43. tétel

Diofantikus egyenletek. Lineáris diofantikus egyenletek. Nevezetes diofantikus problémák. A Fermat-féle problémakör. Pitagoraszi számhármasok: a „descente infinie" módszer bemutatása az $x^4+y^4=z^4$ egyenlet kapcsán.

Def.: $f(x_1, x_2 \dots x_\varepsilon) = c$ diofantikus egyenlet, ahol f ε (≥ 2) változós egész együtthatójú polinom - fgv, c rögzített egész szám, és az egyenlet $x_1, x_2 \dots x_n$ egész megoldásait keressük.

Elsőfokú egyenletek:

Def.: Az $ax+by=c$ alakú kétváltozós lineáris diofantikus egyenlet, ahol $a, b \neq 0$ és c adott egészek, és x, y egész számok körében keressük a megoldást.
A megoldhatóság szükséges feltétele, hogy $(a,b) \mid c$.

Tétel: Ha $(a,b) \mid c \Rightarrow ax+by=c$ egyenlet ekvivalens $\frac{a}{(a,b)}x + \frac{b}{(a,b)}y = \frac{c}{(a,b)}$ egyenlettel, melyben x és y együtthatói relatív prímek.
Tehát elegendő $(a,b)=1$ esettel foglalkozni.

Tétel: Legyenek $a, b \in \mathbb{Z} \setminus \{0\}$, $(a,b)=1$ és c tetszőleges egész. Ekkor $ax+by=c$ egyenletnek ∞ sok x, y egész megoldása van. Továbbá, ha x_0, y_0 egy megoldása az egyenletnek $\Rightarrow$ az összes megoldást $x = x_0 + b \cdot t$, $y = y_0 - a \cdot t$ alakú egészek szolgáltatják, ahol t

végigfut a $\mathbb{Z}$ halmazon.

Biz.: Mivel $(a,b) = 1 \Rightarrow \exists\ x', y'$ egész számok, melyekre

$ax' + by' = 1 \Rightarrow a(cx') + b(cy') = c \Rightarrow x = cx'$ és $y = cy'$

megoldás, tehát az $ax + by = c$ egyenlet megoldható

Tfh.: x_0, y_0 egy megoldás, tehát $ax_0 + by_0 = c$.

Ha $x \wedge y$ egy tetszőleges megoldás $\Rightarrow ax + by = c$

teljesül.

$a(x - x_0) = -b(y - y_0)$ → első egyenletből kivonva a másodikat

Innen $b \mid a(x - x_0)$ $\quad (a,b) = 1 \Rightarrow \exists\ t \in \mathbb{Z} : x - x_0 = b \cdot t$

így $x = x_0 + b \cdot t$. Az $x - x_0 = b \cdot t$ értéket az

$a(x - x_0) = -b(y - y_0)$ egyenletbe helyettesítve:

$a \cdot b \cdot t = -b(y - y_0) \Rightarrow y = y_0 - a \cdot t$ adódik.

Tehát, ha x_0, y_0 megoldásból kiírjuk x, y és megoldása az egyenletnek $\Rightarrow x = x_0 + b \cdot t$, $y = y_0 - a \cdot t$.

$ax + by = a(x_0 + b \cdot t) + b(y_0 - a \cdot t) = ax_0 + by_0 = c$.

Tehát $x = x_0 + b \cdot t$, $y = y_0 - a \cdot t$ számpár $\forall\ t \in \mathbb{Z}$-re megoldása az egyenletnek.

Tétel: Legyenek $(a_1, a_2 \dots a_n)$ $n \geq 2$ nem zérus egészek, legyen $c \in \mathbb{Z}$. Az $a_1x_1 + \dots + a_nx_n = c$ diofantikus egyenletnek $\Leftrightarrow$ van $x_1, \dots x_n$ egész megoldása, ha $(a_1, \dots, a_n) \mid c$. Ha megoldható $\Rightarrow$ ∞ sok megoldása van, melyek $n - 1$ paraméterrel állíthatók elő.

Pitagoraszi egyenlet:

(1.) $x^2 + y^2 = z^2 \qquad x, y, z \in \mathbb{Z}$

Megj.: 1.; $x = 0, y = \pm z$ } triviális megoldások
$y = 0, x = \pm z$ }

2.; Ha x, y, z megoldás $\Rightarrow \pm x, \pm y, \pm z$ is megoldás

3.; Ha x, y, z megoldás $\Rightarrow cx, cy, cz$ is megoldás ($\forall c \in \mathbb{Z}$)

Ha $(x, y, z) = d$, x, y, z megoldás $\Rightarrow \frac{x}{d}, \frac{y}{d}, \frac{z}{d}$ is megoldás

Def.: Az (1.) egyenlet triviálistól különböző pozitív megoldásait, melyekben $(x, y, z) = 1$ primitív megoldásoknak nevezzük.

