Uvod u teoriju brojeva

(skripta)

Andrej Dujella

PMF - Matematički odjel
Sveučilište u Zagrebu

Sadržaj

1. Djeljivost 2

2. Kongruencije 12

3. Kvadratni ostatci 29

4. Kvadratne forme 38

5. Aritmetičke funkcije 47

6. Diofantske aproksimacije 59

7. Diofantske jednadžbe 75

8. Kvadratna polja 86

1. Djeljivost

Teorija brojeva je grana matematike koja se ponajprije bavi proučavanjem svojstava skupa prirodnih brojeva

$$\mathbb{N} = \{1, 2, 3, 4, \dots\}.$$

Jedno od osnovnih svojstava skupa $\mathbb{N}$ je da su na njemu definirane operacije zbrajanja i množenja koje zadovoljavaju zakone komutativnosti, asocijativnosti i distributivnosti. Pored toga, na skupu $\mathbb{N}$ imamo uređaj takav da za svaka dva različita elementa m, n iz $\mathbb{N}$ vrijedi ili $m < n$ ili $n < m$. Nadalje, svaki neprazan podskup od $\mathbb{N}$ ima najmanji element, te vrijedi princip matematičke indukcije. Ova svojstva ćemo u daljnjem često koristiti.

Osim svojstava skupa $\mathbb{N}$, proučavat ćemo i svojstva skupa cijelih brojeva $0, \pm 1, \pm 2, \pm 3, \dots$ kojeg ćemo označavati sa $\mathbb{Z}$, te skupa racionalnih brojeva, tj. brojeva oblika $\frac{p}{q}$ za $p \in \mathbb{Z}$, $q \in \mathbb{N}$, kojeg ćemo označavati s $\mathbb{Q}$.

Pojam djeljivosti je jedan od najjednostavnijih, ali ujedno i najvažnijih pojmova u teoriji brojeva. Stoga ćemo s njim započeti naša razmatranja.

Definicija 1.1. *Neka su $a \neq 0$ i b cijeli brojevi. Kažemo da je b* djeljiv *s a, odnosno da a* dijeli *b, ako postoji cijeli broj x takav da je $b = ax$. To zapisujemo sa $a|b$. Ako b nije djeljiv sa a, onda pišemo $a \nmid b$.*

Ako $a|b$, onda još kažemo da je a djelitelj *od b, a da je b* višekratnik *od a. Oznaka $a^k \| b$ će nam značiti da $a^k | b$, ali $a^{k+1} \nmid b$.*

Uočimo da je relacija "biti djeljiv" relacija parcijalnog uređaja na skupu $\mathbb{N}$, ali nije na skupu $\mathbb{Z}$ (jer $a|b$ i $b|a$ povlači da je $a = \pm b$).

Teorem 1.1 (Teorem o dijeljenju s ostatkom)**.** *Za proizvoljan prirodan broj a i cijeli broj b postoje jedinstveni cijeli brojevi q i r takvi da je $b = qa + r$, $0 \leq r < a$.*

Dokaz: Promotrimo skup $\{b - am : m \in \mathbb{Z}\}$. Najmanji nenegativni član ovog skupa označimo sa r. Tada je po definiciji $0 \leq r < a$ i postoji $q \in \mathbb{Z}$ takav da je $b - qa = r$, tj. $b = qa + r$.

Da bi dokazali jedinstvenost od q i r, pretpostavimo da postoji još jedan par q_1, r_1 koji zadovoljava iste uvjete. Pokažimo najprije da je $r_1 = r$. Pretpostavimo da je npr. $r < r_1$. Tada je $0 < r_1 - r < a$, dok je s druge strane $r_1 - r = a(q - q_1) \geq a$. Prema tome je $r_1 = r$, pa je stoga i $q_1 = q$. □

Definicija 1.2. *Neka su b i c cijeli brojevi. Cijeli broj a zovemo* zajednički djelitelj *od b i c ako $a|b$ i $a|c$. Ako je barem jedan od brojeva b i c različit*

od nule, onda postoji samo konačno mnogo zajedničkih djelitelja od b i c. Najveći među njima zove se najveći zajednički djelitelj *od b i c i označava se s (b, c). Slično se definira najveći zajednički djelitelj brojeva $b_1, b_2, \ldots, b_n$ koji nisu svi jednaki nuli, te se označava s $(b_1, b_2, \ldots, b_n)$.*

Uočimo da je $(b, c) \geq 1$.

Teorem 1.2.

$$(b, c) = \min(\{bx + cy \,:\, x, y \in \mathbb{Z}\} \cap \mathbb{N})$$

Dokaz: Neka je $g = (b, c)$, te neka je l najmanji pozitivni član skupa $S = \{bx + cy \,:\, x, y \in \mathbb{Z}\}$. To znači da postoje cijeli brojevi x_0 i y_0 takvi da je $l = bx_0 + cy_0$.

Pokažimo da $l|b$ i $l|c$. Pretpostavimo da npr. $l \nmid b$. Tada po Teoremu 1.1 postoje cijeli brojevi q i r takvi da je $b = lq + r$ i $0 < r < l$. Sada je

$$r = b - lq = b - q(bx_0 + cy_0) = b(1 - qx_0) + c(-qy_0) \in S,$$

što je u suprotnosti s minimalnošću od l. Dakle, $l|b$, a na isti način se pokazuje da $l|c$. To znači da je $l \leq g$.

Budući da je $g = (b, c)$, to postoje $\beta, \gamma \in \mathbb{Z}$ takvi da je $b = g\beta$, $c = g\gamma$, pa je $l = bx_0 + cy_0 = g(\beta x_0 + \gamma y_0)$. Odavde slijedi da je $g \leq l$, pa smo dokazali da je $g = l$. □

Ako se cijeli broj d može prikazati u obliku $d = bx + cy$, onda je (b, c) djelitelj od d. Posebno, ako je $bx + cy = 1$, onda je $(b, c) = 1$.

Ako je d zajednički djeljitelj od b i c, onda $d|(b.c)$. Zaista, d dijeli b i c, pa onda dijeli i $bx + cy$, te tvrdnja slijedi iz Teorema 1.2.

Definicija 1.3. *Reći ćemo da su cijeli brojevi a i b i* relativno prosti *ako je $(a, b) = 1$. Za cijele brojeve $a_1, a_2, \ldots, a_n$ reći ćemo da su* relativno prosti *ako je $(a_1, a_2, \ldots, a_n) = 1$, a da su* u parovima relativno prosti *ako je $(a_i, a_j) = 1$ za sve $1 \leq i, j \leq n$, $i \neq j$.*

Propozicija 1.3. *Ako je $(a, m) = (b, m) = 1$, onda je $(ab, m) = 1$.*

Dokaz: Po Teoremu 1.2 postoje $x_0, y_0, x_1, y_1 \in \mathbb{Z}$ takvi da je $1 = ax_0 + my_0 = bx_1 + my_1$. Odavde je $ax_0bx_1 = (1 - my_0)(1 - my_1) = 1 - my_2$, gdje je $y_2 = y_0 + y_1 - my_0y_1$. Sada iz $abx_0x_1 + my_2 = 1$ zaključujemo da je $(ab, m) = 1$. □

Propozicija 1.4.

$$(a, b) = (a, b + ax)$$

Dokaz: Označimo $(a, b) = d$, $(a, b + ax) = g$. Po Teoremu 1.2 postoje $x_0, y_0 \in \mathbb{Z}$ takvi da je $d = ax_0 + by_0$, odnosno

$$d = a(x_0 - xy_0) + (b + ax)y_0.$$

Odavde slijedi da $g|d$. Pokažimo sada da $d|g$. Budući $d|a$ i $d|b$ imamo da $d|(b+ax)$. Dakle, d je zajednički djelitelj od a i $b+ax$, pa po Teoremu 1.2 imamo da $d|g$.

Pošto su brojevi d i g pozitivni po definiciji, iz $d|g$ i $g|d$ slijedi da je $d=g$. □

Teorem 1.5 (Euklidov algoritam)**.** *Neka su b i $c>0$ cijeli brojevi. Pretpostavimo da je uzastopnom primjenom Teorema 1.1 dobiven niz jednakosti*

$$\begin{aligned} b &= cq_1 + r_1, \quad 0 < r_1 < c, \\ c &= r_1q_2 + r_2, \quad 0 < r_2 < r_1, \\ r_1 &= r_2q_3 + r_3, \quad 0 < r_3 < r_2, \\ &\dots \\ r_{j-2} &= r_{j-1}q_j + r_j, \quad 0 < r_j < r_{j-1}, \\ r_{j-1} &= r_jq_{j+1}. \end{aligned}$$

Tada je (b,c) jednak r_j, posljednjem ostatku različitom od nule. Vrijednosti od x_0 i y_0 u izrazu $(b,c)=bx_0+cy_0$ mogu se dobiti izražavanjem svakog ostatka r_i kao linearne kombinacije od b i c.

Dokaz: Po Propoziciji 1.4 imamo

$$(b,c)=(b-cq_1,c)=(r_1,c)=(r_1,c-r_1q_2)=(r_1,r_2)=(r_1-r_2q_3,r_2)=(r_3,r_2).$$

Nastavljajući ovaj proces, dobivamo: $(b,c)=(r_{j-1},r_j)=(r_j,0)=r_j$.

Indukcijom ćemo dokazati da je svaki r_i linearna kombinacija od b i c. To je točno za r_1 i r_2, pa pretpostavimo da vrijedi za r_{i-1} i r_{i-2}. Budući da je r_i linearna kombinacija od r_{i-1} i r_{i-2}, po pretpostavci indukcije dobivamo da je i linearna kombinacija od b i c. □

Primjer 1.1. *Odredimo $d=(252,198)$ i prikažimo d kao linearnu kombinaciju brojeva 252 i 198.*

Rješenje:

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

Dakle, $(252,198)=18$. Nadalje, imamo:

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

♢

Rješenja jednadžbe $bx + cy = (b, c)$ mogu se efikasno dobiti na slijedeći način: ako je

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

onda je

$$bx_i + cy_i = r_i, \quad \text{za } i = -1, 0, 1, \ldots, j+1.$$

Ova formula je točna za $i = -1$ i $i = 0$, pa tvrdnja trivijalno slijedi indukcijom, jer obje strane formule zadovoljavaju istu rekuzivnu relaciju. Posebno, vrijedi:

$$bx_j + cy_j = (b, c).$$

Primjer 1.2. *Odredimo $g = (3587, 1819)$ i nađimo cijele brojeve x, y takve da je $3587x + 1819y = g$.*

Rješenje:

$$\begin{aligned} 3587 &= 1819 \cdot 1 + 1768 \\ 1819 &= 1768 \cdot 1 + 51 \\ 1768 &= 51 \cdot 34 + 34 \\ 51 &= 34 \cdot 1 + 17 \\ 34 &= 17 \cdot 2 \end{aligned}$$

i	-1	0	1	2	3	4
q_i			1	1	34	1
x_i	1	0	1	-1	35	-36
y_i	0	1	-1	2	-69	71

Dakle, $g = 17$, te $3587 \cdot (-36) + 1819 \cdot 71 = 17$. ♢

Zadatak 1.1. *Odredite $g = (423, 198)$ i nađite cijele brojeve x, y takve da je $423x + 198y = g$.*

Zadatak 1.2. *Odredite cijele brojeve x, y takve da je*
a) $71x + 50y = 1$, *b)* $93x + 81y = 3$.

Propozicija 1.6. *Za broj koraka j u Euklidovom algoritmu vrijedi $j < 2 \log_2 c$.*

Dokaz: Pogledajmo i-ti korak. Imamo $r_i \leq \frac{r_{i-1}}{2}$ ili $\frac{r_{i-1}}{2} < r_i < r_{i-1}$. U ovom drugom slučaju imamo $q_{i+1} = 1$ i $r_{i+1} = r_{i-1} - r_i < \frac{r_{i-1}}{2}$. Dakle, u svakom slučaju je $r_{i+1} < \frac{r_{i-1}}{2}$. Odavde je

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

ako je j paran, a

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

ako je j neparan.

Dakle, u svakom slučaju je $c = r_0 > 2^{j/2}$, pa je $j < 2\log_2 c$. □

Zadatak 1.3. *Dokažite da, uz oznake iz Teorema 1.5, za $i = 0, 1, \ldots, j+1$ vrijedi $x_{i-1}y_i - x_i y_{i-1} = (-1)^i$, te $(x_i, y_i) = 1$.*

Propozicija 1.7. *Uz oznake iz Teorema 1.5, vrijedi: $|x_j| \leq \frac{c}{2g}$, $|y_j| \leq \frac{c}{2g}$, gdje je $g = (b, c)$.*

Dokaz: Pokažimo indukcijom da je $(-1)^i x_i \leq 0$, $(-1)^i y_i \geq 0$ za $i = -1, 0, 1, \ldots, j+1$. Za $i = -1, 0$ tvrdnja vrijedi po definiciji, a ako pretpostavimo da vrijedi za $i-2$, $i-1$, onda iz $x_i = x_{i-2} - q_i x_{i-1}$ slijedi $(-1)^i x_i = (-1)^{i-2} x_{i-2} + (-1)^{i-1} q_i x_{i-1} \leq 0$. Za y_i je dokaz sasvim analogan.

Prema tome, $|x_i| = |x_{i-2}| + q_i|x_{i-1}|$, $|y_i| = |y_{i-2}| + q_i|y_{i-1}|$. Nadalje, budući da je $r_{j+1} = 0$, imamo $\frac{b}{g}x_{j+1} = -\frac{c}{g}y_{j+1}$, pa iz $(\frac{b}{g}, \frac{c}{g}) = 1$ i $(x_{j+1}, y_{j+1}) = 1$ slijedi $|x_{j+1}| = \frac{c}{g}$, $|y_{j+1}| = \frac{b}{g}$. Uvrstimo li ovo u $|x_{j+1}| = |x_{j-1}| + q_{j+1}|x_j|$, $|y_{j+1}| = |y_{j-1}| + q_{j+1}|y_j|$ i uvažimo da je $q_{j+1} \geq 2$ (zbog $r_j < r_{j-1}$), dobivamo traženi rezultat. □

Definicija 1.4. *Prirodan broj $p > 1$ se zove* prost *ako p nema niti jednog djelitelja d takvog da je $1 < d < p$. Ako prirodan broj $a > 1$ nije prost, onda kažemo da je* složen.

Teorem 1.8. *Svaki prirodan broj $n > 1$ može se prikazati kao produkt prostih brojeva (s jednim ili više faktora).*

Dokaz: Dokazat ćemo teorem matematičkom indukcijom. Broj 2 je prost. Pretpostavimo da je $n > 2$, te da tvrdnja teorema vrijedi za sve m, $2 \leq m < n$. Želimo dokazati da se i n može prikazati kao produkt prostih faktora. Ako je n prost, nemamo što dokazivati. U protivnom je $n = n_1 n_2$, gdje je $1 < n_1 < n$ i $1 < n_2 < n$. Po pretpostavci indukcije, n_1 i n_2 su produkti prostih brojeva, pa stoga i n ima to svojstvo. □

Iz Teorema 1.8 slijedi da svaki prirodan broj n možemo prikazati u obliku

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

gdje su $p_1, \ldots, p_r$ različiti prosti brojevi, a $\alpha_1, \ldots, \alpha_r$ prirodni brojevi. Ovakav prikaz broja n zvat ćemo *kanonski rastav* broja n na proste faktore.

Propozicija 1.9. *Ako je p prost broj i $p|ab$, onda $p|a$ ili $p|b$. Općenitije, ako $p|a_1 a_2 \cdots a_n$, onda p dijeli barem jedan faktor a_i.*

Dokaz: Ako $p \nmid a$, onda je $(p,a)=1$, pa postoje cijeli brojevi x i y takvi da je $ax+py=1$. Sada je $abx+pby=b$, pa p dijeli b.

Općenitiju tvrdnju dokazujemo indukcijom. Pretpostavimo da tvrdnja vrijedi za produkte s manje od n faktora. Sada ako $p|a_1(a_2\cdots a_n)$, onda $p|a_1$ ili $p|a_2a_3\cdots a_n$. Ako $p|a_2a_3\cdots a_n$, onda po induktivnoj pretpostavci $p|a_i$ za neki $i=2,\ldots,n$. □

Teorem 1.10 (Osnovni teorem aritmetike)**.** *Faktorizacija svakog prirodnog broja $n>1$ na proste faktore je jedinstvena do na poredak prostih faktora.*

Dokaz: Pretpostavimo da n ima dvije različite faktorizacije. Dijeleći s prostim brojevima koji su zajednički objema reprezentacijama, dobit ćemo jednakost oblika

$$p_1p_2\cdots p_r = q_1q_2\cdots q_s,$$

gdje su p_i, q_j prosti brojevi, ne nužno različiti, ali takvi da se niti jedan prost broj s lijeve strane ne pojavljuje na desnoj strani, tj. $p_i \neq q_j$ za sve i,j. Međutim, to je nemoguće jer iz $p_1|q_1q_2\cdots q_s$, po Propoziciji 1.9, slijedi pa p_1 dijeli barem jedan q_j. No, to znači da je $p_1=q_j$, kontradikcija. □

Napomena 1.1. U Poglavlju 8 ćemo vidjeti da analogon Teorema 1.10 ne vrijedi za cijele brojeve u (nekim) kvadratnim poljima. Za sada, kao primjer nejednoznačne faktorizacije na proste faktore u prstenu $\mathbb{Z}[\sqrt{-6}] = \{a+b\sqrt{-6} : a,b\in\mathbb{Z}\}$ navedimo ove dvije faktorizacije broja 10:

$$10 = 2\cdot 5 = (2+\sqrt{-6})(2-\sqrt{-6}).$$

U primjenama Teorema 1.10 često ćemo prirodan broj a pisati u obliku $a=\prod_p p^{\alpha(p)}$, gdje je $\alpha(p)\geq 0$ i podrazumijevamo da je $\alpha(p)=0$ za skoro sve proste brojeve p. Ako je $a=1$, onda je $\alpha(p)=0$ za sve p.

Ako je $a=\prod_p p^{\alpha(p)}$, $b=\prod_p p^{\beta(p)}$, $c=\prod_p p^{\gamma(p)}$ i $ab=c$, onda je po Teoremu 1.10, $\alpha(p)+\beta(p)=\gamma(p)$ za sve p. Dakle, ako $a|c$, onda je $\alpha(p)\leq\gamma(p)$. Obratno, ako je $\alpha(p)\leq\gamma(p)$, onda možemo definirati prirodan broj $b=\prod_p p^{\beta(p)}$ sa $\beta(p)=\gamma(p)-\alpha(p)$. Tada je $ab=c$, pa $a|c$. Prema tome, dobili smo da vrijedi

$$a|c \iff \alpha(p)\leq\gamma(p), \quad \forall p. \tag{1}$$

Kao posljedicu formule (1) dobivamo formulu

$$(a,b)=\prod_p p^{\min(\alpha(p),\beta(p))}. \tag{2}$$

Definicija 1.5. *Neka su $a_1,a_2,\ldots,a_n$ cijeli brojevi različiti od nule. Najmanji prirodan broj c za koji vrijedi da $a_i|c$ za sve $i=1,2,\ldots,n$ zove se* najmanji zajednički višekratnik *i označava s $[a_1,a_2,\ldots,a_n]$.*

Iz (1) slijedi da je

$$[a,b] = \prod_p p^{\max(\alpha(p),\beta(p))}. \tag{3}$$

Propozicija 1.11.

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

Dokaz: Po Teoremu 1.10 i formulama (2) i (3), dovoljno je provjeriti da za sve realne brojeve x, y vrijedi:

$$\min(x,y) + \max(x,y) = x + y.$$

Zaista, ako je $x \leq y$, onda je $\min(x,y) + \max(x,y) = x + y$, a ako je $x > y$, onda je $\min(x,y) + \max(x,y) = y + x = x + y$. □

Zadatak 1.4. *Odredite* $[482, 1687]$.

Reći ćemo da je prirodan broj *a (potpun) kvadrat* ako se može zapisati u obliku n^2, $n \in \mathbb{N}$. Iz Teorema 1.10 vidimo da je a potpun kvadrat ako i samo ako su svi eksponenti $\alpha(p)$ parni. Kažemo da je *a kvadratno slobodan* ako je 1 najveći kvadrat koji dijeli a. Stoga je a kvadratno slobodan ako i samo ako su svi eksponenti $\alpha(p)$ jednaki 0 ili 1. Konačno, ako je p prost, onda je $p^k \| a$ ekvivalentno s $k = \alpha(p)$.

Primjer 1.3. *Neka su a i b prirodni brojevi takvi da je* $(a,b) = 1$*, te da je ab potpun kvadrat. Dokazati da su tada a i b potpuni kvadrati.*

Rješenje: Neka je $a = \prod_p p^{\alpha(p)}$, $b = \prod_p p^{\beta(p)}$. Budući da je ab potpun kvadrat, broj $\alpha(p)+\beta(p)$ je paran za sve p. S druge strane, $(a,b) = 1$ povlači da je za sve p barem jedan od brojeva $\alpha(p)$, $\beta(p)$ jednak 0. No, to znači da su brojevi $\alpha(p)$ i $\beta(p)$ parni za sve p, pa su a i b potpuni kvadrati. ♢

Zadatak 1.5. *Nađite prirodan broj n sa svojstvom da je* $\frac{n}{2}$ *kvadrat,* $\frac{n}{3}$ *kub, a* $\frac{n}{5}$ *peta potencija nekog prirodnog broja.*

Primjer 1.4. *Dokazati da svaki složen broj n ima prosti faktor* $p \leq \sqrt{n}$.

Rješenje: Neka je p najmanji djelitelj od n koji je veći od 1. Tada je p očito prost i postoji $m \in \mathbb{N}$ takav da je $n = p \cdot m$. Budući da je $m \geq p$, dobivamo da je $p \leq \sqrt{n}$. ♢

Primjer 1.4 možemo iskoristiti za generiranje tablice prostih brojeva tzv. *Eratostenovim sitom*. Recimo, na primjer, da želimo napraviti tablicu prostih brojeva ≤ 200. Napišemo sve prirodne brojeve od 2 do 200. Prekrižimo sve prave višekratnike broja 2, pa broja 3, pa broja 5. U svakom koraku, prvi neprekriženi broj je prost, te u idućem koraku križamo njegove prave višekratnike (prvi novoprekriženi broj će biti njegov kvadrat, jer su svi manji višekratnici već ranije prekriženi). U našem slučaju, nakon križanja višekratnika od 7, 11 i 13, tablica je gotova (jer je $17 > \sqrt{200}$).

Teorem 1.12 (Euklid)**.** *Skup svih prostih brojeva je beskonačan.*

Dokaz: Pretpostavimo da su $p_1, p_2, \ldots, p_k$ svi prosti brojevi. Promotrimo broj

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

Uočimo da n nije djeljiv ni sa p_1, ni sa p_2, $\ldots$, ni sa p_k. Dakle, svaki prosti faktor p od n je različit od $p_1, \ldots, p_k$. Budući da je n ili prost ili ima prosti faktor, dobili smo prost broj različit od $p_1, \ldots, p_k$, što je kontradikcija. □

Primjer 1.5. *Dokazati da prostih brojeva oblika $4k+3$ ima beskonačno mnogo.*

Rješenje: Pri dijeljenju sa 4 neparni prosti broj može dati ostatak 1 ili 3. Produkt brojeva oblika $4k+1$ i sam ima taj oblik. Zaista,

$$(4s+1)(4t+1) = 4(4st+s+t)+1.$$

Neka su sada $p_1, p_2, \ldots, p_n$ svi prosti brojevi oblika $4k+3$. Promotrimo broj

$$4p_1 p_2 \cdots p_n - 1.$$

Ako bi svi njegovi prosti faktori bili oblika $4k+1$, onda bi i on sam imao taj oblik. Prema tome, on ima barem jedan prosti faktor p oblika $4k+3$. Očito je $p \neq p_i$, za $i = 1, 2, \ldots, n$, pa smo dobili kontradikciju. ♢

Primjer 1.6. *Dokazati da za svaki realan broj $y \geq 2$ vrijedi*

$$\sum_{p \leq y} \frac{1}{p} > \ln\ln y - 1.$$

Odavde neposredno slijedi da red $\sum_{p\ prost} \frac{1}{p}$ divergira, što daje novi dokaz da prostih brojeva ima beskonačno mnogo.

Rješenje: S $\mathcal{N}$ označimo skup svih prirodnih brojeva n koji su sastavljeni samo od prostih faktora p koji su $\leq y$ (uključujući i broj 1). Budući da imamo samo konačno mnogo prostih brojeva p koji su $\leq y$, a u apsolutno konvergentnom redu možemo permutirati članove, imamo

$$\prod_{p \leq y} \left(1 + \frac{1}{p} + \frac{1}{p^2} + \frac{1}{p^3} + \cdots\right) = \sum_{n \in \mathcal{N}} \frac{1}{n}\,. \tag{4}$$

Očito su svi prirodni brojevi koji su $\leq y$ elementi skupa $\mathcal{N}$. Neka je $N = \lfloor y \rfloor$, najveći cijeli broj $\leq y$. Usporedbom (gornje Darbouxove) sume i integrala, dobivamo

$$\sum_{n=1}^{N} \frac{1}{n} \geq \int_1^{N+1} \frac{dx}{x} = \ln(N+1) > \ln y.$$

Prema tome, iz (4) dobivamo

$$\prod_{p\le y}\left(1-\frac{1}{p}\right)^{-1} > \ln y. \tag{5}$$

Dokažimo sada da za sve realne brojeve v, takve da je $0 \le v \le \frac{1}{2}$, vrijedi

$$e^{v+v^2} \ge (1-v)^{-1}. \tag{6}$$

Zaista, neka je $f(v) = (1-v)e^{v+v^2}$. Tada je $f'(v) = -e^{v+v^2} + (1-v)(1+2v)e^{v+v^2} = v(1-2v)e^{v+v^2}$, što je ≥ 0 za $v \in [0, \frac{1}{2}]$. Stoga iz $f(0) = 1$ slijedi da je $f(v) \ge 1$ za $v \in [0, \frac{1}{2}]$.

Uvrstimo li (6) u (5), dobivamo

$$\prod_{p\le y} e^{\frac{1}{p}+\frac{1}{p^2}} > \ln y.$$

Logaritmirajući obje strane ove nejednakosti, dobivamo

$$\sum_{p\le y}\frac{1}{p} + \sum_{p\le y}\frac{1}{p^2} > \ln\ln y.$$

Očito je $\sum_{p\le y}\frac{1}{p^2} < \sum_{n=2}^{\infty}\frac{1}{n^2} < \int_1^{\infty}\frac{dx}{x^2} = 1$, pa je $\sum_{p\le y}\frac{1}{p} > \ln\ln y - 1$. ♢

Primjer 1.7. *Dokazati da za svaki prirodan broj n postoji n uzastopnih složenih brojeva.*

Rješenje: To su npr. brojevi

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

jer je $(n+1)!+j$ djeljivo sa j za $j = 2, 3, \ldots, n+1$. ♢

Primjer 1.8. *Dokazati da ne postoji polinom $f(x)$ s cjelobrojnim koeficijentima, stupnja ≥ 1, takav da je $f(n)$ prost za sve $n \in \mathbb{N}$.*

Rješenje: Neka je $f(1) = p$. Tada je p prost broj. Budući da je $f(1+kp) - f(1)$ djeljivo sa $(1+kp)-1 = kp$ (jer $x-y$ dijeli $x^m - y^m$), slijedi da $p|f(1+kp)$, za svaki $k \in \mathbb{N}$. Međutim, $f(1+kp)$ je prost, pa mora biti $f(1+kp) = p$, $\forall k \in \mathbb{N}$. Budući da polinom $f(x) - p$ ima beskonačno mnogo nultočaka, on mora biti nulpolinom, pa je $f(x) = p$, što je u suprotnosti s pretpostavkom da je $\operatorname{st} f \ge 1$. ♢

Puno teži problem je odrediti polinome $f(x)$ takve da je $f(n)$ prost za beskonačno mnogo prirodnih brojeva n. Zna se da to vrijedi za linearne polinome $f(x) = ax + b$ ako je $(a, b) = 1$ (Dirichletov teorem o prostim brojevima u aritmetičkom nizu). No, već za polinom $f(x) = x^2 + 1$, to je otvoreno pitanje. Hipoteza je da tvrdnja vrijedi za sve polinome koji su ireducibilni i za koje ne postoji prirodan broj $d > 1$ takav da $d|f(n)$, $\forall n \in \mathbb{N}$.

Primjer 1.9. *Neka je broj 2^k+1 prost. Dokazati da je tada $k=0$ ili $k=2^n$ za neki $n \geq 0$.*

Rješenje: Pretpostavimo da k ima neki neparan prosti faktor p. Tada iz $k = p \cdot m$ slijedi da je broj

$$2^k + 1 = (2^m)^p + 1^p = (2^m + 1)(2^{m(p-1)} - 2^{m(p-2)} + \cdots + 1)$$

djeljiv s $2^m + 1$, pa nije prost. ♢

Brojevi $f_n = 2^{2^n} + 1$ nazivaju se *Fermatovi brojevi*. Fermat je smatrao da su svi oni prosti. Zaista, $f_0 = 3$, $f_1 = 5$, $f_2 = 17$, $f_3 = 257$ i $f_4 = 65537$ su prosti. Međutim, $f_5 = 2^{32} + 1$ je složen. Pokažimo to!

$$\begin{aligned} 2^{32} + 1 &= 2^4 \cdot 2^{28} + 1 = (641 - 5^4) \cdot 2^{28} + 1 = 641 \cdot 2^{28} - (5 \cdot 2^7)^4 + 1 \\ &= 641 \cdot 2^{28} - (641 - 1)^4 + 1 \\ &= 641 \cdot (2^{28} - 641^3 + 4 \cdot 641^2 - 6 \cdot 641 + 4) \end{aligned}$$

Prema tome, $641 | f_5$.

Hipoteza je da je samo konačno mnogo Fermatovih brojeva prosto.

Zadatak 1.6. *Dokažite da za $m \neq n$ vrijedi $(f_m, f_n) = 1$. Pokažite da ova činjenica povlači da prostih brojeva ima beskonačno mnogo.*

Primjer 1.10. *Neka je broj $2^n - 1$ prost. Dokazati da je tada i broj n prost.*

Rješenje: Pretpostavimo da je broj n složen, tj. $n = ab$, $a > 1$, $b > 1$. Tada je broj $2^n - 1 = (2^a)^b - 1^b$ djeljiv s $2^a - 1$, pa nije prost. ♢

Brojevi $M_p = 2^p - 1$, gdje je p prost, zovu se *Mersennovi brojevi*. Neki Mersennovi brojevi su prosti, kao npr. $M_7 = 127$, a neki su složeni, kao npr. $M_{11} = 2047 = 23 \cdot 89$. Hipoteza je da Mersennovih brojeva koji su prosti ima beskonačno mnogo. Najveći poznati prosti Mersennov broj je $M_{32582657}$. To je ujedno i najveći danas poznati prosti broj (ima 9808358 znamenaka; otkrili su ga 2006. godine Cooper, Boone, Woltman i Kurowski).

2. Kongruencije

Teoriju kongruencija uveo je u svom djelu *Disquisitiones Arithmeticae* iz 1801. godine Carl Friedrich Gauss (1777-1855), jedan od najvećih matematičara svih vremena. On je također uveo i oznaku za kongruenciju koju i danas rabimo.

Definicija 2.1. *Ako cijeli broj $m \neq 0$ dijeli razliku $a-b$, onda kažemo da je a* kongruentan *b modulo m i pišemo $a \equiv b \pmod{m}$. U protivnom, kažemo da a nije kongruentan b modulo m i pišemo $a \not\equiv b \pmod{m}$.*

Budući da je $a - b$ djeljivo s m ako i samo ako je djeljivo s $-m$, bez smanjenja općenitosti možemo se usredotočiti na pozitivne module i kod nas će ubuduće modul m biti prirodan broj. Kongruencije imaju mnoga svojstva zajednička s jednakostima.

Propozicija 2.1. *Relacija "biti kongruentan modulo m" je relacija ekvivalencije na skupu $\mathbb{Z}$.*

Dokaz: Treba provjeriti refleksivnost, simetričnost i tranzitivnost.

(1) Iz $m|0$ slijedi $a \equiv a \pmod{m}$.

(2) Ako je $a \equiv b \pmod{m}$, onda postoji $k \in \mathbb{Z}$ takav $a - b = mk$. Sada je $b - a = m \cdot (-k)$, pa je $b \equiv a \pmod{m}$.

(3) Iz $a \equiv b \pmod{m}$ i $b \equiv c \pmod{m}$ slijedi da postoje $k, l \in \mathbb{Z}$ takvi da je $a - b = mk$ i $c - b = ml$. Zbrajanjem dobivamo $a - c = m(k + l)$, što povlači $a \equiv c \pmod{m}$. □

Još neka od jednostavnih svojstava kongruencija dana su u sljedećoj propoziciji.

Propozicija 2.2. *Neka su a, b, c, d cijeli brojevi.*

(1) Ako je $a \equiv b \pmod{m}$ i $c \equiv d \pmod{m}$, onda je $a + c \equiv b + d \pmod{m}$, $a - c \equiv b - d \pmod{m}$, $ac \equiv bd \pmod{m}$.

(2) Ako je $a \equiv b \pmod{m}$ i $d|m$, onda je $a \equiv b \pmod{d}$.

(3) Ako je $a \equiv b \pmod{m}$, onda je $ac \equiv bc \pmod{mc}$ za svaki $c \neq 0$.

Dokaz: (1) Neka je $a - b = mk$ i $c - d = ml$. Tada je $(a + c) - (b + d) = m(k + l)$ i $(a - c) - (b - d) = m(k - l)$, pa je $a + c \equiv b + d \pmod{m}$ i $a - c \equiv b - d \pmod{m}$. Zbog $ac - bd = a(c - d) + d(a - b) = m(al + dk)$ slijedi da je $ac \equiv bd \pmod{m}$.

(2) Neka je $m = de$. Tada iz $a - b = mk$ slijedi $a - b = d \cdot (ek)$, pa je $a \equiv b \pmod{d}$.

(3) Iz $a - b = mk$ slijedi $ac - bc = (mc) \cdot k$, pa je $ac \equiv bc \pmod{mc}$. □

Propozicija 2.3. *Neka je f polinom s cjelobrojnim koeficijentima. Ako je $a \equiv b \pmod{m}$, onda je $f(a) \equiv f(b) \pmod{m}$.*

Dokaz: Neka je $f(x) = c_n x^n + c_{n-1}x^{n-1} + \cdots + c_0$, gdje su $c_i \in \mathbb{Z}$. Budući da je $a \equiv b \pmod{m}$, uzastopnom primjenom Propozicije 2.2.1) dobivamo: $a^2 \equiv b^2 \pmod{m}$, $a^3 \equiv b^3 \pmod{m}$, $\ldots$, $a^n \equiv b^n \pmod{m}$. Tada je $c_i a^i \equiv c_i b^i \pmod{m}$ i konačno:

$$c_n a^n + c_{n-1}a^{n-1} + \cdots + c_0 \equiv c_n b^n + c_{n-1}b^{n-1} + \cdots + c_0 \pmod{m}.$$

□

Teorem 2.4. *Vrijedi: $ax \equiv ay \pmod{m}$ ako i samo ako $x \equiv y \pmod{\frac{m}{(a,m)}}$. Specijalno, ako je $ax \equiv ay \pmod{m}$ i $(a,m) = 1$, onda je $x \equiv y \pmod{m}$.*

Dokaz: Ako je $ax \equiv ay \pmod{m}$, onda postoji $z \in \mathbb{Z}$ takav da je $ay - ax = mz$. Sada imamo: $\frac{a}{(a,m)}(y-x) = \frac{m}{(a,m)}z$, tj. $\frac{m}{(a,m)}$ dijeli $\frac{a}{(a,m)}(y-x)$. No, brojevi $\frac{a}{(a,m)}$ i $\frac{m}{(a,m)}$ su relativno prosti, pa zaključujemo da $\frac{m}{(a,m)}$ dijeli $y - x$, tj. da je $x \equiv y \pmod{\frac{m}{(a,m)}}$.

