TEORIJA BROJEVA U KRIPTOGRAFIJI

5. zadaća

12. 5. 2004.

1. Neka je m prirodan broj sa svojstvom da su brojevi $6m+1$, $12m+1$ i $18m+1$ prosti. Dokažite da je tada broj $n = (6m+1)(12m+1)(18m+1)$ Carmichaelov. Odredite sve prirodne brojeve $m \leq 100$ koji posjeduju gore navedeno svojstvo.

2. Odredite sve baze b sa svojstvom da je Carmichaelov broj 561 jaki pseudoprost broj u bazi b.

3. Nađite najmanji prirodan broj n koji je jaki pseudoprost broj i u bazi 3 i u bazi 5.

4. Nađite neki Lucasov pseudoprosti broj s parametrima 1 i -1, tj. neparan složen broj n sa svojstvom da je $F_{n-\left(\frac{5}{n}\right)} \equiv 0 \pmod{n}$.

5. Pocklingtonovom metodom dokažite da je broj 1048583 prost.

6. Zadana je eliptička krivulja E s jednadžbom $y^2 = x^3 + x$ nad poljem $\mathbb{F}_p$, gdje je $p \equiv 3 \pmod{4}$ prost broj. Odredite red grupe $E(\mathbb{F}_p)$.

Rok za predaju zadaće je 2.6.2004.

Andrej Dujella