O PREDSTAVITVI VSEH PRAŠTEVIL S CELOŠTEVILSKIMI KVADRATNIMI FORMAMI DVEH SPREMENLJIVK

MARJAN JENKO[1] IN MARKO PETKOVŠEK[2]

[1]Fakulteta za gradbeništvo in geodezijo, Univerza v Ljubljani
[2]Fakulteta za matematiko in fiziko, Univerza v Ljubljani

Math. Subj. Class. (2010): 11–01, 11A41, 11E25

V članku pokažemo, da unija zalog vrednosti celoštevilskih kvadratnih form $x^2 + y^2$, $2x^2 + y^2$ in $2x^2 - y^2$ vsebuje vsa praštevila ...

ON REPRESENTATION OF ALL PRIMES BY INTEGRAL BINARY QUADRATIC FORMS

We show that the union of ranges of the integral binary quadratic forms $x^2 + y^2$, $2x^2 + y^2$, and $2x^2 - y^2$ contains all primes ...

Uvod

Vsem matematikom je dobro znan

Izrek 1. *Praštevilo p lahko zapišemo v obliki $x^2 + y^2$, kjer sta $x, y \in \mathbb{Z}$, če in samo če p pri deljenju s 4 daje ostanek 1 ali če je $p = 2$.*

Nekaj zgledov:

$2 = 1 + 1 = 1^2 + 1^2 \surd$

$3 = 1 + 2$ *ne gre*, saj število 2 ni popoln kvadrat

$5 = 1 + 4 = 1^2 + 2^2 \surd$

$7 = 1 + 6 = 2 + 5 = 3 + 4$ *ne gre*, saj nobeno od števil $6, 2, 3$ ni popoln kvadrat

Izraz $x^2 + y^2$ je poseben primer *celoštevilske kvadratne forme dveh spremenljivk*, tj. izraza $F(x, y) = ax^2 + bxy + cy^2$, kjer so a, b in c cela števila. Kvadratna forma $F(x, y)$ nam bo hkrati predstavljala tudi pripadajočo preslikavo oziroma funkcijo dveh spremenljivk $F\colon \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$, ki paru celih števil (x, y) priredi vrednost $F(x, y)$. Pri dani kvadratni formi F pa nas bo zanimalo, katera praštevila pripadajo njeni zalogi vrednosti $F(\mathbb{Z} \times \mathbb{Z})$.

Osnovno vprašanje članka: *Ali obstaja taka* ***končna množica*** *celoštevilskih kvadratnih form dveh spremenljivk, da unija njihovih zalog vrednosti vsebuje vsa praštevila?*

V naslednjem razdelku bomo na elementaren način pokazali, da je odgovor na to vprašanje pozitiven.

Predstavitev vseh praštevil

Naj bo $\mathbb{N} = \{1, 2, 3, \dots\}$ množica naravnih števil in p liho praštevilo.

Definicija 2. Število $a \in \mathbb{Z}$ je *kvadrat* po modulu p, če obstaja tako število $b \in \mathbb{Z}$, da je $a \equiv b^2 \pmod{p}$.

Število 0 je kvadrat po vsakem modulu, saj je $0 \equiv 0^2 \pmod{p}$ za vse p. Odslej se pri določanju kvadratne narave celega števila po izbranem praštevilskem modulu p omejimo na števila $a \not\equiv 0 \pmod{p}$. Izkaže se, da je pri tem ugodno uporabljati *Legendrov simbol* $\left(\frac{a}{p}\right)$, katerega vrednost je definirana takole:

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{če je } a \text{ kvadrat po modulu } p, \\ -1, & \text{če } a \text{ ni kvadrat po modulu } p. \end{cases}$$

Po viru [6] povzemamo naslednje rezultate.

