8. Számelmélet gyakorlat (2009/2010)

1. Bizonyítsd be, hogy

(a) két mod p kvadratikus maradék szorzata mod p kavadratikus maradék;

(b) egy mod p kvadratikus maradék és egy mod p kvadratikus nemmaradék szorzata mod p kvadratikus nemmaradék.

2. Bizonyítsd be, hogy ha $p = 4k \pm 1$ prím, akkor k kvadratikus maradék mod p.

3. Legyen $p > 2$ prím. Határozd meg a $\sum_{k=1}^{p-1} \left(\frac{k}{p}\right)$ összeget illetve a $\prod_{k=1}^{p-1} \left(\frac{k}{p}\right)$ szorzatot.

4. Bizonyítsd be, hogy egy $8n^2 - 1$ alakú számnak minden prímosztója $8k \pm 1$ alakú és hogy biztosan van $8k - 1$ alakú prímosztója.

5. Megoldhatók-e a következő kongruenciák?

(a) $x^2 \equiv 31\ (95)$

(b) $x^2 \equiv 589\ (1999)$

6. Legyen $p > 2$ prím, $a_1, \ldots, a_{p-1}$ és $b_1, \ldots, b_{p-1}$ redukált maradékrendszerek mod p. Lehet-e mod p redukált maradékrendszer $a_1 b_1, \ldots, a_{p-1} b_{p-1}$?

1. HF. Legyen $\left(\frac{k}{97}\right) = -1$, ahol k nem primitív gyök mod 97. Ekkor mennyi $o_{97}(k)$?

2. HF. Bizonyítsd be, hogy egy $12n^2 - 1$ alakú számnak minden prímosztója $12k \pm 1$ alakú és hogy biztosan van $12k - 1$ alakú prímosztója.