Kongruentna števila

Milan Hladnik

Moderni izzivi poučevanja matematike
4. februar 2011

Namen seminarja

Podati nekaj karakterizacij kongruentnih števil:

- s primitivnimi pitagorejskimi trikotniki
- z aritmetičnim zaporedjem kvadratov racionalnih števil
- z racionalnimi točkami na eliptični krivulji

Opisati domnevo BSD in Tunnellov izrek

Definicija

Definicija

Pozitivno racionalno število $q \in \mathbb{Q}^+$ je kongruentno število, če je ploščina racionalnega pravokotnega trikotnika:
$q = A(x,y,z) = xy/2$, kjer je $x,y,z \in \mathbb{Q}^+$ in $x^2 + y^2 = z^2$.

Zgled

(1) $x = 3$, $y = 4$, $z = 5$: $3^2 + 4^2 = 5^2$ in $A(3,4,5) = 6$
(najmanjše kongruentno število, ki pripada celoštevilskemu trikotniku, ker je tedaj ploščina vedno deljiva s 6)
(2) $x = 3/2$, $y = 20/3$, $z = 41/6$: $(3/2)^2 + (20/3)^2 = (41/6)^2$ in $A(3/2,20/3,41/6) = 5$
(najmanjše naravno kongruentno število, 1,2,3,4 niso taka)

Redukcija

Iz enega kongruentnega števila jih lahko pridelamo neskončno mnogo:
npr. iz 6 dobimo, da so kongruentna števila tudi
$24 = 4 \cdot 6 = A(6, 8, 10)$,
$3/2 = 6/4 = A(3/2, 2, 5/2)$,
$2/3 = 6/9 = A(1, 4/3, 5/3)$ itd. Nasploh velja:

Dejstvo 1. *Če je $q \in \mathbb{Q}^+$ kongruentno število, je za vsak $s \in \mathbb{Q}^+$ tudi s^2q kongruentno število*.

Res, iz $q = A(x, y, z)$, $x^2 + y^2 = z^2$, sledi $s^2q = A(sx, sy, sz)$, $(sx)^2 + (sy)^2 = (sz)^2$.

Brezkvadratna naravna števila

Dejstvo 2. *Če je $q \in \mathbb{Q}^+$, obstaja tak $s \in \mathbb{Q}^+$, da je s^2q naravno število brez kvadratnih faktorjev* (brezkvadratno naravno število).

Dokaz. Naj bo $q = a/b$, kjer sta si a in b tuji naravni števili. Pišimo $a = a_1^2 a_2$ in $b = b_1^2 b_2$, kjer sta a_2 in b_2 brezkvadratni tuji si števili. Potem za $s = b_1 b_2 / a_1$ dobimo $s^2 q = a_2 b_2$.

Zgled

$q = 24/125 = (4 \cdot 6)/25 \cdot 5) = A(2/5, 24/25, 26/25)$ je kongruentno število, $s = 25/2$, $s^2 q = 30$

SKLEP: Zadošča poiskati vsa brezkvadratna naravna kongruentna števila!

Zveza s primitivnimi pitagorejskimi trojicami

Trditev (1)

Brezkvadratno naravno število n je kongruentno število natanko takrat, ko obstaja tako naravno število s, da je $s^2 n$ ploščina primitivnega pitagorejskega trikotnika.

Dokaz. Če je n kongruentno, tj. $n = A(x,y,z)$, $x,y,z \in \mathbb{Q}^+$, $x^2 + y^2 = z^2$, naj bo s najmanjši skupni imenovalec števil x,y,z. Potem je $s^2 n = A(sx,sy,sz)$; da se pokazati, da je (sx,sy,sz) primitivna pitagorejska trojica.
Obratno, če je za $s \in \mathbb{N}$ število $s^2 n = A(x,y,z)$, kjer je (x,y,z) primitivni pitagorejski trikotnik, je $n = A(x/s, y/s, z/s)$.

