Examen [1]
29 Mai, 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 $v = 5 + ((2 \cdot z + 5 \cdot l) \ mod \ 6)$. Scrieţi valorile $z,\ l,\ v$ pe foaia de examen.

1. (a) Demonstraţi corectitudinea următorului algoritm:

```
PrimitiveRootSafePrime(p)
input:  p prime, p = 2q + 1, q odd prime;
output: a, a primitive root modulo p;
begin
   generate randomly γ ∈ {2, 3, ..., p − 2};
   a := (−γ^2) mod p;
   return(a)
end.
```

(2p)

(b) Generaţi a, o rădăcină primitivă modulo 23 (1p)

(c) Calculaţi $\log_a v \ (mod\ 23)$ folosind unul din algoritmii discutaţi la curs (Shanks sau Pollard) (1p)

(d) Calculaţi ordinul lui v modulo 23 (1p)

2. (a) Daţi un exemplu de un număr a din $\mathbf{Z}_{11}^*$ pentru care ecuaţia $x^2 \equiv a \ mod\ 11$ să nu aibă soluţii întregi. Justificaţi răspunsul (1p)

(b) Folosind Lema lui Hensel, determinaţi o rădăcină pătratică a lui a modulo 121, unde $a = v^2$ (1p)

(c) Folosind algoritmul Tonelli-Shanks, determinaţi o rădăcină pătratică a lui a modulo 17, unde $a = v^2 \ mod\ 17$ (non-reziduurile pătratice din $\mathbf{Z}_{17}^*$ sunt $3,\ 5,\ 6,\ 7,\ 10,\ 11,\ 12,\ 14$) (1p)

3. Fie curba eliptică peste $\mathbf{Z}_{11}$ dată prin ecuaţia $y^2 = x^3 + x + 1$. Decompresaţi punctul $\tilde{P} = (1, 1)$ şi calculaţi $3P$. (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.