ALGEBRA ÉS SZÁMELMÉLET 4

11/1

11. előadás

Másodfokú kongruenciák, kvadratikus maradékok, Legendre-szimbólum

Emlékeztető: Szoros kapcsolat van a lineáris diofantikus egyenletek és a lineáris kongruenciák között:

$ax + by = c$ diofantikus egyenlet

$\Updownarrow$

$ax \equiv c \ (b)$ kongruencia.

Mindkettő megoldhatóságának szükséges és elégséges feltétele: $(a,b) \mid c$; a diofantikus egyenlet megoldásainak maradékosztályai adják a kongruencia megoldásait.

A kongruencia megoldhatóságának vizsgálata egyébként egy véges probléma, tehát elvben megoldható.

Magasabbfokú diofantikus egyenletek

1) $x^2+y^2=z^2$ Pitagoraszi számhármasok; teljes leírás adható

2) $x^2+y^2=n$ Vizsgálata az ún. Gauss-egészekhez vezet.

3) $x^2 - my^2 = 1$, $m \in \mathbb{N}$ nem négyzetszám mégszűkített;
ezek az ún. Pell-egyenletek

4) $x^n + y^n = z^n$ Fermat-sejtés; spec. n-ekre spec. megoldási módszerek

A fenti példák mutatják, hogy a legegyszerűbb diofantikus egyenletek is gyakran előfordulnak a matematikában, és megoldásuk különböző módszereket kívánnak. Ezek néha egészen bonyolultak is lehetnek (pl. Wiles bizonyítása a Fermat-sejtésre)

Néhány ad hoc példa

1) Oldjuk meg a $3x^2 + 20y = 2021$ diofantikus egyenletet!

Megoldás: Nézzük az utolsó számjegyeket! Azt kapjuk, hogy $3x^2$-nek 1-re kellene végződnie, pedig a négyzetszámok utolsó számjegye 0, 1, 4, 9, 6 és 5 lehet, így a 3-szorosuk utolsó jegye 0, 3, 2, 7, 8 és 5 lehet. Ez mutatja, hogy az egyenletnek nincs megoldása.

2) Oldjuk meg az $x^{10} - y^{15} = 20$ diofantikus egyenletet.

Megoldás: (Kicsit nehezebb látni ezt a megoldást.)
modulo 31 nézve: 10. hatvány lehet 0, 1, 5, 25,

15. lehetnek 0, 1 v. 30 ($\equiv -1$). Ezekből a maradékokból nem kaphatunk 20-at (vagy akár 20 maradékot modulo 31).

(Megjegyzés: $10, 15 \mid 30$, $30 = \varphi(31)$, $a^{\varphi(31)} \equiv 1 \ (31)$, ha $(a, 31) = 1$. Így jön a 31 a képbe.)

Mindkét feladatnál azon múlott a megoldás, hogy az egész számok hatványai nem akármilyen maradékot adnak bizonyos modulus szerint. Pl. négyzetszámok utolsó számjegye nem lehet akármi, csak 0, 1, 4, 9, 6 v. 5. Hasonlóképpen pl. négyzetszám nem adhat 2 maradékot modulo 3.

A továbbiakban az előbbi diofantikus egyenletek helyett magasabbfokú kongruenciákat vizsgálunk, nevezetesen ún. binom kongruenciákat, s általában prím modulus fölött.

Def. $x^k \equiv a \pmod{p}$: az ilyen kongruenciákat <u>binom kongruenciáknak</u> nevezzük.

<u>Megjegyzés</u>: 1) Általánosabb lenne: $c \cdot x^k \equiv a \pmod{p}$, de itt $c \equiv 0 \pmod{p}$ esetén a kongruencia triviálissá válna; $c \not\equiv 0 \pmod{p}$, azaz $p \nmid c$ esetén viszont szorozhatunk c reciprokával $\mathbb{Z}_p$-ben, s a kongruenciát visszavezettük a fönti alakra.

2) $a \equiv 0 \pmod{p}$ esetén nyilván csak $x \equiv 0 \pmod{p}$ lesz megoldás, hiszen $p \mid x^k \Rightarrow p \mid x$ (p prím)

Így általában föltesszük: $a \not\equiv 0$ (p).

Mi a továbbiakban csak a $k=2$ esettel foglalkozunk (kvadratikus kongruencia); az általános k esete a primitív gyök fogalmához vezetne ($\rightsquigarrow$ ALGEBRA 5)

Def. Egy a számot $p>2$ prím és $(a,p)=1$ esetén aszerint nevezünk kvadratikus maradéknak vagy kvadratikus nemmaradéknak, hogy az $x^2 \equiv a\ (p)$ kongruencia megoldható-e vagy sem.