Izrek 3. *Naj bosta a in b celi števili, tuji lihemu praštevilu p. Potem velja:*

(i) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ [6, str. 127, izrek 86.(c)]

(ii) $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$ [6, str. 127, izrek 86.(e)]

(iii) $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$ [6, str. 131, izrek 89]

Trditev 4. *Naj bosta $a \in \mathbb{Z}$ ter $p \in \mathbb{N} \setminus \{1\}$ tuji števili. Potem obstajata naravni števili $x, y \in \{1, 2, \dots, \lfloor\sqrt{p}\rfloor\}$, za kateri velja:*

$$ax \equiv y \pmod{p} \quad \textit{ali} \quad ax \equiv -y \pmod{p}. \tag{1}$$

Dokaz: Naj bo $P = \{(x, y);\ x, y \in \{0, 1, \dots, \lfloor\sqrt{p}\rfloor\}$. Število elementov množice P je $\left(\lfloor\sqrt{p}\rfloor + 1\right)^2 > \left(\sqrt{p}\right)^2 = p$, torej obstajata različna urejena para (x_1, y_1), $(x_2, y_2) \in P$, za katera je $ax_1 - y_1 \equiv ax_2 - y_2 \pmod{p}$ oziroma

$$a(x_1 - x_2) \equiv y_1 - y_2 \pmod{p}. \tag{2}$$

Iz $y_1 = y_2$ bi zaradi (2) sledilo $a(x_1 - x_2) \equiv 0 \pmod{p}$, od tod pa zaradi tujosti a in p še $x_1 \equiv x_2 \pmod{p}$ in končno $x_1 = x_2$, saj x_1, x_2 pripadata

množici $\{0, 1, \ldots, \lfloor\sqrt{p}\rfloor\}$, ki ima zaradi $p \geq 2$ kvečjemu p elementov. To pa ni mogoče, saj $(x_1, y_1) \neq (x_2, y_2)$. Iz $x_1 = x_2$ pa bi zaradi (2) sledilo $y_1 \equiv y_2 \pmod{p}$ in od tod $y_1 = y_2$, kar spet ni mogoče. Torej za $x = |x_1 - x_2|$, $y = |y_1 - y_2|$ velja: $x, y \in \{1, 2, \ldots, \lfloor\sqrt{p}\rfloor\}$, od tod in iz (2) pa sledi (1). ∎

Izrek 5. *Naj bo*

$$\begin{aligned} F_0(x, y) &= x^2 + y^2, \\ F_1(x, y) &= 2x^2 + y^2, \\ F_2(x, y) &= 2x^2 - y^2. \end{aligned}$$

Potem:

1. $F_0(\mathbb{Z}\times\mathbb{Z})$ *vsebuje praštevilo 2 in vsa praštevila, ki pri deljenju s 4 dajejo ostanek 1,*
2. $F_1(\mathbb{Z} \times \mathbb{Z})$ *vsebuje vsa praštevila, ki pri deljenju z 8 dajejo ostanek 3,*
3. $F_2(\mathbb{Z} \times \mathbb{Z})$ *vsebuje vsa praštevila, ki pri deljenju z 8 dajejo ostanek 7,*
4. $F_0(\mathbb{Z} \times \mathbb{Z}) \cup F_1(\mathbb{Z} \times \mathbb{Z}) \cup F_2(\mathbb{Z} \times \mathbb{Z})$ *vsebuje vsa praštevila.*

Dokaz:

1. Očitno je $F_0(1, 1) = 1 + 1 = 2$, torej $F_0(\mathbb{Z} \times \mathbb{Z})$ vsebuje praštevilo 2. Naj bo zdaj p praštevilo oblike $4k + 1$, kjer je $k \in \mathbb{N}$. Po izreku 3(ii) je

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = (-1)^{\frac{4k}{2}} = (-1)^{2k} = 1,$$