Obrnuto, ako je $x \equiv y \pmod{\frac{m}{(a,m)}}$, onda po Propoziciji 2.2.3) dobivamo $ax \equiv ay \pmod{\frac{am}{(a,m)}}$. No, (a,m) je djelitelj od a, pa po Propoziciji 2.2.2) dobivamo $ax \equiv ay \pmod{m}$. □

Definicija 2.2. *Skup $\{x_1, \cdots, x_m\}$ se zove* potpuni sustav ostataka *modulo m ako za svaki $y \in \mathbb{Z}$ postoji točno jedan x_j takav da je $y \equiv x_j \pmod{m}$. Drugim riječima, potpuni sustav ostataka dobivamo tako da iz svake klase ekvivalencije modulo m uzmemo po jedan član.*

Očito je da postoji beskonačno mnogo potpunih sustava ostataka modulo m. Jedan od njih je tzv. sustav najmanjih nenegativnih ostataka:

$$\{0, 1, \ldots, m-1\}.$$

Pored njega, često se koristi i sustav apsolutno najmanjih ostataka. Ako je m neparan broj, apsolutno najmanji ostatci su

$$-\frac{m-1}{2}, -\frac{m-3}{2}, \ldots, -1, 0, 1, \ldots, \frac{m-3}{2}, \frac{m-1}{2},$$

a ako je m paran, onda su to

$$-\frac{m-2}{2}, -\frac{m-4}{2}, \ldots, -1, 0, 1, \ldots, \frac{m-2}{2}, \frac{m}{2}.$$

Teorem 2.5. *Neka je $\{x_1, \ldots, x_m\}$ potpuni sustav ostataka modulo m, te neka je $(a,m) = 1$. Tada je $\{ax_1, \ldots, ax_m\}$ također potpuni sustav ostataka modulo m.*

Dokaz: Dovoljno je dokazati da je $ax_i \not\equiv ax_j \pmod{m}$ za $i \neq j$. Pretpostavimo da je $ax_i \equiv ax_j \pmod{m}$. Tada Teorem 2.4 povlači da je $x_i \equiv x_j \pmod{m}$, tj. $i = j$. □

Neka je $f(x)$ polinom s cjelobrojnim koeficijentima. Rješenje kongruencije $f(x) \equiv 0 \pmod{m}$ je svaki cijeli broj x koji je zadovoljava. Ako je x_1 neko rješenje ove kongruencije, a $x_2 \equiv x_1 \pmod{m}$, onda je, po Propoziciji 2.3, x_2 također rješenje. Dva rješenja x i x' smatramo ekvivalentnim ako je $x \equiv x' \pmod{m}$. Broj rješenja kongruencije je broj neekvivalentnih rješenja.

Teorem 2.6. *Neka su a i m prirodni, te b cijeli broj. Kongruencija $ax \equiv b \pmod{m}$ ima rješenja ako i samo ako $d = (a, m)$ dijeli b. Ako je ovaj uvjet zadovoljen, onda gornja kongruencija ima točno d rješenja modulo m.*

Dokaz: Ako kongruencija $ax \equiv b \pmod{m}$ ima rješenja, onda postoji $y \in \mathbb{Z}$ tako da je $ax - my = b$. Odavde je očito da $(a, m)|b$. Pretpostavimo sada da $d = (a, m)$ dijeli b. Stavimo $a' = \frac{a}{d}$, $b' = \frac{b}{d}$, $m' = \frac{m}{d}$. Sada trebamo riješiti kongruenciju $a'x \equiv b' \pmod{m'}$. No, ona ima točno jedno rješenje modulo m'. Zaista, budući da je $(a', m') = 1$, po Teoremu 2.5, kad x prolazi potpunim sustavom ostataka modulo m' i $a'x$ prolazi tim istim sustavom, tj. svaki ostatak modulo m' (pa tako i b') se dobiva točno za jedan x iz potpunog sustava ostataka modulo m'.

Jasno je da ako je x' neko rješenje od $a'x' \equiv b' \pmod{m'}$, onda su sva rješenja od $ax \equiv b \pmod{m}$ u cijelim brojevima dana sa $x = x' + nm'$, za $n \in \mathbb{Z}$, a sva međusobno neekvivalentna rješenja sa $x = x' + nm'$, gdje je $n = 0, 1, \ldots, d-1$. Dakle, ako d dijeli b, onda kongruencija $ax \equiv b \pmod{m}$ ima točno d rješenja modulo m. □

Iz Teorema 2.6 slijedi da ako je p prost broj i a nije djeljiv s p, onda kongruencija $ax \equiv b \pmod{p}$ uvijek ima rješenje i to rješenje je jedinstveno. Ovo pak povlači da skup ostataka $\{0, 1, \ldots, p-1\}$ pri dijeljenju sa p, uz zbrajanje i množenje $\pmod{p}$, čini polje. To polje se obično označava sa $\mathbb{Z}_p$ ili $\mathbb{F}_p$.

Postavlja se pitanje kako riješiti kongruenciju $a'x \equiv b' \pmod{m'}$, gdje je $(a', m') = 1$. Budući da je $(a', m') = 1$, to postoje brojevi $u, v \in \mathbb{Z}$ takvi da je $a'u + m'v = 1$ i u, v se mogu naći pomoću Euklidovog algoritma. Sada je $a'u \equiv 1 \pmod{m'}$, pa je $x \equiv ub' \pmod{m'}$.

Primjer 2.1. *Riješimo kongruenciju* $555x \equiv 15 \pmod{5005}$.

Rješenje: Budući da je $(555, 5005) = 5$ i $5|15$, treba riješiti kongruenciju

$$111x \equiv 3 \pmod{1001}.$$

Primijenimo Euklidov algoritam:

$$\begin{aligned} 1001 &= 111 \cdot 9 + 2 \\ 111 &= 2 \cdot 55 + 1 \\ 2 &= 1 \cdot 2 \end{aligned}$$

i	-1	0	1	2
q_i			9	55
y_i	0	1	-9	496

Dakle, rješenje kongruncije $111u \equiv 1 \pmod{1001}$ je $u \equiv 496 \pmod{1001}$. Stoga je rješenje od $111x \equiv 3 \pmod{1001}$, $x \equiv 1488 \equiv 487 \pmod{1001}$. Konačno, rješenje polazne kongruencije je

$$x \equiv 487, 1488, 2489, 3490, 4491 \pmod{5005}.$$

♢

Zadatak 2.1. *Riješite kongruencije*

a) $589x \equiv 209 \pmod{817}$, *b)* $49x \equiv 5000 \pmod{999}$.

Teorem 2.7 (Kineski teorem o ostatcima)**.** *Neka su $m_1, m_2, \ldots, m_r$ u parovima relativno prosti prirodni brojevi, te neka su $a_1, a_2, \ldots, a_r$ cijeli brojevi. Tada sustav kongruencija*

$$x \equiv a_1 \pmod{m_1}, \quad x \equiv a_2 \pmod{m_2}, \quad \ldots, \quad x \equiv a_r \pmod{m_r} \quad (7)$$

ima rješenja. Ako je x_0 jedno rješenje, onda su sva rješenja od (7) dana sa $x \equiv x_0 \pmod{m_1 m_2 \cdots m_r}$.

Dokaz: Neka je $m = m_1 m_2 \cdots m_r$, te neka je $n_j = \frac{m}{m_j}$ za $j = 1, \ldots, r$. Tada je $(m_j, n_j) = 1$, pa postoji cijeli broj x_j takav da je $n_j x_j \equiv a_j \pmod{m_j}$. Promotrimo broj

$$x_0 = n_1 x_1 + \cdots + n_r x_r.$$

Za njega vrijedi: $x_0 \equiv 0 + \cdots + 0 + n_j x_j + 0 + \cdots + 0 \equiv a_j \pmod{m_j}$. Prema tome, x_0 je rješenje od (7).

Ako su sada x, y dva rješenja od (7), onda je $x \equiv y \pmod{m_j}$ za $j = 1, \ldots, r$, pa jer su m_j u parovima relativno prosti, dobivamo da je $x \equiv y \pmod{m}$. □

Primjer 2.2. *Riješimo sustav:*

$$x \equiv 2 \pmod{5}, \quad x \equiv 3 \pmod{7}, \quad x \equiv 4 \pmod{11}.$$

Rješenje: Uz oznake iz Teorema 2.7 imamo da je $x_0 = 77x_1+55x_2+35x_3$, gdje x_1, x_2, x_3 zadovoljavaju

$$77x_1 \equiv 2 \pmod 5, \quad 55x_2 \equiv 3 \pmod 7, \quad 35x_3 \equiv 4 \pmod{11},$$

odnosno

$$2x_1 \equiv 2 \pmod 5, \quad 6x_2 \equiv 3 \pmod 7, \quad 2x_3 \equiv 4 \pmod{11}.$$

Stoga možemo uzeti $x_1 = 1$, $x_2 = 4$, $x_3 = 2$, što daje $x_0 = 367$. Prema tome, sva rješenja našeg sustava dana su sa $x \equiv 367 \pmod{385}$. ♢

Zadatak 2.2. *Riješite sustav kongruencija*

$$x \equiv 5 \pmod 7, \quad x \equiv 7 \pmod{11}, \quad x \equiv 3 \pmod{13}.$$

Primjer 2.3. *Riješimo sustav kongruencija*

$$x \equiv 3 \pmod{10}, \quad x \equiv 8 \pmod{15}, \quad x \equiv 5 \pmod{84}.$$

Rješenje: Uočimo da brojevi 10, 15 i 84 nisu u parovima relativno prosti, pa ne možemo Kineski teorem o ostatcima primjeniti direktno, a može se dogoditi da takav sustav uopće nema rješenja. Sada postupamo ovako. Naš sustav je ekvivalentan sa

$$x \equiv 3 \pmod 2, \quad x \equiv 3 \pmod 5, \quad x \equiv 8 \pmod 3, \quad x \equiv 8 \pmod 5,$$

$$x \equiv 5 \pmod 4, \quad x \equiv 5 \pmod 3, \quad x \equiv 5 \pmod 7.$$

Dakle, moduli su nam potencije prostih brojeva i sada usporedimo kongruencije koje odgovaraju istom prostom broju:

$$\begin{aligned} x \equiv 3 \pmod 2, \quad x \equiv 5 \pmod 4 &\iff x \equiv 1 \pmod 4, \\ x \equiv 8 \pmod 3, \quad x \equiv 5 \pmod 3 &\iff x \equiv 2 \pmod 3, \\ x \equiv 3 \pmod 5, \quad x \equiv 8 \pmod 5 &\iff x \equiv 3 \pmod 5, \\ x \equiv 5 \pmod 7. & \end{aligned}$$

Prema tome, naš sustav je ekvivalentan sa sustavom

$$x \equiv 1 \pmod 4, \quad x \equiv 2 \pmod 3, \quad x \equiv 3 \pmod 5, \quad x \equiv 5 \pmod 7$$

na kojeg možemo doslovno primijeniti Kineski teorem o ostatcima. Imamo: $m = 4 \cdot 3 \cdot 5 \cdot 7 = 420$, $n_1 = 105$, $n_2 = 140$, $n_3 = 84$, $n_4 = 60$,

$$\begin{aligned} 105x_1 \equiv 1 \pmod 4 &\iff x_1 \equiv 1 \pmod 4 &&\implies x_1 = 1, \\ 140x_2 \equiv 2 \pmod 3 &\iff 2x_1 \equiv 2 \pmod 3 &&\implies x_2 = 1, \\ 84x_3 \equiv 3 \pmod 5 &\iff 4x_3 \equiv 3 \pmod 5 &&\implies x_3 = 2, \\ 60x_4 \equiv 5 \pmod 7 &\iff 4x_4 \equiv 5 \pmod 7 &&\implies x_4 = 3. \end{aligned}$$

Dakle, rješenje je

$$x \equiv 105 \cdot 1 + 140 \cdot 1 + 84 \cdot 2 + 60 \cdot 3 = 593 \equiv 173 \pmod{420}.$$

♢

Definicija 2.3. Reducirani sustav ostataka *modulo m je skup cijelih brojeva* r_i *sa svojstvom da je* $(r_i, m) = 1$, $r_i \not\equiv r_j \pmod m$ *za* $i \neq j$, *te da za svaki cijeli broj* x *takav da je* $(x, m) = 1$ *postoji* r_i *takav da je* $x \equiv r_i \pmod m$. *Jedan reducirani sustav ostataka modulo m je skup svih brojeva* $a \in \{1, 2, \ldots, m\}$ *takvih da je* $(a, m) = 1$. *Jasno je da svi reducirani sustavi ostataka modulo m imaju isti broj elemenata. Taj broj označavamo s* $\varphi(m)$, *a funkciju* φ *zovemo* Eulerova funkcija. *Drugim riječima,* $\varphi(m)$ *je broj brojeva u nizu* $1, 2, \ldots, m$ *koji su relativno prosti sa* m.

Teorem 2.8. *Neka je* $\{r_1, \ldots, r_{\varphi(m)}\}$ *reducirani sustav ostataka modulo* m, *te neka je* $(a, m) = 1$. *Tada je* $\{ar_1, \ldots, ar_{\varphi(m)}\}$ *također reducirani sustav ostataka modulo* m.

Dokaz: Direktno iz Teorema 1.3 i 2.5. □

Primjer 2.4. *Neka su* a *i* n *relativno prosti prirodni brojevi. Izračunajmo sumu* $\sum_{\substack{1 \le x \le n \\ (x,n)=1}} \left\{\frac{ax}{n}\right\}$. *Ovdje je* $\{z\} = z - \lfloor z \rfloor$ *razlomljeni dio od* z, *dok* x *prolazi skupom svih reduciranih ostataka modulo* n.

Rješenje: Budući da je $(a, n) = 1$, brojevi ax također prolaze skupom svih reduciranih ostataka modulo n. Stoga je

$$\sum_{\substack{1 \le x \le n \\ (x,n)=1}} \left\{\frac{ax}{n}\right\} = \sum_{\substack{1 \le y \le n \\ (y,n)=1}} \left\{\frac{y}{n}\right\} = \frac{1}{n} \sum_{\substack{1 \le y \le n \\ (y,n)=1}} y.$$

Kako je $(y, n) = 1 \iff (n - y, n) = 1$, dalje imamo

$$2 \sum_{\substack{1 \le y \le n \\ (y,n)=1}} y = \sum_{\substack{1 \le y \le n \\ (y,n)=1}} y + \sum_{\substack{1 \le y \le n \\ (n-y,n)=1}} y = \sum_{\substack{1 \le y \le n \\ (y,n)=1}} y + \sum_{\substack{1 \le y \le n \\ (y,n)=1}} (n - y)$$
$$= \sum_{\substack{1 \le y \le n \\ (y,n)=1}} n = n\varphi(n).$$

Stoga je tražena suma jednaka $\frac{1}{2}\varphi(n)$. ♢

Teorem 2.9 (Eulerov teorem)**.** *Ako je* $(a, m) = 1$, *onda je* $a^{\varphi(m)} \equiv 1 \pmod m$.

Dokaz: Neka je $\{r_1, r_2, \ldots, r_{\varphi(m)}\}$ reducirani sustav ostataka modulo m. Budući da je, po Teoremu 2.8, $\{ar_1, ar_2, \ldots, ar_{\varphi(m)}\}$ također reducirani sustav ostataka modulo m, zaključujemo da je

$$\prod_{j=1}^{\varphi(m)} (ar_j) \equiv \prod_{i=1}^{\varphi(m)} r_i \pmod{m},$$

odnosno,

$$a^{\varphi(m)} \prod_{j=1}^{\varphi(m)} r_j \equiv \prod_{i=1}^{\varphi(m)} r_i \pmod{m}.$$

Kako je $(r_i, m) = 1$, primjenom Teorema 2.4, dobivamo $a^{\varphi(m)} \equiv 1 \pmod{m}$. □

Teorem 2.10 (Mali Fermatov teorem)**.** *Neka je p prost broj. Ako $p \nmid a$, onda je $a^{p-1} \equiv 1 \pmod{p}$. Za svaki cijeli broj a vrijedi $a^p \equiv a \pmod{p}$.*

Dokaz: Očito je $\varphi(p) = p - 1$, pa tvrdnja teorema slijedi iz Teorema 2.9. □

Primjer 2.5. *Odredimo zadnje dvije znamenke u decimalnom zapisu broja 3^{400}.*

Rješenje: Budući da je $\varphi(25) = 20$, imamo $3^{20} \equiv 1 \pmod{25}$, pa je $3^{400} \equiv 1 \pmod{25}$. Također je $3^2 \equiv 1 \pmod{4}$, pa je $3^{400} \equiv 1 \pmod{4}$. Dakle, $3^{400} \equiv 1 \pmod{100}$, pa su zadnje dvije znamenke 01. ♢

Zadatak 2.3. *Odredite zadnje dvije znamenke broja 2^{1000}.*

Definicija 2.4. *Funkciju $\vartheta : \mathbb{N} \to \mathbb{C}$ za koju vrijedi*
1) $\vartheta(1) = 1$,
2) $\vartheta(mn) = \vartheta(m)\vartheta(n)$ za sve m, n takve da je $(m, n) = 1$,
zovemo multiplikativna funkcija.

Teorem 2.11. *Eulerova funkcija φ je multiplikativna. Nadalje, za svaki prirodan broj $n > 1$ vrijedi $\varphi(n) = n \prod_{p|n}(1 - \frac{1}{p})$.*

Dokaz: Neka su m, n relativno prosti prirodni brojevi, te neka a i b prolaze skupom svih reduciranih ostataka modulo m, odnosno modulo n. Naš je cilj pokazati da tada $an + bm$ prolazi skupom svih reduciranih ostataka modulo mn. Ako to pokažemo, dobit ćemo da je $\varphi(m)\varphi(n) = \varphi(mn)$.

Budući da je $(a, m) = 1$ i $(b, n) = 1$, broj $an + bm$ je relativno prost s m i s n, pa stoga i s mn. Nadalje, svaka dva broja gornjeg oblika su međusobno nekongruentni modulo mn. Zaista, iz $an + bm \equiv a'n + b'm \pmod{mn}$ slijedi $(a - a')n \equiv (b' - b)m \pmod{mn}$. Odavde $m|a - a'$, $n|b' - b$, pa je $a = a'$, $b = b'$. Stoga nam još preostaje pokazati da ako je $(c, mn) = 1$, onda je

$c \equiv an + bm \pmod{mn}$ za neke a, b. Budući je $(m, n) = 1$, postoje cijeli brojevi x, y takvi da je $mx + ny = 1$. Očito je $(cy, m) = 1$, $(cx, n) = 1$, pa brojevi a i b definirani sa $cy \equiv a \pmod{m}$, $cx \equiv b \pmod{n}$ imaju tražena svojstva.

Neka je sada $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$. Jedini brojevi u nizu $1, 2, \ldots, p_i^{\alpha_i}$ koji nisu relativno prosti s $p_i^{\alpha_i}$ su brojevi $p_i, 2p_i, \ldots, p_i^{\alpha_i - 1} \cdot p_i$. Stoga je $\varphi(p_i^{\alpha_i}) = p_i^{\alpha_i} - p_i^{\alpha_i - 1}$. Zbog multiplikativnosti od φ, imamo

$$\begin{aligned}\varphi(n) &= \varphi(\prod_{i=1}^{k} p_i^{\alpha_i}) = \prod_{i=1}^{k} \varphi(p_i^{\alpha_i}) = \prod_{i=1}^{k} p_i^{\alpha_i} \left(1 - \frac{1}{p_i}\right) \\ &= n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right) = n \prod_{p|n} \left(1 - \frac{1}{p}\right).\end{aligned}$$

□

Zadatak 2.4. *Za koje prirodne brojeve n je broj $\varphi(n)$ neparan?*

Primjer 2.6. *Odredimo sve prirodne brojeve n za koje vrijedi $\varphi(n) = 12$.*

Rješenje: Ako je $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, onda je

$$\varphi(n) = p_1^{\alpha_1 - 1}(p_1 - 1) \cdots p_r^{\alpha_r - 1}(p_r - 1).$$

Iz $(p_i - 1) | 12$ slijedi $p_i \in \{2, 3, 5, 7, 13\}$. Ako je $p_i = 2$, onda je $\alpha_i \leq 3$; ako je $p_i = 3$, onda je $\alpha_i \leq 2$; a ako je $p_i \neq 2, 3$, onda je $\alpha_i = 1$. Imamo četiri mogućnosti (s k označavamo broj oblika $2^{\alpha} 3^{\beta}$):

1) $n = 13 \cdot k \implies \varphi(n) = 12 \cdot \varphi(k) = 12$
$\varphi(k) = 1 \implies k = 1$ ili $k = 2 \implies n = 13$ ili $n = 26$;
2) $n = 7 \cdot k \implies \varphi(n) = 6 \cdot \varphi(k) = 12$
$\varphi(k) = 2 \implies k = 3$, $k = 4$ ili $k = 6 \implies n = 21$, $n = 28$ ili $n = 42$;
3) $n = 5 \cdot k \implies \varphi(n) = 4 \cdot \varphi(k) = 12$
$\varphi(k) = 3$, što nema rješenja;
4) $n = k \implies \varphi(n) = 2^{\alpha - 1} 3^{\beta - 1} \cdot 2 = 12$
$\alpha = 2$, $\beta = 2 \implies n = 36$.

Rješenja su: $n = 13, 21, 26, 28, 36, 42$. ♢

Teorem 2.12.

$$\sum_{d|n} \varphi(d) = n$$

Dokaz: Neka je $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$. Zbog multiplikativnosti od φ, imamo:

$$\sum_{d|n} \varphi(d) = \prod_{i=1}^{k} (1 + \varphi(p_i) + \varphi(p_i^2) + \cdots + \varphi(p_i^{\alpha_i})). \tag{8}$$

Naime, množenjem faktora na desnoj strani od (8) dobivamo sumu faktora oblika $\varphi(p_1^{\beta_1})\cdots\varphi(p_k^{\beta_k}) = \varphi(p_1^{\beta_1}\cdots p_k^{\beta_k})$, gdje je $0 \le \beta_i \le \alpha_i$, $i = 1, \ldots, k$, a to je upravo lijeva strana od (8).

Sada je

$$\sum_{d|n}\varphi(d) = \prod_{i=1}^{k}\left(1 + (p_i - 1) + (p_i^2 - p_i) + \cdots + (p_i^{\alpha_i} - p_i^{\alpha_i - 1})\right) = \prod_{i=1}^{k} p_i^{\alpha_i} = n.$$

□

Teorem 2.13 (Wilson)**.** *Ako je p prost broj, onda je* $(p-1)! \equiv -1 \pmod{p}$.

Dokaz: Za $p = 2$ i $p = 3$ kongruencija je očito zadovoljena. Stoga smijemo pretpostaviti da je $p \ge 5$. Grupirajmo članove skupa $\{2, 3, \ldots, p-2\}$ u parove (i, j) sa svojstvom $i \cdot j \equiv 1 \pmod{p}$. Očito je $i \ne j$ jer bi inače broj $(i-1)(i+1)$ bio djeljiv sa p, a to je nemoguće zbog $0 < i - 1 < i + 1 < p$. Tako dobivamo $\frac{p-3}{2}$ parova i ako pomnožimo odgovarajućih $\frac{p-3}{2}$ kongruencija, dobit ćemo

$$2 \cdot 3 \cdots (p-2) \equiv 1 \pmod{p},$$

pa je

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

□

Očito je da vrijedi i obrat Wilsonovog teorema. Zaista, neka vrijedi

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

i pretpostavimo da p nije prost. Tada p ima djelitelj d, $1 < d < p$, i d dijeli $(p-1)!$. No, tada d mora dijeliti i -1, što je kontradikcija.

Primjer 2.7. *Neka je p prost broj. Dokažimo da je $(p-1)! + 1$ potencija od p ako i samo ako je $p = 2$, 3 ili 5.*

Rješenje: Najprije imamo:

$$(2-1)! + 1 = 2^1, \quad (3-1)! + 1 = 3^1, \quad (5-1)! + 1 = 5^2.$$

Ako je $p > 5$, onda se u $(p-1)!$ pojavljuju faktori 2, $p-1$ i $\frac{p-1}{2}$, pa $(p-1)^2 | (p-1)!$. Ako bi bilo

$$\begin{aligned}(p-1)! + 1 &= p^k = [(p-1) + 1]^k \\ &= (p-1)^k + k(p-1)^{k-1} + \cdots + \binom{k}{2}(p-1)^2 + k(p-1) + 1,\end{aligned}$$

onda bi imali da $(p-1) | k$. To bi povlačilo da je $k \ge p - 1$, te $(p-1)! + 1 < (p-1)^{p-1} + 1 < p^{p-1} \le p^k$, što je kontradikcija. ♢

Teorem 2.14. *Neka je p prost broj. Tada kongruencija $x^2 \equiv -1 \pmod{p}$ ima rješenja ako i samo ako je $p = 2$ ili $p \equiv 1 \pmod{4}$.*

Dokaz: Ako je $p = 2$, onda je $x = 1$ jedno rješenje.
Ako je $p \equiv 1 \pmod{4}$, onda iz Wilsonovog teorema imamo:

$$[1 \cdot 2 \cdots \frac{p-1}{2}] \cdot [(p-1)(p-2)\cdots(p-\frac{p-1}{2})] \equiv [(\frac{p-1}{2})!]^2 \equiv -1 \pmod{p},$$

pa je $x = (\frac{p-1}{2})!$ jedno rješenje.

Neka je $p \equiv 3 \pmod{4}$. Pretpostavimo da postoji $x \in \mathbb{Z}$ takav da je $x^2 \equiv -1 \pmod{p}$. Tada je $x^{p-1} \equiv (-1)^{\frac{p-1}{2}} \equiv -1 \pmod{p}$, što je u suprotnosti s Malim Fermatovim teoremom. □

Primjer 2.8. *Dokažimo da postoji beskonačno mnogo prostih brojeva oblika $4k + 1$.*

Rješenje: Neka su $p_1, p_2, \ldots, p_n$ svi prosti brojevi oblika $4k+1$. Promotrimo broj

$$m = 4p_1^2 p_2^2 \cdots p_n^2 + 1.$$

Neka je p neki prosti faktor od m. Tada kongruencija $x^2 \equiv -1 \pmod{p}$ ima rješenje $x = 2p_1 p_2 \cdots p_n$, pa p mora biti oblika $4k + 1$. Očito je $p \neq p_i$, $i = 1, 2, \ldots, n$, pa smo dobili kontradikciju. □

Teorem 2.15 (Lagrange)**.** *Neka je $f(x)$ polinom s cjelobrojnim koeficijentima stupnja n. Pretpostavimo da je p prost broj, te da vodeći koeficijent od f nije djeljiv s p. Tada kongruencija $f(x) \equiv 0 \pmod{p}$ ima najviše n rješenja modulo p.*

Dokaz: Za $n = 1$ tvrdnja teorema vrijedi po Teoremu 2.6. Pretpostavimo da tvrdnja vrijedi za sve polinome stupnja $n-1$, te neka je f polinom stupnja n. Za svaki $a \in \mathbb{Z}$ imamo $f(x) - f(a) = (x-a)g(x)$, gdje je g polinom stupnja $n-1$ s cjelobrojnim koeficijentima i s istim vodećim koeficijentom kao f. Zato ako kongruencija $f(x) \equiv 0 \pmod{p}$ ima rješenje $x = a$, onda sva rješenja ove kongruencije zadovoljavaju $(x-a)g(x) \equiv 0 \pmod{p}$. No, po induktivnoj prepostavci kongruencija $g(x) \equiv 0 \pmod{p}$ ima najviše $n-1$ rješenja, pa kongruencija $f(x) \equiv 0 \pmod{p}$ ima najviše n rješenja. □

Primjer 2.9 (Wolstenholme)**.** *Neka je $p \geq 5$ prost broj. Dokažimo da je brojnik racionalnog broja*

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

djeljiv s p^2.

Rješenje:
Promotrimo polinom

$$f(x) = x^{p-1} - 1 - (x-1)(x-2)\cdots(x-p+1).$$

Kongruencija $f(x) \equiv 0 \pmod{p}$ ima $p-1$ rješenja: $1, 2, \ldots, p-1$. Stupanj od $f(x)$ je $\leq p-2$. Neka je $f(x) = a_{p-2}x^{p-2} + \cdots + a_1 x + a_0$. Ako je n najveći cijeli broj takav da je $a_n \not\equiv 0 \pmod{p}$, onda po Lagrangeovom eoremu kongruencija $f(x) \equiv 0 \pmod{p}$ ima najviše $n \leq p-2$ rješenja. Dakle, $a_n \equiv 0 \pmod{p}$ za $n = 0, 1, \ldots, p-2$. Budući da je $a_0 = -1-(p-1)!$, ovo nam daje drugi dokaz Wilsonovog teorema.

Sada je

$$f(p) = p^{p-1} - 1 - (p-1)! = a_{p-2}p^{p-2} + \cdots + a_2 p^2 + a_1 p + a_0,$$

a zbog $a_0 = -1 - (p-1)!$ slijedi

$$p^{p-2} - a_{p-2}p^{p-3} - \cdots - a_2 p - a_1 = 0.$$

Budući da $p|a_2$, zaključujemo da $p^2|a_1$. No,

$$\frac{a_1}{(p-1)!} = 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p-1}.$$

♢

Neka sada $d|p-1$. Tvrdimo da tada polinom $x^d - 1$ ima točno d nultočaka u $\mathbb{Z}_p$. Zaista, $x^{p-1} - 1 = (x^d - 1)g(x)$, gdje je g polinom stupnja $p-1-d$. No, po Malom Fermatovom teoremu, $x^{p-1} - 1$ ima $p-1$ nultočaka u $\mathbb{Z}_p$, pa $x^d - 1$ ima barem $(p-1) - (p-1-d) = d$ nultočaka u $\mathbb{Z}_p$.

Teorem 2.16 (Henselova lema)**.** *Neka je $f(x)$ polinom s cjelobrojnim koeficijentima. Ako je $f(a) \equiv 0 \pmod{p^j}$ i $f'(a) \not\equiv 0 \pmod{p}$, onda postoji jedinstveni $t \in \{0, 1, 2, \ldots, p-1\}$ takav da je $f(a + tp^j) \equiv 0 \pmod{p^{j+1}}$.*

Dokaz: Koristimo Taylorov razvoj polinoma f oko a:

$$f(a + tp^j) = f(a) + tp^j f'(a) + t^2 p^{2j} \frac{f''(a)}{2!} + \cdots + t^n p^{nj} \frac{f^{(n)}(a)}{n!}. \quad (9)$$

Pokažimo da su brojevi $\frac{f^{(k)}(a)}{k!}$ cijeli. Ovu je tvrdnju dovoljno dokazati za polinome oblika $g(x) = x^m$, gdje je $m \geq k$. No, tada je

$$\frac{g^{(k)}(a)}{k!} = \frac{m(m-1)\cdots(m-k+1)a^{m-k}}{k!} = \binom{m}{k} a^{m-k} \in \mathbb{Z}.$$

Zato iz (9) dobivamo

$$f(a + tp^j) \equiv f(a) + tp^j f'(a) \pmod{p^{j+1}}.$$

Dakle, da bi bilo $f(a+tp^j) \equiv 0 \pmod{p^{j+1}}$, nužno je i dovoljno da bude

$$tf'(a) \equiv -\frac{f(a)}{p^j} \pmod{p}. \tag{10}$$

Budući da je $f'(a) \not\equiv 0 \pmod{p}$, kongruencija (10) ima, po Teoremu 2.6, točno jedno rješenje. □

Propozicija 2.17. *Kongruencija $x^{p-1} - 1 \equiv 0 \pmod{p^j}$ ima točno $p-1$ rješenja za svaki prost broj p i prirodan broj j.*

Dokaz: Za $j = 1$ tvrdnja vrijedi po Malom Fermatovom teoremu. Pretpostavimo da tvrdnja vrijedi za neki $j \in \mathbb{N}$, tj. da su $x_1, \ldots, x_{p-1}$ sva rješenja kongruencije $f(x) = x^{p-1} - 1 \pmod{p^j}$. Tada je $f(x_i) \equiv 0 \pmod{p^j}$ i $f'(x_i) = (p-1)x^{p-2} \not\equiv 0 \pmod{p^j}$, pa po Henselovoj lemi postoji jedinstveni $t_j \in \{0, 1, \ldots, p-1\}$ takav da je $f(x_i + t_i p^j) \equiv 0 \pmod{p^{j+1}}$. Sada su $x_i' = x_i + t_i p^j$, $i = 1, \ldots, p-1$ rješenja kongruencije $f(x) \equiv 0 \pmod{p^{j+1}}$. Pokažimo da su to sva rješenja. Zaista, ako je x' neko rješenje, onda je $f(x') \equiv 0 \pmod{p^j}$, pa je $x' \equiv x_i \pmod{p^j}$ za neki $i = 1, \ldots, p-1$. Sada iz jedinstvenosti od t_i slijedi da je $x' \equiv x_i' \pmod{p^{j+1}}$. □

Primjer 2.10. *Riješimo kongruenciju $x^2 + x + 47 \equiv 0 \pmod{7^3}$.*

Rješenje: Riješimo najprije kongruenciju $x^2 + x + 47 \equiv 0 \pmod 7$. Dobivamo da su rješenja $x \equiv 1 \pmod 7$ i $x \equiv 5 \pmod 7$. Neka je $f(x) = x^2 + x + 47$. Tada je $f'(x) = 2x + 1$, pa je $f'(1) = 3 \not\equiv 0 \pmod 7$ i $f'(5) = 11 \not\equiv 0 \pmod 7$. Stoga možemo primijeniti Henselovu lemu.

Da bi riješili kongruenciju $x^2 + x + 47 \equiv 0 \pmod{7^2}$, trebamo riješiti

$$tf'(a) \equiv -\frac{f(a)}{7} \pmod 7 \quad \text{za } a = 1, 5.$$

Imamo:

1) $t \cdot 3 \equiv -7 \pmod 7 \implies t = 0 \implies a + t \cdot 7 = 1$;
2) $t \cdot 11 \equiv -11 \mod 7 \implies t = 6 \implies a + t \cdot 7 = 47$.

Konačno, da bi riješili polaznu kongruenciju, trebamo riješiti

$$tf'(a) \equiv -\frac{f(a)}{49} \pmod 7 \quad \text{za } a = 1, 47.$$

Imamo:

1) $t \cdot 3 \equiv -1 \mod 7 \implies t = 2 \implies a + t \cdot 49 = 99$;
2) $t \cdot 11 \equiv -47 \mod 7 \implies t = 4 \implies a + t \cdot 49 = 243$.

Dakle, rješenja su $x \equiv 99 \pmod{343}$ i $x \equiv 243 \pmod{343}$. ♢

Zadatak 2.5. *Riješite kongruenciju $x^3 + x^2 - 5 \equiv 0 \pmod{7^3}$.*

Definicija 2.5. *Neka su a i n relativno prosti prirodni brojevi. Najmanji prirodni broj d sa svojstvom da je $a^d \equiv 1 \pmod{n}$ zove se* red *od a modulo n. Još se kaže da a* pripada eksponentu *d modulo n.*

Propozicija 2.18. *Neka je d red od a modulo n. Tada za prirodan broj k vrijedi $a^k \equiv 1 \pmod{n}$ ako i samo ako $d|k$. Posebno, $d|\varphi(n)$.*

Dokaz: Ako $d|k$, recimo $k = d \cdot l$, onda je $a^k \equiv (a^d)^l \equiv 1 \pmod{n}$.

Obratno, neka je $a^k \equiv 1 \pmod{n}$. Podijelimo k sa d, pa dobivamo $k = q \cdot d + r$, gdje je $0 \leq r < d$. Sada je

$$1 \equiv a^k \equiv a^{qd+r} \equiv (a^d)^q \cdot a^r \equiv a^r \pmod{n},$$

pa zbog minimalnosti od d slijedi da je $r = 0$, tj. $d|k$. □

Primjer 2.11. *Dokažimo da svaki prosti djelitelj Fermatovog broja $2^{2^n}+1$, za $n > 1$, ima oblik $p = k \cdot 2^{n+1} + 1$.*

Rješenje: Iz $2^{2^n} + 1 \equiv 0 \pmod{p}$ slijedi $2^{2^n} \equiv -1 \pmod{p}$ i $2^{2^{n+1}} \equiv 1 \pmod{p}$, pa slijedi da 2 pripada eksponentu 2^{n+1} modulo p. Budući da je $\varphi(p) = p-1$, slijedi da $2^{n+1}|p-1$, tj. postoji $k \in \mathbb{N}$ takav da je $p = k \cdot 2^{n+1}+1$. ♢

Definicija 2.6. *Ako je red od a modulo n jednak $\varphi(n)$, onda se a zove* primitivni korijen *modulo n.*

Ako postoji primitivni korijen modulo n, onda je grupa reduciranih ostataka modulo n ciklička. Slijedeći teorem pokazuje da je grupa $(\mathbb{Z}_p^*, \cdot_p)$ ciklička.

Teorem 2.19. *Ako je p prost broj, onda postoji točno $\varphi(p-1)$ primitivnih korijena modulo p.*

Dokaz: Svaki od brojeva $1, 2, \ldots, p-1$ pripada modulo p nekom eksponentu d, koji je djelitelj od $\varphi(p) = p-1$. Označimo sa $\psi(d)$ broj brojeva u nizu $1, 2, \ldots, p-1$ koji pripadaju eksponentu d. Tada je

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

Dovoljno je dokazati da ako je $\psi(d) \neq 0$, onda je $\psi(d) = \varphi(d)$. Zaista, po Teoremu 2.12 je

$$\sum_{d|p-1} \varphi(d) = p - 1,$$

pa ako bi bilo $\psi(d) = 0 < \varphi(d)$ za neki d, onda bi suma $\sum_{d|p-1} \psi(d)$ bila manja od $p-1$. Stoga je $\psi(d) \neq 0$ za svaki d, pa ako pokažemo da to povlači da je $\psi(d) = \varphi(d)$, onda ćemo dobiti da vrijedi $\psi(p-1) = \varphi(p-1)$, što se i tvrdilo u teoremu.