ZGLED: $n = 5 = A(3/2, 20/3, 41/6)$, $s = 6$,
$s^2 n = 180 = A(9,40,41)$,
$(9,40,41)$ je primitivna pitagorejska trojica

Primitivne pitagorejske trojice

Pitagorejska trojica: (x,y,z), $x,y,z \in \mathbb{N}$, $x^2+y^2=z^2$
Primitivna: x,y,z paroma tuja si števila
generira primitivni pitagorejski trikotnik

Lastnosti:

- Ustrezni trikotnik ima najmanjšo ploščino med podobnimi celoštevilskimi trikotniki.
- Natanko eno od števil x,y je sodo (običajno vzamemo, da je to y).
- Obstajata tuji si naravni števili $a > b$, nasprotne parnosti, da je $x = a^2 - b^2$, $y = 2ab$, $z = a^2 + b^2$.
- y je deljiv s 4, x ali y s 3, x,y ali z s 5, ploščina s 6

Tabela brezkvadratnih naravnih kongruentnih števil

Metoda za iskanje kongruentnih števil:
(i) Generiramo vse primitivne pitagorejske trojice
$x = a^2 - b^2$, $y = 2ab$, $z = a^2 + b^2$, kjer so $a, b, c \in \mathbb{N}$, a, b tuji, različne parnosti, $a > b$ in jih razvrstimo v tabelo.
(ii) Za vsako trojico izračunamo ustrezno ploščino
$A = xy/2 = s^2 n$, kjer je n brez kvadratnih faktorjev. Npr.:

a	b	x	y	z	A	n
2	1	3	4	5	6	6
3	2	5	12	13	30	30
4	1	15	8	17	60	15
4	3	7	24	25	84	21
5	2	21	20	29	210	210
5	4	9	40	41	180	5

Neučinkovitost metode

Problem je, ker ne vemo, kako daleč po tabeli je treba gledati, da za konkretno brezkvadratno naravno število ugotovimo, ali je konvergentno.

Npr. Kogruentno število 6 smo našli že v prvi vrstici.

Kongruentno število $5 = A(3/2, 20/3, 41/6)$ najdemo v 6. vrstici pri $a = 5$, $b = 4$; tedaj je $x = 9$, $y = 40$, $z = 41$, $A = 180 = 6^2 \cdot 5$.

Brezkvadratno število 7 je tudi kongruentno, saj je $7 = A(35/12, 24/5, 337/60)$, v tabeli bi ga našli v 52. vrstici pri $a = 16$, $b = 9$; tedaj je $x = 175$, $y = 288$, $z = 337$, $A = 25200 = 60^2 \cdot 7$.

Število 157

Tudi število 157 je kongruentno, vendar je ploščina naslednjega racionalnega pravokotnega trikotnika (števec hipotenuze je zapisan z 48 števkami):

$$x = 411340519227716149383203/216665556937147613096 10,$$
$$y = 6803298487826435051217540/411340519227716149383203$$
in
$$z = 224403517704336969924557513090674863160948472041/$$
$$8912332268928859588025535178967163570016480830$$

Ploščina racionalnega pravokotnega trikotnika

Izrek (1)

Brezkvadratno naravno število n je kongruentno natanko takrat, ko obstajajo taka pozitivna števila $X, Y, Z \in \mathbb{Q}^+$, $X < Y < Z$, $X^2 + Y^2 = Z^2$, da je $n = XY/2$.

To je praktično definicija. Opazimo, da $X = Y$ ne pride v poštev zaradi iracionalnosti $\sqrt{2}$ in da lahko vzamemo $X < Y$. Prav tak ne more veljati $Y = Z$.

Aritmetično zaporedje

Izrek (2)

Brezkvadratno naravno število n je kongruentno natanko takrat, ko obstajajo taka pozitivna racionalna števila $u, v, w \in \mathbb{Q}^+$, da je $u^2 = w^2 + n$ in $v^2 = w^2 - n$.

Dokaz. Če določa trojica (X, Y, Z) racionalen pravokotni trikotnik s ploščino n, izberemo
$u = (X + Y)/2$, $v = (Y - X)/2$ in $w = Z/2$.
Obratno, če zadoščajo števila u, v, w zgornjim pogojem, izberemo pa $X = u - v$, $Y = u + v$ in $Z = 2w$, tako da je $XY = u^2 - v^2 = 2n$.

Racionalna točka na eliptični krivulji

Izrek (3)

Brezkvadratno naravno število n je kongruentno natanko takrat, ko leži na eliptični krivulji $E_n: y^2 = x^3 - n^2x$ vsaj ena racionalna točka (x,y) z lastnostjo $y \neq 0$.