torej obstaja tak $a \in \mathbb{Z}$, da je $a^2 \equiv -1 \pmod{p}$. Po trditvi 4 obstajata števili $x, y \in \{1, 2, \ldots, \lfloor\sqrt{p}\rfloor\}$, za kateri je $ax \equiv \pm y \pmod{p}$. Potem je $a^2x^2 \equiv y^2 \pmod{p}$ in $a^2x^2 \equiv -x^2 \pmod{p}$, torej $y^2 \equiv -x^2 \pmod{p}$ oziroma $x^2+y^2 \equiv 0 \pmod{p}$, kar pomeni, da je $x^2 + y^2 = tp$ za neki $t \in \mathbb{N}$. Iz $1 \leq x, y \leq \lfloor\sqrt{p}\rfloor$ sledi $1 \leq x^2, y^2 \leq \lfloor\sqrt{p}\rfloor^2 < p$, od tod pa $tp = x^2 + y^2 < 2p$ in zato $1 \leq t < 2$, torej $t = 1$ in $p = x^2 + y^2$. Zaključimo, da $F_0(\mathbb{Z} \times \mathbb{Z})$ vsebuje tudi vsa praštevila oblike $4k + 1$.

2. Naj bo p praštevilo oblike $8k + 3$, kjer je $k \in \mathbb{N}$. Po izreku 3(ii) je

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = (-1)^{\frac{8k+2}{2}} = (-1)^{4k+1} = -1,$$

po izreku 3(iii) pa prav tako

$$\begin{aligned} \left(\frac{2}{p}\right) &= (-1)^{\frac{p^2-1}{8}} = (-1)^{\frac{(8k+3)^2-1}{8}} = (-1)^{\frac{64k^2+48k+8}{8}} \\ &= (-1)^{8k^2+6k+1} = -1. \end{aligned}$$

Po izreku 3(i) je torej

$$\left(\tfrac{-2}{p}\right) \;=\; \left(\tfrac{-1}{p}\right)\left(\tfrac{2}{p}\right) \;=\; (-1)^2 \;=\; 1,$$

zato obstaja $a \in \mathbb{Z}$, za katerega je $a^2 \equiv -2 \pmod{p}$. Po trditvi 4 obstajata taka $x, y \in \{1, 2, \ldots, \lfloor\sqrt{p}\rfloor\}$, da je $ax \equiv \pm y \pmod{p}$. Potem je $a^2x^2 \equiv y^2 \pmod{p}$ in $a^2x^2 \equiv -2x^2 \pmod{p}$, torej $y^2 \equiv -2x^2 \pmod{p}$ oziroma $2x^2 + y^2 \equiv 0 \pmod{p}$, kar pomeni, da je $2x^2 + y^2 = tp$ za neki $t \in \mathbb{N}$. Kot zgoraj velja $1 \le x^2, y^2 < p$, zato je $tp = 2x^2 + y^2 < 3p$ in torej $t \in \{1, 2\}$. To pomeni, da praštevilo p dobimo kot vrednost celoštevilske kvadratne forme $2x^2 + y^2$ ali kot vrednost kvadratne forme $x^2 + \frac{y^2}{2}$ z racionalnimi koeficienti. A če je $x^2 + \frac{y^2}{2} = p$, mora biti y sodo število, torej $y = 2z$ za neki $z \in \mathbb{Z}$ in je $p = x^2 + \frac{4z^2}{2} = x^2 + 2z^2$. To pa pomeni, da dobimo praštevilo p tudi kot vrednost forme $2x^2 + y^2$ in torej forme $x^2 + \frac{y^2}{2}$ ne potrebujemo. Zaključimo, da $F_1(\mathbb{Z} \times \mathbb{Z})$ vsebuje vsa praštevila oblike $8k + 3$.

3. Naj bo p praštevilo oblike $8k + 7$, kjer je $k \in \mathbb{N}$. Po izreku 3(iii) je

$$\begin{aligned}\left(\tfrac{2}{p}\right) \;&=\; (-1)^{\frac{p^2-1}{8}} \;=\; (-1)^{\frac{(8k+7)^2-1}{8}} \;=\; (-1)^{\frac{64k^2+112k+48}{8}} \\ &=\; (-1)^{8k^2+14k+6} \;=\; 1,\end{aligned}$$

