Čínská věta o zbytcích

Věta[Čínská věta o zbytcích-CRT]

Buďte $m_i \in \mathbb{N}, i = 1, \ldots, k$, m_i vzájemně nesoudělná, $N = \prod_{i=1}^{k} m_i$ a $a_i \in \mathbb{Z}, i = 1, \ldots, k$ libovolná. Potom soustava kongruencí

$$x \equiv a_1 \pmod{m_1}, \quad \ldots, \quad x \equiv a_k \pmod{m_k},$$

má řešení $c = \sum_{i=1}^{k} a_i N_i M_i \pmod{N}$, kde $N_i = N/m_i$, $M_i = N_i^{-1} \bmod m_i$, a pro každé další řešení c' platí $c' \equiv c \pmod{N}$.

Čínská věta o zbytcích

WIKIPEDIE

Čínská věta o zbytcích

Čínská věta o zbytcích (také známa jako **Čínská věta o zbytku** nebo **Čínská zbytková věta**) je matematické tvrzení z modulární aritmetiky. Pojednává o vlastnostech čísel v grupách kongruence modulo n (grupy $\mathbb{Z}_n$). Využívá se v algoritmech pro zpracování velkých čísel nebo v kryptografii. Nejstarší zmínkou o této větě je problém 26 z knihy *Sun-c' Suan Ťing*, kterou ve 3. století našeho letopočtu napsal čínský matematik Sun-c'.

Čínská věta o zbytcích

Existují dvě ekvivalentní znění této věty:

Aritmetická formulace

Předpokládejme, že $m_1, m_2, \dots, m_r$ jsou navzájem po dvou nesoudělná přirozená čísla, $m_i \geq 2$ pro $i = 1, \dots, r$. Potom každá soustava rovnic:

$$
\begin{aligned}
x &\equiv a_1 \pmod{m_1} \\
x &\equiv a_2 \pmod{m_2} \\
&\vdots \\
x &\equiv a_r \pmod{m_r}
\end{aligned}
$$

má řešení x a toto řešení je určeno jednoznačně v modulo $M = m_1 \cdot m_2 \cdot \ldots \cdot m_r$.

Základní pojmy

Algebraická formulace

Nechť $m_1, m_2, \ldots, m_r$ jsou navzájem nesoudělná přirozená čísla, $m_i \geq 2$ pro $i = 1, \ldots, r$. Pak grupy $Z_{m_1} \times \ldots \times Z_{m_r}$ a $Z_{m_1 \cdot \ldots \cdot m_r}$ jsou izomorfní. Izomorfismem je (kromě jiných) zobrazení $f : Z_{m_1 \cdot \ldots \cdot m_r} \to Z_{m_1} \times \ldots \times Z_{m_r}$ dané předpisem $f(x) = (x \; mod \; m_1, \ldots, x \; mod \; m_r)$.

Ekvivalence předchozích dvou formulací

Nechť platí tvrzení "aritmetická formulace". Zobrazení f z tvrzení "algebraická formulace" je homomorfismus zřejmě. Dále $f(x) = (a_1, \ldots, a_r)$ právě tehdy, když x řeší soustavu příslušnou $a_1, \ldots, a_r$. Proto f je prosté díky jednoznačnosti řešení a f je na díky existenci řešení.

Nechť naopak platí „algebraická formulace“, pak zobrazení f^{-1} poskytuje řešení soustavy z „teoreticky číselné formulace“. Jednoznačnost tohoto řešení plyne z prostoty f.

Čínská věta o zbytcích

Použití

Na základě této věty lze vytvořit algoritmus výpočtu zbytku po dělení velké mocniny zadaného čísla. Tento algoritmus má své uplatnění například v šifrovacím protokolu RSA.

Praktická úloha

Pokud vojáky seřadíme do 5 řad, zbudou 4. Pokud je seřadíme do 7 řad, zbude 1. Kolik je vojáků?

Čínská věta říká, že v rozmezí 1 až 35 je právě jedno číslo, které vyhovuje našemu zadání. Řekněme, že vojáků je a. Zapišme problém matematicky.

$$5 * k + 4 = a$$
$$7 * l + 1 = a$$

Pro nějaká přirozená čísla k, l. Jinými slovy

$$a = 4 \pmod 5$$
$$a = 1 \pmod 7$$

Proveďme substituci

$$5 * k + 4 = 1 \pmod 7$$

Přičtěme trojku, abychom se zbavili čtyřky na levé straně

$$5 * k = 4 \pmod 7$$

Chceme se zbavit pětky, proto rovnici vynásobme "inverzem 5", což je v tomto případě 3

$$3 * 5 * k = 3 * 4 \pmod 7$$
$$15 * k = 12 \pmod 7$$
$$1 * k = 5 \pmod 7$$

Vyšlo nám, že k je 5, vojáků je tedy 5*5+4 = 29.

