UNIVERZA NA PRIMORSKEM
FAKULTETA ZA MATEMATIKO, NARAVOSLOVJE IN
INFORMACIJSKE TEHNOLOGIJE

Magistrsko delo

Nekatere kvadratne diofantske enačbe

(On Some Quadratic Diophantine Equations)

Ime in priimek: *Pia Modrijan*
Študijski program: *Matematične znanosti, 2. stopnja*
Mentor: *prof. dr. Štefko Miklavič*

Koper, maj 2021

Ključna dokumentacijska informacija

Ime in PRIIMEK: Pia MODRIJAN
Naslov magistrskega dela: Nekatere kvadratne diofantske enačbe

Kraj: Koper
Leto: 2021

Število listov: 58
Število referenc: 25
Mentor: prof. dr. Štefko Miklavič

UDK: 511.5(043.2)
Ključne besede: kvadratne diofantske enačbe, teorija števil, Fundamentalni izrek aritmetike, Pitagorova enačba, vsota kvadratov, kvadratne kongruence, Pellova enačba, kvadratne forme
Math. Subj. Class. (2010): 11D09
Izvleček:
V magistrskem delu so predstavljene različne diofantske enačbe in njihove rešitve. V ospredje so postavljene kvadratne diofantske enačbe. V uvodnem poglavju so zapisane definicije in izreki iz področja teorije števil ter algebre, ki služijo kot podlaga za nadaljnje vsebine. V naslednjem poglavju je predstavljen Fundamentalni izrek aritmetike in s pomočjo tega izreka so rešene različne diofantske enačbe. V tem poglavju so na kratko predstavljene tudi diofantske enačbe višjega reda in trije slavni diofantski problemi, ki so svojo rešitev dobili šele pred kratkim. V zadnjem poglavju je predstavljeno reševanje kvadratnih kongruenc. V nadaljevanju tega poglavja je zapisan izrek, ki pove, kdaj ima enačba $x^2 - dy^2 = 1$ neskončno mnogo celoštevilskih rešitev. Na koncu pa je predstavljeno še reševanje enačbe $ax^2 + bxy + cy^2 = n$, ločeno na dva različna primera.

Key document information

Name and SURNAME: Pia MODRIJAN
Title of the thesis: On Some Quadratic Diophantine Equations

Place: Koper
Year: 2021

Number of pages: 58
Number of references: 25
Mentor: Prof. Štefko Miklavič, PhD

UDC: 511.5(043.2)
Keywords: quadratic Diophantine equations, number theory, Fundamental theorem of arithmetic, Pythagorean equation, sum of squares, quadratic congruences, Pell's equation, quadratic forms
Math. Subj. Class. (2010): 11D09
Abstract:
In the master's thesis, various Diophantine equations and their solutions are presented. Quadratic Diophantine equations are placed in the foreground. The introductory chapter contains definitions and theorems from the field of number theory and algebra, which serve as a basis for further content. In the next chapter, the Fundamental Theorem of Arithmetic is presented, and various Diophantine equations are solved with the help of this theorem. This chapter also briefly presents higher-order Diophantine equations and three famous Diophantine problems, which have only recently been solved. In the last chapter, the solution of quadratic congruences are presented. In the continuation of this chapter, a theorem that tells when the equation $x^2 - dy^2 = 1$ has infinitely many integer solutions, is written. In the end, the solution of the equation $ax^2 + bxy + cy^2 = n$, separated into two different examples, is presented.

Kazalo vsebine

Seznam kratic

tj. to je

Zahvala

V prvi vrsti bi se rada zahvalila svojemu mentorju, prof. dr. Štefku Miklaviču, za hitro odzivnost, strokovno pomoč, nasvete ter usmerjanje pri pisanju magistrskega dela.

Prav tako bi se rada zahvalila tudi vsem ostalim profesorjem in asistentom na fakulteti, ki so mi tekom študija predali veliko uporabnega znanja.

Nenazadnje bi se zahvalila še vsem svojim bližnjim, ki so me skozi vsa leta študija podpirali in spodbujali, ter mi s tem pomagali doseči želeni cilj.

1 UVOD

Osrednja tema mojega magistrskega dela bodo kvadratne diofantske enačbe, katerih reševanje je veliko bolj zakomplicirano kot reševanje linearnih diofantskih enačb. Linearno diofantsko enačbo v splošnem zapišemo kot $ax + by = c$, kvadratno diofantsko enačbo pa kot $ax^2+by^2 = c$. Posebnost teh enačb je, da nas zanimajo samo celoštevilske rešitve.

Diofantske enačbe so ime dobile po matematiku Diofantu, ki je živel in delal v Aleksandriji v Egiptu. O njem ni veliko znanega, vendar zgodovinarji ocenjujejo, da se je rodil približno 200 let po našem štetju in umrl leta 284 po našem štetju. Njegovo najbolj znano delo je Aritmetika, ki vsebuje 13 knjig in 130 problemov. Od teh 13 knjig se jih je do danes žal ohranilo le 6.
Prvi, ki je predstavil splošno rešitev linearne diofantske enačbe $ax + by = c$, je bil indijski matematik Brahmagupta. Živel je v letih 598 do 668 po našem štetju. Poleg linearne diofantske enačbe v splošnem, je rešil tudi nekatere posebne primere kvadratnih diofantskih enačb.

Do danes ostaja še veliko odprtih problemov na področju diofantskih enačb, kljub temu pa so te enačbe v praksi zelo uporabne. Uporabljajo se na različnih področjih, najbolj pa velja izpostaviti uporabo na področju teorije kodiranja in kriptografije.

Magistrsko delo je v grobem razdeljeno na tri dele. Poglavje 2 je namenjeno spoznavanju z osnovami iz področja teorije števil in algebre. Tukaj je povzeto znanje, ki je nujno potrebno za razumevanje nadaljnjih vsebin. Glavni cilj poglavij 3 in 4 pa je predstaviti nekatere kvadratne diofantske enačbe in poiskati njihove rešitve.
Poglavje 2 je v večini povzeto po študijskih zapiskih, glavna literatura za poglavji 3 in 4 pa je knjiga [6].

2 UVODNE DEFINICIJE IN IZREKI

V tem poglavju se bomo spoznali z definicijami in izreki iz področja teorije števil in algebre. To znanje bomo potrebovali v nadaljevanju magistrskega dela.

2.1 TEORIJA ŠTEVIL

Izrek 2.1. *(Izrek o deljenju) Vzemimo celi števili a in b in naj bo $b \neq 0$. Potem obstajata enolično določeni celi števili q in r, za kateri je $a = qb + r$. Pri tem je $0 \leq r < |b|$. Števili q in r imenujemo kvocient oziroma ostanek pri deljenju števila a s številom b.*

Primer 2.2. Vzemimo števili $a = 17$ in $b = -3$. Potem lahko zapišemo:

$$17 = (-5) \cdot (-3) + 2,$$

torej $q = -5$ in $r = 2$.

Definicija 2.3. Celo število a je *deljivo* s celim številom $b \neq 0$, če je ostanek pri deljenju števila a z b enak 0, tj. $a = qb$ za $q \in \mathbb{Z}$. Število a imenujemo *večkratnik* števila b, število b pa imenujemo *delitelj* števila a.

Definicija 2.4. *Celoštevilsko linearno kombinacijo* števil b in c definiramo kot $xb+yc$, pri čemer sta $x, y \in \mathbb{Z}$.

Lema 2.5. *Naj bodo $a, b, c \in \mathbb{Z}$. Če $a|b$ in $a|c$, potem $a|xb+yc$ za vsak $x, y \in \mathbb{Z}$. Torej a deli vsako celoštevilsko linearno kombinacijo števil b in c.*

Dokaz. Ker $a|b$, sledi, da je $b = qa$ za nek $q \in \mathbb{Z}$. Ker $a|c$, sledi, da je $c = q'a$ za nek $q' \in \mathbb{Z}$. Zapišemo lahko torej:

$$xb + yc = xqa + yq'a = a(xq + yq').$$

Iz tega sledi, da $a|xb + yc$. □

Definicija 2.6. Za $a, b \in \mathbb{Z}$, kjer je $a \neq 0$ ali $b \neq 0$, pravimo, da je število d njun *največji skupni delitelj*, če velja:

1. $d|a$ in $d|b$;

2. če $c|a$ in $c|b$, potem je $c \leq d$.

Največji skupni delitelj števil a in b označimo z $gcd(a, b)$.

Primer 2.7. Vzemimo števili $a = 12$ in $b = 40$. Njuni skupni delitelji so: $\pm 1, \pm 2$ in ± 4, torej je $gcd(12, 40) = 4$.

Definicija 2.8. Za števili $a, b \in \mathbb{Z}$, kjer je $a \neq 0$ ali $b \neq 0$, pravimo, da sta *tuji*, če je $gcd(a, b) = 1$.

Definicija 2.9. Naj bo $n \in \mathbb{N}$ in $a, b \in \mathbb{Z}$. Števili a in b sta *kongruentni* po modulu n, če $n|(a - b)$. To zapišemo kot: $a \equiv b \ (mod\ n)$.

Primer 2.10. Velja:

$$18 \equiv 3 \ (mod\ 5)$$
$$18 \not\equiv 3 \ (mod\ 6).$$

Lema 2.11. *Naj bo $n \geq 2$ in $a, b, c \in \mathbb{Z}$. Če je $a \equiv b \ (mod\ n)$ in $b \equiv c \ (mod\ n)$, potem je $a \equiv c \ (mod\ n)$. To lastnost imenujemo tranzitivnost.*

Dokaz. Naj bo $n \geq 2$ in naj bodo a, b in c taka cela števila, da je $a \equiv b \ (mod\ n)$ in $b \equiv c \ (mod\ n)$. Potem je:

$$a = b + kn;\ k \in \mathbb{Z}$$
$$b = c + hn;\ h \in \mathbb{Z}.$$

Zapišemo torej lahko:

$$a = b + kn = (c + hn) + kn = c + (h + k)n;\ h, k \in \mathbb{Z}.$$

Sledi, da je $a \equiv c \ (mod\ n)$. [25] □

Lema 2.12. *Če je $ca \equiv cb \ (mod\ n)$, potem je $a \equiv b \ (mod\ \frac{n}{d})$, kjer je $d = gcd(c, n)$.*

Dokaz. Zapišemo lahko:

$$ca - cb = c(a - b) = kn;\ k \in \mathbb{Z}.$$

Z d označimo $gcd(c, n)$. Naj bo $c = d \cdot r$ in $n = d \cdot s$, za $r, s \in \mathbb{Z}$ z $gcd(r, s) = 1$. Zapišemo lahko torej:

$$dr(a - b) = kds \quad \text{oziroma} \quad r(a - b) = ks.$$

Iz tega sledi, da s deli $r(a - b)$ in ker je $gcd(r, s) = 1$, mora s deliti $(a - b)$. Velja torej, da je $a \equiv b \ (mod\ \frac{n}{d})$. □

Primer 2.13. Poglejmo si primer $14 \equiv 6 \ (mod\ 8)$.
Ker je $14 = 2 \cdot 7$, $6 = 2 \cdot 3$ in $gcd(2, 8) = 2$, po lemi 2.12 sledi, da je $7 \equiv 3 \ (mod\ 4)$.

Lema 2.14. *Naj bo $a \geq b > 0$ in $a = qb + r$, kjer je $0 \leq r < b$. Potem je:*

$$gcd(a, b) = gcd(b, r).$$

Dokaz. Označimo: $d_1 = gcd(a, b)$ in $d_2 = gcd(b, r)$.
Velja, da $d_1|a$ in $d_1|b$, iz česar sledi, da $d_1|1 \cdot a + (-q) \cdot b = r$ (to velja po lemi 2.5). Sledi, da je $d_1 \leq d_2$, saj je d_1 skupni delitelj b in r in je kvečjemu enak njunemu največjemu skupnemu delitelju.
Po drugi strani pa velja, da $d_2|b$ in $d_2|r$, iz česar sledi, da $d_2|q \cdot b + 1 \cdot r = a$. Analogno kot zgoraj sledi, da je $d_2 \leq d_1$.
Ker mora biti hkrati $d_1 \leq d_2$ in $d_2 \leq d_1$, mora biti $d_2 = d_1$. □

V nadaljevanju bomo opisali *Evklidov algoritem*, ki ga uporabljamo za iskanje največjega skupnega delitelja dveh števil.

Evklidov algoritem: Vzemimo dve celi števili, a in b. Zanima nas njun največji skupni delitelj. V primeru, ko je $a = 0$, je $gcd(a, b) = |b|$, ko pa je $b = 0$, je $gcd(a, b) = |a|$. Zato lahko predpostavimo, da sta števili a in b neničelni. Vemo, da je $gcd(a, b) = gcd(|a|, |b|)$ in zato privzemimo še, da sta a in b pozitivni števili. Imamo torej števili a in b, za kateri velja: $a \geq b > 0$.
Po izreku 2.1 lahko zapišemo $a = qb + r$, kjer je $0 \leq r < b$. Če ta pogoj večkrat uporabimo, dobimo:

$$\begin{aligned}
a &= q_1 b + r_1 \quad (0 < r_1 < b) \\
b &= q_2 r_1 + r_2 \quad (0 < r_2 < r_1) \\
r_1 &= q_3 r_2 + r_3 \quad (0 < r_3 < r_2) \\
r_2 &= q_4 r_3 + r_4 \quad (0 < r_4 < r_3) \\
&\vdots \\
r_{n-2} &= q_n r_{n-1} + r_n \quad (0 < r_n < r_{n-1}) \\
r_{n-1} &= q_{n+1} r_n + 0.
\end{aligned}$$

Postopek zaključimo, ko dobimo ničelni ostanek.
Po lemi 2.14 velja, da je $gcd(a, b) = gcd(b, r)$, torej je $gcd(a, b) = gcd(b, r_1) = gcd(r_1, r_2) = \cdots = gcd(r_{n-1}, r_n) = gcd(r_n, 0) = r_n$. Največji skupni delitelj dveh števil je torej enak zadnjemu neničelnemu ostanku pri Evklidovem algoritmu.

Primer 2.15. Vzemimo števili $a = 12.378$ in $b = 3.054$. Zapišemo lahko:

$$\begin{aligned} 12.378 &= 4 \cdot 3.054 + 162 \\ 3.054 &= 18 \cdot 162 + 138 \\ 162 &= 1 \cdot 138 + 24 \\ 138 &= 5 \cdot 24 + 18 \\ 24 &= 1 \cdot 18 + 6 \\ 18 &= 3 \cdot 6 + 0. \end{aligned}$$

Torej je $gcd(12.378, 3.054) = 6$.

Lema 2.16. *Če je $d = gcd(a, b)$ in $a, b \in \mathbb{Z}$ nista oba enaka 0, potem obstajata taka $x, y \in \mathbb{Z}$, da velja:*

$$d = ax + by. \tag{2.1}$$

Dokaz. Najprej si poglejmo primer, ko sta a in b neničelni pozitivni števili. Ideja dokaza je, da preberemo Evklidov algoritem v nasprotno smer, torej iz spodaj navzgor, pri tem pa vsakič izrazimo ostanek s pomočjo prejšnjih dveh. Namesto celega števila bomo pisali $*$.

$$\begin{aligned} gcd(a, b) = r_n &= r_{n-2} - r_{n-1}q_n \\ &= r_{n-2}(1 + q_n q_{n-1}) - r_{n-3}q_n \\ &= r_{n-3} \cdot * + r_{n-4} \cdot * \\ &\vdots \\ &= b \cdot * + r_1 \cdot * \\ &= a \cdot * + b \cdot * \\ &= a \cdot x + b \cdot y \end{aligned}$$

Lema 2.16 torej res velja, ko sta a in b neničelni pozitivni števili. Kaj pa v primeru, ko je a ali b enak 0? Brez škode za splošnost lahko predpostavimo, da je $a = 0$. V tem primeru je $d = gcd(a, b) = gcd(0, b) = b$. Opazimo, da $x = 0$ in $y = 1$ zadoščata enačbi (2.1), saj $b = a \cdot 0 + b \cdot 1$.

Pogledati moramo še primer, ko je vsaj eden izmed a in b negativen. Vemo, da je $d = gcd(a, b) = gcd(|a|, |b|)$. Tudi v tem primeru preberemo Evklidov algoritem v nasprotno smer in celi števili, ki ju dobimo v zadnjem koraku, ustrezno pomnožimo z (-1). To pomeni, da če je $a < 0$, namesto x vzamemo $-x$ in če je $b < 0$, namesto y vzamemo $-y$. Na ta način dobimo rešitev enačbe (2.1). □

Primer 2.17. Naj bo $a = 12.378$ in $b = 3.054$. Iz primera 2.15 lahko razberemo:

$$\begin{aligned} 6 &= 24 - 18 \\ &= 6 \cdot 24 - 138 \\ &= 6 \cdot 162 - 7 \cdot 138 \\ &= 132 \cdot 162 - 7 \cdot 3.054 \\ &= 132 \cdot 12.378 - 535 \cdot 3.054. \end{aligned}$$

Torej je $x = 132$ in $y = -535$.

Lema 2.18. *Naj bodo $a, b, c \in \mathbb{Z}$ in $c \neq 0$. Če c deli produkt ab in je $gcd(a, c) = 1$, potem mora c deliti b.*

Dokaz. Če c deli ab, potem obstaja tako celo število m, da je $ab = mc$. Ker sta a in c tuji, obstajata po lemi 2.16 taki celi števili x in y, da velja $ax + cy = 1$. Če to enačbo pomnožimo z b, dobimo $abx + cby = b$, oziroma $b = mcx + cby = c(mx + by)$. Torej c res deli b. □

Definicija 2.19. Naj bo $n \in \mathbb{N}$ in $a \in \mathbb{Z}$. Pravimo, da je *a obrnljiv modulo n*, če obstaja tak x, da je $ax \equiv 1 \ (mod\ n)$. Rešitvi te kongruence pravimo *multiplikativni inverz* števila a po modulu n.

Posledica 2.20. *Naj bosta $n > 1$ in a celi števili. Potem sta a in n tuji natanko tedaj, ko obstaja x, za katerega velja $ax \equiv 1 \ (mod\ n)$.*
Torej je $gcd(a, n) = 1$ natanko tedaj, ko je a obrnljiv modulo n.

Dokaz. Kongruenca je ekvivalenta obstoju celega števila y, za katerega je $ax + ny = 1$. Vsak skupni delitelj d, števil a in n, zato po lemi 2.5 deli število 1. Sledi torej, da je d enak bodisi 1 bodisi -1, kar pa pomeni, da sta števili a in n tuji.
Obratno, če sta a in n tuji števili, potem je 1 njun največji skupni delitelj. Če uporabimo lemo 2.16, vidimo, da obstajata celi števili x in y, tako da je $ax + ny = 1$, iz česar sledi, da je $ax \equiv 1 \ (mod\ n)$. □

Definicija 2.21. Naravno število $p \geq 2$ je *praštevilo*, če sta 1 in p njegova edina pozitivna delitelja.

