Algebra és számelmélet gyakorlat
2023/2024 I. félév

2023. November 23.

1. Emlékeztető

1.1. Előadás (2023. november 15.)

Számelmélet: Fokszám tétel bizonyítása. Wilson tétel (csak az I. bizonyítás volt). Számelméleti függvények. Nevezetes függvények $(d(n), \sigma(n), \omega(n), \Omega(n), \varphi(n))$, ezek multiplikativitása, explicit képlete. Multiplikatív függvény összegzési függvénye is multiplikatív. Möbius féle megfordítási formula (bizonyítás nélkül). *Irodalom:* Elemi Számelmélet jegyzet, 120-125, 132-160 oldal.

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

1.1. Definíció (Wilson prím). *Wilson prímnek nevezünk egy p számot, ha*

$$p^2 | (p-1)! + 1$$

1.2. Definíció (Számelméleti függvény). *Az $f(n)$ függvényt számelméleti függvénynek nevezzük, ha értelmezési tartománya a természetes számok összessége. Értékkészlete lehet komplex vagy valós.*

Példák:

- tetszőleges polinomfüggvény
- logaritmus függvény
- Euler-féle φ függvény

1.3. Definíció (Multiplikatív függvény). *Az $f(n)$ számelméleti függvényt multiplikatívnak nevezzük, ha*

$$f(ab) = f(a)f(b)$$

minden $(a, b) = 1$ számpárra. Ha a $f(ab) = f(a)f(b)$ összefüggés tetszőleges a, b természetes számok mellett is érvényes, akkor a függvényt teljesen multiplikatív függvénynek nevezzük.

1.4. Definíció (Additív függvény). *Az $f(n)$ számelméleti függvényt additívnak nevezzük, ha*

$$f(ab) = f(a) + f(b)$$

minden $(a, b) = 1$ számpárra. Ha a $f(ab) = f(a)+f(b)$ összefüggés tetszőleges a, b természetes számok mellett is érvényes, akkor a függvényt teljesen additív függvénynek nevezzük.

Multiplikatív függvény pl. az Euler-féle φ függvény, additív a logaritmus függvény.

1.5. Definíció. *Egy $n > 0$ egész pozitív osztóinak a számát $d(n)$-nel jelöljük*

1.6. Definíció. *Egy $n > 0$ egész pozitív osztóinak összege $\sigma(n)$-nel jelöljük*

1.7. Definíció (Möbius-függvény). *Legyen n prímtényezos felbontása $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$, ahol $p_1, p_2, \dots, p_r$ különböző prímek és $\alpha_1 \geq 1, \alpha_2 \geq 1, \dots, \alpha_r \geq 1$. Ekkor $\mu(n)$ Möbius-függvényt a következő módon értelmezzük:*

$$\mu(n) = \begin{cases} 1 & \text{ha } n = 1 \\ (-1)^r & \text{ha } \alpha_1 = \dots = \alpha_r = 1 \\ 0, & \text{ha } \exists\, p \text{ prím, hogy } p^2 | n \text{ azaz, ha } n \text{ nem négyzetmentes} \end{cases}$$

példa:

$$\mu(10) = (-1)^2 \quad \mu(20) = 0, \quad \mu(30) = (-1)^3$$

1.8. Definíció. *Az $\omega(n)$ az n különböző pozitív prímosztóinak száma. Amennyiben n prímtényezos felbontása $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$, akkor $\omega(n) = r$, az $\Omega(n)$ függvény pedig a prímosztók száma multiplicitással számolva, vagyis:*

$$\Omega(n) = \alpha_1 + \alpha_2 + \dots + \alpha_r$$

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

1.2. Tétel. *A*

$$d(n), \sigma(n), \mu(n), \varphi(n)$$

függvények multiplikatív számelméleti függvények.

Nevezetes additív függvények a következők:

1.3. Tétel. *Az $\Omega(n)$ függvény teljesen additív, az $\omega(n)$ függvény pedig additív függvény.*

1.4. Tétel. *Az Euler-féle $\varphi(n)$ függvény explicit alakja:*

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_r}\right) = n\prod_{p|n}\left(1 - \frac{1}{p}\right)$$

1.5. Tétel. *A $d(n)$ függvény explicit alakja*

$$(\alpha_1 + 1)(\alpha_2 + 1)\cdots(\alpha_r + 1)$$

ahol az n szám prímtényezos felbontása

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

és $d(1) = 1$

1.6. Tétel. *A $\sigma(n)$ függvény explicit alakja*

$$\sigma(n) = \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{\alpha_2+1} - 1}{p_2 - 1} \cdots \frac{p_r^{\alpha_r+1} - 1}{p_r - 1}$$

ahol az n szám prímtényezos felbontása

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

és $\sigma(1) = 1$

Multiplikatív függvények összegzési függvénye is multiplikatív.

1.7. Tétel. *Legyen $f(n)$ multiplikatív függvény. Ekkor*

$$g(n) = \sum_{d|n} f(d)$$

függvény is multiplikatív.

1.8. Tétel.

$$\sum_{d|n} \varphi(n) = n$$

2. Feladatok

1. Oldjuk meg az alábbi kongruenciákat:

   (1) $14!x \equiv 5 \pmod{17}$

   (2) $(p-3)!x \equiv 1 \pmod{p}$

2. Mi 1357^{8642} utolsó két számjegye (tízes számrendszerben)?

3. Hány pozitív osztója van a 490-nek?

4. Keressük meg azt a legkisebb n természetes számot, melyre $d(n) = 23, 25, 24!$

5. Számítsuk ki $\varphi(n)$ értékeit az $n = 1, 2, 3, \ldots, 12$ behelyettesítési értékeken.

6. Mutassuk meg, hogy $\varphi(5186) = \varphi(5187) = \varphi(5188)$

7. Mennyi 13 rendje modulo 17?

8. Mennyi $2, 3, 71$ rendje modulo 31?

9. Állapítsuk meg 11 rendjét modulo 23, ha tudjuk, hogy $11^{11} \not\equiv 1 \pmod{23}$!

10. Igaz-e, hogy ha $a|b$, akkor $\varphi(a)|\varphi(b)$?

11. Milyen értéket vehet fel egy multiplikatív függvény 1-ben?

12. Milyen lehet egy multiplikatív függvény, ami az 1-ben nullát vesz fel?

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