Čínská věta o zbytcích

Další příklad použití

Máme spočíst zbytek čísla 12^{316803} po dělení číslem 26741, neboli v Z_{26741}. Nejprve musíme mít daný prvočíselný rozklad čísla $26741 = 11^2 \cdot 13 \cdot 17$. Protože čísla 11^2, 13 a 17 jsou navzájem nesoudělná, je podle čínské věty o zbytcích číslo 12^{316803} v Z_{26741} určeno jednoznačně svými zbytky po dělení čísly 11^2, 13 a 17.

Následně využijeme faktu, že $a^{\varphi(m)} = 1$ v Z_m (Eulerova funkce) a spočteme tyto zbytky:

$12^{316803} = 12^{110 \cdot 2880+3} = 12^3 = 34$ v Z_{121}
$12^{316803} = 12^{12 \cdot 26400+3} = 12^3 = 12$ v Z_{13}
$12^{316803} = 12^{16 \cdot 19800+3} = 12^3 = 11$ v Z_{17}

(protože $\varphi(11^2) = 110$,$\varphi(13) = 12$,$\varphi(17) = 16$)

Nyní použijeme čínskou vetu o zbytcích, kde $m_1 = 11^2$, $m_2 = 13$ a $m_3 = 17$. Pak platí:
$12^{316803} = (34 \cdot M_1 \cdot N_1) + (12 \cdot M_2 \cdot N_2) + (11 \cdot M_3 \cdot N_3)$ v Z_{26741},
kde

$M_1 = 13 \cdot 17 = 221$
$M_2 = 11^2 \cdot 17 = 2057$
$M_3 = 11^2 \cdot 13 = 1573$

$N_1 = M_1^{-1} = 100^{-1} = 23$ v Z_{121}
$N_2 = M_2^{-1} = 3^{-1} = 9$ v Z_{13}
$N_3 = M_3^{-1} = 9^{-1} = 2$ v Z_{17}
Tudíž $12^{316803} = (34 \cdot 221 \cdot 23) + (12 \cdot 2057 \cdot 9) + (11 \cdot 1573 \cdot 2) = 1728$ v Z_{26741}

Pohligův-Hellmanův algoritmus

Věta

Buď G grupa, $g, \tilde{g}, h, \tilde{h} \in G$, $\tilde{g}$ prvek řádu q^e a předpokládejme, že umíme vyřešit $\tilde{g}^{\tilde{x}} = \tilde{h}$ v $O\left(S\left(q^e\right)\right)$ krocích. Dále nechť g je řádu $N = q_1^{e_1} \cdot q_2^{e_2} \ldots q_k^{e_k}$ a faktorizace N je známa. Potom $g^x = h$ lze řešit v $O(\Sigma_{i=1}^k S(q_i^{e_i}) + \log N)$ krocích následujícím algoritmem:

1. pro $1 \leq i \leq k$ položíme $g_i = g^{N/q_i^{e_i}}$ a $h_i = h^{N/q_i^{e_i}}$,
2. pro $1 \leq i \leq k$ najdeme y_i takové, že $g_i^{y_i} = h_i$, což z předpokladu lze v $O(S(q_i^{e_i}))$ krocích, neboť řád g_i je $q_i^{e_i}$,
3. pomocí CRT najdeme řešení soustavy kongruencí

$$x \equiv y_1 \pmod{q_1^{e_1}}, \quad \ldots, \quad x \equiv y_k \pmod{q_k^{e_k}}$$

Pohligův-Hellmanův algoritmus

Důkaz

Dokažme nejprve, že algoritmus řeší $g^x = h$. Řešení soustavy kongruencí x lze psát jako $x = y_i + q_i^{e_i} z_i$ pro nějaká $z_i \in \mathbb{Z}$. Tedy

$$(g^x)^{N/q_i^{e_i}} = (g^{y_i + q_i^{e_i} z_i})^{N/q_i^{e_i}} = (g^{N/q_i^{e_i}})^{y_i} g^{N z_i} = (g^{N/q_i^{e_i}})^{y_i} = g_i^{y_i} = h_i = h^{N/q_i^{e_i}}.$$