Primer 2.22. Števila $2, 3, 5, 7, 11, 13, 17, \ldots$ so praštevila.

Izrek 2.23. *(Fermatov mali izrek) Naj bo p praštevilo, $a \in \mathbb{Z}$ in naj p ne deli a. Potem je:*

$$a^{p-1} \equiv 1 \ (mod\ p).$$

Dokaz. Vzemimo $1 \leq i \leq p-1$. Zanima nas, ali je lahko $ia \equiv 0 \ (mod\ p)$. Če to drži, potem sledi, da p deli ia. Vemo pa, da je $gcd(p,a) = 1$, ker je p praštevilo in p ne deli a. Iz tega sledi, da mora p deliti i. To pa je v protislovju z našo začetno predpostavko $1 \leq i \leq p-1$. Torej $ia \not\equiv 0 \ (mod\ p)$.
Vzemimo sedaj $1 \leq i, j \leq p-1$. Zanima nas, ali je lahko $ia \equiv ja \ (mod\ p)$. Če to drži, potem p deli $ia - ja = a(i-j)$. Iz tega sledi, da p deli $i-j$, saj po predpostavki p ne deli a. Iz naše začetne predpostavke sledi, da je $-(p-2) \leq i-j \leq p-2$ in na tem intervalu je s p deljivo le število 0. Torej sledi, da je $i-j=0$ oziroma, da je $i=j$.
Naj bo b poljubno celo število. Potem obstaja enolično določeno število r $(0 \leq r \leq p-1)$, tako da je $b \equiv r \ (mod\ p)$. Za vsak i $(1 \leq i \leq p-1)$ obstaja enolično določeno število r_i $(0 \leq r_i \leq p-1)$, tako da velja $(\star)$:

$$\begin{aligned} a &\equiv r_1 \ (mod\ p) \\ 2a &\equiv r_2 \ (mod\ p) \\ &\vdots \\ (p-1)a &\equiv r_{p-1} \ (mod\ p). \end{aligned}$$

Ali se lahko zgodi, da je $r_i = 0$? V tem primeru bi imeli $ia \equiv 0 \ (mod\ p)$, to pa smo pokazali, da ni mogoče.
Ali se lahko zgodi, da je $r_i = r_j$? V tem primeru bi imeli $ia \equiv ri = r_j \equiv ja \ (mod\ p)$, iz česar sledi, da je $ia \equiv ja \ (mod\ p)$. Pokazali smo, da je potem $i = j$.
Dokazali smo torej, da so $r_1, r_2, \ldots r_{p-1}$ paroma različna neničelna števila. Ker smo na omejenem intervalu, števila $r_1, r_2, \ldots r_{p-1}$ zavzamejo ravno vse vrednosti od 1 do $p-1$, tj. $\{r_1, r_2, \ldots r_{p-1}\} = \{1, 2, \ldots, p-1\}$. Velja:

$$a \cdot 2a \cdot 3a \cdot \cdots \cdot (p-1)a = (p-1)! \cdot a^{p-1} \overset{(\star)}{\equiv} (p-1)! \ (mod\ p). \tag{2.2}$$

Če obe strani enačbe (2.2) delimo s $(p-1)!$, po lemi 2.12 dobimo naslednjo kongruenco:

$$a^{p-1} \equiv 1 \left(mod\ \frac{p}{gcd(p,(p-1)!)} \right) \quad \text{oziroma} \quad a^{p-1} \equiv 1 \ (mod\ p).$$

□

Izrek 2.24. *(al-Haythamov oziroma Wilsonov izrek) Celo število $n > 1$ je praštevilo natanko tedaj, ko:*

$$(n-1)! \equiv -1 \ (mod\ n).$$

Dokaz. Najprej pokažimo, da kongruenca velja, ko je n praštevilo. Predpostavimo, da je $n = p$ liho praštevilo (kongruenca je očitna za $n = 2$). Vsako celo število $1 < a < p-1$ ima enolično določen multiplikativni inverz različen od a modulo p. Enoličnost je očitna, za različnost pa vemo, da $a^2 \equiv 1 \ (mod\ p)$ implicira $p|(a+1)(a-1)$,

iz česar sledi, da je $a \equiv \pm 1 \ (mod\ p)$. V produktu $(p-1)! = (p-1) \cdot (p-2) \cdots 3 \cdot 2 \cdot 1$ se torej po modulu p pokrajšajo vsi členi razen prvega in zadnjega. Očitno je, da je njun produkt -1 modulo p.
Sedaj moramo izrek pokazati še v drugo smer. Naj bo $n \in \mathbb{Z}$ in naj velja, da je $(n-1)! \equiv -1 \ (mod\ n)$. Recimo, da n ni praštevilo. Potem lahko zapišemo $n = d \cdot r$, kjer je $1 < d$ in $r < n$. Velja, da je $d \leq n-1$ in zapišemo lahko $(n-1)! = 1 \cdot 2 \cdots (d-1) \cdot d \cdot (d+1) \cdots (n-1)$, iz česar sledi, da d deli $(n-1)!$. Ker smo predpostavili, da je $n = d \cdot r$, velja tudi, da d deli n. Vemo, da n deli $(n-1)!+1$ in zato d deli $(n-1)!+1$. Ker pa d deli tudi $(n-1)!$, deli tudi linearno kombinacijo $((n-1)!+1) - (n-1)! = 1$, kar pa je v protislovju z našo predpostavko, da je $1 < d$. Torej je n res praštevilo. □

2.2 ALGEBRAIČNE STRUKTURE

Definicija 2.25. Matrika $A \in \mathbb{R}^{nxn}$ je *obrnljiva* matrika, če obstaja taka matrika $A^{-1} \in \mathbb{R}^{nxn}$, da je $AA^{-1} = A^{-1}A = I_n$, pri čemer je $I_n = \begin{bmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & & & \\ 0 & \dots & 0 & 1 \end{bmatrix}$ identična matrika. [12]

Lema 2.26. *Če sta matriki $A, B \in \mathbb{R}^{nxn}$, potem je* $\det AB = \det A \cdot \det B$. *[16]*

Leme 2.26 tu ne bomo dokazali, bralec pa lahko dokaz poišče v skripti [16, str. 79].

Primer 2.27. Vzemimo matriki $A = \begin{bmatrix} 2 & 2 \\ 1 & 3 \end{bmatrix}$ in $B = \begin{bmatrix} 2 & -1 \\ 1 & 1 \end{bmatrix}$.
Izračunajmo najprej matriko AB:

$$AB = \begin{bmatrix} 6 & 0 \\ 5 & 2 \end{bmatrix}.$$

Izračunajmo sedaj determinanto te matrike:

$$\det AB = 6 \cdot 2 - 5 \cdot 0 = 12.$$

Izračunajmo sedaj še produkt determinant obeh matrik:

$$\det A \cdot \det B = (2 \cdot 3 - 1 \cdot 2) \cdot (2 \cdot 1 - (-1) \cdot 1) = 4 \cdot 3 = 12.$$

Lema 2.28. *Matrika $A \in \mathbb{R}^{nxn}$ je obrnljiva natanko tedaj, ko je* $\det A \neq 0$. *[16]*

Dokaz. Če je A obrnljiva, potem je $\det A \cdot \det(A^{-1}) = det(A \cdot A^{-1}) = \det I = 1$. Sledi, da je $\det A \neq 0$.
Lemo 2.28 je potrebno dokazati še v drugo smer, torej da če je $\det A \neq 0$, potem je matrika A obrnljiva. Ta del dokaza si lahko bralec prebere v skripti [16, str. 81]. □

Definicija 2.29. Naj bo K poljubna množica. Operaciji $\cdot : K \times K \to K$ rečemo binarna operacija na množici K. Naj bo sedaj $\cdot$ binarna operacija na množici K. Paru $(K, \cdot)$ pravimo *polgrupa*, če je $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ za poljubne $a, b, c \in K$. To lastnost imenujemo asociativnost. [13]

Primer 2.30. Množica $(\mathbb{N}, +)$ je polgrupa, saj za $a, b, c \in \mathbb{N}$ velja:

- zaprtost za operacijo: $a + b \in \mathbb{N}$;
- asociativnost: $a + (b + c) = (a + b) + c$. [22]

Definicija 2.31. Naj bo K poljubna množica. Operaciji $\cdot : K \times K \to K$ rečemo binarna operacija na množici K. Naj bo sedaj $\cdot$ binarna operacija na množici K. Paru $(K, \cdot)$ pravimo *grupa*, če za $a, b, c \in K$ velja:

- asociativnost: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$;
- obstaja nevtralni element $e \in K$: $a \cdot e = e \cdot a = a$;
- obstaja nasprotni element $a^{-1} \in K$: $a \cdot a^{-1} = a^{-1} \cdot a = e$.

Če za par $(K, \cdot)$ velja še komutativnost, tj. $a \cdot b = b \cdot a$ za $a, b \in K$, ga imenujemo *Abelova grupa*. [13]

Primer 2.32. Množica $(\mathbb{R}, +)$ je Abelova grupa. Preverimo, da veljajo vse lastnosti:

- zaprtost za operacijo: $a + b \in \mathbb{R}$, za $a, b \in \mathbb{R}$;
- asociativnost: $(a + b) + c = a + (b + c)$, za $a, b, c \in \mathbb{R}$;
- nevtralni element je 0: $a + 0 = 0 + a = a$, za $a \in \mathbb{R}$;
- nasprotni element je $-a$: $a + (-a) = (-a) + a = 0$, za $a \in \mathbb{R}$;
- komutativnost: $a + b = b + a$, za $a, b \in \mathbb{R}$. [15]

Primer 2.33. Vzemimo množico $\mathbb{Z}/n\mathbb{Z}$ oziroma krajše $\mathbb{Z}_n$. Velja, da ta množica vsebuje elemente $\{0, 1, 2, \ldots, n-1\}$. Operacija $+ : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$ je definirana kot seštevanje po modulu n.
Na primer, če vzamemo dva elementa iz množice $\mathbb{Z}_6 = \{0, 1, 2, \ldots, 5\}$, je:

$$(3 + 5)(mod\ 6) = 2.$$

Par $(Z_n, +)$ je Abelova grupa. [1]

Definicija 2.34. Naj bo G grupa. Za poljuben $g \in G$ je *red elementa* g enak najmanjšemu naravnemu številu n, za katerega velja, da je $\underbrace{g \cdot g \cdots g}_{\text{n-krat}} = g^n = e$, če tako število obstaja. Pri tem je e nevtralni element grupe G. [10]

Primer 2.35. Vzemimo grupo $(\mathbb{Z}_6, +)$. Red elementa $2 \in \mathbb{Z}_6$ je 3, saj je:

$$2 + 2 + 2 = 6 \equiv 0 \ (mod\ 6).$$

Definicija 2.36. *Red grupe* $(G, \cdot)$ je kardinalnost oziroma moč njene pripadajoče množice G. Red grupe G označimo z $|G|$. [10]

Primer 2.37. Vzemimo grupo $(\mathbb{Z}_6, +)$. Množica $\mathbb{Z}_6$ vsebuje elemente $\{0, 1, 2, 3, 4, 5\}$. Red grupe je torej $|\mathbb{Z}_6| = 6$.

Definicija 2.38. Grupa $(G, \cdot)$ je *ciklična*, če obstaja tak element $a \in G$, da lahko vse elemente grupe G zapišemo s pomočjo potenc elementa a, tj. $G = \{e, a, a^2, \ldots, a^{r-1}\}$ in $a^r = e$. Elementu a pravimo *generator* grupe G. [21]

Primer 2.39. Poiščimo vse generatorje grupe $(\mathbb{Z}_{12}, +)$. Množica $\mathbb{Z}_{12}$ vsebuje elemente $\{0, 1, 2, \ldots, 11\}$. Generatorji $\mathbb{Z}_{12}$ so:

- 1, saj $1 + 1 = 2$, $1 + 1 + 1 = 3$, $\ldots$, na ta način dobimo vse elemente $\mathbb{Z}_{12}$;
- 5, saj $5 + 5 + 5 + 5 + 5 = 25 \equiv 1 \ (mod\ 12)$ in za 1 že vemo, da je generator;
- 7, saj je $7 + 7 + 7 + 7 + 7 + 7 + 7 = 49 \equiv 1 \ (mod\ 12)$ in za 1 že vemo, da je generator;
- 11, saj $11 + 11 + \cdots + 11 = 121 \equiv 1 \ (mod\ 12)$ in za 1 že vemo, da je generator. [21]

Definicija 2.40. Naj bo $(G, \cdot)$ grupa. Neprazna podmnožica $H \subseteq G$ je *podgrupa* grupe G, če je H grupa za operacijo $\cdot$. To označimo s $H \leq G$. [10]

Definicija 2.41. Naj bo G grupa in $H \leq G$ njena podgrupa. Za poljuben $g \in G$ je *levi odsek* grupe G po podgrupi H enak množici $gH = \{gh : h \in H\}$. Analogno definiramo tudi *desni odsek*. Množico vseh levih odsekov grupe G po podgrupi H imenujemo *kvocientna množica* grupe G po podrgupi H in jo označimo z G/H. [10]

Primer 2.42. Naj bo n naravno število. Z $n\mathbb{Z}$ označimo množico celih števil, ki so deljiva z n. V primeru, ko je $n = 3$, je torej $3\mathbb{Z} = \{\ldots, -6, -3, 0, 3, 6, \ldots\}$. Množica $3\mathbb{Z}$ tvori podgrupo grupe $(\mathbb{Z}, +)$. Preverimo, da to res velja:

- podmnožica: $3\mathbb{Z} \subseteq \mathbb{Z}$;
- zaprtost za operacijo: če sta $a, b \in 3\mathbb{Z}$, potem $3|a$ in $3|b$ in po lemi 2.5 sledi, da 3 deli tudi njuno linearno kombinacijo $a + b$, torej je vsota $a + b$ vsebovana v $3\mathbb{Z}$;
- asociativnost: za $a, b, c \in 3\mathbb{Z}$ je $(a + b) + c = a + (b + c)$;
- nevtralni element: za $a \in 3\mathbb{Z}$ je $a + 0 = 0 + a = a$ in $0 \in 3\mathbb{Z}$;

- nasprotni element: za $a \in 3\mathbb{Z}$ je $a + (-a) = (-a) + a = 0$ in $-a \in 3\mathbb{Z}$.

Poiščimo sedaj leve odseke grupe $\mathbb{Z}$ po podgrupi $3\mathbb{Z}$. Za poljuben $g \in \mathbb{Z}$ je:

$$g + 3\mathbb{Z} = \{g + h : h \in 3\mathbb{Z}\}.$$

Vidimo, da imamo le tri različne možnosti in sicer za $g = 0, g = 1$ in $g = 2$, saj je množica $3 + 3\mathbb{Z}$ že enaka množici $0 + 3\mathbb{Z}$. Vsi možni levi odseki so torej:

- $3\mathbb{Z} = \{\ldots, -6, -3, 0, 3, 6, \ldots\}$;
- $1 + 3\mathbb{Z} = \{\ldots, -5, -2, 1, 4, 7, \ldots\}$;
- $2 + 3\mathbb{Z} = \{\ldots, -4, -1, 2, 5, 8, \ldots\}$.

Iskana kvocientna množica je torej $\mathbb{Z}/3\mathbb{Z} = \{3\mathbb{Z}, 1 + 3\mathbb{Z}, 2 + 3\mathbb{Z}\}$.

Definicija 2.43. Naj bo R poljubna množica ter $+$ in $\cdot$ binarni operaciji na množici R. Urejena trojica $(R, +, \cdot)$ je *kolobar*, če velja:

- $(R, +)$ je Abelova grupa;
- $(R, \cdot)$ je polgrupa;
- operaciji $+$ in $\cdot$ povezujeta zakona distributivnosti:
  - $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$;
  - $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$. [13]

Primer 2.44. Množica $(\mathbb{R}, +, \cdot)$ je kolobar. Da je $(\mathbb{R}, +)$ Abelova grupa smo preverili v primeru 2.32, preveriti moramo še, da je $(\mathbb{R}, \cdot)$ polgrupa in da operaciji $+$ in $\cdot$ povezujeta zakona distributivnosti:

- zaprtost za operacijo: $a \cdot b \in \mathbb{R}$, za $a, b \in \mathbb{R}$;
- asociativnost: $a \cdot (b \cdot c) = (a \cdot b) \cdot c$, za $a, b, c \in \mathbb{R}$, torej je $(\mathbb{R}, \cdot)$ res polgrupa;
- $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$, za $a, b, c \in \mathbb{R}$;
  $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$, za $a, b, c \in \mathbb{R}$. [15]

Definicija 2.45. Kolobar $(R, +, \cdot)$ je komutativen, če je polgrupa $(R, \cdot)$ komutativna. [13]

Primer 2.46. Trdimo, da je kolobar $(\mathbb{Z}, +, \cdot)$ komutativen. Preveriti moramo, da je $(\mathbb{Z}, \cdot)$ komutativna polgrupa:

- zaprtost za operacijo: $a \cdot b \in \mathbb{Z}$, za $a, b \in \mathbb{Z}$;

- asociativnost: $a \cdot (b \cdot c) = (a \cdot b) \cdot c$, za $a, b, c \in \mathbb{Z}$;
- komutativnost: $a \cdot b = b \cdot a$, za $a, b \in \mathbb{Z}$.

Definicija 2.47. Naj bo $(F, +, \cdot)$ komutativen kolobar in naj bo 0 nevtralni element za binarno operacijo $+$. Potem je $(F, +, \cdot)$ *polje*, če je $(F \setminus \{0\}, \cdot)$ Abelova grupa in je $0 \neq 1$, kjer je 1 nevtralni element grupe $(F \setminus \{0\}, \cdot)$. [8]

Primer 2.48. Racionalna števila so polje. Preverimo, da res izpolnjujejo vse aksiome. Vzemimo racionalna števila $\frac{a}{b}$, $\frac{c}{d}$ in $\frac{e}{f}$:

- zaprtost za operacijo: $\frac{a}{b} + \frac{c}{d} \in \mathbb{Q}$ in $\frac{a}{b} \cdot \frac{c}{d} \in \mathbb{Q}$;
- asociativnost: $\frac{a}{b} + (\frac{c}{d} + \frac{e}{f}) = (\frac{a}{b} + \frac{c}{d}) + \frac{e}{f}$ in $\frac{a}{b} \cdot (\frac{c}{d} \cdot \frac{e}{f}) = (\frac{a}{b} \cdot \frac{c}{d}) \cdot \frac{e}{f}$;
- komutativnost: $\frac{a}{b} + \frac{c}{d} = \frac{c}{d} + \frac{a}{b}$ in $\frac{a}{b} \cdot \frac{c}{d} = \frac{c}{d} \cdot \frac{a}{b}$;
- nevtralni element: $\frac{a}{b} + 0 = \frac{a}{b}$ in $\frac{a}{b} \cdot 1 = \frac{a}{b}$;
- nasprotni element: $\frac{a}{b} + (-\frac{a}{b}) = 0$ in $\frac{a}{b} \cdot \frac{b}{a} = 1$, ko je $\frac{a}{b} \neq 0$;
- distributivnost: $\frac{a}{b} \cdot (\frac{c}{d} + \frac{e}{f}) = \frac{ac}{bd} + \frac{ae}{bf}$;
- različnost nevtralnih elementov: $0 \neq 1$.

