SZÁMELMÉLET ELŐADÁS
Összefoglaló

2024. Március 5.

1. Osztók száma, kanonikus alak

1.1. Definíció. *Az f egységtől és 0-tól különböző számot felbonthatatlannak nevezzük, ha csak úgy bontható fel két egész szám szorzatára, hogy valamelyik tényező egység, azaz:*

$$f = ab \;\Rightarrow\; a \;\; vagy \;\; b \;\; egység.$$

1.2. Definíció. *A p egységtől és 0-tól különböző számot prímszámnak (prímnek) nevezzük, ha csak úgy lehet osztója két egész szám szorzatának, ha legalább az egyik tényezőnek osztója, azaz*

$$p \mid ab \;\Rightarrow\; p \mid a \;\; vagy \;\; p \mid b$$

1.1. Tétel. *Az egész számok körében p akkor és csak akkor prím, ha felbonthatatlan.*

1.2. Tétel (Kanoniks alak). *Minden $n > 1$ egész szám felírható*

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r} = \prod_{i=1}^{r} p_i^{\alpha_i}$$

alakban, ahol $p_1, p_2, \ldots, p_r$ különböző prímek és $\alpha_i > 0$ egész. Ez a felírás a $p_i^{\alpha_i}$ prímhatványtényezők sorrendjétől eltekintve egyértelmű.

1.3. Tétel (Osztók száma). *Az*

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$$

kanonikus alakú n egész szám pozitív osztóinak a száma.

$$d(n) = (\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_r + 1)$$

1.4. Tétel. *Ha az a és b pozitív egészek kanonikus alakja*

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r} \quad \text{és} \quad b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_r^{\beta_r}, \quad \text{ahol} \quad \alpha_i \geq 0, \beta_i \geq 0,$$

akkor

$$[a, b] = p_1^{\max(\alpha_1, \beta_1)} p_2^{\max(\alpha_2, \beta_2)} \cdots p_r^{\max(\alpha_r, \beta_r)}$$

illetve

$$(a, b) = p_1^{\min(\alpha_1, \beta_1)} p_2^{\min(\alpha_2, \beta_2)} \cdots p_r^{\min(\alpha_r, \beta_r)}$$

2. Kongruenciák

Oszthatósági kérdések vizsgálatánál gyakran tapasztaljuk, hogy tulajdonképpen csak egy adott számmal való osztási maradék számít, vagyis teljesen egyformán viselkednek azok az egészek, amelyeknek az adott számmal osztva azonos a maradéka. Ez (is) indokolja a következő fogalom bevezetését:

2.1. Definíció (FGY: 2.1.1). *Legyenek a és b egész számok és m pozitív egész. Azt mondjuk, hogy a kongruens b-vel modulo m, ha $m \mid a - b$.*

Jelölés: $a \equiv b \pmod{m}$ vagy röviden $a \equiv b \ (m)$. Az (általában rögzített) m számot modulusnak nevezzük.

Mivel $m \mid a - b \iff m \mid b - a$, ezért

$$a \equiv b \pmod{m} \iff b \equiv a \pmod{m}$$

és így helyes az "a és b kongruensek modulo m" szóhasználat is. (A "modulo m" helyett a "mod m" vagy "az m modulusra nézve" vagy "az m modulus szerint" kifejezéseket is szokás mondani.)

Az is világos, hogy a és b akkor és csak akkor kongruensek modulo m, ha a és b az m-mel osztva ugyanazt a maradékot adják. (Itt maradékon a szokásos legkisebb nemnegatív maradékot értjük, de ugyanez érvényes akkor is, ha - mindkét számnál - a legkisebb abszolút értékű maradékról van szó.)

Ha a és b nem kongruensek modulo m, akkor ezt $a \not\equiv b \pmod{m}$ jelöli, és azt mondjuk, hogy a és b inkongruensek modulo m (vagy a inkongruens b-vel modulo m).