torej obstaja $a \in \mathbb{Z}$, za katerega je $a^2 \equiv 2 \pmod{p}$. Po trditvi 4 obstajata taka $x, y \in \{1, 2, \ldots, \lfloor\sqrt{p}\rfloor\}$, da je $ax \equiv \pm y \pmod{p}$. Potem je $a^2x^2 \equiv y^2 \pmod{p}$ in $a^2x^2 \equiv 2x^2 \pmod{p}$, torej $y^2 \equiv 2x^2 \pmod{p}$, kar pomeni, da je $2x^2 - y^2 = tp$ za neki $t \in \mathbb{Z}$. Kot zgoraj velja $1 \le x^2, y^2 < p$, zato je $2 - p < 2x^2 - y^2 = tp < 2p - 1$ in torej $t \in \{0, 1\}$. Iz $t = 0$ bi sledilo $y^2 = 2x^2$, torej $\frac{y}{x} = \pm\sqrt{2}$. A to ne gre, saj je leva stran zadnje enačbe racionalna, desna pa ne. Sledi $t = 1$ in $p = 2x^2 - y^2$. Zaključimo, da $F_2(\mathbb{Z} \times \mathbb{Z})$ vsebuje vsa praštevila oblike $8k + 7$.

4. Praštevila oblike $4k + 3$ pri deljenju z 8 dajejo ostanek 3 ali 7, torej množica $F_1(\mathbb{Z} \times \mathbb{Z}) \cup F_2(\mathbb{Z} \times \mathbb{Z})$ vsebuje vsa praštevila oblike $4k + 3$. Ker $F_0(\mathbb{Z} \times \mathbb{Z})$ vsebuje praštevilo 2 in vsa praštevila oblike $4k + 1$, množica $F_0(\mathbb{Z} \times \mathbb{Z}) \cup F_1(\mathbb{Z} \times \mathbb{Z}) \cup F_2(\mathbb{Z} \times \mathbb{Z})$ vsebuje vsa praštevila. ∎

S tremi kvadratnimi formami $x^2 + y^2$, $2x^2 + y^2$ in $2x^2 - y^2$ lahko torej predstavimo vsa praštevila, s čimer smo pozitivno odgovorili na osnovno vprašanje iz uvoda.

Dodatno vprašanje: *Ali lahko predstavimo vsa praštevila že z dvema kvadratnima formama dveh spremenljivk? Ali morda celo z eno sámo?*

Drugi del gornjega vprašanja ni nesmiseln, saj je Lagrange leta 1770 dokazal *izrek štirih kvadratov*, ki pravi, da vsako naravno število, in torej

tudi vsako praštevilo, pripada zalogi vrednosti celoštevilske kvadratne forme štirih spremenljivk $L(x_1, x_2, x_3, x_4) = x_1^2 + x_2^2 + x_3^2 + x_4^2$.

Nekaj zgodovinskih opomb in napotkov na dodatne vire

Teorija števil sodi skupaj z geometrijo med najstarejša področja matematike. Fragment babilonske glinene tablice iz časa pribl. 1800 pred Kristusom, imenovane *Plimpton 322*, vsebuje 15 pitagorejskih trojic. Evklid iz Aleksandrije (deloval okrog leta 300 pred Kristusom) je dokazal, da je praštevil neskončno mnogo, po Diofantu (prav tako iz Aleksandrije, živel v 3. stoletju po Kristusu) pa so poimenovane diofantske enačbe in diofantska aproksimacija.

Nov razcvet je doživela teorija števil v 17. stoletju s Fermatom, Girardom, Mersennom in Pascalom. Girard je leta 1625 prvi opisal vsa naravna števila (ne nujno praštevila), ki jih lahko zapišemo v obliki vsote dveh popolnih kvadratov, Fermat pa je 25. decembra 1640 v pismu Mersennu navedel tudi število možnih zapisov potenc danega praštevila v tej obliki. To je najbrž razlog, da izrek 1 iz uvoda (omejen na liha praštevila p) včasih imenujejo *Girardov izrek* ali tudi *Fermatov (božični) izrek*. Žal niti Girard niti Fermat nista navedla dokazov svojih trditev – tako je prvi dokaz tega izreka podal šele Euler leta 1749.

