SZÁMELMÉLET ELŐADÁS
Összefoglaló

2024. Március 19.

1. Maradékosztályok és maradékrendszerek

1.1. Definíció. *Rögzített m modulus mellett az a-val kongruens elemek halmazát az a által reprezentált maradékosztálynak nevezzük. Jelölés:* $(a)_m$.

Az $(a)_m$ maradékosztály tehát egy "mindkét irányban végtelen számtani sorozat", amelynek egyik eleme a és a differenciája m. A modulo m maradékosztályok száma m, és minden maradékosztálynak végtelen sok eleme van. A definíció alapján $(a)_m = (c)_m \iff a \equiv c \pmod{m}$.

1.1. Példa. $(23)_7 = \{\dots, -5, 2, 9, 16, 23, 30, \dots\} = (100)_7$

1.2. Definíció. *Ha rögzített m modulus mellett minden maradékosztályból egy és csak egy elemet kiveszünk, az így kapott számokat modulo m teljes maradékrendszernek nevezzük.*

1.2. Példa. $\{33, -5, 11, -11, -8\}$ *teljes maradékrendszer modulo* 5.

A leggyakrabban a következő teljes maradékrendszereket használjuk:

(A) legkisebb nemnegatív maradékok: $0, 1, \dots, m-1$.

(B) legkisebb abszolút értékű maradékok:

$$0, \pm 1, \pm 2, \dots, \pm\frac{m-1}{2} \quad \text{ha } m \text{ páratlan}$$

illetve

$$0, \pm 1, \pm 2, \dots, \pm\frac{m-2}{2}, \frac{m}{2} \quad \text{ha } m \text{ páros}$$

(nyilván ez utóbbi esetben $m/2$ helyett $-m/2$ is vehető).

Azt, hogy adott számok teljes maradékrendszert alkotnak-e, általában az alábbi egyszerű kritérium alapján tudjuk gyorsan eldönteni:

1.1. Tétel (T 2.2.3). *Adott egész számok akkor és csak akkor alkotnak teljes maradékrendszert modulo m, ha*

(i) számuk m, és

(ii) páronként inkongruensek modulo m.

Ha egy teljes maradékrendszert a modulushoz relatív prím számmal végigszorzunk, és ehhez egy tetszőleges egészt hozzáadunk, akkor ismét teljes maradékrendszert kapunk:

1.2. Tétel (T 2.2.4). *Legyen $r_1, r_2, \ldots, r_m$ teljes maradékrendszer modulo m, $(a; m) = 1$ és b tetszőleges. Ekkor*

$$ar_1 + b, ar_2 + b, \ldots, ar_m + b$$

is teljes maradékrendszer modulo m.

Most azt vizsgáljuk meg, hogy a modulushoz relatív prím egészek hogyan helyezkednek el az egyes maradékosztályokban. Megmutatjuk, hogy egy maradékosztálynak vagy az összes eleme relatív prím a modulushoz, vagy pedig egyetlen eleme sem relatív prím hozzá:

Legyen $a \equiv b \pmod{m}$. Ekkor $(a, m) = 1 \Longleftrightarrow (b, m) = 1$.

Az alábbi tételben ennél erősebb állítást bizonyítunk:

1.3. Tétel (T 2.2.5). $a \equiv b \pmod{m} \Longrightarrow (a, m) = (b, m)$

Fontos szerepet játszanak azok a maradékosztályok, amelyeknek az elemei relatív prímek a modulushoz:

1.3. Definíció (D 2.2.6). *Az $(a)_m$ maradékosztályt modulo m redukált maradékosztálynak nevezzük, ha $(a, m) = 1$.*

1.4. Definíció (Euler-féle φ-függvény). *Tetszőleges n pozitív egész esetén $\varphi(n)$ az $1, 2, \ldots, n$ számok közül az n-hez relatív prímek számát jelenti.*

1.3. Példa.

$$\varphi(1) = 1, \quad \varphi(10) = 4, \quad \varphi(n) = n - 1, \Longleftrightarrow \textit{ ha } n \textit{ prím}$$

.

Világos, hogy $\varphi(n)$ éppen a modulo n redukált maradékosztályok száma. Az n kanonikus alakjából könnyen kiszámítható $\varphi(n)$ értéke.

Most a teljes maradékrendszer mintájára a redukált maradékrendszer fogalmát definiáljuk:

1.5. Definíció (D 2.2.8). *Ha rögzített m modulus mellett minden redukált maradékosztályból egy és csak egy elemet kiveszünk, az így kapott számokat modulo m redukált maradékrendszernek nevezzük.*

1.4. Példa. $\{17, -5, 11, -11\}$ *redukált maradékrendszer modulo* 12.

A legegyszerűbben úgy gyárthatunk redukált maradékrendszereket, ha a legkisebb nemnegatív maradékokból, illetve a legkisebb abszolút értékű maradékokból kiválasztjuk a modulushoz relatív prímeket.

1.4. Tétel (2.2.9). *Adott egész számok akkor és csak akkor alkotnak redukált maradékrendszert modulo m, ha*

(i) számuk $\varphi(n)$

(ii) páronként inkongruensek modulo m, és

(iii) valamennyien relatív prímek m-hez.

1.5. Tétel (2.2.10). *Legyen $r_1, r_2, \ldots, r_{\varphi(m)}$ redukált maradékrendszer modulo m, $(a; m) = 1$. Ekkor*

$$ar_1, ar_2, \ldots, ar_{\varphi(m)}$$

is redukált maradékrendszer modulo m.

2. Az Euler-féle φ-függvény

Most egy olyan képletet tekintünk, amely az n kanonikus alakjának segítségével megadja $\varphi(n)$ értékét:

2.1. Tétel (T 2.3.1). *Legyen n kanonikus alakja*

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r} = \prod_{i=1}^{r} p_i^{\alpha_i}, \quad ahol \;\; \alpha_i > 0.$$

Ekkor

$$\varphi(n) = \left(p_1^{\alpha_1} - p_1^{\alpha_1 - 1}\right) \cdots \left(p_r^{\alpha_r} - p_r^{\alpha_r - 1}\right) = \prod_{i=1}^{r} \left(p_i^{\alpha_i} - p_i^{\alpha_i - 1}\right).$$

Felhívjuk a figyelmet arra, hogy $\varphi(n)$ fenti képlete csak akkor érvényes, ha az n kanonikus alakjában az α_i kitevők valóban pozitívak. A fenti képlet néhány másik, ekvivalens alakja:

$$\varphi(n) = \prod_{i=1}^{r} p_i^{\alpha_i - 1} (p_i - 1) = n \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$$

3. Euler-Fermat-tétel

3.1. Tétel (Euler-Fermat-tétel).

$$(a, m) = 1 \Longrightarrow a^{\varphi(m)} \equiv 1 \pmod{m}$$

Tekintsük most azt a fontos speciális esetet, amikor a modulus egy p prímszám. Ekkor $\varphi(p) = p - 1$ alapján a következő tételt kapjuk:

3.2. Tétel (A "kis" Fermat-tétel egyik alakja). *Ha p prím és $(a, p) = 1$, akkor*

$$a^{p-1} \equiv 1 \pmod{p}$$

3.3. Tétel (A "kis" Fermat-tétel másik alakja). *Ha p prím, akkor bármely a egész számra*

$$a^p \equiv a \pmod{p}$$

3.4. Tétel (Wilson-tétel). *Ha p (pozitív)prím, akkor* $(p-1)! \equiv -1 \pmod{p}$

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