# Számelmélet 2005/2006 ősz
# 8. gyakorlat: Hensel-felemelés

1. Mutassuk meg, hogy tetszőleges $p$ prím, $\alpha$ pozitív egész és $f(x)$ egész együtthatós polinom esetén

   (a) $f(z+p^\alpha y) \equiv f(z) + p^\alpha y f'(z) \ (p^{\alpha+1})$;

   (b) ha $f(z) \equiv 0 \ (p^\alpha)$ és $f'(z) \not\equiv 0 \ (p)$, akkor $f(z+p^\alpha y) \equiv 0 \ (p^{\alpha+1})$ megoldható $y$-ra és a megoldás modulo $p$ egyértelmű.

2. (*Hensel-felemelés*)
   Keressük meg az $5x^{22} \equiv 6 \ (7^2)$ kongruencia összes megoldását!

   (a) Oldjuk meg először $f(x) = 5x^{22} - 6 \equiv 0 \ (7)$-et.

   (b) Ha $f(c) \equiv 0 \ (7)$, számojuk ki $f(c) \mod 7^2$ értékét *gyors hatványozás*sal. Ez a következőt jelenti: határozzuk meg a $c$, $c^2$, $c^4$, $c^8$, $c^{16}$ számokat modulo $7^2$ és használjuk ki, hogy $22 = 16+4+2$ miatt $c^{22} \equiv c^{16}c^4c^2 \ (7^2)$.

   (c) Az $f(x) \equiv 0 \ (7^2)$ megoldását $x = c + 7y$ alakban keressük. Az előző feladat szerint $0 \equiv f(x) = f(c+7y) \equiv f(c) + 7yf'(c) \ (7^2)$.

3. Keressük meg az

   (a) $x^5 - 23 \equiv 0 \ (27)$;

   (b) $x^5 - 23 \equiv 0 \ (25)$;

   (c) $x^{18} + 3x - 4 \equiv 0 \ (49)$;

   (d) $x^{11} + x + 1 \equiv 0 \ (363)$.

   kongruenciák összes megoldását a Hensel-felemelés segítségével.

4. Tegyük fel, hogy $p$ prím, $\alpha \geq 2$ egész és $f(x)$ egész együtthatós polinom, amelyre $f(x_1) \equiv 0 \ (p)$. Bizonyítsuk be, hogy

   (a) amennyiben $f'(x_1) \not\equiv 0 \ (p)$, akkor modulo $p^\alpha$ egyetlen olyan $x_\alpha$ van, amelyre $f(x_\alpha) \equiv 0 \ (p^\alpha)$ és $x_\alpha \equiv x_1 \ (p)$;

   (b) amennyiben $f'(x_1) \equiv 0 \ (p)$, akkor az előbbi egyenlet megoldásainak száma osztható $p$-vel, azaz

   $$|\{x_\alpha \in \mathbb{Z} : \ f(x_\alpha) \equiv 0 \quad (p^\alpha), \ \ x_\alpha \equiv x_1 \quad (p) \quad \text{és } 0 \leq x_\alpha < p^\alpha\}|$$

   osztható $p$-vel.

5. Legyen $p$ prím és jelölje az $f(x) \equiv 0 \ (p)$ kongruencia (modulo $p$ páronként különböző) megoldásainak számát $r$. Lássuk be, hogy

   $$r \equiv -\sum_{a=1}^{p} f(a)^{p-1} \quad (p).$$