Pravi »kvantni preskok« v sodobno algebraično teorijo števil pa je prinesla Gaussova knjiga *Disquisitiones Arithmeticae* iz leta 1801, v kateri je Gauss med drugim dokazal kvadratni reciprocitetni zakon za Legendrove simbole (prim. [6, str. 131, izrek 90]) in razvil teorijo celoštevilskih kvadratnih form dveh in treh spremenljivk. Kot se izkaže, je zaloga vrednosti celoštevilske kvadratne forme $F(x, y) = ax^2 + bxy + c^2$ odvisna od njene diskriminante $\Delta F = b^2 - 4ac$. Tako je npr. za kvadratne forme iz izreka 5

$$\begin{aligned} \Delta F_0 &= 0 - 4 \cdot 1 \cdot 1 = -4, \\ \Delta F_1 &= 0 - 4 \cdot 2 \cdot 1 = -8, \\ \Delta F_2 &= 0 - 4 \cdot 2 \cdot (-1) = 8, \end{aligned}$$

kar ni nepovezano z dejstvom, da je pri določanju zaloge vrednosti F_0 pomemben modul 4, pri določanju zaloge vrednosti F_1 in F_2 pa modul 8. Več o tem lahko zainteresirana bralka in bralec izvesta v virih [1] in [12]. Vir [3] pa vsebuje dokaz, da množica $G_1(\mathbb{Z}\times\mathbb{Z}) \cup G_2(\mathbb{Z}\times\mathbb{Z})$, kjer je $G_1(x, y) = x^2 + 2y^2$ in $G_2(x, y) = x^2 - 2y^2$, vsebuje vsa praštevila oblike $4k+3$. Pripomnimo, da to ni v neskladju z našim izrekom 5, iz katerega izhaja enaka trditev za množico $F_1(\mathbb{Z}\times\mathbb{Z}) \cup F_2(\mathbb{Z}\times\mathbb{Z})$, kjer je $F_1(x, y) = 2x^2 + y^2$ in $F_2(x, y) = 2x^2 - y^2$. Formi F_1 in G_1 imata očitno enako zalogo vrednosti, saj se razlikujeta le v poimenovanju spremenljivk. Enako velja tudi za formi F_2 in G_2, ki sta

ekvivalentni, tj. povezani s spremembo baze, kot pokaže naslednji račun. Forma G_2 ima pri $x = 2a + b$, $y = a + b$ enako vrednost kot forma F_2 pri $x = a$, $y = b$, saj je $(2a + b)^2 - 2(a + b)^2 = 2a^2 - b^2$, forma F_2 pa ima pri $x = a - b$, $y = 2b - a$ enako vrednost kot forma G_2 pri $x = a$, $y = b$, saj je $2(a - b)^2 - (2b - a)^2 = a^2 - 2b^2$.

Zgodovinske opombe zaključimo z nekaj podatki o teoriji števil v Sloveniji po ustanovitvi ljubljanske univerze l. 1919. Zanimivo je, da sta bila njena prva rektorja, Josip Plemelj in Rihard Zupančič, oba matematika. Profesor Plemelj je v svojih predavanjih iz algebre in teorije števil, ki so bila izdana v obliki učbenika šele mnogo kasneje [15], obdelal sodobno algebraično teorijo števil (kvadratne obsege števil, idealske module, idealske razrede in njihovo število itd.). V njegovi bibliografiji najdemo vsaj en znanstveni članek s tega področja [14]. Po drugi svetovni vojni je bil daleč največji pospeševalec in popularizator teorije števil pri nas profesor Josip Grasselli, o čemer po eni strani priča 24 člankov na to témo v reviji Presek, 9 člankov v Obzorniku za matematiko in fiziko, učbenik [7], pet knjig v knjižnici Sigma [4], [6], [8], [9], [11], monumentalna *Enciklopedija števil* na 691 straneh [10] in poročilo o raziskovalni nalogi [5], po drugi strani pa mentorstva pri kar 38 diplomskih delih in nalogah ter enem magisteriju s področja teorije števil. Da je bil velik ljubitelj teorije števil tudi profesor Ivan Vidav, pa kažejo knjige [16], [17, poglavja V, VI, X], [18] in [19]. V zadnjem času je na FMF UL teorijo števil predaval profesor Sašo Strle, ki je tudi soavtor znanstvenega članka [13] s tega področja.