Dokažimo sada tvrdnju da $\psi(d) \neq 0$ povlači $\psi(d) = \varphi(d)$. Neka je $\psi(d) \neq 0$, te neka je a broj koji pripada eksponentu d modulo p. Promotrimo kongruenciju

$$x^d \equiv 1 \pmod{p}.$$

Ona ima rješenja $a, a^2, \ldots, a^d$ i po Lagrangeovom teoremu to su sva rješenja. Pokažimo da brojevi a^m, za $1 \leq m \leq d$ i $(m,d) = 1$, predstavljaju sve brojeve koji pripadaju eksponentu d modulo p. Zaista, svaki od njih ima red d, jer ako je $a^{md'} \equiv 1 \pmod{p}$, onda $d|md'$, pa $d|d'$. Ako je b bilo koji broj koji pripada eksponentu d modulo p, onda je $b \equiv a^m$ za neki m, $1 \leq m \leq d$. Budući da je

$$b^{\frac{d}{(m,d)}} \equiv (a^d)^{\frac{m}{(m,d)}} \equiv 1 \pmod{p},$$

to je $(m,d) = 1$. Dakle, dobili smo da je $\psi(d) = \varphi(d)$. □

Teorem 2.20. *Neka je p neparan prost broj, te neka je g primitivni korijen modulo p. Tada postoji $x \in \mathbb{Z}$ takav da je $g' = g + px$ primitivni korijen modulo p^j za sve $j \in \mathbb{N}$.*

Dokaz: Imamo $g^{p-1} = 1 + py$, za neki $y \in \mathbb{Z}$. Po binomnom teoremu je

$$g'^{p-1} = 1 + py + (p-1)pxg^{p-2} + \binom{p-1}{2} p^2x^2g^{p-3} + \cdots + p^{p-1}x^{p-1},$$

tj. $g'^{p-1} = 1 + pz$, gdje je $z \equiv y + (p-1)g^{p-2}x \pmod{p}$. Koeficijent uz x nije djeljiv sa p, pa možemo odabrati x tako da bude $(z,p) = 1$. Tvrdimo da tada g' ima traženo svojstvo. Dokažimo to.

Pretpostavimo da g' pripada eksponentu d modulo p^j. Tada d dijeli $\varphi(p^j) = p^{j-1}(p-1)$. No, g' je primitivni korijen modulo p, pa $p-1$ dijeli d. Dakle, $d = p^k(p-1)$ za neki $k < j$. Nadalje, imamo

$$(1+pz)^p = 1 + p^2z_1, \quad (1+pz)^{p^2} = (1+p^2z_1)^p = 1 + p^3z_2, \quad \ldots,$$

$$(1+pz)^{p^k} = 1 + p^{k+1}z_k,$$

gdje je $(z_i, p) = 1$ za $i = 1, \ldots, k$. Budući da je $g'^d \equiv 1 \pmod{p^j}$, odavde zaključujemo da je $j = k+1$, što povlači da je $d = \varphi(p^j)$. □

Teorem 2.21. *Za prirodan broj n postoji primitivni korijen modulo n ako i samo ako je $n = 2$, 4, p^j ili $2p^j$, gdje je p neparan prost broj.*

Dokaz: Jasno je da je 1 primitivni korijen modulo 2, te da je 3 primitivni korijen modulo 4. Neka je g primitivni korijen modulo p^j. Odaberimo među brojevima g i $g + p^j$ onaj koji je neparan. Tada je on primitivni korijen modulo $2p^j$ jer je $\varphi(2p^j) = \varphi(p^j)$.

Ostaje još dokazati nužnost. Neka je najprije $n = 2^j$ za $j \geq 3$. Tada za neparan broj a vrijedi $a^2 \equiv 1 \pmod{8}$. Budući da $8|a^2 - 1$ i $2|a^2 + 1$

imamo $a^4 \equiv 1 \pmod{16}$. Ponavljajući ovaj argument dobivamo: $a^{2^{j-2}} \equiv 1 \pmod{2^j}$ za $j \geq 3$. Budući da je $\varphi(2^j) = 2^{j-1}$, dokazali smo da ne postoji primitivni korijen modulo 2^j za $j \geq 3$.

Konačno, neka je $n = n_1 n_2$, gdje je $(n_1, n_2) = 1$, $n_1 > 2$, $n_2 > 2$. Brojevi $\varphi(n_1)$ i $\varphi(n_2)$ su parni, pa imamo

$$a^{\frac{1}{2}\varphi(n)} \equiv \left(a^{\varphi(n_1)}\right)^{\frac{1}{2}\varphi(n_2)} \equiv 1 \pmod{n_1},$$
$$a^{\frac{1}{2}\varphi(n)} \equiv \left(a^{\varphi(n_2)}\right)^{\frac{1}{2}\varphi(n_1)} \equiv 1 \pmod{n_2}.$$

Stoga je $a^{\frac{1}{2}\varphi(n)} \equiv 1 \pmod{n}$, što znači da ne postoji primitivni korijen modulo n. □

Primjer 2.12. *Nađimo najmanji primitivni korijen*
a) modulo 5, *b) modulo* 11, *c) modulo* 23.

Rješenje: a) $2^2 \not\equiv 1 \pmod{5} \implies$ 2 je primitivni korijen modulo 5.
b) $2^2 \not\equiv 1 \pmod{11}$, $2^5 \not\equiv 1 \pmod{11} \implies$ 2 je primitivni korijen modulo 11.
c) $2^{11} = 32 \cdot 64 \equiv 9 \cdot (-5) \equiv 1 \pmod{23}$, $3^{11} = 27^3 \cdot 9 \equiv 64 \cdot 9 \equiv (-5) \cdot 9 \equiv 1 \pmod{23}$, $4^{11} = (2^{11})^2 \equiv 1 \pmod{23}$, $5^{11} = (25)^5 \cdot 5 \equiv 32 \cdot 5 \equiv 9 \cdot 5 \equiv -1 \not\equiv 1 \pmod{23} \implies$ 5 je primitivni korijen modulo 23. ♢

Zadatak 2.6. *Nađite najmanji primitivni korijen*
a) modulo 13, *b) modulo* 17, *c) modulo* 41.

Napomena 2.1. T*zv. Artinova hipoteza glasi: Neka je* $\pi(N)$ *broj prostih brojeva* $\leq N$, *a* $v_2(N)$ *broj prostih brojeva* $q \leq N$ *za koje je* 2 *primitivni korijen. Tada je* $v_2(N) \sim A \cdot \pi(N)$, *gdje je* $A = \prod_p (1 - \frac{1}{p(p-1)}) \approx 0.3739558$.

Definicija 2.7. *Neka je* g *primitivni korijen modulo* n. *Lako se vidi da tada brojevi* g^l, $l = 0, 1, \ldots, \varphi(n) - 1$ *tvore reducirani sustav ostataka modulo* n. *Stoga za svaki cijeli broj* a *takav da je* $(a, n) = 1$ *postoji jedinstveni* l *takav da je* $g^l \equiv a \pmod{n}$. *Eksponent* l *se zove* indeks *od* a *u odnosu na* g *i označava se sa* $\operatorname{ind}_g a$ *ili* $\operatorname{ind} a$.

Teorem 2.22.
1) $\operatorname{ind} a + \operatorname{ind} b \equiv \operatorname{ind}(ab) \pmod{\varphi(n)}$
2) $\operatorname{ind} 1 = 0$, $\operatorname{ind} g = 1$
3) $\operatorname{ind}(a^m) \equiv m \operatorname{ind} a \pmod{\varphi(n)}$ *za* $m \in \mathbb{N}$
4) $\operatorname{ind}(-1) = \frac{1}{2}\varphi(n)$ *za* $n \geq 3$

Dokaz: Svojstva 1) – 3) slijede direktno iz definicije, a svojstvo 4) slijedi iz $g^{2 \operatorname{ind}(-1)} \equiv (-1)^2 \equiv 1 \pmod{n}$ i $2 \operatorname{ind}(-1) < 2\varphi(n)$. □

Uočimo da su svojstva indeksa 1) – 3) potpuno analogna svojstvima logaritamske funkcije.

Propozicija 2.23. *Ako je* $(n, p-1) = 1$*, onda kongruencija* $x^n \equiv a \pmod{p}$ *ima jedinstveno rješenje.*

Dokaz: Iz $x^n \equiv a \pmod{p}$, po Teoremu 2.22, dobivamo

$$n \operatorname{ind} x \equiv \operatorname{ind} a \pmod{p-1},$$

pa jer je $(n, p-1) = 1$, ova kongruencija ima jedinstveno rješenje. □

Primjer 2.13. *Riješimo kongruenciju* $x^5 \equiv 2 \pmod{7}$.

Rješenje: Imamo: $3^2 \equiv 2 \pmod{7}$, $3^3 \equiv 6 \pmod{7}$, $3^6 \equiv 1 \pmod{7}$. Stoga je 3 primitivni korijen modulo 7 i $\operatorname{ind}_3 2 = 2$. Dakle, dobivamo kongruenciju

$$5 \operatorname{ind}_3 x \equiv 2 \pmod{6},$$

čije je rješenje $\operatorname{ind}_3 x = 4$, pa je $x \equiv 3^4 \equiv 4 \pmod{7}$. ♢

Primjer 2.14. *Riješimo kongruenciju* $5x^4 \equiv 3 \pmod{11}$.

Rješenje: Iz Primjera 2.12 znamo da je 2 primitivni korijen modulo 11. Nadalje je $2^4 \equiv 5 \pmod{11}$, $2^8 \equiv 3 \pmod{11}$, pa dobivamo

$$\operatorname{ind}_2 5 + 4\operatorname{ind}_2 x \equiv \operatorname{ind}_2 3 \pmod{10}, \quad 4\operatorname{ind}_2 x \equiv 8 - 4 \equiv 4 \pmod{10}.$$

Prema tome, trebamo riješiti kongruenciju $2\operatorname{ind}_2 x \equiv 2 \pmod{5}$. Odavde je $\operatorname{ind}_2 x \equiv 1$ ili $6 \pmod{10}$, pa su rješenje $x \equiv 2 \pmod{11}$ i $x \equiv 2^6 \equiv 9 \pmod{11}$. ♢

Zadatak 2.7. *Riješite kongruencije*
a) $2x^8 \equiv 5 \pmod{13}$, *b)* $x^6 \equiv 5 \pmod{17}$, *c)* $x^{12} \equiv 37 \pmod{41}$.

Primjer 2.15. *Riješimo kongruenciju* $3^x \equiv 2 \pmod{23}$.

Rješenje: Iz Primjera 2.12 znamo da je 5 primitivni korijen modulo 23. Nadalje je $5^2 \equiv 2 \pmod{23}$, $5^5 \equiv 2^2 \cdot 5 \equiv -3 \pmod{23}$, $5^{11} \equiv -1 \pmod{23}$, što povlači da je $5^{16} \equiv 3 \pmod{23}$. Imamo:

$$x\operatorname{ind}_5 3 \equiv \operatorname{ind}_5 2 \pmod{22}, \quad 16x \equiv 2 \pmod{22}.$$

Sada je $(16, 22) = 2$, po dobivamo $8x \equiv 1 \pmod{11}$, odakle je $x \equiv 7 \pmod{11}$. Dakle, rješenja su $x \equiv 7, 18 \pmod{22}$. ♢

Zadatak 2.8. *Riješite kongruenciju* $7^x \equiv 6 \pmod{17}$.

Primjer 2.16. *Neka je* $\alpha \geq 3$*. Dokazati da brojevi*

$$\pm 5, \pm 5^2, \pm 5^3, \ldots, \pm 5^{2^{\alpha-2}}$$

čine reducirani sustav ostataka modulo 2^α.

Rješenje: Ovih brojeva ima $2 \cdot 2^{\alpha-2} = 2^{\alpha-1} = \varphi(2^\alpha)$ i svi su neparni. Stoga još trebamo samo dokazati da su oni međusobno nekongruentni modulo 2^α.

Pokažimo da za $k \geq 2$ vrijedi $2^k \parallel (5^{2^{k-2}} - 1)$. Ovo je točno za $k = 2$, pa pretpostavimo da vrijedi za neki k. Tada je

$$5^{2^{k-1}} - 1 = \left(5^{2^{k-2}} - 1\right)\left(5^{2k-2} + 1\right).$$

Broj $5^{2^{k-2}} + 1$ je paran, ali nije djeliv s 4, pa $2^{k-1} \parallel \left(5^{2^{k-1}} - 1\right)$.

Upravo dokazana tvrdnja, za $k = \alpha$ povlači da je red od 5 modulo 2^α jednak $2^{\alpha-2}$. To znači da su brojevi $5, 5^2, \ldots, 5^{2^{\alpha-2}}$ međusobno nekongruentni modulo 2^α. Ostaje još provjeriti da ne može biti $5^a \equiv -5^b \pmod{2^\alpha}$, no to je očito, jer je $5^a + 5^b \equiv 2 \pmod 4$. $\diamondsuit$

3. Kvadratni ostatci

Definicija 3.1. *Neka je* $(a, m) = 1$. *Ako kongruencija* $x^2 \equiv a \pmod{m}$ *ima rješenja, onda kažemo da je* a kvadratni ostatak *modulo* m. *U protivnom kažemo da je* a kvadratni neostatak *modulo* m.

Primjer 3.1. *Kvadratni ostatci modulo* 5 *su* 1 *i* 4, *a neostatci su* 2 *i* 3.

Teorem 3.1. *Neka je* p *neparan prost broj. Reducirani sustav ostataka modulo* p *sastoji se od* $\frac{p-1}{2}$ *kvadratnih ostataka i* $\frac{p-1}{2}$ *kvadratnih neostataka.*

Dokaz: Svaki kvadratni ostatak modulo p kongruentan je kvadratu nekog od brojeva

$$-\frac{p-1}{2}, \ldots, -1, 1, \ldots, \frac{p-1}{2},$$

tj. kongruentan je nekom od brojeva $1^2, 2^2, \ldots, (\frac{p-1}{2})^2$. Preostaje pokazati da je ovih $\frac{p-1}{2}$ brojeva međusobno nekongruentno modulo p. Pa pretpostavimo da je $k^2 \equiv l^2 \pmod{p}$, gdje je $1 \leq k < l \leq \frac{p-1}{2}$. Tada je $(l-k)(l+k) \equiv 0 \pmod{p}$, pa je $l - k \equiv 0 \pmod{p}$ ili $l + k \equiv 0 \pmod{p}$, što je u suprotnosti s pretpostavkama na k i l, jer je $0 < l - k < p$ i $0 < l + k < p$. □

Zadatak 3.1. *Odredite sve kvadratne ostatke modulo* 7 *i modulo* 17.

Definicija 3.2. *Neka je* p *neparan prost broj. Po definiciji,* Legendreov simbol $(\frac{a}{p})$ *je jednak* 1 *ako je* a *kvadratni ostatak modulo* p, -1 *ako je* a *kvadratni neostatak modulo* p, *a* 0 *ako* $p|a$.

Dakle, broj rješenja kongruencije $x^2 \equiv a \pmod{p}$ je jednak $1 + (\frac{a}{p})$.

Teorem 3.2 (Eulerov kriterij)**.**

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$$

Dokaz: Ako je $(\frac{a}{p}) = 0$, onda $p|a$, pa je tvrdnja očito zadovoljena.

Ako je $(\frac{a}{p}) = 1$, onda postoji $x_0 \in \mathbb{Z}$ takav da je $x_0^2 \equiv a \pmod{p}$. Sada je iz Malog Fermatovog teorema $a^{\frac{p-1}{2}} \equiv x_0^{p-1} \equiv 1 \equiv (\frac{a}{p}) \pmod{p}$.

Neka je $(\frac{a}{p}) = -1$. Za svaki $i \in \{1, \ldots, p-1\}$ odaberimo $j \in \{1, \ldots, p-1\}$ tako da vrijedi $i \cdot j \equiv a \pmod{p}$ (to je moguće po Teoremu 2.5). Uočimo da je $i \neq j$, budući da kongruencija $x^2 \equiv a \pmod{p}$ nema rješenja. Dakle, skup $\{1, \ldots, p-1\}$ se raspada na $\frac{p-1}{2}$ parova (i, j) za koje vrijedi $i \cdot j \equiv a$

(mod p). Množenjem ovih $\frac{p-1}{2}$ kongruencija, te koristeći Wilsonov teorem, dobivamo

$$a^{\frac{p-1}{2}} \equiv (p-1)! \equiv -1 \pmod{p}.$$

□

Propozicija 3.3.

1) Ako je $a \equiv b \pmod{p}$, *onda je* $(\frac{a}{p}) = (\frac{b}{p})$.

2) $(\frac{a}{p})(\frac{b}{p}) = (\frac{ab}{p})$

3) Ako je $(a,p) = 1$, *onda je* $(\frac{a^2}{p}) = 1$.

4) $(\frac{1}{p}) = 1, \quad (\frac{-1}{p}) = (-1)^{\frac{p-1}{2}}$.

Dokaz: 1) Ako je $a \equiv b \pmod{p}$, onda kongruencija $x^2 \equiv a \pmod{p}$ ima rješenja ako i samo ako rješenja ima kongruencija $x^2 \equiv b \pmod{p}$.

2) Iz

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \equiv a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv (ab)^{\frac{p-1}{2}} \equiv \left(\frac{ab}{p}\right) \pmod{p}$$

slijedi $(\frac{a}{p})(\frac{b}{p}) = (\frac{ab}{p})$.

3) Kongruencija $x^2 \equiv a^2 \pmod{p}$ očito ima rješenje $x = a$.

4) Prva tvrdnja je specijalni slučaj od 3), dok druga slijedi uvrštavanjem $a = -1$, u Eulerov kriterij. □

Teorem 3.4 (Gaussova lema)**.** *Neka je* p *neparan broj i* $(a,p) = 1$. *Promotrimo brojeve* $a, 2a, 3a, \ldots, \frac{p-1}{2} \cdot a$, *te njihove najmanje nenegativne ostatke pri dijeljenju s* p. *Označimo s* n *broj ostataka koji su veći od* $\frac{p}{2}$. *Tada je* $(\frac{a}{p}) = (-1)^n$.

Dokaz: Neka su $r_1, \ldots, r_n$ ostatci koji su veći od $\frac{p}{2}$, a neka su $s_1, \ldots, s_k$ preostali ostatci. Brojevi $r_1, \ldots, r_n, s_1, \ldots, s_k$ su međusobno različiti (po Teoremu 2.5) i niti jedan od njih nije jednak nuli. Nadalje, $n + k = \frac{p-1}{2}$.

Brojevi $p - r_i$ su međusobno različiti i $0 < p - r_i < \frac{p}{2}$, za $i = 1, \ldots, n$. Također, niti jedan $p - r_i$ nije jednak nekom s_j. Zaista, ako je $p - r_i = s_j$, onda je $r_i \equiv \alpha a \pmod{p}$, $s_j \equiv \beta a \pmod{p}$ za neke $1 \leq \alpha, \beta \leq \frac{p-1}{2}$, pa iz $a(\alpha + \beta) \equiv 0 \pmod{p}$ i $(a,p) = 1$ slijedi da je $\alpha + \beta \equiv 0 \pmod{p}$, što je nemoguće jer je $2 \leq \alpha + \beta \leq p - 1$.

Prema tome, brojevi $p - r_1, \ldots, p - r_n, s_1, \ldots, s_k$ su svi međusobno različiti, ima ih $\frac{p-1}{2}$ i elementi su skupa $\{1, \ldots, \frac{p-1}{2}\}$. Stoga su to upravo brojevi $1, 2, \ldots, \frac{p-1}{2}$ u nekom poretku. Množeći ih, dobivamo

$$(p - r_1) \cdots (p - r_n) s_1 \cdots s_k = 1 \cdot 2 \cdots (\frac{p-1}{2}).$$

Odavde je

$$\begin{aligned} 1 \cdot 2 \cdots \frac{p-1}{2} &\equiv (-r_1) \cdots (-r_n) s_1 \cdots s_k \equiv (-1)^n r_1 \cdots r_n s_1 \cdots s_k \\ &\equiv (-1)^n a \cdot 2a \cdot 3a \cdots (\frac{p-1}{2}) a \pmod{p}. \end{aligned}$$

Skratimo li ovu kongruenciju s $(\frac{p-1}{2})!$, dobivamo $1 \equiv (-1)^n a^{\frac{p-1}{2}} \pmod p$, pa je po Eulerovom kriteriju

$$(\frac{a}{p}) \equiv a^{\frac{p-1}{2}} \equiv (-1)^n \pmod p.$$

□

Teorem 3.5. *Ako je p neparan prost broj i $(a, 2p) = 1$, onda je $(\frac{a}{p}) = (-1)^t$, gdje je $t = \sum_{j=1}^{\frac{p-1}{2}} \lfloor \frac{ja}{p} \rfloor$. Također vrijedi: $(\frac{2}{p}) = (-1)^{\frac{p^2-1}{8}}$, tj. broj 2 je kvadratni ostatak modulo p ako i samo ako je p oblika $8k \pm 1$.*

Dokaz: Koristit ćemo iste oznake kao u dokazu Teorema 3.4. Ponovo su r_i i s_i ostatci pri dijeljenju brojeva ja s p, $j = 1, \ldots, \frac{p-1}{2}$. Kvocijenti pri tom dijeljenju su brojevi $\lfloor \frac{ja}{p} \rfloor$. Ako je sada $(a, p) = 1$, onda imamo

$$\sum_{j=1}^{\frac{p-1}{2}} ja = \sum_{j=1}^{\frac{p-1}{2}} p\lfloor \frac{ja}{p} \rfloor + \sum_{i=1}^{n} r_i + \sum_{i=1}^{k} s_i,$$

te

$$\sum_{j=1}^{\frac{p-1}{2}} j = \sum_{i=1}^{n} (p - r_i) + \sum_{i=1}^{k} s_i = np - \sum_{i=1}^{n} r_i + \sum_{i=1}^{k} s_i.$$

Oduzimanjem ova dva izraza, dobivamo

$$(a-1) \sum_{j=1}^{\frac{p-1}{2}} j = p\Big(\sum_{j=1}^{\frac{p-1}{2}} \lfloor \frac{ja}{p} \rfloor - n \Big) + 2 \sum_{i=1}^{n} r_i.$$

Nadalje je

$$\sum_{j=1}^{\frac{p-1}{2}} j = \frac{\frac{p-1}{2} \cdot \frac{p+1}{2}}{2} = \frac{p^2-1}{8},$$

pa je

$$(a-1)\frac{p^2-1}{8} \equiv \sum_{j=1}^{\frac{p-1}{2}} \lfloor \frac{ja}{p} \rfloor - n \pmod 2.$$

Ako je sada a neparan, tj. $(a, 2p) = 1$, onda odavde dobivamo da je $n \equiv \sum_{j=1}^{\frac{p-1}{2}} \lfloor \frac{ja}{p} \rfloor \pmod 2$, a ako je $a = 2$, onda dobivamo $n \equiv \frac{p^2-1}{8} \pmod 2$, jer je $\lfloor \frac{2j}{p} \rfloor = 0$ za $j = 1, \ldots, \frac{p-1}{2}$. Sada tvrdnja Teorema 3.5 slijedi iz Gaussove leme. □

Teorem 3.6 (Gaussov kvadratni zakon reciprociteta)**.** *Ako su p i q različiti neparni prosti brojevi, onda vrijedi*

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

Drugim riječima, ako su p i q oba oblika $4k+3$, onda jedna od kongruencija $x^2 \equiv p \pmod{q}$, $x^2 \equiv q \pmod{p}$ ima rješenja, a druga nema. Ako barem jedan od brojeva p i q ima oblik $4k+1$, onda ili obje ove kongruencije imaju rješenja ili obje nemaju rješenja.

Dokaz: Neka je $\mathcal{S} = \{(x,y) : x,y \in \mathbb{Z}, 1 \le x \le \frac{p-1}{2}, 1 \le y \le \frac{q-1}{2}\}$. Skup $\mathcal{S}$ ima $\frac{p-1}{2}\cdot\frac{q-1}{2}$ članova. Podijelimo $\mathcal{S}$ na dva disjunktna podskupa $\mathcal{S}_1$ i $\mathcal{S}_2$ prema tome da li je $qx > py$ ili je $qx < py$. Uočimo da ne može biti $qx = py$. Skup $\mathcal{S}_1$ je, dakle, skup svih parova (x,y) takvih da je $1 \le x \le \frac{p-1}{2}$ i $1 \le y < \frac{qx}{p}$. Takvih parova ima $\sum_{x=1}^{\frac{p-1}{2}} \lfloor \frac{qx}{p} \rfloor$. Slično se $\mathcal{S}_2$ sastoji od svih parova (x,y) takvih da je $1 \le y \le \frac{q-1}{2}$ i $1 \le x < \frac{py}{q}$, a takvih parova ima $\sum_{y=1}^{\frac{q-1}{2}} \lfloor \frac{py}{q} \rfloor$.

Prema tome je

$$\sum_{j=1}^{\frac{p-1}{2}} \lfloor \frac{qj}{p} \rfloor + \sum_{j=1}^{\frac{q-1}{2}} \lfloor \frac{pj}{q} \rfloor = \frac{p-1}{2}\cdot\frac{q-1}{2},$$

pa je po Teoremu 3.5

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

□

Primjer 3.2. *Izračunajmo* $\left(\frac{-42}{61}\right)$.

Rješenje: Imamo:

$$\begin{aligned}
&(\frac{-42}{61}) = (\frac{-1}{61})(\frac{2}{61})(\frac{3}{61})(\frac{7}{61}), \quad (\frac{-1}{61}) = (-1)^{\frac{60}{2}} = 1,\\
&(\frac{2}{61}) = (-1)^{\frac{61^2-1}{8}} = -1, \quad (\frac{3}{61}) = (\frac{61}{3}) = (\frac{1}{3}) = 1,\\
&(\frac{7}{61}) = (\frac{61}{7}) = (\frac{5}{7}) = (\frac{7}{5}) = (\frac{2}{5}) = (-1)^{\frac{5^2-1}{8}} = -1,
\end{aligned}$$

pa je $(\frac{-42}{61}) = 1$. ♢

Primjer 3.3. *a) Odredimo sve proste brojeve p takve da je -2 kvadratni ostatak modulo p.*

b) Dokažimo da postoji beskonačno mnogo prostih brojeva oblika $8k+3$.

Rješenje: a) Trebamo naći sve proste brojeva za koje vrijedi $\left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right) = 1$. Imamo dvije mogućnosti:

1) $\left(\frac{-1}{p}\right) = 1 \quad \& \quad \left(\frac{2}{p}\right) = 1$. Prvi uvjet je ekvivalentan s $p \equiv 1 \pmod 4$, a drugi s $p \equiv 1, 7 \pmod 8$, što zajedno daje $p \equiv 1 \pmod 8$.

2) $\left(\frac{-1}{p}\right) = -1 \quad \& \quad \left(\frac{2}{p}\right) = -1$. Prvi uvjet je ekvivalentan s $p \equiv 3 \pmod 4$, a drugi s $p \equiv 3, 5 \pmod 8$, što zajedno daje $p \equiv 3 \pmod 8$.

Dakle, $p \equiv 1$ ili $3 \pmod 8$.

b) Neka su $p_1, p_2, \ldots, p_n$ svi prosti brojevi oblika $8k + 3$. Promotrimo broj

$$m = p_1^2 p_2^2 \cdots p_n^2 + 2.$$

Prema a), svi prosti faktori od m su oblika $8k + 1$ ili $8k + 3$. No, $m \equiv 3 \pmod 8$, pa ne mogu svi faktori biti oblika $8k + 1$. Dakle, postoji prosti faktor p oblika $8k + 3$. Kako je očito $p \neq p_i$, $i = 1, 2, \ldots, n$, dobili smo kontradikciju. ♢

Zadatak 3.2. *Odredite sve proste brojeve p takve da je $\left(\frac{-3}{p}\right) = 1$. Dokažite da postoji beskonačno mnogo prostih brojeva oblika $6k + 1$.*

Primjer 3.4. *a) Neka je $p \equiv 3 \pmod 4$ prost broj takav da je $q = 2p + 1$ također prost. Dokažimo da je tada $2^p \equiv 1 \pmod q$.*

b) Pokažimo da Mersennov broj $M_{251} = 2^{251} - 1$ nije prost.

Rješenje: a) Kako je $\varphi(q) = q - 1 = 2p$, imamo da je $2^{2p} - 1 = (2^p - 1)(2^p + 1) \equiv 0 \pmod q$. Dakle, $2^p \equiv 1 \pmod q$ ili $2^p \equiv -1 \pmod q$. Po pretpostavci je $p = 4k + 3$, $q = 8k + 7$. Ako bi bilo $2^p \equiv 1 \pmod q$, to bi značilo da je $2^{4k+3} \equiv -1 \pmod q$, odnosno

$$x^2 \equiv -2 \pmod q,$$

za $x = 2^{2k+2}$, a to je nemoguće prema Primjeru 3.3.

b) Brojevi 251 i $2 \cdot 251 + 1 = 503$ su prosti i $251 \equiv 3 \pmod 4$, pa iz a) slijedi da $503 | M_{251}$, što znači da M_{251} nije prost. ♢

Primjer 3.5. *Prosti brojevi p i q zovu se* prosti brojevi blizanci *ako je $q = p + 2$. (Još uvijek je nedokazana slutnja da postoji beskonačno mnogo parova prostih brojeva blizanaca.) Dokažimo da postoji $a \in \mathbb{Z}$ takav da $p | (a^2 - q)$ ako i samo ako postoji $b \in \mathbb{Z}$ takav da $q | (b^2 - p)$.*

Rješenje: Uočimo da jedan od brojeva p, q ima oblik $4k + 1$, a drugi $4k + 3$. Stoga vrijedi

$$\begin{aligned} \exists a \in \mathbb{Z},\, a^2 \equiv q \pmod p \quad &\iff \quad \left(\frac{q}{p}\right) = 1 \quad \iff \quad \left(\frac{p}{q}\right) = 1 \\ &\iff \quad \exists b \in \mathbb{Z},\, b^2 \equiv p \pmod q. \end{aligned}$$

♢

Primjer 3.6. *Neka je* $\left(\frac{a}{p}\right) = 1$. *Nađimo rješenja kongruencije* $x^2 \equiv a \pmod{p}$ *ako je* $p = 4k+3$ *ili* $p = 8k+5$.

Rješenje: 1) Ako je $p = 4k+3$, onda je $a^{(p-1)/2} = a^{2k+1} \equiv 1 \pmod{p}$, pa je $(a^{k+1})^2 \equiv a \pmod{p}$. Dakle, $x \equiv \pm a^{k+1} \pmod{p}$.

2) Ako je $p = 8k+5$, onda je $a^{4k+2} \equiv 1 \pmod{p}$. Odavde je $a^{2k+1} \equiv \pm 1 \pmod{p}$, pa je $a^{2k+2} \equiv a \pmod{p}$. Budući da je $\left(\frac{2}{p}\right) = -1$, imamo $2^{4k+2} \equiv -1 \pmod{p}$. Prema tome, rješenja su

$$x \equiv \pm a^{k+1} \pmod{p} \quad \text{ili} \quad x \equiv \pm a^{k+1} 2^{2k+1} \pmod{p}.$$

♢

Primjer 3.7. *Neka je* $p \equiv 1 \pmod{4}$. *Izračunajmo sumu svih kvadratnih ostataka* r *modulo* p, *takvih da je* $1 \le r \le p-1$.

Rješenje: Kako je $p \equiv 1 \pmod{4}$, imamo $\left(\frac{p-r}{p}\right) = \left(\frac{-r}{p}\right) = \left(\frac{r}{p}\right)$. To znači da je r kvadratni ostatak modulo p ako i samo ako je $p-r$ kvadratni ostatak modulo p. Stoga je

$$2 \sum_{\substack{1 \le r \le p-1 \\ \left(\frac{r}{p}\right)=1}} r = \sum_{\substack{1 \le r \le p-1 \\ \left(\frac{r}{p}\right)=1}} r + \sum_{\substack{1 \le r \le p-1 \\ \left(\frac{r}{p}\right)=1}} (p-r) = p \cdot \frac{p-1}{2},$$

pa je tražena suma jednaka $\frac{1}{4}p(p-1)$. ♢

Zadatak 3.3. *Neka je* $(a,p) = 1$. *Izračunajte:* $\sum_{x=1}^{p} \left(\frac{ax+b}{p}\right)$.

Primjer 3.8. *Neka je* $(k,p) = 1$. *Izračunajmo:* $\sum_{x=1}^{p-1} \left(\frac{x(x+k)}{p}\right)$.

Rješenje: Za $x \in \{1, \dots p-1\}$, odaberimo $x' \in \{1, \dots, p-1\}$ tako da vrijedi $x \cdot x' \equiv 1 \pmod{p}$. Tada je

$$\sum_{x=1}^{p-1} \left(\frac{x(x+k)}{p}\right) = \sum_{x=1}^{p-1} \left(\frac{xx'(xx'+kx')}{p}\right) = \sum_{x=1}^{p-1} \left(\frac{1+kx'}{p}\right).$$

Kada x prolazi skupom svih reducuranih ostataka modulo p, onda i x' prolazi tim istim skupom, pa $1+kx'$ prolazi skupom svih ostataka, osim ostatka $1 + k \cdot 0 = 1$. Kako kvadratnih ostataka i kvadratnih neostataka ima jednak broj, to je $\sum_{j=0}^{p-1} \left(\frac{j}{p}\right) = 0$. Stoga je

$$\sum_{x=1}^{p-1} \left(\frac{1+kx'}{p}\right) = \sum_{j=0}^{p-1} \left(\frac{j}{p}\right) - \left(\frac{1}{p}\right) = -1.$$

♢

Definicija 3.3. *Neka je Q neparan prirodan broj, te neka je $Q = q_1 \cdots q_s$, gdje su q_i neparni prosti brojevi, ne nužno različiti. Tada se* Jacobijev simbol $(\frac{a}{Q})$ *definira sa*

$$\Big(\frac{a}{Q}\Big) = \prod_{j=1}^{s} \Big(\frac{a}{q_j}\Big),$$

gdje je $(\frac{a}{q_j})$ Legendreov simbol.

Ako je Q prost broj, onda se Legendreov i Jacobijev simbol podudaraju. Ako je $(a, Q) > 1$, onda je $(\frac{a}{Q}) = 0$; inače je $(\frac{a}{Q}) \in \{-1, 1\}$. Ako je a kvadratni ostatak modulo Q, onda je a kvadratni ostatak modulo q_j za svaki j. Zato je $(\frac{a}{q_j}) = 1$ za svaki j, pa je i $(\frac{a}{Q}) = 1$.

Primijetimo međutim da $(\frac{a}{Q}) = 1$ *ne povlači* da je a kvadratni ostatak modulo Q. Na primjer, $(\frac{2}{15}) = (\frac{2}{3})(\frac{2}{5}) = (-1)(-1) = 1$, ali kongruencija $x^2 \equiv 2 \pmod{15}$ nema rješenja. Da bi a bio kvadratni ostatak modulo Q nužno je i dovoljno da svi $(\frac{a}{q_j})$ budu jednaki 1.

Propozicija 3.7. *Neka su Q i Q' neparni prirodni brojevi. Tada vrijedi*

1) $(\frac{a}{Q})(\frac{a}{Q'}) = (\frac{a}{QQ'})$

2) $(\frac{a}{Q})(\frac{a'}{Q}) = (\frac{aa'}{Q})$

3) Ako je $(a, Q) = 1$, onda je $(\frac{a^2}{Q}) = (\frac{a}{Q^2}) = 1$.

4) Ako je $a \equiv a' \pmod{Q}$, onda je $(\frac{a}{Q}) = (\frac{a'}{Q})$.

Dokaz: Sve tvrdnje slijede direktno iz definicije Jacobijevog simbola i Propozicije 3.3. □

Propozicija 3.8. *Ako je Q neparan prirodan broj, onda je*

$$\Big(\frac{-1}{Q}\Big) = (-1)^{\frac{Q-1}{2}}, \quad \Big(\frac{2}{Q}\Big) = (-1)^{\frac{Q^2-1}{8}}.$$

Dokaz: Imamo:

$$\Big(\frac{-1}{Q}\Big) = \prod_{j=1}^{s} \Big(\frac{-1}{q_j}\Big) = \prod_{j=1}^{s} (-1)^{\frac{q_j-1}{2}} = (-1)^{\sum_{j=1}^{s} \frac{q_j-1}{2}}.$$

Ako su a i b neparni, onda je

$$\frac{ab-1}{2} - \Big(\frac{a-1}{2} + \frac{b-1}{2}\Big) = \frac{(a-1)(b-1)}{2} \equiv 0 \pmod{2},$$

pa je

$$\frac{ab-1}{2} \equiv \frac{a-1}{2} + \frac{b-1}{2} \pmod{2}.$$

Koristeći ovu relaciju, lako se indukcijom dokaže da vrijedi

$$\sum_{j=1}^{s} \frac{q_j - 1}{2} \equiv \frac{1}{2}\Big(\prod_{j=1}^{s} q_j - 1\Big) \equiv \frac{Q-1}{2} \pmod{2}, \tag{11}$$

pa je $(\frac{-1}{Q}) = (-1)^{\frac{Q-1}{2}}$.

