DIOFANTSKE APROKSIMACIJE I PRIMJENE

5. zadaća

1. Neka je $(n, e) = (32311427, 22100011)$ Bobov javni RSA ključ. Poznato je da tajni eksponent d zadovoljava nejednakost $d < \frac{1}{3}\sqrt[4]{n}$. Odredite d (Bobov tajni RSA ključ) i pomoću njega dešifrirajte šifrat $y = 843$ koji je Alice poslala Bobu.

2. Alice je poslala istu poruku m nekolicini agenata. Eva je presrela šifrate c_1, c_2, c_3 za trojicu agenata čiji su javni ključevi n_1, n_2 i n_3. Poznato je da Alice i agenti koriste RSA kriptosustav s javnim eksponentom $e = 3$. Za zadane

$$\begin{aligned} n_1 &= 407, \qquad c_1 = 356, \\ n_2 &= 533, \qquad c_2 = 281, \\ n_3 &= 551, \qquad c_3 = 468. \end{aligned}$$

   pokažite kako će Eva otkriti poruku m (bez poznavanja faktorizacije modula n_1, n_2, n_3).

3. Primjenite Coppersmithovu metodu na polinom $f(x) = x^2 + ax + b$ uz $m = 1$. Za dovoljno veliki N, metoda nalazi rješenje x_0 kongruencije $f(x_0) \equiv 0 \pmod{N}$ ako je $|x_0| \leq N^\delta$. Odredite eksponent δ.

4. Neka je $P(x) = a_d x^d + \cdots + a_0$ minimalni polinom algebarskog broja α, te neka su $\alpha^{(1)} = \alpha$, $\alpha^{(2)}$, $\ldots$, $\alpha^{(d)}$ korijeni od P. Dokažite da se tada za konstantu $c(\alpha)$ u Liouvilleovom teoremu može uzeti

$$c(\alpha) = a_d^{-1} \prod_{j=2}^{d} (1 + |\alpha| + |\alpha^{(j)}|)^{-1} .$$

5. Dokažite da tvrdnja Rothovog teorema vrijedi za sve $\alpha \in \mathbb{C} \setminus \mathbb{R}$.

Andrej Dujella