O nastajanju pričujočega članka

Prvega avtorja najbolje predstavimo s sporočilom Fakultete za gradbeništvo in geodezijo UL iz leta 2020 [2].

Marjan Jenko 1928–2020

Fakulteta za gradbeništvo in geodezijo Univerze v Ljubljani z žalostjo sporoča, da je sklenil svojo življenjsko pot Marjan Jenko.

Marjan Jenko je deloval na področju geodetskih referenčnih koordinatnih sistemov. Na fakulteti je bil zaposlen kot asistent v obdobju od 1959 do 1969, kot učitelj s skrajšanim delovnim časom pa v obdobju 1973 do 1995. Leta 1983 je bil izvoljen v naziv docent. Bil je tudi nosilec več raziskovalnih nalog. Rezultati njegovih raziskav so objavljeni v obsežnih elaboratih z naslovom »Temeljne triangulacijske mreže SRS«. Kot priznani strokovnjak je imel vrsto predavanj doma in v tujini.

Pomembna dela Marjana Jenka so vodstvo računske faze geodetskih del za Coastal Belt Water Project v Libiji, v dolžini nad 1200 km, sodelovanje in strokovno mentorstvo pri geodetskih delih za karavanški predor, geodetska

opazovanja v geodinamičnih in mikro-triangulacijskih geodetskih mrežah ter izdelava več geodetskih programskih paketov. Leta 1981 je izračunal lego geometričnega središča Slovenije GEOSS.

Marjan Jenko je bil spoštovan pedagog in raziskovalec. Rezultati njegovega dela kažejo, da si je vseskozi prizadeval za razvoj in modernizacijo geodetske znanosti in stroke. Svoja znanja ter bogate praktične izkušnje je znal na zelo preprost, pa vendar znanstveni način prenašati na mlajši rod, tako na fakulteti kot širše v stroki. Za prispevek k razvoju geodezije in vzgoji kadrov mu je ob svoji 100-letnici Univerza v Ljubljani, Fakulteta za gradbeništvo in geodezijo podelila srebrno priznanje.

Prvi avtor pa ni bil le odličen geodet in pedagog, ampak tudi izvrsten rodoslovec in navdušen ljubiteljski matematik, ki je svoj prosti čas posvečal številnim projektom s teh področij. Dne 28. 2. 2018 je drugemu avtorju sporočil, da se je s svojim programabilnim elektronskim kalkulatorjem lotil generiranja praštevil s pomočjo primitivnih pitagorejskih trojic $(m^2 - n^2, 2mn, m^2 + n^2)$, saj je opazil, da je hipotenuza $m^2 + n^2$ pogosto praštevilo. Ker s formo $m^2 + n^2$ ni dobil vseh praštevil, je dodajal in preskušal še druge kvadratne polinome dveh spremenljivk. Dne 26. 4. 2018 je napisal tole:

Raziskoval sem še naprej in prišel do lepega rezultata: v množici vrednosti naslednjih 4 izrazov

$$m^2 + n^2,$$
$$m^2 + mn + n^2,$$
$$m^2 + 3mn + n^2,$$
$$2m^2 + mn + 2n^2,$$

kjer je m naravno in n celo število, nastopajo vsa praštevila od 1 do 3001.

Drugi avtor je s pomočjo programa *Mathematica* preveril, da te štiri kvadratne forme generirajo tudi vsa praštevila med 3000 in 10^6, in prvemu avtorju obljubil, da bo raziskal, ali morda na ta način dobimo sploh vsa praštevila. Lotil se je študija obsežnega vira [12], a zaradi obilice drugih dolžnosti ni prišel daleč. Po pomoč se je obrnil na zdaj tudi že pokojnega kolega dr. Marjana Jermana, ki je prijazno svetoval vir [1]. Potem pa je nastopil covid-19 in nato še druge nevšečnosti, tako da prvi avtor rešitve problema žal ni dočakal. Drugi avtor se je lahko ponovno lotil problema šele jeseni 2022. Prebral je Grassellijev dokaz izreka 98 v viru [6, str. 154–56], ki pravi, da je vsako praštevilo oblike $4k + 1$ mogoče izraziti s celoštevilsko kvadratno formo $x^2 + y^2$. Opazil je, da je s pomočjo lastnosti Legendrovega simbola mogoče na podoben način dokazati izrazljivost vsakega praštevila oblike $8k + 3$ s kvadratno formo $2x^2 + y^2$ in izrazljivost vsakega praštevila oblike $8k + 7$ s kvadratno formo $2x^2 - y^2$, kar pomeni, da je odgovor na

