Algebra és számelmélet gyakorlat
2023/2024 I. félév

2023. Október 5.

1. Számelmélet

1.1. Elmélet

1.1. Definíció. *Az f egységtől és 0-tól külöböző 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

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

1.3. 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.*

Példa: $\varphi(1) = 1, \quad \varphi(10) = 4, \quad \varphi(n) = n - 1$, ha n prím.
Világos, hogy $\varphi(n)$ éppen a modulo n redukált maradékosztályok száma. Az n kanonikus alakjából könnyen kiszámítható $\varphi(n)$ értéke:

1.5. Tétel. *Legyen n kanonikus alakja*

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

Ekkor

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

Ezzel ekvivalens alak(ok):

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

ahol p prím.

1.6. Tétel (Euler-Fermat tétel).

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

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

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

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

.

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

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

.

1.2. Gyakorlat

1. Hány osztója van a $11 \cdot 12^2 \cdot 13^3 \cdot 14^4$ számnak?
2. Melyik az a legkisebb n szám, amelyre
   a.) $d(n) = 2$
   b.) $d(n) = 3$
   c.) $d(n) = 6$
3. Keressünk egy olyan n számot, amelyre $d(n) = 4$ és $d(n+1) = 5$.
4. Határozzuk meg azokat a p számokat, amelyre $p, p+2$ és $p+4$ is prím.
5. Mely n számokra lesz $n^4 + 4$ prím?
6. Mely p prímekre lesz $p^2 + 4$ és $p^2 + 6$ is prím?
7. Tekintsük oszthatósági szempontból az $S = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$ számkört.
   a.) Döntsük el, hogy S-ben $12 - 7\sqrt{2}$ osztható-e $3 + 4\sqrt{2}$
   b.) Igazoljuk, hogy S-ben $1 + \sqrt{2}$ egység.
8. Határozzuk meg a $3, 8, 17, -17, 120, 54, -40, 236, 237$ számok legkisebb nemnegatív maradékait modulo 11?
9. Számítsuk ki $\varphi(9)$-et, $\varphi(540)$!
10. Mely n természetes számokra teljesül $\varphi(n) = 1$?
11. A gonosz boszorkány azt állítja, hogy a 109033 számnak van egy 10000 és 15000 közé eső osztója. Bizonyítsuk be, hogy hazudik!

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