Dokaz. Če je n kongruentno število, izberemo $x = w^2$ in $y = uvw$, kjer so u,v,w pozitivna racionalna števila iz izreka 2, in velja $y^2 = x^3 - n^2x$ ter $y > 0$.
Obratno, če je $y \neq 0$, lahko vzamemo $y > 0$; potem so za racionalno točko $(x,y) \in E_n$ števila $X = |x^2 - n^2|/y$, $Y = 2n|x|/y$ in $Z = (x^2 + n^2)/y$ stranice pravokotnega racionalnega trikotnika s ploščino $nx(x^2 - n^2)/y^2 = n$ in n je kongruentno število.

Direktna zveza med pravokotnimi trikotniki in točkami na eliptični krivulji

Trditev

Naj bo $n \in \mathbb{Q}^+$ *pozitivno racionalno število,*
$S_n = \{(a,b,c) \in \mathbb{R}^3;\ a^2+b^2=c^2,\ ab=2n\}$ *in*
$T_n = \{(x,y) \in \mathbb{R}^2;\ y^2 = x^3 - n^2x,\ y \neq 0\}$.

Obstaja bijekcija $f:\ S_n \to T_n$, *podana s predpisom:*
$x = n(a+c)/b$ *in* $y = 2n^2(a+c)/b^2$

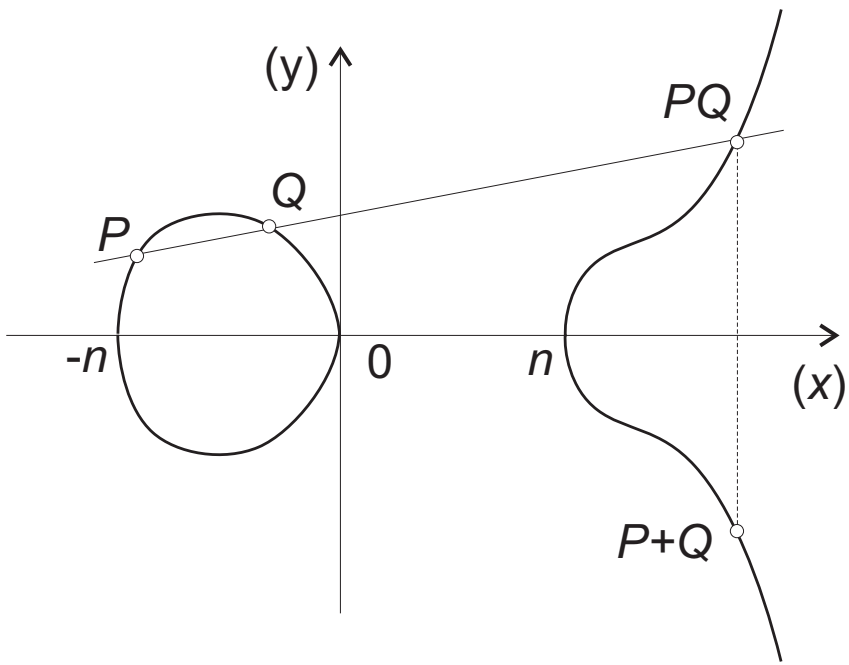
Inverzna preslikava:
$a = (x^2-n^2)/y,\ \ b = 2nx/y$ *in* $c = (x^2+n^2)/y$

Dokaz: preprosto preverjanje. Vidimo tudi
$a,b,c \in \mathbb{Q} \iff x,y \in \mathbb{Q}$ in $a,b,c \in \mathbb{Q}^+ \iff x,y \in \mathbb{Q}^+$

Abelova grupa racionalnih točk na eliptični krivulji

$E_n: \ y^2 = x^3 - n^2 x$ je poseben primer eliptične krivulje oblike $E: \ y^2 = x^3 - Ax - B$ (kjer je $4A^3 - 27B^2 \neq 0$).

Znano je, da je za vsako eliptično krivuljo množica $E(\mathbb{Q})$ vseh racionalnih točk na E Abelova grupa za operacijo seštevanja s sekantami (in tangentami).



Teorija

Mordell (1922): Grupa $E(\mathbb{Q})$ je vedno končno generirana.
Mazur (1976): torzijska grupa $E(\mathbb{Q})_{tor}$ (podgrupa elementov končnega reda) in je vedno končna (moč kvečjemu 16).

