VSOTA ŠTIRIH KVADRATOV IN WARINGOV PROBLEM
(SEMINAR)

NIK GLOBOČNIK

Povzetek. V tem članku bomo spoznali Lagrangeov izrek, ki pravi, da je mogoče vsako naravno število zapisati kot vsoto štirih kvadratov celih števil. Ogledali si bomo še enega od njegovih posplošitvev; Waringov problem.

1. Uvod

Zapis naravnega števila kot vsoto kvadratov, kubov, četrtih in višjih potenc celih števil, so že dolgo problemi matematičnih raziskovalcev. Izkaže se, da je to možno storiti s konstantnim številom sumandov za vsako potenco posebej. Domneva štirih kvadratov se je pojavila še Diofantovi *Aritmetiki*, leta 1770 pa jo je dokazal Lagrange. Od takrat naprej se ta domneva imenuje *Lagrangeov izrek štirih kvadratov* (povzeto po [1]). Kasneje pa so se pojavile še mnoge posplošitve Lagrangeovega izreka, kot je Waringov problem.

Dokaz Lagrangeovega izreka bo natančneje predstavljen v 3. poglavju, Waringov problem pa v 4. poglavju.

Članek je povzet po [3] in [4].

2. Uvodna izreka

Oglejmo si najprej dva izreka, ki sta podobna izreku o štirih kvadratih. Govorita o tem, kdaj lahko naravno število zapišemo kot vsoto dveh kvadratov ali pa kot vsoto treh kvadratov.

Poskusimo sedaj poiskati zapis naravnega števila kot vsoto dvek kvadratov celih števil.

$$\begin{aligned} 1 &= 1^2 + 0^2 \\ 2 &= 1^2 + 1^2 \\ 3 &= ? \\ 4 &= 2^2 + 0^2 \\ 5 &= 2^2 + 1^2 \\ 6 &= ? \\ 7 &= ? \end{aligned}$$

V tem poskusu ne opazimo nekega očitnega zaporedja, zato si poglejmo, kdaj lahko *praštevilo* zapišemo kot vsoto dveh kvadratov. Praštevila bomo razdelili glede na ostanek pri deljenju s 4. Dobimo:

$p = 2$	$p \equiv 1 \pmod 4$	$p \equiv 3 \pmod 4$
$2 = 1^2 + 1^2$	$5 = 2^2 + 1^2$	$3 = ?$
	$13 = 3^2 + 2^2$	$7 = ?$
	$17 = 4^2 + 1^2$	$11 = ?$
	$29 = 5^2 + 2^2$	$19 = ?$
	$\vdots$	$\vdots$

Od tu lahko sklepamo, da lahko liho praštevilo zapišemo kot vsoto dveh kvadratov celih števil natanko tedaj, ko daje ostanek 1 pri deljenju s 4. Po podobnem razmisleku za poljubmo naravno število n dobimo naslednji izrek.

Izrek 2.1 (Fermat)**.** *Naravno število n lahko zapišemo kot vsoto dveh kvadratov celih števil natanko tedaj, ko ima vsak prafaktor p števila n, ki zadošča $p \equiv 3 \pmod 4$, v praštevilskem razcepu sod eksponent.*

Izrek, ki pove, kdaj je naravno število vstota treh kvadratov celih števil bomo samo navedli.

Izrek 2.2 (Legendre)**.** *Naravno število n lahko zapišemo kot vsoto treh kvadratov celih števil natanko tedaj, ko n ni oblike $4k(8\ell + 7)$, za neki nenegativni celi števili k in ℓ.*

3. Lagrangeov izrek

V tem poglavju bomo spoznali glaven izrek našega članka. Preden pa se lotimo njegove formulacije in dokaza pa si poglejmo lemo, ki nam bo pomagala pri njegovem dokazu.

Lema 3.1. *Naj bo p liho praštevilo. Potem obstajajo cela števila x, y in m, da je*

$$1 + x^2 + y^2 = mp, \quad 0 < m < p.$$

Primer 3.2. Za $p = 3$ imamo $1+1^2+2^2 = 2\cdot 3$, za $p = 7$ pa imamo $1+2^2+4^4 = 3\cdot 7$.