Slično, ako su a i b neparni, onda je

$$\frac{a^2b^2-1}{8} - \Big(\frac{a^2-1}{8} + \frac{b^2-1}{8}\Big) = \frac{(a^2-1)(b^2-1)}{8} \equiv 0 \pmod 2,$$

pa je

$$\Big(\frac{2}{Q}\Big) = \prod_{j=1}^{s}\Big(\frac{2}{q_j}\Big) = (-1)^{\sum_{j=1}^{s}\frac{q_j^2-1}{8}} = (-1)^{\frac{1}{8}(\sum_{j=1}^{s} q_j^2-1)} = (-1)^{\frac{Q^2-1}{8}}.$$

□

Propozicija 3.9. *Ako su P i Q neparni prirodni brojevi i $(P,Q)=1$, onda je*

$$\Big(\frac{P}{Q}\Big)\Big(\frac{Q}{P}\Big) = (-1)^{\frac{P-1}{2}\cdot\frac{Q-1}{2}}.$$

Dokaz: Neka je $P = \prod_{i=1}^{r} p_i$, $Q = \prod_{j=1}^{s} q_j$. Tada je

$$\begin{aligned}\Big(\frac{P}{Q}\Big) &= \prod_{j=1}^{s}\Big(\frac{p}{q_j}\Big) = \prod_{j=1}^{s}\prod_{i=1}^{r}\Big(\frac{p_i}{q_j}\Big) = \prod_{j=1}^{s}\prod_{i=1}^{r}\Big(\frac{q_j}{p_i}\Big)(-1)^{\frac{p_i-1}{2}\cdot\frac{q_j-1}{2}} \\ &= \Big(\frac{Q}{P}\Big)(-1)^{\sum_{j=1}^{s}\sum_{i=1}^{r}\frac{p_i-1}{2}\cdot\frac{q_j-1}{2}}.\end{aligned}$$

Ali, prema (11) je

$$\sum_{j=1}^{s}\sum_{i=1}^{r}\frac{p_i-1}{2}\cdot\frac{q_j-1}{2} = \Big(\sum_{i=1}^{r}\frac{p_i-1}{2}\Big)\Big(\sum_{j=1}^{s}\frac{q_j-1}{2}\Big) \equiv \frac{P-1}{2}\cdot\frac{Q-1}{2} \pmod 2,$$

pa je $\Big(\frac{P}{Q}\Big)\Big(\frac{Q}{P}\Big) = (-1)^{\frac{P-1}{2}\cdot\frac{Q-1}{2}}$. □

Primjer 3.9. *Izračunajmo* $\Big(\frac{105}{317}\Big)$.

Rješenje: Imamo: $\Big(\frac{105}{317}\Big) = \Big(\frac{317}{105}\Big) = \Big(\frac{2}{105}\Big) = 1.$ ♢

Zadatak 3.4. *Izračunati:* $\Big(\frac{-23}{83}\Big)$, $\Big(\frac{51}{71}\Big)$, $\Big(\frac{7}{227}\Big)$.

Primjer 3.10. Fibonaccijevi brojevi *su definirani s* $F_0 = 1$, $F_1 = 1$, $F_{n+2} = F_{n+1} + F_n$. *Vrijedi tzv.* Binetova formula*:*

$$F_n = \frac{1}{\sqrt{5}}(\alpha^n - \beta^n), \quad \alpha = \frac{1+\sqrt{5}}{2},\ \beta = \frac{1-\sqrt{5}}{2}.$$

Dokazati:

a) Ako je p prost broj oblika $10k \pm 1$, onda je $F_{p-1} \equiv 0 \pmod p$.

b) Ako je p prost broj oblika $10k \pm 3$, onda je $F_{p+1} \equiv 0 \pmod p$.

Rješenje: a) Iz Binetove formule imamo

$$F_{p-1} = \frac{1}{2^{p-2}}\Big[\binom{p-1}{1} + \binom{p-1}{3}\cdot 5 + \cdots + \binom{p-1}{p-2}\cdot 5^{(p-3)/2}\Big].$$

Za $0 < k < p$ je $\binom{p-1}{k-1} + \binom{p-1}{k} = \binom{p}{k} = \frac{p(p-1)\cdots(p-k+1)}{k!} \equiv 0 \pmod p$. Odavde je $\binom{p-1}{0} \equiv -\binom{p-1}{1} \equiv \binom{p-1}{2} \equiv -\binom{p-1}{3} \equiv \cdots \equiv \binom{p-1}{p-1} \pmod p$, pa zbog $\binom{p-1}{0} = 1$ imamo: $\binom{p-1}{1} \equiv \binom{p-1}{3} \equiv \cdots \equiv \binom{p-1}{p-2} \equiv -1 \pmod p$. Stoga je

$$\begin{aligned} 2^{p-1}F_{p-1} &\equiv -2(1 + 5 + \cdots + 5^{(p-3)/2}) \equiv -\frac{5^{(p-1)/2} - 1}{2} \\ &\equiv -\frac{1}{2}\Big[\Big(\frac{5}{p}\Big) - 1\Big] \pmod p. \end{aligned}$$

Budući da je $\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right)$, a kvadratni ostatci modulo 5 su 1 i 4, imamo da je $\left(\frac{5}{p}\right) = 1$ ako je $p \equiv \pm 1 \pmod{10}$, dok je $\left(\frac{5}{p}\right) = -1$ ako je $p \equiv \pm 3 \pmod{10}$. Odavde je $F_{p-1} \equiv 0 \pmod p$ za $p = 10k \pm 1$.

b) Imamo:

$$F_{p+1} = \frac{1}{2^p}\Big[\binom{p+1}{1} + \binom{p+1}{3}\cdot 5 + \cdots + \binom{p+1}{p}\cdot 5^{(p-1)/2}\Big].$$

Iz $\binom{p+1}{k} = \binom{p}{k} + \binom{p}{k-1}$ slijedi da je $\binom{p+1}{k} \equiv 0 \pmod p$ za $1 < k < p$. Stoga je

$$2^p F_{p+1} \equiv 1 + 5^{(p-1)/2} \equiv 1 + \Big(\frac{5}{p}\Big) \equiv 0 \pmod p,$$

pa je $F_{p+1} \equiv 0 \pmod p$ za $p = 10k \pm 3$. ♢

Zadatak 3.5. *Neka je $m \geq 2$ prirodan broj. Dokažite da je niz $(F_n \bmod m)$, ostataka Fibonaccijevih brojeva pri dijeljenju s m, periodičan. Označimo njegov period s $k(m)$. Dokažite da vrijedi $k(m) \leq m^2$.*

Zadatak 3.6. *Dokažite: ako je p prost broj broj oblika $10l \pm 1$, onda $k(p)|(p-1)$, a ako je p prost broj oblika $10l \pm 3$, onda $k(p)|(2p+2)$.*

4. Kvadratne forme

Promatrat ćemo tzv. *binarne kvadratne forme*

$$f(x,y) = ax^2 + bxy + cy^2, \quad a,b,c \in \mathbb{Z},$$

tj. homogene polinome od dvije varijable drugog stupnja s cjelobrojnim koeficijentima. *Diskriminanta* od f je broj $d = b^2 - 4ac$. Očito je $d \equiv 0 \pmod 4$ ako je b paran i $d \equiv 1 \pmod 4$ ako je b neparan. Vrijedi i obrat. Naime, forme $x^2 - \frac{1}{4}dy^2$ ako je $d \equiv 0 \pmod 4$, te $x^2 + xy + \frac{1}{4}(1-d)y^2$ ako je $d \equiv 1 \pmod 4$, imaju diskriminantu jednaku d i zovemo ih *glavne forme* s diskriminantom d.

Imamo:

$$4af(x,y) = (2ax + by)^2 - dy^2.$$

Prema tome, ako je $d < 0$, onda f poprima ili samo pozitivne ili samo negativne vrijednosti. U skladu s tim, kažemo da je f *pozitivno*, odnosno *negativno definitna*. Ako je $d > 0$, onda f poprima i pozitivne i negativne vrijednosti, pa se zove *indefinitna*. Ako je $d = 0$, onda kažemo da je f *poludefinitna*.

Definicija 4.1. *Reći ćemo da su dvije kvadratne forme f i g* ekvivalentne *ako se jedna može transformirati u drugu pomoću cjelobrojnih unimodularnih transformacija, tj. supstitucija oblika*

$$x = px' + qy', \qquad y = rx' + sy',$$

gdje je $p,q,r,s \in \mathbb{Z}$ i $ps - qr = 1$. Pišemo: $f \sim g$.

Matrično f možemo zapisati kao $X^\tau F X$, gdje je

$$F = \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix}, \qquad X = \begin{pmatrix} x \\ y \end{pmatrix},$$

a supstituciju sa $X = UX'$, gdje je

$$U = \begin{pmatrix} p & q \\ r & s \end{pmatrix}, \qquad X' = \begin{pmatrix} x' \\ y' \end{pmatrix}.$$

Uvjet unimodularnosti je tada $\det U = 1$. Pritom f prelazi u $X'^\tau G X'$, gdje je $G = U^\tau F U$.

Označimo s Γ skup svih matrica oblika $\begin{pmatrix} p & q \\ r & s \end{pmatrix}$, $p, q, r, s, \in \mathbb{Z}$, $ps - qr = 1$. Tada Γ čini grupu s obzirom na množenje matrica. Zaista, neka su $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, $B = \begin{pmatrix} p & q \\ r & s \end{pmatrix} \in \Gamma$. Tada je

$$AB^{-1} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} s & -q \\ -r & p \end{pmatrix} = \begin{pmatrix} as - br & -aq + bp \\ cs - dr & -cq + dp \end{pmatrix}$$

i

$$\det(AB^{-1}) = \det A \cdot (\det B)^{-1} = 1,$$

pa je $AB^{-1} \in \Gamma$. Elemente grupe Γ zovemo *unimodularne matrice*.

Propozicija 4.1. *Neka su f, g, h binarne kvadratne forme. Tada vrijedi:*

1. $f \sim f$,
2. $f \sim g \Rightarrow g \sim f$,
3. $f \sim g,\ g \sim h \Rightarrow f \sim h$.

Drugim riječima, $\sim$ je relacija ekvivalencije.

Dokaz: 1) Očito je $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in \Gamma$.

2) Ako je $f \sim g$, onda postoji $U \in \Gamma$ tako da je $G = U^\tau F U$. Odavde je $F = (U^{-1})^\tau G U^{-1}$. No, Γ je grupa, pa je $U^{-1} \in \Gamma$, što znači da je $g \sim f$.

3) Ako je $f \sim g$ i $g \sim h$, onda je $G = U^\tau F U$, $H = V^\tau G V$ za neke $U, V \in \Gamma$. Odavde je $H = (UV)^\tau F (UV)$, a budući je $UV \in \Gamma$, to je $f \sim h$. □

Definicija 4.2. *Kažemo da kvadratna forma* reprezentira *cijeli broj n ako postoje $x_0, y_0 \in \mathbb{Z}$ takvi da je $f(x_0, y_0) = n$. Ako je pritom $(x_0, y_0) = 1$, onda kažemo da reprezentacija* prava*; inače je* neprava.

Propozicija 4.2. *Neka su f i g ekvivalentne kvadratne forme, te $n \in \mathbb{Z}$. Tada:*

1) f reprezentira n ako i samo ako g reprezentira n,
2) f pravo reprezentira n ako i samo ako g pravo reprezentira n,
3) diskriminante od f i g su jednake.

Dokaz: 1) Zbog Propozicije 4.1, dovoljno je provjeriti jednu implikaciju. Neka je $G = U^\tau F U$. Ako je $n = X_0^\tau F X_0$, onda je $n = X_1^\tau G X_1$, gdje je $X_1 = U^{-1} X_0$.

2) Neka je $X_0 = \begin{pmatrix} x_0 \\ y_0 \end{pmatrix}$, $X_1 = \begin{pmatrix} x_1 \\ y_1 \end{pmatrix}$. Pretpostavimo da je $(x_0, y_0) = 1$. Iz $x_0 = px_1 + qy_1$, $y_0 = rx_1 + sy_1$ slijedi da je $(x_1, y_1) = 1$.

3) Označimo sa d_0 i d_1 diskriminante od f, odnosno g. Tada je $d_0 = -4\det F$, $d_1 = -4\det G$, a $\det G = \det U^\tau \det F \det U = \det F$, pa je $d_0 = d_1$. □

Opisat ćemo redukciju pozitivno definitnih kvadratnih formi. Dakle, pretpostavljamo da je $d < 0$ i $a > 0$, pa je i $c > 0$.

Definicija 4.3. *Reći ćemo da je pozitivno definitna kvadratna forma* $f(x, y) = ax^2 + bxy + cy^2$ reducirana *ako je* $-a < b \leq a < c$ *ili* $0 \leq b \leq a = c$.

Teorem 4.3. *Svaka pozitivno definitna kvadratna forma je ekvivalentna nekoj reduciranoj formi.*

Dokaz: Promotrimo supstitucije čije su matrice

$$U = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \quad \text{i} \quad V = \begin{pmatrix} 1 & \pm 1 \\ 0 & 1 \end{pmatrix}.$$

Pokažimo da korištenjem konačno mnogo ovih transformacija možemo postići da je

$$|b| \leq a \leq c.$$

Zaista, $U^\tau F U = \begin{pmatrix} c & -b/2 \\ -b/2 & a \end{pmatrix}$, što znači da U zamjenjuje a i c, pa ako smo u F imali $a > c$, onda ćemo u $U^\tau F U$ imati $a < c$. Nadalje

$$V^\tau F V = \begin{pmatrix} a & \pm a + \frac{b}{2} \\ \pm a + \frac{b}{2} & a \pm b + c \end{pmatrix},$$

što znači da V zamjenjuje b s $b \pm 2a$, dok a ostavlja nepromjenjenim. Stoga koristeći ovu transformaciju konačno mnogo puta možemo postići da je $|b| \leq a$. Ovaj proces mora završiti budući svaka primjena prve transformacije smanjuje vrijednost od a.

Ako je sada $b = -a$, onda primjenom supstitucije s matricom V možemo postići da je $b = a$, uz nepromjenjeni c. Ako je $a = c$, onda primjenom supstitucije s matricom U možemo postići da je $b \geq 0$. □

Primjer 4.1. *Nađimo reduciranu formu ekvivalentnu sa* $133x^2 + 108xy + 22y^2$.

Rješenje: Krećemo od matrice $\begin{pmatrix} 133 & 54 \\ 54 & 22 \end{pmatrix}$. Primijenimo U i dobivamo $\begin{pmatrix} 22 & -54 \\ -54 & 133 \end{pmatrix}$, potom dvaput primjenimo V^+, pa dobivamo $\begin{pmatrix} 22 & -32 \\ -32 & 47 \end{pmatrix}$ i $\begin{pmatrix} 22 & -10 \\ -10 & 5 \end{pmatrix}$. Ponovo primjenimo U i dobivamo $\begin{pmatrix} 5 & 10 \\ 10 & 22 \end{pmatrix}$. Sada dvostruka primjena V^- daje $\begin{pmatrix} 5 & 5 \\ 5 & 7 \end{pmatrix}$ i $\begin{pmatrix} 5 & 0 \\ 0 & 2 \end{pmatrix}$. Konačno, U daje $\begin{pmatrix} 2 & 0 \\ 0 & 5 \end{pmatrix}$. Dakle, tražena forma je $2x^2 + 5y^2$. ♢

Zadatak 4.1. *Nađite reduciranu formu ekvivalentnu sa* $7x^2+25xy+23y^2$.

Teorem 4.4. *Postoji samo konačno mnogo reduciranih formi s danom diskriminantom* d.

Dokaz: Ako je f reducirana, onda je $-d = 4ac - b^2 \geq 3ac$, pa su i a i c i $|b|$ manji od $\frac{1}{3}|d|$. □

Definicija 4.4. *Broj reduciranih formi s diskriminantom* d *zove se* broj klasa *od* d *i označava se s* $h(d)$.

Primjer 4.2. *Izračunajmo* $h(-4)$.

Rješenje: Iz $3ac \leq 4$ slijedi $a = c = 1$, pa je $b = 0$. Dakle, $h(-4) = 1$. ♢

Poznato je da je $h(d) = 1$ za samo 9 negativnih cijelih brojeva: $d = -3, -4, -7, -8, -11, -19, -43, -67, -163$. Nadalje vrijedi da je $\lim\limits_{d\to-\infty} h(d) = \infty$.

Zadatak 4.2. *Dokažite da je* $h(d) = 1$ *za* $d = -7,\ -8,\ -11$.

Primjer 4.3. *Izračunajmo* $h(-20)$.

Rješenje: Iz $-d = 4ac - b^2 \geq 3ac \geq 3a^2$ slijedi $a \leq 2$. Imamo dva slučaja:
1) $a = 1$. Sada je $b \in \{0, 1\}$. Iz $4c - b^2 = 20$ slijedi da je b paran. To znači da je $b = 0$ i $c = 5$.
2) $a = 2$. Sada je $b \in \{-1, 0, 1, 2\}$. Iz $8c - b^2 = 20$ slijedi da je b paran. Za $b = 0$ nema rješenja, a za $b = 2$ dobivamo $c = 3$.
Dakle, postoje dvije reducurane forme s diskriminantom -20, to su $x^2 + 5y^2$ i $2x^2 + 2xy + 3y^2$, pa je $h(-20) = 2$. ♢

Sljedeći teorem pokazuje da je $h(d)$ upravo broj neekvivalentnih binarnih kvadratnih formi s diskriminatnom d. Napomenimo da analogna tvrdnja za $d > 0$ ne vrijedi.

Teorem 4.5. *Ako su* f *i* f' *dvije ekvivalentne reducirane forme, onda je* $f = f'$.

Dokaz: Ako su $x, y \in \mathbb{Z} \setminus \{0\}$ i $|x| \geq |y|$, onda je

$$f(x, y) \geq |x|(a|x| - |by|) + c|y|^2 \geq |x|^2(a - |b|) + c|y|^2 \geq a - |b| + c.$$

Na isti način se provjerava da ako je $|y| \geq |x|$, onda je također $f(x, y) \geq a - |b| + c$. Dakle, tri najmanje vrijednosti koje može poprimiti $f(x, y)$ su a, c i $a - |b| + c$ i to upravo u tom redosljedu, a poprimaju se za $(x, y) = (1, 0), (0, 1)$, te $(1, 1)$ ili $(1, -1)$. Budući da, po Propoziciji 4.2.2), f' poprima iste vrijednosti za $(x, y) = 1$ kao i f, te budući je f' također reducirana, zaključujemo da je $a = a'$. Pretpostavimo da je $a < c$. Tada je $a < c < a - |b| + c$. Ako bi bilo $a = c'$, onda bi broj a imao više reprezentacija pomoću forme f' nego pomoću forme f. Stoga je $a < c'$, pa je $c = c'$. Iz

$b^2 = d + 4ac = b'^2$, dobivamo $|b| = |b'|$. Dakle, još samo treba pokazati da $b = -b'$ povlači $b = 0$.

Sada možemo pretpostaviti da je $-a < b < a < c$. Naime, budući je f' reducirana, imamo $-a < -b$, pa je $a \neq b$, a ako je $a = c$, onda iz $b \geq 0$ i $-b \geq 0$ slijedi $b = 0$. Prema tome je $f(x, y) \geq a - |b| + c > c > a$ za sve $x, y \in \mathbb{Z} \setminus \{0\}$.

Neka je $\begin{pmatrix} p & q \\ r & s \end{pmatrix}$ matrica prijelaza iz f u f'. Tada je

$$a' = f(p, r), \quad b' = 2apq + b(ps + qr) + 2crs, \quad c' = f(q, s). \tag{12}$$

Budući je u našem slučaju $a' = a = ap^2 + bpr + cr^2$, to je $p = \pm 1$ i $r = 0$. Sada iz $ps - qr = 1$ slijedi $s = \pm 1$, a iz $c = f(q, s)$ slijedi $q = 0$. To znači da je $b = b'$, pa je $b = 0$.

Ostaje razmotriti slučaj $a = c$. Tada broj a ima barem 4 reprezentacije pomoću f, pa mora imati i barem 4 reprezentacije pomoću f', a to povlači da je $c' = a = c$. Ponovo dobivamo da je $|b| = |b'|$, ali u ovom slučaju iz definicije reduciranosti imamo da je $b \geq 0$, $b' \geq 0$, pa je $b = b'$. □

Teorem 4.6. *Neka su $d < 0$ i $n > 0$ cijeli brojevi. Tada je n pravo reprezentiran nekom binarnom kvadratnom formom s diskriminantom d ako i samo ako kongruencija $x^2 \equiv d \pmod{4n}$ ima rješenja.*

Dokaz: Pretpostavimo da gornja kongruencija ima rješenja i da je $x = b$ rješenje. Definirajmo c s $b^2 - 4nc = d$ i stavimo $a = n$. Sada forma $f(x, y) = ax^2 + bxy + cy^2$ ima diskriminantu d i $f(1, 0) = n$, pa f pravo reprezentira broj n.

Obratno, pretpostavimo da forma f ima diskriminantu d i da je $n = f(p, r)$ za neke $p, r \in \mathbb{Z}$, $(p, r) = 1$. Tada postoje $q, s \in \mathbb{Z}$ takvi da je $ps - rq = 1$. Sada je f ekvivalentna s f' koja je dobivena iz f pomoću matrice prijelaza $\begin{pmatrix} p & q \\ r & s \end{pmatrix}$ i po (12) vrijedi: $a' = f(p, r) = n$. Ali f i f' imaju istu diskriminantu, pa je

$$b'^2 - 4nc' = d.$$

Dakle, kongruencija $x^2 \equiv d \pmod{4n}$ ima rješenje $x = b'$. □

Primjer 4.4. *Dokažimo da se prost broj p može prikazati u obliku $x^2 + 5y^2$, $x, y \in \mathbb{N}$ ako i samo ako je $p \equiv 1$ ili $9 \pmod{20}$.*

Rješenje: Nužan i dovoljan uvjet da bi se p mogao prikazati nekom kvadratnom formom s diskriminantom -20 je da kongruencija $x^2 \equiv -20 \pmod{4p}$ ima rješenja. To znači da $\exists z \in \mathbb{Z}$ takav da je $z^2 \equiv -5 \pmod{p}$, tj. $\left(\frac{-5}{p}\right) = 1$.

Iz Primjera 4.3 znamo da postoje točno dvije neekvivalentne forme s diskriminatnom -20.

Ako je $p = x^2 + 5y^2$, onda je $x^2 \equiv p \pmod 5$, tj. $\left(\frac{p}{5}\right) = 1$.

Ako je $p = 2x^2+2xy+3y^2$, onda je $2p = (2x+y)^2+5y^2$, pa je $(2x+y)^2 \equiv 2p \pmod 5$, tj. $\left(\frac{2p}{5}\right) = 1$. No, $\left(\frac{2p}{5}\right) = \left(\frac{2}{5}\right)\left(\frac{p}{5}\right) = -\left(\frac{p}{5}\right)$, pa je $\left(\frac{p}{5}\right) = -1$.

Dakle, traženi brojevi p su oni za koje vrijedi $\left(\frac{-5}{p}\right) = 1$ i $\left(\frac{p}{5}\right) = 1$. Kako je $\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right)$, naši uvjeti su ekvivalentni sa $\left(\frac{p}{5}\right) = 1$ i $\left(\frac{-1}{p}\right) = 1$, tj. $p \equiv 1$ ili $4 \pmod 5$ i $p \equiv 1 \pmod 4$, odakle je $p \equiv 1$ ili $9 \pmod{20}$. ♢

Teorem 4.7. *Prirodan broj n se može prikazati u obliku $n = x^2 + y^2$, $x, y \in \mathbb{Z}$ ako i samo ako se u rastavu broja n na proste faktore svaki prosti faktor p za koji je $p \equiv 3 \pmod 4$ javlja s parnom potencijom.*

Dokaz: Pretpostavimo da je $n = x^2 + y^2$, te da je n djeljiv s prostim brojem $p \equiv 3 \pmod 4$. Tada je $x^2 \equiv -y^2 \pmod p$. Ako p ne dijeli x i y, onda odavde dobivamo da je $\left(\frac{-1}{p}\right)$, što je kontradikcija. Stoga p dijeli x i y, pa je n djeljiv sa p^2. Sada je $(\frac{x}{p})^2 + (\frac{y}{p})^2 = \frac{n}{p^2}$, pa indukcijom slijedi da se p u rastavu broja n javlja s parnom potencijom.

Da bi dokazali obrat, dovoljno je dokazati da ako je n kvadratno slobodan i svi neparni faktori p od n zadovoljavaju $p \equiv 1 \pmod 4$, onda se n može prikazati u obliku $x^2 + y^2$. Zaista, ako je $n = x^2 + y^2$, onda je $n \cdot m^2 = (xm)^2 + (ym)^2$.

Promotrimo sada binarnu kvadratnu formu $f(x, y) = x^2 + y^2$. To je reducirana forma s diskriminantom -4. U Primjeru 4.2 pokazali smo da je $h(-4) = 1$. Stoga je to jedina reducirana forma s diskriminantom -4. Iz Teorema 4.6 slijedi da je n pravo reprezentiran formom $x^2 + y^2$ ako i samo ako kongruencija $x^2 \equiv -4 \pmod{4n}$ ima rješenja. Ova kongruencija je ekvivalentna sa $z^2 \equiv -1 \pmod n$. Neka je $n = p_1 p_2 \cdots p_k$. Po pretpostavci je $p_i \equiv 1 \pmod 4$, pa kongruencija $z^2 \equiv -1 \pmod{p_i}$ ima rješenje; neka je to rješenje $z = z_i$. Po Kineskom teoremu o ostacima, postoji cijeli broj z koji zadovoljava sustav

$$z \equiv z_1 \pmod{p_1}, \ldots, z \equiv z_k \pmod{p_k}.$$

Sada je $z^2 \equiv z_i^2 \equiv -1 \pmod{p_i}$ za svaki i, pa je $z^2 \equiv -1 \pmod n$. □

Teorem 4.8. *Cijeli broj n se može prikazati u obliku $x^2 - y^2$ ako i samo ako $n \not\equiv 2 \pmod 4$.*

Rješenje: Pretpostavimo da je $n \equiv 2 \pmod 4$, te da je $n = x^2 - y^2 = (x - y)(x + y)$. Budući je n paran, to je jedan od faktora $x - y$, $x + y$ paran. No, $x + y = (x - y) + 2y$, pa je i drugi faktor također paran. To znači da je $n \equiv 0 \pmod 4$, pa smo dobili kontradikciju.

Neka je sada $n \not\equiv 2 \pmod 4$. Razlikujemo dva slučaja:

1) $n = 2k + 1$. Tada je $n = (k + 1)^2 - k^2$.

2) $n = 4k$. Tada je $n = (k + 1)^2 - (k - 1)^2$. ♢

Primjer 4.5. *Neka je $r(n)$ broj uređenih parova (x, y) cijelih brojeva takvih da je $(x, y) = 1$ i $x^2 + y^2 = n$, te neka je $N(n)$ broj rješenja kongruencije $z^2 \equiv -1 \pmod{n}$.*

a) Dokazati da je $r(n) = 4N(n)$.

b) Neka je $n = \prod_p p^{\alpha(p)}$. Ako je $\alpha(2) = 0$ ili 1, te $\alpha(p) = 0$ za sve $p \equiv 3 \pmod 4$, onda je $r(n) = 2^{t+2}$, gdje je t broj prostih faktora od n oblika $4k+1$. U protivnom je $r(n) = 0$.

c) Ako je p prost broj oblika $4k + 1$, onda je prikaz broja p u obliku $x^2 + y^2$, $x, y \in \mathbb{N}$ jedinstven do na poredak pribrojnika.

Rješenje: a) Neka je $P(n)$ broj prikaza broja n u obliku $x^2 + y^2$, gdje je $(x, y) = 1, x > 0, y \geq 0$. Tada je $r(n) = 4P(n)$. Pokažimo da je $P(n) = N(n)$. Neka je (x, y) par s gornjim svojstvom. Definirajmo $z \in \{0, 1, \ldots, n-1\}$ sa $xz \equiv y \pmod n$. Tada iz $x^2 \equiv -y^2 \pmod n$ slijedi $z^2 \equiv -1 \pmod n$. Treba pokazati da je preslikavanje $(x, y) \mapsto z$ bijekcija.

Pretpostavimo da $(x_1, y_1) \mapsto z$ i $(x_2, y_2) \mapsto z$. Tada iz $x_1y_2z \equiv y_1y_2 \equiv x_2y_1z \pmod n$ slijedi $x_1y_2 \equiv x_2y_1 \pmod n$. No, $x_i^2 \leq n$ i $y_i^2 < n$, pa je $x_i \leq \sqrt{n}$, $y_i < \sqrt{n}$, te $0 \leq x_1y_2 < n$, $0 \leq x_2y_1 < n$. To znači da je $x_1y_2 = x_2y_1$. Odavde slijedi $x_1|x_2$, $x_2|x_1$, tj. $x_1 = x_2$, pa je i $y_1 = y_2$, što dokazuje da je promatrano preslikavanje injekcija.

Neka je sada $z^2 \equiv -1 \pmod n$. Definirajmo $c \in \mathbb{Z}$ sa $(2z)^2 - 4nc = -4$. Tada forma $g(x, y) = nx^2 + 2zxy + cy^2$ ima diskriminantu -4, pa je ekvivalentna s $f(x, y) = x^2 + y^2$. Neka je g dobivena iz f matricom prijelaza $\begin{pmatrix} p & q \\ r & s \end{pmatrix}$. Tada je $n = f(p, r) = p^2 + r^2$, te $z = pq + rs$. Bez smanjenja općenitosti možemo pretpostaviti da je $p > 0$, $q \geq 0$. Budući je

$$pz \equiv p^2q + prs \equiv -r^2q + r(1 - qr) \equiv r \pmod n,$$

vidimo da $(p, q) \mapsto z$, pa je naše preslikavanje surjekcija.

b) Po Kineskom teoremu o ostatcima je $N(n) = \prod_p N(p^{\alpha(p)})$. Očito je $N(2) = 1$ i $N(4) = 0$, pa je $N(2^\alpha) = 0$ za $\alpha \geq 2$. Ako je $p \equiv 3 \pmod 4$, onda je $N(p) = 0$, pa je $N(p^\alpha) = 0$ za $\alpha \geq 1$. Konačno, ako je $p \equiv 1 \pmod 4$, onda je $N(p) = 2$, pa po Henselovoj lemi slijedi da je $N(p^\alpha) = 2$ za sve $\alpha \geq 1$. Prema tome, ako je $\alpha(2) = 0$ ili 1, te $\alpha(p) = 0$ za sve $p \equiv 3 \pmod 4$, onda je $N(n) = 2^t$, pa je $r(n) = 2^{t+2}$.

c) Slijedi iz b), jer je $r(p) = 8$. ♢

Teorem 4.9 (Teorem o četiri kvadrata (Lagrange))**.** *Svaki prirodan broj n može se prikazati u obliku sume kvadrata četiri cijela broja, tj. u obliku $n = x^2 + y^2 + z^2 + w^2$, $x, y, z, w \in \mathbb{Z}$.*

Dokaz: Uočimo da vrijedi identitet

$$\begin{aligned}&(x^2+y^2+z^2+w^2)(a^2+b^2+c^2+d^2)\\&=(ax+by+cz+dw)^2+(ay-bx+dz-cw)^2+(az-cx+bw-dy)^2\\&+(aw-dx+cy-bz)^2.\end{aligned}\tag{13}$$

Stoga je tvrdnju teorema dovoljno provjeriti za proste brojeve. Jasno je da je $2=1^2+1^2+0^2+0^2$, pa pretpostavimo da je p neparan prost broj. Promotrimo brojeve

$$0^2,1^2,2^2,\ldots,\Big(\frac{p-1}{2}\Big)^2.\tag{14}$$

Nikoja dva među njima nisu kongruentna modulo p (vidi Teorem 3.1). Isto vrijedi i za brojeve

$$-1-0^2,-1-1^2,-1-2^2,\ldots,-1-(\frac{p-1}{2})^2.\tag{15}$$

U (14) i (15) imamo ukupno $p+1$ brojeva. Po Dirichletovom principu, dva među njima daju isti ostatak pri dijeljenju sa p. To znači da postoje cijeli brojevi x i y takvi da je $x^2\equiv -1-y^2 \pmod p$ i vrijedi $x^2+y^2+1<1+2\cdot(\frac{p}{2})^2<p^2$. Dakle, dobili smo da je $mp=x^2+y^2+1$ za neki cijeli broj $0<m<p$.

Neka je sada l najmanji prirodan broj takav da je $lp=x^2+y^2+z^2+w^2$ za neke $x,y,z,w\in\mathbb{Z}$. Tada je $l\le m<p$. Nadalje, l je neparan. Naime, ako bi l bio paran, onda bi među brojevima x,y,z,w imali parno mnogo neparnih brojeva, pa bi mogli pretpostaviti da su brojevi $x+y$, $x-y$, $z+w$, $z-w$ parni. Ali tada bi iz

$$\frac{1}{2}lp=\Big(\frac{x+y}{2}\Big)^2+\Big(\frac{x-y}{2}\Big)^2+\Big(\frac{z+w}{2}\Big)^2+\Big(\frac{z-w}{2}\Big)^2$$

dobili kontradikciju s minimalnošću od l.

Da bi dokazali teorem, moramo pokazati da je $l=1$. Stoga pretpostavimo da je $l>1$ i pokušajmo dobiti kontradikciju.

Neka su x',y',z',w' najmanji ostatci po apsolutnoj vrijednosti pri dijeljenju brojeva x,y,z,w s l, te neka je

$$n=x'^2+y'^2+z'^2+w'^2.$$

Tada je $n\equiv 0 \pmod l$ i $n>0$, jer bi inače l dijelio p. Nadalje, budući je l neparan, imamo da je $n<4\cdot(\frac{l}{2})^2=l^2$. Stoga je $n=kl$ za neki cijeli broj k takav da je $0<k<l$.

Iz identiteta (13) slijedi da se broj $(kl)(lp)$ može prikazati kao suma kvadrata četiri cijela broja, i štoviše, svaki od tih kvadrata djeljiv je sa l^2. Odavde slijedi da se broj kp može prikazati kao suma četiri kvadrata, no to je u kontradikciji s minimalnošću od l. □

Metoda koju smo upotrijebili u posljednjem dijelu dokaza Teorema 4.9 naziva se *Fermatova metoda beskonačnog spusta*.

Legendre i Gauss su dokazali da se prirodan broj n može prikazati kao suma tri kvadrata ako i samo ako n nije oblika $4^j(8k+7)$, $j, k \geq 0$. Nužnost, kao što ćemo pokazati u sljedećem primjeru, slijedi iz činjenice da kvadrati daju ostatke 0, 1 ili 4 pri dijeljenju sa 8, dok je dokaz dovoljnosti znatno teži i koristi teoriju ternarnih kvadratnih formi.

Primjer 4.6. *Neka je $n = 4^m(8k+7)$, $m, k \geq 0$. Dokažimo da se n ne može u obliku $x^2 + y^2 + z^2$, $x, y, z \in \mathbb{Z}$.*

Rješenje: Pretpostavimo da tvrdnja nije točna, te da je n najmanji prirodni broj za kojeg tvrdnja ne vrijedi. Tada je

$$n = 4^m(8k + 7) = x^2 + y^2 + z^2.$$

Kvadrat neparnog broja $(2a+1)^2 = 8 \cdot \frac{a(a+1)}{2} + 1$ daje ostatak 1 pri dijeljenju s 8. Ako među brojevima x, y, z ima 1, 2 ili 3 neparna broja, onda je $x^2+y^2+z^2$ oblika $4l + 1$, $4l + 2$ ili $8l + 3$. No, n nema niti jedan od ovih oblika. Stoga su x, y, z svi parni, recimo: $x = 2x_1$, $y = 2y_2$, $z = 2z_1$. Sada je

$$\frac{n}{4} = 4^{m-1}(8k + 7) = x_1^2 + y_1^2 + z_1^2,$$

pa smo dobili kontradikciju s minimalnošću od n. ♢

Zadatak 4.3. *Dokažite da se svaki prirodan broj $n > 169$ može prikazati kao suma kvadrata pet prirodnih brojeva.*

5. Aritmetičke funkcije

Podsjetimo se da za funkciju $f : \mathbb{N} \to \mathbb{C}$ kažemo da je multiplikativna ako je $f(1) = 1$, te ako je $f(mn) = f(m)f(n)$ za $(m, n) = 1$. Jedan primjer multiplikativne funkcije je Eulerova funkcija.

