Számelmélet gyakorlat
2023/2024 II. félév

2024. Március 14.

1. Emlékeztető

1.1. Tétel. *Tekintsük az $ax+by=c$ diophantoszi egyenletet, ahol $a,b,c \in \mathbb{Z}$ és $a,b \neq 0$*

- *Az egyenletnek akkor és csak akkor van megoldása, ha $(a,b) \mid c$*
- *Ha (x_0, y_0) egy partikuláris megoldás, akkor az általános megoldás:*

$$x_t = x_0 + \frac{b}{(a,b)}t \qquad y_t = y_0 - \frac{a}{(a,b)}t$$

Megoldás lépései:

1. lnko, azaz (a,b) kiszámítása
2. ha $(a,b) \nmid c$, akkor nincs megoldás; ha $(a,b) \mid c$, akkor következö lépés:
3. euklideszi algoritmusból: $au + bv = (a,b)$
4. beszorozzuk azzal, amivel kell: $ax_0 + by_0 = c$
5. felírjuk az általános megoldás képletét
6. kiválogatjuk a feladat szövegének megfelelő megoldásokat.

1.1. Definíció. *Lineáris kongruencián $ax \equiv b \pmod{m}$ alakú egyenleteket értünk, ahol $a,b,m \in \mathbb{Z}$, ahol $a \neq 0$, $m \geq 2$ és az x ismeretlent is az egész számok körében keressük.*

$$ax \equiv b \pmod{m} \Rightarrow m \mid ax - b \Rightarrow \exists y \in \mathbb{Z} : \; ax - b = my$$

amiből

$$ax - my = b$$

ami egy diophantikus egyenlet, aminek akkor és csak akkor van megoldása, ha $(a, m) \mid b$. Ha van megoldás, akkor a megoldások egyetlen maradékosztályt alkotnak modulo $\frac{m}{(a,m)}$. Tehát ha x_0 egy megoldás, akkor az általános megoldás így fest:

$$x \equiv x_0 \pmod{\frac{m}{(a,m)}}$$

2. Lineáris kongruenciák - feladatok

1. Döntsük el, hogy megoldhatók-e az alábbi kongruenciák és ha igen, oldjuk is meg!

   a.) $3x \equiv 5 \pmod{17}$

   b.) $14x \equiv 8 \pmod{21}$

   c.) $11x \equiv 12 \pmod{18}$

   d.) $26x \equiv 16 \pmod{34}$

   e.) $30x \equiv 48 \pmod{58}$

   f.) $40x \equiv 28 \pmod{62}$

   g.) $104x \equiv 74 \pmod{60}$

2. Egy nyúl ugrál egy szabályos 28-szög csúcsain. Mekkorákat ugorjon, hogy a 10.-dik ugrással a 26-dik csúcsba jusson.
   Megoldás:

   1. $10x \equiv 26 \pmod{28}$, kivonunk 2×28-at a 26-ból, ekkor $10x \equiv -30 \pmod{28}$, majd leosztunk 10-zel, figyelembe véve, hogy $(10, 28) = 2$, tehát a modulust is osztjuk 2-vel: $x \equiv -3 \pmod{14}$
   2. $10x \equiv 26 \pmod{28}$, osszuk le 2-vel: $5x \equiv 13 \pmod{14}$, majd változtassunk mindkét oldalon: $-9x \equiv 27 \pmod{14}$. Osszuk le -9-cel: $x \equiv -3 \pmod{14}$ itt $(-9, 14) = 1$ miatt a modulus maradt változatlan!
   3. $5x \equiv 13 \pmod{14}$ szorozzuk meg 3-mal. $15x \equiv 39 \pmod{14}$, amiből: $x \equiv 11 \pmod{14}$

3. Oldjuk meg kétféleképpen a következő kongruenciát:

$$29x \equiv 17 \pmod{73}$$

4. Oldjuk meg minél egyszerűbben a következő kongruenciákat:

   a.) $202x \equiv 157 \pmod{203}$

   b.) $309x \equiv 451 \pmod{617}$

   c.) $5x \equiv 561 \pmod{1968}$

   d.) $105x \equiv 741 \pmod{809}$

5. Oldjuk meg $32x \equiv 23 \pmod{77}$

6. Melyek megoldhatók az alábbi lineáris diophantikus egyenletek közül:

$$\begin{aligned} 15x + 13y &= 19 \\ 17x + 11y &= 22 \\ 12x + 30y &= 26 \\ 18x + 28y &= 10 \end{aligned}$$

   A megoldhatókat oldjuk is meg!

7. Számítsuk ki 1357^{8642} utolsó két számjegyét (tízes számrendszerben)!

8. Oldjuk meg a következő lineáris kongruenciákat.

   - $4x \equiv 27 \pmod{84}$
   - $4x \equiv 27 \pmod{43}$
   - $4x \equiv 26 \pmod{82}$

Müllner Károly
Email: mullni@hotmail.com
https://mullni.web.elte.hu