Dokaz. Za $x \in \left\{0, 1, \ldots, \frac{p-1}{2}\right\}$ imajo števila x^2 same različne ostanke pri deljenju s p. Če bi za različna x_1 in x_2 veljalo $x_1^2 \equiv x_2^2 \pmod p$, bi to pomenilo, da p deli $(x_1 + x_2)(x_1 - x_2)$. Torej bi imeli $x_1 \equiv \pm x_2 \pmod p$, kar pa je protislovje. Podobno za $y \in \left\{0, 1, \ldots, \frac{p-1}{2}\right\}$ sklepamo, da dajo števila $-1 - y^2$ različne ostanke pri deljenju s p.

V zgornjih dveh množicah imamo natanko $p + 1$ števil, a le p možnih ostankov pri deljenju v p. Zato morata po *načelu golobnjaka* obstajati taki števili x in y, da data x^2 in $-1 - y^2$ isti ostanek pri deljenju z p. Imamo torej

$$x^2 \equiv -1 - y^2 \pmod p.$$

Od tod sledi, da je

$$1 + x^2 + y^2 \equiv 0 \pmod p.$$

Zato mora obstajati naravno število m, da je

$$1 + x^2 + y^2 = mp.$$

Da dobimo oceno za število m, ocenimo $x^2 < \left(\frac{p}{2}\right)^2$ in $y^2 < \left(\frac{p}{2}\right)^2$. Zato imamo

$$mp = 1 + x^2 + y^2 < 1 + 2 \cdot \left(\frac{p}{2}\right)^2 < p^2.$$

Torej res dobimo oceno $m < p$. □

Že v prvem poglavju smo videli, da vsakega naravnega števila ni možno zapisati kot vsote dveh ali treh kvadratov celih števil. Naslednji izrek, ki govori o vsoti štirih kvadratov celih števil, bo hkrati tudi glavni izrek v tem članku.

Izrek 3.3 (Lagrange)**.** *Vsako naravno število lahko zapišemo kot vsoto štirih kvadratov celih števil.*

Primer 3.4. Vidimo, da je $5 = 2^2 + 1^2 + 0^2 + 0^2$, $21 = 4^2 + 2^2 + 1^1 + 0^2$ in $127 = 11^2 + 2^2 + 1^2 + 1^2$.

Dokaz. Pri dokazu si bomo pomagali s t. i. *Eulerjevo identiteto*:

$$\begin{aligned}(x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2) = \\ (x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4)^2 \\ + (x_1y_2 - x_2y_1 + x_3y_4 - x_4y_3)^2 \\ + (x_1y_3 - x_3y_1 + x_4y_2 - x_2y_4)^2 \\ + (x_1y_4 - x_4y_1 + x_2y_3 - x_3y_2)^2.\end{aligned}$$

Vidimo, da je produkt števil, ki sta vstoti štirih kvadratov, tudi vsota štirih kvadratov celih števil. Za število 1 je izrek trivialen. Ker pa vemo, da je mogoče vsako naravno število, ki je večje od 1, zapisati kot produkt praštevil, iz *Eulerjeve identitete* sledi, da je dovolj izrek dokazati zgolj za praštevila.

Za $p = 2$ imamo $2 = 1^2 + 1^2 + 0^2 + 0^2$. Recimo sedaj, da je praštevilo p liho. Iz prej dokazane leme 3.1 pa sledi, da obstaja tako naravno število m, $0 < m < p$, da je

$$mp = x_1^2 + x_2^2 + x_3^2 + x_4^2.$$

Dokazali bomo, da je najmanjši tak m kar $m = 1$. Označimo z m_0 najmanjši tak m, da je

$$mp = x_1^2 + x_2^2 + x_3^2 + x_4^2.$$

Če je $m_0 = 1$ smo končali z dokazom. Predpostavimo sedaj, da je $1 < m_0 < p$.