Strukturni izreku za končno generirane Abelove grupe:
$E(\mathbb{Q}) = E(\mathbb{Q})_{tor} \oplus \mathbb{Z}^r$,
kjer je r nenegativno celo število, rang grupe $E(\mathbb{Q})$ oziroma rang eliptične krivulje E.

Rang je pozitiven natanko takrat, kadar v grupi $E(\mathbb{Q})$ obstajajo tudi elementi neskončnega reda.

Torzijska grupa eliptične krivulje E_n

Za poseben primer eliptične krivulje $E_n: \ y^2 = x^3 - n^2 x$, je moč torzijske podgrupe $E_n(\mathbb{Q})_{tor}$ enaka 4 in

$$0_\infty, \ (0,0), \ (n,0) \ \text{ in } \ (-n,0)$$

so edini elementi v $E_n(\mathbb{Q})$ končnega reda.

Dokaz je malo težji.

Novi karakterizaciji

Izrek (4)

Brezkvadratno naravno število n je kongruentno natanko takrat, ko velja vsaj ena (in zato vsaka) od naslednjih trditev:

(a) Abelova grupa $E_n(\mathbb{Q})$ vseh racionalnih točk na eliptični krivulji E_n vsebuje element neskončnega reda;

(b) Eliptična krivulja E_n ima pozitiven rang.

Dokaz. Zaradi zadnje ugotovitve o torzijski grupi $E_n(\mathbb{Q})$ ima vsaka točka $(x, y) \in E_n(\mathbb{Q})$ neskončen red natanko takrat, ko je $y \neq 0$.
Natanko takrat je rang pozitiven.

Problem iskanja kongruentnih števil

Nekaj karakterizacij kongruentnih števil smo našli.
Ne poznamo pa efektivne procedure za iskanje takih števil.

Problem: *Poiskati* preprost *algoritem (test), s katerimi bi lahko za vsako (brezkvadratn) naravno število ugotovili, ali je kongruentno ali ne*.

Ta problem je (skoraj) rešil J.B. Tunnell leta 1983, ko je dokazal naslednji izrek.

Tunnellov izrek

O brezkvadratnem naravnem številu n imejmo trditve:

(A) *Število n je kongruentno*.

(B) *Število vseh rešitev diofantske enačbe $2x^2+y^2+8z^2=n$ je dvakrat večje od števila vseh rešitev diofantske enačbe $2x^2+y^2+32z^2=n$.*

(C) *Število vseh rešitev diofantske enačbe $8x^2+2y^2+16z^2=n$ je dvakrat večje od števila vseh rešitev diofantske enačbe $8x^2+2y^2+64z^2=n$.*

Naj velja šibka BSD domneva. Potem je (A) $\iff$ (B), če je n liho število, in (A) $\iff$ (C), če je n sodo število.

Brez predpostavke o veljavnosti šibke BSD domneve velja le (A) $\implies$ (B) oziroma (A) $\implies$ (C).

Dokaz Tunnellovega izreka ni lahek, izrek pa zelo uporaben.

Birch in Swinnerton-Dyerjeva domneva

V zvezi z rangom eliptične krivulje E obstaja naslednja slavna šibka BSD domneva:

Domneva

Rang eliptične krivulje E je pozitiven natanko takrat, ko za (komplicirano definirano) Hasse-Weilovo funkcijo $L(E,s)$ velja $L(E,1) = 0$.

Te domneve še niso potrdili in ostaja eden od šestih velikih še vedno nerešenih problemov sodobne matematike.

Zgled (a)

(a) *Ali je število 3 kongruentno?*

Tunnellovi enačbi za liho število 3 se glasita: $2x^2+y^2+8z^2=3$ in $2x^2+y^2+32z^2=3$. Pri obeh mora biti rešitev taka, da je $z=0$. Obe imata štiri rešitve (pri $x=\pm1$, $y=\pm1$, $z=0$):

$$(1,1,0),\ (1,-1,0),\ (-1,1,0),\ (-1,-1,0)$$

Tunnellov pogoj (B) ni izpolnjen, zato število 3 ni kongruentno.

Podobno se lahko hitro prepričamo, da tudi 1,2,4 niso kongruentna števila.

