Algebra és számelmélet gyakorlat (matematika BSc) 2024/2025 I. félév

2024. November 18.

1. Magasabb fokú kongruenciák

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) meg-

oldásai:

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

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

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