Cvičení 5. 4. 2013

Diofantické rovnice jsou rovnice, jejichž řešení hledáme pouze mezi celými (nebo přirozenými) čísly. Obecně je jejich řešení těžké, ale existují na ně užitečné triky. Dneska se naučíme tři takové triky:

1. Počítat modulo nějaké malé číslo.
2. Využít jednoznačného rozkladu na prvočinitele.

Příklad 1. Najděte všechna celočíselná řešení rovnic:

1. $2x + 3y = 5$
2. $x(x + 3) = 4y - 1$
3. $y^3 - x^3 = 91$

Příklad 2. Faktorizujte číslo $N = 6557$, víte-li, že je součinem dvou prvočísel p, q splňujících $|p - q| < 10$ (jde to bez kalkulačky!).

Příklad 3. Jsme útočníci na RSA, známe $n = 851, e = 7$, ale nikoli tajný exponent d.

Zachytili jsme zašifrovanou zprávu $C = 42$ od Alice. Rádi bychom si přečetli, co Alice psala. Přesvědčili jsme ji proto, aby dešifrovala (tj. umocnila na d-tou modulo n) nevinně se tvářící zprávu $M = 270 \equiv 2^e C \pmod{n}$ a sdělila nám výsledek $V = 603$. Jak teď dešifrujeme C?

Kreativní úlohy

Příklad 4. Tři malá prasátka mají každé svůj privátní klíč (d_1, N_1), (d_2, N_2) a (d_3, N_3) a všechna používají veřejný exponent $e = 3$. Červená Karkulka poslala každému prasátku identickou pozvánku M na narozeninovou oslavu zašifrovanou pomocí jeho veřejného klíče, tj. zprávy mají tvar

$$\begin{aligned} C_1 &= M^e \pmod{N_1}, \\ C_2 &= M^e \pmod{N_2}, \\ C_3 &= M^e \pmod{N_3}. \end{aligned}$$

Velký zlý vlk všechny tři zašifrované zprávy zachytil a zná veřejné klíče. Poraďte mu, jak z C_1, C_2, C_3 získat M.