Algebra és számelmélet gyakorlat
2023/2024 I. félév

2023. November 24.

1. Emlékeztető

1.1. Előadás (2023. november 16.)

Számelmélet: Tökéletes számok, barátságos számok, hiányos és bővelkedő számok (a bizonyítások nem szerepeltek). Rend. Rend alaptulajdonságai. *Irodalom:* Elemi Számelmélet jegyzet, 150-160 oldal.

1.1. Definíció. *Az n szám tökéletes, ha pozitív osztóinak összege egyenlő a szám kétszeresével. Vagyis*

$$\sigma(n) = 2n$$

Tökéletes szám pl. a $6, 28, 496, 8128$.

$$\begin{aligned} 2 \cdot 6 &= 1 + 2 + 3 + 6 \\ 2 \cdot 28 &= 1 + 2 + 4 + 7 + 14 + 28 \end{aligned}$$

1.1. Tétel (Eukleidész). *Ha $2^p - 1$ Mersenne-prím, akkor $2^{p-1}(2^p - 1)$ tökéletes szám.*

1.2. Tétel (Euler). *Minden páros tökéletes szám felírható $2^{p-1}(2^p-1)$ alakban, ahol $2^p - 1$ Mersenne prím.*

1.2. Definíció. *Az a és b természetes számok barátságos számok, ha az egyik szám önmagánál kisebb osztóinak összege éppen a másik szám és ez fordítva is igaz. Másképpen megfogalmazva:*

$$\sigma(a) - a = b \quad \textit{és} \quad \sigma(b) - b = a.$$

Például a 220 és 284 barátságos számok, hiszen a 220 megfelelő osztói $1, 2, 4, 5, 10, 11, 20, 22, 44, 55$ és 110, ezek összege 284. Fordítva pedig, 284 megfelelő osztói $1, 2, 4, 71$ és 142, ezek összege 220.

1.3. Tétel (Szábit ibn Kurra). *Legyen n rögzített, $x = 3 \cdot 2^n - 1$, $y = 3 \cdot 2^{n-1} - 1$ és $z = 9 \cdot 2^{2n-1}$. Ha x, y, z prímek , akkor az*

$$a = 2n \cdot x \cdot y \quad \text{és} \quad b = 2n \cdot z$$

számok barátságos számot alkotnak.

1.3. Definíció. *Legyen $(a, m) = 1$. A t pozitív egészet az a rendjének nevezzük modulo m, ha*

$$a^t \equiv 1 \pmod{m}$$

de bármely $0 < i < t$ esetén

$$a^i \not\equiv 1 \pmod{m}$$

Jelölés: $o_m(a)$.

1.1. Állítás (Euler–Fermat-tétel következménye). *Ha $(a, m) = 1$, akkor $o_m(a) \leq \varphi(m)$*

1.2. Állítás. *Ha $(a, m) = (b, m) = 1$ és $a \equiv b \pmod{m}$ akkor $o_m(a) = o_m(b)$.*

1.4. Tétel. *Legyen $(a, m) = 1$ és $t \in \mathbb{N}$, ekkor*

$$a^t \equiv 1 \pmod{m} \iff o_m(a) | t$$

1.5. Tétel. *Legyen $u, v \in \mathbb{N}$, $(a, m) = 1$. Ekkor*

$$a^u \equiv a^v \pmod{m} \iff u \equiv v \pmod{o_m(a)}$$

A rend mindig osztója $\varphi(m)$-nek, ahol m a modulus.

1.6. Tétel. *Legyen $(a, m) = 1$, ekkor $o_m(a) | \varphi(m)$.*

2. Feladatok

1. Az alábbi függvények közül melyek additívak és melyek multiplikatívak?

   (1) $f(n) = \begin{cases} 1 & \text{ha } n = 1 \\ 0, & \text{egyébként} \end{cases}$

   (2) $g(n) = -3\log(n)$

   (3) $h(n) = (-1)^{n+1}$

2. Létezik $f(n)$ multiplikatív függvény, amely az $f(1) = 1$ értéket kivéve csak negatív értékeket vesz fel?

3. Számítsuk ki $\mu(42)$, $\mu(630)$, $\mu(462)$ értékét, ahol $\mu(n)$ a Möbius függvény!

4. Számítsuk ki $\sigma(35)$, $\sigma(103)$, $\sigma(144)$ értékét, ahol $\sigma(n)$ az n pozitív osztóinak összege! Explicit képlete:

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

5. Számítsuk ki a 13 rendjét modulo 59.

6. Számítsuk ki a 17 rendjét modulo 29.

7. Tudjuk, hogy

$$\begin{aligned} 18^{15} &\equiv 1 \pmod{41} \\ 18^{25} &\equiv 1 \pmod{41} \end{aligned}$$

   Mennyi a 18 rendje modulo 41?

8. Végezzük el az alábbi polinomosztásokat:

   (1) $(2x^3 + 2x^2 + 3x + 2) : (x^2 + 1)$

   (2) $(x^3 - 2) : (2x^2 + 2x - 3)$

   (3) $(x^4 - 2x^3 + 4x^2 - 6x + 8) : (x - 1)$

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