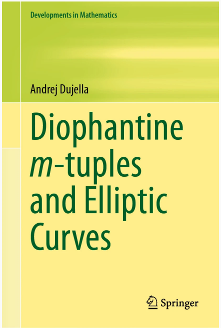
Predstavljanje knjige akademika Andreja Dujelle: Diophantine *m*-tuples and Elliptic Curves

Knjižnica HAZU
10. listopad 2024.



Pregled znanstvenog rada akademika Dujelle

- Zadatak je gotovo nemoguć za ovako kratko izlaganje, s obzirom na to da je akademik Dujella objavio čak 135 radova iz različitih područja teorije brojeva i kriptografije.
- Najviše je doprinio teoriji Diofantovih m-torki i eliptičkih krivulja.
- Autor sveučilišnog udžbenika "Teorija brojeva".
- 53 koautora
- 1772 citata (MathSciNet)
- Mentor 13 doktorskih disertacija: Borka Jadrijević, Zrinka Franušić, Alan Filipin, Bernadin Ibrahimpašić, Filip Najman , Mirela Jukić Bokun, Petra Tadić, Vinko Petričević, Tomislav Pejković, Ivan Soldo, Miljen Mikić, Sanda Bujačić

Pregled znanstvenog rada akademika Dujelle

- Zadatak je gotovo nemoguć za ovako kratko izlaganje, s obzirom na to da je akademik Dujella objavio čak 135 radova iz različitih područja teorije brojeva i kriptografije.
- Najviše je doprinio teoriji Diofantovih m-torki i eliptičkih krivulja.
- Autor sveučilišnog udžbenika "Teorija brojeva".
- 53 koautora
- 1772 citata (MathSciNet)
- Mentor 13 doktorskih disertacija: Borka Jadrijević, Zrinka Franušić, Alan Filipin, Bernadin Ibrahimpašić, Filip Najman , Mirela Jukić Bokun, Petra Tadić, Vinko Petričević, Tomislav Pejković, Ivan Soldo, Miljen Mikić, Sanda Bujačić

U ostatku izlaganja ću se fokusirati i malo dublje objasniti jedan rezultat iz teorije racionalnih Diofantovih m-torki.

Racionalne Diofantove m-torke

Racionalne Diofantova m-torka je skup od m racionalnih brojeva sa svojstvom da je umnožak bilo koja dva njegova različita elementa za jedan manji od potpunog kvadrata.

Diofant iz Aleksandrije

Figure 1: Korice izdanja iz 1621.

Diofant iz Aleksandrije


DIOPHANTI
ALEXANDRINI
ARITHMETICORVM
LIBRI SEX,
ET DE NVMERIS MVLTANGVLIS
LIBER VNVS.
Nunc primùm Græcè & Latinè editi, atque absolutissimis Commentariis illustrati.
AVCTORE CLAVDIO GASPARE BACHETO MEZIRIACO SEBVSIANO, V.C.
LVTETIAE PARISIORVM,
Sumptibus SEBASTIANI CRAMOISY, via Iacobæa, sub Ciconiis.
M. DC. XXI.
CVM PRIVILEGIO REGIS.

Figure 1: Korice izdanja iz 1621.

Diofant: $\{1/16, 33/16, 17/4, 105/16\}$

Fermat

Figure 2: Pierre de Fermat

Fermat

Figure 2: Pierre de Fermat

Fermat: $\{1, 3, 8, 120\}$

Fermat

Figure 2: Pierre de Fermat

Fermat: $$\{1, 3, 8, 120\}$$

$$1 \cdot 3 + 1 = 2^2 \quad 1 \cdot 8 + 1 = 3^2 \quad 1 \cdot 120 + 1 = 11^2$$
$$3 \cdot 8 + 1 = 5^2 \quad 3 \cdot 120 + 1 = 19^2 \quad 8 \cdot 120 + 1 = 31^2.$$

Euler

Figure 3: Leonhard Euler

Euler

Figure 3: Leonhard Euler

Euler: $\{1, 3, 8, 120, 777480/8288641\}$

Koliko veliki ti skupovi mogu biti?

Koliko veliki ti skupovi mogu biti?

