Algebra és számelmélet 3 előadás
Számelméleti függvények

Waldhauser Tamás
2014 őszi félév

Tartalom

1. Osztók száma, osztók összege

2. Az Euler-féle φ-függvény

3. Összegzési és megfordítási függvény

Tartalom

1. Osztók száma, osztók összege

2. Az Euler-féle φ-függvény

3. Összegzési és megfordítási függvény

Nevezetes számelméleti függvények

1. Definíció.

Számelméleti függvényen olyan leképezést értünk, amely a természetes számok halmazán van értelmezve, értékei pedig valós (vagy komplex) számok.

2. Definíció.

Definiálunk néhány számelméleti függvényt:

- $\tau(n) = \sum_{d|n} 1$ — n pozitív osztóinak száma;
- $\sigma(n) = \sum_{d|n} d$ — n pozitív osztóinak összege;
- $\mathrm{id}(n) = n$;
- $\mathbf{1}(n) = 1$;
- $\delta(n) = \begin{cases} 1, & \text{ha } n = 1; \\ 0, & \text{ha } n > 1. \end{cases}$

Gyenge multiplikativitás

3. Definíció.

Azt mondjuk, hogy az f számelméleti függvény **gyengén multiplikatív**, ha $f(1) = 1$ és minden $a, b \in \mathbb{N}$ esetén

$$\text{lnko}(a, b) = 1 \implies f(ab) = f(a) \cdot f(b).$$

4. Tétel.

Egy f számelméleti függvény akkor és csak akkor gyengén multiplikatív, ha $f(1) = 1$ és tetszőleges páronként különböző $p_1, \ldots, p_n$ prímszámok és $\alpha_1, \ldots, \alpha_n$ pozitív kitevők esetén

$$f\left(p_1^{\alpha_1} \cdot \ldots \cdot p_n^{\alpha_n}\right) = f\left(p_1^{\alpha_1}\right) \cdot \ldots \cdot f\left(p_n^{\alpha_n}\right).$$

5. Tétel.

A $\tau, \sigma, \text{id}, \mathbf{1}, \delta$ számelméleti függvények gyengén multiplikatívak.

Házi feladat.

Az id, $\mathbf{1}$, és δ függvények gyenge multiplikativitásának igazolása.

Képletek

6. Tétel.

Legyen az n természetes szám prímtényezős felbontása $n = \prod_{i=1}^{k} p_i^{\alpha_i}$. Ekkor

$$\tau(n) = \prod_{i=1}^{k} (\alpha_i + 1);$$

$$\sigma(n) = \prod_{i=1}^{k} \left(1 + p_i + p_i^2 + \cdots + p_i^{\alpha_i}\right) = \prod_{i=1}^{k} \frac{p_i^{\alpha_i+1} - 1}{p_i - 1}.$$

Példa.

$\tau(1500) = ?$, $? = 3 \cdot 2 \cdot 4 = 24$ $\quad \sigma(1500) = ?$ $? = 7 \cdot 4 \cdot 156 = 4368$

Házi feladat.

$\tau(7!) = ?, \quad \sigma(7!) = ?$

Házi feladat.

Melyek azok a számok, amelyeknek pontosan négy osztójuk van?

Házi feladat.

Melyek azok a számok, amelyeknek páratlan sok osztójuk van?

Tökéletes számok

7. Definíció.

Az n természetes számot **tökéletes számnak** nevezzük, ha megegyezik pozitív valódi osztóinak összegével, azaz $\sigma(n) = 2n$.

8. Tétel (Euler tétele).

Az n páros szám akkor és csak akkor tökéletes, ha előáll $n = 2^{p-1}(2^p - 1)$ alakban, ahol p és $2^p - 1$ is prímszám.

Házi feladat.

Az elegendőség (Euklidesz része) igazolása.

Házi feladat.

