Kongruentna števila

Milan Hladnik

Seminar 2
4. januar 2011

Namen seminarja

Povzeti dosedanje in podati nekaj novih karakterizacij kongruentnih števil:

- Dosedanje znane karakterizacije
- Racionalne točke na eliptični krivulji
- Domneva BSD in Tunnellov izrek

Dosedanje karakterizacije

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

(1) Obstajajo taka pozitivna števila $X, Y, Z \in \mathbb{Q}$, $X < Y < Z$, $X^2 + Y^2 = Z^2$, da je $n = XY/2$;

(2) Obstajajo taka pozitivna števila $u, v, w \in \mathbb{Q}$, da je $u^2 = w^2 + n$ in $v^2 = w^2 - n$;

(3) Obstajata taki pozitivni števili $x, y \in \mathbb{Q}$, da je x kvadrat racionalnega števila, ima sodi imenovalec in števec tuj proti n, ter velja $y^2 = x^3 - n^2 x$;

(4) Na eliptični krivulji $E_n : \ y^2 = x^3 - n^2 x$ leži vsaj ena racionalna točka (x, y) z lastnostjo $y \neq 0$;

Dokaz in pojasnilo

(1) To je skoraj definicija (število n je kongruentno, če je enako ploščini racionalnega pravokotnega trikotnika); opazimo, da $X = Y$ ne pride v poštev zaradi iracionalnosti $\sqrt{2}$ in da lahko vzamemo $X < Y$.
(1) $\Longleftrightarrow$ (2) Izberemo $u = (X+Y)/2$, $v = (Y-X)/2$ in $w = Z/2$; obratno pa $X = u - v$, $Y = u + v$ in $Z = 2w$, tako da je $XY = u^2 - v^2 = 2n$.
(2) $\Longrightarrow$ (3) Izberemo $x = w^2$, $y = uvw$; izkaže se, da imata x in y iskane lastnosti (dokazali na seminarju).
(3) $\Longrightarrow$ (4) Točka (x, y) iz (3) leži na eliptični krivulji E_n in zanjo velja $y \neq 0$.
(4) $\Longrightarrow$ (1) Če je $y \neq 0$, lahko vzamemo $y > 0$; potem so za racionalno točko $(x, y) \in E_n$ števila $(x^2 - n^2)/y$, $2nx/y$ in $(x^2 + n^2)/y$ stranice pravokotnega racionalnega trikotnika s ploščino $nx(x^2 - n^2)/y^2 = n$.

Abelova grupa racionalnih točk na eliptični krivulji

Znano je, da je za vsako eliptično krivuljo $E: \ y^2 = x^3 - Ax - B$ $(4A^3 - 27B^2 \neq 0)$ množica $E(\mathbb{Q})$ vseh racionalnih točk na E Abelova grupa za operacijo seštevanja s sekantami in tangentami (pokazali na seminarju, glej tudi [6], [2], [3]).

Mordell je leta 1922 dokazal, da je ta grupa vedno končno generirana. Podmnožica vseh elementov končnega reda se imenuje *torzijska grupa* $E(\mathbb{Q})_{tor}$ in je vedno končna (Mazur je leta 1976 dokazal, da ima moč kvečjemu 16).

Celo grupo lahko potem zapišemo kot $E(\mathbb{Q}) = E(\mathbb{Q})_{tor} \oplus \mathbb{Z}^r$, kjer je r nenegativno celo število, ki ga imenujemo *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 se da pokazati, da je moč torzijske podgrupe $E_n(\mathbb{Q})_{tor}$ enaka 4 in da so

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

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

(Dokaz je malo težji, vendar v okviru obravnave v [4].)

Nove karakterizacije

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

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

(6) Eliptična krivulja E_n ima pozitiven rang.

Dokaz

(4) $\iff$ (5) Zaradi zadnje ugotovitve, ima vsaka točka $(x, y) \in E_n(\mathbb{Q})$ neskončen red natanko takrat, ko je $y \neq 0$.
(5) $\iff$ (6) Prej smo videli, da je rang pozitiven natanko takrat, ko grupa vsebuje elemente neskončnega reda.

Šibka Birch in Swinnerton-Dyerjeva domneva

V zvezi z rangom eliptične krivulje E oblike $y^2 = x^3 - Ax - B$, kjer sta A, B celi števili in je $4A^3 - 27B^2 \neq 0$, obstaja naslednja slavna domneva:

Šibka Birch in Swinnerton-Dyerjeva domneva (krajše: **šibka BSD 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 (glej npr. [1]).

Problem iskanja kongruentnih števil

Na začetku smo si zastavili vprašanje o karakterizaciji kongruentnih števil (nanj smo pravkar zadovoljivo odgovorili) in tudi vprašanje 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, posvečena mu je skoraj cela knjiga [2].

Zgled (a)

(a) Ali je število 3 kongruentno?

Tunnellovi enačbi za liho število 3 se glasita: $2x^2 + y^2 + 8z^2 = 3$ in $8x^2 + y^2 + 32z^2 = 3$. Pri obeh mora biti rešitev taka, da je $z = 0$. Obe imata štiri rešitve (pri $x = \pm 1,\ y = \pm 1,\ z = 0$):

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

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.

Literatura

- K. Devlin, *The Millenium Problems, The seven Greatest Unsolved Mathematical Puzzles of Our Time*, BAsic Books
- N. Koblitz, *Introduction to Elliptic Curves and Modular Forms*, 2nd ed., Springer-Verlag, New York, 1993.
- J.S. Milne, *Elliptic Curves*, BookSurge Publ., 2006.
- Judith D. Sally, Paul J. Sally, Jr., *Roots to Research, A vertical development of mathematical problems*, poglavje 2, AMS, 2007.
- J.H. Silverman, J. Tate, *Rational points on Ellipptic Curves*, Springer-Verlag, New York, 1992.
- I. Vidav, *Eliptične krivulje in eliptične funkcije*, DMFA Slovenije, Ljubljana 1991.