6. számelmélet gyakorlat (2008/2009)

1. Old meg az alábbi kongruenciákat:

(a) $10x^{84} + 3x + 7 \equiv 0 \ (245)$,

(b) $2x^{20} + 3x + 4 \equiv 0 \ (176)$.

2. Wilson Tétel:

(a) Mennyi $(m-1)!$ maradéka m-el osztva?

(b) Bizonyítsd be, hogy ha $p = 4k - 1$ prím, akkor $(\frac{p-1}{2})! \equiv \pm 1 \ (p)$.

3. Mutass példát olyan 1 főegyütthatós $f \in \mathbb{Z}[x]$ polinómra, melynek a fokánál több gyöke van mod 25.

4. Határozd meg a következő rendeket: $o_{77}(155)$, $o_{100}(199)$, $o_{65}(2)$, $o_{47}(43)$.

5. Legyen p prím és $o_p(a) = 3$.

(a) Bizonyítsd be, hogy $1 + a + a^2 \equiv 0 \ (p)$.

(b) Határozd meg $o_p(1 + a)$-t.

6. Bizonyítsd be, hogy ha $(a, m) = 1$, akkor

$$o_m(a^k) = \frac{o_m(a)}{(o_m(a), k)}.$$

7. Keresd meg a legkisebb pozitív primitív gyököt mod 7, 13 és 17. Készítsd el a hozzájuk tartozó indextáblázatot.

8. Legyen $p > 2$ prím. Milyen maradékot ad az összes páronként inkongruens mod p primitív gyök szorzata p-vel osztva?

9.* Legyenek $a_1, \ldots, a_{\varphi(m)}$ redukált maradékrendszer mod m. Bizonyítsd be, hogy $\sum_{k=1}^{\varphi(m)} o_m(a_i)$ páratlan.

HF. Legyen p prím és $(a, p) = 1$. Milyen maradékot ad $\sum_{k=1}^{o_p(a)} a^k$ illetve $\prod_{k=1}^{o_p(a)} a^k$ p-vel osztva?