Često uz multiplikativnu funkciju f vežemo funkciju $g(n) = \sum_{d|n} f(d)$. Pokažimo da je g također multiplikativna. Neka je $(m, n) = 1$. Tada je

$$\begin{aligned} g(mn) &= \sum_{d|m} \sum_{d'|n} f(dd') = \sum_{d|m} \sum_{d'|n} f(d)f(d') = \left(\sum_{d|m} f(d) \right) \left(\sum_{d'|n} f(d') \right) \\ &= g(m)g(n). \end{aligned}$$

Definicija 5.1. *Möbiusova funkcija $\mu(n)$, $n \in \mathbb{N}$ je definirana sa*

$$\mu(n) = \begin{cases} 0, & \text{ako } n \text{ nije kvadratno slobodan} \\ (-1)^k, & \text{ako je } n = p_1 p_2 \cdots p_k, \text{ gdje su } p_i \text{ različiti prosti brojevi.} \end{cases}$$

Očito je funkcija μ multiplikativna, pa je i funkcija $\nu(n) = \sum_{d|n} \mu(d)$ također multiplikativna. To znači da je $\nu(1) = 1$, dok je za $n > 1$

$$\begin{aligned} \nu(n) &= \nu(p_1^{\alpha_1} \cdots p_k^{\alpha_k}) = \nu(p_1^{\alpha_1}) \cdots \nu(p_k^{\alpha_k}) \\ &= (\mu(1) + \mu(p_1) + \mu(p_1^2) + \cdots) \cdots (\mu(1) + \mu(p_k) + \mu(p_k^2) + \cdots) \\ &= (1 - 1 + 0 + \cdots) \cdots (1 - 1 + 0 + \cdots) = 0. \end{aligned}$$

Primjer 5.1. *Dokažimo da je $\sum_{n \le x} \mu(n) \left\lfloor \frac{x}{n} \right\rfloor = 1$, te da je $\left| \sum_{n \le x} \frac{\mu(n)}{n} \right| \le 1$.*

Rješenje:

$$\sum_{n \le x} \mu(n) \left\lfloor \frac{x}{n} \right\rfloor = \sum_{n \le x} \mu(n) \sum_{k,\, kn \le x} 1 = \sum_{m \le x} \sum_{n|m} \mu(n) = \sum_{m \le x} \nu(m) = 1.$$

Prema upravo dokazanom je $\sum_{n \le x} \mu(n) \left(\frac{x}{n} - \left\{ \frac{x}{n} \right\} \right) = 1$, pa imamo

$$\begin{aligned} x \cdot \left| \sum_{n \le x} \frac{\mu(n)}{n} \right| &\le 1 + \left| \sum_{n \le x} \mu(n) \left\{ \frac{x}{n} \right\} \right| \le 1 + \sum_{n \le x} \left\{ \frac{x}{n} \right\} \\ &\le 1 + \{x\} + (\lfloor x \rfloor - 1) \cdot 1 = x. \end{aligned}$$

$\diamondsuit$

Teorem 5.1 (Möbiusova formula inverzije)**.** *Neka je $f : \mathbb{N} \to \mathbb{C}$ proizvoljna funkcija, te neka je $F(n) = \sum_{d|n} f(d)$, $n \in \mathbb{N}$. Tada je*

$$f(n) = \sum_{d|n} \mu(d) F(\frac{n}{d}).$$

Obrnuto, ako je $f(n) = \sum_{d|n} \mu(d) F(\frac{n}{d})$ za svaki $n \in \mathbb{Z}$, onda je $F(n) = \sum_{d|n} f(d)$.

Dokaz: Imamo:

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

Da bi dokazali obrat, zapišimo jednakost $f(n) = \sum_{d|n} \mu(d) F(\frac{n}{d})$ u obliku $f(n) = \sum_{d'|n} \mu(\frac{n}{d'}) F(d')$. Sada je

$$\sum_{d|n} f(d) = \sum_{d|n} f(\frac{n}{d}) = \sum_{d|n} \sum_{d'|\frac{n}{d}} \mu(\frac{n}{dd'}) F(d') = \sum_{d'|n} F(d') \nu(\frac{n}{d'}) = F(n).$$

□

Primjenimo li Teorem 5.1 na relaciju $\sum_{d|n} \varphi(d) = n$ (vidi Teorem 2.12), dobivamo

$$\varphi(n) = n \sum_{d|n} \frac{\mu(d)}{d}. \tag{16}$$

Definicija 5.2. *Neka je n prirodan broj. S $\tau(n)$ ćemo označavati broj pozitivnih djelitelja broja n, a sa $\sigma(n)$ sumu svih pozitivnih djelitelja broja n.*

Jasno je da vrijedi $\tau(n) = \sum_{d|n} 1$, $\sigma(n) = \sum_{d|n} d$. Stoga su funkcije τ i σ multiplikativne. Budući da je $\tau(p^j) = j + 1$, $\sigma(p^j) = 1 + p + p^2 + \cdots p^j = \frac{p^{j+1}-1}{p-1}$, dobivamo sljedeće formule za τ i σ:

$$\begin{aligned}\tau(p_1^{\alpha_1} \cdots p_k^{\alpha_k}) &= \prod_{i=1}^{k} (\alpha_i + 1), \\ \sigma(p_1^{\alpha_1} \cdots p_k^{\alpha_k}) &= \prod_{i=1}^{k} \frac{p_i^{\alpha_i+1} - 1}{p_i - 1}.\end{aligned}$$

Primjer 5.2. *Za prirodan broj n kažemo da je* savršen *ako je $\sigma(n) = 2n$, tj. ako je n jednak sumi svojih pravih djelitelja. Npr. 6 i 28 su savršeni brojevi. Nije poznato postoji li iti jedan neparan savršen broj. Dokažimo da je paran broj n savršen ako i samo ako ima oblik $2^{p-1}(2^p - 1)$, gdje su p i $2^p - 1$ prosti brojevi.*

Rješenje: Ako je $n = 2^{p-1}(2^p - 1)$, gdje su p i $2^p - 1$ prosti, onda je

$$\begin{aligned}\sigma(n) &= 1 + 2 + \cdots + 2^{p-1} + (2^p - 1)(1 + 2 + \cdots + 2^{p-1}) \\ &= 2^p - 1 + (2^p - 1)^2 = (2^p - 1) \cdot 2^p = 2n.\end{aligned}$$

Obrnuto, pretpostavimo da je $\sigma(n) = 2n$ i $n = 2^k \cdot m$, gdje su $k, m \in \mathbb{N}$ i m neparan. Iz $\sigma(n) = \sigma(2^k)\sigma(m) = (2^{k+1} - 1)\sigma(m) = 2^{k+1}m$ slijedi da je $\sigma(m) = 2^{k+1} \cdot l$ i $m = (2^{k+1} - 1)l$ za neki $l \in \mathbb{N}$. Ako je $l > 1$, onda je $\sigma(m) \geq l + m + 1 > 2^{k+1}l = \sigma(m)$, što je kontradikcija. Stoga je $l = 1$ i $\sigma(m) = m + 1$, što povlači da je m prost. No, ako je $2^{k+1} - 1$ prost, onda je $k + 1 = p$ također prost, pa je $n = 2^{p-1}(2^p - 1)$. ♢

Zadatak 5.1. *Izračunajte:* $\displaystyle\sum_{d|n} \frac{1}{d}$.

Propozicija 5.2.

1) $\sigma(n) < n(1 + \ln n)$ *za* $n \geq 2$.

2) $\varphi(n) > \frac{1}{4} \cdot \frac{n}{\ln n}$ *za* $n \geq 2$.

Dokaz:

1) Imamo:

$$\sigma(n) = \sum_{d|n} d = \sum_{d|n} \frac{n}{d} \leq n \sum_{d \leq n} \frac{1}{d} < n \cdot \left(1 + \int_1^n \frac{1}{x}\, dx\right) = n(1 + \ln n).$$

2) Funkcija $f(n) = \frac{\sigma(n)\varphi(n)}{n^2}$ je multiplikativna. Nadalje,

$$f(p^j) = \frac{(p^{j+1} - 1)p^{j-1}(p - 1)}{(p - 1)p^{2j}} = 1 - \frac{1}{p^{j+1}} \geq 1 - \frac{1}{p^2},$$

pa je

$$f(n) \geq \prod_{p|n} (1 - \frac{1}{p^2}) \geq \prod_{m=2}^{\infty} (1 - \frac{1}{m^2}) = \frac{1 \cdot 3}{2 \cdot 2} \cdot \frac{2 \cdot 4}{3 \cdot 3} \cdot \frac{3 \cdot 5}{4 \cdot 4} \cdot \frac{4 \cdot 6}{5 \cdot 5} \cdots = \frac{1}{2}.$$

Prema tome, $\sigma(n)\varphi(n) \geq \frac{1}{2}n^2$. Iz 1) slijedi $\sigma(n) < 2n \ln n$ za $n > 2$, odakle je $\varphi(n) > \frac{1}{4} \cdot \frac{n}{\ln n}$. □

Često je od interesa ispitati asimptotsko ponašanje aritmetičkih funkcija, tj. ocijeniti sume oblika $\sum_{n \leq x} f(n)$, gdje je x dovoljno velik realan broj. Mi ćemo to učiniti za funkcije τ, σ i φ. Pritom ćemo rabiti sljedeću oznaku: $f(x) = O(g(x))$ ako postoji konstanta C takva da je $|f(x)| \leq Cg(x)$ za sve x.

Na primjer, budući da je $\lfloor x \rfloor = x - \{x\}$, a $\{x\}$ je omeđena funkcija, možemo pisati: $\lfloor x \rfloor = x + O(1)$. Također, zbog

$$\int_1^{\lfloor x \rfloor} \frac{1}{t}\, dt \leq \sum_{n \leq x} \frac{1}{n} < 1 + \int_1^x \frac{1}{t} dt,$$

tj. $\ln\lfloor x\rfloor \le \sum_{n\le x}\frac{1}{n} < 1+\ln x$, možemo pisati:

$$\sum_{n\le x}\frac{1}{n} = \ln x + O(1).$$

Lema 5.3. *Vrijedi:* $\displaystyle\sum_{n=1}^{\infty}\frac{1}{n^2} = \frac{\pi^2}{6}$.

Dokaz: Pokažimo najprije da za svaki $N\in\mathbb{N}$ vrijedi

$$\sum_{n=1}^{N}\operatorname{ctg}^2\frac{n\pi}{2N+1} = \frac{N(2N-1)}{3}.$$

Iz de Moivreove formule slijedi da je

$$\cos m\vartheta + i\sin m\vartheta = \sin^m\vartheta(\operatorname{ctg}\vartheta + i)^m,$$

pa je

$$\sin(2N+1)\vartheta = \sin^{2N+1}\vartheta\cdot F(\operatorname{ctg}^2\vartheta),$$

gdje je

$$F(x) = \binom{2N+1}{1}x^N - \binom{2N+1}{3}x^{N-1} + \cdots + (-1)^N.$$

Ako je $\vartheta = \frac{n\pi}{2N+1}$, onda je $F(\operatorname{ctg}^2\vartheta) = 0$, pa vidimo da su $\operatorname{ctg}^2\frac{n\pi}{2N+1}$, $n = 1,\dots,N$ upravo korijeni polinoma F. Po Viètеovim fomulama je sada

$$\sum_{n=1}^{N}\operatorname{ctg}^2\frac{n\pi}{2N+1} = \frac{\binom{2N+1}{3}}{\binom{2N+1}{1}} = \frac{N(2N-1)}{3}.$$

Iz $\sin\vartheta < \vartheta < \operatorname{tg}\vartheta$ slijedi $\operatorname{ctg}^2\vartheta < \frac{1}{\vartheta^2} < 1+\operatorname{ctg}^2\vartheta$. Uvrstimo li ovdje $\vartheta = \frac{n\pi}{2N+1}$ i sumiramo, dobivamo

$$\frac{N(2N-1)}{3} < \sum_{n=1}^{N}\frac{(2N+1)^2}{n^2\pi^2} < N + \frac{N(2N-1)}{3}.$$

Odavde je

$$\frac{\pi^2}{3}\cdot\frac{2N^2-N}{4N^2+4N+1} < \sum_{n=1}^{N}\frac{1}{n^2} < \frac{\pi^2}{3}\cdot\frac{2N^2+2N}{4N^2+4N+1},$$

pa za $N\to\infty$ dobivamo $\displaystyle\sum_{n=1}^{\infty}\frac{1}{n^2} = \frac{\pi^2}{6}$. □

Propozicija 5.4.

1) $\sum_{n\le x}\tau(n) = x\ln x + O(x)$

2) $\sum_{n\le x}\sigma(n) = \frac{1}{12}\pi^2 x^2 + O(x\ln x)$

3) $\sum_{n\le x}\varphi(n) = \frac{3}{\pi^2}\cdot x^2 + O(x\ln x)$

Dokaz:

1)

$$\begin{aligned}\sum_{n\le x}\tau(n) &= \sum_{n\le x}\sum_{d|n}1 = \sum_{d\le x}\sum_{m\le\frac{x}{d}}1 = \sum_{d\le x}\Big\lfloor\frac{x}{d}\Big\rfloor = \sum_{d\le x}\Big(\frac{x}{d}+O(1)\Big)\\ &= x\ln x + O(x)\end{aligned}$$

2) Primijetimo da je

$$\sum_{n\le x}\sigma(n) = \sum_{n\le x}\sum_{d|n}\frac{n}{d} = \sum_{d\le x}\sum_{m\le\frac{x}{d}} m.$$

Nadalje je

$$\sum_{m\le\frac{x}{d}} m = \frac{1}{2}\lfloor\frac{x}{d}\rfloor\Big(\Big\lfloor\frac{x}{d}\Big\rfloor+1\Big) = \frac{1}{2}\Big(\frac{x}{d}\Big)^2 + O\Big(\frac{x}{d}\Big).$$

Sada je

$$\sum_{d\le x}\frac{1}{d^2} - \sum_{d=1}^{\infty}\frac{1}{d^2} = O\Big(\int_x^\infty\frac{1}{t^2}\,dt\Big) = O\Big(\frac{1}{x}\Big).$$

Konačno je, po Lemi 5.3, $\sum_{d=1}^{\infty}\frac{1}{d^2} = \frac{\pi^2}{6}$. Napomenimo da se ova formula može takodjer dobiti i iz razvoja u Fourierov red funkcije x^2 na segmentu $[-\pi,\pi]$:

$$x^2 = \frac{\pi^2}{3} + 4\sum_{n=1}^{\infty}(-1)^n\frac{\cos nx}{n^2}.$$

Iz svega gore navedenoga slijedi

$$\begin{aligned}\sum_{n\le x}\sigma(n) &= \sum_{d\le x}\Big[\frac{1}{2}(\frac{x}{d})^2 + O(\frac{x}{d})\Big] = \Big[\frac{\pi^2}{12}x^2 + O(x)\Big] + O(x\ln x)\\ &= \frac{\pi^2}{12}x^2 + O(x\ln x).\end{aligned}$$

3) Prema (16), imamo:

$$\sum_{n\le x}\varphi(n) = \sum_{n\le x}\sum_{d|n}\mu(d)\cdot\frac{n}{d} = \sum_{d\le x}\mu(d)\sum_{m\le\frac{x}{d}} m.$$

Već smo vidjeli da je posljednja suma jednaka $\frac{1}{2}(\frac{x}{d})^2 + O(\frac{x}{d})$. Nadalje je

$$\sum_{d\le x} \frac{\mu(d)}{d^2} = \sum_{d=1}^{\infty} \frac{\mu(d)}{d^2} + O\Big(\frac{1}{x}\Big).$$

Da bi izračunali sumu $\sum_{d=1}^{\infty} \frac{\mu(d)}{d^2}$, pomnožimo je sa $\sum_{d=1}^{\infty} \frac{1}{d^2}$. Dobivamo:

$$\Big(\sum_{d=1}^{\infty} \frac{\mu(d)}{d^2}\Big)\Big(\sum_{d=1}^{\infty} \frac{1}{d^2}\Big) = \sum_{m=1}^{\infty} \frac{1}{m^2} \sum_{d|m} \mu(d) = \sum_{m=1}^{\infty} \frac{\nu(m)}{m^2} = 1.$$

Prema tome, dobili smo da je $\sum_{d=1}^{\infty} \frac{\mu(d)}{d^2} = \frac{6}{\pi^2}$, pa konačno imamo:

$$\sum_{n\le x} \varphi(n) = \sum_{d\le x} \Big[\frac{\mu(d)}{2}\Big(\frac{x}{d}\Big)^2 + O\Big(\frac{x}{d}\Big)\Big] = \frac{3}{\pi^2}x^2 + O(x\ln x).$$

□

Budući da je $\sum_{n\le x} \varphi(n) \sim \frac{3}{\pi^2}x^2$, $\sum_{n\le x} n \sim \frac{1}{2}x^2$, rezultat iz Propozicije 5.4.3) može se interpretirati i tako da kažemo da je vjerojatnost da su dva nasumce izabrana cijela broja relativno prosta jednaka $\frac{6}{\pi^2} \approx 0.6079$.

Zadatak 5.2. Fareyev niz $\mathcal{F}_n$ *reda* n *je niz svih racionalnih brojeva* $\frac{h}{k}$, *gdje su* h *i* k *cijeli brojevi takvi da je* $0 \le h \le k \le n$ *i* $(h,k) = 1$. *Označimo sa* S_n *broj elemenata u nizu* $\mathcal{F}_n$. *Pokažite da je* $S_n \sim \frac{3}{\pi^2}\, n^2$.

Pri ocjenjivanju sume $\sum_{n\le x} F(n)$ korisno je funkciju F prikazati u obliku $F(n) = \sum_{d|n} f(d)$. To se može napraviti npr. pomoću Möbiusove formule inverzije. Tada je

$$\sum_{n\le x} F(n) = \sum_{n\le x}\sum_{d|n} f(d) = \sum_{\substack{d,\ m\\ dm\ \le\ x}} f(d) = \sum_{d\le x} f(d)\Big\lfloor \frac{x}{d}\Big\rfloor$$
$$= x\sum_{d\le x} \frac{f(d)}{d} + O\Big(\sum_{d\le x} |f(d)|\Big).$$

Primjer 5.3. *Dokažimo da vrijedi* $\displaystyle\sum_{n\le x} \frac{\varphi(n)}{n} = \frac{6}{\pi^2}\, x + O(\ln x)$.

Rješenje: Za $F(n) = \frac{\varphi(n)}{n}$ imamo $f(n) = \frac{\mu(n)}{n}$, jer je $\frac{\varphi(n)}{n} = \sum_{d|n} \frac{\mu(d)}{d}$. Sada je

$$x\sum_{d\le x} \frac{f(d)}{d} = x\sum_{d\le x} \frac{\mu(d)}{d^2} = x\sum_{d=1}^{\infty} \frac{\mu(d)}{d^2} - x\sum_{d>x} \frac{\mu(d)}{d^2}\,.$$

Imamo: $\sum_{d=1}^{\infty} \frac{\mu(d)}{d^2} = \frac{6}{\pi^2}$, dok je $x\sum_{d>x} \frac{\mu(d)}{d^2} < x\int_{x-1}^{\infty} \frac{1}{u^2}du = \frac{x}{x-1} = O(1)$. Konačno je $O\Big(\sum_{d\le x} |f(d)|\Big) = O\Big(\sum_{d\le x} \frac{1}{d}\Big) = O(\ln x)$. ♢

Zadatak 5.3. *Dokažite da vrijedi* $\sum_{n\le x}\frac{\sigma(n)}{n}=\frac{\pi^2}{6}\,x+O(\ln x)$.

Sada ćemo promotriti neke funkcije koje su povezane s distribucijom prostih brojeva.

Definicija 5.3. *S* $\pi(x)$ *ćemo označavati broj prostih brojeva* p *takvih da je* $p\le x$. Von Mangoldtova funkcija $\Lambda(n)$, $n\in\mathbb{N}$ *je definirana s* $\Lambda(n)=\ln p$ *ako je* $n=p^k$, $\Lambda(n)=0$ *inače. Stavimo nadalje*

$$\psi(x)=\sum_{n\le x}\Lambda(n),\quad \vartheta(x)=\sum_{p\le x}\ln p,\quad T(x)=\sum_{n\le x}\ln n.$$

Godine 1896. Hadamard i de la Vallée Poussin su dokazali da je $\pi(x)\sim\frac{x}{\ln x}$ kad $x\to\infty$. Mi ćemo dokazati nešto slabiju tvrdnju. Naime pokazat ćemo da postoje pozitivni realni brojevi a i b takvi da je

$$a\frac{x}{\ln x}<\pi(x)<b\frac{x}{\ln x}$$

za dovoljno velike x.

Teorem 5.5.

$$\sum_{d|n}\Lambda(d)=\ln n.$$

Dokaz: Neka je $n=\prod_{i=1}^k p_i^{\alpha_i}$. Tada je $\ln n=\sum_{i=1}^k\alpha_i\ln p_i$. No, $p_i^{\alpha_i}\parallel n$, pa $p_i^e\mid n$ ako i samo ako je e jedan od brojeva $1,2,\dots,\alpha_i$. Stoga je

$$\sum_{i=1}^k\alpha_i\ln p_i=\sum_{i=1}^k\sum_{p_i^e|n}\ln p_i=\sum_{d|n}\Lambda(d).$$

□

Propozicija 5.6. *Za svaki realan broj* $x\ge 1$ *postoji realan broj* α, $|\alpha|\le 1$, *tako da je* $T(x)=x\ln x-x+\alpha\ln ex$.

Dokaz: Izvest ćemo najprije donju ogradu za $T(x)$. Neka je $N=\lfloor x\rfloor$. Budući da je funkcija ln rastuća, vrijedi $\int_{n-1}^n\ln u\,du\le\ln n$, pa dobivamo

$$T(x)=\sum_{n=2}^N\ln n\ge\sum_{n=2}^N\int_{n-1}^n\ln u\,du=\int_1^N\ln u\,du=\int_1^x\ln u\,du-\int_N^x\ln u\,du.$$

Prvi integral je $[u\ln u-u]\Big|_1^x=x\ln x-x$, a drugi je $\le\ln x$. Stoga je

$$T(x)\ge x\ln x-x-\ln x.$$

U izvodu gornje ograde za $T(x)$ krećemo od nejednakosti $\int_n^{n+1} \ln u\, du \geq \ln n$. Odavde je

$$T(x) = \ln N + \sum_{n=1}^{N-1} \ln n \leq \ln x + \sum_{n=1}^{N-1} \int_n^{n+1} \ln u\, du = \ln x + \int_1^N \ln u\, du$$
$$\leq \ln x + \int_1^x \ln u\, du,$$

pa je

$$T(x) = x \ln x - x + 1 + \ln x = x \ln x - x + \ln ex.$$

□

Ako je zadan niz realnih brojeva $\gamma(d)$ takav da je $\gamma(d) = 0$ za $d > D$, onda Propoziciju 5.6 možemo iskoristiti da bi ocijenili sumu

$$\sum_{d \leq D} \gamma(d) T(\frac{x}{d}). \tag{17}$$

Zaista, ova suma je za $x \geq D$ jednaka

$$x(\ln x - 1) \sum_{d \leq D} \frac{\gamma(d)}{d} - x \sum_{d \leq D} \frac{\gamma(d) \ln d}{d} + \alpha \ln ex \sum_{d \leq D} |\gamma(d)|,$$

gdje α zadovoljava $|\alpha| \leq 1$. Da bi eliminirali prvi član, ograničit ćemo se na nizove za koje vrijedi

$$\sum_{d \leq D} \frac{\gamma(d)}{d} = 0. \tag{18}$$

Neka je

$$N(y) = \sum_{d \leq D} \gamma(d) \lfloor \frac{y}{d} \rfloor. \tag{19}$$

Tada je

$$\sum_{d \leq D} \gamma(d) T(\frac{x}{d}) = \sum_{d=1}^{D} \gamma(d) \sum_{n \leq \frac{x}{d}} \ln n = \sum_{\substack{d,\, n \\ dn \,\leq\, x}} \gamma(d) \sum_{r \mid n} \Lambda(r) =$$
$$\sum_{\substack{d,\, r,\, m \\ drm \,\leq\, x}} \gamma(d) \Lambda(r) = \sum_{r \leq x} \Lambda(r) \sum_{d \leq \frac{x}{r}} \sum_{m \leq \frac{x}{rd}} 1 = \sum_{r \leq x} \Lambda(r) N(\frac{x}{r}).$$

Uvrstimo li $\lfloor \frac{y}{d} \rfloor = \frac{y}{d} - \{\frac{y}{d}\}$ u (19), te uvažimo (18), dobivamo da je

$$N(y) = -\sum_{d \leq D} \gamma(d) \{\frac{y}{d}\}.$$

Budući da je funkcija $\{\frac{y}{d}\}$ peridična s periodom d, zaključujemo da je funkcija $N(y)$ periodična s periodom q, gdje je q najmanji zajednički višekratnik onih brojeva d za koje je $\gamma(d) \neq 0$.

Mi ćemo izabrati $\gamma(d)$ tako da brojevi $N(\frac{x}{r})$ budu blizu jedinice, što će značiti da je suma (17) bliska funkciji $\psi(x)$.

Do sada smo dokazali

$$\sum_{r\leq x} \Lambda(r) N(\frac{x}{r}) = -x \sum_{d\leq D} \frac{\gamma(d)\ln d}{d} + \alpha \ln ex \sum_{d\leq D} |\gamma(d)|, \tag{20}$$

za $x \geq D$.

Teorem 5.7. *Neka je* $a_0 = \frac{1}{3}\ln 2 + \frac{1}{2}\ln 3 \approx 0.7804$, $b_0 = \frac{3}{2}a_0 \approx 1.1705$. *Ako je* $a < a_0$ *i* $b > b_0$, *onda postoji realan broj* x_0 *(koji ovisi o* a *i* b*) takav da je*

$$ax < \psi(x) < bx$$

za sve $x > x_0$.

Dokaz: Izaberimo $\gamma(1) = 1$, $\gamma(2) = -1$, $\gamma(3) = -2$, $\gamma(6) = 1$, te $\gamma(d) = 0$ inače. Lako se provjeri da je sada (18) zadovoljeno. Nadalje, $N(y)$ ima period jednak 6, a iz (19) vidimo da je

$$N(y) = \begin{cases} 0, \text{ za } 0 \leq y < 1 \\ 1, \text{ za } 1 \leq y < 3 \\ 0, \text{ za } 3 \leq y < 5 \\ 1, \text{ za } 5 \leq y < 6. \end{cases}$$

Budući da je $N(y) \leq 1$ za sve y, lijeva strana od (20) je $\leq \psi(x)$. Stoga iz (20) dobivamo ocjenu

$$\psi(x) \geq a_0 x - 5\ln ex$$

za $x \geq 6$. Stoga je $\psi(x) > ax$ za sve dovoljno velike x ako je $a < a_0$.

Da bi dobili gornju ogradu za $\psi(x)$, uočimo da je $N(y) \geq 0$ za sve y, te da je $N(y) = 1$ za $1 \leq y < 3$. Stoga je lijeva strana od (20) $\geq \sum_{\frac{x}{3}<n\leq x} \Lambda(n) = \psi(x) - \psi(\frac{x}{3})$. Dakle,

$$\psi(x) - \psi(\frac{x}{3}) \leq a_0 x + 5\ln ex$$

za $x \geq 6$. Direktnim uvrštavanjem vidi se da formula vrijedi i za $1 \leq x \leq 6$. Neka je 3^K najveća potencija od 3 koja je $\leq x$. Tada imamo

$$\psi(x) = \sum_{k=0}^{K} \Big[\psi\Big(\frac{x}{3^k}\Big) - \psi\Big(\frac{x}{3^{k-1}}\Big)\Big] \leq \sum_{k=0}^{K} (a_0 \frac{x}{3^k} + 5\ln ex).$$

Budući da je $\sum_{k=0}^{\infty} \frac{1}{3^k} = \frac{3}{2}$ i $K = \lfloor \frac{\ln x}{\ln 3} \rfloor < \ln x$, zaključujemo da je

$$\psi(x) < b_0 x + 5(\ln ex)^2$$

za $x \geq 1$. Stoga, ako je $b > b_0$, onda je $\psi(x) < bx$ za sve dovoljno velike x. □

Teorem 5.8. *Za $x \geq 1$ vrijedi: $\vartheta(x) = \psi(x) + O(\sqrt{x})$.*

Dokaz: Iz definicije je $\vartheta(x) \leq \psi(x)$ za sve x. Dakle, moramo još naći donju ogradu za razliku $\psi(x) - \vartheta(x)$. Imamo:

$$\psi(x) = \sum_{n \leq x} \Lambda(x) = \sum_{p^k \leq x} \ln p = \sum_k \sum_{p \leq \sqrt[k]{x}} \ln p = \sum_k \vartheta(\sqrt[k]{x}).$$

Stavimo $K = \lfloor \frac{\ln x}{\ln 2} \rfloor$. Ako je $k > K$, onda je $\sqrt[k]{x} < 2$, pa je $\vartheta(\sqrt[k]{x}) = 0$. Stoga je

$$\psi(x) - \vartheta(x) = \sum_{2 \leq k \leq K} \vartheta(\sqrt[k]{x}) \leq \sum_{2 \leq k \leq K} \psi(\sqrt[k]{x}) = \sum_{2 \leq k \leq K} O(\sqrt[k]{x}),$$

po Teoremu 5.7. Konstanta u O ne ovisi o k, a članovi u sumi opadaju. Zato je

$$\psi(x) - \vartheta(x) = O(\sqrt{x} + K\sqrt[3]{x}) = O(\sqrt{x} + \sqrt[3]{x} \ln x) = O(\sqrt{x}).$$

□

Teorem 5.9. *Za $x \geq 2$ vrijedi:*

$$\pi(x) = \frac{\theta(x)}{\ln x} + O\Big(\frac{x}{\ln^2 x}\Big).$$

Dokaz: Pokažimo najprije da za $x \geq 2$ vrijedi

$$\pi(x) = \frac{\theta(x)}{\ln x} + \int_2^x \frac{\vartheta(u)}{u \ln^2 u}\, du. \tag{21}$$

Zaista,

$$\int_2^x \frac{\vartheta(u)}{u \ln^2 u}\, du = \int_2^x (\sum_{p \leq n} \ln p) u^{-1} \ln^{-2} u\, du = \sum_{p \leq x} \ln p \int_p^x u^{-1} \ln^{-2} u\, du =$$
$$= \sum_{p \leq x} \ln p \Big(\frac{1}{\ln p} - \frac{1}{\ln x}\Big) = \pi(x) - \frac{\vartheta(x)}{\ln x}.$$

Budući da je $0 \leq \vartheta(x) \leq \psi(x)$, iz Teorema 5.7 slijedi da je $\vartheta(x) = O(x)$. Zato je integral u (21) $O(\int_2^x \ln^{-2} u\, du)$. Rastavimo područje integracije na dva dijela: $2 \leq u \leq \sqrt{x}$ i $\sqrt{x} \leq u \leq x$. Na prvom dijelu, podintegralna funkcija je omeđena, pa je doprinos tog dijela $O(\sqrt{x})$. Na drugom dijelu, podintegralna funkcija je $\leq \frac{4}{\ln^2 x}$, pa je doprinos drugog dijela $O(\frac{x}{\ln^2 x})$. □

Teorem 5.10. *Neka su brojevi a_0 i b_0 kao u Teoremu 5.7. Ako je $a < a_0$ i $b > b_0$, onda nejednakost*

$$a\frac{x}{\ln x} < \pi(x) < b\frac{x}{\ln x} \tag{22}$$

vrijedi za sve dovoljno velike x.

Dokaz: Koristeći Teoreme 5.9, 5.8 i 5.7, imamo:

$$\pi(x) = \frac{\vartheta(x)}{\ln x} + O\Big(\frac{x}{\ln^2 x}\Big) = \frac{\psi(x)}{\ln x} + O\Big(\frac{x}{\ln^2 x}\Big) \le b_0 \frac{x}{\ln x} + O\Big(\frac{x}{\ln^2 x}\Big).$$

To daje gornju ogradu u (22) za dovoljno velike x ako je $b > b_0$. Slično se dobiva

$$\pi(x) \ge a_0 \frac{x}{\ln x} + O\Big(\frac{x}{\ln^2 x}\Big),$$

što daje donju ogradu u (22) za dovoljno velike x. □

Primjer 5.4. *Dokažimo da vrijedi* $\displaystyle\sum_{n\le x} \frac{\Lambda(n)}{n} = \ln x + O(1)$.

Rješenje: Neka je $T(x) = \sum_{n\le x} \ln n$. Znamo da je $T(x) = x \ln x + O(x)$. Iz $\sum_{d|n} \Lambda(d) = \ln n$ slijedi:

$$\begin{aligned} T(x) &= \sum_{n\le x} \sum_{d|n} \Lambda(d) = x \sum_{d\le x} \frac{\Lambda(d)}{d} + O\Big(\sum_{d\le x} \Lambda(d)\Big) \\ &= x \sum_{d\le x} \frac{\Lambda(d)}{d} + O(\psi(x)). \end{aligned}$$

Dijeljenjem sa x dobivamo $\displaystyle\sum_{d\le x} \frac{\Lambda(d)}{d} = \ln x + O(1)$. ♢

Zadatak 5.4. *Dokažite da je* $\displaystyle\sum_{p\le x} \frac{\ln p}{p} = \ln x + O(1)$.

Riemannova zeta fukcija je definirana sa $\zeta(s) = \displaystyle\sum_{n=1}^{\infty} \frac{1}{n^s}$, gdje je $s \in \mathbb{C}$ i $\operatorname{Re} s > 1$ (da bi red bio konvergentan). U Lemi 5.3 smo pokazali da je $\zeta(2) = \frac{\pi^2}{6}$. Osnovnu vezu između Riemannove zeta funkcije i prostih brojeva daje tzv. *Eulerova produktna formula*:

$$\zeta(s) = \prod_p \Big(1 - \frac{1}{p^s}\Big)^{-1}.$$

Skicirajmo dokaz ove formule. Za $N \in \mathbb{N}$ imamo:

$$\prod_{p\le N} \Big(1 - \frac{1}{p^s}\Big)^{-1} = \prod_{p\le N} (1 + p^{-s} + p^{-2s} + \cdots) = \sum\nolimits'_m m^{-s},$$

gdje suma ide po svim $m \in \mathbb{N}$ koji su djeljivi samo s prostim brojevima $\le N$. Budući da

$$\Big|\sum\nolimits'_m m^{-s} - \sum_{n\le N} n^{-s}\Big| \le \sum_{n>N} n^{-\operatorname{Re} s} \to 0$$

za $N \to \infty$, dobivamo traženu formulu.

Zadatak 5.5. *Dokažite da vrijedi* $\displaystyle\sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} = \frac{1}{\zeta(s)}$.

6. Diofantske aproksimacije

Za dani realni broj α s $\{\alpha\}$ ćemo označavati razlomljeni dio od α, tj. $\{\alpha\} = \alpha - \lfloor\alpha\rfloor$, a sa $\|\alpha\|$ označavat ćemo udaljenost od α do najbližeg cijelog broja, tj. $\|\alpha\| = \min(\{\alpha\}, 1-\{\alpha\})$. Očito je $0 \leq \{\alpha\} < 1$ i $0 \leq \|\alpha\| \leq \frac{1}{2}$.

Teorem 6.1 (Dirichlet)**.** *Neka su α i Q realni brojevi i $Q > 1$. Tada postoje cijeli brojevi p, q takvi da je $1 \leq q < Q$ i $\|\alpha q\| = |\alpha q - p| \leq \frac{1}{Q}$.*

Dokaz: Pretpostavimo najprije da je Q prirodan broj. Promotrimo sljedećih $Q+1$ brojeva:

$$0, 1, \{\alpha\}, \{2\alpha\}, \ldots, \{(Q-1)\alpha\}.$$

Svi ovi brojevi leže na segmentu $[0,1]$. Podijelimo segment $[0,1]$ na Q disjunktnih podintervala duljine $\frac{1}{Q}$:

$$[0, \frac{1}{Q}\rangle,\ [\frac{1}{Q}, \frac{2}{Q}\rangle,\ [\frac{2}{Q}, \frac{3}{Q}\rangle,\ \ldots,\ [\frac{Q-1}{Q}, 1].$$

Prema Dirichletovom principu, barem jedan podinterval sadrži dva (ili više) od gornjih $Q+1$ brojeva. Uočimo da broj $\{r\alpha\}$ ima oblik $r\alpha - s$, $r, s \in \mathbb{Z}$, a brojevi 0 i 1 se također mogu zapisati u tom obliku (uz $r = 0$). Dakle, postoje cijeli brojevi r_1, r_2, s_1, s_2 takvi da je $0 \leq r_i < Q$, $i = 1, 2$, $r_1 \neq r_2$ i da vrijedi

$$|(r_1\alpha - s_1) - (r_2\alpha - s_2)| \leq \frac{1}{Q}.$$

Možemo pretpostaviti da je $r_1 > r_2$. Stavimo: $q = r_1 - r_2$, $p = s_1 - s_2$. Tada je $1 \leq q < Q$ i $|\alpha q - p| \leq \frac{1}{Q}$, čime je tvrdnja teorema dokazana u slučaju $Q \in \mathbb{N}$.

Pretpostavimo sada da Q nije prirodan broj. Neka je $Q' = \lfloor Q\rfloor + 1$. Prema prije dokazanom, postoje cijeli brojevi p, q takvi da je $1 \leq q < Q'$ i $|\alpha q - p| \leq \frac{1}{Q'}$. No sada je $|\alpha q - p| < \frac{1}{Q}$, a $1 \leq q < Q'$ povlači da je $1 \leq q \leq \lfloor Q\rfloor$, odnosno $1 \leq q < Q$. □

Korolar 6.2. *Ako je α iracionalan broj, onda postoji beskonačno mnogo parova p, q relativno prostih cijelih brojeva takvih da je*

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}. \tag{23}$$

Dokaz: Tvrdnja Teorema 6.1 očito vrijedi i ukoliko zahtjevamo da su p i q relativno prosti. Dakle, za $Q > 1$ postoje relativno prosti cijeli brojevi p, q takvi da je $|\alpha - \frac{p}{q}| \leq \frac{1}{Qq} < \frac{1}{q^2}$. Budući da je α iracionalan, to je $\alpha q - p \neq 0$.

