BIZ: lsd tk $\frac{1}{6} \cdot \frac{x}{\log x} < T(x) < 6 \cdot \frac{x}{\log x}$

(new tell, csak megnézni!)

$p_1 = 2$, $p_2 = 3$, ... $p_n =$

T.: A n. prímszám aszimptotikusan egyenlő $n \cdot \log n$-nel.

$$p_n \sim n \log n$$

$n >>$: $c_1' \cdot n \log n < p_n < c_2' n \log n$

$\exists c_1', c_2' \in \mathbb{R}$

BIZ: (lsd tk) ——

Páros Goldbach-sejtés:

$n > 4$ páros

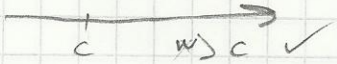
$n = p_1 + p_2$, ahol p_1 és p_2 páratlan prímek

Biz van eddig: $p_1 + \underbrace{Q}_{p_2 \cdot p_3}$

Páratlan Goldbach-sejtés:

$n > 7$ páratlan $n = p_1 + p_2 + p_3$ páratlan prímek összege

Biz: Vinogradov oldotta meg



10. előadás

Diofantikus egyenletek

Zay Béla tanár úr

Def. $f(x_1, x_2, \dots x_k) = c$ diofantikus egyenlet, ahol f $k\ (\geq 2)$ változós egész együtthatójú polinom, 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 és $b \neq 0$ és c adott egészek, és x, y egész számok körében keressük a megoldást.
A megoldhatóság szükséges feltétele, hogy $(a,b) \mid c$.

T: 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.

T: 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,

akol 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 és y egy tetszőleges megoldás $\Rightarrow ax+by=c$ teljesül.

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

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

és így $\underline{x = x_0 + b\cdot t}$. 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 megoldásaiból kiírjuk x, y is megoldása az egyenletnek $\Rightarrow x = x_0 + b\cdot t$, $y = y_0 - a\cdot t$.

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

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 zéres egészek és 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 $\Rightarrow \infty$ sok megoldása van, melyek $n-1$ paraméterrel

JH

állítható ℤ első.

Biz.: ——

Pitagoraszi egyenlet:

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

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

Def.: A (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 és y felcserélésétől eltekintve) az $x=2uv$, $y=u^2-v^2$, $z=u^2+v^2$ alakú számhármasok, ahol u és v pozitív egészek, u és v relatív prímek, $u>v$ és u,v paritása különböző.

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

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

$\Rightarrow$ x,y,z párosukat 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) között 1 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 $\Rightarrow$ (1)-ből következik $4x_1^2 + 4x_1 + 1 + 4y_1^2 + 4y_1 + 1 = 4z_1^2$

ellentmondás, mert a jobb oldal osztható 4-gyel, a bal oldal pedig nem.

Szimmetriai okok miatt feltehetjük, hogy x páros és y és z páratlan. (1) egyenletből:

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

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

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

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

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

Így $\left(\frac{z+y}{2} \text{ és } \frac{z-y}{2}\right) = 1$ esét a (2) következik, u.

$\frac{z+y}{2} = u^2$ 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 értéket (1)-be helyettesítve:

$(2uv)^2 + (u^2 - v^2)^2 = (u^2 + v^2)^2$ így valóban megoldások

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, vagyis ha u és v egészekre az előbbi feltételek teljesülnek, akkor az általuk meghatározott (x,y,z) párosként relatív prím megoldása (1)-nek

Pl.: $(z,y)=1=d$ Biz: $d \mid z+y = u^2+v^2+u^2-v^2 = 2u^2$

$d \mid z-y = u^2+v^2-(u^2-v^2) = 2v^2$

$(u,v)=1 \Rightarrow d \mid 2 \Rightarrow d=1$ vagy 2

ha $d=2 \mid z=u^2+v^2$ nem lehetséges, mert u és v különböző paritásúak $\Rightarrow u^2+v^2$ páratlan.

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

$7x+10y+16z=500$ $\quad x,y,z \in \mathbb{Z}$

$x=\frac{500-10y-16z}{7}=71-y-2z+\frac{3-3y-2z}{7}=$

u

$=71-y-22+u$

$2z+3y+7u=3$

$z=\frac{3-3y-7u}{2}=1-2y-3u+\frac{1+y-u}{2}=1-2y-3u+v$

v

$$\frac{1+y-u}{2} = v \qquad y = u + 2v - 1$$

$$z = 1 - 2(u+2v-1) - 3u + v = -5u - 3v + 3$$

$$x = \underbrace{11 - (u+2v-1)}_{y} - 2\underbrace{(-5u-3v+3)}_{z} + u =$$

$$= 10u + 6v + 66 \qquad \forall u, v \in \mathbb{Z}$$

V. 6. 11. előadás

$x^u + y^u = z^u$, ha $u = 1$ megoldható

$u = 2$ — " —

$u \geq 3$ triviális megoldás, ha $x_0 = y_0 = z_0 = 0$ és

$x_0^u + y_0^u = z_0^u$.