Definicija 2.49. *Karakteristika polja* F je tako najmanjše naravno število n, da če multiplikativno enoto 1 n-krat seštejemo samo s sabo, dobimo aditivno enoto 0. Če vsota multiplikativne enote 1 ni nikoli enaka aditivni enoti 0, potem je karakteristika polja F enaka 0. [9]

Primer 2.50. Za polje F vzemimo racionalna števila. Karakteristika polja F je enaka 0, saj ne glede na to, kolikokrat seštejemo multiplikativno enoto 1, ne bomo nikoli dobili rezultata 0, tj. $1 + 1 + \cdots + 1 \neq 0$.

Definicija 2.51. Naj bo $(R, +, \cdot)$ kolobar, ki premore nevtralni element $1 \in R$ za binarno operacijo $\cdot$: $x \cdot 1 = 1 \cdot x = x$ za vsak element x iz R. Rečemo, da je $x \in R$ *obrnljiv*, če obstaja tak $x^{-1} \in R$, da je $x \cdot x^{-1} = x^{-1} \cdot x = 1$. Množico vseh obrnljivih elementov kolobarja R označimo z R^*. [14]

Definicija 2.52. Naj bo $(R, +, \cdot)$ kolobar, ki premore nevtralni element $1 \in R$ za binarno operacijo $\cdot$. Naj bo R^* množica vseh obrnljivih elementov kolobarja R. Bralcu za vajo prepuščamo, da preveri, da je $(R^*, \cdot)$ grupa. Grupi $(R^*, \cdot)$ pravimo *multiplikativna grupa* kolobarja R. [20]

Primer 2.53. Multiplikativna grupa celih števil modulo n je grupa za operacijo množenja po modulu n nad obrnljivimi elementi $\mathbb{Z}_n$. Če n ni praštevilo, potem obstajajo poleg elementa 0 še drugi elementi, ki niso obrnljivi.
Vzemimo na primer $n = 18$. V tem primeru je $\mathbb{Z}_n = \{0, 1, 2, \ldots, 17\}$ in množica obrnljivih elementov je $\mathbb{Z}_n^* = \{1, 5, 7, 11, 13, 17\}$, saj:

$$1 \cdot 1 = 1$$
$$5 \cdot 11 = 11 \cdot 5 = 55 \equiv 1 \ (mod\ 18)$$
$$7 \cdot 13 = 13 \cdot 7 = 91 \equiv 1 \ (mod\ 18)$$
$$17 \cdot 17 = 289 \equiv 1 \ (mod\ 18).$$

Za števili 11 in 13 sledi direktno iz 2. in 3. kongruence, da sta obrnljiva elementa.

Definicija 2.54. Naj bo w poljubno kompleksno število. Definirajmo množico $\mathbb{Z}[w]$ kot:

$$\mathbb{Z}[w] = a + wb;\ a, b \in \mathbb{Z}.$$

Bralec lahko sam za vajo preveri, da je množica $\mathbb{Z}[w]$ kolobar za operaciji običajnega seštevanja in množenja kompleksnih števil. Kolobar $\mathbb{Z}[w]$ premore tudi enoto za operacijo množenja, saj je število 1 vedno element kolobarja $\mathbb{Z}[w]$.

3 DIOFANTSKE ENAČBE

Diofantska enačba je enačba, za katero zahtevamo, da so njene rešitve cela števila. Ime je dobila po grškem matematiku Diofantu iz Aleksandrije, ki je znan predvsem po svoji knjigi Aritmetika. Ta knjiga je imela velik vpliv na razvoj algebre in teorije števil. [11]

3.1 FUNDAMENTALNI IZREK ARITMETIKE

Fundamentalni izrek aritmetike je bil naverjetneje poznan že v Antiki. Preden ga lahko zapišemo, moramo pogledati tri leme, ki so potrebne za dokaz Fundamentalnega izreka aritmetike.

Lema 3.1. *Za $a, b, c \in \mathbb{Z}$ velja: če $a|b$ in $b|c$, potem $a|c$. To lastnost imenujemo tranzitivnost.*

Dokaz. Ker $a|b$, sledi, da obstaja tak $m_1 \in \mathbb{Z}$, da je $a \cdot m_1 = b$. Ker $b|c$, sledi, da obstaja tak $m_2 \in \mathbb{Z}$, da je $b \cdot m_2 = c$. Z uporabo substitucije dobimo:

$$m_2 \cdot m_1 \cdot a = c.$$

Sledi, da obstaja tak $m \in \mathbb{Z}$, da je $m \cdot a = c$, pri čemer je $m = m_1 \cdot m_2$. Iz tega sledi, da $a|c$. [5] □

Lema 3.2. *Naj bo p praštevilo in $a_1, a_2, \ldots, a_k \in \mathbb{Z}$. Če $p|a_1 \cdots a_k$, potem obstaja $1 \leq i \leq k$, tako da $p|a_i$.*

Dokaz.
Če $p|a_1$, je dokaz zaključen, sicer moramo pogledati naprej.
Če $p \nmid a_1$, potem je $gcd(a_1, p) = 1$, saj je p praštevilo, torej mora p deliti $a_2 \cdots a_k$.
Če $p|a_2$ je dokaz zaključen, sicer moramo pogledati naprej.
Če $p \nmid a_2$, potem je $gcd(a_2, p) = 1$, iz česar sledi, da $p|a_3 \cdots a_k$.
⋮
Analogno bi nadaljevali dokaz, dokler ne bi prišli do zaključka. □

Lema 3.3. *Naj bodo p in $q_1, q_2, \ldots, q_k$ praštevila. Če $p|q_1 \cdots q_k$, potem je $p = q_i$ za nek $i \in \{1, \ldots, k\}$.*

Dokaz. Po lemi 3.2 obstaja $1 \leq i \leq k$, tako da $p|q_i$, iz česar sledi, da je $p = q_i$. □

Izrek 3.4. *(Fundamentalni izrek aritmetike) Vsako naravno število večje od* 1*, lahko zapišemo kot produkt praštevil. Pri tem velja, da je razcep na praštevila enolično določen, če zanemarimo vrstni red množencev.*

Dokaz. Naj bo $n \geq 2$ naravno število. Če je n praštevilo, je dokaz zaključen. Pogledati moramo primer, ko n ni praštevilo. Tedaj obstaja $d \in \mathbb{N}$, tako da je $1 < d < n$ in $d|n$. Naj bo p_1 najmanjši tak delitelj. Če p_1 ni praštevilo, potem obstaja tak d, da je $1 < d < p_1$ in $d|p_1$. Torej $d|p_1$ in $p_1|n$, iz tega pa sledi, da $d|n$. Prišli smo do protislovja, saj mora biti p_1 najmanjši delitelj števila n, ki je večji od 1. Torej p_1 je praštevilo in zapišemo lahko: $n = p_1 \cdot n_1$, kjer je $n_1 \geq 2$.
Če je n_1 praštevilo, je dokaz zaključen. Pogledati moramo primer, ko n_1 ni praštevilo. V tem primeru obstaja praštevilo p_2, ki deli n_1. Zapišemo lahko $n_1 = p_2 \cdot n_2$, kjer je $n_2 \geq 2$. Torej je $n = p_1 \cdot p_2 \cdot n_2$.
Če je n_2 praštevilo, je dokaz zaključen. Pogledati moramo primer, ko n_2 ni praštevilo. Tedaj obstaja praštevilo p_3, tako da $n_2 = p_3 \cdot n_3$. Torej je $n = p_1 \cdot p_2 \cdot p_3 \cdot n_3$.
$\vdots$
Ta postopek ponavljamo, dokler ne dobimo razcepa števila n na sama praštevila. Postopek se bo zagotovo ustavil, saj so ti n-ji vedno manjši.
Sedaj moramo pokazati še enoličnost takega zapisa. Ponovno predpostavimo, da je $n \geq 2$ naravno število. Za dokaz bomo uporabili protislovje.
Naj bo $n = p_1 \cdot p_2 \cdots p_r = q_1 \cdot q_2 \cdots q_s$, pri tem so $\{p_1, p_2, \ldots, p_r, q_1, q_2, \ldots, q_s\}$ praštevila. Naj bo $p_1 \leq p_2 \leq \cdots \leq p_r$ in $q_1 \leq q_2 \leq \cdots \leq q_s$. Ker $p_1|q_1 \cdot q_2 \cdots q_s$, po lemi 3.3 sledi, da $p_1 = q_i$, kjer je $i \in \{1, \ldots, s\}$, torej je $p_1 \geq q_1$. Ker pa tudi $q_1|p_1 \cdot p_2 \cdots p_r$, po lemi 3.3 analogno sledi, da je $q_1 = p_i$, kjer je $i \in \{1, \ldots, r\}$ in je torej $q_1 \geq p_1$. Iz obeh pogojev skupaj dobimo, da mora biti $p_1 = q_1$ in zaradi začetne predpostavke sledi, da je potem $p_2 \cdots p_r = q_2 \cdots q_s$.
Analogno bi pokazali, da je $p_2 = q_2$ in tako naprej. V primeru, ko sta r in s enaka, je torej dokaz zaključen. Kaj pa ko nista enaka?
Če je $r > s$: $p_{s+1} \cdot p_{s+2} \cdots p_r = 1$, kar pa je protislovje, saj produkt praštevil ne more biti enak 1.
Če je $r < s$: $1 = q_{r+1} \cdot q_{r+2} \cdots q_s$, kar pa je protislovje, saj produkt praštevil ne more biti enak 1. □

Primer 3.5. Število 300 lahko razcepimo na produkt praštevil na naslednji način:

$$300 = 2^2 \cdot 3 \cdot 5^2.$$

3.2 PITAGOROVA ENAČBA

V tem poglavju si bomo pogledali zvezo med Fundamentalnim izrekom aritmetike ter študijo polinomskih diofantskih problemov.

Za začetek vzemimo enačbo:

$$x^2 + y^2 = z^2. \tag{3.1}$$

Vemo, da je enačba take oblike povezana s pravokotnim trikotnikom, ki ima stranice dolžine x, y in z. Imenujemo jo *Pitagorova enačba*, po grškem matematiku, ki jo je povezal s pravokotnim trikotnikom. Naš cilj je poiskati vse možne celoštevilske rešitve, tj. trojice celih števil (x, y, z), ki zadoščajo enačbi (3.1).

Enačbo (3.1) lahko zapišemo kot:

$$x^2 = z^2 - y^2 = (z + y)(z - y). \tag{3.2}$$

Če bi vedeli, da je $gcd(z + y, z - y) = 1$, bi lahko na podlagi Fundamentalnega izreka aritmetike trdili, da morata biti $z + y$ in $z - y$ kvadrata, ter na ta način dobili vse trojice, ki rešijo enačbo (3.1).

Predpostavimo sedaj, da trojica (x, y, z) ne vsebuje skupnega praštevilskega faktorja. To lahko predpostavimo, saj v kolikor ga vsebuje, le delimo s kvadratom tega faktorja. Trojica (x, y, z) se imenuje *primitivna rešitev* enačbe (3.1), če x, y in z nimajo skupnega faktorja. Predpostavimo lahko še, da je le eno izmed teh števil sodo, saj če sta sodi dve, mora biti tudi tretje in to je v nasprotju z našo prvo predpostavko.

Če je z sodo število, potem je $z^2 \equiv 0 \ (mod\ 4)$. Vsako liho število je kongruentno 1 ali 3 po modulu 4, torej je kvadrat poljubnega lihega števila kongruenten 1 po modulu 4. Ker sta x in y lihi števili, je torej $x^2 + y^2 \equiv 2 \ (mod\ 4)$, kar pa je v protislovju s tem, da je z^2 kongruentno 0 po modulu 4. Torej z ne more biti sodo število. Zato lahko predpostavimo, da je eno izmed števil x in y sodo. Brez škode za splošnost lahko predpostavimo, da je sodo število x in zapišemo lahko $x = 2x'$. Če to vstavimo v enačbo (3.2), dobimo:

$$x'^2 = \left(\frac{z + y}{2}\right) \cdot \left(\frac{z - y}{2}\right). \tag{3.3}$$

Ker sta z in y lihi števili, sta $\frac{z+y}{2}$ in $\frac{z-y}{2}$ celi števili. Še več, biti morata tudi tuji, saj mora katerikoli skupni faktor dveh števil izmed x, y in z deliti tretje število. Recimo, da imata $\frac{z+y}{2}$ in $\frac{z-y}{2}$ skupen delitelj d. Potem ta delitelj d deli tudi vsoto in razliko teh dveh števil, tj. z in y. Torej d^2 deli $z^2 - y^2 = x^2$, od koder sledi, da d deli x, kar pa je v nasprotju z našo predpostavko, da je trojica (x, y, z) primitivna.

Sedaj lahko uporabimo Fundamentalni izrek aritmetike in pridemo do sklepa, da sta $\frac{z+y}{2}$ in $\frac{z-y}{2}$ kvadrata. Zapišemo lahko:

$$z + y = 2m^2, z - y = 2n^2;\ m > n. \tag{3.4}$$

Predpostavljamo, da sta z in y pozitivni števili, torej je $z + y > z - y$. Če rešimo enačbi (3.4) za z in y in nato uporabimo enačbo (3.1), da najdemo x, dobimo naslednji rezultat.

Izrek 3.6. *Primitivne celoštevilske rešitve Pitagorove enačbe $x^2 + y^2 = z^2$ s sodim x so dane z:*

$$\begin{aligned} x &= 2mn; \\ y &= m^2 - n^2; \\ z &= m^2 + n^2, \end{aligned}$$

kjer sta m in n celi tuji števili, ne obe sodi in velja $m > n$.

3.3 FUNDAMENTALNI IZREK ARITMETIKE V DRUGIH KONTEKSTIH

Če gledamo samo cela števila, je Fundamentalni izrek aritmetike direktna posledica Evklidovega algoritma, kar pa ne velja za določene kolobarje. Mi se bomo osredotočili na komutativne kolobarje z multiplikativnim nevtralnim elementom 1.

Definicija 3.7. Pravimo, da je komutativen kolobar R *Evklidov*, če obstaja funkcija $N : R \setminus \{0\} \to \mathbb{N}$, za katero velja:

1. $N(ab) = N(a)N(b)$ za vse $a, b \in R$;
2. za vse $a, b \in R$, če je $b \neq 0$, potem obstajata $q, r \in R$, tako da:

$$a = bq + r \text{ in velja, da je } r = 0 \text{ ali } N(r) < N(b).$$

Tako funkcijo imenujemo *norma* na R.

Primer 3.8. Naj bo $R = \mathbb{Z}[i] = \{x + iy | x, y \in \mathbb{Z}\}$, kjer je $i^2 = -1$. Tak R imenujemo *Gaussova cela števila*. Naj bo $N(x + iy) = x^2 + y^2$. Preverimo, da je R res Evklidov kolobar.

1. Vzemimo $a = x + iy, b = z + iu \in R$. Velja:

$$\begin{aligned} N((x + iy)(z + iu)) &= N(xz + ixu + iyz - yu) \\ &= N((xz - yu) + i(xu + yz)) \\ &= (xz - yu)^2 + (xu + yz)^2 \\ &= x^2z^2 - 2xzyu + y^2u^2 + x^2u^2 + 2xuyz + y^2z^2 \\ &= x^2(z^2 + u^2) + y^2(u^2 + z^2) \\ &= (z^2 + u^2)(x^2 + y^2). \end{aligned}$$

Po drugi strani je:

$$N(x+iy)N(z+iu) = (x^2+y^2)(z^2+u^2).$$

Torej je 1. točka definicije 3.7 izpolnjena.

2. Naj bosta $a, b \neq 0 \in R$ in pišimo $ab^{-1} = p + it$, kjer $p, t \in \mathbb{Q}$. Definirajmo $m, n \in \mathbb{Z}$ kot:
$$m \in \left[\frac{p-1}{2}, \frac{p+1}{2}\right), n \in \left[\frac{t-1}{2}, \frac{t+1}{2}\right).$$
Naj bo $q = m + in \in R$ in $r = a - b(m + in)$. Torej je res $a = bq + r$. Za $r \neq 0$ velja:

$$\begin{aligned} N(r) &= N((a - b(m + in)) \\ &= N((ab^{-1} - m - in)b) \\ &= N(p + it - m - in)N(b) \\ &= N(p - m + i(t - n))N(b) \leq \left(\frac{1}{4} + \frac{1}{4}\right)N(b) < N(b). \end{aligned}$$

Pokazali smo, da za naš R res veljata obe lastnosti iz definicije 3.7.

V poljubnem kolobarju lahko definiramo relacijo deljivosti ter največji skupni delitelj na povsem enak način kot v kolobarju celih števil. V vsakem Evklidovem kolobarju pa lahko s pomočjo norme N definiramo tudi Evklidov algoritem, ki ga tako kot pri celih številih, uporabimo za iskanje največjega skupnega delitelja.

Definicija 3.9. Naj bo R poljuben kolobar.

1. Naj bosta α, β elementa kolobarja R. Pravimo, da α deli β (oziroma $\alpha|\beta$), če obstaja tak $\gamma \in R$, da $\beta = \alpha\gamma$.

2. Element u kolobarja R je enota, če u deli 1.

3. Element π (različen od 0 ter od enote) kolobarja R je praštevilo, če za vsak $\alpha, \beta \in R$ velja: $\pi|\alpha\beta \Rightarrow \pi|\alpha$ ali $\pi|\beta$.

4. Ne-enota $\mu \in R$ je nerazcepna, če velja: $\mu = \alpha\beta \Rightarrow \alpha$ ali β je enota.

Opazimo, da je $u \in R$ enota natanko tedaj, ko obstaja tak μ, da je $u\mu = 1$. V poglavju 2 smo takšnim elementom rekli obrnljivi elementi kolobarja R. Množico vseh enot komutativnega kolobarja R označimo z $U(R)$ ali R^*.

