Diofantilised võrrandid

Konstantin Tretjakov

14. juuni 2003. a.

Diofantiline võrrand on võrrand kujul

$$f(x_1, x_2, \ldots, x_n) = 0 \tag{1}$$

kus $n \geq 2$. Kui f on täisarvuliste kordajatega polünoom, siis see on *algebraline diofantiline võrrand*. Diofantilise võrrandi lahendiks nimetakse selle võrrandi rahuldava *täisarvude* komplekti $(x_1^0, x_2^0, \ldots, x_n^0)$.

Elementaarsed lahendusvõtted

1. **Teguriteks lahutus.** Esitame esialgse võrrandi (1) kujul

$$f_1(x_1, x_2, \ldots, x_n) f_2(x_1, x_2, \ldots, x_n) \ldots f_k(x_1, x_2, \ldots, x_n) = a$$

kus $f_1, f_2, \ldots, f_k \in \mathbb{Z}[X_1, X_2, \ldots, X_s]$

Näiteks:

$$\begin{aligned}
&(x^2+1)(y^2+1) + 2(x-y)(1-xy) = 4(1+xy) \qquad \Leftrightarrow \\
&(xy - 1 - (x-y))^2 = 4 \qquad \Leftrightarrow \\
&(x+1)(y-1) = \pm 2
\end{aligned}$$

2. **Läbivaatus.** Näitame, et lahendid kuuluvad mingisse lõpliku hulka, ning vaatame kõik läbi.

Näiteks:

$$\begin{aligned}
&x^3 + y^3 = (x+y)^2 \qquad \Leftrightarrow \\
&x + y = 0 \quad \text{või} \quad x^2 - xy + y^2 = x + y \qquad \Leftrightarrow \\
&x = -y \quad \text{või} \quad (x-y)^2 + (x-1)^2 + (y-1)^2 = 2
\end{aligned}$$

3. **Parameetriline esitus.** Tihti, kui on vaja näidata, et võrrandil (1) on lõpmata palju lahendeid, võib proovida leida parameetriline esitus tema lahenditele, s.t. esitada iga lahend kujul:

$$x_1 = g_1(k_1, \ldots, k_l),\ x_2 = g_2(k_1, \ldots, k_l),\ \ldots,\ x_n = g_n(k_1, \ldots, k_l)$$

(Kuid tavaliselt ikka ei ole võimalik esitada parameetriliselt kõiki lahendeid).

Näiteks: Näidata, et võrrandil $x^3 + y^3 + z^3 = x^2 + y^2 + z^2$ leidub lõpmata palju lahendeid.

Lahendus: Kui paneme $z = -y$, siis saame et $x^3 = x^2 + 2y^2$. Kui nüüd võtta $y = mx$, $m \in \mathbb{Z}$, siis saame, et $x = 1 + 2m^2$. Seega võrrandit rahuldavad kõik kolmikud $(1 + 2m^2, m(1 + 2m^2), -m(1 + 2m^2))$.

4. **Moodulo aritmeetika.** Väga tore asi.
   Näiteks: Näidata, et võrrandil $x^5 - y^2 = 4$ ei leidu täisarvulisi lahendeid.

   Lahendus: Vaatleme võrrandi modulo 11 järgi. $x^5 - 4$ saab olla modulo 11 järgi ainult $6, 7$ või 8, mis ei võrdu ühtegi täisarvu ruuduga modulo 11.

5. **Matemaatiline induktsioon.** Kõige otsesem lähenemine ülesannetele, kus sõnastuses esineb "näita, et iga n korral...".

   Näiteks: Näidata, et iga $n \in \mathbb{Z}_+$ korral võrrand $x^2 + y^2 + z^2 = 59^n$ on lahenduv.

   Lahendus: $n = 0$ ja $n = 1$ jaoks sobivad lahendid on vastavalt $(x_1, y_1, z_1) = (1, 3, 7)$ ning $(x_2, y_2, z_2) = (14, 39, 42)$. Nüüd iga $n \geq 3$ jaoks defineerime $(x_n, y_n, z_n) = (59^2 x_{n-2},\ 59^2 y_{n-2},\ 59^2 z_{n-2})$.

6. **Fermat' lõpmatu languse meetod.** "Anti-induktsioon".

   Näiteks: Näidata, et võrrandil $x^3 + 2y^3 = 4z^3$ ei leidu positiivseid täisarvulisi lahendeid.

   Lahendus: Oletame, et (x_1, y_1, z_1) on mingi lahend, $(x_1, y_1, z_1 \in \mathbb{Z}_+)$. Siis $(x_2, y_2, z_2) = (\frac{x_1}{2}, \frac{y_1}{2}, \frac{z_1}{2})$ peab olema ka lahend, ning $x_2, y_2, z_2 \in \mathbb{Z}_+$. Jätkates, saame lõpmatu kahaneva positiivsete täisarvude jada $x_1 > x_2 > x_3 > \ldots$, mis on võimatu.

Lineaarne diofantiline võrrand on võrrand kujul

$$a_1 x_1 + a_2 x_2 + \cdots + a_n x_n = b \tag{2}$$

kus $a_1, a_2, \ldots, a_n, b \in \mathbb{Z}$.