Recimo, da je m_0 sod. Torej morajo biti vsi x_i, $i \in \{1, 2, 3, 4\}$, sodi oz. lihi ali pa sta dva od njih soda in dva liha. Predpostavimo lahko, da sta x_1 in x_2 soda. Potem, so v vsakem od zgornjih primerih števila $x_1 \pm x_2$ in $x_3 \pm x_4$ soda. Zato lahko zapišemo

$$\frac{m_0}{2}p = \left(\frac{x_1 + x_2}{2}\right)^2 + \left(\frac{x_1 - x_2}{2}\right)^2 + \left(\frac{x_3 + x_4}{2}\right)^2 + \left(\frac{x_3 - x_4}{2}\right)^2,$$

kar je v protislovju z minimalnostjo m_0.

Izberimo sedaj tako celo število y_i, da velja

$$y_i \equiv x_i \pmod{m_0}, \quad |y_i| < \frac{m_0}{2}$$

za $i \in \{1, 2, 3, 4\}$. To lahko storimo, saj je $\{y \mid -\frac{m_0-1}{2} \leqslant y \leqslant \frac{m_0-1}{2}\}$ popoln sistem ostankov modulo m_0. Opazimo, da ne morajo biti vsi x_i deljivi z m_0, saj bi potem imeli $m_0^2 \mid m_0p$ in od tod $m_0 \mid p$, kar pa je protislovje. Zato imamo

$$y_1^2 + y_2^2 + y_3^2 + y_4^2 > 0$$

in

$$y_1^2 + y_2^2 + y_3^2 + y_4^2 < m_0^2 \text{ ter } y_1^2 + y_2^2 + y_3^2 + y_4^2 \equiv 0 \pmod{m_0}.$$

Iz zgornjih (ne)enakosti sledi

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 = m_0p \ (m_0 < p)$$

in

$$y_1^2 + y_2^2 + y_3^2 + y_4^2 = m_0 m_1,$$

za nek m_1, $0 < m_1 < m_0$. Če sedaj pomnožimo zadnji dve enakosti dobimo

$$m_1 m_0^2 p = z_1^2 + z_2^2 + z_3^2 + z_4^4,$$

kjer so z_i primerni členi iz *Eulerjeve identitete*. Oglejmo si sedaj število $z_1 = x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4$:

$$z_1 = x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4 \equiv x_1^2 + x_2^2 + x_3^2 + x_4^2 \equiv 0 \pmod{m_0}.$$

Torej je $z_1 \equiv 0 \pmod{m_0}$, podobno pa pokažemo, še za ostala števila z_i. Cela števila z_i so zato deljiva z m_0, zatorej je

$$z_i = m_0 w_i,$$

za primerna cela števila w_i. Če enakost

$$m_1 m_0^2 p = z_1^2 + z_2^2 + z_3^2 + z_4^2$$

sedaj delimo z m_0^2 dobimo

$$m_1 p = w_1^2 + w_2^2 + w_3^2 + w_4^2,$$

kar pa je spet protislovje z minimalnostjo m_0.

Zato je $m_0 = 1$. □

Omenimo samo še, da je mogoče izračunati število vseh celoštevilskih rešitev enačbe

$$n = x_1^2 + x_2^2 + x_3^2 + x_4^2,$$

za $n \in \mathbb{N}$. Formulo nam da naslednji izrek.

Izrek 3.5 (Jacobi, [2])**.** *Označimo z $r_4(n)$ število celoštevilskih rešitev enačbe*

$$n = x_1^2 + x_2^2 + x_3^2 + x_4^2.$$

Imamo

$$r_4(n) = 8 \sum_{\substack{d|n \\ 4\nmid d}} d.$$

Pri preštevanju rešitev ta izrek upošteva tudi vrstni red števil x_i.

4. Waringov problem

Leta 1770 je britanski matematik Edward Waring v svojem delu *Meditationes algebraicae* predstavil posplošitev Lagrangeovega izreka o štirih kvadratih. Izrek, ki da ganes poznamo kot Hilbert-Waringov izrek pa je leta 1909 dokazal nemški matematik David Hilbert. Izrek bomo spoznali kasneje v poglavju.

