7. számelmélet gyakorlat (2008/2009)

1. Legyen g primitív gyök mod m. Bizonyítsd be az alábbiakat:

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

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

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

3. Keresd meg a legkisebb pozitív primitív gyököt mod 7, 13, és 17. Készítsd el az ezekhez a primitív gyökökhöz tartozó indextáblázatokat.

4. Old meg az alábbi kongruenciákat:

(a) $5x^{22} \equiv 6 \ (13)$,

(b) $3x^5 \equiv 2 \ (13)$,

(c) $5x^{14} \equiv 14x^2 \ (17)$,

(d) $4x^7 + 7x^4 \equiv 0 \ (13)$,

(e) $3x^{10} \equiv 4 \ (13)$.

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

6. Bizonyítsd be, hogy

$$\forall\, n \in \mathbb{N}\backslash\{0,1\}\ \exists\, a,b,c \in \mathbb{N}\ (n \mid a^2+b^2+c^2 \wedge n^2 \nmid a^2+b^2+c^2).$$

7.* Bizonyítsd be, hogy $2n-1$ egész számból mindig kiválasztható n olyan, amelyek összege osztható n-nel.

HF. Legyen p prím. Mi a szükséges és elégséges feltétele annak, hogy létezzen k-adik hatvány-nemmaradék mod p és bármely két k-adik hatvány-nemmaradék szorzata k-adik hatványmaradék legyen?