1. **Põhiteoreem.** Võrrand $ax + by = c$ on lahenduv parajasti siis, kui $\text{süt}(a, b) | c$. Seejuures iga lahend omab kuju

   $$(x, y) = (x_0 + \frac{b}{\text{süt}(a, b)} t, y_0 - \frac{a}{\text{süt}(a, b)} t)$$

   kus (x_0, y_0) on mingi konkreetne lahend, ning $t \in \mathbb{Z}$.

   Näide: Lahendada täisarvudes võrrand $6x + 10y + 15z = 7$.

   Lahendus: $(6x + 10y) + 15z = 7 \quad \Leftrightarrow \quad 2(3x + 5y) + 15z = 7$.
   Olgu $(3x+5y) = w$, siis $2w+15z = 7$. Lahendame alguses seda võrrandi. Eukleidese algoritmiga saame $1 = 2 \cdot (-7) + 15 \cdot 1$, seega $2 \cdot (-49) + 15 \cdot 7 = 7$, s. t. $(w_0, z_0) = (-49, 7)$ on viimase võrrandi erilahend. Teoreemist saame, et

   $$\begin{aligned} w &= -49 + 15u \\ z &= 7 - 2u \end{aligned}$$

   kus $u \in \mathbb{Z}$. Jääb lahendada $3x + 5y = -49 + 15u$. Jälle Eukleidese algoritmiga saame, et $3 \cdot 2 + 5 \cdot (-1) = 1$. Siis $(2 \cdot (-49 + 15u), -1 \cdot (-49 + 15u))$ on erilahend, seega

   $$\begin{aligned} x &= -98 + 30u + 5v \\ y &= 49 - 15u - 3v \\ z &= 7 - 2u \end{aligned}$$

   kus $u \in \mathbb{Z},\ v \in \mathbb{Z}$, mis ongi otsitav lahend.

2. **Järeldus.** Võrrand (2) on lahenduv parajasti siis, kui süt$(a_1, a_2, \ldots, a_n)|b$, ning iga lahend on avaldatav kui $n-1$ parameetritega lineaarne funktsioon.

3. **Boonusteoreem.** Olgu täisarvud $a_1, \ldots, a_m > 0$. Tähistagu A_n võrrandi $a_1x_1 + \cdots + a_mx_m = n$ lahendite arv. Siis jada (A_n) genereeriv funktsioon on

$$f(x) = \frac{1}{(1-x^{a_1})\cdots(1-x^{a_m})}, \quad |x| < 1$$

s.t. A_n võrdub x^n ees oleva kordajaga antud funktsiooni astmereaks arenduses. Sellest tulenevalt kehtib võrdus

$$A_n = \frac{1}{n!}f^{(n)}(0)$$

Näide: Leida võrrandi $x + 2y = n$ positiivse täisarvuliste lahendite arv.

Lahendus: Kasutame teoreemi juhul $f(t) = \frac{1}{(1-t)(1-t^2)}$.

Pythagorase võrrand on diofantiline võrrand kujul

$$x^2 + y^2 = z^2 \tag{3}$$

1. **Põhiteoreem.** Iga võrrandi (3) lahend omab kuju

$$x = k(m^2 - n^2) \qquad y = k(2mn) \qquad z = k(m^2 + n^2)$$

kus $k, m, n \in \mathbb{Z}$.

Ülesanded

1. Olgu $p, q \in \mathbb{P}$ (s. t. algarvud). Lahendada täisarvudes võrrand: $\frac{1}{x} + \frac{1}{y} = \frac{1}{pq}$
2. Olgu $p \in \mathbb{P}$, $p > 3$, $x, y, z \in \mathbb{Z}_+$. Lahendada võrrand: $x^3 + y^3 + z^3 - 3xyz = p$.
3. Leida positiivsed täisarvulised lahendid: $\frac{1}{x} + \frac{1}{y} + \frac{1}{z} = \frac{3}{5}$.
4. Näidata, et võrrandil $x^2 + y^2 = 13^z$ leidub lõpmata palju täisarvulisi lahendeid.
5. Leida võrrandi $\frac{1}{x} + \frac{1}{y} = \frac{1}{z}$ kõik täisarvulised lahendid.
6. Leida võrrandi $p^3 - q^5 = (p+q)^2$ kõik algarvulised lahendid.
7. Näita, et iga $n \geq 3$ jaoks, võrrandil $\frac{1}{x_1} + \frac{1}{x_2} + \cdots + \frac{1}{x_n} = 1$ leidub lahend, kus kõik x_i on erinevad positiivsed täisarvud.
8. Leida võrrandi $x_1^3 + x_2^3 + \cdots + x_m^3 = (x_1 + x_2 + \cdots + x_m)^2$ kõik lahendid, kus kõik x_i on erinevad positiivsed täisarvud.
9. Leida kõik mittenegatiivsed täisarvud, mis rahuldavad võrrandi $2^x - 1 = xy$.
10. Olgu $m, n \in \mathbb{Z}$, $1 \geq m, n \geq 1000$, $(n^2 - mn - m^2)^2 = 1$. Leida $\max(m^2 + n^2)$
11. Leida positiivsed täisarvulised lahendid: $7^x + x^4 + 47 = y^2$.
12. Näita, et ei leidu kaht positiivset täisarvu, mille ruutude summa ning vahe oleksid mõlemad täisruudud.

Allikas

- Titu Andreescu, Dorin Andrica. *An Introduction to Diophantine Equations.* GIL Publishing House, 2002. ISBN 973-9238-88-2.