Izrek 3.10. *V vsakem Evklidovem kolobarju velja Fundamentalni izrek aritmetike.*

Dokaz. Očitno je, da za vsak nerazcepen μ velja $N(\mu) \geq 2$. Podobno kot smo pokazali pri celih številih, tudi tu velja, da je razcepljanje na nerazcepna števila končno. Pokazati moramo le, da je vsako nerazcepno število praštevilo. To sledi po lemi 2.16. Naj bo μ nerazcepen in predpostavimo, da μ deli $\alpha\beta$, vendar ne deli α. Očitno je, da je največji skupni delitelj μ in α enak 1, saj ima μ le dva delitelja in sicer samega sebe ter enoto. Zapišemo lahko:

$$\mu x + \alpha y = 1, \tag{3.5}$$

za neka $x, y \in R$, po lemi 2.16. Če enačbo (3.5) sedaj pomnožimo z β, dobimo:

$$\mu x\beta + \alpha\beta y = \beta. \tag{3.6}$$

Ker po naši predpostavki μ deli oba člena na levi strani enačbe (3.6), mora deliti tudi člen na desni strani enačbe (3.6). Torej je predpostavka za praštevilskost iz definicije 3.9 izpolnjena. □

3.4 VSOTA KVADRATOV

Rešitev Pitagorove enačbe (enačbe (3.1)) je dobro poznan rezultat. Sedaj bomo pokazali še, kako Fundamentalni izrek aritmetike v drugih kontekstih pripelje do rešitev manj znanih diofantskih enačb. Vzemimo naslednji problem: Katera cela števila lahko zapišemo kot vsoto dveh kvadratov? To so rešitve diofantske enačbe

$$n = x^2 + y^2.$$

Če vzamemo nekaj majhnih praštevil za število n, opazimo naslednje.

Izrek 3.11. *Praštevilo p lahko zapišemo kot vsoto dveh kvadratov natanko tedaj, ko je $p = 2$ ali $p \equiv 1 \ (mod\ 4)$.*

Preden dokažemo izrek 3.11 si moramo pogledati še eno lemo.

Lema 3.12. *Če je $p = 2$ ali pa je p praštevilo kongruentno 1 modulo 4, potem je kongruenca $T^2 + 1 \equiv 0 \ (mod\ p)$ rešljiva v celih številih.*

Dokaz. Za $p = 2$ je očitno. Predpostavimo sedaj, da je $p = 4n + 1$, za neko pozitivno celo število n. Po izreku 2.24 velja:

$$(p-1)! = (p-1) \cdot (p-2) \cdots 3 \cdot 2 \cdot 1 \equiv -1 \ (mod\ p).$$

Če iz začetne predpostavke izrazimo $4n$, dobimo:

$$\begin{aligned} 4n = p - 1 &\equiv -1 \ (mod\ p) \\ 4n - 1 = p - 2 &\equiv -2 \ (mod\ p) \\ &\vdots \\ 2n + 1 = p - 2n &\equiv -2n \ (mod\ p). \end{aligned}$$

Sledi, da je:

$$(p-1)! = 4n! = 4n(4n-1)(4n-2)\cdots(2n+1)2n(2n-1)\cdots 3\cdot 2\cdot 1.$$

Če torej upoštevamo zgornje kongruence, dobimo, da je:

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

Ker pa po izreku 2.24 velja, da je $(p-1)!$ kongruentno -1 po modulu p, je za $T = (2n)!$ izpolnjen pogoj $T^2 + 1 \equiv 0 \ (mod\ p)$. □

Sedaj bomo dokazali izrek 3.11. Za dokaz bomo uporabili Fundamentalni izrek aritmetike v kolobarju $R = \mathbb{Z}[i]$ z normo $N : R \to \mathbb{N}$, definirano kot $N(x+iy) = x^2 + y^2$.

Dokaz. Za $p = 2$ je dokaz trivialen. V primeru, ko je $p \equiv 3 \ (mod\ 4)$, hitro opazimo, da se p ne da zapisati kot vsoto dveh kvadratov, ker so kvadrati vedno kongruenti 0 ali 1 modulo 4 in je zato vsota dveh kvadratov vedno kongruentna $0, 1$ ali 2 po modulu 4. Predpostavimo torej, da je $p \equiv 1 \ (mod\ 4)$ in naj bo p praštevilo. Po lemi 3.12 lahko zapišemo:

$$cp = T^2 + 1 = (T+i)(T-i) \text{ v } R = \mathbb{Z}[i], \text{ za } T, c \in \mathbb{Z}.$$

Izrek bomo dokazali s protislovjem. Predpostavimo, da je p nerazcepen v R. Ker v $\mathbb{Z}[i]$ velja Fundamentalni izrek aritmetike, je p praštevilo. Sledi, da mora p deliti enega izmed $T \pm i$ v R, ker deli njun produkt. Recimo, da p deli $T + i$. Obstaja torej tak element $a + bi \in R$, da je $T + i = p(a + bi)$. Torej je $T = pa$ in $1 = pb$. To pa je nemogoče, ker sta p in b celi števili in $p \geq 2$. Podobno dokažemo, da p ne more deliti $T - i$. Sledi, da p ne more biti nerazcepen v R, torej lahko zapišemo:

$$p = \mu\nu,$$

kjer sta μ in ν ne-enoti v R. Če vzamemo normo obeh strani, dobimo:

$$p^2 = N(\mu\nu) = N(\mu)N(\nu).$$

To je enačba v $\mathbb{Z}$ in po Fundamentalnem izreku aritmetike imamo tri možnosti:

1. $N(\mu) = 1$ in $N(\nu) = p^2$, kar je nemogoče, saj μ ni enota;
2. $N(\nu) = 1$ in $N(\mu) = p^2$, kar je nemogoče, saj ν ni enota;
3. $N(\mu) = N(\nu) = p$, iz česar sledi, da obstaja netrivialna rešitev enačbe $p = x^2 + y^2$.

□

Izrek 3.13. *Naj bo n naravno število in naj bo $n = p_1^{q_1} \cdot p_2^{q_2} \cdots p_r^{q_r}$ praštevilski razcep števila n. Število n lahko zapišemo kot vsoto dveh kvadratov natanko tedaj, ko za vsak p_i z lastnostjo $p_i \equiv 3 \ (mod\ 4)$ velja, da je q_i sodo število. Pri tem je $i \in \{1, 2, \ldots, r\}$. [3]*

Izreka 3.13 tu ne bomo dokazali, bralec pa lahko dokaz poišče v skripti [3, str. 8].

Primer 3.14. Vzemimo število 2.450. Njegov praštevilski razcep je:

$$2.450 = 2 \cdot 5^2 \cdot 7^2.$$

Od vseh praštevil, ki nastopajo v razcepu, je samo $7 \equiv 3 \ (mod\ 4)$ in število 7 v razcepu res nastopa na sodo potenco. Po izreku 3.13 lahko število 2.450 zapišemo kot vsoto dveh kvadratov. Velja: $2.450 = 7^2 + 49^2$. [24]

Izrek 3.15. *Naravno število n lahko zapišemo kot vsoto treh kvadratov natanko tedaj, ko n ni oblike $n = 4^a(8b + 7)$ za nenegativni celi števili a in b. [2]*

Izreka 3.15 tu ne bomo dokazali, bralec pa lahko za dokaz sledi članku [2].

Primer 3.16. Vzemimo število 129. Najprej moramo preveriti njegovo deljivost s številom 4. Praštevilski razcep števila 129 je:

$$129 = 3 \cdot 43.$$

Ker število 4 ne nastopa v praštevilskem razcepu, velja, da je $a = 0$. Sedaj moramo preveriti še ali je ostanek števila 129 pri deljenju s številom 8 enak 7, tj. ali lahko zapišemo $129 = 8b + 7$ za neko celo število b? Če enačbo malo preoblikujemo, dobimo $8b = 122$ in vidimo, da ne obstaja celo število b, ki bi rešilo to enačbo. Po izreku 3.15 lahko torej število 129 zapišemo kot vsoto treh kvadratov. Velja: $129 = 2^2+5^2+10^2$. [17]

3.4.1 Lagrangeov izrek štirih kvadratov

Eden izmed številnih klasičnih rezultatov elementarne teorije števil posploši izrek 3.11 na vsa cela števila, pri čemer dovoljuje, da se sešteje več kvadratov. Francoski matematik Bachet je predvidel rezultat, formuliral pa ga je Diofant. Domneva se, da je dokaz morda imel že Fermat, vendar je bil prvi objavljen dokaz Lagrangeov (1770) in tega si bomo pogledali mi.

Lema 3.17. *Naj bo p liho praštevilo. Potem obstajata celi števili a in b, tako da je:*

$$a^2 + b^2 + 1 \equiv 0 \ (mod\ p).$$

Dokaz. Definirajmo množici:

$$A = \left\{ a^2;\ 0 \leq a \leq \frac{p-1}{2} \right\} \quad \text{in} \quad B = \left\{ -b^2 - 1;\ 0 \leq b \leq \frac{p-1}{2} \right\}.$$

Vzemimo $0 \leq a_1 < a_2 \leq \frac{p-1}{2}$ in predpostavimo, da je $a_2^2 \equiv a_1^2 \ (mod\ p)$. Torej p deli $a_2^2 - a_1^2 = (a_2 + a_1)(a_2 - a_1)$. Ker je p praštevilo, velja, da p bodisi deli $a_2 + a_1$ bodisi

deli $a_2 - a_1$. Vendar pa je $1 \leq a_2 + a_1 \leq p-2$ in $1 \leq a_2 - a_1 \leq \frac{p-1}{2}$ in zato p ne more deliti niti $a_2 + a_1$ niti $a_2 - a_1$. Sledi, da števili a_1^2 in a_2^2 ne moreta biti kongruentni po modulu p. Na enak način bi pokazali, da tudi množica B ne vsebuje dveh elementov, ki bi bila kongruenta po modulu p. Sledi, da vsaka izmed teh dveh množic vsebuje $\frac{p+1}{2}$ elementov, ki so paroma nekongruentni po modulu p. Po Dirichletovem principu[1] mora obstajati nek element iz A, ki je enak nekemu elementu iz B po modulu p, saj obstaja le p različnih celih števil modulo p. Torej je $a^2 \ (mod\ p) \equiv -b^2 - 1 \ (mod\ p)$, za neki števili $0 \leq a, b \leq \frac{p-1}{2}$. Iz tega sledi, da obstajata celi števili a in b, tako da velja:

$$a^2 + b^2 + 1 \equiv 0 \ (mod\ p).$$

□

Izrek 3.18. *(Lagrange) Vsako pozitivno celo število je vsota kvadratov štirih celih števil.*

Dokaz. Najprej opazimo, da velja Eulerjeva identiteta štirih kvadratov:

$$(a^2 + b^2 + c^2 + d^2)(w^2 + x^2 + y^2 + z^2) = (aw + bx + cy + dz)^2 + (ax - bw - cz + dy)^2 + (ay + bz - cw - dx)^2 + (az - by + cx - dw)^2.$$

Dokaz identitete je enostaven, potrebno je le na daljše zapisati desno stran identitete. Identiteta nam pove, da se lastnost zapisa v obliki vsote kvadratov štirih števil ohrani pri množenju. Po Fundamentalnem izreku aritmetike je torej dovolj pokazati, da je vsako praštevilo vsota štirih kvadratov celih števil. Ker pa je $2 = 1^2 + 1^2 + 0^2 + 0^2$, je dovolj pokazati, da je vsako liho praštevilo vsota kvadratov štirih celih števil.
Naj bo p liho praštevilo. Po lemi 3.17 velja, da obstajajo $a, b, c, d \in \mathbb{Z}$ in $m \in \mathbb{Z}$, tako da velja:

$$mp = a^2 + b^2 + c^2 + d^2. \tag{3.7}$$

Če je $m = 1$, je dokaz zaključen. Predpostavimo torej, da je $m > 1$. Poiskati moramo zapis $m'p$ kot vsoto štirih kvadratov, pri čemer je $0 < m' < m$. To lahko ponavljamo dokler ne najdemo zapisa za praštevilo p, pri tem pa zmanjšujemo velikost m na vsakem koraku.
Če imamo sodo celo število $2n$ in ga zapišemo kot vsoto dveh kvadratov, tj. $2n = x^2 + y^2$, potem sta x in y obe sodi ali obe lihi števili. Sledi, da identiteta

$$n = \left(\frac{x+y}{2}\right)^2 + \left(\frac{x-y}{2}\right)^2 \tag{3.8}$$

izraža n kot vsoto kvadratov dveh celih števil. Če se sedaj vrnemo k enačbi (3.7) opazimo, da če je m sodo število, potem ni nobeno, sta dve ali pa so vsa štiri števila

[1] Dirichletov princip pravi, da če želimo $Q + 1$ elementov razporediti v Q škatel, mora vsaj ena škatla vsebovati več kot en element.

izmed a, b, c in d soda. Sedaj lahko dvakrat uporabimo enačbo (3.8) in sklepamo, da je $(\frac{m}{2})p$ vsota štirih kvadratov. V tem primeru smo prepolovili vrednost m.
Če je m liho število, potem pa najprej poiščimo števila w, x, y in z, za katera velja, da je $-\frac{m}{2} < w, x, y, z < \frac{m}{2}$ ter:

$$\begin{aligned} w &\equiv a \ (mod\ m) \\ x &\equiv b \ (mod\ m) \\ y &\equiv c \ (mod\ m) \\ z &\equiv d \ (mod\ m). \end{aligned}$$

Torej je:

$$w^2 + x^2 + y^2 + z^2 \equiv a^2 + b^2 + c^2 + d^2 = mp \equiv 0 \ (mod\ m) \quad \text{in} \quad w^2 + x^2 + y^2 + z^2 < m^2.$$

Sledi, da je:

$$w^2 + x^2 + y^2 + z^2 = km, \text{ za } 0 < k < m.$$

V Eulerjevi identiteti štirih kvadratov

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

je leva stran enaka km^2p. Glede na našo izbiro w, x, y, z je $ax \equiv bw$ in $dy \equiv cz$ modulo m, torej je $(ax - bw - cz + dy)^2$ deljiv z m^2. Podobno lahko pokažemo, da sta tudi $(ay + bz - cw - dx)^2$ in $(az - by + cx - dw)^2$ deljiva z m^2. Za prvi člen na desni strani Eulerjeve identitete pa velja:

$$aw + bx + cy + dz \equiv w^2 + x^2 + y^2 + z^2 \equiv 0 \ (mod\ m).$$

Desna stran Eulerjeve identitete štirih kvadratov je torej deljiva z m^2 in zato jo lahko pokrajšamo z m^2, kar nam da zapis za kp kot vsoto štirih kvadratov, kjer je $0 < k < m$. Če končno mnogokrat ponovimo ta postopek, bomo m zmanjšali na 1 in dobili zapis lihega praštevila p kot vsoto štirih kvadratov. □

3.5 SIEGELOV IZREK

V tem poglavju si bomo pogledali, kako lahko s pomočjo Fundamentalnega izreka aritmetike v kolobarjih, ki so večji od celih števil, dobimo vse celoštevilske rešitve nekaterih kubičnih enačb. Primer takega kolobarja so Gaussova cela števila.

Izrek 3.19. *Edina celoštevilska rešitev enačbe $y^2 = x^3 + x$, je $x = 0, y = 0$.*

Dokaz. Naj bosta x in y celi števili in naj bo $y^2 = x^3 + x$. To enačbo lahko zapišemo tudi kot $y^2 = x(x^2 + 1)$. Katerikoli x bo delil x^2, zato bo katerikoli skupni delitelj x in $x^2 + 1$ delil 1. Iz tega sledi, da sta x in $x^2 + 1$ tuji števili in po Fundamentalnem izreku aritmetike velja, da morata biti obe kvadrata, saj je njun produkt enak y^2. Zapišemo lahko:

$$z^2 = x^2 + 1 \quad \text{oziroma} \quad 1 = z^2 - x^2 = (z + x)(z - x).$$

Po Fundamentalnem izreku aritmetike v $\mathbb{Z}$, morata biti oba, tako $z + x$ kot tudi $z - x$, enaka 1 ali oba enaka -1. Iz enačbe $z^2 = x^2 + 1$ hitro sledi, da mora biti x enak 0 v obeh primerih. □

Izrek 3.20. *Edina celoštevilska rešitev enačbe $y^2 = x^3 - 1$, je $x = 1, y = 0$.*

Dokaz. Na prvi pogled izgleda, da bi morali desno stran enačbe $y^2 = x^3 - 1$ razcepiti v $\mathbb{Z}$, vendar je za dokaz lažje, če se premaknemo v kolobar $\mathbb{Z}[i]$, kjer prav tako velja Fundamentalni izrek aritmetike.
Enačbo iz izreka 3.20 lahko zapišemo kot $y^2 + 1 = x^3$ in če levo stran razcepimo v $\mathbb{Z}[i]$, dobimo:

$$(y + i)(y - i) = x^3. \tag{3.9}$$

Če bi vedeli, da sta števili $y + i$ in $y - i$ med seboj tuji, tj. $gcd(y + i, y - i) = 1$, bi lahko na podlagi Fundamentalnega izreka aritmetike trdili, da morata biti $y + i$ in $y - i$ kuba v kolobarju $\mathbb{Z}[i]$.
Če nek večkratnik števila 2 deli $y + i$ ali $y - i$, potem iz enačbe (3.9) sledi, da je x sodo število. Če je x sodo število, potem je $x^3 \equiv 0 \ (mod\ 8)$. Iz tega sledi, da je tudi $y^2 + 1 \equiv 0 \ (mod\ 8)$, ta kongruenca pa nima rešitve. Torej mora biti x liho število, y pa sodo število.
Naj bo $\delta = gcd(y + i, y - i)$. Če δ ni enota kolobarja $\mathbb{Z}[i]$, potem obstaja praštevilo p kolobarja $\mathbb{Z}[i]$, ki deli δ ter zato deli tudi $y + i$ in $y - i$. Sledi, da p deli tudi razliko števil $y + i$ in $y - i$, torej število $2i$. Število $2i$ se v kolobarju $\mathbb{Z}[i]$ razcepi na produkt praštevil takole: $2i = (1 + i)^2$. Število $1 + i$ je praštevilo kolobarja $\mathbb{Z}[i]$. Zapišemo lahko torej: $p = 1 + i$. Ker p deli $y + i$, obstaja tako število $a + ib$ kolobarja $\mathbb{Z}[i]$, da je $y + i = (1 + i)(a + ib)$. Torej mora veljati, da je $y = a - b$ in $1 = a + b$. Ker je $1 = a + b$, je eno od števil a, b sodo, drugo pa liho. Ker je $y = a - b$ sledi, da je y liho število, kar pa je v protislovju s tem, kar smo dokazali zgoraj. Torej je δ enota kolobarja $\mathbb{Z}[i]$ in sta $y + i$ ter $y - i$ med seboj tuji števili v kolobarju $\mathbb{Z}[i]$.
Po Fundamntalnem izreku aritmetike v $\mathbb{Z}[i]$ sledi, da sta $y + i$ in $y - i$ kuba v $\mathbb{Z}[i]$, torej lahko zapišemo:

$$y + i = (a + bi)^3; \ a, b \in \mathbb{Z}. \tag{3.10}$$

Če sedaj enačimo le imaginarni del, dobimo:

$$1 = 3a^2b - b^3 = b(3a^2 - b^2).$$

Po Fundamentalnem izreku aritmetike v $\mathbb{Z}$ velja:

$$b = (3a^2 - b^2) = \pm 1.$$

Če je $b = 1$, mora biti $3a^2 - 1 = 1$, kar pa je nemogoče, saj nobeno celo število a ne reši enačbe $3a^2 = 2$. Druga možnost je, da je $b = -1$. Tedaj je $3a^2 - 1 = -1$, torej je $3a^2 = 0$ oziroma $a = 0$.
Če sedaj dobljena a in b vstavimo v enačbo (3.10), dobimo rešitev $y = 0$. Iz enačbe $y^2 = x^3 - 1$ potem sledi, da je $x = 1$. □

Izrek 3.21. *(Siegelov izrek) Naj bodo $a, b, c \in \mathbb{Q}$. Potem obstaja le končno mnogo celoštevilskih parov (x, y), ki so rešitev enačbe*

$$y^2 = x^3 + ax^2 + bx + c, \tag{3.11}$$

pod pogojem, da kubični polinom $x^3 + ax^2 + bx + c$ nima večkratnih ničel.

