7. Számelmélet gyakorlat (2009/2010)

1. Oldd meg az $f(x) = x^6 + 4x - 3 \equiv 0 \ (7^3)$ kongruenciát a következő lépéseken keresztül:

(1) Oldd meg az $f(x) \equiv 0 \ (7)$ kongruenciát, egy megoldást jelöljön c.

(2) Gondold meg, hogy $f'(c)$ mivel kongruens mod 7.

(3) Az $x = c+7t$ helyettesítéssel keresd meg az egyetlen olyan c_2 megoldását az $f(x) \equiv 0 \ (7^2)$ kongruenciának, melyre $c_2 \equiv c \ (7)$.

(4) Az $x = c_2+7^2 s$ helyettesítéssel keresd meg az egyetlen olyan c_3 megoldását az $f(x) \equiv 0 \ (7^3)$ kongruenciának, melyre $c_3 \equiv c \ (7)$.

2. Bizonyítsd be, hogy ha $77 \mid a^2 + b^2$, akkor $77^2 \mid a^2 + b^2$.

3. Legyen p prím. Bizonyítsd be, hogy

(a) ha $o_p(a)$ páratlan, akkor a kvadratikus maradék mod p;

(b) ha g primitív gyök mod p, akkor g kvadratikus nemmaradék mod p.

4. Melyek oldhatók meg az alábbi kongruenciák közül?

(a) $x^2 \equiv 66 \ (191)$;

(b) $x^2 \equiv 94! \ (101)$;

(c) $x^2 \equiv 30 \ (70)$.

5. Mely p prímekre oldhatók meg a következő kongruenciák?

(a) $x^2 \equiv -2 \ (p)$;

(b) $x^2 \equiv 3 \ (p)$;

(c) $x^2 \equiv -3 \ (p)$.

1. HF. Bizonyítsd be, hogy ha $1999 \mid a^2 + 2b^2$, akkor $1999 \mid a$ és $1999 \mid b$.

2. HF. Mely p prímekre oldható meg az $x^4 \equiv 4 \ (p)$ kongruencia?