(Megjegyzés: $p \mid a$ esetén nyilván a kvadratikus maradéknak lenne tekintendő, hiszen pl. $0^2 \equiv a\ (p)$, de a p-vel osztható számokat általában nem tekintjük sem kvadratikus maradéknak, sem kvadratikus nemmaradéknak.)

Miként a kongruenciáknál általában, itt is gondolhatunk a megoldásokra mint kongruenciaosztályokra, azaz modulo p maradékokra (s nem mint egész számokra). Az $x^2 \equiv a\ (p)$ kongruencia megoldásai tehát maradékosztályok, és a-ra is gondolhatunk inkább mint egy maradékosztályra.

Áll.: $p>2$ prím, $a_1, \dots, a_{p-1}$ egy redukált maradékrendszer modulo p. Ekkor az a_i-knek pontosan a fele, azaz $\frac{p-1}{2}$ lesz kvadratikus maradék, fele pedig kvadratikus nemmaradék.

Biz. Tekintsük az $1^2, 2^2, \ldots, (p-1)^2$ elemek maradékosztályait: nyilván pontosan ezek adják a kvadratikus maradékok osztályait. De:

$$i^2 \equiv j^2 \ (p) \iff p \mid i^2 - j^2 = (i-j)(i+j),$$

tehát azonos maradékot ezek akkor kapunk, ha $i \equiv j \ (p)$ v. $i \equiv -j \ (p)$.

Ilyen módon, mivel $i \not\equiv -i \ (p)$, hisz $2i \not\equiv 0 \ (p)$, minden kvadratikus maradékot pontosan 2-szer kapunk meg, ez azt jelenti, hogy pontosan $\frac{p-1}{2}$ db kvadratikus maradékunk van.

(Nyilván ezeket mind megkapjuk, ha vesszük az $1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2$ maradékosztályait.)

Áll: 1) a, b kvadratikus maradék $\Rightarrow$ $a \cdot b$ is kv. mar.

2) a kv. maradék, b kv. nemmaradék $\Longrightarrow$ $a \cdot b$ kvadratikus nemmaradék

3) a, b kvadratikus nemmaradék $\Longrightarrow$ $a \cdot b$ kvadratikus maradék.

Biz. 1) Világos: $u^2 \equiv a \ (p)$, $v^2 \equiv b \ (p) \Longrightarrow$ $u^2 v^2 = (uv)^2 \equiv a \cdot b \ (p)$.

2) Ha $u^2 \equiv a \ (p)$, $v^2 \equiv a \cdot b \ (p)$, akkor:

$v^2 \equiv u^2 \cdot b \ (p)$, és szorozva u inverzével $\mathbb{Z}_p$-ben (azaz az $u \cdot x \equiv 1 \ (p)$ megoldásával – ilyen van!)

$x^2 \cdot v^2 = x^2 u^2 \cdot b = 1 \cdot b \;(p)$, tehát ez azt jelentené, hogy b is kvadratikus maradék mod p. Tehát ab nem lehet kvadratikus maradék.

c) Legyen a kvadratikus nemmaradék, és szorozzuk végig a-val egy redukált maradékrendszert mod p. Nyilván így ismét egy redukált maradékrendszert kapunk. A b) rész alapján a-val szorozva a $\frac{p-1}{2}$ db. kvadratikus maradékot, a szorzat kvadratikus nemmaradék lesz; így a többi szorzat már „kénytelen" kvadratikus maradék lenni.

Áll. Legyen $(a,p)=1$, $p>2$ pr. Ekkor

1) a kvadratikus maradék $\Longleftrightarrow a^{\frac{p-1}{2}} \equiv 1 \;(p)$

2) a kvadratikus nemmaradék $\Longleftrightarrow a^{\frac{p-1}{2}} \equiv -1 \;(p)$.

Biz. Ismét célszerű a lehetséges a osztályokra mint a nem nulla maradékokra, azaz mint a $\mathbb{Z}_p$ test nem nulla elemeire gondolni: ezekből van $(p-1)$ db.

A kis Fermat-tétel miatt $(a,p)=1$ esetén $a^{p-1} \equiv 1 \;(p)$, azaz $\mathbb{Z}_p$ nem nulla elemei gyökei az $x^{p-1}-1$ polinomnak.

