

Fr: Uveďte MR sedem, ada $n=929$ je prvočíslo, s pravděpodobností omylu nejvýš 2%.

Při 3 pokusech mám pravděpodobnost omylu $\frac{1}{9^3} = \frac{1}{729} = 0,015625 < 0,02$, tedy budou mi stačit 3 pokusy.
 1) Zvolím $a=123$ $123 \xrightarrow{29} 18 \xrightarrow{2} 324 \xrightarrow{2} 928 = (-1) \xrightarrow{2} 1 \dots \checkmark$
 2) Zvolím $a=2$ $2 \xrightarrow{29} 883 \xrightarrow{2} 258 \xrightarrow{2} 605 \xrightarrow{2} 928 = (-1) \xrightarrow{2} 1 \dots \checkmark$
 3) Zvolím $a=58$ $58 \xrightarrow{29} 605 \xrightarrow{2} 928 = -1 \xrightarrow{2} 1 \dots \checkmark$

Ano, 929 je prvočíslo.

Fr: Při generování prvočísla $p-1$ byla vygenerovaná posloupnost $621, 221, 73, 75, 49, 22, 3, 2, 2$. Uvěřte, ada bylo generování nesprávné a k tomu použijte MR sedem s možností $s, k=2, s=10$. (Tj. zkoušme všechna prvočísla do $s=10$, a vybereme $k=2$ svídku.)

vygenerujeme si množinu S malých prvočísel, $p < s = 10$, $S = \{2, 3, 5, 7\}$.

posloupnosti nejdříve všechna složená čísla sedem MRS(., 2)

~~621, 221, 73, 75, 49, 22, 3, 2, 2~~ (3, 2, 2)

$$n-1 = 73 \cdot 3 \cdot 2 \cdot 2 = 876, \text{ kdy } n=877.$$

$$\text{MRS}(877, 2), \quad n-1 = 876 = 2^2 \cdot 219$$

Zkouším dělitelnost prvočíslky v S

$$\text{Zkouším } a = 5 : 5 \xrightarrow{219} 159 \xrightarrow{2} 876 = -1 \xrightarrow{2} 1 \quad \checkmark$$

$$\text{Zkouším } a = 102 : 102 \xrightarrow{219} 1 \quad \checkmark$$

Nášli jsme prvočíslo $n=877$ a máme rozklad $n-1$.

Definice: Budu $y \geq 0$ reálné číslo. Přirozené číslo $m \geq 1$ je y -bladké, jestliže každé prvočíslo, které dělí m , je menší nebo rovno y .

Necht $0 \leq y \leq x$ jsou reálná čísla. Označme $\mathbb{P}(y, x)$ počet všech y -bladkých čísel do x (včetně x).

Předměstka
9.5.2019

Kolik je 3-bladkých čísel do 10?

Je jich 7: {1, 2, 3, 4, 6, 8, 9}

Kolik je 3-bladkých čísel do 100?

$$\left. \begin{array}{l} 3^0 \cdot 2^1, \text{ když bude menší nebo rovno } 10^2 \text{? Pro } 0 \leq i \leq 6, \text{ tedy celkem 7 čísel} \\ 3^1 \cdot 2^1, \quad 0 \leq i \leq 5 \Rightarrow 6 \text{ čísel} \\ 3^2 \cdot 2^1, \quad 0 \leq i \leq 3 \Rightarrow 4 \text{ čísla} \\ 3^3 \cdot 2^1, \quad 0 \leq i \leq 1 \Rightarrow 2 \text{ čísla} \\ 3^4 \cdot 2^1, \quad 0 \leq i \leq 0 \Rightarrow 1 \text{ číslo} \end{array} \right\} \begin{array}{l} \text{celkem 20} \\ 3 \text{-bladkých čísel} \end{array}$$

Exponenciální složitost: $\mathcal{O}(n) = \mathcal{O}(2^{\text{len}(n)})$

Subexponenciální složitost: $\mathcal{O}(n) = \mathcal{O}(2^{f(\text{len}(n))})$, kde $f(x) \in \mathcal{o}(x)$

Připominku lineární algebry:

$$c_1(3, 2) + c_2(0, 1) + c_3(3, 2) = 0 \quad \forall \mathbb{Z}_7$$

$$\left. \begin{array}{l} 3c_1 + 0 + 3c_3 = 0 \\ 2c_1 + c_2 + 2c_3 = 0 \end{array} \right\} \text{tahle budeme řešit Gaußovou eliminací. Když budu dělit dle 3,} \quad \begin{array}{l} \text{tahle budeme řešit Gaußovou eliminací. Když budu dělit dle 3,} \\ \text{dělit čílem 3, můžu mít řešení } 3^{-1}, \text{ které v této soustavě neexistuje.} \end{array}$$

$$\left(\begin{array}{ccc|c} 3 & 0 & 3 & 0 \\ 2 & 1 & 2 & 0 \end{array} \right) \xrightarrow{R_1 \rightarrow R_1 - 3R_2} \left(\begin{array}{ccc|c} 1 & 0 & 1 & 0 \\ 2 & 1 & 2 & 0 \end{array} \right) \xrightarrow{R_2 \rightarrow R_2 - 2R_1} \left(\begin{array}{ccc|c} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{array} \right) = \left(\begin{array}{ccc|c} 1 & 0 & a & 0 \\ 0 & 1 & b & 0 \end{array} \right)$$

$\uparrow \uparrow \uparrow$
 $c_1 \quad c_2 \quad c_3$

Zvolíme $c_3 = 1$ a dopocítáme hodnoty c_1 a c_2

$$c_1 = -a = -1 = 6$$

$$c_2 = -b = 0$$

$$c_3 = 1$$

$$\text{Řešení je } (c_1, c_2, c_3) = (-1, 0, 1)$$

Reprezentace prvků v grupě: Nechť G je cyklická群組 řádu n o generátorem a , prvek $b \in G$. Reprezentace prvku $g \in G$ vzhledem ke generátoru a a prvku b je koudu dojice $(s, t) \in \mathbb{Z}_n \times \mathbb{Z}_n$, taková, že $g = a^s \cdot b^t \sim G$. Je-li násobík $1 \in \mathbb{Z}_n^*$, mluvíme o nefiriální reprezentaci.

