6. Számelmélet gyakorlat (2009/2010)

1. Számold ki a következő rendeket: $o_{77}(155)$, $o_{100}(199)$, $o_{65}(2)$, $o_{47}(43)$, $o_{21}(23)$ és $o_{89}(86)$.

2. Legyen p prím és $o_p(a) = 3$.

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

(b) Mennyi lehet $o_p(1 + a)$?

3. Bizonyítsd be, hogy ha $(a, m) = 1$ és $k \in \mathbb{N}$, akkor $o_m(a^k) = \frac{o_m(a)}{(o_m(a),k)}$.

4. Legyen g primitív gyök mod m. Bizonyítsd be, hogy ekkor

(a) g^n pontosan akkor primitív gyök mod m, ha $(n, \varphi(m)) = 1$;

(b) $\varphi(\varphi(m))$ darab páronként inkongruens primitív gyök van mod m.

5. Keresd meg a legkisebb pozitív primitív gyököt mod 13 és készíts hozzá indextáblázatot, majd oldd meg az alábbi binom kongruenciákat:

(a) $3x^5 \equiv 2 \ (13)$;

(b) $3x^{10} \equiv 4 \ (13)$;

(c) $4x^7 + 7x^4 \equiv 0 \ (13)$.

6. Legyen p prím és k egy természetes szám. Milyen maradékot ad p-vel osztva $\sum_{a=1}^{p-1} a^k$?

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

1. HF. Old meg indextáblázat segítségével az $5x^{22} \equiv 6 \ (17)$ kongruenciát.

2. HF. Legyen $p > 2$ prím. Határozd meg a $p - 1$-edik illetve $\frac{p-1}{2}$-edik hatványmaradékokat mod p.