Pro diskrétní logaritmy proto platí kongruence

$$\frac{N}{q_i^{e_i}} x \equiv \frac{N}{q_i^{e_i}} \log_g h \pmod N, \quad \text{pro } \forall i = 1, \ldots, k. \tag{1}$$

Všimneme si, že pro $i \neq j$ sice nejsou $\frac{N}{q_i^{e_i}}, \frac{N}{q_j^{e_j}}$ nesoudělná, ale $\gcd\left(\frac{N}{q_1^{e_1}}, \ldots, \frac{N}{q_k^{e_k}}\right) = 1$. Aplikací rozšířeného Euklidova algoritmu lze najít taková $c_i \in \mathbb{Z}$, že $\frac{N}{q_1^{e_1}} c_1 + \ldots + \frac{N}{q_k^{e_k}} c_k = 1$. Znásobíme-li obě strany (1) číslem c_i a sečteme přes $i = 1, \ldots, k$, dostaneme

$$\sum_{i=1}^{k} \frac{N}{q_i^{e_i}} c_i x \equiv \sum_{i=1}^{k} \frac{N}{q_i^{e_i}} c_i \log_g h \pmod N,$$

z čehož plyne, že $x \equiv \log_g h \pmod N$.

Věta[PHalgoritmus-redukce]

Buď G grupa, q prvočíslo a předpokládejme, že dokážeme řešit $\tilde{g}^{\tilde{x}} = \tilde{h}$ pro $\tilde{g}$ řádu q v $S(q)$ krocích. Je-li g prvek řádu $q^e, e \geq 1$, pak $g^x = h$ lze řešit v $O\left(e(S(q) + \log q)\right)$ krocích.

Pohligův-Hellmanův algoritmus

Důkaz

Neznámý exponent zapíšeme ve tvaru

$$x = x_0 + x_1 q + x_2 q^2 + \ldots + x_{e-1} q^{e-1}, \qquad \text{kde } 0 \leq x_i < q,$$

a postupně určíme $x_0, \ldots, x_{e-1}$. Platí, že

$$h^{q^{e-1}} = (g^x)^{q^{e-1}} = (g^{x_0 + \ldots + x_{e-1} q^{e-1}})^{q^{e-1}} = g^{x_0 q^{e-1}} (g^{q^e})^{x_1 + x_2 q + \ldots + x_{e-1} q^{e-2}} = (g^{q^{e-1}})^{x_0}.$$

Všimneme si, že $g^{q^{e-1}}$ má řád q, takže z předpokladu dokážeme v předchozí rovnosti najít x_0 v $S(q)$ krocích. Podobnou úvahu provedeme pro x_1.

$$h^{q^{e-2}} = (g^x)^{q^{e-2}} = (g^{x_0 + \ldots + x_{e-1} q^{e-1}})^{q^{e-2}} = g^{x_0 q^{e-2}} g^{x_1 q^{e-1}} (g^{q^e})^{x_2 + \ldots + x_{e-1} q^{e-3}} = g^{x_0 q^{e-2}}$$

Jelikož jsme v předchozím kroku určili x_0, nalezneme nyní x_1 jako řešení

$$(g^{q^{e-1}})^{x_1} = (h g^{-x_0})^{q^{e-2}}.$$

Stejným způsobem nalezneme i ostatní koeficienty x_i jako řešení

$$(g^{q^{e-1}})^{x_i} = (h g^{-x_0 - \ldots - x_{i-1} q^{i-1}})^{q^{e-i-1}}.$$

Dohromady tedy máme $O(eS(q))$ kroků potřebných pro řešení dílčích DLP. Měli bychom však ještě započítat všechny potřebné operace násobení (umocňování a inverze), kterých bude $O(e \log q)$, celkem tedy $O\left(e(S(q) + \log q)\right)$.