Zgled (b)

(b) *Ali je število 5 kongruentno?*

Tunnellovi enačbi $2x^2+y^2+8z^2=5$ in $2x^2+y^2+32z^2=5$ zdaj nimata celih rešitev. Spet namreč mora biti obakrat $z=0$, enačba $2x^2+y^2=5$ pa ni rešljiva, kar lahko ugotovimo s preskusom, saj je za x^2 in y^2 le končno mnogo možnosti. Tunnellov pogoj (B) je zdaj izpolnjen, prva enačba ima dvakrat več (nič) rešitev kot druga (tudi nič).

Ker pa ne vemo, ali velja šibka BSD domneva, ne moremo odtod sklepati, da je 5 kongruentno število. (V resnici je!)

Podobno spoznamo, da je pogoj (B) izpolnjen tudi za število 7 in pogoj (C) za število 6. Obe ti dve števili sta, kot vemo, kongruentni.

Kaj vemo o kongruentnih številih

Kongruentna števila do 50:

5, **6**, **7**, **13**, **14**, **15**, 20, **21**, **22**, **23**, 24, 28, **29**, **30**, **31**, 34, **37**, **38**, **39**, 41, **45**, **46**, **47**

Domneva

Če je $n \equiv 5, 6$ *ali* $7 \pmod 8$, *je n kongruentno število*

Dokazano za $p \equiv 5$ ali $7 \pmod 8$, če je p praštevilo, in za $n = 2p$, če je p praštevilo, $p \equiv 3 \pmod 8$ (Stephens 1975)

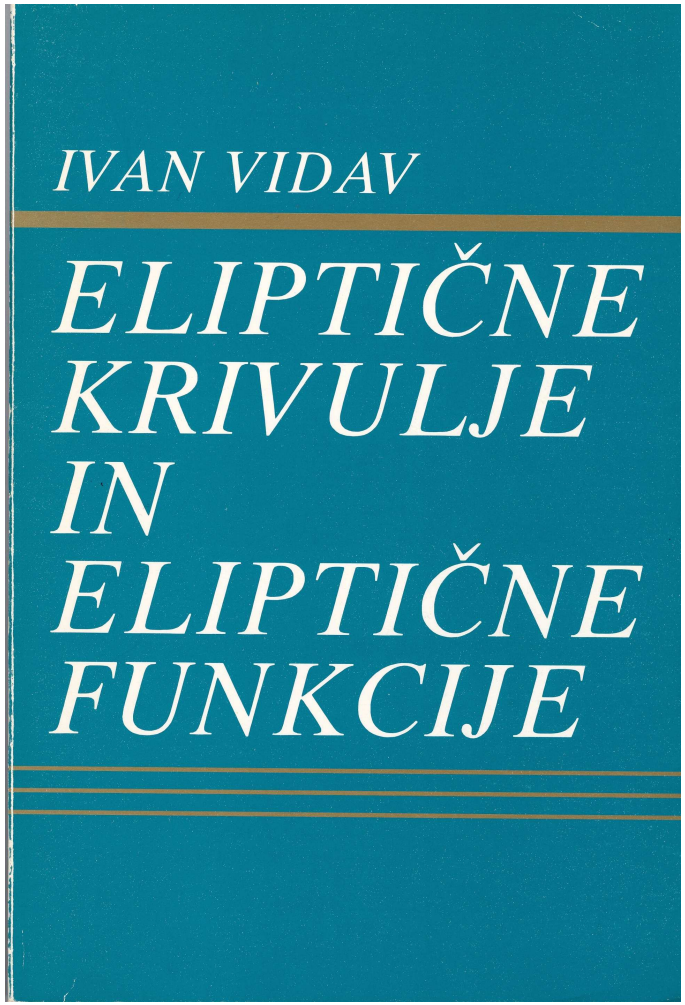
Nekongruentna števila

Za naslednja števila vemo, da niso kongruentna:

- p praštevilo, $p \equiv 3 \pmod 8$
  n je produkt dveh takih praštevil,
- $n = 2p$, p praštevilo, $p \equiv 5 \pmod 8$
  n je dvakratni produkt dveh takih praštevil, itd. (Bastien)

Za število 288 ne vemo, podobno za 482 in 543 (Guy).

Vidav, Eliptične krivulje in eliptične funkcije



Koblitz, Introduction to Elliptic Curves and Modular Forms