Algebra és számelmélet gyakorlat
2023/2024 I. félév

2023. December 07.

1. Emlékeztető

1.1. Előadás (2023. november 29.)

Számelmélet: Primitív gyök, diszkrét logaritmus (index). Binom kongruencia megoldhatósága. Diffie-Hellman kulcscsere, DHP és DLP.
Irodalom: Elemi Számelmélet jegyzet: 161-177 oldal.

1.1. 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.

1.1. Tétel. *Ha p prím, akkor modulo p létezik primitív gyök.*

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

1.3. 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.*

1.4. 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 $\varphi(p-1)$.

1.2. Definíció (Diszkrét logaritmus). *Legyen* p *prím,* g *primitív gyök* $(\mathrm{mod}\ p)$ *és* $(a,p)=1$. *Ekkor* a*-nak a* g *alapú diszkrét logaritmusán vagy indexén azt a* $0 \leq k \leq p-2$ *számot értjük, amelyre*

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

Jelölés: $k = ind_g a$

1.5. Tétel. *Legyen* p *prím és* $(a,p)=1$. *Az*

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

kongruencia akkor és csak akkor oldható meg, ha

$$a^{\frac{p-1}{(k,p-1)}} \equiv 1 \pmod{p}$$

Megoldhatóság esetén a páronként inkongruens megoldások száma $(k, p-1)$.

A második feltétel ekvivalens azzal, hogy

$$(k, p-1) | ind_g a$$

telejsül, ahol g egy tetszőleges primitív gyök

2. Feladatok

1. Tudjuk, hogy $11^{40} \equiv -1 \pmod{17}$. Bizonyítsuk be, hogy 11 primitív gyök modulo 17!

2. Határozzuk meg az összes primitív gyököt modulo m, ha m értéke

$$a.)\ 7; \qquad b.)\ 10; \qquad c.)\ 18.$$

3. Adjunk meg egy olyan számot, amely egyszerre primitív gyök (mod 11) és (mod 14) is.

4. Mely p prímekre lesz $ind_{p,7}(2) = 3$?

5. Keressük meg az alábbi prímekhez a legkisebb pozitív primitív gyököt és készítsünk indextáblázatot!

$$a.)\ 7; \qquad b.)\ 11; \qquad c.)\ 17.$$

6. Oldjuk meg a következő binom kongruenciákat!

   a) $5x^{22} \equiv 6 \pmod{13}$

   b) $3x^3 \equiv 7 \pmod{11}$

   c) $4 \cdot 9^x \equiv 11 \pmod{13}$

7. Oldjuk meg indextáblázat segítségével a

$$5x^6 \equiv 3 \pmod{11}$$

8. Készítsen indextáblázatot modulo 13, majd oldja meg az indextáblázat segítségével az alábbi kongruenciát:

$$49^x \equiv 11 \pmod{13}$$

9. Bontsuk föl a $2x^4 - 4$ polinomot az $\mathbb{R}$ és $\mathbb{C}$ fölött irreducibilis polinomok szorzatára:

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