Pretpostavimo da postoji samo konačno mnogo racionalnih brojeva $\frac{p}{q}$ koji zadovoljavaju (23). Neka su to brojevi $\frac{p_j}{q_j}$, $j = 1, \ldots, n$. Izaberimo prirodan broj m tako da je $\frac{1}{m} < |\alpha q_j - p_j|$ za sve $j = 1, \ldots, n$. Primijenimo sada Teorem 6.1 uz $Q = m$, pa dobivamo racionalan broj $\frac{p}{q}$ koji zadovoljava (23) i za koji vrijedi $|\alpha q - p| \leq \frac{1}{m}$. Prema tome, $\frac{p}{q}$ je različit od $\frac{p_1}{q_1}, \ldots, \frac{p_n}{q_n}$, što je kontradikcija. □

Napomena 6.1. *Tvrdnja Korolara 6.2 ne vrijedi ukoliko je α racionalan. Zaista, neka je $\alpha = \frac{u}{v}$. Ako je $\frac{p}{q} \neq \alpha$, onda je*

$$|\alpha - \frac{p}{q}| = |\frac{u}{v} - \frac{p}{q}| = |\frac{uq - vp}{vq}| \geq \frac{1}{vq},$$

pa (23) povlači da je $q < v$. To znači da (23) može biti zadovoljeno samo za konačno parova p, q relativno prostih cijelih brojeva.

Neka je α proizvoljan realan broj. Stavimo: $a_0 = \lfloor \alpha \rfloor$. Ako je $a_0 \neq \alpha$, onda zapišimo α u obliku $\alpha = a_0 + \frac{1}{\alpha_1}$, tako da je $\alpha_1 > 1$, i stavimo $a_1 = \lfloor \alpha_1 \rfloor$. Ako je $a_1 \neq \alpha_1$, onda α_1 zapišimo u obliku $\alpha_1 = a_1 + \frac{1}{\alpha_2}$, tako da je $\alpha_2 > 1$, i stavimo $a_2 = \lfloor \alpha_2 \rfloor$. Ovaj proces možemo nastaviti u nedogled, ukoliko nije $a_n = \alpha_n$ za neki n. Jasno je da ako je $a_n = \alpha_n$ za neki n, onda je α racionalan broj. Naime, tada je

$$\alpha = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots + \cfrac{1}{a_n}}}, \tag{24}$$

Ovo ćemo kraće zapisivati u obliku $\alpha = [a_0, a_1, \ldots, a_n]$.

Pretpostavimo sada da je $a_n \neq \alpha_n$ za sve n. Definirajmo racionalne brojeve $\frac{p_n}{q_n}$ sa

$$\frac{p_n}{q_n} = [a_0, a_1, \ldots, a_n].$$

Teorem 6.3. *Brojevi p_n, q_n zadovoljavaju rekurzije*

$$\begin{aligned} p_n &= a_n p_{n-1} + p_{n-2}, \quad p_0 = a_0, \quad p_1 = a_0 a_1 + 1; \\ q_n &= a_n q_{n-1} + q_{n-2}, \quad q_0 = 1, \quad q_1 = a_1. \end{aligned}$$

Dokaz: Za $n = 2$ tvrdnja se provjerava direktno. Pretpostavimo da je $n > 2$ i da tvrdnja vrijedi za $n-1$. Definirajmo brojeve p'_j, q'_j sa $\frac{p'_j}{q'_j} = [a_1, a_2, \ldots, a_{j+1}]$. Tada je

$$p'_{n-1} = a_n p'_{n-2} + p'_{n-3}, \quad q'_{n-1} = a_n q'_{n-2} + q'_{n-3}.$$

No,

$$\frac{p_j}{q_j} = a_0 + \frac{1}{[a_1, \ldots, a_j]} = a_0 + \frac{q'_{j-1}}{p'_{j-1}} = \frac{a_0 p'_{j-1} + q'_{j-1}}{p'_{j-1}}.$$

Stoga je $p_j = a_0 p'_{j-1} + q'_{j-1}$, $q_j = p'_{j-1}$. Prema tome,

$$\begin{aligned} p_n &= a_0(a_n p'_{n-2} + p'_{n-3}) + (a_n q'_{n-2} + q'_{n-3}) \\ &= a_n(a_0 p'_{n-2} + q'_{n-2}) + (a_0 p'_{n-3} + q'_{n-3}) = a_n p_{n-1} + p_{n-2}, \\ q_n &= a_n p'_{n-2} + p'_{n-3} = a_n q_{n-1} + q_{n-2}. \end{aligned}$$

□

Dogovorno uzimamo da je $p_{-2} = 0$, $p_{-1} = 1$, $q_{-2} = 1$, $q_{-1} = 0$. Lako se provjerava da uz ovaj dogovor Teorem 6.3 vrijedi za sve $n \geq 0$.

Teorem 6.4. *Za sve $n \geq -1$ vrijedi: $q_n p_{n-1} - p_n q_{n-1} = (-1)^n$.*

Dokaz: Teorem dokazujemo indukcijom. Za $n = -1$ imamo: $q_{-1}p_{-2} - p_{-1}q_{-2} = 0 \cdot 0 - 1 \cdot 1 = (-1)^{-1}$. Pretpostavimo da tvrdnja vrijedi za $n-1$. Tada je

$$\begin{aligned} q_n p_{n-1} - p_n q_{n-1} &= (a_n q_{n-1} + q_{n-2}) p_{n-1} - (a_n p_{n-1} + p_{n-2}) q_{n-1} \\ &= -(q_{n-1} p_{n-2} - p_{n-1} q_{n-2}) = -(-1)^{n-1} = (-1)^n. \end{aligned}$$

□

Korolar 6.5. *Brojevi p_n i q_n su relativno prosti.*

Teorem 6.6.

1) $\frac{p_0}{q_0} < \frac{p_2}{q_2} < \frac{p_4}{q_4} < \cdots$,

2) $\frac{p_1}{q_1} > \frac{p_3}{q_3} > \frac{p_5}{q_5} > \cdots$,

3) Ako je n paran, a m neparan, onda je $\frac{p_n}{q_n} < \frac{p_m}{q_m}$.

Dokaz: Iz Teorema 6.3 i 6.4 je

$$\begin{aligned} \frac{p_{n-2}}{q_{n-2}} - \frac{p_n}{q_n} &= \frac{p_{n-2}(a_n q_{n-1} + q_{n-2}) - (a_n p_{n-1} + p_{n-2}) q_{n-2}}{q_n q_{n-2}} \\ &= \frac{(-1)^{n-1} a_n}{q_n q_{n-2}}. \end{aligned} \tag{25}$$

Primijenimo li (25) za n paran, dobivamo $\frac{p_{n-2}}{q_{n-2}} < \frac{p_n}{q_n}$, a za n neparan dobivamo $\frac{p_{n-2}}{q_{n-2}} > \frac{p_n}{q_n}$.

Preostaje dokazati tvrdnju 3). Neka je $n < m$. Budući da je $\frac{p_n}{q_n} \leq \frac{p_{m-1}}{q_{m-1}}$, dovoljno je dokazati da je $\frac{p_{m-1}}{q_{m-1}} < \frac{p_m}{q_m}$. No, zadnja nejednakost je točna jer je, po Teoremu 6.4, $q_m p_{m-1} - p_m q_{m-1} = (-1)^m = -1 < 0$. Slučaj $n > m$ se dokazuje sasvim analogno. □

Teorem 6.7.

$$\lim_{n\to\infty} \frac{p_n}{q_n} = \alpha$$

Dokaz: Budući da je $\frac{p_0}{q_0} < \frac{p_2}{q_2} < \cdots < \frac{p_1}{q_1}$, to $\lim\limits_{\substack{n\to\infty \\ n \text{ paran}}} \frac{p_n}{q_n}$ postoji. Iz sličnog razloga postoji i $\lim\limits_{\substack{n\to\infty \\ n \text{ neparan}}} \frac{p_n}{q_n}$. Ali ova dva limesa su jednaka jer je $\frac{p_{n-1}}{q_{n-1}} - \frac{p_n}{q_n} = \frac{(-1)^n}{q_{n-1}q_n}$ i zbog $q_n \geq n$ je $\lim_{n\to\infty} \frac{(-1)^n}{q_{n-1}q_n} = 0$. Neka je $\vartheta = \lim_{n\to\infty} \frac{p_n}{q_n}$.

Iz definicije brojeva $\alpha_1, \alpha_2, \ldots$ slijedi da je $\alpha = [a_0, a_1, \ldots, a_n, \alpha_{n+1}]$, gdje je $0 < \frac{1}{\alpha_{n+1}} \leq \frac{1}{a_{n+1}}$. To znači da α leži između brojeva $\frac{p_n}{q_n}$ i $\frac{p_{n+1}}{q_{n+1}}$. Prema Teoremu 6.6, to znači da je $\frac{p_n}{q_n} < \alpha < \frac{p_{n+1}}{q_{n+1}}$ za n paran i $\frac{p_{n+1}}{q_{n+1}} < \alpha < \frac{p_n}{q_n}$ za n neparan. Dakle, $\alpha = \vartheta$. □

Sada možemo zaključiti da ako je α racionalan, onda je $a_n = \alpha_n$ za neki n. Zaista, u protivnom bi, zbog toga što α leži između $\frac{p_n}{q_n}$ i $\frac{p_{n+1}}{q_{n+1}}$, imali

$$\left|\alpha - \frac{p_n}{q_n}\right| < \left|\frac{p_{n+1}}{q_{n+1}} - \frac{p_n}{q_n}\right| = \frac{1}{q_{n+1}q_n} < \frac{1}{q_n^2} \tag{26}$$

za svaki n. To bi značilo da postoji beskonačno mnogo racionalnih brojeva $\frac{p}{q}$ takvih da je $|\alpha - \frac{p}{q}| < \frac{1}{q^2}$, što je u suprotnosti s Napomenom 6.1.

Definicija 6.1. *Ako je a_0 cijeli broj, $a_1, \ldots, a_n$ prirodni brojevi, te ako je $\alpha = [a_0, a_1, \ldots, a_n]$, onda ovaj izraz zovemo razvoj broja α u* konačni jednostavni verižni (neprekidni) razlomak*; $\frac{p_i}{q_i} = [a_0, \ldots, a_i]$ je i-ta* konvergenta *od α, a_i je i-ti* parcijalni kvocijent *od α, a $\alpha_i = [a_i, a_{i+1}, \ldots, a_n]$ je i-ti* potpuni kvocijent *od α.*

Ako je α iracionalan broj, onda uvodimo oznaku $\lim\limits_{n\to\infty} [a_0, a_1, \ldots, a_n] = [a_0, a_1, a_2, \ldots]$. Ako je $\alpha = [a_0, a_1, a_2, \ldots]$, onda ovaj izraz zovemo razvoj od α u (beskonačni) jednostavni verižni razlomak*; $\frac{p_i}{q_i} = [a_0, \ldots, a_i]$ je i-ta* konvergenta *od α, a_i je i-ti* parcijalni kvocijent*, a $\alpha_i = [a_i, a_{i+1}, \ldots]$ je i-ti* potpuni kvocijent *od α.*

Primjer 6.1. *Dokažimo da nazivnici q_n u konvergentama razvoja u jednostavni verižni razlomak iracionalnog broja α zadovoljavaju nejednakost $q_n \geq F_n$, gdje F_n označava n-ti Fibonaccijev broj.*

Rješenje: Najprije imamo da je $q_0 = 1 > F_0$ i $q_1 = a_1 \geq 1 = F_1$. Pretpostavimo da je $q_{n-2} \geq F_{n-2}$ i $q_{n-1} \geq F_{n-1}$. Tada je

$$q_n = a_n q_{n-1} + q_{n-2} \geq q_{n-1} + q_{n-2} \geq F_{n-1} + F_{n-2} = F_n.$$

♢

Zadatak 6.1. *Izračunajte prve četiri konvergente* $\frac{p_o}{q_o}$, $\frac{p_1}{q_1}$, $\frac{p_2}{q_2}$, $\frac{p_3}{q_3}$ *u razvoju broja* $\pi = 3.1415926\cdots$ *u jednostavni verižni razlomak.*

Neka je $\frac{b}{c}$ racionalan broj, $(b, c) = 1$ i $b > c > 0$. Primijenimo na njega Euklidov algoritam:

$$b = cq_1 + r_1,\ c = r_1 q_2 + r_2,\ \cdots,\ r_{j-1} = r_j q_{j+1}.$$

Tada je

$$\frac{b}{c} = q_1 + \frac{1}{\frac{c}{r_1}} = q_1 + \frac{1}{q_2 + \frac{1}{\frac{r_1}{r_2}}} = \cdots = [q_1, q_2, \ldots, q_{j+1}].$$

Primjer 6.2. *Razvijmo broj* $\frac{41}{47}$ *u jednostavni verižni razlomak.*

Rješenje:

$$\begin{aligned} 47 &= 41 \cdot 1 + 6 \\ 41 &= 6 \cdot 6 + 5 \\ 6 &= 5 \cdot 1 + 1 \\ 5 &= 1 \cdot 5 \end{aligned}$$

Odavde je $\frac{47}{41} = [1, 6, 1, 5]$, pa je $\frac{41}{47} = [0, 1, 6, 1, 5]$. ♢

Zadatak 6.2. *Razvijte u jednostavni verižni razlomak brojeve* $\frac{3}{17}$ *i* $\frac{101}{11}$.

Neka je α iracionalan broj. Prema formuli (26) svaka konvergenta od α zadovoljava nejednakost $|\alpha - \frac{p}{q}| < \frac{1}{q^2}$.

Teorem 6.8. *Neka su* $\frac{p_{n-1}}{q_{n-1}}$ *i* $\frac{p_n}{q_n}$ *dvije uzastopne konvergente od* α. *Tada barem jedna od njih zadovoljava nejednakost*

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{2q^2}.$$

Dokaz: Brojevi $\alpha - \frac{p_n}{q_n}$, $\alpha - \frac{p_{n-1}}{q_{n-1}}$ imaju suprotni predznak, pa je

$$\left|\alpha - \frac{p_n}{q_n}\right| + \left|\alpha - \frac{p_{n-1}}{q_{n-1}}\right| = \left|\frac{p_n}{q_n} - \frac{p_{n-1}}{q_{n-1}}\right| = \frac{1}{q_n q_{n-1}} < \frac{1}{2q_n^2} + \frac{1}{2q_{n-1}^2}$$

(jer je $2ab < a^2 + b^2$ za $a \neq b$). Prema tome, vrijedi

$$\left|\alpha - \frac{p_n}{q_n}\right| < \frac{1}{2q_n^2} \quad \text{ili} \quad \left|\alpha - \frac{p_{n-1}}{q_{n-1}}\right| < \frac{1}{2q_{n-1}^2}.$$

□

Teorem 6.9 (Borel)**.** *Neka su* $\frac{p_{n-2}}{q_{n-2}}$, $\frac{p_{n-1}}{q_{n-1}}$, $\frac{p_n}{q_n}$ *tri uzastopne konvergente od* α*. Tada barem jedna od njih zadovoljava nejednakost*

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{\sqrt{5}q^2}.$$

Dokaz: Stavimo $\alpha = [a_0, a_1, \dots]$, $\alpha_i = [a_i, a_{i+1}, \dots]$ i $\beta_i = \frac{q_{i-2}}{q_{i-1}}$ za $i \geq 1$. Imamo $\alpha = [a_0, a_1, \dots, a_n, \alpha_{n+1}]$, pa je

$$q_n\alpha - p_n = q_n \cdot \frac{\alpha_{n+1}p_n + p_{n-1}}{\alpha_{n+1}q_n + q_{n-1}} - p_n = \frac{(-1)^n}{\alpha_{n+1}q_n + q_{n-1}}. \tag{27}$$

Stoga je

$$\left|\alpha - \frac{p_n}{q_n}\right| = \frac{1}{q_n^2(\alpha_{n+1} + \beta_{n+1})}. \tag{28}$$

Da bi dovršili dokaz, moramo pokazati da ne postoji prirodan broj n takav da za $i = n-1, n, n+1$ vrijedi

$$\alpha_i + \beta_i \leq \sqrt{5}. \tag{29}$$

Pretpostavimo da je (29) ispunjeno za $i = n-1, n$. Tada iz

$$\alpha_{n-1} = a_{n-1} + \frac{1}{\alpha_n}, \quad \frac{1}{\beta_n} = \frac{q_{n-1}}{q_{n-2}} = a_{n-1} + \frac{q_{n-3}}{q_{n-2}} = a_{n-1} + \beta_{n-1}$$

slijedi

$$\frac{1}{\alpha_n} + \frac{1}{\beta_n} = \alpha_{n-1} + \beta_{n-1} \leq \sqrt{5}.$$

Stoga je $1 = \alpha_n \cdot \frac{1}{\alpha_n} \leq (\sqrt{5} - \beta_n)(\sqrt{5} - \frac{1}{\beta_n})$, što je ekvivalentno sa $\beta_n^2 - \sqrt{5}\beta_n + 1 \leq 0$. Odavde slijedi da je $\beta_n \geq \frac{\sqrt{5}-1}{2}$, odnosno, budući da je β_n racionalan, $\beta_n > \frac{\sqrt{5}-1}{2}$.

Ako bi (29) također bilo ispunjeno za $i = n, n+1$, onda bi bilo $\beta_{n+1} > \frac{\sqrt{5}-1}{2}$, pa bi dobili da je

$$1 \leq a_n = \frac{q_n}{q_{n-1}} - \frac{q_{n-2}}{q_n} = \frac{1}{\beta_{n+1}} - \beta_n < \frac{2}{\sqrt{5}-1} - \frac{\sqrt{5}-1}{2} = 1,$$

što je kontradikcija. □

Primjer 6.3. *Neka je* $\alpha = [1, 1, 1, \dots]$*. Tada iz* $\alpha = 1 + \frac{1}{[1,1,1,\dots]} = 1 + \frac{1}{\alpha}$ *slijedi* $\alpha^2 - \alpha - 1 = 0$*, pa iz* $\alpha \geq 1$ *dobivamo* $\alpha = \frac{\sqrt{5}+1}{2}$*.*

Konvergente $\frac{p_n}{q_n}$ *zadovoljavaju rekurzije*

$$\begin{aligned} p_n &= p_{n-1} + p_{n-2}, \quad p_0 = 1, \quad p_1 = 2, \\ q_n &= q_{n-1} + q_{n-2}, \quad q_0 = 1, \quad q_1 = 1. \end{aligned}$$

Prema tome je $p_n = F_{n+2}$*,* $q_n = F_{n+1}$*, gdje je* (F_n) *niz Fibonaccijevih brojeva.*

♢

Teorem 6.10. *Pretpostavimo da α ima razvoj u verižni razlomak oblika*

$$\alpha = [a_0, a_1, \dots, a_N, 1, 1, 1, \dots].$$

Tada je $\lim_{n\to\infty} \left|\alpha - \frac{p_n}{q_n}\right| = \frac{1}{\sqrt{5}}$.

Dokaz: Uz oznake iz dokaza Teoreme 6.9, imamo:

$$\left|\alpha - \frac{p_n}{q_n}\right| = \frac{1}{q_n^2(\alpha_{n+1} + \beta_{n+1})}.$$

Ovdje je, za n dovoljno velik, $\alpha_{n+1} = [1, 1, 1, \dots] = \frac{\sqrt{5}+1}{2}$ i

$$\begin{aligned}\frac{1}{\beta_{n+1}} &= \frac{q_n}{q_{n-1}} = a_n + \frac{1}{\frac{q_{n-1}}{q_{n-2}}} = a_n + \frac{1}{a_{n-1} + \frac{1}{\frac{q_{n-2}}{q_{n-3}}}} = \cdots = [a_n, a_{n-1}, \dots, a_1] \\ &= [\underbrace{1, 1, \dots, 1}_{n-N}, a_N, \dots, a_1].\end{aligned}$$

Budući da su $[\underbrace{1, 1, \dots, 1}_{n-N-1}]$ i $[\underbrace{1, 1, \dots, 1}_{n-N}]$ susjedne konvergente od $\frac{1}{\beta_{n+1}}$, to se $\frac{1}{\beta_{n+1}}$ nalazi između njih. Stoga je $\lim_{n\to\infty} \frac{1}{\beta_{n+1}} = [1, 1, 1, \dots] = \frac{\sqrt{5}+1}{2}$. Prema tome,

$$\lim_{n\to\infty} \beta_{n+1} = \left(\frac{\sqrt{5}+1}{2}\right)^{-1} = \frac{\sqrt{5}-1}{2} \quad \text{i} \quad \lim_{n\to\infty} (\alpha_{n+1} + \beta_{n+1}) = \sqrt{5}.$$

□

Teorem 6.11 (Legendre)**.** *Neka su p, q cijeli brojevi takvi da je $q \geq 1$ i*

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{2q^2}.$$

Tada je $\frac{p}{q}$ neka konvergenta od α.

Dokaz: Možemo pretpostaviti da je $\alpha \neq \frac{p}{q}$; inače je tvrdnja trivijalno zadovoljena. Tada možemo pisati $\alpha - \frac{p}{q} = \frac{\varepsilon\vartheta}{q^2}$, gdje je $0 < \vartheta < \frac{1}{2}$ i $\varepsilon = \pm 1$. Neka je

$$\frac{p}{q} = [b_0, b_1, \dots, b_{n-1}]$$

razvoj od $\frac{p}{q}$ u jednostavni verižni razlomak, gdje je n izabran tako da vrijedi $(-1)^{n-1} = \varepsilon$. To uvijek možemo postići jer je $[a_0, a_1, \dots, a_m] = [a_0, a_1, \dots, a_m - 1, 1]$.

Definirajmo ω sa

$$\alpha = \frac{\omega p_{n-1} + p_{n-2}}{\omega q_{n-1} + q_{n-2}}, \tag{30}$$

tako da je $\alpha = [b_0, b_1 \dots, b_{n-1}, \omega]$. Sada je, po formuli (27),

$$\frac{\varepsilon\vartheta}{q^2} = \alpha - \frac{p}{q} = \frac{1}{q_{n-1}}(\alpha q_{n-1} - p_{n-1}) = \frac{1}{q_{n-1}} \cdot \frac{(-1)^{n-1}}{\omega q_{n-1} + q_{n-2}},$$

pa je $\vartheta = \frac{q_{n-1}}{\omega q_{n-1}+q_{n-2}}$. Rješavanjem ove relacije po ω, dobivamo $\omega = \frac{1}{\vartheta} - \frac{q_{n-2}}{q_{n-1}}$. Odavde slijedi da je $\omega > 2 - 1 = 1$. Razvijmo ω u (konačan ili beskonačan) jednostavan verižni razlomak:

$$\omega = [b_n, b_{n+1}, b_{n+2}, \dots].$$

Budući da je $\omega > 1$, svi b_j $(j = n, n+1, \dots)$ su prirodni brojevi. Stoga je

$$\alpha = [b_0, b_1, \dots, b_{n-1}, b_n, b_{n+1}, \dots]$$

razvoj u jednostavni verižni razlomak od α i

$$\frac{p}{q} = \frac{p_{n-1}}{q_{n-1}} = [b_0, b_1, \dots, b_{n-1}]$$

je konvergenta od α, što je i trebalo dokazati. □

Teorem 6.12 (Hurwitz)**.** *(i) Za svaki iracionalan broj α postoji beskonačno mnogo racionalnih brojeva $\frac{p}{q}$ takvih da je*

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{\sqrt{5}q^2}.$$

(ii) Tvrdnja (i) ne vrijedi ukoliko se $\sqrt{5}$ zamijeni s bilo kojom konstantom $A > \sqrt{5}$.

Dokaz: Tvrdnja (i) slijedi direktno iz Teorema 6.9, dok tvrdnja (ii) slijedi iz Teorema 6.10 i 6.11. Naime, ako iracionalan broj α ima oblik iz Teorema 6.10, onda se po Teoremu 6.11 sva rješenja nejednadžbe $\left|\alpha - \frac{p}{q}\right| < \frac{1}{Aq^2}$, gdje je $A > \sqrt{5}$, nalaze među konvergentama od α, a po Teoremu 6.10 ovu nejednadžbu zadovoljava samo konačno mnogo konvergenti od α. □

Teorem 6.13 (Zakon najboljih aproksimacija)**.** *Neka je α iracionalan broj, te $\frac{p_0}{q_0}, \frac{p_1}{q_1}, \dots$ konvergente od α. Tada vrijedi:*

(i) $|\alpha q_0 - p_0| > |\alpha q_1 - p_1| > |\alpha q_2 - p_2| > \cdots$

(ii) Ako je $n \geq 1$ i $1 \leq q \leq q_n$, te ako je $(p, q) \neq (p_{n-1}, q_{n-1}), (p_n, q_n)$, onda je $|\alpha q - p| > |\alpha q_{n-1} - p_{n-1}|$.

Dokaz: Po formuli (27) je

$$|\alpha q_n - p_n| = \frac{1}{\alpha_{n+1}q_n + q_{n-1}} < \frac{1}{q_n + q_{n-1}},$$
$$|\alpha q_{n-1} - p_{n-1}| = \frac{1}{\alpha_n q_{n-1} + q_{n-2}} > \frac{1}{(a_n+1)q_{n-1} + q_{n-2}} = \frac{1}{q_{n-1} + q_n},$$

čime je dokazana tvrdnja (i).

Da bi dokazali (ii), definirajmo brojeve μ, ν pomoću jednadžbi

$$\mu p_n + \nu p_{n-1} = p,$$
$$\mu q_n + \nu q_{n-1} = q.$$

Matrica ovog sustava ima determinantu ± 1, pa su brojevi μ, ν cijeli brojevi. Ako je $\nu = 0$, onda je $p = \mu p_n$, $q = \mu q_n$, a to je nemoguće jer je $0 < q \leq q_n$ i $(p, q) \neq (p_n, q_n)$. Ako je $\mu = 0$, onda je $p = \nu p_{n-1}$, $q = \nu q_{n-1}$. Budući da je $(p, q) \neq (p_{n-1}, q_{n-1})$, to je $\nu \geq 2$ i zato je

$$|\alpha q - p| \geq 2|\alpha q_{n-1} - p_{n-1}| > |\alpha q_{n-1} - p_{n-1}|.$$

Ako su $\mu \neq 0$, $\nu \neq 0$, onda zbog $1 \leq q \leq q_n$, μ i ν imaju suprotne predznake, pa brojevi $\mu(\alpha q_n - p_n)$ i $\nu(\alpha q_{n-1} - p_{n-1})$ imaju iste predznake. Stoga je

$$|\alpha q - p| = |\mu(\alpha q_n - p_n)| + |\nu(\alpha q_{n-1} - p_{n-1})|,$$

pa je, zbog $\mu\nu \neq 0$, $|\alpha q - p| > |\alpha q_{n-1} - p_{n-1}|$. □

Razlomke oblika $\frac{p_{n,r}}{q_{n,r}} = \frac{rp_{n+1} + p_n}{rq_{n+1} + q_n}$, $r = 1, 2, \ldots, a_{n+2} - 1$, $n \geq -1$, nazivamo *sekundarne konvergente* verižnog razlomka $[a_0, a_1, \ldots]$. Uočimo: $\frac{p_{n,0}}{q_{n,0}} = \frac{p_n}{q_n}$, $\frac{p_{n,a_{n+2}}}{q_{n,a_{n+2}}} = \frac{p_{n+2}}{q_{n+2}}$.

Propozicija 6.14. *Za n paran vrijedi*

$$\frac{p_n}{q_n} < \cdots < \frac{p_{n,r}}{q_{n,r}} < \frac{p_{n,r+1}}{q_{n,r+1}} < \cdots < \frac{p_{n+2}}{q_{n+2}},$$

dok za n neparan vrijedi

$$\frac{p_n}{q_n} > \cdots > \frac{p_{n,r}}{q_{n,r}} > \frac{p_{n,r+1}}{q_{n,r+1}} > \cdots > \frac{p_{n+2}}{q_{n+2}}.$$

Nadalje, za svaki prirodan broj n vrijedi

$$q_{n,r+1}p_{n,r} - p_{n,r+1}q_{n,r} = (-1)^{n+1}. \tag{31}$$

Dokaz: Dovoljno je dokazati relaciju (31). Imamo:

$$\begin{aligned} &q_{n,r+1}p_{n,r} - p_{n,r+1}q_{n,r} \\ &\quad = [(r+1)q_{n+1} + q_n](rp_{n+1} + p_n) - [(r+1)p_{n+1} + p_n](rq_{n+1} + q_n) \\ &\quad = q_{n+1}p_n - p_{n+1}q_n = (-1)^{n+1}. \end{aligned}$$

□

Primjer 6.4. *Reći ćemo da je racionalan broj* $\frac{a}{b}$, $b > 0$, dobra aproksimacija *iracionalnog broja* α *ako vrijedi*

$$\left|\alpha - \frac{a}{b}\right| = \min\{\left|\alpha - \frac{x}{y}\right| : x, y \in \mathbb{Z},\ 0 < y \leq b\}.$$

a) Dokažimo da je svaka dobra aproksimacija od α *ili konvergenta ili sekundarna konvergenta od* α*.*

b) Pokažimo primjerom da ne mora svaka sekundarna konvergenta biti dobra aproksimacija.

Rješenje: a) Neka je $\frac{a}{b}$ dobra aproksimacija od α koja nije ni konvergenta ni sekundarna konvergenta od α. Bez smanjenja općenitosti možemo pretpostaviti da je $\frac{a}{b} > \alpha$. Tada postoje uzastopne (obične ili sekundarne) konvergente $\frac{P}{Q}$ i $\frac{P'}{Q'}$ od α takve da je

$$\alpha < \frac{P}{Q} < \frac{a}{b} < \frac{P'}{Q'} \quad \text{i} \quad P'Q - PQ' = 1.$$

Sada je

$$\frac{1}{Q'b} \leq \frac{P'}{Q'} - \frac{a}{b} < \frac{P'}{Q'} - \frac{P}{Q} = \frac{1}{Q'Q}.$$

Dakle, dobili smo da je $Q < b$ i $\left|\alpha - \frac{P}{Q}\right| < \left|\alpha - \frac{a}{b}\right|$, što je kontradikcija.

b) Neka je $\alpha = [1, 2, 2, 2, \dots]$. Tada je $\frac{1}{\alpha - 1} = \alpha + 1$, pa je stoga $\alpha = \sqrt{2}$. Konvergente od α su: 1, $\frac{3}{2}$, $\frac{7}{5}$, $\frac{17}{12}$, $\dots$, a sekundarne konvergente: $\frac{4}{3}$, $\frac{10}{7}$, $\frac{24}{17}$, $\dots$. Međutim, $\left|\sqrt{2} - \frac{7}{5}\right| \approx 0.0142$, $\left|\sqrt{2} - \frac{10}{7}\right| \approx 0.0144$, pa $\frac{10}{7}$ nije dobra aproksimacija broja $\sqrt{2}$. ♢

Definicija 6.2. *Za beskonačni verižni razlomak* $[a_0, a_1, a_2, \dots]$ *kažemo da je* periodski *ako postoje cijeli brojevi* $k \geq 0$, $m \geq 1$ *takvi da je* $a_{m+n} = a_n$ *za sve* $n \geq k$*. U tom slučaju verižni razlomak pišemo u obliku*

$$[a_0, a_1, \dots, a_{k-1}, \overline{a_k, a_{k+1}, \dots, a_{k+m-1}}],$$

gdje "crta" iznad brojeva $a_k, \dots, a_{k+m-1}$ *znači da se taj blok brojeva ponavlja u nedogled.*

Primjer 6.5. *(i) Neka je* $\beta = [2,3,2,3,\dots] = [\overline{2,3}]$. *Tada je* $\beta = 2 + \frac{1}{3+\frac{1}{\beta}}$. *To daje kvadratnu jednadžbu za* β: $3\beta^2 - 6\beta - 2 = 0$, *pa zbog* $\beta > 0$, *dobivamo da je* $\beta = \frac{3+\sqrt{15}}{3}$.

(ii) Neka je sada $\alpha = [4,1,\overline{2,3}]$. *Imamo:*

$$\alpha = 4 + \frac{1}{1+\frac{1}{\beta}} = 4 + \frac{\beta}{\beta+1} = \frac{29+\sqrt{15}}{7}.$$

♢

Ova dva primjera ilustriraju opću situaciju.

Definicija 6.3. *Za iracionalan broj* α *kažemo da je* kvadratna iracionalnost *ako je* α *korijen kvadratne jednadžbe s racionalnim koeficijentima.*

Teorem 6.15 (Euler, Lagrange)**.** *Razvoj u jednostavni verižni razlomak realnog broja* α *je periodski ako i samo ako je* α *kvadratna iracionalnost.*

Dokaz: Neka je $\alpha = [b_0, b_1, \dots, b_{k-1}, \overline{a_0, a_1, \dots, a_{m-1}}]$, te neka je $\beta = [\overline{a_0, a_1, \dots, a_{m-1}}]$, tj. neka je β čisto periodski dio od α. Iz

$$\beta = [a_0, a_1, \dots, a_{m-1}, \beta]$$

slijedi da je

$$\beta = \frac{\beta p_{m-1} + p_{m-2}}{\beta q_{m-1} + q_{m-2}},$$

a to je kvadratna jednadžba za β (s cjelobrojnim koeficijentima). Budući da je β iracionalan (jer mu je razvoj beskonačan), to je β kvadratna iracionalnost.

Zapišimo α pomoću β:

$$\alpha = \frac{\beta p + p'}{\beta q + q'}, \tag{32}$$

gdje su $\frac{p}{q}$ i $\frac{p'}{q'}$ zadnje dvije konvergente od $[b_0, b_1, \dots, b_{k-1}]$. Međutim, β ima oblik $\frac{a+\sqrt{b}}{c}$, pa iz (32) slijedi da i α ima isti oblik. Budući da α nije racionalan, prvi dio teorema je dokazan.

Dokažimo sada obrat. Neka je α kvadratna iracionalnost, tj. neka je $\alpha = \frac{a+\sqrt{b}}{c}$, $a, b, c \in \mathbb{Z}$, $b > 0$, $c \neq 0$ i b nije potpun kvadrat. Množeći brojnik i nazivnik od α sa $|c|$, dobivamo

$$\alpha = \frac{ac + \sqrt{bc^2}}{c^2} \quad \text{ili} \quad \alpha = \frac{-ac + \sqrt{bc^2}}{-c^2},$$

u ovisnosti o tome je li c pozitivan ili negativan. Stoga α možemo zapisati u obliku

$$\alpha = \frac{s_0 + \sqrt{d}}{t_0},$$

gdje su $d, s_0, t_0 \in \mathbb{Z}$, $t_0 \neq 0$, d nije potpun kvadrat i $t_0 | (d - s_0^2)$.

Sada ćemo opisati razvoj $[a_0, a_1, \dots]$ u jednostavni verižni razlomak broja α. Neka je $\alpha_0 = \alpha$, te neka je

$$a_i = \lfloor \alpha_i \rfloor, \quad \alpha_i = \frac{s_i + \sqrt{d}}{t_i}, \quad s_{i+1} = a_i t_i - s_i, \quad t_{i+1} = \frac{d - s_{i+1}^2}{t_i}. \tag{33}$$

Imamo:

$$\begin{aligned} \alpha_i - a_i &= \frac{s_i + \sqrt{d} - a_i t_i}{t_i} = \frac{\sqrt{d} - s_{i+1}}{t_i} = \frac{d - s_{i+1}^2}{t_i(\sqrt{d} + s_{i+1})} = \frac{t_{i+1}}{\sqrt{d} + s_{i+1}} \\ &= \frac{1}{\alpha_{i+1}}, \end{aligned}$$

pa je zaista $\alpha = [a_0, a_1, \dots]$.

Pokažimo sada matematičkom indukcijom da su s_i, t_i cijeli brojevi takvi da je $t_i \neq 0$ i $t_i | (d - s_i^2)$. To vrijedi za $i = 0$. Ako tvrdnja vrijedi za neki i, onda iz $s_{i+1} = a_i t_i - s_i$ slijedi da je broj s_{i+1} cijeli. Relacija

$$t_{i+1} = \frac{d - s_{i+1}^2}{t_i} = \frac{d - s_i^2}{t_i} + 2a_i s_i - a_i^2 t_i$$

pokazuje da je i t_{i+1} cijeli broj. Nadalje, $t_{i+1} \neq 0$, jer bi inače $d = s_{i+1}^2$ bio potpun kvadrat. Konačno, iz $t_i = \frac{d - s_{i+1}^2}{t_{i+1}}$ slijedi da $t_{i+1} | (d - s_{i+1}^2)$.