Tétel: Az $x^2 + y^2 = z^2$ egyenlet összes primitív megoldását szolgáltatják (x, y felcserélésétől eltekintve) az $x = 2uv$, $y = u^2 - v^2$, $z = u^2 + v^2$ alakú számhármasok, ahol u, v pozitív egészek, u, v relatív prímek, $u > v$ és u, v paritása különböző.

Biz.: Az (1.) egyenlet megoldható : pl.: $x = 3, y = 4, z = 5$

Tfh.: x, y, z egy primitív megoldás $\Rightarrow (x, y, z) = 1 \Rightarrow$

$\Rightarrow x, y, z$ páronként is relatív prímek.

(pl.: ha p prím $| (x, y) \Rightarrow$ (1.)-ből $p | z$ is adódik)

(1.)-ből következik, nem lehet x, y, z mindegyike páratlan.

x, y, z között nem lehet két páros és egy páratlan

(x, y, z között nem lehet mind páros : $(x, y, z) = 1$)

Tehát : x, y, z közül egy páros és 2 páratlan

Z nem lehet páros : indirekt.

Tfh $z = 2 \cdot z_1$ alakú, $x = 2x_1 + 1$, $y = 2y_1 + 1$ alakú $\Rightarrow$

(I.) -ből következik : $4x_1^2 + 4x_1 + 1 + 4y_1^2 + 4y_1 + 1 = 4z_1^2$

$\nexists$ a jobb oldal osztható 4-gyel , a bal pedig nem.

Szimmetriai okok miatt feltehetjük, hogy x páros , y és z páratlan.

(I.) -ből :

$$(II.) \quad \left(\frac{x}{2}\right)^2 = \frac{z^2 - y^2}{4} = \left(\frac{z}{2}\right)^2 - \left(\frac{y}{2}\right)^2 = \frac{z+y}{2} \cdot \frac{z-y}{2}$$

ahol : $\frac{x}{2}$, $\frac{z+y}{2}$, $\frac{z-y}{2} \in \mathbb{Z}$

Tfh.: $d = \left(\frac{z+y}{2} ; \frac{z-y}{2}\right) \Rightarrow d \mid \frac{z+y}{2} + \frac{z-y}{2} = z$

$$d \mid \frac{z+y}{2} - \frac{z-y}{2} = y$$

$d \mid (z, y) = 1 \Rightarrow d = 1$

Így $\left(\frac{z+y}{2} , \frac{z-y}{2}\right) = 1$, mivel (II.) -ből

$\frac{z+y}{2} = u^2$ és $\frac{z-y}{2} = v^2$, ahol u és v pozitív egészek

Innen : $z = \frac{z+y}{2} + \frac{z+y}{2} = u^2 + v^2$

$y = \frac{z+y}{2} - \frac{z-y}{2} = u^2 - v^2$

$x = 2\sqrt{\frac{z+y}{2} \cdot \frac{z-y}{2}} = 2uv$

A kapott értékeket (I.) -be helyettesítve :

$(2uv)^2 + (u^2 - v^2)^2 = (u^2 + v^2)^2$ így megoldásokat!

Ha x, y, z egy primitív megoldás $\Rightarrow u > v$ (mert $y > 0$)

$(u, v) = 1$ és u, v paritása különböző, mert különben

x, y, z nem lennének relatív prímek.

És fordítva is igaz, azaz u és v egészekre az előbbi feltételek teljesülnek $\Rightarrow$ az általuk meghatározott (x, y, z) pitagoraszi relatív prím megoldása (I.) -nek.

43/11

Következmény: Az (1.) egyenlet összes pozitív megoldása

$x = d \cdot u \cdot v$, $y = d(u^2 - v^2)$, $z = d(u^2 + v^2)$,

ahol u és v eleget tesz a tételben leírt feltételeknek.

Tétel: (Fermat-sejtés, Nagy Fermat-tétel)

$x^n + y^n = z^n$ nincs pozitív egész megoldása

$n > 2$ esetén.

Biz.: Euler: $n = 3$-ra.

$E := \{a + bs \,;\, a, b \in \mathbb{Z}\}$; $s = -\frac{1}{2} + \frac{\sqrt{3}}{2}$;

Euler E-ben oldotta meg a F.-sejtést.