Bizonyítsa be, hogy minden $n \in \mathbb{N}$ esetén

$$2^n - 1 \text{ prímszám} \implies n \text{ prímszám}.$$

Mersenne-prímek

9. Definíció.

Az $M_n = 2^n - 1$ alakú számokat **Mersenne-számoknak**, az ilyen alakú prímeket **Mersenne-prímeknek** nevezzük.

10. Megjegyzés.

Abból, hogy n prím, még nem következik, hogy M_n is az, például M_{11} nem prím.

Nem ismert, hogy létezik-e végtelen sok Mersenne-prím, tehát azt sem tudjuk, hogy létezik-e végtelen sok páros tökéletes szám. Páratlan tökéletes számot egyet sem ismerünk, de nincs bizonyítva az sem, hogy ilyen nem létezik.

A jelenleg* ismert legnagyobb prímszám is Mersenne-prím: $M_{57\,885\,161}$, ami tízes számrendszerben 17 425 170 számjegyből áll.

*2014.08.21. Forrás: `www.mersenne.org`.

Mersenne-prímek

p	$M_p = 2^p - 1$	$2^{p-1}\left(2^p - 1\right)$	
2	3	6	ókori görögök
3	7	28	ókori görögök
5	31	496	ókori görögök
7	127	8128	ókori görögök
13	8 191	3 3550 336	1456
17	131 071	8 589 869 056	1588, Cataldi
19	524 287	137 438 691 328	1588, Cataldi
31	2 147 483 647	2 305 843 008 139 952 128	1772, Euler
61	$\sim$ 2 trillió	$\sim$ 2 szextillió	1883, Pervushin
89	27-jegyű szám	54-jegyű szám	1911, Powers
107	33-jegyű szám	65-jegyű szám	1914, Powers
127	39-jegyű szám	77-jegyű szám	1876, Lucas
$\vdots$	$\vdots$	$\vdots$	$\vdots$
57 885 161	17 425 170-jegyű szám	34 850 340-jegyű szám	2013, GIMPS

Fermat-prímek

Házi feladat.

Bizonyítsa be, hogy minden $n \in \mathbb{N}$ esetén

$$2^n + 1 \text{ prímszám} \implies n \text{ kettőhatvány.}$$

11. Definíció.

Az $F_n = 2^{2^n} + 1$ alakú számokat **Fermat-számoknak**, az ilyen alakú prímeket **Fermat-prímeknek** nevezzük.

12. Megjegyzés.

Fermat azt sejtette, hogy F_n mindig prím. Az első öt Fermat-szám valóban prím:

$$F_0 = 3,\ F_1 = 5,\ F_2 = 17,\ F_3 = 257,\ F_4 = 65536,$$

de Euler észrevette, hogy $F_5 = 641 \cdot 6\,700\,417$. Minden további Fermat-szám, amit sikerült megvizsgálni (részben számítógéppel), összetettnek bizonyult.
Az általánosan elfogadott sejtés az, hogy csak véges sok Fermat-prím van (valószínűleg csak az első öt).

Tartalom

1. Osztók száma, osztók összege

2. Az Euler-féle φ-függvény

3. Összegzési és megfordítási függvény

Az Euler-féle φ-függvény

13. Definíció.

Jelöljük $\varphi(m)$-mel az m-nél nem nagyobb természetes számok közül azoknak a számát, amelyek m-hez relatív prímek:

$$\varphi(m) = \left|\{a : 1 \leq a \leq m \text{ és } \operatorname{lnko}(a, m) = 1\}\right|.$$

Az így kapott függvényt **Euler-féle φ függvény**nek nevezzük. Tömörebben:

$$\varphi\colon \mathbb{N} \to \mathbb{N},\ m \mapsto \left|\mathbb{Z}_m^*\right|.$$

Példa.

$\varphi(5) = 4$, $\varphi(6) = 2$, $\varphi(10) = 4$, $\varphi(81) = ?$, $? = 54$ $\varphi(216) = ?$ $? = 72$

Házi feladat.

$\varphi(625) = ?$, $\varphi(1000) = ?$

Képletek

14. Tétel.

Az Euler-féle φ függvény gyengén multiplikatív.

