**Aspecte Computaţionale în Teoria Numerelor**

**Examen** [1]
**2 Aprilie 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 $v = 20 + ((3 \cdot z + 5 \cdot l)\ mod\ 20)$. Scrieţi valorile $z,\ l,\ v$ pe foaia de examen.

1. Descrieţi un algoritm de tip Karatsuba pentru calculul expresiei $a^2$, unde $a \in \mathbf{N}$. Exemplificaţi-l pentru $a = 1000 + v$ (1p)
2. Notăm cu $M(n)$ complexitatea înmulţirii a două polinoame de grad strict mai mic decât $n$ (având, deci, $n$ coeficienţi), aceasta fiind cuantificată prin numărul de operaţii efectuate la nivel de coeficienţi (atenţie, nu se face deosebirea între înmulţiri şi adunări/scăderi). Demonstraţi că, oricare ar fi $n \geq 2$, are loc relaţia $M(n+1) \leq M(n) + 4n$ (2p)
3. Fie $p$ prim şi $a, b, c \in \mathbf{Z}_p$. Arătaţi cum se poate calcula eficient tripletul ($a^{-1}\ mod\ p$, $b^{-1}\ mod\ p$, $c^{-1}\ mod\ p$), folosind o singură operaţie de inversare şi cât mai puţine înmulţiri modulare suplimentare (1p)
4. Folosind Teorema Chineză a Resturilor, calculaţi $v^{29}\ mod\ 105$ (2p)
5. Fie $(a_0, a_1, \ldots, a_t)$ un lanţ aditiv pentru $n$ şi $(b_0, b_1, \ldots, b_s)$ un lanţ aditiv pentru $m$. Cum se pot utiliza/combina cele două lanţuri pentru a forma un lanţ aditiv pentru $n \cdot m$, de lungime $t + s$? Construiţi un lanţ aditiv pentru $8 \cdot v$ (2p)
6. Calculaţi $\left(\frac{v}{71}\right)$ (1p)
7. Utilizând testul lui Pépin, decideţi dacă numărul $2^{2^2} + 1$ este prim (1p)

[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.