TEORIJA BROJEVA U KRIPTOGRAFIJI

2. zadaća

18. 2. 2004.

1. Koliko znamenaka ima najmanji prirodan broj n za koji vrijedi

$$\ln^{10} n < e^{\sqrt{\ln n \ln \ln n}} < \sqrt[10]{n} \ ?$$

2. Pokažite kako se pozivima algoritma za problem odluke "Ima li prirodan broj N faktor M takav da je $2 \le M \le k$?", binarnim pretraživanjem, može naći netrivijalni faktor broja 247.

3. Direktno množenje brojeva $x = 2^{2n}u_2 + 2^n u_1 + u_0$ i $y = 2^{2n}v_2 + 2^n v_1 + v_0$ zahtjeva 9 množenja n-bitnih brojeva u_i, v_j. Pokažite da se $x \cdot y$ može izračunati sa samo 5 množenja n-bitnih brojeva. (Uputa: polinom $(u_2t^2 + u_1t + u_0)(v_2t^2 + v_1t + v_0)$ je potpuno određen svojim vrijednostima u $t = -2, -1, 0, 1, 2$.)

4. Neka je $m = 187$, $R = 1000$. Nađite primjere za T koji će pokazati da u Montgomeryjevoj redukciji broj $(T + Um)/R - (TR^{-1} \bmod m)$ može biti jednak 0 i može biti jednak m.

5. Pomoću Montgomeryjevog potenciranja uz $R = 1000$ izračunajte $57^{13} \bmod 187$. Prikažite sve međukorake (z-ove) u računanju.

6. Za sve prirodne brojeve između 32 i 63 odredite njihov NAF prikaz. Kolike su prosječna duljina i prosječna težina svih tih prikaza?

Rok za predaju zadaće je 10.3.2004.

Andrej Dujella