15. Tétel.

Legyen az n természetes szám prímtényezős felbontása $n = \prod_{i=1}^{k} p_i^{\alpha_i}$. Ekkor

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

Példa.

$\varphi(1500) = ?$ $? = 2 \cdot 2 \cdot 100 = 400$

Házi feladat.

$\varphi(7!) = ?$

Teljes maradékrendszerek

16. Definíció.

Modulo m **teljes maradékrendszer**nek nevezzük egész számok egy olyan rendszerét, amely minden mod m maradékosztályból pontosan egy elemet tartalmaz.

17. Tétel.

Ha az $a_1, a_2, \ldots, a_m$ egész számok teljes maradékrendszert alkotnak modulo m, és $b, c \in \mathbb{Z}$, $\text{lnko}(c, m) = 1$, akkor $ca_1 + b, ca_2 + b, \ldots, ca_m + b$ is teljes maradékrendszer modulo m.

Példa.

Teljes maradékrendszer-e $1, 11, 21, 31, \ldots, 751, 761$ modulo 77?

Igen, mert 77-en vannak, és páronként inkongruensek, hiszen $\text{lnko}(10, 777) = 1$.

Házi feladat.

Teljes maradékrendszer-e $7, 22, 37, 52, \ldots, 11632, 11647$ modulo 777?

Redukált maradékrendszerek

18. Definíció.

Modulo m **redukált maradékrendszer**nek nevezzük egész számok egy olyan rendszerét, amely minden mod m redukált maradékosztályból pontosan egy elemet tartalmaz.

19. Tétel.

Ha az $a_1, a_2, \ldots, a_{\varphi(m)}$ *egész számok redukált maradékrendszert alkotnak modulo* m*, és* $c \in \mathbb{Z}, \text{lnko}\,(c, m) = 1$*, akkor* $ca_1, ca_2, \ldots, ca_{\varphi(m)}$ *is redukált maradékrendszer modulo* m*.*

Példa.

Redukált maradékrendszer-e $15, 35, 55, \ldots, 295, 315$ modulo 32?

Nem, mert $15 \equiv 175 \pmod{32}$.

Házi feladat.

Redukált maradékrendszer-e $1, 4, 7, \ldots, 157, 160$ modulo 81?

Az Euler–Fermat-tétel

20. Tétel (Euler–Fermat-tétel).

Ha az a egész szám relatív prím az m modulushoz, akkor $a^{\varphi(m)} \equiv 1 \pmod{m}$.

21. Következmény (kis Fermat-tétel).

Ha p prímszám és a nem osztható p-vel, akkor $a^{p-1} \equiv 1 \pmod{p}$.

22. Következmény.

Ha $a \in \mathbb{Z}$ relatív prím az m modulushoz, akkor

$$k_1 \equiv k_2 \pmod{\varphi(m)} \implies a^{k_1} \equiv a^{k_2} \pmod{m}.$$

Példa.

- $2014^{2014} \equiv ? \pmod{7}$ $? \equiv 2 \pmod{7}$.
- $13^{170} \equiv ? \pmod{40}$ $? \equiv 9 \pmod{40}$.
- $303^{4039} \equiv ? \pmod{100}$ $? \equiv 67 \pmod{100}$.

Házi feladat.

- $123^{123} \equiv ? \pmod{11}$
- $10^{188} \equiv ? \pmod{27}$
- $4447^{2018} \equiv ? \pmod{44}$

Tartalom

1. Osztók száma, osztók összege

2. Az Euler-féle φ-függvény

3. Összegzési és megfordítási függvény

Konvolúció

23. Definíció.

Az f és g számelméleti függvények **konvolúció**ján az alábbi képlettel definiált $f * g$ számelméleti függvényt értjük:

$$(f * g)(n) = \sum_{d|n} f(d) \cdot g\left(\frac{n}{d}\right).$$

24. Tétel.

A konvolúció művelete kommutatív és asszociatív, továbbá minden f számelméleti függvényre $f * \delta = \delta * f = f$.