Za naravno število n si sedaj oglejmo enačbo

$$n = x_i^k + x_2^k + \ldots + x_s^k,$$

za $x_i \in \mathbb{N}_0$ in $k \geqslant 2$. Če fiksiramo k in je število sumandov s premajhno, smo že videli, da enačba nima rešitve za vsak $n \in \mathbb{N}$. Zanimalo nas bo ali se da za dan k najti tak s, ki je odvisen od k, da ima zgornja enačba rešitev. Recimo sedaj, da obstaja tak s, da ima zgornja enačba za fiksen k vedno rešitev. Zato ima rešitev tudi za vsako večje število $s' > s$. Od tod sklepamo, da mora obstajati najmanjše tako število s. Povzemimo to v naslednji definiciji.

Definicija 4.1. Naj bo $k \geqslant 2$. Število $g = g(k)$ je najmanjše naravno število, za katero je mogoče vsako naravno število zapisati kot vsoto g k-tih potenc nenegativnih celih števil.

Primer 4.2. Poskušajmo zapisati število 454 kot vsoto kvadratov, kubov, četrtih in petih potenc. Dobimo

$$\begin{aligned} 454 &= 3^2 + 11^2 + 18^2 \\ &= 1^3 + 1^3 + 1^3 + 3^3 + 3^3 + 3^3 + 3^3 + 7^3 \\ &= 1^4 + 2^4 + 2^4 + 2^4 + 3^4 + 3^4 + 3^4 + 3^4 + 3^4 \\ &= 1^5 + 1^5 + 1^5 + 1^5 + 1^5 + 1^5 + 2^5 + 2^5 + 2^5 + 2^5 + 2^5 \\ &\quad + 2^5 + 2^5 + 2^5 + 2^5 + 2^5 + 2^5 + 2^5 + 2^5 + 2^5 \end{aligned}$$

Opazimo, da potrebujemo vsaj tri kvadrate, vsaj osem kvadratov, vsaj devet četrtih in vsaj dvajset petih potenc. Sklepamo lahko, da je $g(2) \geqslant 3$, $g(3) \geqslant 8$, $g(4) \geqslant 9$ in $g(5) \geqslant 20$.

Sedaj se porodijo vprašanja, ali je število $g(k)$ končno za vsak $k \geqslant 2$, ali je število $g(k)$ omejeno in če obstaja kakšna eksplicitna formula za $g(k)$. Pritrdilen odgovor na prvi dve vprašannji bo dal naslednji izrek. Eksplicitnih mej pa spodnji izrek ne da, saj je njegov dokaz eksistenčen.

Izrek 4.3 (Hilbert-Waringov izrek)**.** *Za vsa naravna števila $n \geqslant 2$ obstaja tako končno število $g = g(k)$, da je možno n zapisati kot vsoto najmanj g k-tih potenc nenegativnih celih števil.*

Opomba 4.4. Dokazali smo že, da je $g(2) = 4$. Waring pa je izjavil, da se da vsako naravno število zapisati še kot vsoto devetih kubov, ter vsoto 19 četrtih potenc.

V naslednjih izrekih pa bomo poskušali najti meje za število $g(k)$.

Izrek 4.5 (Liouville)**.** $g(4)$ *obstaja in je* $\leqslant 53$.

Dokaz. Označimo z B_s število, ki je vsota s četrtih potenc. Velja identiteta

$$\begin{aligned} 6(a^2 + b^2 + c^2 + d^2)^2 &= (a+b)^4 + (a-b)^4 + (c+d)^4 + (c-d)^4 \\ &\quad + (a+c)^4 + (a-c)^4 + (b+d)^4 + (b-d)^4 \\ &\quad + (a+d)^4 + (a-d)^4 + (b+c)^4 + (b-c)^4. \end{aligned}$$

Od tod je $6(a^2 + b^2 + c^2 + d^2)^2 = B_{12}$. Sedaj iz Lagrangeovega izreka o štirih kvadratih sledi

$$6x^2 = B_{12},$$

za vsak $x \in \mathbb{N}$. Vemo že, da je vsako naravno število n oblike $6t + r$ za $0 \leqslant r \leqslant 5$. Če še enkrat uporabimo izrek o štirih kvadratih na številu t dobimo

$$n = 6(x_1^2 + x_2^2 + x_3^2 + x_4^2) + r.$$

Torej je

$$n = B_{12} + B_{12} + B_{12} + B_{12} + r \leqslant B_{53},$$

saj lahko r zapišemo kot vstot največ petih četrtih potenc ($r = 1^4+1^4+1^4+1^4+1^4$). Zato $g(4)$ obstaja in je največ 53. □

Kmalu po tem ko je Waring leta 1772 postavil svojo domnevo, je Euler predstavil svojo oceno za $g(k)$ in jo dokazal na zelo spreten način.