Tvrzení: Pro koudu $t \in \mathbb{Z}_n$ existuje právě jedno $s \in \mathbb{Z}_n$, tak, že (s, t) je reprezentace prvku g vzhledem ke generátoru a a prvku b .

Dk: s je zadáno, hledáme s : $g = a^s b^t$, $a^s = b^t g^{-1}$, $a^s \in G$. Protože $G = \langle a \rangle$, jde s dopustit, a to jednoznačně.

Tvrzení: Známe-li nefiriální reprezentaci (s, t) prvku 1 vzhledem ke generátoru a , a prvku b , pak můžeme spočítat diskrétní logaritmus: $\text{dlog}_a(b) = -st \sim \mathbb{Z}_n$.

Dk: $\text{dlog}_a(b) = x \sim G$, $a^x = b$. Máme $1 = a^s b^t$, kde $s \in \mathbb{Z}_n^*$.

$$\text{Dosadím: } 1 = a^0 = a^s \cdot (a^x)^t = a^{s+tx}$$

$$0 = s + tx$$

$$tx = -s$$

$$x = -s \cdot t^{-1} \quad \text{inverse existuje protože } t \neq 0 \text{ je } \mathbb{Z}_n^*$$

$$\leftarrow \text{jsem v } G$$

$$\leftarrow \text{jsem v } \mathbb{Z}_n^* \text{ (exponentech)}$$

Př: $\text{N} \mathbb{Z}_{17}^* = \langle 3 \rangle = G$ počítejme $\text{dlog}_3(11)$, a známe $1 = a^s b^t = 3^3 \cdot 11^5$

$$1 = a^0 = a^s \cdot (a^x)^2 \quad 5^{-1} = -3 \sim \mathbb{Z}_{16}^* \text{ bách, exponenty jsou mod 16}$$

$$a^0 = a^s \cdot a^{xt}$$

$$0 = s + xt$$

$$x = -s \cdot t^{-1}$$

$$x = -13 \cdot 5^{-1}$$

$$x = -13 \cdot 5^{-1} = -13 \cdot (-3) = 39 = 7 \text{ mod } 16$$

$$\Rightarrow \text{dlog}_3(11) = 7$$

Algoritmus SEDL - Sub Exponential Discrete Logarithm

Vstup: p, q, a, b , kde $G = \langle a \rangle$ je podgrupa řádu q v grupě \mathbb{Z}_p^* , p, q jsou pročísla, $b \in G$. Nauč $|Z_p^*| = p-1 = q \cdot m$, kde $q \mid m$.

Výstup: $\text{dlog}_a(b)$, nebo bláznka neúspěch.

Tvrzení: Nechť $|Z_p^*| = q \cdot m$, kde p, q jsou pročísla a $q \mid m$, a nechť G je podgrupa řádu q a H je podgrupa řádu m v grupě \mathbb{Z}_p^* . Pak Z_p^* je minimální direktní součin podgrup G a H , tj.:

$$- G \cap H = \{1\}$$

$$- G \cdot H = \mathbb{Z}_p^*$$

$\begin{matrix} G \in G & H \in H \\ \downarrow & \uparrow \end{matrix}$

Amb: $G \times H \cong \mathbb{Z}_p^*$ a každý prvek $z \in \mathbb{Z}_p^*$ lze vyjádat jednoznačně ve formě $z = g \cdot h$

Dk: 1) pro $a \in G \cap H$ platí:

$$a \in G \iff r(a) \mid q \quad \left. \begin{array}{l} \text{lady } r(a) \mid \text{ord}(q, m) \\ a \in H \iff r(a) \mid m \end{array} \right\} \text{lady } r(a) \mid \text{gcd}(q, m), \text{ ale } \text{gcd}(q, m) = 1$$

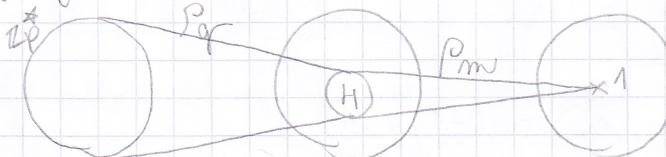
(tikáme, že nutné musí $r(a) \mid 1$, když $r(a) = 1$, a to ophojuje jedinou $a = 1$).

2) Když někdo říká, že $G \cap H = \{1\}$, pak $\varphi: G \times H \rightarrow G \cdot H : (g, h) \mapsto g \cdot h$

(je grupou) isomorfismus. $|G \cdot H| = |G \times H| = q \cdot m = |\mathbb{Z}_p^*|$, tj. $G \cdot H = \mathbb{Z}_p^*$
podgrupa v \mathbb{Z}_p^*

2) Da 2) dosláme, že $\mathbb{Z}_p^* = G \cdot H$ je minimální direktní součin

\mathbb{Z}_p^* je cyklická, $H = P_m = \{x \in \mathbb{Z}_p^* \mid x^m = 1\}$, když $H = \text{ker } P_m = \text{Im } \varphi$



$$\forall a \in \mathbb{Z}_p^*: (ar)^m = a^q \cdot m = a^{p-1} = 1 \text{ dle EF}$$

Poznatek: do H se dostanu, když odklidím možnosti na q .