osnovno vprašanje tega članka pozitiven. Odprta pa ostaja (vsaj za drugega avtorja) domneva, da je mogoče vsa praštevila izraziti tudi s pomočjo kvadratnih form x^2+y^2, x^2+xy+y^2, $x^2+3xy+y^2$ in $2x^2+xy+2y^2$, do katerih je pri svojem delu prišel prvi avtor.

LITERATURA

[1] P. L. Clark, *8430 Handout 3: Elementary theory of quadratic forms*, ogled 18. 12. 2022, dostopno na `https://silo.tips/download/8430-handout-3-elementary-theory-of-quadratic-forms`, 14 str.

[2] Fakulteta za gradbeništvo in geodezijo UL, *Marjan Jenko 1928 – 2020*, ogled 4. 1. 2023, dostopno na `https://www.fgg.uni-lj.si/marjan-jenko-1928-2020/`.

[3] S. Galovich in J. Resnick, *Representing primes by binary quadratic forms*, Math. Magazine **64** (1991), 1, 34–38.

[4] J. Grasselli, *Osnove teorije števil*, Knjižnica Sigma 14, Državna založba Slovenije, Ljubljana 1966.

[5] J. Grasselli, *Adicijski izreki v teoriji grup in teoriji števil*, raziskovalno poročilo, Ljubljana 1974.

[6] J. Grasselli, *Osnove teorije števil*, 2. predelana izdaja, Knjižnica Sigma 14a, Državna založba Slovenije, Ljubljana 1975.

[7] J. Grasselli, *Algebraična števila*, zbirka Matematika, DMFA Slovenije, Ljubljana 1983.

[8] J. Grasselli, *Diofantske enačbe*, Knjižnica Sigma 38, DMFA Slovenije, Ljubljana 1984.

[9] J. Grasselli, *Diofantski približki*, Knjižnica Sigma 51, DMFA Slovenije, Ljubljana 1992.

[10] J. Grasselli, *Enciklopedija števil*, DMFA Slovenije, Ljubljana 2008.

[11] J. Grasselli, *Elementarna teorija števil*, Knjižnica Sigma 87, DMFA Slovenije, Ljubljana 2009.

[12] A. Hatcher, *Topology of Numbers*, ogled 18. 12. 2022, dostopno na `https://pi.math.cornell.edu/~hatcher/TN/TNpage.html`, 348 str.

[13] B. Owens in S. Strle, *A characterization of the $\mathbb{Z}^n \oplus \mathbb{Z}(\delta)$ lattice and definite nonunimodular intersection forms*, Amer. J. Math., **134** (2012), 4, 891–913.

[14] J. Plemelj, *Die Unlösbarkeit von $x^5+y^5+z^5=0$ im Körper $k\sqrt{5}$*, Monatsh. Math. Phys. **23** (1912), 1, 305–308.

[15] J. Plemelj, *Algebra in teorija števil*, Slovenska akademija znanosti in umetnosti, Ljubljana 1962.

[16] I. Vidav, *Rešeni in nerešeni problemi matematike*, Knjižnica Sigma 1, Mladinska knjiga, Ljubljana 1959.

[17] I. Vidav, *Algebra*, zbirka Matematika, Mladinska knjiga, Ljubljana 1972.

[18] I. Vidav, *Teorija števil in elementarna geometrija: izbor člankov*, Knjižnica Sigma 62, DMFA Slovenije, Ljubljana 1996.

[19] I. Vidav, *O deljenju z ostankom in še čem*, DMFA – založništvo, Ljubljana 2016.