2.1. Tétel (2.1.1). *(i) Minden a-ra* $a \equiv a \pmod{m}$

(ii) $a \equiv b \pmod{m} \Rightarrow b \equiv a \pmod{m}$

(iii) $a \equiv b \pmod{m},\ b \equiv c \pmod{m} \Rightarrow a \equiv c \pmod{m}$

(iv) $a \equiv b \pmod{m},\ c \equiv d \pmod{m} \Rightarrow a + c \equiv b + d \pmod{m}$ *és* $a - c \equiv b - d \pmod{m}$

(v) $a \equiv b \pmod{m},\ c \equiv d \pmod{m} \Rightarrow ac \equiv bd \pmod{m}$

Az (i), (ii) és (iii) tulajdonságok azt fejezik ki, hogy a kongruencia reflexív, szimmetrikus és tranzitív reláció, azaz ekvivalenciareláció. Ennek alapján az egész számokat (páronként) diszjunkt halmazok egyesítésére lehet bontani: egy halmazba kerülnek az "egymással kongruens" számok, vagyis azok, amelyek ugyanolyan maradékot adnak m-mel osztva (az idézőjeles kijelentésnek éppen az (i)–(iii) tulajdonságok alapján van egyáltalán értelme). Ezek a halmazok lesznek a modulo m maradékosztályok, amelyekkel később foglalkozunk.

A (iv) és (v) tulajdonságok alapján a(z ugyanazon modulus szerinti) kongruenciák "összeadhatók, kivonhatók és összeszorozhatók". Ezekből azonnal következik, hogy egy kongruencia mindkét oldalához hozzáadhatjuk ugyanazt a számot, és ugyanez vonatkozik a kivonásra és a szorzásra is, továbbá egy kongruenciát önmagával is akárhányszor összeszorozhatunk, vagyis egy kongruenciát szabad (pozitív egész kitevős) hatványra emelni:

(vi) $a \equiv b \pmod{m} \Rightarrow a + c \equiv b + c \pmod{m}$ és $a - c \equiv b - c \pmod{m}$

(vii) $a \equiv b \pmod{m} \Rightarrow ac \equiv bc \pmod{m}$

(viii) $a \equiv b \pmod{m} \Rightarrow a^n \equiv b^n \pmod{m}$

Mindezek ismételt alkalmazásával az alábbi jól használható összefüggést nyerjük:

(ix) Legyen f egy egész együtthatós polinom. Ekkor:

$$a \equiv b \pmod{m} \Rightarrow f(a) \equiv f(b) \pmod{m}$$

Láttuk, hogy az összeadás, kivonás és szorzás műveletére vonatkozóan a kongruenciák ugyanúgy viselkednek, mint az egyenlőségek. Az osztás műveleténél azonban jelentős eltérés van, két kongruenciát nem szabad egymással elosztani. Először is, osztáskor nem feltétlenül kapunk egész

számokat, és ekkor a hányadosok közötti kongruenciának eleve nem is lehet értelme, hiszen a kongruenciákban egész számoknak kell szerepelniük. Azonban még abban az esetben sem lesz általában igaz az osztáskor kapott kongruencia, ha az osztás után mindkét oldalon egész számok maradnak.

A tiltások után térjünk rá arra, hogy ebben a kérdéskörben mi az, ami megengedett. Csak az osztás speciális esetével, az egyszerűsítéssel foglalkozunk. Az alábbi tétel azt mondja ki, hogy az egyszerűsítést csak úgy lehet elvégezni, hogy közben a modulust is meg kell változtatni:

2.2. Tétel (2.1.3). *Legyen $d = (c, m)$. Ekkor*

$$ac \equiv bc \pmod{m} \iff a \equiv b \pmod{\frac{m}{d}}$$

A 2.1.3 Tétel fontos speciális eseteként kapjuk, hogy ha c és a modulus relatív prímek, akkor a c-vel történő egyszerűsítés után a kongruencia változatlan modulus mellett érvényben marad:

2.3. Tétel (2.1.3A).

$$ac \equiv bc \pmod{m},\ (c, m) = 1 \Rightarrow a \equiv b \pmod{m}$$

3. Lineáris kongruencia, lineáris diofantikus egyenletek

3.1. 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.

3.1. 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:

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

FGY: Freud-Gyarmati: Számelmélet. Nemzeti Tankönyvkiadó Rt., Budapest, 2000.
FL: Fuchs László: Bevezetés az algebrába és a számelméletbe I. Tankönyvkiadó, Budapest, 1964.

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