Izrek 4.6 (Eulerjeva ocena)**.** *Za $k \geqslant 2$ je*

$$g(k) \geqslant \left\lfloor \left(\frac{3}{2}\right)^k \right\rfloor + 2^k - 2.$$

Dokaz. Označimo $q := \left\lfloor \left(\frac{3}{2}\right)^k \right\rfloor$. Oglejmo si število

$$n = 2^k q - 1 < 3^k.$$

Od tod sledi, da lahko le s seštevanjem potenc 1^k in 2^k pridemo do števila n. Da minimiziramo število potrebnih sumandov, uporabimo karseda veliko potenc 2^k. Najmanjše število sumandov je dano v

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

Zato za število n potrebujemo najmanj $q + 2^k - 2$ sumandov. Torej je

$$g(k) \geqslant q + 2^k - 2.$$

□

Opomba 4.7. Ne potrebujejo pa vsa naravna števila, za svoj zapis, natanko $g(k)$ k-tih potenc naravnih števil. Vemo že, da je $g(3) = 9$, vendar le števili 23 in 239 potrebujeta devet kubov, samo petnajst števil potrebuje osem kubov in smao 121 števil potrebuje sedem kubov. Ostala jih potrebujejo manj, kar je preveril Jacobi do števila 12 000. Linnik pa je dokazal, da za dovolj veliko naravno število potrebujemo sedem ali manj kubov.

Kasneje pa se je pojavil še tako imenovani *Idealni Waringov problem*, ki da eksplicitno formulo za izračun števila $g(k)$.

Izrek 4.8 (Idealni Waringov problem)**.** *Označimo $q := \left\lfloor \left(\frac{3}{2}\right)^k \right\rfloor$ in $p := \left\lfloor \left(\frac{4}{3}\right)^k \right\rfloor$. Za $k \geqslant 2$ je*

$$g(k) = \begin{cases} q + 2^k - 2, & \text{če } 2^k \left(\left(\frac{3}{2}\right)^k - q \right) + q \leqslant 2^k, \\ 2^k + p + q - \theta, & \text{sicer}, \end{cases}$$

kjer je

$$\theta := \begin{cases} 2, & \text{če } pq + p + q = 2^k, \\ 3, & \text{če } pq + p + q > 2^k. \end{cases}$$

Kuniba in Wunderich sta dokazala da prvi pogoj iz zgornjega izreka velja za $k \leqslant 471\,600\,000$. Leta 1957 pa je Mahler dokazal, da je v zgornjem izreku največ končno mnogo izjem, če sploh so. Zato je mogoče sklepati, da je Eulerjeva ocena za število $g(k)$ kar njegova natančna vrednost.

Za dokaz Idealnega Waringovega problema, bi bilo dovolj pokazati neenakost

$$\left(\frac{3}{2}\right)^k - \left\lfloor \left(\frac{3}{2}\right)^k \right\rfloor \leqslant 1 - \left(\frac{3}{4}\right)^k,$$

za vsako naravno število $k \geqslant 2$. Najbližje dokazu je leta 2009 prišel Pupyrev, ki je dokazal neenakost

$$\left(\frac{3}{2}\right)^k - \left\lfloor \left(\frac{3}{2}\right)^k \right\rfloor \leqslant 1 - a^k,$$

kjer je $a = 0,5795$, za $k \geqslant 871\,387\,440\,264$.

Nazadnje se posvetimo še enemu številu, ki je povezano v Waringovim problemom. To število veliko bolj temeljno, kot število $g(k)$, o njem pa vemo veliko manj kot o $g(k)$. Oglejmo si njegovo definicijo.

