KITK/2 – 2. domača naloga (do torka 17. marca, 2008)

1. Dokaži, da imamo pri poljubnem RSA sistemu vsaj 9 čistopisov za katere je $E_k(M) = M$.

2. Spomnimo se naslednjih lastnosti Legendrovega simbola. Če sta p in q lihi praštevili, potem je

   (a) $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$, (b) $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$, (c) $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)(-1)^{(p-1)(q-1)/4}$.

   Naj bo $n \geq 3$ liho naravno število.

   (d) Pokaži, da za lihi naravni števili n_1 in n_2 velja
   $$\frac{n_1 n_2 - 1}{2} \equiv \frac{n_1 - 1}{2} + \frac{n_2 - 1}{2} \pmod 2.$$
   Od tod izpelji $\left(\frac{-1}{n}\right) = (-1)^{(n-1)/2}$.

   (e) Pokaži, da za lihi naravni števili n_1 in n_2 velja
   $$\frac{n_1^2 n_2^2 - 1}{8} \equiv \frac{n_1^2 - 1}{8} + \frac{n_2^2 - 1}{8} \pmod 2.$$
   Od tod izpelji $\left(\frac{2}{n}\right) = (-1)^{(n^2-1)/8}$.

   (f) Pokaži, da za liho naravno število $a \geq 3$, velja $\left(\frac{a}{n}\right)\left(\frac{n}{a}\right) = (-1)^{(a-1)(n-1)/4}$.

3. (a) S pomočjo lastnosti Jacobijevih simbolov izračunaj $\left(\frac{43691}{65537}\right)$.

   (b) Naj bo $n = 624142660586694101446291308147581805825611279851037995772020202145871$. Preveri ali n je ali ni praštevilo (lahko uporabiš MAPLE/MATEMATICA). Dokaži svoj odgovor in opiši kako bi lahko jaz (zlahka) preveril tvoj dokaz. Kopijo števila n boste našli na domači strani.

4. (a) Naj bo p liho praštevilo in n naravno število. Dokaži, da je število rešitev enačbe
   $$x^a \equiv 1 \pmod p$$
   v $\mathbb{Z}_p$ enako $D(a, p-1)$.

   (b) Naj bosta p, q lihi praštevili in $n = pq$. Naj bo $f(x)$ polinom s celoštevilčnimi koeficienti. Naj bo S_n (zaporedoma S_p in S_q) množica rešitev iz $\mathbb{Z}_n$ (zaporedoma $\mathbb{Z}_p$, $\mathbb{Z}_q$) enačbe $f(x) \equiv 0 \pmod n$ (zaporedoma (mod p), (mod q)).
   Dokaži $|S_n| = |S_p| \cdot |S_q|$.

   (c) Naj bo $n = pq$ produkt dveh lihih različnih praštevili in $n = pq$ in naj bo $1 \leq a \leq n-1$. Če je $a^{n-1} \not\equiv 1 \pmod n$, potem imenujemo a **Frematova priča** za n, sicer pa mu pravimo **Frematov lažnjivec** za n. Poišči formulo za število Frematovih lažnjivcev za n.