Postoji beskonačno mnogo cjelobrojnih Diofantovih m-torki, npr.

$$\{k, k+2, 4k+k, 16k^3+48k^2+44k+12\}$$

Koliko veliki ti skupovi mogu biti?

Postoji beskonačno mnogo cjelobrojnih Diofantovih m-torki, npr.

$$\{k, k+2, 4k+k, 16k^3+48k^2+44k+12\}$$

Dujella(2004): Ne postoje cjelobrojne Diofantove šestorke i postoji najviše konačno mnogo cjelobrojnih Diofantovih petorki.

Koliko veliki ti skupovi mogu biti?

Postoji beskonačno mnogo cjelobrojnih Diofantovih m-torki, npr.

$$\{k, k+2, 4k+k, 16k^3+48k^2+44k+12\}$$

Dujella(2004): Ne postoje cjelobrojne Diofantove šestorke i postoji najviše konačno mnogo cjelobrojnih Diofantovih petorki.

He, Togbe, Ziegler (2018): Ne postoje cjelobrojne Diofantove petorke.

Koliko veliki ti skupovi mogu biti?

Postoji beskonačno mnogo cjelobrojnih Diofantovih m-torki, npr.

$$\{k, k+2, 4k+k, 16k^3+48k^2+44k+12\}$$

Dujella(2004): Ne postoje cjelobrojne Diofantove šestorke i postoji najviše konačno mnogo cjelobrojnih Diofantovih petorki.

He, Togbe, Ziegler (2018): Ne postoje cjelobrojne Diofantove petorke.

Gibbs (1999): prva racionalna šestorka

$$\left\{\frac{11}{192}, \frac{35}{192}, \frac{155}{27}, \frac{512}{27}, \frac{1235}{48}, \frac{180873}{16}\right\}$$

Koliko veliki ti skupovi mogu biti?

Postoji beskonačno mnogo cjelobrojnih Diofantovih m-torki, npr.

$$\{k, k+2, 4k+k, 16k^3+48k^2+44k+12\}$$

Dujella(2004): Ne postoje cjelobrojne Diofantove šestorke i postoji najviše konačno mnogo cjelobrojnih Diofantovih petorki.

He, Togbe, Ziegler (2018): Ne postoje cjelobrojne Diofantove petorke.

Gibbs (1999): prva racionalna šestorka

$$\left\{\frac{11}{192}, \frac{35}{192}, \frac{155}{27}, \frac{512}{27}, \frac{1235}{48}, \frac{180873}{16}\right\}$$

Dujella, Kazalicki, Mikić, Szikszai (2016): Postoji beskonačno mnogo racionalnih Diofantovih šestorki.

Primjer beskonačne familije

$$\{a, b, c, d, e, f\}$$

Primjer beskonačne familije

$$\{a, b, c, d, e, f\}$$

$$\begin{aligned}
a &= \frac{18t(t-1)(t+1)}{(t^2-6t+1)(t^2+6t+1)}, \\
b &= \frac{(t-1)(t^2+6t+1)^2}{6t(t+1)(t^2-6t+1)}, \\
c &= \frac{(t+1)(t^2-6t+1)^2}{6t(t-1)(t^2+6t+1)}, \\
d &= d_1/d_2, \\
e &= e_1/e_2, \\
f &= f_1/f_2.
\end{aligned}$$