$x^n + y^n = z^n$

n ↙ ↘

$n = q \cdot p$ $n = 2^\varepsilon$ p: páratlan prím

a.; ha $n = 2^\varepsilon$ $x^{2^\varepsilon} + y^{2^\varepsilon} = z^{2^\varepsilon}$

$$\left(x^{2^{\varepsilon-2}}\right)^4 + \left(y^{2^{\varepsilon-2}}\right)^4 = \left(z^{2^{\varepsilon-2}}\right)^4$$

$$\underbrace{x^4}_{} + \underbrace{y^4}_{} = \underbrace{z^4}_{}$$

→ ha ez megoldható, a másik is.

elegendő belátni,

n : $x^4 + y^4 + z^4$ $x, y, z \in \mathbb{Z}^+$-ban $\nexists$ megoldás.

$x^4 + y^4 = (z^2)^2 \Rightarrow x^4 + y^4 = Z^2$ végtelen leszállás módszere. *

b.; ha $n = q \cdot p$

$x^{qp} + y^{qp} = z^{qp}$ →

$(x^q)^p + (y^q)^p = (z^q)^p$ ha ez megoldható, ez is!

$x^p + y^p = z^p$ ←

Elegendő belátni, n $x^p + z^p = z^p$ $x, y, z \in \mathbb{Z}^+$-ban $\nexists$ megoldás

Andrew Wiles 1993-ban bejelenti: megoldott egy problémát elliptikus görbékkel kapcsolatban, amelyből következik Fermat állítása.

$y^2 = x^3 + ax^2 + bx + c \qquad a, b, c \in \mathbb{Z}$

Elliptikus görbe.

pl.: $y^2 = x^3 - 2 \quad (25 = 27 - 2) \Rightarrow$ ez is elliptikus görbe.

*(43/5) Végtelen leszállás (descente infinie) elve.

Tétel: Az $x^4 + y^4 = z^2$ (*) diofantikus egyenletnek nincs x, y, z pozitív egész megoldása.

Biz.: Tfh.: (*)-nak F minimális ($x, y, z \neq$ zérus) megoldása

Ekkor F x, y, z pozitív egész megoldás, ahol z minimális.

Megoldásra: $(x, y, z) = 1$.

Mivel (*) : $(x^2)^2 + (y^2)^2 = z^2$ alakban írható,

x^2, y^2, z relatív prímek $\Rightarrow$ x^2, y^2, z a pitagoraszi egyenlet-nek primitív megoldása. Így

(**) $x^2 = 2uv$, $y^2 = u^2 - v^2$, $z = u^2 + v^2$, ahol

u, v: különböző paritású, relatív prím pozitív egészek

$u > v$ feltétellel. (**) alapján: $v^2 + y^2 = u^2$ $\quad (u, v) = 1$ u: páros, $(u, v, y) = 1$ y: páratlan

így (***) $v = 2mn$, $y = m^2 - n^2$, $u = m^2 + n^2$

m és n különböző paritású, relatív prím pozitív egészekkel.

De: (**) és (***)-vel:

$$x^2 = 2uv = 4mn$$

$$\left(\frac{x}{2}\right)^2 = mn$$

De: $(m, n) = 1 \Rightarrow u = m^2 + n^2$ miatt u, m, n páronként relatív prímek, így:

$m = a^2$, $n = b^2$, $u = c^2$ (a, b, c pozitív egészek)

$u = m^2 + n^2$ egyenlőségbe írva:

$a^4 + b^4 = c^2$

(*) és miatt $c < u < z$ ↯ z minimalitásának.

Így az egyenletnek nem létezik triviálistól különböző pozitív megoldása.

Waring - probléma:

Tétel: Legyen n természetes szám. Az $x^2 + y^2 = n$ diofantikus egyenlet nem oldható meg, ha n alakja:

$n = 2^q(4\ell + 3)$, ahol $q, \ell \in \mathbb{N}$.

Tétel: Legyen $q, \ell \in \mathbb{N}$. Ha $n = 4^q(8\ell + 7)$ alakú ⇒

$x^2 + y^2 + z^2 = n$ egyenletnek nincs egész megoldása.

Tétel: Minden pozitív egész szám felírható négy négyzetszám összegeként.

$\ell \geq 2$ ($\ell \in \mathbb{N}$) esetén jelöljük $g(\ell)$-val azt a pozitív egészet, melyre $\forall$ term. szám felírható $g(\ell)$ darab ℓ-adik hatvány összegeként.

1909-ben Hilbert igazolta ezt.

pl.: $\ell = 2$ $g(\ell) = 4$

$\ell = 3$ $g(\ell) = 9$

$k = 4$ $g(k) = 19$

Tétel: $\forall\ \ell \geq 2$ pozitív egész esetén

$$g(\ell) \geq 2^\ell + \left[\left(\frac{3}{2}\right)^\ell\right] - 2$$

Tétel: (1957-ben Mahler sejtette)

Ha $\varepsilon > 7$, $\Rightarrow g(\varepsilon) = 2^{\varepsilon} + \left[\left(\frac{3}{2}\right)^{\varepsilon}\right] - 2$