Izreka 3.21 tu ne bomo dokazali, bralec pa lahko za dokaz sledi knjigi [6, str. 54].

Krivuljo, ki jo opisuje enačba (3.11), imenujemo *Eliptična krivulja*, pod pogojem, da desna stran nima večkratnih ničel.

Definicija 3.22. Število $a \in \mathbb{Z}$, ki ni kvadrat nekega celega števila, imenujemo *ne-kvadratno celo število.*

Primer 3.23. Ne-kvadratna cela števila so na primer $2, 3, 5, 6, \ldots$.

Določanje vseh celoštevilskih rešitev po Siegelovem izreku je v splošnem težka naloga. Šele proti koncu 20. stoletja so bile dodelane potrebne metode za praktično reševanje dane enačbe.

3.6 FERMAT, CATALAN IN EULER

V tem poglavju si bomo pogledali tri slavne diofantske probleme, ki so svojo rešitev dobili šele pred kratkim.

3.6.1 Fermat

Fermatov veliki izrek oziroma Fermatov zadnji izrek pravi, da enačba

$$x^n + y^n = z^n;\ n \geq 3 \tag{3.12}$$

nima netrivialnih celoštevilskih rešitev, torej je vsaj eden izmed x, y ali z enak 0. Enačbo (3.12) imenujemo *Fermatova enačba.*

Dokaz tega izreka je leta 1994 predstavil britanski matematik Andrew Wiles. Očitno je, da je izrek dovolj dokazati le za primer, ko je n praštevilo. Rešitev je odvisna od zapletenih rezultatov s področja aritmetike eliptične krivulje. Enačba $a^p + b^p + c^p = 0$, za neko praštevilo p in cela števila a, b in c različna od 0, je protiprimer Fermatovi enačbi. Ta protiprimer nas vodi do eliptične krivulje z enačbo $y^2 = x(x - a^p)(x + b^p)$ in izkaže se, da ta eliptična krivulja nima lastnosti, za katere je Wiles uspel dokazati, da jih mora imeti.

3.6.2 Catalan

Leta 1844 je belgijski matematik Catalan predstavil enačbo

$$u^x - v^y = 1,$$

za naravna števila $u, v, x, y \geq 2$. Hitro lahko preverimo, da je $u = 3, v = 2, x = 2, y = 3$ rešitev Catalanove enačbe:

$$3^2 - 2^3 = 9 - 8 = 1.$$

Torej Catalanova enačba premore vsaj eno celoštevilsko rešitev. Catalanov problem pa je pokazati, da je ta rešitev edina in to je leta 2002 dokazal romunski matematik Mihăilescu.

3.6.3 Euler

Leta 1769 je švicarski matematik Euler predstavil tako imenovano Eulerjevo domnevo, ki pravi, da n-ta potenca ne more biti izražena kot vsota manj kot n, ampak vsaj dveh, netrivialnih n-tih potenc za $n \geq 3$.
Lander in Parkin sta s pomočjo računalnika poiskala netrivialne rešitve diofantske enačbe

$$\sum_{i=1}^{n} x_i^5 = y^5;\ n \leq 6.$$

Med preostalimi rešitvami sta našla tudi protiprimer Eulerjevi domnevi za $n = 5$:

$$27^5 + 84^5 + 110^5 + 133^5 = 144^5.$$

V tem primeru je 5-ta potenca izražena kot vsota štirih 5-ih potenc, kar se ne ujema z Eulerjevo domnevo.
Poleg tega je bilo dokazano tudi, da v primeru, ko je $n = 4$, diofantska enačba

$$u^4 + v^4 + w^4 = x^4 \tag{3.13}$$

nima pozitivne celoštevilske rešitve za $x < 220.000$. Elkies je ugotovil, da ima enačba (3.13) naslednjo rešitev:

$$2.682.440^4 + 15.365.639^4 + 18.796.760^4 = 20.615.673^4.$$

Kasneje pa je Roger Frye poiskal minimalno rešitev enačbe (3.13) in ta je:

$$95.800^4 + 217.519^4 + 414.560^4 = 422.481^4.$$

Pokazal je tudi, da ne obstaja nobena druga rešitev za $u \leq v \leq w < x < 1.000.000$.

4 KVADRATNE DIOFANTSKE ENAČBE

Poskusi nadgradnje Pitagorove diofantske enačbe so hitro pripeljali do vprašanj o kvadratnih diofantskih enačbah. V tem poglavju jih bomo pobližje spoznali.

4.1 KVADRATNE KONGRUENCE

Na tem mestu bi želeli posplošiti rezultate iz prejšnjega poglavja in razložiti diofantsko enačbo

$$x^2 + 2y^2 = p, \tag{4.1}$$

kjer je p praštevilo, x in y pa sta celi števili. To lahko naredimo s pomočjo lastnosti kolobarja $R = \mathbb{Z}[\sqrt{-2}]$, vendar pa moramo tudi bolje spoznati aritmetiko celih števil modulo p, ko je p praštevilo.
Za razlago in razumevanje enačbe (4.1) bomo uporabili enolično določeno faktorizacijo v R skupaj z znanjem o kongruencah. Kongruenca, ki jo bomo preučevali, je

$$T^2 + 2 \equiv 0 \ (mod\ p).$$

Potrebovali bomo orodje, ki nam bo zagotavljalo obstoj rešitve kongurence oziroma nam bo povedalo, da neka kongruenca ni rešljiva. Območje, ki ga bomo gledali je $\mathbb{Z}_p$. Izkaže se, da je lastnost, ki jo potrebujemo, direktno povezana s konceptom iz teorije grup.

Definicija 4.1. Element $a \in \mathbb{Z}_p$ je *primitivni koren* modulo p, če je vsak neničelen element kolobarja $\mathbb{Z}_p$ enak neki potenci elementa a.

Primer 4.2. Vzemimo $a = 2$ in $p = 5$. Pokažimo, da potence števila a generirajo vse neničelne ostanke modulo p.
Možni neničelni ostanki modulo 5 so $1, 2, 3$ in 4. Poglejmo katere potence števila 2 generirajo neničelne ostanke modulo 5:

$$2^0 = 1 \equiv 1 \ (mod\ 5)$$
$$2^1 = 2 \equiv 2 \ (mod\ 5)$$
$$2^2 = 4 \equiv 4 \ (mod\ 5)$$
$$2^3 = 8 \equiv 3 \ (mod\ 5).$$

Torej je 2 primitivni koren modulo 5.

Množica $\mathbb{Z}_p$ tvori polje. Obstoj primitivnega korena a modulo p, je ekvivalenten temu, da je multiplikativna grupa $\mathbb{Z}_p^*$ polja $\mathbb{Z}_p$ ciklična, generirana z a. To pa lahko zapišemo na več različnih med seboj ekvivalnetnih načinov.

Z G označimo končno Abelovo grupo z n elementi. Tedaj je a generator grupe G natanko tedaj, ko velja eden izmed izmed naslednjih ekvivalentnih pogojev:

1. če je $a^m = 1$, kjer je $1 < m \leq n$, potem je $m = n$;
2. red elementa a je n;
3. če je $a^m = 1$, kjer je $1 < m$, potem $n|m$.

Izrek 4.3. *Multiplikativna grupa poljubnega končnega polja je ciklična.*

Preden dokažemo izrek 4.3, si moramo pogledati še nekaj drugih rezultatov.

Izrek 4.4. *(Kitajski izrek o ostankih) Naj bosta $m, n \in \mathbb{N}$ tuji števili ter a, b poljubni celi števili. Potem imata kongruenci $x \equiv a \ (mod\ m)$ in $x \equiv b \ (mod\ n)$ rešitev $x \in \mathbb{N}$ za vsaka $a, b \in \mathbb{Z}$. Rešitev je enolično določena po modulu mn.*

Kitajski izrek o ostankih je predstavil kitajski matematik Sun-tzu v 4. stoletju. Posebne rezultate sta pri svojem delu uporabljala tudi matematika Fibonacci in al-Haytham.

Sedaj bomo Kitajski izrek o ostankih še dokazali.

Dokaz. Pogoj, da sta števili tuji, nam zagotavlja, da obstajata taka m' in n', za katera velja $mm' \equiv 1 \ (mod\ n)$ in $nn' \equiv 1 \ (mod\ m)$. To velja zaradi posledice 2.20. Potem rešitev $x = bmm' + ann'$ zadošča obem kongruencam, saj je $bmm' + ann' \equiv a \ (mod\ m)$, ker je $bmm' \equiv 0 \ (mod\ m)$ in $ann' \equiv 1 \ (mod\ m)$. Podobno je $bmm' + ann' \equiv b \ (mod\ n)$.
Pokazati moramo še enoličnost rešitve modulo mn. Če x in y zadostita obem kongruencam, potem je razlika $(x - y)$ deljiva z m in n. Ker sta m in n tuji števili, mora biti razlika $(x - y)$ deljiva z mn. Torej sta x in y kongruentna po modulu mn. □

Primer 4.5. Zanima nas rešitev kongruenc $x \equiv 2 \ (mod\ 17)$ in $x \equiv 8 \ (mod\ 11)$.
Označimo:

- $a_1 = 2$ in $a_2 = 8$;
- $N_1 = 11$ in $N_2 = 17$;

- $N = N_1 \cdot N_2 = 11 \cdot 17 = 187$.

Iz kongruenc $11x_1 \equiv 1 \ (mod\ 17)$ in $17x_2 \equiv 1 \ (mod\ 11)$ dobimo, da je $x_1 = 14$ in $x_2 = 2$. Rešitev, ki jo iščemo, je:

$$\begin{aligned} X &= x_1 \cdot N_1 \cdot a_1 + x_2 \cdot N_2 \cdot a_2 \\ &= 14 \cdot 11 \cdot 2 + 2 \cdot 17 \cdot 8 \\ &= 580. \end{aligned}$$

Vse ostale rešitve so kongruentne 580 po modulu 187.

Definicija 4.6. *Aritmetična funkcija* je poljubna funkcija $f : \mathbb{N} \to \mathbb{C}$. Če za aritmetično funkcijo velja, da je $f(1) \neq 0$ ter da za poljubni tuji naravni števiili m in n velja $f(mn) = f(m)f(n)$, potem pravimo, da je f *multiplikativna funkcija*. Opazimo, da v tem primeru nujno velja $f(1) = 1$.
Če ima funkcija f to lastnost tudi za ne-tuji števili m in n, potem f imenujemo *popolnoma multiplikativna* funkcija.

Primer 4.7. Ena izmed najpomembnejših artimetičnih funkcij je:

$$\phi(n) = |\{1 \leq a \leq n | gcd(a, n) = 1\}|.$$

Funkciji ϕ pravimo *Eulerjeva ϕ funkcija*.

Lema 4.8. *Naj bo p praštevilo in $\alpha \geq 1$. Potem je $\phi(p^\alpha) = p^\alpha - p^{\alpha-1}$.*

Dokaz. Naj bo $1 \leq k \leq p^\alpha$ in $gcd(k, p^\alpha) = d \geq 2$.
Ker d deli p^α in ker je p praštevilo, je $d = p^\beta$, pri čemer je $1 \leq \beta \leq \alpha$. Sledi, da p deli d in ker d deli k velja, da p deli k. Število k je torej večkratnik števila p. Ker p deli k in p deli p^α, je $gcd(k, p^\alpha) \geq p \geq 2$.
Dokazali smo, da je $gcd(k, p^\alpha) \geq 2$ natanko tedaj, ko je k večkratnik števila p, torej za $k \in \{p, 2p, 3p, \ldots, p^{\alpha-1}p\}$. Teh večkratnikov števila p pa je ravno $p^{\alpha-1}$. □

Lema 4.9. *Eulerjeva ϕ funkcija je multiplikativna.*

Dokaz. Naj bosta m in n tuji števili. Za $x \in \mathbb{Z}_{mn}$ naj bo x_m enolično določeno število v $\mathbb{Z}_m$, ki je kongruentno številu x po modulu m. Podobno naj bo x_n enolično določeno število v $\mathbb{Z}_{mn}$, ki je kongruentno številu x po modulu n. Definirajmo preslikavo

$$f : \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$$

kot:

$$x \to (x_m, x_n).$$

Trdimo, da je f bijektivna funkcija. Za bijektivnost mora veljati, da se vsaka dva različna elementa iz $\mathbb{Z}_{mn}$ preslikata v različna elementa iz $\mathbb{Z}_m \times \mathbb{Z}_n$ ter da je vsak

element iz $\mathbb{Z}_m \times \mathbb{Z}_n$ slika vsaj enega elementa iz $\mathbb{Z}_{mn}$. Števili x_m in x_n smo definirali tako, da velja:

$$x \equiv x_m \ (mod\ m)$$
$$x \equiv x_n \ (mod\ n).$$

Po Kitajskem izreku o ostankih velja, da imata ti dve kongruenci rešitev x za poljubna x_m, x_n in ta rešitev je enolično določena po modulu mn. Iz tega direktno sledi bijektivnost funkcije f.
Definirajmo še $(\mathbb{Z}_n)^\star = \{1 \leq a \leq n : gcd(a, n) = 1\}$ ter analogno še za m in mn.
Ker je x tuj mn natanko takrat, ko je x_m tuj m in x_n tuj n, lahko definiramo še funkcijo

$$F : (\mathbb{Z}_{mn})^\star \to (\mathbb{Z}_m)^\star \times (\mathbb{Z}_n)^\star.$$

Za funkcijo F prav tako velja, da je bijektivna.
Po definiciji je kardinalnost $(\mathbb{Z}_m)^\star$ kar $F(m)$. Analogno velja tudi za n in mn, kar zaključi dokaz, da je F multiplikativna funkcija. □

Posledica 4.10. *Naj bo $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ praštevilska faktorizacija naravnega števila n. Potem je $\phi(n) = \prod_{p_i}(p_i - 1)p_i^{\alpha_i - 1} = n \prod_{p_i} \frac{p_i - 1}{p_i}$.*

Dokaz. Enakost $\phi(n) = \prod_{p_i}(p_i - 1)p_i^{\alpha_i - 1}$ sledi direktno iz leme 4.8.
Ker je funkcija ϕ multiplikativna, lahko zapišemo:

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

S tem smo pokazali še enakost $\phi(n) = n \prod_{p_i} \frac{p_i - 1}{p_i}$. □

Primer 4.11. $\phi(360) = \phi(2^3 \cdot 3^2 \cdot 5) = (2^3 - 2^2)(3^2 - 3^1)(5^1 - 5^0) = 4 \cdot 6 \cdot 4 = 96.$

Izrek 4.12. *Za vsak $n \in \mathbb{N}$, je*

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

Pri tem d preteče vse pozitivne delitelje števila n.

Dokaz. Opazimo, da rezultat očitno drži za $n = 1$, zato privzemimo, da je $n \geq 2$. Preverimo najprej enakost za primer, ko je $n = p^r$, torej potenca praštevila. V tem primeru je:

$$\sum_{d|n} \phi(d) = 1 + \sum_{i=1}^{r} (p-1)p^{i-1} = 1 + (p^r - 1) = p^r = n.$$

Definirajmo funkcijo $F(n) = \sum_{d|n} \phi(d)$. Pokažimo, da je funkcija F multiplikativna. Vemo, da d deli mn natanko tedaj, ko obstajata taka d_1 in d_2, da d_1 deli m in d_2 deli n, pri čemer je $d = d_1 d_2$. Torej za poljubni tuji števili m in n velja:

$$F(mn) = \sum_{d|mn} \phi(d) = \sum_{d_1|m} \sum_{d_2|n} \phi(d_1 d_2) = \sum_{d_1|m} \phi(d_1) \sum_{d_2|n} \phi(d_2) = F(m)F(n).$$

Naj bo sedaj $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$. Ker je funkcija F multiplikativna in ker smo že dokazali, da izrek 4.12 velja za potence praštevil, velja:

$$F(n) = F(p_1^{\alpha_1}) \cdots F(p_k^{\alpha_k}) = p_1^{\alpha_1} \cdots p_k^{\alpha_k} = n.$$

Torej izrek 4.12 velja za poljubno naravno število n. □

Primer 4.13. Vzemimo $n = 15$. Vsi pozitivni delitelji števila 15 so $1, 3, 5$ in 15. Po izreku 4.12 velja torej:

$$\phi(1) + \phi(3) + \phi(5) + \phi(15) = 15.$$

Če vrednosti izračunamo po definiciji Eulerjeve ϕ funkcije dobimo:

$$\phi(1) + \phi(3) + \phi(5) + \phi(15) = 1 + 2 + 4 + 8 = 15.$$

Sedaj imamo vse potrebno za dokaz izreka 4.3. V dokazu bomo uporabili splošno končno polje, ki ga lahko vedno eksplicitno zapišemo s polinomi, vendar bomo uporabili bolj abstraktno metodo.

Dokaz. Naj bo $\mathbb{F}_q$ končno polje s q elementi. Pokazali bomo, da če je $g \in \mathbb{F}_q^\star$, potem ima g^j enak red kot g natanko tedaj, ko je $gcd(j, q-1) = 1$. Pri tem $\mathbb{F}_q^\star$ predstavlja multiplikativno grupo polja $\mathbb{F}_q$. Na ta način bomo ugotovili, koliko elementov posameznega reda imamo, s čimer bomo pokazali, da ima grupa $\mathbb{F}_q^\star$ natanko $\phi(q-1)$ različnih generatorjev.

Za lažje razumevanje si poglejmo primer. Različne potence števila 3 v $\mathbb{F}_7^\star$ so:

$$3^0 \equiv 1, 3^1 \equiv 3, 3^2 \equiv 2, 3^3 \equiv 6, 3^4 \equiv 4 \text{ in } 3^5 \equiv 5 \text{ modulo } 7,$$

torej je 3 generator grupe $F_7^\star$. Edini vrednosti j, za kateri je $1 \leq j \leq 6$ in $gcd(j, 6) = 1$, sta 1 in 5. Ker je $3^5 \equiv 5 \ (mod\ 7)$, je tudi 5 generator $\mathbb{F}_7^\star$.