Example cont'd

$$
\begin{aligned}
d_1 &= 6(t+1)(t-1)(t^2+6t+1)(t^2-6t+1)(8t^6+27t^5+24t^4-54t^3+24t^2+27t+8) \\
&\quad \times (8t^6-27t^5+24t^4+54t^3+24t^2-27t+8)(t^8+22t^6-174t^4+22t^2+1), \\
d_2 &= t(37t^{12}-885t^{10}+9735t^8-13678t^6+9735t^4-885t^2+37)^2, \\
e_1 &= -2t(4t^6-111t^4+18t^2+25)(3t^7+14t^6-42t^5+30t^4+51t^3+18t^2-12t+2) \\
&\quad \times (3t^7-14t^6-42t^5-30t^4+51t^3-18t^2-12t-2)(t^2+3t-2)(t^2-3t-2) \\
&\quad \times (2t^2+3t-1)(2t^2-3t-1)(t^2+7)(7t^2+1), \\
e_2 &= 3(t+1)(t^2-6t+1)(t-1)(t^2+6t+1) \\
&\quad \times (16t^{14}+141t^{12}-1500t^{10}+7586t^8-2724t^6+165t^4+424t^2-12)^2, \\
f_1 &= 2t(25t^6+18t^4-111t^2+4)(2t^7-12t^6+18t^5+51t^4+30t^3-42t^2+14t+3) \\
&\quad \times (2t^7+12t^6+18t^5-51t^4+30t^3+42t^2+14t-3)(2t^2+3t-1)(2t^2-3t-1) \\
&\quad \times (t^2-3t-2)(t^2+3t-2)(t^2+7)(7t^2+1), \\
f_2 &= 3(t+1)(t^2-6t+1)(t-1)(t^2+6t+1) \\
&\quad \times (12t^{14}-424t^{12}-165t^{10}+2724t^8-7586t^6+1500t^4-141t^2-16)^2.
\end{aligned}
$$

Eliptičke krivulje i Diofantove m-torke

Svakoj Diofantovoj trojci $\{a, b, c\}$ možemo pridružiti eliptičku krivulju

$$E_{abc} : y^2 = (x + ab)(x + ac)(x + bc),$$

s točkama $P = [0, abc]$ i $S = [1, \sqrt{(ab + 1)(ac + 1)(bc + 1)}]$.

Eliptičke krivulje i Diofantove m-torke

Svakoj Diofantovoj trojci $\{a, b, c\}$ možemo pridružiti eliptičku krivulju

$$E_{abc} : y^2 = (x + ab)(x + ac)(x + bc),$$

s točkama $P = [0, abc]$ i $S = [1, \sqrt{(ab+1)(ac+1)(bc+1)}]$.

Neka $T \in E_{abc}(\mathbb{Q})$. Tada je $\{a, b, c, \frac{x(T)}{abc}\}$ Diofantova četvorka ako i samo ako $T - P \in 2E_{abc}(\mathbb{Q})$.

$3S = \mathcal{O}$

Nije teško pokazati da je

$$\left\{a, b, c, \frac{x(T)}{abc}, \frac{x(T+S)}{abc}, \frac{x(T-S)}{abc}\right\}$$

skoro Diofantova m-torka, jedini uvjet koji nedostaje je $x(T-S)x(T+S) + (abc)^2 = \square$.

$3S = \mathcal{O}$

Nije teško pokazati da je

$$\left\{a, b, c, \frac{x(T)}{abc}, \frac{x(T+S)}{abc}, \frac{x(T-S)}{abc}\right\}$$

skoro Diofantova m-torka, jedini uvjet koji nedostaje je $x(T-S)x(T+S) + (abc)^2 = \square$.

Preostali uvjet će biti zadovoljen ako je $3S = \mathcal{O}$.

Pitanje

Kako opisati Diofantove trojke $\{a, b, c\}$ za koje $S \in E_{abc}$ zadovoljava $3S = \mathcal{O}$?

Parametrizacija

Takve trojke su parametrizirane racionalnim točkama na eliptičkoj krivulji

$E: y^2 = x^3 + 3(t^2 - 3t + 1)(t^2 + 3t + 1)x^2 + 3(t^2 + 1)^2(t^4 - 178t^2 + 1)x + (t^2 + 1)^2(t^4 + 110t^2 + 1)^2.$

Parametrizacija

Takve trojke su parametrizirane racionalnim točkama na eliptičkoj krivulji

$$E : y^2 = x^3 + 3(t^2 - 3t + 1)(t^2 + 3t + 1)x^2 + 3(t^2 + 1)^2(t^4 - 178t^2 + 1)x + (t^2 + 1)^2(t^4 + 110t^2 + 1)^2.$$

$P = [-(t^2 + 1)(t^2 + 18t + 1), 27t(t + 1)^2(t^2 + 1)] \in E(\mathbb{Q}(t))$ je točka beskonačnog reda, pa iz višekratnika od P dobivamo beskonačno mnogo Diofantovih trojki koje se mogu proširiti na beskonačno mnogo načina do Diofantove šestorke.