25. Tétel.

Gyengén multiplikatív számelméleti függvények konvolúciója is gyengén multiplikatív.

Összegzési függvény

26. Definíció.

Az f számelméleti függvény **összegzési függvényén** az $F(n) = \sum_{d|n} f(d)$ számelméleti függvényt értjük. Az f függvényt az F függvény **megfordítási függvényének** nevezzük.

Jelölés.

Azt a tényt, hogy F az f összegzési függvénye gyakran egyszerűen csak $f \to F$ jelöli.

27. Tétel.

Gyengén multiplikatív számelméleti függvény összegzési függvénye is gyengén multiplikatív.

28. Tétel.

A tanult nevezetes számelméleti függvények között fennállnak az alábbi összefüggések:

$$\delta \to \mathbf{1} \to \tau, \quad \varphi \to \mathrm{id} \to \sigma.$$

Házi feladat.

$\delta \to \mathbf{1} \to \tau$ és $\mathrm{id} \to \sigma$ bizonyítása.

A Möbius-féle μ-függvény

29. Definíció.

Az n természetes számot **négyzetmentes**nek nevezzük, ha nem osztható egyetlen 1-nél nagyobb négyzetszámmal sem.

30. Megjegyzés.

Könnyű meggondolni, hogy egy szám akkor és csak akkor négyzetmentes, ha prímfelbontásában minden prím csak egyszer (azaz első hatványon) fordul elő.

31. Definíció.

Möbius-függvénynek nevezzük az alábbi képlettel definiált μ számelméleti függvényt:

$$\mu(n) = \begin{cases} 0, & \text{ha } n \text{ nem négyzetmentes;} \\ (-1)^k, & \text{ha } n \text{ előáll } k \text{ különböző prím szorzataként.} \end{cases}$$

32. Tétel.

A Möbius-függvény összegzési függvénye a δ függvény, azaz $\mu \to \delta$.

Házi feladat.

A μ függvény gyenge multiplikativitásának igazolása.

Möbius-féle inverziós formula

33. Tétel (Möbius-féle megfordítási képlet).

Tetszőleges F számelméleti függvény esetén F-nek egyetlen megfordítási függvénye van, mégpedig $F * \mu$.

Másképpen fogalmazva $f \to F$ akkor és csak akkor áll fenn, ha $f = F * \mu$.

Részletesebben: tetszőleges f, F számelméleti függvények esetén

$$\forall n \in \mathbb{N} : F(n) = \sum_{d|n} f(d) \iff \forall n \in \mathbb{N} : f(n) = \sum_{d|n} F(d) \cdot \mu\left(\frac{n}{d}\right).$$

34. Következmény.

Gyengén multiplikatív számelméleti függvény megfordítási függvénye is gyengén multiplikatív.

Példa.

Legyen $f \to F$, ahol $F(n) = n^2$ minden n-re. $f(12) = ?$ $? = 144 - 36 - 16 + 4 = 96$

Házi feladat.

Legyen $f \to F$, ahol $F(n) = \log n$ minden n-re. $f(36) = ?$, $f(81) = ?$

Megértést ellenőrző kérdések

Igazak-e az alábbi állítások?

- A 8219 tökéletes szám.
- Minden n természetes számra $\sum_{d|n} d\mu\left(\frac{n}{d}\right) = \varphi(n)$.
- Az n természetes szám akkor és csak akkor tökéletes, ha $\varphi(n) = 2n$.
- Az identikus függvény összegzési függvénye a σ (osztók összege) függvény.
- Tetszőleges a, m $(m \geq 2)$ egész számok esetén,
  $a \equiv 1 \pmod{m} \implies a^{m-1} \equiv 1 \pmod{m}$.
- Tetszőleges n pozitív egész szám esetén: n prím $\implies 2^n - 1$ prím.
- Bármely két modulo m redukált maradékrendszernek ugyanannyi eleme van.
- Ha n nem négyzetszám, akkor $\mu(n) \neq 0$.