Poglejmo si še $\mathbb{F}_{11}^{\star} =< 2 >$. Vrednosti j, za katere je $1 \leq j \leq 10$ in $gcd(j, 10) = 1$, so $1, 3, 7$ in 9. Iz tega sledi, da imamo štiri generatorje grupe $\mathbb{F}_{11}^{\star}$, in sicer:

$$2^1 \equiv 2, 2^3 \equiv 8, 2^7 \equiv 7 \text{ in } 2^9 \equiv 6 \text{ modulo } 11.$$

Nadaljujmo sedaj z dokazom. Naj bo $a \in \mathbb{F}_q^{\star}$ ter naj bo d red elementa a. Vemo, da d deli red grupe $\mathbb{F}_q^{\star}$, torej $d|(q-1)$. Iz definicije reda elementa a sledi, da če je $a^m = 1$ za nek m $(0 \leq m < d)$, potem je nujno $m = 0$. Trdimo, da so elementi $1, a, a^2, \ldots a^{d-1}$ paroma različni. Recimo, da obstajata taka $i, j \in \{0, 1, \ldots d-1\}$, kjer je $i \leq j$ in velja $a^i = a^j$. Potem je $a^{j-i} = 1$, iz česar sledi, da je $j - i = 0$ oziroma $i = j$. Elementi $1, a, a^2, \ldots a^{d-1}$ so torej res paroma različni.

Trdimo, da so preostali elementi reda d v $\mathbb{F}_q^{\star}$ natanko tisti a^j z $1 \leq j < d$, za katere je $gcd(j, d) = 1$. Torej, če obstaja element reda d, bo takih natanko $\phi(d)$. Če je red elementa a enak d, potem morajo preostali elementi reda d biti med potencami a^j, saj vsak element reda d zadošča enačbi $x^d - 1 = 0$ v $\mathbb{F}_q$. Ta enačba ima kvečjemu d ničel in vsaka potenca a^j, kjer je $0 \leq j < d$, zadošča tej enačbi. Torej morajo biti vsi elementi reda d med temi potencami. Katere potence pa imajo red d? Pokazali bomo, da je red a^j enak d $(1 \leq j < d)$ natanko tedaj, ko je $gcd(j, d) = 1$.

Če je $1 < gcd(j, d) = d' < d$, potem je $1 < \frac{d}{d'} < d$ in $(a^j)^{\frac{d}{d'}} = (a^d)^{\frac{j}{d'}} = 1^{\frac{j}{d'}} = 1$. Torej je red elementa a^j manjši ali enak $\frac{d}{d'}$ in zato ni enak d.

Obratno, predpostavimo sedaj, da je $gcd(j, d) = 1$ in da ima a^j red d'', pri čemer je $1 < d'' \leq d$. Potem je $a^{jd''} = 1$, torej $d|jd''$, saj je red a enak d. Ker je $gcd(j, d) = 1$, sledi, da $d|d''$. Po drugi strani pa je $d'' \leq d$, iz česar sledi, da je $d = d''$. Torej je red a^j res enak d natanko tedaj, ko je $gcd(j, d) = 1$.

Vsak izmed $(q-1)$ elementov $\mathbb{F}_q^{\star}$ ima red, ki deli $(q-1)$. Po izreku 4.12 sledi, da je $\sum_{d|(q-1)} \phi(d) = q - 1$.

Torej moramo za vsak d, ki deli $(q-1)$, imeti $\phi(d)$ elementov reda d. V posebnem imamo $\phi(q-1) \geq 1$ elementov reda $(q-1)$, torej je grupa $F_q^{\star}$ res ciklična. □

Z dokazom smo pokazali, koliko elementov polja $\mathbb{F}_q$ je vsakega možnega reda in ugotovili smo, da mora biti vsaj en element reda $(q-1)$, kateri je torej primitivni koren.

Primer 4.14. Število 3 je primitivni koren za $p = 7$. Poglejmo zakaj:

$$3^1 = 3 \equiv 3 \ (mod\ 7)$$
$$3^2 = 9 \equiv 2 \ (mod\ 7)$$
$$3^3 = 27 \equiv 6 \ (mod\ 7)$$
$$3^4 = 81 \equiv 4 \ (mod\ 7)$$
$$3^5 = 243 \equiv 5 \ (mod\ 7)$$
$$3^6 = 729 \equiv 1 \ (mod\ 7)$$
$$3^7 = 2187 \equiv 3 \ (mod\ 7).$$

Vidimo, da je red elementa 3 enak $7-1=6$ in zato je 3 primitivni koren za $p=7$.

Na tem področju ostaja še veliko odprtih vprašanj in eno izmed njih je *Artinova domneva*.
Artinova domneva: Vsako celo število, ki ni kvadrat ali -1, je primitivni koren modulo p za neskončno mnogo praštevil p.

Še eno odprto vprašanje pa je, ali obstaja algoritem, s katerim bi lahko določili primitivni koren. Če je na primer p dano praštevilo, ali lahko določimo primitivni koren za p? Najbolj očitna metoda je, da po vrsti preizkušamo cela števila $2, 3, 5, 6, \ldots$ in upamo, da bomo hitro našli primitivni koren.
Leta 1992 je matematik Victor Shoup pogojno pokazal, da je najmanjši primitivni koren modulo p navzgor omejen s $C(\log p)^6$, pri čemer je C neka konstanta. Ta rezultat sicer temelji na še nedokazani hipotezi, vseeno pa se v praksi izkaže, da je zelo uporaben.

4.2 EULERJEV KRITERIJ

Veliko problemov iz področja kvadratnih kongruenc se lahko prevede na reševanje najenostavnejše kvadratne kongruence, tj. $x^2 \equiv a \ (mod\ p)$ za praštevilo p in poljubno celo število a. Tako celo število a imenujemo *kvadratni ostanek* modulo p. Eulerjev kriterij nam pove, ali je neko celo število kvadratni ostanek po modulu p.

Definicija 4.15. Naj bo p liho praštevilo in a celo število. *Legendrov simbol* definiramo kot:

$$\left(\frac{a}{p}\right) = \begin{cases} 0; & \text{če } p \text{ deli } a, \\ 1; & \text{če } p \text{ ne deli } a \text{ in ima } x^2 \equiv a \ (mod\ p) \text{ rešitev}, \\ -1; & \text{sicer.} \end{cases}$$

Če je $a \neq 0$ in $\left(\frac{a}{p}\right) = -1$, pravimo, da je a *kvadratni neostanek* modulo p, sicer pa je a *kvadratni ostanek* modulo p.

V splošnem za Legendrov simbol velja, da če je $a \equiv b \ (mod\ p)$, potem je $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$ in za vsak $a \neq 0$ je $\left(\frac{a^2}{p}\right) = 1$.

Izrek 4.16. *(Eulerjev kriterij) Naj bo p liho praštevilo. Potem je:*

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \ (mod\ p). \tag{4.2}$$

Dokaz. V primeru, ko je $a \equiv 0 \ (mod\ p)$, rezultat sledi direktno iz definicije 4.15. Predpostavimo sedaj, da sta a in p tuji števili. Opazimo, da so edino kvadratni koreni od 1 modulo p kongruentni ± 1, saj je $x^2 - 1 = (x-1)(x+1)$ v poljubnem polju.
Po izreku 2.23 velja:

$$(a^{(p-1)/2})^2 = a^{p-1} \equiv 1 \ (mod\ p),$$

iz česar sledi, da je $a^{(p-1)/2} \equiv \pm 1 \ (mod\ p)$.
Označimo z g generator ciklične grupe $\mathbb{Z}_p^\star$. Potem je $a \equiv g^j \ (mod\ p)$ za nek j in a je kvadratni ostanek natanko tedaj, ko je j sodo število. Predpostavimo, da je a kvadratni ostanek. Zapišemo lahko $j = 2j'$ za neko celo število j'. Po izreku 2.23 velja:

$$a^{(p-1)/2} \equiv (g^j)^{(p-1)/2} = g^{j'(p-1)} = (g^{p-1})^{j'} \equiv 1 \ (mod\ p).$$

Torej $\left(\frac{a}{p}\right) = 1$ implicira, da je $a^{(p-1)/2} \equiv 1 \ (mod\ p)$.
Obratno, če je $a^{(p-1)/2} \equiv 1 \ (mod\ p)$, potem je $g^{j(p-1)/2} \equiv 1 \ (mod\ p)$. Red elementa g je $p-1$ modulo p, zato $p-1$ deli $\frac{j(p-1)}{2}$. Iz tega sledi, da $2(p-1)$ deli $j(p-1)$ in če pokrajšamo $(p-1)$ na obeh straneh, vidimo, da mora biti j sodo število. Torej kongruenca $a^{(p-1)/2} \equiv 1 \ (mod\ p)$ implicira, da je $\left(\frac{a}{p}\right) = 1$. □

Posledica 4.17. *Legendrov simbol zadošča enačbi:*

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

Torej, če Legendrov simbol pogledamo kot aritmetično funkcijo $\left(\frac{\cdot}{p}\right) : \mathbb{Z} \to \{0, \pm 1\}$*, je popolnoma multiplikativna.*

Ta posledica sledi direktno iz izreka 4.16, saj je desna stran enačbe (4.2) popolnoma multiplikativna.

4.3 KVADRATNI RECIPROČNOSTNI ZAKON

Glavni rezultat o kvadratnih ostankih je Kvadratni recipročnostni zakon. Gauss se je veliko ukvarjal s kvadratnimi ostanki in zanimalo ga je, če morda obstaja povezava med tem, da je p kvadratni ostanek modulo q in tem, da je q kvadratni ostanek modulo p, ko sta p in q praštevili. Na podlagi obsežnih izračunov je domneval in kasneje tudi dokazal naslednje:
Ko je eden izmed p in q kongruenten 1 modulo 4, sta obe spodnji kongruenci rešljivi ali pa obe nerešljivi:

$$x^2 \equiv q \ \ (mod\ p),\ y^2 \equiv p \ \ (mod\ q).$$

Če sta p in q oba kongruenta 3 modulo 4, potem je ena izmed kongruenc rešljiva natanko tedaj, ko druga ni.

Izrek 4.18. *(Kvadratni recipročnosti zakon) Naj bosta p in q lihi praštevili. Če je $p \equiv q \equiv 3 \pmod 4$, potem je*

$$\left(\frac{q}{p}\right) = -\left(\frac{p}{q}\right).$$

Če je vsaj eden izmed p in q kongruenten 1 modulo 4, pa je

$$\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right).$$

Izrek 4.18 lahko zapišemo kot bolj urejeno formulo. Če sta p in q lihi praštevili, potem je

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

Primer, ko imamo sodo praštevilo 2, moramo obravnavati ločeno.

Izrek 4.19. *Če je p liho praštevilo, potem je*

$$\left(\frac{2}{p}\right) = 1 \text{ natanko tedaj, ko je } p \equiv \pm 1 \pmod 8.$$

Preden dokažemo izrek 4.19 si moramo pogledati še eno lemo.

Lema 4.20. *Naj bo p liho praštevilo. Definirajmo funkcijo $f : \mathbb{Z} \to \{0, \pm 1\}$ kot:*

$$f(j) = \begin{cases} 0; \ j \text{ sod}, \\ (-1)^{(j^2-1)/8}; \ j \text{ lih}. \end{cases}$$

Potem je $f(p)f(jp) = f(j)$.

Dokaz. Po predpostavki je p liho preštevilo in zato je $p^2 - 1 \equiv 0 \pmod 8$. Rezultat leme 4.20 je očiten, če je j sodo število. Predpostavimo, da je j liho število. Če poračunamo $f(jp)$, dobimo:

$$\begin{aligned} f(jp) &= (-1)^{((jp)^2-1)/8} \\ &= (-1)^{((jp)^2-p^2+p^2-1)/8} \\ &= ((-1)^{p^2})^{(j^2-1)/8}(-1)^{(p^2-1)/8} \\ &= (-1)^{(j^2-1)/8}(-1)^{(p^2-1)/8}. \end{aligned}$$

Opazimo, da je $f(jp) = f(j)f(p)$. Če obe strani te enačbe pomnožimo z $f(p)$, dobimo:

$$f(jp)f(p) = f(j)f(p)^2. \tag{4.3}$$

Ker je $f(p) = \pm 1$, je $f(p)^2 = 1$. Enačbo (4.3) lahko torej zapišemo kot:

$$f(jp)f(p) = f(j). \tag{4.4}$$

Enačba (4.4) je ravno rezultat leme 4.20. □

Sedaj bomo dokazali izrek 4.19, ki nam služi kot test za dokaz izreka 4.18.

Dokaz. Praštevilo p je po predpostavki liho in zato je $p^2 - 1 \equiv 0 \ (mod\ 8)$. Označimo z $\mathbb{F}$ polje, ki ima p^2 elementov. Potem je $\mathbb{F}^\star$ ciklična grupa reda $p^2 - 1$ (po izreku 4.3). Ker je $p^2 - 1$ deljiv z 8, $\mathbb{F}^\star$ vsebuje element reda 8. Označimo ta element s k. Velja, da je $(k^4)^2 = k^8 = 1$, iz česar sledi, da je $k^4 = -1$, saj je k reda 8 in zato k^4 ne more biti enak 1. Sledi, da je $k^5 = -k$ in $k^7 = -k^3$.
Naj bo $G = k - k^3 - k^5 + k^7$. Zapišemo torej lahko:

$$G = 2(k - k^3) \quad \text{in} \quad G^2 = 4(k - k^3)^2 = 4(k^2 - 2k^4 + k^6).$$

Vemo, da je $k^4 = -1$ oziroma $k^4 + 1 = 0$, iz česar sledi, da je $k^6 + k^2 = 0$. Velja torej, da je $G^2 = -8k^4 = 8$.
Izrek 4.19 bomo dokazali tako, da bomo za G^p poiskali dva različna izraza.
Prvi izraz za G^p:

$$\begin{aligned} G^p &= G \cdot G^{p-1} \\ &= G \cdot (G^2)^{(p-1)/2} \\ &= G \cdot (8)^{(p-1)/2} \\ &= G \cdot \left(\frac{8}{p}\right) \text{ (po izreku 4.16)} \\ &= G \cdot \left(\frac{4}{p}\right) \cdot \left(\frac{2}{p}\right) \text{ (po posledici 4.17)} \\ &= G \cdot \left(\frac{2^2}{p}\right) \cdot \left(\frac{2}{p}\right) \\ &= G \cdot 1 \cdot \left(\frac{2}{p}\right) \\ &= G \cdot \left(\frac{2}{p}\right). \end{aligned}$$

Drugi izraz za G^p: Definirajmo funkcijo $f : \mathbb{Z} \to \{0, \pm 1\}$ kot:

$$f(j) = \begin{cases} 0; \text{ j sod}, \\ (-1)^{(j^2-1)/8}; \text{ j lih}. \end{cases}$$

Poglejmo, za katere j je $f(j) = 1$. Vemo, da je $Z_8 = \{0, 1, 2, \ldots, 7\}$. Ker mora biti j liho število, da je lahko $f(j) = 1$, nam preostanejo elementi $\{1, 3, 5, 7\}$. Če te elemente vstavimo v enačbo $(-1)^{(j^2-1)/8}$ vidimo, da dobimo $f(j) = 1$ za $j = 1$ in $j = 7$. Vemo, da je $1 \equiv 1 \ (mod\ 8)$ in $7 \equiv -1 \ (mod\ 8)$. Velja torej, da je $f(j) = 1$ natanko tedaj, ko je $j \equiv \pm 1 \ (mod\ 8)$. Podobno se lahko prepričamo, da je $f(j) = -1$ natanko tedaj, ko je $j \equiv 3$ ali $5 \ (mod\ 8)$.
Polje $\mathbb{F}$ ima karakteristiko p, torej je $(a + b)^p = a^p + b^p$ v $\mathbb{F}$, saj so vsi binomski koeficienti, razen robnih, deljivi s p. Po indukciji sledi:

$$(a_1 + \cdots + a_n)^p = a_1^p + \cdots + a_n^p.$$

Z uporabo enačbe $G = k - k^3 - k^5 + k^7$ in definicije funkcije f lahko zapišemo:

$$\begin{aligned} G &= f(1)k + f(3)k^3 + f(5)k^5 + f(7)k^7 \\ &= f(0) + f(1)k + f(2)k^2 + \cdots + f(7)k^7 \\ &= \sum_{j=0}^{7} f(j)k^j. \end{aligned}$$

Sledi, da je:

$$G^p = \left(\sum_{j=0}^{7} f(j)k^j \right)^p = \sum_{j=0}^{7} f(j)^p k^{jp} = \sum_{j=0}^{7} f(j)k^{jp}. \tag{4.5}$$

Z uporabo leme 4.20 lahko enačbo (4.5) zapišemo kot:

$$G^p = \sum_{j=0}^{7} f(j)k^{jp} = \sum_{j=0}^{7} f(p)f(jp)k^{jp} = f(p)\sum_{j=0}^{7} f(jp)k^{jp}.$$

Naj bo p fiksen. Potem jp $(mod\ 8)$ zavzame vsako od vrednosti $0, 1, \ldots, 7$, ko gre j od 0 do 7. Iz tega sledi, da je $G^p = f(p)G$. To je drugi izraz za G^p. Če sedaj enačimo oba izraza za G^p, dobimo:

$$G \cdot \left(\frac{2}{p}\right) = f(p)G. \tag{4.6}$$

Ker je $G^2 = 8$, G ni enak 0 v $\mathbb{F}$ in zato lahko obe strani enačbe (4.6) delimo z G. Dobimo enačbo:

$$\left(\frac{2}{p}\right) = f(p) = 1 \text{ natanko tedaj, ko je } p \equiv \pm 1 \ (mod\ 8).$$

□

Sedaj smo pripravljeni na dokaz Kvadratnega recipročnostnega zakona (izrek 4.18).

Dokaz. Predpostavimo, da imamo polje $\mathbb{F}$ s p^{q-1} elementi. Potem je $\mathbb{F}^\star$ ciklična grupa reda $p^{q-1} - 1$ (po izreku 4.3). Po Malem Fermatovem izreku je $p^{q-1} \equiv 1 \ (mod\ q)$ in zato v $\mathbb{F}^\star$ obstaja element reda q. Označimo ta element s k.
Definirajmo:

$$G = \sum_{j=1}^{q-1} \left(\frac{j}{q}\right) k^j. \tag{4.7}$$

Vsoto (4.7) imenujemo *Gaussova vsota*.

