $n = 2^k$ за неки $k \geq 0$.*

Доказ. Претпоставимо супротно, да је $n = 2^k m$, гдје је m непаран број већи од 1. Тада је

$$2^n + 1 = \left(2^{2^k}\right)^m + 1,$$

па $2^{2^k} + 1 \mid 2^n + 1$, јер $x + y \mid x^m + y^m$ за непарно m. □

Бројеви облика $2^{2^n} + 1$ називају се **Фермаови бројеви**. Иако је Ферма сматрао да су сви бројеви ог облика прости, постоје и сложени Фермаови бројеви. На примјер, број $2^{32} + 1$ је сложен.

Примјер 2.6. *Нека је број $2^m - 1$ прост. Доказати да је тада m прост број.*

Доказ. Ако би било $n = n_1 n_2$, $1 < n_1, n_2 < n$, број $2^n - 1 = (2^{n_1})^{n_2} - 1$ би био дјељив са $2^{n_1} - 1$. □

Бројеви облика $M_p = 2^p - 1$, за прост број p, називају се **Мерсенови бројеви**. Неки Мерсенови бројеви су прости као на примјер $M_7 = 127$, а неки сложени, као на примјер $M_{11} = 2047 = 23 \cdot 89$. Хипотеза је да има бесконачно много простих Мерсенових бројева.

2.1 Теорема о дистрибуцији простих бројева

Једно важно питање које се тиче простих бројева је процјена колико их има у неком интервалу, односно колико има простих бројева који су мањи од неког задатог природног броја n?

Дефинишимо функцију $\pi(n)$ као број простих бројева који су мањи или једнаки n

$$\pi(n) = |\{p \in \mathbf{P} \mid p \leq n\}|.$$

У следећој табели су дате неколико првих вриједности функције $\pi(n)$. Примјетимо да је функција монотоно растућа

n	2	3	4	5	6	7	8	9	10	11	...
$\pi(n)$	1	2	2	3	3	4	4	4	4	5	...

У криптографији, врло често се користе веома велики прости бројеви. Иако је показано да простих бројева има бесконачно много, један од проблема је и како наћи довољно велики прости број. Овај проблем је везан за питање дистрибуције простих бројева. На примјер, колико је вјероватно да дати интервал садржи прост број? Следећа теорема, коју дајемо без доказа, даје одговор на претходно питање. Наиме, каже да је могуће наћи прост број задате величине, а и да то, с обзиром на густину простих бројева $\mathbf{P}$ унутар скупа природних бројева, није тешко.

Теорема 2.4.

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

Дакле, претходна теорема даје прилично тачну апроксимацију о броју простих бројва мањих или једнаких n

$$\pi(n) \approx \frac{n}{\ln(n)},$$

што значи да је број простих бројева у интервалу (n_1, n_2) приближно $\pi(n_2) - \pi(n_1)$, односно

$$\frac{n_2}{\ln(n_2)} - \frac{n_1}{\ln(n_1)}.$$

Многи велики проблеми у историји математике су везани за просте бројеве. Још увијек постоји много отворених проблема из ове области, а ми ћемо навести неке. На примјер, претпоставља се да постоји бесконачно много *простих близанаца*, односно парова простих бројева p и $p+2$. Такође, чувена *Голдбахова хипотеза* каже да је сваки паран број могуће представити као збор два проста броја.

Задатак 2.5. *Доказати да је $n^4 + 4$ сложен ако је $n \in \mathbb{N}$, $n > 1$. (Овај задатак је познат као задатак Софије Жермен)*

Рјешење. *Пошто је*

$$n^4 + 1 = (n^2 - 2n + 2)(n^2 + 2n + 2)$$

и оба фактора на десној страни су већа од 1 за $n > 1$, тиме је тврђење доказано.

Задатак 2.6. *Ако су p и $8p^2 + 1$ прости бројеви, доказати да је и $8p^2 + 2p + 1$ прост број.*

Рјешење. *Очигледно, тврђење вриједи за $p = 3$. Сви остали прости бројеви, већи од 3, су облика $3k - 1$, односно $3k + 1$. У случају да је p облика $3k - 1$ или $3k + 1$ видимо да је $8p^2 + 1$ дјељив са 3. Тиме је показано да је за $p > 3$, број $8p^2 + 1 > 3$ и дјељив са 3, што значи да није прост. Дакле, једина могућност је $p = 3$.*

Задатак 2.7. *Ако је p прост број већи од 2, доказати да је бројилац сведеног разломка једнаког збиру*

$$1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p-1}$$

дјељив са p.

