Aspecte Computaţionale în Teoria Numerelor

Examen [1]
26 Martie 2021

Fie z şi l ziua, respectiv, luna din data dumneavoastră de naştere ($z \in \{1, 2, 3, \ldots, 31\}$, $l \in \{1, 2, 3, \ldots, 12\}$) şi $v = 20 + ((2 \cdot z + 3 \cdot l) \; mod \; 13)$. Scrieţi valorile $z, \; l, \; v$ pe foaia de examen.

1. Generaţi aleator două numere, fiecare pe exact 4 cifre (în baza zece) şi calculaţi produsul lor folosind algoritmul lui Karatsuba. Evidenţiati clar cele 3 înmulţiri de numere pe 2 cifre care apar. (1p)

2. Demonstraţi corectitudinea următorului algoritm de reducere modulară modulo p_{224}, unde $p_{224} = 2^{224} - 2^{96} + 1$: (2p)

   `input:` $0 \leq c < p_{224}^2$, $c = (c_{13}c_{12} \cdots c_1c_0)_{2^{32}}$;
   `output:` $c \; mod \; p_{224}$;
   `begin`
   $s_1 := (c_6c_5c_4c_3c_2c_1c_0)_{2^{32}}$; $s_2 := (c_{10}c_9c_8c_7000)_{2^{32}}$; $s_3 := (0c_{13}c_{12}c_{11}000)_{2^{32}}$;
   $s_4 := (c_{13}c_{12}c_{11}c_{10}c_9c_8c_7)_{2^{32}}$; $s_5 := (0000c_{13}c_{12}c_{11})_{2^{32}}$;
   return($(s_1 + s_2 + s_3 - s_4 - s_5) \; mod \; p_{224}$)
   `end`

3. Determinaţi inversul lui v modulo 71 folosind varianta extinsă a unul algoritm pentru determinarea celui mai mare divizor comun
   (1p) pentru alg. Euclid sau (2p) pentru alg. binar

4. Folosind algoritmul lui Garner, rezolvaţi sistemul de ecuaţii (1p)

$$\begin{cases} x & \equiv & v \; mod \; 5 \\ x & \equiv & (v+1) \; mod \; 7 \\ x & \equiv & z \; mod \; 9 \end{cases}$$

5. Determinaţi un lanţ aditiv cât mai scurt pentru numărul $(z + 2v)$. (1p)

6. Calculaţi $7^{(z+2v)} \; mod \; 9$ (1p)

7. Aplicaţi algoritmul Lucas-Lehmer pentru a decide dacă numărul $M_7 = 2^7 - 1$ este prim sau compus. Pentru reducerea modulară modulo M_7, utilizaţi şi algoritmul discutat la curs (măcar pentru unul dintre ultimii trei paşi din algoritm, la alegere) (2p)

[1] Timp de lucru: 80 minute, plus înca maxim 10 minute pentru uploadarea fotografiilor soluţiilor în Google Classroom. La 9.30 fix se incheie preluarea solutiilor.