Algebra és számelmélet gyakorlat
2023/2024 I. félév

2023. November 10.

1. Emlékeztető

1.1. Előadás (2023. október 27.)

Összetett modulusú kongruencia visszavezetése prímhatvány modulusúra. Prímhatvány modulusú kongruenciák megoldása. Fokszám redukció. Fokszám tétel. Elemi Számelmélet jegyzet: 116-121. oldal

1.1. Tétel (Magasabb fokú kongruenciák). *Legyen $n \in \mathbb{N}$, $n > 1$ és $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ az n prímtényezős felbontása, továbbá*

$$f(x) \in \mathbb{Z}[x].$$

Az

$$f(x) \equiv 0 \pmod{n} \tag{1.1}$$

kongruencia pontosan akkor oldható meg, ha megoldható az

$$\begin{aligned} f(x) &\equiv 0 \pmod{p_1^{\alpha_1}} \\ f(x) &\equiv 0 \pmod{p_2^{\alpha_2}} \\ &\vdots \\ f(x) &\equiv 0 \pmod{p_k^{\alpha_k}} \end{aligned}$$

szimultán kongruencia-rendszer. Ha ezek közül valamelyik kongruenciának nincs megoldása, akkor az (1.1) kongruenciának sincs megoldása. Ha a (1.2)-

t alkotó kongruenciáknak $h_1, h_2, \ldots, h_k$ egy-egy megoldása, akkor a (1.1) megoldásai:

$$\begin{aligned} x &\equiv h_1 \pmod{p_1^{\alpha_1}} \\ x &\equiv h_2 \pmod{p_2^{\alpha_2}} \\ &\vdots \\ x &\equiv h_k \pmod{p_k^{\alpha_k}} \end{aligned}$$

szimultán kongruencia-rendszer megoldásai között keresendők.

Egy magas fokú kongruencia esetében a fokszám a modulusnál kisebb számmá redukálható, az alábbi tétel alapján:

1.2. Tétel (Fokszám redukció). *Ha p prím és $f(x) \in \mathbb{Z}[x]$, akkor létezik (egyetlen) olyan g egész együtthatós polinom, amelynek foka legfeljebb $p-1$ (vagy nem létezik foka – azaz az összes együttható 0), és minden $c \in \mathbb{Z}$-re*

$$f(c) \equiv g(c) \pmod{p}$$

1.3. Tétel (Fokszám-tétel). *Legyen p prímszám. Ha $f(x) \in \mathbb{Z}[x]$ egy n-edfokú polinom és van olyan együtthatója, ami nem osztható p-vel, akkor az*

$$f(x) \equiv 0 \pmod{n}$$

kongruenciának legfeljebb n megoldása van

2. Feladatok

2.1. Kínai maradéktétel - folyt.

1. Oldjuk meg a következő kongruencia-rendszert:

$$\begin{aligned} 7x &\equiv 11 \pmod{12} \\ 13x &\equiv 17 \pmod{21} \end{aligned}$$

2. Egy négyjegyű természetes szám 72-vel osztva 46, 127-tel osztva 97 maradékot ad. Melyik ez a szám?

3. Keressük meg a kínai maradéktétel alkalmazásával azt az egytől különböző, legkisebb pozitív egész x számot, amely egyidejűleg kielégíti

az

$$\begin{aligned} x &\equiv 1 \pmod 3 \\ x &\equiv 1 \pmod 5 \\ x &\equiv 1 \pmod 7 \end{aligned}$$

kongruenciákat.

4. Keressük meg a kínai maradéktétel alkalmazásával az összes egész számot, amely egyidejűleg kielégíti az

$$\begin{aligned} x &\equiv 2 \pmod 3 \\ x &\equiv 3 \pmod 5 \\ x &\equiv 5 \pmod 2 \end{aligned}$$

kongruenciákat!

5. Oldjuk meg a kínai maradéktétel alkalmazásával az alábbi kongruenciarendszert:

$$\begin{aligned} x &\equiv 1 \pmod 4 \\ x &\equiv 0 \pmod 3 \\ x &\equiv 5 \pmod 7 \end{aligned}$$

6. Keressük meg a kínai maradéktétel alkalmazásával azokat az egész számokat, amelyek 3-mal osztva 1-et, 4-gyel osztva 2-t, 5-tel osztva 3-at adnak maradékul.

7. Melyek megoldhatók az alábbi szimultán kongruenciák közül? A megoldhatókat oldjuk is meg!

   a.)

$$\begin{aligned} x &\equiv 3 \pmod 5 \\ x &\equiv 4 \pmod 7 \end{aligned}$$

   b.)

$$\begin{aligned} x &\equiv 3 \pmod 6 \\ x &\equiv 6 \pmod 8 \end{aligned}$$

c.)

$$\begin{aligned} x &\equiv 2 \pmod 5 \\ x &\equiv 3 \pmod 6 \\ x &\equiv 4 \pmod 8 \end{aligned}$$

d.)

$$\begin{aligned} x &\equiv 3 \pmod 5 \\ x &\equiv 1 \pmod 6 \\ x &\equiv 7 \pmod 9 \end{aligned}$$

2.2. Prímhatvány modulusú kongruenciák megoldása

1. Oldjuk meg az alábbi kongruenciát úgy, hogy a felírt kongruenciát visszavezetjük prímszámhatvány-modulusú kongruenciákra.

$$3x^2 + 5x - 2 \equiv 0 \pmod{12}$$

2. Oldjuk meg az

$$x^3 + x + 3 \equiv 0 \pmod{125}$$

kongruenciát!

2.3. Rend

2.1. Definíció. *Legyen* $(a, m) = 1$. *A* k *pozitív egészt az* a *rendjének nevezzük modulo* m, *ha* $a^k \equiv 1 \pmod m$, *de bármely* $0 < i < k$ *esetén* $a^i \not\equiv 1 \pmod m$

Az a rendjét $o_m(a)$-val jelöljük. Például $o_7(2) = 3$, $o_{10}(3) = 4$ stb. Az Euler-Fermat-tételből következik, hogy minden $(a, m) = 1$ esetén létezik az a-nak rendje és $o_m(a) \leq \varphi(m)$.
A rend fogalma csak $(a, m) = 1$ esetén értelmezhető: ha $(a, m) \neq 1$, akkor egyáltalán nem létezik olyan $k > 0$ kitevő, amelyre $a^k \equiv 1 \pmod m$ teljesülne.

1. Határozzuk meg az alábbi rendeket:

   a.) $o_{13}(4)$

b.) $o_{13}(2)$

c.) $o_{107}(4)$

d.) $o_{67}(-3)$

2. Melyek azok a prímszámok, amelyekre

a.) $o_p(2) = 8$

b.) $o_p(3) = 5$

c.) $o_p(2) = 6$

2.3.1. Hasznos linkek

modulo m hatványozás
Waldhauser Tamás youtube - Az Euler féle φ függvény

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