

Algebra és számelmélet gyakorlat (matematika BSc) 2024/2023 II. félév

2024. November 29.

1. Emlékeztető

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*

$$p^2 \mid (p - 1)! + 1$$

1.2. Definíció (Számelméleti függvény). *Az $f(n)$ függvényt számelméleti függvénynek nevezük, 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 multiplikatívnek nevezük, 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 nevezük.

1.4. Definíció (Additív függvény). Az $f(n)$ számelméleti függvényt *additív*nak 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 prímtényezős 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 prímtényezős 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 $1, 2, \dots, n$ 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 prímtényezős 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 prímtényezős 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.

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

1.10. Definíció. Egy g számot primitív gyöknek nevezünk modulo m , ha

$$o_m(g) = \varphi(m).$$

Pl. modulo 17 összesen 8 darab primitív gyök van. Ezek: 3, 5, 6, 7, 10, 11, 12 és 14.

1.9. Tétel. Ha p prím, akkor modulo p létezik primitív gyök.

1.10. Tétel. Egy g szám akkor és csak akkor primitív gyök modulo m , ha $1, g, g^2, \dots, g^{\varphi(m)-1}$ redukált maradékrendszer modulo m .

1.11. Tétel. Az $m > 1$ modulusra nézve akkor és csak akkor létezik primitív gyök, ha $m = p^\alpha, 2p^\alpha, 2$ vagy 4, ahol $p > 2$ prím és $\alpha > 0$ egész szám.

1.12. Tétel. Legyen a modulus egy p prímszám.

(i) Egy primitív gyök i -edik hatványa akkor és csak akkor primitív gyök, ha $(i, p-1) = 1$.

(ii) A páronként inkongruens primitív gyökök száma $\varphi(p-1)$.

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