Sa α_i' označimo konjugat od α_i, tj. $\alpha_i' = \frac{s_i - \sqrt{d}}{t_i}$. Budući da je konjugat kvocijenta jednak kvocijentu konjugata, imamo: $\alpha_0' = \frac{\alpha_n' p_{n-1} + p_{n-2}}{\alpha_n' q_{n-1} + q_{n-2}}$. Odavde je

$$\alpha_n' = -\frac{q_{n-2}}{q_{n-1}} \Big(\frac{\alpha_0' - \frac{p_{n-2}}{q_{n-2}}}{\alpha_0' - \frac{p_{n-1}}{q_{n-1}}} \Big).$$

Kad n teži u ∞, $\frac{p_{n-1}}{q_{n-1}}$ i $\frac{p_{n-2}}{q_{n-2}}$ teže prema α_0, a $\alpha_0 \neq \alpha_0'$. Stoga izraz u zagradi teži prema 1, pa je zbog toga pozitivan za dovoljno velike n, recimo za $n > N$. Sada je za $n > N$ broj α_n' negativan. No, α_n je pozitivan za $n \geq 1$, pa je $\alpha_n - \alpha_n' = \frac{2\sqrt{d}}{t_n} > 0$. Dakle, $t_n > 0$ za $n > N$. Nadalje, za $n > N$ imamo:

$$s_n^2 < s_n^2 + t_{n-1} t_n = d \implies |s_n| < \sqrt{d},$$

dok iz $\alpha_n > 1$ i upravo dokazanog slijedi

$$t_n < s_n + \sqrt{d} < 2\sqrt{d}.$$

Odavde slijedi da uređeni parovi (s_n, t_n) mogu poprimiti samo konačno mnogo vrijednosti, pa postoje prirodni brojevi j, k, $j < k$, takvi da je $s_j = s_k$, $t_j = t_k$. Sada (33) povlači da je $\alpha_j = \alpha_k$, pa je

$$\alpha = [a_0, \dots, a_{j-1}, \overline{a_j, a_{j+1}, \dots, a_{k-1}}],$$

što je i trebalo dokazati. □

Uočimo da je u formuli (33),

$$a_i = \left\lfloor \frac{s_i + \sqrt{d}}{t_i} \right\rfloor = \left\lfloor \frac{s_i + \lfloor \sqrt{d} \rfloor}{t_i} \right\rfloor,$$

pa se u računanju razvoja kvadratnih iracionalnosti uopće ne pojavljuju iracionalni brojevi.

Primjer 6.6. *Razvijmo broj $\sqrt{15}$ u jednostavni verižni razlomak.*

Rješenje: Imamo:

$$\begin{aligned}
&s_0 = 0,\ t_0 = 1,\ a_0 = 3,\\
&s_1 = a_0 t_0 - s_0 = 3,\ t_1 = \frac{15 - s_1^2}{t_0} = 6,\ a_1 = \left\lfloor \frac{s_1 + \lfloor \sqrt{d} \rfloor}{t_1} \right\rfloor = \left\lfloor \frac{3 + \lfloor \sqrt{15} \rfloor}{6} \right\rfloor = 1,\\
&s_2 = 3,\ t_2 = 1,\ a_2 = \left\lfloor \frac{3 + \lfloor \sqrt{15} \rfloor}{1} \right\rfloor = 6,\\
&s_3 = 3,\ t_3 = 6.
\end{aligned}$$

Dakle, $(s_1, t_1) = (s_3, t_3)$, pa je $\sqrt{15} = [3, \overline{1, 6}]$. ♢

Zadatak 6.3. *Razvijte u jednostavni verižni razlomak brojeve $\sqrt{23}$ i $\frac{2+\sqrt{5}}{3}$.*

Primjer 6.7. *Neka je $d \geq 2$ prirodan broj. Dokažimo da vrijedi:*

$$\sqrt{d^2 - d} = [d - 1, \overline{2, 2d - 2}].$$

Rješenje: Imamo:

$$\begin{aligned}
&s_0 = 0,\ t_0 = 1,\ a_0 = d - 1,\\
&s_1 = d - 1,\ t_1 = \frac{d^2 - d - (d-1)^2}{1} = d - 1,\\
&a_1 = \left\lfloor \frac{d - 1 + \lfloor \sqrt{d^2 - d} \rfloor}{d - 1} \right\rfloor = \left\lfloor \frac{d - 1 + d - 1}{d - 1} \right\rfloor = 2,\\
&s_2 = d - 1,\ t_2 = 1,\ a_2 = \left\lfloor \frac{d - 1 + \lfloor \sqrt{d^2 - d} \rfloor}{1} \right\rfloor = 2d - 2,\\
&s_3 = d - 1,\ t_3 = d - 1.
\end{aligned}$$

Dakle, $(s_1, t_1) = (s_3, t_3)$, pa je $\sqrt{d^2 - d} = [d - 1, \overline{2, 2d - 2}]$. ♢

Teorem 6.16. *Kvadratna iracionalnost α ima čisto periodski razvoj u jednostavni verižni razlomak ako i samo ako je $\alpha > 1$, te $-1 < \alpha' < 0$, gdje je α' konjugat od α. (Za takvu kvadratnu iracionalnost kažemo da je* reducirana.*)*

Dokaz: Neka je $\alpha > 1$ i $-1 < \alpha' < 0$. Stavimo $\alpha_0 = \alpha$, te definirajmo α_i rekurzivno sa $\frac{1}{\alpha_{i+1}} = \alpha_i - a_i$. Tada je

$$\frac{1}{\alpha'_{i+1}} = \alpha'_i - a_i. \tag{34}$$

Sada je $a_i \geq 1$ za sve $i \geq 0$ (čak i za $i = 0$ zbog $\alpha > 1$). Zbog toga, ako je $\alpha'_i < 0$, onda je $\frac{1}{\alpha'_{i+1}} < -1$, odnosno $-1 < \alpha'_{i+1} < 0$. Budući da je $-1 < \alpha'_0 < 0$, indukcijom slijedi da je $-1 < \alpha'_i < 0$ za sve $i \geq 0$. Sada iz (34) slijedi

$$0 < -\frac{1}{\alpha'_{i+1}} - a_i < 1, \quad \text{tj.} \quad a_i = \left\lfloor -\frac{1}{\alpha'_{i+1}} \right\rfloor.$$

Iz Teorema 6.15 slijedi da postoje prirodni brojevi takvi da je $j < k$ i $\alpha_j = \alpha_k$. Sada je $\alpha'_j = \alpha'_k$, te

$$a_{j-1} = \left\lfloor -\frac{1}{\alpha'_j} \right\rfloor = \left\lfloor -\frac{1}{\alpha'_k} \right\rfloor = a_{k-1},$$
$$\alpha_{j-1} = a_{j-1} + \frac{1}{\alpha_j} = a_{k-1} + \frac{1}{\alpha_k} = \alpha_{k-1}.$$

Dakle, $\alpha_j = \alpha_k$ povlači da je $\alpha_{j-1} = \alpha_{k-1}$. Primijenimo li ovu implikaciju j puta, dobivamo $\alpha_0 = \alpha_{k-j}$, tj. $\alpha = [\overline{a_o, a_1, \ldots, a_{k-j}}]$.

Obrnuto, pretpostavimo da je razvoj od α čisto periodski,

$$\alpha = [\overline{a_0, a_1 \ldots, a_{n-1}}],$$

$a_0, a_1, \ldots, a_{n-1} \in \mathbb{N}$ (zbog $a_0 = a_n$). Imamo: $\alpha > a_0 \geq 1$. Također je

$$\alpha = [a_0, \ldots, a_{n-1}, \alpha] = \frac{\alpha p_{n-1} + p_{n-2}}{\alpha q_{n-1} + q_{n-2}}.$$

Prema tome, α zadovoljava jednadžbu

$$f(x) = x^2 q_{n-1} + x(q_{n-2} - p_{n-1}) - p_{n-2} = 0.$$

Ova kvadratna jednadžba ima dva korijena, α i α'. Budući da je $\alpha > 1$, dovoljno je provjeriti da $f(x)$ ima korijen između -1 i 0. To ćemo provjeriti tako da pokažemo da $f(-1)$ i $f(0)$ imaju različite predznake. Najprije je $f(0) = -p_{n-2} < 0$, a potom

$$f(-1) = q_{n-1} - q_{n-2} + p_{n-1} - p_{n-2} > 0.$$

□

Definicija 6.4. *Kompleksan broj α zove se* algebarski broj *ako postoji polinom $f(x)$ s racionalnim koeficijentima, različit od nulpolinoma, takav da je $f(\alpha) = 0$. Kompleksan broj se zove* transcendentan *ako nije algebarski.*

Teorem 6.17. *Neka je α algebarski broj. Tada postoji jedinstveni ireducibilni normirani polinom $g(x)$ s racionalnim koeficijentima takav da je $g(\alpha) = 0$. Nadalje, svaki polinom nad $\mathbb{Q}$ kojeg α poništava djeljiv je sa $g(x)$.*

Dokaz: Neka je $G(x)$ polinom nad $\mathbb{Q}$ najmanjeg stupnja kojeg α poništava. Ako je vodeći koeficijent od $G(x)$ jednak c, definirajmo $g(x) = \frac{1}{c}G(x)$. Tada je $g(\alpha) = 0$ i g je normiran. Pokažimo da je g ireducibilan. U protivnom bi bilo $g(x) = h_1(x)h_2(x)$, pa bi imali $h_1(\alpha) = 0$ ili $h_2(\alpha) = 0$, protivno pretpostavci o minimalnosti stupnja od $G(x)$.

Neka je sada $f(x)$ bilo koji polinom nad $\mathbb{Q}$ sa svojstvom da je $f(\alpha) = 0$. Podijelimo polinom $f(x)$ sa $g(x)$. Dobivamo $f(x) = g(x)q(x) + r(x)$, gdje je $\deg r < \deg g$. No, $r(\alpha) = 0$, pa zbog minimalnosti stupnja od $G(x)$, mora biti $r(x)$ nulpolinom. Dakle, $f(x)$ je djeljiv s $g(x)$.

Konačno, pokažimo jedinstvenost od $g(x)$. Neka je $g_1(x)$ ireducibilan normiran polinom nad $\mathbb{Q}$ takav da je $g_1(\alpha) = 0$. Tada, prema upravo dokazanom, postoji polinom $q(x)$ takav da je $g_1(x) = g(x)q(x)$. No, ireducibilnost od $g_1(x)$ povlači da je $q(x)$ konstanta. U stvari, $q(x) = 1$, budući su $g(x)$ i $g_1(x)$ normirani. □

Definicija 6.5. Minimalni polinom *algebarskog broja α je polinom $g(x)$ opisan u Teoremu 6.17.* Stupanj *algebarskog broja je stupanj njegovog minimalnog polinoma.*

Teorem 6.18 (Liouville)**.** *Neka je α realan algebarski broj stupnja d. Tada postoji konstanta $c(\alpha) > 0$ tako da vrijedi*

$$\left|\alpha - \frac{p}{q}\right| > \frac{c(\alpha)}{q^d}$$

za sve racionalne brojeve $\frac{p}{q}$, gdje je $q > 0$ i $\frac{p}{q} \neq \alpha$.

Dokaz: Neka je $g(x)$ minimalni polinom od α. Odaberimo prirodan broj m tako da polinom $P(x) = m \cdot g(x)$ ima cjelobrojne koeficijente.

Bez smanjenja općenitosti možemo pretpostaviti da je $|\alpha - \frac{p}{q}| \leq 1$ (inače možemo staviti $c(\alpha) = 1$). Razvijemo li $P(x)$ u Taylorov red oko α, dobivamo:

$$|P(\frac{p}{q})| = \Big|\sum_{i=1}^{d}(\frac{p}{q} - \alpha)^i \frac{1}{i!}P^{(i)}(\alpha)\Big| < \frac{1}{c(\alpha)} \cdot |\alpha - \frac{p}{q}|, \tag{35}$$

gdje je $c(\alpha) = \frac{1}{2\sum_{i=1}^{d}\frac{1}{i!}|P^{(i)}(\alpha)|}$.

Budući da je polinom $P(x)$ ireducibilan, to je $P(\frac{p}{q}) \neq 0$. Stoga je broj $q^d|P(\frac{p}{q})|$ prirodan, pa je $|P(\frac{p}{q})| \geq \frac{1}{q^d}$. Usporedimo li ovo sa (35), dobivamo tvrdnju teorema. □

Primjer 6.8. *Broj $\alpha = \sum_{n=1}^{\infty} 2^{-n!}$ je transcendentan.*

Zaista, ako stavimo $q(k) = 2^{k!}$, $p(k) = 2^{k!} \sum_{n=1}^{k} 2^{-n!}$, onda je

$$\left|\alpha - \frac{p(k)}{q(k)}\right| = \sum_{n=k+1}^{\infty} 2^{-n!} < 2^{-(k+1)!} + 2^{-(k+1)!-1} + 2^{-(k+1)!-2} + \cdots$$
$$= 2 \cdot 2^{-(k+1)!} = \frac{2}{[q(k)]^{k+1}}.$$

Odavde slijedi da za svaki prirodan broj d i svaki $c > 0$ postoji $k_0 \in \mathbb{N}$ takav da za sve $k \geq k_0$ vrijedi

$$\left|\alpha - \frac{p(k)}{q(k)}\right| < \frac{c}{[q(k)]^d}.$$

Po Liouvilleovom teoremu, α ne može biti algebarski broj stupnja d za niti jedan d, pa je stoga α transcendentan. ♢

Zadatak 6.4. *Dokažite da za sve* $p, q \in \mathbb{N}$ *vrijedi* $\left|\frac{\sqrt{2}}{2} - \frac{p}{q}\right| > \frac{1}{4q^2}$.

7. Diofantske jednadžbe

Teorem 7.1. *Neka su a, b, c cijeli brojevi i $d = (a, b)$. Ako $d \nmid c$, onda jednadžba*

$$ax + by = c \tag{36}$$

nema cjelobrojnih rješenja. Ako $d|c$, onda jednadžba (36) ima beskonačno mnogo cjelobrojnih rješenja. Ako je (x_1, y_1) jedno rješenje, onda su sva rješenja dana sa $x = x_1 + \frac{b}{d} \cdot t$, $y = y_1 - \frac{a}{d} \cdot t$, gdje je $t \in \mathbb{Z}$.

Dokaz: Ako (36) ima rješenja, onda očito $d|c$. Pretpostavimo sada da $d|c$ i promotrimo kongruenciju

$$ax \equiv c \pmod{b}. \tag{37}$$

Po Teoremu 2.6 ova kongruencija ima rješenja i ako je x_1 neko rješenje, onda su sva rješenja od (37) dana sa $x \equiv x_1 + \frac{b}{d} \cdot k \pmod{b}$, gdje je $k = 0, 1, \ldots, d-1$. Stoga su sva rješenja od (36) dana sa $x = x_1 + \frac{b}{d} \cdot t$, $t \in \mathbb{Z}$. Uvrstimo li ovo u (36), dobivamo $by = c - ax_1 - \frac{ab}{d} \cdot t = by_1 - \frac{ab}{d} \cdot t$, pa je $y = y_1 - \frac{a}{d} \cdot t$. □

Teorem 7.2. *Neka su $a_1, a_2, \ldots, a_n$ cijeli brojevi različiti od nule. Tada linearna diofantska jednadžba*

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = c \tag{38}$$

ima rješenja ako i samo ako $(a_1, a_2, \ldots, a_n)|c$. Nadalje, ako jednadžba (38) ima barem jedno rješenje, onda ih ima beskonačno mnogo.

Dokaz: Postojanje rješenja od (38) očito povlači da $(a_1, a_2, \ldots, a_n)|c$. Dokazat ćemo matematičkom indukcijom da ako $(a_1, a_2, \ldots, a_n)|c$, onda (38) ima beskonačno mnogo rješenja. Za $n = 2$ tvrdnja vrijedi po Teoremu 7.1, pa pretpostavimo da vrijedi za jednadžbe s $n-1$ varijabli. Neka je $d = (a_{n-1}, a_n)$. Po pretpostavci, jednadžba $a_1x_1 + \cdots + a_{n-2}x_{n-2} + dy = c$ ima beskonačno mnogo rješenja $(x_1, \ldots, x_{n-2}, y)$. Za svako rješenje ove jednadžbe, promotrimo jednadžbu

$$a_{n-1}x_{n-1} + a_nx_n = dy.$$

Zbog $(a_{n-1}, a_n)|dy$ slijedi da ova jednadžba ima beskonačno mnogo rješenja (x_{n-1}, x_n). Na taj način smo dobili beskonačno mnogo rješenja $(x_1, \ldots, x_n)$ jednadžbe (38). □

Definicija 7.1. *Uređenu trojku prirodnih brojeva* (x, y, z) *zovemo* Pitagorina trojka *ako su* x, y *katete,* z *hipotenuza nekog pravokutnog trokuta, tj. ako vrijedi*

$$x^2 + y^2 = z^2. \tag{39}$$

Ako su x, y, z *relativno prosti, onda kažemo da je* (x, y, z) primitivna Pitagorina trojka. *(Takav trokut zovemo (primitivni) Pitagorin trokut.)*

Uočimo najprije da je u svakoj primitivnoj Pitagorinoj trojki točno jedan od brojeva x, y neparan. Zaista, ako bi x i y bili parni, onda trojka ne bi bila primitivna, a ako bi x i y bili neparni, onda bi iz $x^2 + y^2 \equiv 2 \pmod 4$ i $z^2 \equiv 0 \pmod 4$ dobili kontradikciju.

Teorem 7.3. *Sve primitivne Pitagorine trojke* (x, y, z) *u kojima je* y *paran, dane su formulama*

$$x = m^2 - n^2, \quad y = 2mn, \quad z = m^2 + n^2, \tag{40}$$

gdje je $m > n$ *i* m, n *su relativno prosti prirodni brojevi različite parnosti.*

Dokaz: Jednadžbu (39) možemo pisati u obliku $y^2 = (z+x)(z-x)$. Neka je $y = 2c$. Brojevi $z + x$ i $z - x$ su parni, pa postoje prirodni brojevi a i b takvi da je $z + x = 2a$, $z - x = 2b$. Sada je

$$c^2 = ab.$$

Iz $z = a + b$, $x = a - b$, zaključujemo da je $(a, b) = 1$, pa postoje $m, n \in \mathbb{N}$, $(m, n) = 1$, takvi da je $a = m^2$, $b = n^2$. Odavde je

$$x = m^2 - n^2, \quad z = m^2 + n^2, \quad y = 2mn.$$

Brojevi m i n moraju biti različite parnosti jer je broj $x = m^2 - n^2$ neparan.

Lako se provjeri da brojevi x, y, z definirani sa (40) zadovoljavaju (39). Zaista,

$$(m^2 - n^2)^2 + (2mn)^2 = m^4 + 2m^2n^2 + n^4 = (m^2 + n^2)^2.$$

Treba još provjeriti da su relativno prosti. Pretpostavimo da je $(x, z) = d > 1$. Tada je d neparan, $d|(m^2+n^2)+(m^2-n^2) = 2m^2$ i $d|(m^2+n^2)-(m^2-n^2) = 2n^2$. No, ovo je u kontradikciji s pretpostavkom da su m i n, pa stoga i m^2 i n^2, relativno prosti. □

Iz Teorema 7.3 slijedi da su sve Pitagorine trojke dane identitetom:

$$[d(m^2 - n^2)]^2 + (2dmn)^2 = [d(m^2 + n^2)]^2. \tag{41}$$

Primjer 7.1. *Nađimo sve Pitagorine trokute u kojima je jedna stranica jednaka a)* 39, *b)* 1999.

Rješenje: a) Sve Pitagorine trojke su dane identitetom (41). U ovom slučaju imamo tri mogućnosti: $d = 1$, $d = 3$, $d = 13$.

Ako je $d = 1$, onda je $m^2+n^2 \neq 39$, pa mora biti $m^2-n^2 = (m-n)(m+n) = 39$. Odavde je $m - n = 1$, $m + n = 39$ ili $m - n = 3$, $m + n = 13$, što povlači da je $m = 20$, $n = 19$ ili $m = 8$, $n = 5$. Tako dobivamo Pitagorine trojke $(39, 760, 761)$ i $(39, 80, 89)$.

Ako je $d = 3$, onda je $m^2 - n^2 = 13$ ili $m^2 + n^2 = 13$, što povlači da je $m = 7$, $n = 6$ ili $m = 3$, $n = 2$. Dobivene trojke su $(39, 252, 255)$ i $(15, 36, 39)$.

Ako je $d = 13$, onda je $m^2 - n^2 = 3$. Odavde je $m = 2$, $n = 1$, što daje trojku $(39, 52, 65)$.

b) Sada je $d = 1$, pa iz $m^2 - n^2 = 1999$ slijedi $m = 1000$, $n = 999$, te je jedina trojka $(1999, 1998000, 1998001)$. ♢

Zadatak 7.1. *Nađite sve Pitagorine trokute kojima je jedna stranica jednaka a)* 34, *b)* 2001.

Zadatak 7.2. *Nađite sve primitivne Pitagorine trokute čije sve tri stranice leže između* 2000 *i* 3000.

Teorem 7.4. *Jednadžba $x^4 + y^4 = z^2$ nema rješenja u prirodnim brojevima. Drugim riječima, ne postoji pravokutni trokut kojem su duljine kateta kvadrati prirodnih brojeva.*

Dokaz: Pretpostavimo da takav trokut postoji i izaberimo među svim takvim trokutima onaj s najmanjoj hipotenuzom. Tako dobivamo Pitagorinu trojku (x^2, y^2, z). Pokažimo da su x i y relativno prosti. U protivnom bi bilo $x = a \cdot d$, $y = b \cdot d$, $d > 1$. Tada bi iz $z^2 = d^4(a^4+b^4)$ slijedilo da postoji $c \in \mathbb{N}$ takav da je $z = d^2 \cdot c$, te bi dobili Pitagorinu trojku (a^2, b^2, c) s hipotenuzom manjom od z, što je kontradikcija.

Dakle, (x^2, y^2, z) je primitivna Pitagorina trojka, pa po Teoremu 7.3 (ako odaberemo da je y paran) postoje relativno prosti prirodni brojevi različite parnosti m i n tako da vrijedi

$$x^2 = m^2 - n^2, \quad y^2 = 2mn, \quad z = m^2 + n^2.$$

Iz $x^2+n^2 = m^2$ slijedi da je n paran, a m neparan. Stavimo: $n = 2k$, $y = 2t$, pa dobivamo

$$t^2 = mk.$$

Odavde slijedi da postoje prirodni brojevi r i s takvi da je $m = r^2$ i $k = s^2$. Budući da je (x, n, m) primitivna Pitagorina trojka, po Teoremu 7.3 postoje u, v takvi da je $(u, v) = 1$, $n = 2uv$, $m = u^2 + v^2$. Sada iz $n = 2s^2$ slijedi da je $s^2 = uv$, pa postoje $a, b \in \mathbb{N}$ takvi da je $u = a^2$, $v = b^2$. Prema tome, $a^4 + b^4 = r^2$, pa je (a^2, b^2, r) Pitagorina trojka za čiju hipotenuzu vrijedi: $r < r^2 = m < m^2 + n^2 = z$, što je u suprotnosti s minimalnošću od z. □

Napomena 7.1. *Iz Teorema 7.4 slijedi da jednadžba $x^4 + y^4 = z^4$ nema rješenja u prirodnim brojevima. Ovo je specijalni slučaj tzv. Velikog Fermatovog teorema koji kaže da jednadžba $x^n + y^n = z^n$ nema rješenja u prirodnim brojevima za $n \geq 3$. Ovaj teorem je dokazao 1995. godine Andrew Wiles.*

Propozicija 7.5. *Ne postoji Pitagorin trokut u kome su hipotenuza i jedna kateta kvadrati prirodnih brojeva.*

Dokaz: Pretpostavimo suprotno i neka je (x, y, z) Pitagorina trojka s najmanjom hipotenuzom koja ima zadano svojstvo. Jasno je da je trojka (x, y, z) primitivna. Neka je $x = a^2$, $z = c^2$.

Ako je y paran, onda postoje $m, n \in \mathbb{N}$ takvi da je

$$a^2 = x = m^2 - n^2, \quad y = 2mn, \quad c^2 = z = m^2 + n^2.$$

Odavde je $(ac)^2 = m^4 - n^4$, pa je u Pitagorinoj trojki (n^2, ac, m^2) hipotenuza $m^2 < z$, te smo dobili kontradikciju.

Prema tome, y mora biti neparan, što znači da je a paran. Iz $y^2 = c^4 - a^4 = (c^2 - a^2)(c^2 + a^2)$, slijedi da postoje prirodni brojevi r, s takvi da je

$$c^2 - a^2 = r^2, \quad c^2 + a^2 = s^2.$$

Odavde je $2c^2 = r^2 + s^2$, odnosno $c^2 = (\frac{s+r}{2})^2 + (\frac{s-r}{2})^2$. Dakle, postoje $m, n \in \mathbb{N}$ takvi da je

$$\frac{s \pm r}{2} = m^2 - n^2, \quad \frac{s \mp r}{2} = 2mn, \quad c = m^2 + n^2,$$

pa je $2a^2 = s^2 - r^2 = 8mn(m-n)(m+n)$. Budući su m i n relativno prosti brojevi različite parnosti, brojevi m, n, $m-n$ i $m+n$ su u parovima relativno prosti. Stoga postoje $k, l, p, q \in \mathbb{N}$ takvi da je

$$m = k^2, \quad n = l^2, \quad m - n = p^2, \quad m + n = q^2.$$

Odavde je $k^4 - l^4 = (pq)^2$, pa smo dobili Pitagorinu trojku (l^2, pq, k^2) s hipotenuzom $k^2 = m < m^2 + n^2 = c < c^2 = z$, što je kontradikcija. □

Korolar 7.6. *Ne postoji Pitagorin trokut čija je površina potpun kvadrat.*

Dokaz: Pretpostavimo da takav trokut (x, y, z) postoji. Tada je

$$x^2 + y^2 = z^2 \quad \text{i} \quad xy = 2P.$$

Po pretpostavci, postoji $u \in \mathbb{N}$ takav da je $P = u^2$, odnosno $2xy = (2u)^2$. Sada je

$$z^2 + (2u)^2 = (x + y)^2, \quad z^2 - (2u)^2 = (x - y)^2.$$

Odavde dobivamo: $z^4 = (2u)^4 + (x^2 - y^2)^2$. Dakle, dobili smo Pitagorin trokut čija je hipotenuza z^2, a jedna kateta $(2u)^2$, što je u suprotnosti s Propozicijom 7.5. □

Primjer 7.2. *Nađimo sva rješenja diofantske jednadžbe* $x^2 + 5y^2 = z^2$ *uz uvjet* $(x, y, z) = 1$.

Rješenje: Imamo:

$$5y^2 = (z - x)(z + x). \tag{42}$$

Pretpostavimo najprije da je y paran. Tada su x i z neparni. Iz (42) slijedi

$$5 \cdot \left(\frac{y}{2}\right)^2 = \frac{z - x}{2} \cdot \frac{z + x}{2}.$$

Brojevi $\frac{z-x}{2}$ i $\frac{z+x}{2}$ su relativno prosti, pa postoje $m, n \in \mathbb{N}$ takvi da je

$$\frac{z \pm x}{2} = 5m^2, \quad \frac{z \mp x}{2} = n^2, \quad \frac{y}{2} = mn.$$

Odavde je $x = \pm(5m^2 - n^2)$, $y = 2mn$, $z = 5m^2 + n^2$.

Neka je sada y neparan. Tada je x paran i z neparan. Iz (42) slijedi da postoje $a, b \in \mathbb{N}$ takvi da je

$$z \pm x = 5a^2, \quad z \mp x = b^2, \quad y = ab.$$

Brojevi a i b su neparni, pa možemo staviti da je $b - a = 2c$, $c \in \mathbb{Z}$. Tada je

$$x = \pm(2a^2 - 2ac - 2c^2), \quad y = a^2 + 2ac, \quad z = 3a^2 + 2ac + 2c^2.$$

♢

Definicija 7.2. *Diofantska jednadžba*

$$x^2 - dy^2 = 1, \tag{43}$$

gdje je $d \in \mathbb{N}$ *i* d *nije potpun kvadrat, zove se* Pellova jednadžba *(iako J. Pell nije značajnije doprinio njezinom proučavanju). Jednadžbu oblika*

$$x^2 - dy^2 = N, \tag{44}$$

gdje je d *kao gore i* $N \in \mathbb{N}$, *zovemo* pellovska jednadžba.

Ako je d cijeli broj takav da je $d < 0$ ili je d potpun kvadrat, onda očito jednadžbe (43) i (44) imaju konačno mnogo rješenja. Koristeći razvoj u verižni razlomak broja $\sqrt{d}$ pokazat ćemo da Pellova jednadžba uvijek ima beskonačno mnogo rješenja.

Teorem 7.7. *Ako prirodan broj* d *nije potpun kvadrat, onda razvoj u jednostavni verižni razlomak od* $\sqrt{d}$ *ima oblik*

$$\sqrt{d} = [a_0, \overline{a_1, a_2, \ldots, a_{r-1}, 2a_0}],$$

gdje je $a_0 = \lfloor \sqrt{d} \rfloor$, *a* $a_1, \ldots, a_{r-1}$ *su centralno simetrični, tj.* $a_1 = a_{r-1}$, $a_2 = a_{r-2}$, $\ldots$. *Nadalje, u (33) uz* $\alpha_0 = \sqrt{d}$, $t_0 = 1$, $s_0 = 0$, *imamo* $t_i \neq -1$, *te* $t_i = 1$ *ako i samo ako* $r|i$ *(ovdje* r *označava duljinu najmanjeg perioda u razvoju od* $\sqrt{d}$*).*

Dokaz: Promotrimo broj $\beta = \sqrt{d} + \lfloor\sqrt{d}\rfloor$. Očito je broj β reduciran, pa po Teoremu 6.16 ima čisto periodičan razvoj

$$\sqrt{d} + \lfloor\sqrt{d}\rfloor = [\overline{b_0, b_1, \ldots, b_{r-1}}] = [b_0, \overline{b_1, \ldots, b_{r-1}, b_0}]. \tag{45}$$

Razvoji od β i $\sqrt{d}$ se razlikuju samo u prvom članu, tj. $b_i = a_i$ za $i \geq 1$. Uočimo da je $b_0 = \lfloor\sqrt{d} + \lfloor\sqrt{d}\rfloor\rfloor = 2\lfloor\sqrt{d}\rfloor$. Sada je

$$\begin{aligned}\sqrt{d} &= -\lfloor\sqrt{d}\rfloor + \beta = -\lfloor\sqrt{d}\rfloor + [2\lfloor\sqrt{d}\rfloor, \overline{b_1, \ldots, b_{r-1}, b_0}] \\ &= [\lfloor\sqrt{d}\rfloor, \overline{b_1, \ldots, b_{r-1}, b_0}] \\ &= [a_0, \overline{a_1, \ldots, a_{r-1}, 2a_0}].\end{aligned}$$

Da bi dokazali centralnu simetričnost, uočimo da je $\beta = b_0 + \frac{1}{\beta_1}$, gdje je

$$\begin{aligned}\beta_1 &= (\sqrt{d} - \lfloor\sqrt{d}\rfloor)^{-1} = -\frac{1}{\beta'} = -\frac{1}{\beta'_r} = (\text{zbog } 34) = [b_{r-1}, -\frac{1}{\beta'_{r-1}}] = \cdots \\ &= [b_{r-1}, b_{r-2}, \ldots, b_0, -\frac{1}{\beta'}] = [\overline{b_{r-1}, b_{r-2}, \ldots, b_0}].\end{aligned}$$

Dakle, $\beta = [b_0, \overline{b_{r-1}, b_{r-2}, \ldots, b_0}]$. Usporedimo li ovo s (45), dobivamo: $b_1 = b_{r-1}$, $b_2 = b_{r-2}$, $\ldots$.

Budući da je r duljina najmanjeg perioda, imamo da je $\beta_i = \beta$ akko $r|i$. Ako sada primijenimo algoritam (33) na $\beta_0 = \sqrt{d} + \lfloor\sqrt{d}\rfloor$, $t_0 = 1$, $s_0 = \lfloor\sqrt{d}\rfloor$, onda za sve $j \geq 0$ imamo:

$$\frac{s_{jr} + \sqrt{d}}{t_{jr}} = \beta_{jr} = \beta_0 = \frac{s_0 + \sqrt{d}}{t_0} = \lfloor\sqrt{d}\rfloor + \sqrt{d},$$

odnosno

$$s_{jr} - t_{jr}\lfloor\sqrt{d}\rfloor = (t_{jr} - 1)\sqrt{d},$$

pa je $t_{jr} = 1$ jer je $\sqrt{d}$ iracionalan. Nadalje, $t_i \neq 1$ za sve ostale vrijednosti od i. Zaista, $t_i = 1$ povlači $\beta_i = s_i + \sqrt{d}$. Međutim, β_i ima čisto periodski razvoj, pa je, po Teoremu 6.16, $-1 < s_i - \sqrt{d} < 0$. Odavde je $\sqrt{d} - 1 < s_i < \sqrt{d}$, tj. $s_i = \lfloor\sqrt{d}\rfloor$, pa je $\beta_i = \beta$, što povlači da $r|i$.

Neka je sada $t_i = -1$. Onda je $\beta = -s_i - \sqrt{d}$, pa Teorem 6.16 povlači da je $-s_i - \sqrt{d} > 1$ i $-1 < -s_i + \sqrt{d} < 0$, pa je $\sqrt{d} < s_i < -\sqrt{d} - 1$, što je očito nemoguće. □

Teorem 7.8.

$$p_n^2 - dq_n^2 = (-1)^{n+1} t_{n+1}, \quad \textit{za sve } n \geq -1.$$

Dokaz: Iz (33) imamo:

$$\sqrt{d} = \alpha_0 = \frac{\alpha_{n+1}p_n + p_{n-1}}{\alpha_{n+1}q_n + q_{n-1}} = \frac{(s_{n+1} + \sqrt{d})p_n + t_{n+1}p_{n-1}}{(s_{n+1} + \sqrt{d})q_n + t_{n+1}q_{n-1}}.$$

Budući da je $\sqrt{d}$ iracionalan, odavde slijedi

$$s_{n+1}q_n + t_{n+1}q_{n-1} - p_n = 0, \quad s_{n+1}p_n + t_{n+1}p_{n-1} - dq_n = 0.$$

Eliminirajući s_{n+1}, dobivamo

$$p_n^2 - dq_n^2 = (p_nq_{n-1} - p_{n-1}q_n)t_{n+1} = (-1)^{n-1}t_{n+1}.$$

□

Teorem 7.9. *Neka je d prirodan broj koji nije potpun kvadrat, te neka su $\frac{p_n}{q_n}$ konvergente u razvoju od $\sqrt{d}$. Neka je N cijeli broj, $|N| < \sqrt{d}$. Tada svako pozitivno rješenje $x = u$, $y = v$ jednadžbe $x^2 - dy^2 = N$, takvo da je $(u, v) = 1$, zadovoljava $u = p_n$, $v = q_n$ za neki $n \in \mathbb{N}$.*

Dokaz: Neka su E i M prirodni brojevi takvi da je $(E, M) = 1$ i $E^2 - \varrho M^2 = \sigma$, gdje je $\sqrt{\varrho}$ iracionalan i $0 < \sigma < \sqrt{\varrho}$. Ovdje su ϱ i σ realni brojevi, ne nužno cijeli. Tada je $\frac{E}{M} - \sqrt{\varrho} = \frac{\sigma}{M(E+M\sqrt{\varrho})}$ pa je

$$0 < \frac{E}{M} - \sqrt{\varrho} < \frac{\sqrt{\varrho}}{M(E + M\sqrt{\varrho})} = \frac{1}{M^2(\frac{E}{M\sqrt{\varrho}} + 1)} < \frac{1}{2M^2}\,.$$

Po Teoremu 6.11, $\frac{E}{M}$ je konvergenta u razvoju od $\sqrt{\varrho}$.

Ako je $N > 0$, uzmimo $\sigma = N$, $\varrho = d$, $E = u$, $M = v$, pa dobivamo tvrdnju teorema u ovom slučaju.

Ako je $N < 0$, onda je $v^2 - \frac{1}{d}u^2 = -\frac{N}{d}$, pa možemo uzeti $\sigma = -\frac{N}{d}$, $\varrho = \frac{1}{d}$, $E = v$, $M = u$. Dobivamo da je $\frac{v}{u}$ konvergenta u razvoju od $\frac{1}{\sqrt{d}}$. No, ako je $\frac{v}{u}$ n-ta konvergenta od $\frac{1}{\sqrt{d}}$, onda je $\frac{u}{v}$ $(n-1)$-va konvergenta od $\sqrt{d}$, pa je teorem dokazan i u ovom slučaju. □

Iz Teorema 7.7, 7.8 i 7.9 neposredno slijedi

Teorem 7.10. *Sva rješenja u prirodnim brojevima jednadžbi $x^2 - dy^2 = \pm 1$ nalaze se među $x = p_n$, $y = q_n$, gdje su $\frac{p_n}{q_n}$ konvergente u razvoju od $\sqrt{d}$. Neka je r duljina perioda u razvoju od $\sqrt{d}$.*

Ako je r paran, onda jednadžba $x^2 - dy^2 = -1$ nema rješenja, a sva rješenja od $x^2 - dy^2 = 1$ su dana sa $x = p_{nr-1}$, $y = q_{nr-1}$ za $n \in \mathbb{N}$.

Ako je r neparan, onda su sva rješenja jednadžbe $x^2 - dy^2 = -1$ dana sa $x = p_{nr-1}$, $y = q_{nr-1}$ za n neparan, dok su sva rješenja jednadžbe $x^2 - dy^2 = 1$ dana sa $x = p_{nr-1}$, $y = q_{nr-1}$ za n paran.