Definicija 4.9. Naj bo $k \geqslant 2$. Število $G = G(k)$ je najmanjše naravno število, za katero je mogoče vsako *dovolj veliko* naravno število zapisati kot vsoto G k-tih potenc nenegativnih celih števil.

Besedno zvezo *dovolj veliko naravno število* v definiciji lahko interpretiramo tudi kot *vsako naravno število z končno mnogo izjemami*. Iz definicije očitno sledi, da je

$$G(k) \leqslant g(k), \tag{$\triangle$}$$

za vsak $k \geqslant 2$. Oglejmo si še primer za $k = 2$. Že v prvem poglavju smo povedali, da vsakega naravnega števila ni mogoče zapisati kot vsote dveh ozirima treh kvadratov naravnih (celih) števil, vemo pa že, da je $g(2) = 4$. Torej nam preostane le še $G(2) = 4$. Število $G(k)$ je določeno le še za $k = 4$ in je $G(4) = 16$.

Za druge k imamo na voljo le ocene. Zgornjo mejo za $G(k)$ že imamo v neenakosti $\triangle$, čeprav se izkaže, da je ta ocena precej nenatančna. Spodnji izrek nam pa bo dal še oceno za spodnjo mejo števila $G(k)$.

Izrek 4.10. *Za $k \geqslant 2$ je*

$$G(k) \geqslant k + 1.$$

Dokaz. Glej [3] izrek 8. □

Seveda pa obstajajo tudi natančnejše zgornje meje za število $G(k)$. Ena od ocen je

$$G(k) < ck \log k,$$

za neko konstanto c. Trenutno najboljša ocena za velike k pa je

$$G(k) \leqslant k \left(\log k + \log \log k + 2 + \mathcal{O}\left(\frac{\log \log k}{\log k} \right) \right).$$

Za konec si oglejmo še tabelo, v kateri so predstavljena števila $g(k)$ in $G(k)$ za $k \geqslant 2$, oziroma ocene za njih.

k	$g(k)$	$G(k)$
2	4	4
3	9	$\leqslant 7$
4	19	16
5	37	$\leqslant 17$
6	73	$\leqslant 24$
7	143	$\leqslant 31$
8	279	$\leqslant 39$
9	548	$\leqslant 47$
10	1079	$\leqslant 55$
11	2132	$\leqslant 63$
12	4223	$\leqslant 72$
13	8384	$\leqslant 81$
14	16673	$\leqslant 90$

5. Zaključek

Lagrangeov izrek o štirih kvadratoh in Waringov problem sta zanana izreka iz področja teorije števil. Predvsem Hilbert-Waringov izrekje eden tistih matematičnih izrekov, ki je formuliran zelo preprosto, a se takoj, ko se vanj poglobimo, pokaže, da je v svoji osnovi zelo zahteven.

V moderni teoriji števil se pojavljajo mnoge posplošitve Waringovega problema na kolobarje polinomov in matrik. Prav tako, pa se pojavlja v povezavi z Goldbachovo domnevo v Waring-Goldbachovem izreku, ki pravi, da za vsako naravno število k obstaja tako končno število g, da je vsako dovolj veliko naravno število vsota največ g k-tih potenc praštevil.

Literatura

[1] A. N. Arslan, *A variant of Waring's problem*, Notes on Number Theory and Discrete Mathematics **21**(3) (2015) 22–26.

[2] *Jacobi's four-square theorem*, [ogled 1. 5. 2020], dostopno na `https://en.wikipedia.org/wiki/Jacobi%27s_four-square_theorem`.

[3] M. M. Lalín, *Every Positive Integer is the Sum of Four Squares! (and other exciting problems)*, 2002, [ogled 16. 4. 2020], dostopno na `https://dms.umontreal.ca/~mlalin/Lagrange.pdf`.

[4] J. Soumalainen, *Waring's problem*, magistsko delo, Faculty of Science, Department of Mathematics and Statistics, University of Helsinki, 2016, [ogled 7. 5. 2020], dostopno na `https://helda.helsinki.fi/bitstream/handle/10138/166733/gradu.pdf?sequence=3`.