Рјешење. *Бројилац датог збира је*

$$\frac{(p-1)!}{1} + \frac{(p-1)!}{2} + \frac{(p-1)!}{3} + \cdots + \frac{(p-1)!}{p-2} + \frac{(p-1)!}{p-1}.$$

У претходном збиру имамо паран број сабирака, па можемо сабирати у паровима: први и последњи, други и претпоследњи... На овај начин добијамо збирове облика

$$\frac{(p-1)!}{k} + \frac{(p-1)!}{p-k} = \frac{p(p-1)!}{k(p-k)}, \text{ за } k < p.$$

Јасно је да је на десној страни претходне једнакости цијели број, представљен у облику разломка у чијем бројиоцу је и фактор p. Пошто су k и $p-k$ строго мањи од простог броја p, то значи да се прости број p не може скратити ни са чим из имениоца $k(p-k)$. То значи да је

$$\frac{p(p-1)!}{k(p-k)}, \text{ за } k < p,$$

цијели број дјељив са p. Тиме је доказано да је и посматрани збир дјељив са p.

Задатак 2.8. *Нека је n природан број и p прост број такав да $n \mid (p-1)$ и $p \mid (n^6-1)$. Доказати да је бар један од бројева $p-n$ и $p+n$ потпун квадрат.*

Рјешење. *Како је $n \mid (p-1)$, слиједи да је $p = 1 + an$ за неки природан број a. Из услова*

$$p \mid (n^6-1) = (n^3-1)(n^3+1) = (n-1)(n^2+n+1)(n+1)(n^2-n+1)$$

слиједи да $p \mid (n-1)$, $p \mid (n+1)$, $p \mid (n^2+n+1)$ или $p \mid (n^2-n+1)$.

Разматрамо сваки до ових услова посебно.

Ако $p \mid (n-1)$, онда је $n-1 \geq p = 1+na \geq n+1$, а ово је немогуће.

Ако $p \mid (n+1)$, онда је $n+1 \geq p = 1+na$, па онда слиједи да је $a = 1$, одакле слиједи да је $p-n = 1$ потпун квадрат.

Ако $p \mid (n^2+n+1)$ имамо да је $n^2+n+1 = pb$ за неки природан број b. Замјеном $p = 1+na$ добијамо $n^2+n+1 = nab+b$, односно $n(n-ab+1) = b-1$. Одавде слиједи да је $n \mid b-1$ и $b = 1+nc$

за неки ненегативан цио број c. Вратимо се још једном на израз $n^2+n+1 = nab+b$ и уврстимо добијене изразе

$$n^2+n+1 = na(nc+1)+(nc+1) = n^2ac+n(a+c)+1,$$

одакле даље слиједи

$$n+1 = acn+a+c.$$

Ако је $ac \geq 1$ тада је $a+c \geq 2$ и посљедња једнакост није могућа. Дакле, $ac = 0$, одакле из услова да је a природан број, слиједи да је $c = 0$, па је $a = n+1$. Стога је

$$p+n = (1+na)+n = 1+n(n+1)+n = n^2+2n+1 = (n+1)^2.$$

Следећи случај тече скоро идентично као претходни.

Ако $p \mid (n^2-n+1)$ имамо да је $n^2-n+1 = pb$ за неки природан број b. Замјеном $p = 1+na$ добијамо $n^2-n+1 = nab+b$, односно $n(n-ab-1) = b-1$. Одавде слиједи да је $n \mid b-1$ и $b = 1+nc$ за неки ненегативан цио број c. Вратимо се још једном на израз $n^2-n+1 = nab+b$ и уврстимо добијене изразе

$$n^2+n+1 = na(nc+1)+(nc+1) = n^2ac+n(a+c)+1,$$

одакле даље слиједи

$$n-1 = acn+a+c.$$

Ако је $ac \geq 1$ тада је $a+c \geq 2$ и посљедња једнакост није могућа. Дакле, $ac = 0$, одакле из услова да је a природан број, слиједи да је $c = 0$, па је $a = n-1$. Стога је

$$p-n = (1+na)-n = 1+n(n-1)-n = n^2-2n+1 = (n-1)^2,$$

чиме је тврђење у потпуности доказано.