□

Teorem 7.11. *Ako je (x_1, y_1) najmanje rješenje u prirodnim brojevima jednadžbe $x^2 - dy^2 = 1$, onda su sva rješenja ove jednadžbe dana sa (x_n, y_n) za $n \in \mathbb{N}$, gdje su x_n i y_n prirodni brojevi definirani sa*

$$x_n + y_n\sqrt{d} = (x_1 + y_1\sqrt{d})^n. \tag{46}$$

Dokaz: Iz (46) slijedi $x_n - y_n\sqrt{d} = (x_1 - y_1\sqrt{d})^n$, pa je

$$x_n^2 - dy_n^2 = (x_1^2 - dy_1^2)^n = 1,$$

što znači da su (x_n, y_n) zaista rješenja.

Pretpostavimo sada da je (s,t) rješenje koje se ne nalazi u familiji

$$\{(x_n, y_n) : n \in \mathbb{N}\}.$$

Budući da je $x_1 + y_1\sqrt{d} > 1$ i $s + t\sqrt{d} > 1$, to postoji $m \in \mathbb{N}$ takav da je

$$(x_1 + y_1\sqrt{d})^m < s + t\sqrt{d} < (x_1 + y_1\sqrt{d})^{m+1}. \tag{47}$$

Pomnožimo li (47) sa $(x_1 - y_1\sqrt{d})^m$, dobivamo

$$1 < (s + t\sqrt{d})(x_1 - y_1\sqrt{d})^m < x_1 + y_1\sqrt{d}.$$

Definirajmo $a, b \in \mathbb{Z}$ s $a + b\sqrt{d} = (s + t\sqrt{d})(x_1 - y_1\sqrt{d})^m$. Imamo: $a^2 - db^2 = (s^2 - dt^2)(x_1^2 - dy_1^2)^m = 1$. Iz $a + b\sqrt{d} > 1$ slijedi $0 < a - b\sqrt{d} < 1$, pa je

$$\begin{aligned} 2a &= (a + b\sqrt{d}) + (a - b\sqrt{d}) > 0, \\ 2b\sqrt{d} &= (a + b\sqrt{d}) - (a - b\sqrt{d}) > 0. \end{aligned}$$

Stoga je (a,b) rješenje u prirodnim brojevima jednadžbe $x^2 - dy^2 = 1$ i $a + b\sqrt{d} < x_1 + y_1\sqrt{d}$, što je kontradikcija. □

Teorem 7.12. *Neka je (x_n, y_n), $n \in \mathbb{N}$ niz svih rješenja Pellove jednadžbe $x^2 - dy^2 = 1$ u prirodnim brojevima, zapisan u rastućem redosljedu. Uzmimo da je $(x_0, y_0) = (1, 0)$. Tada vrijedi:*

$$x_{n+2} = 2x_1x_{n+1} - x_n, \quad y_{n+2} = 2x_1y_{n+1} - y_n, \quad n \geq 0.$$

Dokaz: Vrijedi: $x_n + y_n\sqrt{d} = (x_1 + y_1\sqrt{d})^n$. Odavde je

$$\begin{aligned} (x_{n+1} + y_{n+1}\sqrt{d})(x_1 + y_1\sqrt{d}) &= x_{n+2} + y_{n+2}\sqrt{d}, \\ (x_{n+1} + y_{n+1}\sqrt{d})(x_1 - y_1\sqrt{d}) &= x_n + y_n\sqrt{d}. \end{aligned}$$

Sada imamo:

$$\begin{aligned} x_{n+2} &= x_1x_{n+1} + dy_1y_{n+1}, \\ x_n &= x_1x_{n+1} - dy_1y_{n+1}, \end{aligned}$$

odakle zbrajanjem dobivamo $x_{n+2} = 2x_1x_{n+1} - x_n$. Analogno je

$$\begin{aligned} y_{n+2} &= x_1y_{n+1} + y_1x_{n+1}, \\ y_n &= x_1y_{n+1} - y_1x_{n+1}, \end{aligned}$$

pa ponovo zbrajanjem dobivamo $y_{n+2} = 2x_1y_{n+1} - y_n$. □

Primjer 7.3. *Nađimo sva rješenja jednadžbi* $x^2-15y^2=-1$ *i* $x^2-15y^2=1$, *za koja vrijedi* $1<x<1000$.

Rješenje: Prema Primjeru 6.6 je $\sqrt{15}=[3,\overline{1,6}]$. Dakle, period $r=2$ je paran, pa jednadžba $x^2-15y^2=-1$ nema rješenja. Najmanje rješenje jednadžbe $x^2-15y^2=1$ je očito $(x_1,y_1)=(4,1)$. Dalje imamo: $x_2=8\cdot 4-1=31$, $y_2=8$; $x_3=8\cdot 31-4=244$, $y_3=63$, dok je već $x_4>1000$. ♢

Primjer 7.4. *Nađimo najmanja rješenja jednadžbi* $x^2-29y^2=-1$ *i* $x^2-29y^2=1$ *u prirodnim brojevima (ako postoje).*

Rješenje: Razvijanjem u verižni razlomak dobiva se

$$\sqrt{29}=[5,\overline{2,1,1,2,10}].$$

To znači da je period $r=5$ neparan, pa je najmanje rješenje od $x^2-29y^2=-1$ dano sa (p_4,q_4), a najmanje rješenje od $x^2-29y^2=1$ sa (p_9,q_9).

n	-1	0	1	2	3	4	5	6	7	8	9
a_n		5	2	1	1	2	10	2	1	1	2
p_n	1	5	11	16	27	70	727	1524	2251	3775	9801
q_n	0	1	2	3	5	13	135	283	418	701	1820

Dakle, $(p_4,q_4)=(70,13)$, $(p_9,q_9)=(9801,1820)$.
Uočimo da je $(70+13\sqrt{29})^2=9801+1820\sqrt{29}$. ♢

Zadatak 7.3. *Nađite najmanja rješenja u prirodnim brojevima jednadžbi*

$$x^2-13y^2=\pm 1,\quad x^2-14y^2=\pm 1,\quad x^2-31y^2=\pm 1.$$

Primjer 7.5. *Neka je* p *prost broj i* $p\equiv 1 \pmod 4$. *Dokažimo da tada jednadžba* $x^2-py^2=-1$ *ima rješenja.*

Rješenje: Neka je (x_1,y_1) najmanje rješenje jednadžbe $x^2-py^2=1$. Tada je x_1 neparan, a y_1 paran, Iz

$$\frac{x_1-1}{2}\cdot\frac{x_1+1}{2}=p\cdot\left(\frac{y_1}{2}\right)^2$$

i $\left(\frac{x_1-1}{2},\frac{x_1+1}{2}\right)=1$ slijedi da postoje $u,v\in\mathbb{N}$ takvi da je

$$\frac{x_1\pm 1}{2}=pu^2,\quad \frac{x_1\mp 1}{2}=v^2,\quad \frac{y_1}{2}=uv.$$

Odavde je $v^2-pu^2=\mp 1$. No, iz $u<y_1$ slijedi ovdje ne možemo imati predznak $+$, tj. vrijedi $v^2-pu^2=-1$. ♢

Zadatak 7.4. *Dokažite da za proizvoljni* $k\in\mathbb{Z}$ *jednadžba* $x^2-(k^2-1)y^2=-1$ *nema rješenja u cijelim brojevima* x *i* y.

Definicija 7.3. Eliptička krivulja E *nad* $\mathbb{Q}$ *je skup svih točaka* $(x, y) \in \mathbb{Q}^2$ *koje zadovoljavaju jednadžbu*

$$y^2 = f(x) = x^3 + ax^2 + bx + c,$$

gdje su $a, b, c \in \mathbb{Q}$ *i polinom* $f(x)$ *nema višestrukih korijena, zajedno s "točkom u beskonačnosti" koju ćemo označavati s* $\mathcal{O}$*. Slično se definira pojam eliptičke krivulje nad proizvoljnim poljem* $\mathbb{K}$*.*

Polinom $f(x)$ može imati 1 ili 3 realna korijena. U ovisnosti o tome, graf funkcije $y^2 = f(x)$ ima jednu ili dvije komponente.

Definirat ćemo operaciju zbrajanja na E. Neka su $P, Q \in E$. Povucimo pravac kroz točke P i Q. On siječe krivulju $y^2 = f(x)$ u tri točke. Treću točku označimo sa $P * Q$. Budući su koordinate točke P i Q racionalne, to su i koordinate točke $P * Q$ racionalne. Konačno, neka je $P + Q$ osnosimetrična točka točki $P * Q$ s obzirom na os x. Ako je $P = Q$, onda umjesto sekante povlačimo tangentu kroz točku P. Po definiciji stavljamo da je $P + \mathcal{O} = P$ za svaki $P \in E$.

Može se pokazati da je E uz ovako definiranu operaciju zbrajanja abelova grupa. Očito je $\mathcal{O}$ neutralni element, dok je $-P$ osnosimetrična točka točki P u odnosu na os x. Najteže je provjeriti asocijativnost. To se može napraviti korištenjem eksplicitnih formula za zbrajanje, koje ćemo sada navesti.

Ako je $P = (x_1, y_1)$, $Q = (x_2, y_2)$, onda je

$$\begin{aligned} x(P + Q) &= \left(\frac{y_2 - y_1}{x_2 - x_1}\right) - a - x_1 - x_2, \\ x(2P) &= \frac{x_1^4 - 2bx_1^2 - 8cx_1 + b^2 - 4ac}{4y_1^2}. \end{aligned}$$

Važna činjenica o eliptičkim krivuljama nad $\mathbb{Q}$ je *Mordell-Weilov teorem* koji kaže da je grupa E konačno generirana. To znači da postoji konačno mnogo točaka $P_1, \ldots, P_n$ sa svojstvom da se sve točke na E mogu dobiti iz njih metodom sekante i tangente. Preciznije, svaka točka $P \in E$ ima oblik $P = m_1P_1 + \cdots m_nP_n$, $m_i \in \mathbb{Z}$.

Mordell je dokazao i drugi važan teorem o eliptičkim krivuljama koji kaže da je broj cjelobrojnih točaka na eliptičkoj krivulji konačan. Općenito je problem nalaženja svih cjelobrojnih točaka na eliptičkoj krivulji vrlo težak. Međutim u nekim specijalnim slučajevima moguće ga je riješiti prilično jednostavno.

Primjer 7.6. *Dokazati da jednadžba* $y^2 = x^3 + 7$ *nema cjelobrojnih rješenja.*

Rješenje: Budući da je $y^2 \equiv 0, 1 \pmod 4$, slijedi da je x neparan. Štoviše, $x \equiv 1 \pmod 4$. Prikažimo danu jednadžbu u obliku

$$y^2 + 1 = (x + 2)(x^2 - 2x + 4).$$

Prema Teoremu 2.14, svi prosti faktori od $y^2 + 1$ su oblika $4k + 1$. S druge strane, desna strana jednadžbe ima faktor $x + 2$ koji je pozitivan i $\equiv 3 \pmod 4$. Dakle, dana jednadžba nema rješenja. $\diamondsuit$

8. Kvadratna polja

Definicija 8.1. *Algebarski broj z je* algebarski cijeli broj *ako njegov minimalni polinom ima cjelobrojne koeficijente.*

Propozicija 8.1. *Među racionalnim brojevima jedini algebarski cijeli brojevi su upravo cijeli brojevi.*

Dokaz: Svaki $m \in \mathbb{Z}$ je algebarski cijeli broj jer poništava polinom $f(x) = x - m$. S druge strane, ako je $\frac{m}{q}$ algebarski cijeli broj, onda možemo pretpostaviti da je $(m, q) = 1$, pa imamo

$$\Big(\frac{m}{q}\Big)^n + a_1\Big(\frac{m}{q}\Big)^{n-1} + \cdots + a_n = 0,$$
$$m^n + a_1 q m^{n-1} + \cdots + a_n q^n = 0.$$

Dakle, $q | m^n$, pa je $q = \pm 1$, što znači da je $\frac{m}{q} \in \mathbb{Z}$. □

Definicija 8.2. *Neka je d kvadratno slobodan cijeli broj i $d \neq 1$.* Kvadratno polje $\mathbb{Q}(\sqrt{d})$ *je skup svih brojeva oblika $u + v\sqrt{d}$, $u, v \in \mathbb{Q}$, uz uobičajene operacije zbrajanja i množenja kompleksnih brojeva.*

Lako se provjeri da je $\mathbb{Q}(\sqrt{d})$ stvarno polje. Na primjer, $(u + v\sqrt{d})^{-1} = \frac{u - v\sqrt{d}}{u^2 - dv^2}$.

Za svaki element $\alpha = u + v\sqrt{d} \in \mathbb{Q}(\sqrt{d})$ definira se *norma* od α kao $N(\alpha) = u^2 - dv^2$. Dakle, $N(\alpha) = \alpha\overline{\alpha}$, gdje je $\overline{\alpha} = u - v\sqrt{d}$ konjugat od α. Specijalno, polje $\mathbb{Q}(\sqrt{-1})$ se zove *polje Gaussovih brojeva* i uobičajeno je njegove elemente označavati u obliku $u + iv$. U ovom slučaju je $N(\alpha) = u^2 + v^2$.

Teorem 8.2. *Ako je $d \equiv 2$ ili $3 \pmod 4$, onda su algebarski cijeli brojevi u $\mathbb{Q}(\sqrt{d})$ svi brojevi oblika $u + v\sqrt{d}$, $u, v \in \mathbb{Z}$. Ako je $d \equiv 1 \pmod 4$, onda su algebarski cijeli brojevi u $\mathbb{Q}(\sqrt{d})$ svi brojevi oblika $s + t \cdot \frac{1+\sqrt{d}}{2}$, $s, t \in \mathbb{Z}$. Drugim riječima, algebarski cijeli brojevi u $\mathbb{Q}(\sqrt{d})$ su svi brojevi oblika $u + v\sqrt{d}$, $u, v \in \mathbb{Z}$, te ako je $d \equiv 1 \pmod 4$, još i brojevi oblika $\frac{u+v\sqrt{d}}{2}$, u, v neparni.*

Dokaz: Neka je $\alpha = u + v\sqrt{d}$ algebarski cijeli broj u $\mathbb{Q}(\sqrt{d})$, te neka je $a = 2u$, $b = 2v$, $c = N(\alpha) = u^2 - dv^2$. Tada je α nultočka polinoma $f(x) = x^2 - ax + c$. Prema tome, racionalni brojevi a i c moraju biti cijeli. Imamo $db^2 = a^2 - 4c$ i budući je d kvadratno slobodan, vidimo da je i $b \in \mathbb{Z}$.

Neka je sada $d \equiv 2$ ili $3 \pmod 4$. Iz $a^2 \equiv b^2 d \pmod 4$, $a^2 \equiv 0$ ili $1 \pmod 4$, $b^2 d \equiv 0$, 2 ili $3 \pmod 4$, slijedi da su a i b parni brojevi, pa su $u, v \in \mathbb{Z}$.

Ako je $d \equiv 1 \pmod 4$, onda iz $a^2 \equiv b^2 \pmod 4$ slijedi da su a i b iste parnosti. Stoga je broj $u - v = \frac{1}{2}(a - b)$ cijeli. Stavimo: $s = u - v$, $t = 2v$. Tada je $s, t \in \mathbb{Z}$ i $u + v\sqrt{d} = s + t \cdot \frac{1+\sqrt{d}}{2}$. □

Definicija 8.3. Jedinica *(ili invertibilni element) u* $\mathbb{Q}(\sqrt{d})$ *je algebarski cijeli broj* ε *sa svojstvom da je* $\frac{1}{\varepsilon}$ *također algebarski cijeli broj.*

Teorem 8.3.

1) $N(\alpha\beta) = N(\alpha)N(\beta)$

2) $N(\alpha) = 0 \iff \alpha = 0$

3) Ako je α *algebarski cijeli broj u* $\mathbb{Q}(\sqrt{d})$*, onda je* $N(\alpha) \in \mathbb{Z}$.

4) Neka je γ *algebarski cijeli broj u* $\mathbb{Q}(\sqrt{d})$*. Tada je* γ *jedinica ako i samo ako je* $N(\gamma) = \pm 1$.

Dokaz: 1) Neka je $\alpha = u + v\sqrt{d}$, $\beta = s + t\sqrt{d}$. Tada je

$$\begin{aligned}\overline{\alpha\beta} &= \overline{(us + vtd + (ut + vs)\sqrt{d})} = us + vtd - (ut + vs)\sqrt{d} \\ &= (u - v\sqrt{d})(s - t\sqrt{d}) = \overline{\alpha} \cdot \overline{\beta}.\end{aligned}$$

Prema tome,

$$N(\alpha\beta) = \alpha\beta\overline{\alpha\beta} = \alpha\beta\overline{\alpha}\overline{\beta} = (\alpha\overline{\alpha})(\beta\overline{\beta}) = N(\alpha)N(\beta).$$

2) Ako je $\alpha = 0$, onda je $\overline{\alpha} = 0$ i $N(\alpha) = 0$. Ako je $N(\alpha) = 0$, onda je $\alpha\overline{\alpha} = 0$, pa je $\alpha = 0$ ili $\overline{\alpha} = 0$. No, $\overline{\alpha} = 0$ povlači $\alpha = 0$.

3) Dokazano u dokazu Teorema 8.2.

4) Ako je γ jedinica, onda je $N(\gamma)N(\frac{1}{\gamma}) = N(1) = 1$, pa budući su $N(\gamma)$ i $N(\frac{1}{\gamma})$ cijeli brojevi, slijedi da je $N(\gamma) = \pm 1$.

Obratno, ako je $N(\gamma) = \pm 1$, onda je $\gamma\overline{\gamma} = 1$, pa je $\frac{1}{\gamma} = \pm\overline{\gamma}$ algebarski cijeli broj, što znači da je γ jedinica. □

Za kvadratno polje $\mathbb{Q}(\sqrt{d})$ kažemo da je *realno* ako je $d > 0$, a *imaginarno* ako je $d < 0$.

Teorem 8.4. *Neka je* d *negativan kvadratno slobodan cijeli broj. Kvadratno polje* $\mathbb{Q}(\sqrt{d})$ *ima jedinice* ± 1 *i to su jedine jedinice osim u slučajevima* $d = -1$ *i* $d = -3$*. Jedinice u* $\mathbb{Q}(i)$ *su* ± 1, $\pm i$*, a u* $\mathbb{Q}(\sqrt{-3})$ *su* ± 1, $\frac{1\pm\sqrt{-3}}{2}$, $\frac{-1\pm\sqrt{-3}}{2}$.

Dokaz: Prema Teoremu 8.3.4), moramo pronaći sve algebarske cijele brojeve α takve da je $N(\alpha) = \pm 1$. Ako je $d \equiv 2$ ili $3 \pmod 4$, onda α ima oblik $\alpha = x + y\sqrt{d}$, $x, y \in \mathbb{Z}$, pa treba riješiti jednadžbu $x^2 - dy^2 = \pm 1$. Budući da je d negativan, to slučaj $x^2 - dy^2 = -1$ otpada. Ako je $d \leq -2$, onda

je $x^2 - dy^2 \geq 2y^2$, pa je jedino rješenje $y = 0$, $x = \pm 1$, otkuda je $\alpha = \pm 1$. Ako je $d = -1$, onda imamo jednadžbu $x^2 + y^2 = 1$ čija su rješenja $x = \pm 1$, $y = 0$ i $x = 0$, $y = \pm 1$, tj. $\alpha = \pm 1, \pm i$.

Ako je $d \equiv 1 \pmod 4$, onda α ima oblik $x + y \cdot \frac{1+\sqrt{d}}{2}$, pa je $N(\alpha) = (x + \frac{y}{2})^2 - \frac{1}{4}dy^2$. Ponovo, zbog $d < 0$, jednadžba $N(\alpha) = -1$ nema rješenja. Ako je $d \leq -7$, onda je $(x + \frac{y}{2})^2 - \frac{1}{4}dy^2 \geq \frac{7}{4}y^2$, pa iz $N(\alpha) = 1$ slijedi $y = 0$, $x = \pm 1$, tj. $\alpha = \pm 1$. Ako je $d = -3$, onda imamo jednadžbu

$$\left(x + \frac{y}{2}\right)^2 + \frac{3}{4}y^2 = 1, \tag{48}$$

odnosno $x^2 + xy + y^2 = 1$. Iz (48) slijedi $|y| \leq 1$. Ako je $y = 0$, onda je $x = \pm 1$, pa je $\alpha = \pm 1$. Ako je $y = 1$, onda je $x = 0$ ili $x = -1$, pa je $\alpha = \frac{1+\sqrt{-3}}{2}$ ili $\alpha = \frac{-1+\sqrt{-3}}{2}$, ako je $y = -1$, onda je $x = 0$ ili $x = -1$, pa je $\alpha = \frac{-1-\sqrt{-3}}{2}$ ili $\alpha = \frac{1-\sqrt{-3}}{2}$. □

Teorem 8.5. *U svakom realnom kvadratnom polju postoji beskonačno mnogo jedinica.*

Dokaz: Brojevi $\alpha = x + y\sqrt{d}$, $x, y \in \mathbb{Z}$, su algebarski cijeli brojevi u $\mathbb{Q}(\sqrt{d})$ s normom $N(\alpha) = x^2 - dy^2$. Ako je $x^2 - dy^2 = 1$, onda je α jedinica. No, jednadžba $x^2 - dy^2 = 1$ je Pellova jednadžba i ona, za kvadratno slobodan broj $d > 1$, ima beskonačno mnogo rješenja. □

Definicija 8.4. *Za algebarske cijele brojeve α, β kažemo da α* dijeli *β i pišemo $\alpha|\beta$ ako postoji algebarski cijeli broj γ takav da je $\beta = \alpha\gamma$. Prema tome, jedinice su upravo djelitelji broja 1. Kažemo da su α i β* pridruženi (asocirani) *ako je α/β jedinica.*

Algebarski cijeli broj α koji nije jedinica u $\mathbb{Q}(\sqrt{d})$ zove se prost *ako je djeljiv samo s jedinicama i sebi pridruženim brojevima. To je slično kao u $\mathbb{Q}$, jedino smo tamo tražili da je prost broj pozitivan, a ovdje ako je π prost i ε jedinica, onda je i $\varepsilon\pi$ prost.*

Teorem 8.6. *Ako je norma algebarskog cijelog broja α u $\mathbb{Q}(\sqrt{d})$ jednaka $\pm p$, gdje je p prost broj, onda je α prost.*

Dokaz: Pretpostavimo da je $\alpha = \beta\gamma$, gdje su β i γ cijeli u $\mathbb{Q}(\sqrt{d})$. Po teoremu 8.3.1), $N(\alpha) = N(\beta)N(\gamma) = \pm p$. Budući su $N(\beta)$ i $N(\gamma)$ cijeli brojevi, jedan od njih mora biti jednak ± 1. Prema tome, jedan od brojeva β, γ je jedinica, a drugi je pridružen α. □

Teorem 8.7. *Svaki algebarski cijeli broj α u $\mathbb{Q}(\sqrt{d})$, koji nije 0 ni jedinica, može se prikazati kao produkt prostih brojeva u $\mathbb{Q}(\sqrt{d})$.*

Dokaz: Ako α nije prost, onda se može rastaviti na produkt $\beta\gamma$, gdje β i γ nisu jedinice. Nastavljajući ovaj postupak, faktoriziramo β i γ ako nisu prosti. Ovaj proces faktorizacije mora završiti budući bi inače dobili da α

ima oblik $\beta_1\beta_2\cdots\beta_n$, gdje je n po volji velik, a niti jedan od β_j nije jedinica. To bi povlačilo da je

$$|N(\alpha)| = \prod_{j=1}^{n} |N(\beta_j)| \geq 2^n,$$

jer je $|N(\beta_j)|$ prirodan broj veći od 1. No, to je očito kontradikcija. □

Iako smo pokazali da faktorizacija na proste faktore u $\mathbb{Q}(\sqrt{d})$ uvijek postoji, ona ne mora biti jedinstvena.

Primjer 8.1. *Promotrimo broj* 10 *i njegove dvije faktorizacije u* $\mathbb{Q}(\sqrt{-6})$*:*

$$10 = 2 \cdot 5 = (2 + \sqrt{-6})(2 - \sqrt{-6}).$$

Brojevi 2, 5, $2 + \sqrt{-6}$, $2 - \sqrt{-6}$ *su prosti u* $\mathbb{Q}(\sqrt{-6})$*. Zaista, primjetimo najprije da ako algebarski cijeli broj* α *u* $\mathbb{Q}(\sqrt{-6})$ *nije* 0 *ni jedinica, onda je* $N(\alpha) = N(a + b\sqrt{-6}) = a^2 + 6b^2 \geq 4$ *i* $N(\alpha) \neq 5$*. Ako je sada* $2 = \alpha\beta$*, onda iz* $N(\alpha)N(\beta) = 4$ *slijedi da je* $N(\alpha) = \pm 1$ *ili* $N(\beta) = \pm 1$*. Analogno, ako je* $5 = \alpha\beta$*, onda iz* $N(\alpha)N(\beta) = 25$ *slijedi* $N(\alpha) = \pm 1$ *ili* $N(\beta) = \pm 1$*. Konačno, ako je* $2 \pm \sqrt{-6} = \alpha\beta$*, onda iz* $N(\alpha)N(\beta) = 10$ *ponovo slijedi* $N(\alpha) = \pm 1$ *ili* $N(\beta) = \pm 1$*.*

Prema tome, broj 10 *nema jedinstvenu faktorizaciju na proste faktore u* $\mathbb{Q}(\sqrt{-6})$*.* ♢

Važno pitanje je za koje vrijednosti od d, $\mathbb{Q}(\sqrt{d})$ ima svojstvo jedinstvene faktorizacije. Vidjet ćemo da je to pitanje u vezi s Euklidovim algoritmom.

Definicija 8.5. *Kažemo da kvadratno polje* $\mathbb{Q}(\sqrt{d})$ *ima* svojstvo jedinstvene faktorizacije *ako se svaki algebarski cijeli broj u* $\mathbb{Q}(\sqrt{d})$*, koji nije* 0 *ni jedinica, može faktorizirati na proste faktore jednoznačno, do na poredak faktora i zamjenu faktora pridruženim brojevima.*

Za kvadratno polje kažemo da je euklidsko *ako algebarski cijeli brojevi u* $\mathbb{Q}(\sqrt{d})$ *zadovoljavaju Euklidov algoritam, tj. ako za* α, β *cijele u* $\mathbb{Q}(\sqrt{d})$*,* $\beta \neq 0$*, postoje algebarski cijeli brojevi* γ *i* δ *u* $\mathbb{Q}(\sqrt{d})$ *takvi da je* $\alpha = \beta\gamma + \delta$ *i* $|N(\delta)| < |N(\beta)|$*.*

Teorem 8.8. *Svako euklidsko kvadratno polje ima svojstvo jedinstvene faktorizacije.*

Dokaz: Pokažimo najprije da ako su α i β algebarski cijeli brojevi u $\mathbb{Q}(\sqrt{d})$ koji nemaju zajedničkih djelitelja osim jedinica, onda postoje algebarski cijeli brojevi λ_0, μ_0 u $\mathbb{Q}(\sqrt{d})$ takvi da je

$$\alpha\lambda_0 + \beta\mu_0 = 1.$$

Neka je $\mathcal{S}$ skup svih brojeva oblika $\alpha\lambda + \beta\mu$ kad λ i μ prolaze skupom svih algebarskih cijelih brojeva u $\mathbb{Q}(\sqrt{d})$. Brojevi $|N(\alpha\lambda + \beta\mu)|$ su nenegativni cijeli brojevi, pa izaberimo element $\varepsilon = \alpha\lambda_1 + \beta\mu_1$ skupa $\mathcal{S}$ takav da $|N(\varepsilon)|$ poprima najmanju pozitivnu vrijednost među brojevima $|N(\alpha\lambda+\beta\mu)|$. Primjenom Euklidovog algoritma na brojeve α i ε dobivamo

$$\alpha = \varepsilon\gamma + \delta, \quad |N(\delta)| < |N(\varepsilon)|.$$

Tada je $\delta = \alpha - \gamma(\alpha\lambda_1 + \beta\mu_1) = \alpha(1 - \gamma\lambda_1) + \beta(-\gamma\mu_1) \in \mathcal{S}$. Po definiciji od ε imamo da je $N(\delta) = 0$, tj. $\delta = 0$. Dakle, $\alpha = \varepsilon\gamma$ i $\varepsilon|\alpha$. Slično se pokazuje da $\varepsilon|\beta$, pa je ε jedinica. Sada je i ε^{-1} jedinica i imamo:

$$1 = \varepsilon^{-1}\varepsilon = \varepsilon^{-1}(\alpha\lambda_1 + \beta\mu_1) = \alpha(\varepsilon^{-1}\lambda_1) + \beta(\varepsilon^{-1}\mu_1) = \alpha\lambda_0 + \beta\mu_0.$$

Dokažimo sada da ako je π prost u $\mathbb{Q}(\sqrt{d})$ i ako $\pi|\alpha\beta$, onda $\pi|\alpha$ ili $\pi|\beta$. Zaista, ako $\pi \nmid \alpha$, onda π i α nemaju zajedničkih djelitelja osim jedinica, pa postoje algebarski cijeli brojevi λ_0 i μ_0 takvi da je $\pi\lambda_0 + \alpha\mu_0 = 1$. Tada je $\beta = \pi\beta\lambda_0 + \alpha\beta\mu_0$, pa $\pi|\beta$. Odavde indukcijom slijedi da ako $\pi|(\alpha_1 \cdots \alpha_n)$, onda π dijeli neki α_j.

Dalje je dokaz identičan dokazu Teorema 1.10. □

Poznato je da postoji točno 21 euklidsko polje $\mathbb{Q}(\sqrt{d})$ (Chatland i Davenport (1950)):

$$d = -11, -7, -3, -2, -1, 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 41, 57, 73.$$

To nisu sva polja s jedinstvenom faktorizacijom. Baker i Stark su 1966. pokazali da ako, je $d < 0$, onda je $d = -1, -2, -3, -7, -11, -19, -43, -67, -163$ (usporedite ovu listu s listom negativnih diskriminanti d za koje je broj klasa $h(d) = 1$). Hipoteza je da za $d > 0$ takvih polja ima beskonačno.

Teorem 8.9. *Kvadratna polja $\mathbb{Q}(\sqrt{d})$ za $d = -11, -7, -3, -2, -1, 2, 3, 5$ su euklidska.*

Dokaz: Neka su α, β algebarski cijeli brojevi u $\mathbb{Q}(\sqrt{d})$ i $\beta \neq 0$. Tada je $\frac{\alpha}{\beta} = u + v\sqrt{d}$, $u, v \in \mathbb{Q}$. Odaberimo $x, y \in \mathbb{Z}$ koji su najbliži u i v, tj.

$$0 \leq |u - x| \leq \frac{1}{2}, \quad 0 \leq |v - y| \leq \frac{1}{2}.$$

Označimo: $x + y\sqrt{d} = \gamma$, $\alpha - \beta\gamma = \delta$. Brojevi γ i δ su cijeli u $\mathbb{Q}(\sqrt{d})$ i

$$\begin{aligned} N(\delta) &= N(\alpha - \beta\gamma) = N(\beta)N(\frac{\alpha}{\beta} - \gamma) = N(\beta)N((u - x) + (v - y)\sqrt{d}) \\ &= N(\beta)[(u - x)^2 - d(v - y)^2], \end{aligned}$$

pa je

$$|N(\delta)| = |N(\beta)| \cdot |(u - x)^2 - d(v - y)^2|. \tag{49}$$

Ako je $d > 0$, onda je $-\frac{d}{4} \leq (u-x)^2 - d(v-y)^2 \leq \frac{1}{4}$, a ako je $d < 0$, onda je $0 \leq (u-x)^2 - d(v-y)^2 \leq \frac{1}{4} + \frac{1}{4}(-d)$. Prema tome, ako je $d = 2, 3, -1, -2$, onda iz (49) dobivamo $|N(\delta)| < |N(\beta)|$, pa je za te vrijednosti od d polje $\mathbb{Q}(\sqrt{d})$ euklidsko.

Za $d = -11, -7, -3, 5$ postupamo malo drugačije. Uočimo da je u svim ovim slučajevima $d \equiv 1 \pmod 4$. Neka su u i v definirani kao prije. Izaberimo $y \in \mathbb{Z}$ najbliži broju $2v$ i stavimo $s = v - \frac{1}{2}y$. Tada je $|s| \leq \frac{1}{4}$. Nadalje, izaberimo $x \in \mathbb{Z}$ najbliži broju $u - \frac{1}{2}y$ i stavimo $r = u - x - \frac{1}{2}y$. Tada je $|r| \leq \frac{1}{2}$. Označimo: $x + y \cdot \frac{1+\sqrt{d}}{2} = \gamma$, $\alpha - \beta\gamma = \delta$. Sada je $N(\delta) = N(\beta)(r^2 - ds^2)$. Budući da je $|d| \leq 11$, imamo $|r^2 - ds^2| \leq \frac{1}{4} + 11 \cdot \frac{1}{16} < 1$, pa je $|N(\delta)| < |N(\beta)|$, što je i trebalo dokazati. □

Teorem 8.10. *Neka $\mathbb{Q}(\sqrt{d})$ ima svojstvo jedinstvene faktorizacije. Tada svakom prostom broju π u $\mathbb{Q}(\sqrt{d})$ odgovara točno jedan prost prirodan broj p takav da $\pi|p$.*

Dokaz: Prost broj π dijeli cijeli broj $N(\pi)$, pa prema tome postoje prirodni brojevi koji su djeljivi sa π. Neka je p najmanji takav broj. Dokažimo da je p prost. U protivnom bi bilo $p = n_1 n_2$, pa zbog svojstva jedinstvene faktorizacije $\pi|n_1$ ili $\pi|n_2$, što je kontradikcija budući da je $1 < n_1, n_2 < p$.

Pretpostavimo da π dijeli još neki prost prirodan broj q. Tada je $(p, q) = 1$, pa postoje cijeli brojevi x, y takvi da je $px + qy = 1$. Odavde slijedi da $\pi|1$, što je kontradikcija. Prema tome, prost broj p je jedinstven. □

Teorem 8.11. *Prosti brojevi u $\mathbb{Q}(i)$ su prosti brojevi oblika $p = 4k + 3$, faktori π, π' iz faktorizacije $p = \pi\pi'$ prostih prirodnih brojeva oblika $p = 4k + 1$, broj $1 + i$, te brojevi koji su pridruženi gore navedenima (tj. oni koji se dobiju iz njih množenjem s ± 1 ili $\pm i$).*

Dokaz: Neka je p prost prirodan broj. Ako je p djeljiv s nekim prostim brojem π u $\mathbb{Q}(i)$, onda iz $p = \pi\lambda$ slijedi $N(\pi)N(\lambda) = p^2$. Sada imamo dvije mogućnosti: ili je $N(\lambda) = 1$, što znači da je p prost u $\mathbb{Q}(i)$, ili je $N(\lambda) = p$, što povlači da je $N(\pi) = p$, pa je $p = \pi\lambda$ produkt dva prosta broja u $\mathbb{Q}(i)$.

Ako je $p \equiv 3 \pmod 4$, onda ne može biti $N(\pi) = N(a+bi) = a^2 + b^2 = p$. Stoga je p prost u $\mathbb{Q}(i)$.

Ako je $p \equiv 1 \pmod 4$, onda postoje prirodni brojevi a, b takvi da je $p = a^2 + b^2 = (a+bi)(a-bi)$, te su u skladu s prijašnjom diskusijom brojevi $a + bi$ i $a - bi$ prosti u $\mathbb{Q}(i)$.

Za broj 2 imamo: $2 = (1+i)(1-i)$. Brojevi $1 + i$, $1 - i$ su prosti u $\mathbb{Q}(i)$, a k tome su i pridruženi, čime je dokaz dovršen. □

Primjer 8.2. *Naći sva cjelobrojna rješenja jednadžbe $y^2 = x^3 - 11$.*

Rješenje: Iz Teorema 8.10 znamo da $\mathbb{Q}(\sqrt{-11})$ ima svojstvo jedinstvene faktorizacije. Jedinice u $\mathbb{Q}(\sqrt{-11})$ su ± 1. Stoga iz

$$(y + \sqrt{-11})(y - \sqrt{-11}) = x^3$$

slijedi da postoji algebarski cijeli broj $w \in \mathbb{Q}(i)$ takav da je

$$y + \sqrt{-11} = \pm w^3.$$

Budući da je $-w^3 = (-w)^3$, predznak $-$ možemo izostaviti. Dakle,

$$y + \sqrt{-11} = w^3, \quad w = a + \frac{b}{2}(1 + \sqrt{-11}) = (a + \frac{b}{2}) + \frac{b}{2}\sqrt{-11}.$$

Izjednačavanjem koeficijenata uz $\sqrt{-11}$, dobivamo:

$$1 = 3(a + \frac{b}{2})^2 \cdot \frac{b}{2} - 11 \cdot (\frac{b}{2})^3,$$

odnosno

$$b(3a^2 + 3ab - 2b^2) = 2.$$

Odavde je $b = \pm 1$ ili ± 2, pa je $(a, b) = (0, -1), (1, -1), (1, 2), (-3, 2)$. Sada iz $y = (a + \frac{b}{2})^2 + 3(a + \frac{b}{2}) \cdot (\frac{b}{2})^2 \cdot (-11)$ slijedi $y = \pm 4, \pm 58$, pa su sva rješenja zadane jednadžbe $(x, y) = (3, \pm 4),\ (15, \pm 58)$. ♢