Ha $a \equiv u^2 \;(p)$, akkor nyilván $(a,p)=1$ miatt $(u,p)=1$ is teljesül, és így

$$a^{\frac{p-1}{2}} \equiv (u^2)^{\frac{p-1}{2}} = u^{p-1} \equiv 1 \quad (p).$$

Ez azt jelenti, hogy a kvadratikus maradékoknak megfelelő maradékosztályok gyökei az $x^{p-1}-1 = (x^{\frac{p-1}{2}}-1)(x^{\frac{p-1}{2}}+1)$ felbontásának első tényezőjének. Ezzel az 1) állítás egyik iránya megvan. De ilyen módon az $x^{\frac{p-1}{2}}-1$ polinom összes gyökét megtaláltuk, hiszen kvadratikus maradékból $\frac{p-1}{2}$ darab van, és egy $\frac{p-1}{2}$-edfokú polinomnak $\frac{p-1}{2}$-nél több gyöke nem lehet. Ez egyúttal azt is jelenti, hogy a kvadratikus nemmaradékok gyökei a második tényezőnek, azaz $x^{\frac{p-1}{2}}+1$-nek.

Vagyis: a kv. maradék $\Longrightarrow a^{\frac{p-1}{2}} \equiv 1 \quad (p)$

a kv. nemmaradék $\Longrightarrow a^{\frac{p-1}{2}} \equiv -1 \quad (p).$

Ezzel mindkét állítás mindkét irányát beláttuk. □

Köv.: (-1) pontosan akkor kvadratikus maradék modulo p, ha $p=4k+1$, és akkor kvadratikus nemmaradék, ha $p=4k-1$.

Biz.: $$(-1)^{\frac{p-1}{2}} = \begin{cases} 1 & \text{ha } p=4k+1 \quad (\Rightarrow p \text{ kv. mar.}) \\ -1 & \text{ha } p=4k-1 \quad (\Rightarrow p \text{ kv. nemmar.}) \end{cases}$$

Megj.: $p=2$-re természetesen $-1 \equiv 1$ kvadratikus maradék.

Legendre-szimbólum

A kvadratikus maradékokkal kapcsolatban az alábbi jelölést vezetjük be:

Def.: p prím, $(a,p)=1$ esetén:

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{ha } a \text{ kvadratikus maradék} \\ -1 & \text{ha } a \text{ kvadratikus nemmaradék} \end{cases}$$

Olvasd: „a per p Legendre-szimbólum"

Tétel: $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \ (p)$ (*)

A L.-szimbólum néhány tulajdonsága:

Áll: 1) $a \equiv b \ (p) \Rightarrow \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$

2) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\cdot\left(\frac{b}{p}\right)$

3) $\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{ha } p=4k+1 \\ -1 & \text{ha } p=4k-1 \end{cases}$

Biz: Az állítások mind következnek a fenti (*)-ból.

Következmény: Ha az $\left(\frac{n}{p}\right)$ Legendre-szimbólumot akarjuk kiszámolni, akkor elegendő meghatározni a $\left(\frac{2}{p}\right)$ és $\left(\frac{q}{p}\right)$ Legendre-szimbólumokat $q>2$ prímre (nyilván csak $q \mid n$ esetén érdekes), de 1) miatt még $q<p$ is feltehető!

Ez is egyszerűsítés, de a nagy segítséget az ún. kvadratikus reciprocitási tétel adja majd.

Ahhoz, hogy a Legendre-szimbólummal jól tudjunk számolni, kimondjuk az alábbi két állítást bizonyítás nélkül (a bizonyítás megtalálható a Freud–Gyarmati-könyvben).

Tétel (A $\left(\frac{2}{p}\right)$ Legendre-szimbólum értéke):

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{ha } p = 8k \pm 1 \\ -1 & \text{ha } p = 8k \pm 3 \end{cases}$$

Köv. A 2 kvadratikus maradék modulo 7 (valóban, $3^2 = 9 \equiv 2 \ (7)$), és kvadratikus nemmaradék modulo 11 (a kv. maradékok itt: 1, 4, 9, 5, 3)

Tétel (Kvadratikus reciprocitási tétel)

Legyenek $p, q > 2$ prímek, $p \neq q$. Ekkor:

$$\left(\frac{q}{p}\right) \cdot \left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$$

Ez úgy is mondható, hogy:

$$\left(\frac{q}{p}\right) = \begin{cases} -\left(\frac{p}{q}\right) & \text{ha } p, q \ 4k-1 \text{ alakú} \\ \left(\frac{p}{q}\right) & \text{ha legalább az egyik } 4k+1 \text{ alakú} \end{cases}$$

(A két tétel közül az első állítás bizonyítása könnyebb)

Számolási példa: (2020-hoz legközelebbi prím: 2017, ezért ezzel számolunk ☺)

ASZ 4

11/10

Döntsük el, megoldható-e az $x^2 \equiv 334 \pmod{2017}$ kongruencia.