Melyek lesznek a nem triviális megoldások?

$x_0^u + y_0^u = z_0^u \quad x_0 \cdot y_0 \cdot z_0 \neq 0$

Fermat-féle probléma:

$x^u + y^u = z^u \qquad u \geq 3 \qquad x, y, z \in \mathbb{Z}^+$

Megoldható-e?

Fermat-sejtés: $\nexists$ megoldás

(Nagy Fermat tétel)

(Fermat utolsó tétele) Ez volt az a tétel, amit még nem igazoltak

Euler: Nézzük meg $n=3$-ra.

$n=3$-ra igaz a Fermat sejtés

BIZ: $E := \{ a+b\varrho \,;\, a,b \in \mathbb{Z} \}$

$\varrho = -\frac{1}{2} + \frac{\sqrt{3}}{2} i$

Euler E-ben oldotta meg a Fermat sejtést.

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

$\swarrow^{n} \searrow$

$n = q \cdot p$ $\qquad$ $n = 2^k$ $\qquad$ p pl. páratlan prím

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

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

$x^4 + y^4 = z^4$ → ha ez megoldható, akkor a másik is.

↳ elegendő belátni, h. ez nem oldható meg.

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

(ezt kell belátni)

Ha ezt belátjuk ⇒ az is 2 hatványra belátjuk.

BIZ: $x^4 + y^4 = \left(z^2\right)^2$ $\qquad$ Biz. ind. Hk.

$x^4 + y^4 = Z^2$ $\qquad$ módszer végtelen leszállás módszere

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

$x^{qp} + y^{qp} = z^{qp}$ $\qquad$ ha ez megoldható, akkor

$\left(x^q\right)^p + \left(y^q\right)^p = \left(z^q\right)^p$

$X^p + Y^p = Z^p$ → ez is megoldható

Elegendő bizonyítani, h. $x^p + y^p = z^p$ $x, y, z \in \mathbb{Z}^+$ -ban $n \geq 3$

$\nexists$ megoldás

1992. Andrew Wiles

Wiles - Taylor

segítőtársa volt, fél évig a padláson sínálltak a bizonyítást

1995: A bizonyítás 1200 oldal

$y^2 = x^3 - 2$

$25 = 27 - 2$

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

↘ ez is elliptikus görbe

Waring - probléma:

pl.: $x^2 + y^2 = n \quad \forall n \in \mathbb{Z}^+$

Előállítható $\forall n \in \mathbb{Z}^+$ két egész szám négyzetének összegeként.

$x^2 + y^2 = 3$ Ez nem megoldható.

Az $x^2 + y^2 = 2^k (4\ell + 3)$ egyenletek nem oldhatók meg.

$x^2 + y^2 + z^2 = n$

$x^2 + y^2 + z^2 = 3$ megint nem oldható meg!

$x^2 + y^2 + z^2 + t^2 = u$ $\forall$ minden megoldható!

$g(\ell)$ jelöli azt a minimális pozitív egészt, amely $\forall\ u \in \mathbb{Z}^+$ előállítható $g(\ell)$ db ℓ-dik hatvány összegeként.

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

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

$\ell = 4$ $\quad g(\ell) = 19$

Tétel: $g(\ell)$-ra van egy becslés:

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

BIZ: —

Tétel: Ha $\ell >>$ (elég nagy), akkor $g(\ell) = 2^\ell + \left[\left(\frac{3}{2}\right)^\ell\right] - 2$

Diofantikus approximáció

(közelítés)

$\alpha \in \mathbb{R}^+$

$\sqrt{2} \sim 1{,}4 \sim 1{,}41 \ldots$

$\alpha \in \mathbb{R}^+$, $\ell \in \mathbb{R}^+$ $\quad c = c(\alpha) \in \mathbb{R}^+$

Def.: α ℓ-ad rendben approximálható, $\frac{p}{q}$ racionális számokkal, ha $\exists\ c = c(\alpha)$, hogy

$$0 < \left|\alpha - \frac{p}{q}\right| < \frac{c}{q^\ell} \qquad q > 0$$

végtelen sok q, p-re megoldható.