Dokaz bo potekal na enak način kot dokaz izreka 4.19 in sicer bomo poiskali dva različna izraza za G^p.
Prvi izraz za G^p: Za zapis prvega izraza G^p bomo potrebovali G^2. Zapišemo lahko:

$$G^2 = \sum_{j=1}^{q-1} \left(\frac{j}{q}\right) k^j \sum_{i=1}^{q-1} \left(\frac{-i}{q}\right) k^{-i},$$

saj ko i preteče $1, \ldots, q-1$, $-i$ prav tako preteče $1, \ldots, q-1$ modulo q. Po posledici 4.17 je

$$\left(\frac{-i}{q}\right) = \left(\frac{-1}{q}\right) \cdot \left(\frac{i}{q}\right).$$

Zapišemo lahko torej:

$$G^2 = \sum_{j=1}^{q-1} \left(\frac{j}{q}\right) k^j \sum_{i=1}^{q-1} \left(\frac{-1}{q}\right) \left(\frac{i}{q}\right) k^{-i}. \tag{4.8}$$

Če v enačbi (4.8) faktor $\left(\frac{-1}{q}\right)$ izpostavimo pred vsoto in v drugi vsoti zamenjamo i z ji, dobimo:

$$G^2 = \left(\frac{-1}{q}\right) \sum_{j=1}^{q-1} \sum_{i=1}^{q-1} \left(\frac{j}{q}\right) \left(\frac{ji}{q}\right) k^{j(1-i)}. \tag{4.9}$$

Po posledici 4.17 je $\left(\frac{j}{q}\right)\left(\frac{ji}{q}\right) = \left(\frac{i}{q}\right)$ in zato lahko enačbo (4.9) zapišemo kot:

$$G^2 = \left(\frac{-1}{q}\right) \sum_{j=1}^{q-1} \sum_{i=1}^{q-1} \left(\frac{i}{q}\right) k^{j(1-i)}.$$

Opazimo, da je $\sum_{i=1}^{q-1} \left(\frac{i}{q}\right) k^{0(1-i)} = 0$, saj je polovica neničelnih ostankov po modulu q kvadratov in zato je polovica vrednosti simbola enaka 1, polovica pa -1. Zapišemo lahko torej:

$$G^2 = \left(\frac{-1}{q}\right) \sum_{j=0}^{q-1} \sum_{i=1}^{q-1} \left(\frac{i}{q}\right) k^{j(1-i)}.$$

Če dvojno vsoto zapišemo nekoliko drugače, dobimo:

$$G^2 = \left(\frac{-1}{q}\right) \sum_{i=1}^{q-1} \left(\frac{i}{q}\right) \sum_{j=0}^{q-1} k^{j(1-i)}. \tag{4.10}$$

Izraz za $i = 1$ k G^2 prispeva $\left(\frac{-1}{q}\right) q = (-1)^{(q-1)/2} q$ (po izreku 4.16). Trdimo, da vsi ostali izrazi enačbe (4.10) k G^2 ne prispevajo nič. Predpostavimo, da je $i \neq 1$ in pišimo $\eta = k^{1-i}$. Potem je η netrivialen q-ti koren od 1. Definirajmo: $S = 1 + \eta + \cdots + \eta^{q-1}$. Trdimo, da je $S = 0$. Zapišemo lahko:

$$\eta S = \eta + \eta^2 + \ldots \eta^{q-1} + \eta^q = \eta + \eta^2 + \cdots + \eta^{q-1} + 1 = S.$$

Enačba $\eta S = S$ ima dve možni rešitvi, $\eta = 1$ in $S = 0$. Če je $\eta = k^{1-i} = 1$, je $1 - i = 0$ oziroma $i = 1$. To je v nasprotju z našo predpostavko in zato sledi, da je $S = 0$. S tem smo pokazali, da je sumand desne strani enačbe (4.10), ki ga doprinese $i \neq 1$, res

enak 0. Velja torej, da je $G^2 = (-1)^{(q-1)/2}q$. Sedaj imamo vse kar potrebujemo, da izpeljemo prvi izraz za G^p:

$$\begin{aligned} G^p &= GG^{p-1} \\ &= G(G^2)^{(p-1)/2} \\ &= G((-1)^{(q-1)/2}q)^{(p-1)/2} \\ &= G(-1)^{(q-1)/2\cdot(p-1)/2}q^{(p-1)/2} \\ &= G(-1)^{(q-1)/2\cdot(p-1)/2}\left(\frac{q}{p}\right) \text{ (po izreku 4.16).} \end{aligned}$$

Drugi izraz za G^p:
Po definiciji Gaussove vsote lahko zapišemo:

$$G^p = \left(\sum_{j=1}^{q-1}\left(\frac{j}{q}\right)k^j\right)^p = \sum_{j=1}^{q-1}\left(\frac{j}{q}\right)k^{jp}. \tag{4.11}$$

V enačbi (4.11) smo uporabili dejstvo, da je karakteristika polja $\mathbb{F}$ enaka p ter da je $\left(\frac{j}{q}\right)^p = \left(\frac{j}{q}\right)$. Zaradi posledice 4.17 lahko enačbo (4.11) dalje zapišemo kot:

$$G^p = \sum_{j=1}^{q-1}\left(\frac{p\cdot p}{q}\right)\left(\frac{j}{q}\right)k^{jp} = \left(\frac{p}{q}\right)\sum_{j=1}^{q-1}\left(\frac{jp}{q}\right)k^{jp}, \tag{4.12}$$

saj je $\left(\frac{p}{q}\right) = \pm 1$ in je torej $\left(\frac{p}{q}\right)^2 = 1$. Vemo, da jp $(mod\ q)$ zavzame vsako od vrednosti $0, 1, \ldots, q-1$, ko gre j od 0 do $q-1$. Z uporabo tega dejstva iz enačbe (4.12) dobimo še drugi izraz za G^p:

$$G^p = \left(\frac{p}{q}\right)G. \tag{4.13}$$

Če sedaj enačimo oba izraza za G^p, dobimo:

$$G(-1)^{(q-1)/2\cdot(p-1)/2}\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)G. \tag{4.14}$$

Ker je $G^2 = (-1)^{(q-1)/2}q$, G ni enak 0 v $\mathbb{F}$ in zato lahko obe strani enačbe (4.14) delimo z G. S tem je Kvadratni recipročnostni zakon dokazan. □

Kvadratni recipročnostni zakon je pomemben zato, ker nam omogoča hitro računanje Legendrovega simbola.

Primer 4.21. Izračunajmo Legendrov simbol $\left(\frac{91}{167}\right)$ z uporabo Kvadratnega recipročnostnega zakona. Najprej opazimo, da lahko zapišemo:

$$\left(\frac{91}{167}\right) = \left(\frac{7}{167}\right)\left(\frac{13}{167}\right).$$

Ker je

$$7 \equiv 3 \ (mod\ 4)$$
$$13 \equiv 1 \ (mod\ 4)$$
$$167 \equiv 3 \ (mod\ 4),$$

lahko s pomočjo Kvadratnega recipročnostnega zakona zapišemo:

$$\left(\frac{91}{167}\right) = \left(\frac{7}{167}\right)\left(\frac{13}{167}\right) = -\left(\frac{167}{7}\right)\left(\frac{167}{13}\right) = -\left(\frac{6}{7}\right)\left(\frac{11}{13}\right).$$

Če uporabimo še definicjo 4.15, dobimo:

$$\left(\frac{6}{7}\right) = \left(\frac{2}{7}\right)\left(\frac{3}{7}\right) = 1 \cdot \left(\frac{3}{7}\right) = -\left(\frac{7}{3}\right) = -\left(\frac{1}{3}\right) = -1$$

in

$$\left(\frac{11}{13}\right) = \left(\frac{13}{11}\right) = \left(\frac{2}{11}\right) = -1.$$

Če to sedaj združimo, dobimo rezultat: $\left(\frac{91}{167}\right) = -1$.

4.4 ENOTE V KOLOBARJU

V tem poglavju si bomo pogledali več o enotah v kolobarju $\mathbb{Z}[\sqrt{d}]$ za celo število $d > 0$. Za $d < 0$ ima kolobar $\mathbb{Z}[\sqrt{d}]$ le končno mnogo enot.

Definicija 4.22. Za število a pravimo, da je *kvadratov prosto celo število*, če v njegovem praštevilskem razcepu ni dveh enakih praštevil. Ekvivalentno, število a je *kvadratov prosto celo število*, če ni deljivo z nobenim popolnim kvadratom razen z 1. [23]

Direktno iz definicije sledi, da so praštevila trivialna kvadratov prosta cela števila. Po dogovoru je tudi število 1 kvadratov prosto celo število.

Primer 4.23. Poglejmo število 15. Praštevilski razcep števila 15 je:

$$15 = 3 \cdot 5.$$

Po definiciji je torej število 15 kvadratov prosto celo število.
Poglejmo še število 100. Preštevilski razcep števila 100 je:

$$100 = 4 \cdot 25 = 2^2 \cdot 5^2.$$

Po definiciji torej število 100 ni kvadratov prosto celo število.

Naj bo sedaj d kvadratov prosto celo število. Oglejmo si kolobar

$$\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d};\ a, b \in \mathbb{Z}\}.$$

Na kolobarju $\mathbb{Z}[\sqrt{d}]$ definirajmo funkcijo $N : \mathbb{Z}[\sqrt{d}] \to \mathbb{Z}$ takole:

$$N(a + b\sqrt{d}) = a^2 - b^2 d.$$

Funkciji N včasih rečemo tudi norma na kolobarju $\mathbb{Z}[\sqrt{d}]$, čaprav se to ne ujema z našo definicijo 3.7, saj ima naša funkcija N lahko tudi negativne vrednosti. Velja pa naslednja lema.

Lema 4.24. *Naj bo $\alpha, \beta \in \mathbb{Z}[\sqrt{d}]$. Potem je $N(\alpha\beta) = N(\alpha)N(\beta)$.*

Dokaz. Naj bo $\alpha = a + b\sqrt{d}$ in $\beta = e + f\sqrt{d}$. Poračunajmo $N(\alpha\beta)$ in $N(\alpha)N(\beta)$.

1. $$\begin{aligned} N(\alpha\beta) &= N((a + b\sqrt{d})(e + f\sqrt{d})) \\ &= N((ae + bfd) + (af + be)\sqrt{d}) \\ &= (ae + bfd)^2 - (af + be)^2 d \\ &= a^2e^2 + b^2f^2d^2 - a^2f^2d - b^2e^2d \end{aligned}$$

2. $$\begin{aligned} N(\alpha)N(\beta) &= N(a + b\sqrt{d})N(e + f\sqrt{d}) \\ &= (a^2 - b^2d)(e^2 - f^2d) \\ &= a^2e^2 - a^2f^2d - b^2e^2d + b^2f^2d^2 \end{aligned}$$

Vidimo torej, da sta ti dve vrednosti res enaki. □

Spomnimo se, da je element $\alpha \in \mathbb{Z}[\sqrt{d}]$ enota kolobarja $\mathbb{Z}[\sqrt{d}]$, če obstaja tak element $\beta \in \mathbb{Z}[\sqrt{d}]$, da je $\alpha\beta = 1$. Naj bo sedaj $\alpha = x + y\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$ in privzemimo, da je $N(\alpha) = 1$. Potem je očitno α enota kolobarja $\mathbb{Z}[\sqrt{d}]$, saj za element $\beta = x - y\sqrt{d}$ velja, da je $\alpha\beta = 1$. Podobno vidimo, da je element $\alpha \in \mathbb{Z}[\sqrt{d}]$ enota tudi v primeru, ko je $N(\alpha) = -1$. Dokažimo sedaj, da velja tudi obratno.

Lema 4.25. *Naj bo $\alpha \in \mathbb{Z}[\sqrt{d}]$ enota. Potem je $N(\alpha) = \pm 1$.*

Dokaz. Ker je α enota kolobarja $\mathbb{Z}[\sqrt{d}]$, obstaja tak $\beta \in \mathbb{Z}[\sqrt{d}]$, da je $\alpha\beta = 1$. Po lemi 4.24 torej velja:

$$N(\alpha)N(\beta) = N(\alpha\beta) = N(1) = 1. \tag{4.15}$$

Ker sta $N(\alpha)$ in $N(\beta)$ celi števili, je zgornja enakost lahko izpolnjena samo v primeru, ko je $N(\alpha) = \pm 1$. □

Iskanje enot v kolobarju $\mathbb{Z}[\sqrt{d}]$ je torej ekvivalentno iskanju celoštevilskih rešitev enačb $x^2 - dy^2 = \pm 1$. V tem poglavju se bomo ukvarjali z enačbo $x^2 - dy^2 = 1$, ki ji pravimo tudi *Pellova enačba*.

Predpostavimo sedaj, da je naš $d > 0$ fiksno kvadratov prosto celo število. Za realno število t označimo neceli del števila s $\{t\}$.

Lema 4.26. *Naj bo $d > 1$ kvadratov prosto celo število. Potem obstaja neskončno mnogo parov pozitivnih celih števil p in q, za katere je $gcd(p, q) = 1$ in $|q\sqrt{d} - p| < \frac{1}{q}$.*

Dokaz. Naj bo $Q > 1$ celo število. Razdelimo interval $[0, 1)$ na Q podintervalov. Ti podintervali so:

$$\left[0, \frac{1}{Q}\right), \left[\frac{1}{Q}, \frac{2}{Q}\right), \ldots.$$

Vzemimo še $Q + 1$ števil:

$$0, \{\sqrt{d}\}, \{2\sqrt{d}\}, \ldots, \{Q\sqrt{d}\}.$$

Imamo torej $Q + 1$ števil in Q intervalov in po Dirichletovem principu, ki smo ga uporabili že v poglavju 3.4.1, morata vsaj dve števili ležati v istem intervalu. Iz tega sledi, da morata obstajati celi števili q_1 in q_2, tako da je $0 \leq q_1 < q_2 \leq Q$ in da velja:

$$\left|\{q_2\sqrt{d}\} - \{q_1\sqrt{d}\}\right| < \frac{1}{Q}.$$

Ker imamo neceli del števila, morata obstajati celi števili p_1 in p_2, za kateri je:

$$\left|q_2\sqrt{d} - p_2 - q_1\sqrt{d} + p_1\right| = \left|(q_2 - q_1)\sqrt{d} - (p_2 - p_1)\right| < \frac{1}{Q}.$$

Označimo sedaj $q = q_2 - q_1$ in $p = p_2 - p_1$. Opazimo, da je $Q \geq q > 0$, ter da je

$$|q\sqrt{d} - p| < \frac{1}{Q} \leq \frac{1}{q}.$$

Če slučajno p ni pozitivno število, potem dobimo $\frac{1}{2} \geq \frac{1}{Q} > |q\sqrt{d} - p| \geq q\sqrt{d} \geq \sqrt{d} \geq 1$, kar pa je seveda protislovje. Torej sta števili p in q res obe pozitivni.
Naj bo sedaj d največji skupni delitelj števil p in q. Zapišemo lahko $p = dp_1$ in $q = dq_1$ za neki pozitivni celi števili p_1 in q_1. Če neenačbo $|q\sqrt{d} - p| < \frac{1}{q}$ delimo z d, dobimo:

$$|q_1\sqrt{d} - p_1| < \frac{1}{qd} \leq \frac{1}{q_1},$$

torej lahko predpostavimo tudi, da sta števili p in q tuji.
Preostane nam torej samo še pokazati, da je takih parov števil p in q neskončno mnogo. Zgoraj smo pokazali, kako lahko za fiksno pozitivno celo število $Q > 1$ poiščemo tuji pozitivni celi števili p in q, za kateri velja:

$$|q\sqrt{d} - p| < \frac{1}{Q} \leq \frac{1}{q}.$$

Ker število $\sqrt{d}$ ni racionalno, je število $|q\sqrt{d}-p|$ vedno pozitivno. Izberimo si sedaj pozitivno celo število Q_1 tako, da bo $\frac{1}{Q_1} < |q\sqrt{d}-p|$. Po zgoraj opisanem postopku lahko poiščemo tuji pozitivni števili p_1 in q_1, za kateri velja:

$$|q_1\sqrt{d}-p_1| < \frac{1}{Q_1} \leq \frac{1}{q_1}.$$

Ker pa je bil Q_1 izbran tako, da je $\frac{1}{Q_1} < |q\sqrt{d}-p|$, par (p_1, q_1) ni enak paru (p, q). S tem smo zaključili dokaz leme. □

To lemo je prvi dokazal Dirichlet in je osnova za teorijo diofantskih približkov. To je področje teorije števil, ki se ukvarja s tem, kako dobro lahko aproksimiramo iracionalno število z racionalnimi števili.

Izrek 4.27. *Če je $d > 1$ kvadratov prosto celo število, potem ima enačba $x^2 - dy^2 = 1$ neskončno mnogo rešitev $(x, y) \in \mathbb{Z}$.*

Dokaz. Uporabili bomo lemo 4.26. Vzemimo $p, q > 0$ in naj bo:

$$|q\sqrt{d}-p| < \frac{1}{q}. \tag{4.16}$$

Potem je:

$$p - \frac{1}{q} < q\sqrt{d} < p + \frac{1}{q},$$

iz česar sledi:

$$q\sqrt{d} + p < 2q\sqrt{d} + \frac{1}{q}. \tag{4.17}$$

Če pomnožimo neenačbi (4.16) in (4.17), dobimo:

$$|p^2 - dq^2| < 2\sqrt{d} + \frac{1}{q^2} < 2\sqrt{d} + 1. \tag{4.18}$$

Želeli bi pokazati, da je leva stran neenačbe (4.18) enaka 1 za neskončno mnogo parov (p, q). Opazimo, da je desna stran neenačbe (4.18) neodvisna od števil p in q. Sledi, da mora obstajati tak $e \in \mathbb{Z}$, da je $1 \leq e < 2\sqrt{d} + 1$, ter da za neskončno mnogo parov p in q velja, da je:

$$|p^2 - dq^2| = e. \tag{4.19}$$

Zakaj e ne more biti 0? Če je $p^2 - dq^2 = 0$, potem je $\sqrt{d} = \frac{p}{q}$, kar pa ni mogoče, ker je d kvadratov prosto število in je zato $\sqrt{d}$ iracionalno število.
Ker obstaja neskončno mnogo parov (p, q), ki rešijo enačbo (4.19), obstaja tudi neskončno mnogo parov (p, q) in (p_1, q_1), ki rešijo enačbo (4.19), poleg tega pa še velja, da je $p \equiv p_1 \ (mod\ e)$ in $q \equiv q_1 \ (mod\ e)$. Torej velja:

$$pp_1 - dqq_1 \equiv p^2 - dq^2 \equiv 0 \ (mod\ e) \quad \text{in} \quad pq_1 - qp_1 \equiv 0 \ (mod\ e).$$

Zato obstajata celi števili x_0 in y_0, za kateri velja:

$$pp_1 - dqq_1 = x_0 e \quad \text{in} \quad pq_1 - qp_1 = y_0 e. \tag{4.20}$$

Potem je:

$$\begin{aligned} x_0^2 - dy_0^2 &= \left(\frac{pp_1 - dqq_1}{e}\right)^2 - d\left(\frac{pq_1 - qp_1}{e}\right)^2 \\ &= \frac{1}{e^2}(p^2(p_1^2 - dq_1^2) - dq^2(p_1^2 - dq_1^2)) \\ &= \frac{1}{e}(p^2 - dq^2) \\ &= 1. \end{aligned}$$

Torej sta števili x_0, y_0 res rešitev naše enačbe. Ker pa imamo neskončno mnogo možnosti izbire para (p_1, q_1), na tak način dobimo neskončno mnogo rešitev enačbe $x^2 - dy^2 = 1$. □

Primer 4.28. Vzemimo $d = 3$. Opazimo, da je $(p, q) = (3, 2)$ ena od rešitev neenačbe (4.16), za katero je $|p^2 - 3q^2| = 3$. Tudi $(p_1, q_1) = (45, 26)$ je rešitev neenačbe (4.16), za katero je $|p_1^2 - 3q_1^2| = 3$. Poleg tega je $p \equiv p_1 \ (mod\ 3)$ in $q \equiv q_1 \ (mod\ 3)$. Definirajmo sedaj celi števili x_0, y_0 na enak način kot v enačbah (4.20):

$$x_0 = \frac{3 \cdot 45 - 3 \cdot 2 \cdot 26}{3} = -7 \quad \text{in} \quad y_0 = \frac{3 \cdot 26 - 2 \cdot 45}{3} = -4.$$

Par $(x_0, y_o) = (-7, -4)$ je res rešitev enačbe $x^2 - 3y^2 = 1$.