Itt $334 = 2 \cdot 3^2 \cdot 13$, így: $\left(\frac{334}{2017}\right) = \left(\frac{2}{2017}\right) \cdot \left(\frac{3}{2017}\right)^2 \cdot \left(\frac{13}{2017}\right)$

Ezek közül, mivel $2017 = 8k+1$, ezért:

$$\left(\frac{2}{2017}\right) = 1.$$

A $\left(\frac{3}{2017}\right)$ értékével nem kell foglalkoznunk, mivel úgyis a négyzeten szerepel.

Hogyan számoljuk $\left(\frac{13}{2017}\right)$ értékét? Természetesen nem szeretnénk a $13^{\frac{2017-1}{2}}$ maradékát kiszámolni.

Helyette alkalmazzuk a reciprocitási tételt.

Itt most 13 is, 2017 is $4k+1$ alakú (elég lenne csak az egyik), így:

$$\left(\frac{13}{2017}\right) = \left(\frac{2017}{13}\right)$$

Itt viszont az a jó, hogy 2017-et kicserélhetjük egy vele kongruensre: $2017 = 155 \cdot 13 + 2$, tehát:

$$\left(\frac{2017}{13}\right) = \left(\frac{2}{13}\right)$$

Mivel $13 = 8k-3$, ezért: $\left(\frac{2}{13}\right) = -1$.

Azt kaptuk tehát, hogy az $x^2 \equiv 334 \ (2017)$ kongruencia nem megoldható, mert $\left(\frac{334}{2017}\right) = -1$.

Mikor lesz a 3 kvadratikus maradék modulo p?

Számoljuk ki a $\left(\frac{3}{p}\right)$ Legendre-szimbólum értékét.

$$\left(\frac{3}{p}\right) = \begin{cases} \left(\frac{p}{3}\right) & \text{ha } p = 4k+1 \text{ alakú} \quad (p \equiv 1 \ (4)) \\ -\left(\frac{p}{3}\right) & \text{ha } p = 4k-1 \text{ alakú} \quad (p \equiv -1 \ (4)) \end{cases}$$

↑ reciprocitási tétel, a 3 ugyanis $4k-1$ alakú.

$$\left(\frac{p}{3}\right) = \begin{cases} 1 & \text{ha } p = 3k+1 \text{ alakú} \quad (p \equiv 1 \ (3)) \\ -1 & \text{ha } p = 3k-1 \text{ alakú} \quad (p \equiv -1 \ (3)) \end{cases}$$

Mikor kapunk tehát 1-et?

1) eset: $p \equiv 1 \ (4)$ ÉS $p \equiv 1 \ (3)$ $\Longrightarrow$ $p = 12k+1$ alakú

2) eset: $p \equiv -1 \ (4)$ ÉS $p \equiv -1 \ (3)$ $\Longrightarrow$ $p = 12k-1$ alakú

Minden egyéb esetben 3 kvadratikus nemmaradék.

Megjegyzés: A Legendre-szimbólum számolása tehát viszonylag gyors, feltéve, ha tudjuk az előforduló számok faktorizációját: az előforduló számok ugyanis a reciprocitási tétel és a maradékos osztások segítségével gyorsan csökkennek.

Sajnos: baj lehet a faktorizációval.

Ennek kiküszöbölésére vezették be a Jacobi-szimbólumot, amit most nem tárgyalunk.

Alkalmazás: a Dirichlet-tétel egy speciális esete:

Áll: Végtelen sok $12k-1$ alakú prím van.

Biz. S. áll: $n = 12c^2 - 1$-nek minden prímosztója $p = 12k \pm 1$ alakú.

Biz.: T. fel: $p \mid 12c^2 - 1$, azaz

$$12c^2 \equiv 1 \pmod p.$$

Ez azt jelenti, hogy $12c^2$ kvadratikus maradék mod p. Így persze 12 is kv. maradék, és $12 = 3 \cdot 2^2$ miatt:

$$\left(\frac{12}{p}\right) = \left(\frac{3}{p}\right) \cdot \left(\frac{2}{p}\right)^2 = \left(\frac{3}{p}\right) = 1.$$

De tudjuk: $\left(\frac{3}{p}\right) = 1 \iff p = 12k \pm 1$.

T. most fel: $p_1, p_2, \ldots p_k$ az összes $12k-1$ alakú prím. Legyen $c = p_1 \cdots p_k$, és legyen $n = 12c^2 - 1$. Ekkor $p_i \nmid n$ világos. De ha n-nek – melyről tudjuk, hogy a prímosztói $12k \pm 1$ alakúak – csak $12k+1$ alakú prímosztója lenne, akkor n is ilyen alakú lenne (azaz $n \equiv 1 \ (12)$ teljesülne), de ez nem igaz. Így n-nek van egy új $12k-1$ alakú prímosztója, ami nem szerepel a listán.