Opazimo, da je tudi par $(p_2, q_2) = (627, 362)$ rešitev neenačbe (4.16), za katero je $|p_2^2 - 3q_2^2| = 3$. Velja, da je $p \equiv p_2 \ (mod\ 3)$ in $q \equiv q_2 \ (mod\ 3)$. Če definiramo celi števili x_1, y_1 na enak način kot v enačbah (4.20), dobimo:

$$x_1 = \frac{3 \cdot 627 - 3 \cdot 2 \cdot 362}{3} = -97 \quad \text{in} \quad y_1 = \frac{3 \cdot 362 - 2 \cdot 627}{3} = -56.$$

Par $(x_1, y_1) = (-97, -56)$ je res rešitev enačbe $x^2 - 3y^2 = 1$.

Primer 4.29. Vzemimo $d = 5$. Opazimo, da je $(p, q) = (4, 2)$ ena od rešitev neenačbe (4.16), za katero je $|p^2 - 5q^2| = 4$. Tudi $(p_1, q_1) = (76, 34)$ je rešitev neenačbe (4.16), za katero je $|p_1^2 - 5q_1^2| = 4$. Poleg tega je $p \equiv p_1 \ (mod\ 4)$ in $q \equiv q_1 \ (mod\ 4)$. Definirajmo celi števili x_0, y_0 na enak način kot v enačbah (4.20):

$$x_0 = \frac{4 \cdot 76 - 5 \cdot 2 \cdot 34}{4} = -9 \quad \text{in} \quad y_0 = \frac{4 \cdot 34 - 2 \cdot 76}{4} = -4.$$

Par $(x_0, y_o) = (-9, -4)$ je res rešitev enačbe $x^2 - 5y^2 = 1$.

Izrek 4.27 nam pove, da ima enačba $x^2 - dy^2 = 1$ neskončno mnogo rešitev. Bralec si lahko v članku [18, str. 2] prebere, kako te rešitve poiščemo.

4.5 KVADRATNE FORME

Vzemimo diofantsko enačbo

$$ax^2 + bxy + cy^2 = n, \tag{4.21}$$

za katero iščemo celoštevilsko rešitev (x, y) za dane $a, b, c, n \in \mathbb{Z}$.
Diskriminanta Δ kvadratne forme $ax^2 + bxy + cy^2$ je definirana kot: $\Delta = b^2 - 4ac$. Podobno kot pri Pitagorovi enačbi lahko tudi tukaj problem razdelimo na tri podprobleme.

1. Če je $gcd(a, b, c) = d > 1$, potem mora d deliti tudi n in enačbo (4.21) lahko zapišemo kot:
$$\left(\frac{a}{d}\right)x^2 + \left(\frac{b}{d}\right)xy + \left(\frac{c}{d}\right)y^2 = \left(\frac{n}{d}\right),$$
torej lahko brez škode za splošnost privzamemo, da je $gcd(a, b, c) = 1$.

2. Če je $gcd(x, y) = e > 1$, potem mora e^2 deliti tudi n in enačbo (4.21) lahko zapišemo kot:
$$a\left(\frac{x}{e}\right)^2 + b\left(\frac{x}{e}\right)\left(\frac{y}{e}\right) + c\left(\frac{y}{e}\right)^2 = \left(\frac{n}{e^2}\right),$$
iz česar lahko brez škode za splošnost privzamemo, da sta x in y tuji števili. Rešitve (x, y) z $gcd(x, y) = 1$ so primitivne rešitve.

3. Če je diskriminanta Δ kvadrat, potem ima enačba $at^2 + bt + c = 0$ racionalne rešitve, ki jih lahko zapišemo kot $\frac{u_1}{v_1}$ in $\frac{u_2}{v_2}$, kjer sta v_1 in v_2 pozitivna. Enačbo $at^2 + bt + c = 0$ lahko v ničelni obliki zapišemo kot $a(t - \frac{u_1}{v_1})(t - \frac{u_2}{v_2}) = 0$. Podobno lahko enačbo (4.21) v ničelni obliki zapišemo kot $a(x - \frac{u_1}{v_1}y)(x - \frac{u_2}{v_2}y) = n$. Če sedaj ničelno obliko te enačbe pomnožimo z v_1v_2 na obeh straneh, dobimo:

$$a(v_1x - u_1y)(v_2x - u_2y) = nv_1v_2.$$

To enačbo lahko smatramo kot par linearnih enačb. Namreč, za vsak celoštevilski par (r, s), kjer je $ars = nv_1v_2$, rešimo enačbi:

$$v_1x - u_1y = r,$$
$$v_2x - u_2y = s.$$

Celoštevilske rešitve teh dveh enačb (v kolikor obstajajo), rešijo enačbo (4.21).

V nadaljevanju si bomo pogledali diofantsko enačbo (4.21), za katero Δ ni kvadrat. V ta namen enačbi (4.21) priredimo parameter ρ takole:

$$\rho = \frac{1 - (-1)^b}{2}. \tag{4.22}$$

Opazimo, da je ρ enak 0, ko je b sodo število in enak 1, ko je b liho število. Naj bo sedaj b sodo število. Potem je b^2 deljiv s 4 in je zato $\frac{\Delta-\rho}{4} = \frac{\Delta}{4}$ celo število. Če pa je b liho število, potem je b^2 kongruenten 1 po modulu 4 in je zato $b^2 - 1$ deljiv s 4. Posledično je $\frac{\Delta-\rho}{4} = \frac{\Delta-1}{4}$ zopet celo število.

Izrek 4.30. *(Lagrange) Naj bo Δ ne-kvadratno celo število. Potem obstaja kvadratna forma $ax^2 + bxy + cy^2$ z diskriminanto Δ, ki ima primitivno rešitev za enačbo*

$$ax^2 + bxy + cy^2 = n$$

natanko tedaj, ko ima kongruenca

$$z^2 + \rho z - \left(\frac{\Delta - \rho}{4}\right) \equiv 0 \ (mod\ n) \tag{4.23}$$

rešitev z. Pri tem je ρ definiran tako kot v enačbi (4.22).

Dokaz. Predpostavimo, da je (α, γ) primitivna celoštevilska rešitev enačbe (4.21). Po lemi 2.16 obstajata taki celi števili β in δ, da velja: $\alpha\delta - \beta\gamma = 1$.
Naj bo:

$$\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \cdot \begin{bmatrix} X \\ Y \end{bmatrix}. \tag{4.24}$$

Opazimo, da je $\det \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} = \alpha\delta - \beta\gamma = 1$, zato je to obrnljiva matrika (po lemi 2.28).
Izrazimo sedaj enačbo (4.21) s spremenljivkama X in Y. Dobimo:

$$\begin{aligned} n &= a(\alpha X + \beta Y)^2 + b(\alpha X + \beta Y)(\gamma X + \delta Y) + c(\gamma X + \delta Y)^2 \\ &= X^2(a\alpha^2 + b\alpha\gamma + c\gamma^2) + XY(2a\alpha\beta + b(\alpha\delta + \beta\gamma) + 2c\gamma\delta) + Y^2(a\beta^2 + b\beta\delta + c\delta^2) \\ &= nX^2 + (2r + \rho)XY + sY^2. \end{aligned}$$

Pri tem je $s = a\beta^2 + b\beta\delta + c\delta^2$ in $2r + \rho = 2a\alpha\beta + 2c\gamma\delta + b(\alpha\delta + \beta\gamma)$.
Velja, da je s celo število. Opazimo, da je $\alpha\delta + \beta\gamma = 1 + 2\beta\gamma$ liho število, torej je $b(\alpha\delta + \beta\gamma) - \rho$ sodo število in sledi, da je tudi število $r = a\alpha\beta + c\gamma\delta + \frac{1}{2}(b(\alpha\delta + \beta\gamma) - \rho)$ celo število.
Enačba

$$n = nX^2 + (2r + \rho)XY + sY^2 \tag{4.25}$$

ima rešitev $X = 1$, $Y = 0$, ki ustreza

$$\begin{bmatrix} \alpha \\ \gamma \end{bmatrix} = \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 0 \end{bmatrix}.$$

Diskriminanta enačbe (4.25) je

$$\Delta = (2r + \rho)^2 - 4sn, \tag{4.26}$$

iz česar zaradi $\rho^2 = \rho$ sledi, da je:

$$r^2 + \rho r - \left(\frac{\Delta - \rho}{4}\right) = sn \equiv 0 \ (mod\ n).$$

Torej je r celoštevilska rešitev kongruence (4.23).
Izrek 4.30 moramo sedaj dokazati še v drugo smer. Predpostavimo, da je r rešitev kongruence (4.23). Če rešimo enačbo (4.26), dobimo celo število s in zato celoštevilsko rešitev enačbe (4.25), $X = 1$ in $Y = 0$.
Če sedaj to prevedemo nazaj na spremenljivki x in y z uporabo

$$\begin{bmatrix} X \\ Y \end{bmatrix} = \begin{bmatrix} \gamma & \delta \\ -\beta & \alpha \end{bmatrix} \cdot \begin{bmatrix} x \\ y \end{bmatrix},$$

dobimo celoštevilsko rešitev enačbe $nx^2 + (2r + \rho)xy + sy^2 = n$, ki ima diksriminanto Δ. □

Primer 4.31. Naj bo $a = 1,\ b = 0,\ c = 5$ in $n = 7$. Torej je:

$$\rho = 0 \quad \text{in} \quad \Delta = b^2 - 4ac = 0 - 20 = -20.$$

Izrek 4.30 nam pove, da obstaja kvadratna forma za število 7, z diskriminanto -20, natanko tedaj, ko ima kongruenca

$$z^2 + 5 \equiv 0 \ (mod\ 7) \tag{4.27}$$

rešitev. Opazimo, da je $z = 3$ rešitev enačbe (4.27).
Dokaz izreka 4.30 nam da formo:

$$7x^2 + 6xy + 2y^2. \tag{4.28}$$

Vidimo, da enačba (4.28) predstavlja število 7, ko je $x = 1$ in $y = 0$.

5 ZAKLJUČEK

Glavni cilj magistrskega dela je bil predstaviti diofantske enačbe in za nekatere od njih poiskati tudi rešitve. Ukvarjala sem se predvsem s kvadratnimi diofantskimi enačbami.

V začetku poglavja 3 sem predstavila Fundamentalni izrek aritmetike, ki ima pomembno vlogo pri reševanju diofantskih enačb. Z uporabo Fundamentalnega izreka aritmetike sem izpeljala rešitve diofantske enačbe $x^2 + y^2 = z^2$, ki jo imenujemo Pitagorova enačba.
V nadaljevanju sem predstavila še Fundamentalni izrek aritmetike v drugih kontekstih, ki nas pripelje do rešitev manj znanih diofantskih enačb. Podala sem odgovor na vprašanje, katera praštevila ter katera naravna števila lahko zapišemo kot vsoto dveh kvadratov. Reševanje tega problema je namreč ekvivalentno reševanju diofantske enačbe $n = x^2 + y^2$. Za naravno število n sem problem razširila še na vsoto treh kvadratov, pokazala pa sem tudi, da se lahko vsako pozitivno celo število zapiše kot vsota kvadratov štirih celih števil.
Na koncu tega poglavja sem se dotaknila še diofantskih enačb višjega reda in predstavila tri slavne diofantske probleme, ki so svojo rešitev dobili šele pred kratkim.

V poglavju 4 sem s pomočjo Legendrovega simbola zapisala Eulerjev kriterij. Ta kriterij nam pove, ali je neko celo število kvadratni ostanek po modulu p. Veliko problemov iz področja kvadratnih kongruenc namreč lahko prevedemo na reševanje najenostavnejše kvadratne kongruence, tj. $x^2 \equiv a \ (mod\ p)$, kjer je a kvadratni ostanek. Zapisala sem še Kvadratni recipročnosti zakon, ki nam omogoča hitro računanje Legendrovega simbola.
V nadaljevanju sem predstavila Pellovo enačbo $x^2 - dy^2 = 1$ in pokazala sem, da ima ta enačba neskončno mnogo celoštevilskih rešitev za $d > 1$ kvadratov prosto celo število.
Na koncu tega poglavja sem pogledala še reševanje enačbe $ax^2 + bxy + cy^2 = n$. Definirala sem diskriminanto $\Delta = b^2 - 4ac$ in reševanje enačbe ločila na dva primera. V primeru, ko je Δ kvadrat, sem reševanje enačbe prevedla na reševanje dveh linearnih enačb. Za primer, ko Δ ni kvadrat, pa sem zapisala izrek, ki nam pove, kdaj lahko tako enačbo rešimo s pomočjo kvadratne forme $ax^2 + bxy + cy^2$.

6 LITERATURA IN VIRI

[1] J. A. Al-Bar, *A short Note Disscusing The Set $\mathbb{Z}_n$ under addition and multiplication mod n*, https://www.kau.edu.sa/Files/0003550/Files/61821_note1foraalgebra.pdf. (Datum ogleda: 1. 2. 2021.) *(Citirano na strani 9.)*

[2] N. C. Ankeny, *Sums of three squares*, https://www.ams.org/journals/proc/1957-008-02/S0002-9939-1957-0085275-8/S0002-9939-1957-0085275-8.pdf. (Datum ogleda: 3. 2. 2021.) *(Citirano na strani 21.)*

[3] J. Bhaskar, *Sum of two squares*, https://www.math.uchicago.edu/~may/VIGRE/VIGRE2008/REUPapers/Bhaskar.pdf. (Datum ogleda: 3. 2. 2021.) *(Citirano na straneh 20 in 21.)*

[4] *Brahmagupta*, https://sl.wikipedia.org/wiki/Brahmagupta. (Datum ogleda: 22. 3. 2021.) *(Ni citirano.)*

[5] *Division transitivity*, https://proofwiki.org/wiki/Divisor_Relation_is_Transitive. (Datum ogleda: 19. 5. 2020.) *(Citirano na strani 14.)*

[6] G. Everest in T. Ward, *An introduction to number theory*. Springer-Verlag, 2005. *(Citirano na straneh 1 in 25.)*

[7] *Fermatov veliki izrek*, https://sl.wikipedia.org/wiki/Fermatov_veliki_izrek. (Datum ogleda: 31. 3. 2021.) *(Ni citirano.)*

[8] *Field*, http://www.math.lsa.umich.edu/~jchw/2015Math110Material/FieldAxioms-Math110-W2015.pdf. (Datum ogleda: 11. 8. 2020.) *(Citirano na strani 12.)*

[9] *Field's characteristic*, https://en.wikipedia.org/wiki/Characteristic_(algebra). (Datum ogleda: 26. 10. 2020.) *(Citirano na strani 12.)*

[10] M. Glavan, *Diedrska simetrija*, http://pefprints.pef.uni-lj.si/4687/1/Diploma_MarkoGlavan.pdf. (Datum ogleda: 11. 8. 2020.) *(Citirano na straneh 9 in 10.)*

[11] J. Grasselli, *Diofantske enačbe*, DMFA-založništvo, 1984. *(Citirano na strani 14.)*

[12] M. A. Khamsi, *Invertible matrices*, http://www.sosmath.com/matrix/matinv/matinv.html. (Datum ogleda: 4. 1. 2021.) *(Citirano na strani 8.)*

[13] *Kolobar*, https://sl.wikipedia.org/wiki/Kolobar_(algebra). (Datum ogleda: 20. 5. 2020.) *(Citirano na straneh 9 in 11.)*

[14] *Kolobarji, obsegi in polinomi*, https://ucilnica1314.fmf.uni-lj.si/pluginfile.php/12042/mod_resource/content/0/Kolobarji.pdf. (Datum ogleda: 1. 2. 2021.) *(Citirano na strani 12.)*

[15] T. Košir, *Algebraične strukture*, https://www.fmf.uni-lj.si/~kosir/poucevanje/skripta/strukture.pdf. (Datum ogleda: 22. 7. 2020.) *(Citirano na straneh 9 in 11.)*

[16] T. Košir, *Determinanta matrike*, https://www.fmf.uni-lj.si/~kosir/poucevanje/skripta/determinante.pdf. (Datum ogleda: 4. 1. 2021.) *(Citirano na strani 8.)*

[17] *Legendre three square theorem*, https://gaurish4math.wordpress.com/tag/legendre-three-square-theorem/. (Datum ogleda: 5. 2. 2021.) *(Citirano na strani 21.)*

[18] H.W. Lenstra, Solving the Pell equation. *MSRI Publications* 44 (2008) 1–23. *(Citirano na strani 45.)*

[19] S. Meece, C. Rakes, A. Zerhusen, *Diophantine Equations*, http://www.ms.uky.edu/~carl/ma330/projects/diophanfin.html. (Datum ogleda: 22. 3. 2021.) *(Ni citirano.)*

[20] *Multiplicative group*, https://en.wikipedia.org/wiki/Multiplicative_group. (Datum ogleda: 11. 8. 2020.) *(Citirano na strani 12.)*

[21] M. Polajnar, *Algebra*, https://www.fmf.uni-lj.si/~skreko/Pouk/ds2/Zapiski/Polajnar-DS2-3.pdf. (Datum ogleda: 11. 8. 2020.) *(Citirano na strani 10.)*

[22] *Polgrupa*, https://sl.wikipedia.org/wiki/Polgrupa. (Datum ogleda: 22. 7. 2020.) *(Citirano na strani 9.)*

[23] *Squarefree integer*, https://mathworld.wolfram.com/Squarefree.html. (Datum ogleda: 10. 11. 2020.) *(Citirano na strani 41.)*

[24] *Sum of two squares theorem*, https://en.wikipedia.org/wiki/Sum_of_two_squares_theorem. (Datum ogleda: 5. 2. 2021.) *(Citirano na strani 21.)*

[25] P. Thangarajah, *MATH 2150: Higher Arithmetic*, Mount Royal University, 2017. *(Citirano na strani 3.)*