Příklad

Řešme nyní problém $23^x = 9689 \pmod{11251}$. 23 je generátorem $\mathbb{Z}_{11251}^{\times}$ řádu 11250. Všimneme si, že $11250 = 2 \cdot 3^2 \cdot 5^4$ je součinem malých čísel, takže Pohligův-Hellmanův algoritmus by měl být efektivní. Označíme proto

$$p = 11251, \qquad N = 11250 = 2 \cdot 3^2 \cdot 5^4, \qquad g = 23, \qquad h = 9689.$$

Problém nejprve rozdělíme v souladu s prvním tvrzením na tři.

q	e	$g^{\frac{p-1}{q^e}}$	$h^{\frac{p-1}{q^e}}$	řešení $(g^{\frac{p-1}{q^e}})^y = h^{\frac{p-1}{q^e}}$
2	1	11250	11250	1
3	2	5029	10724	4
5	4	5448	6909	511

Pohligův-Hellmanův algoritmus

Zastavme se pouze u řešení poslední rovnosti $5448^y = 6909$. Z předchozího je zřejmě řád 5448 v $\mathbb{Z}_{11251}^{\times}$ roven 5^4. Zapíšeme proto $y = y_0 + y_1 \cdot 5^1 + y_2 \cdot 5^2 + y_3 \cdot 5^3$. y_0 získáme řešením rovnosti

$$(5448^{5^3})^{y_0} \equiv 6909^{5^3} \pmod{11251},$$

což se ale přímo redukuje na $11089^{y_0} \equiv 11089 \pmod{11251}$ a tedy $y_0 = 1$. Dále řešíme

$$(5448^{5^3})^{y_1} \equiv (6909 \cdot 5448^{-y_0})^{5^2} \equiv (6909 \cdot 5448^{-1})^{5^2} \pmod{11251},$$

což je snadné, neboť stačí vyzkoušet jednu ze čtyř možných hodnot y_1. Jako řešení dostaneme $y_1 = 2$. Následuje řešení

$$(5448^{5^3})^{y_2} \equiv (6909 \cdot 5448^{-y_0 - y_1 \cdot 5})^5 \equiv (6909 \cdot 5448^{-11})^5 \pmod{11251}$$

s výsledkem $y_2 = 0$ a řešení

$$(5448^{5^3})^{y_3} \equiv 6909 \cdot 5448^{-y_0 - y_1 \cdot 5 - y_2 \cdot 5^2} \equiv 6909 \cdot 5448^{-11} \pmod{11251},$$

s výsledkem $y_3 = 4$. Celkem tedy máme $y = 1 + 2 \cdot 5 + 0 \cdot 5^2 + 4 \cdot 5^3 = 511$.
Zbývá použít CRT k řešení soustavy kongruencí

$$x \equiv 1 \pmod{2}, \qquad x \equiv 4 \pmod{3^2}, \qquad x \equiv 511 \pmod{5^4},$$

s výsledkem $x = 4261$. Snadno ověříme, že je splněno $23^{4261} \equiv 9689 \pmod{11251}$.

Pohligův-Hellmanův algoritmus

Příklad 38. Nechť $G = \mathbb{Z}_{73}^*$, $\alpha = 11$ generuje $\mathbb{Z}_{73}^*$ a $\beta = 19$. Prvek α má tedy řád $d = 72$. Pomocí algoritmu Pohlig–Hellman spočítáme $\log_{11} 19$ následovně:

1. Najdeme prvočíselný rozklad čísla 72: $72 = 2^3 \cdot 3^2$.

2. Postupně spočteme pro $p_1 = 2$ a $e_1 = 3$ následující:
   $\overline{\alpha} = \alpha^{d/p_1} = 11^{72/2} \bmod 73 = 72$,
   $\overline{\beta} = \beta_0^{d/p_1} = 19^{72/2} \bmod 73 = 1$, $\log_{\overline{\alpha}} \overline{\beta} = 0$,
   $\overline{\beta} = \beta_1^{d/p_1^2} = 19^{72/2} \bmod 73 = 72$, $\log_{\overline{\alpha}} \overline{\beta} = 1$,
   $\overline{\beta} = \beta_2^{d/p_1^3} = 19^{72/2} \bmod 73 = 1$, $\log_{\overline{\alpha}} \overline{\beta} = 0$.
   Tedy $x_1 = 0 + 1 \cdot 2 + 0 \cdot 2^2 = 2$.

3. Postupně spočteme pro $p_2 = 3$ a $e_2 = 2$ následující:
   $\overline{\alpha} = \alpha^{d/p_2} = 11^{72/3} \bmod 73 = 8$,
   $\overline{\beta} = \beta_0^{d/p_2} = 19^{72/3} \bmod 73 = 64$, $\log_{\overline{\alpha}} \overline{\beta} = 2$,
   $\overline{\beta} = \beta_1^{d/p_2^2} = 19^{72/3} \bmod 73 = 64$, $\log_{\overline{\alpha}} \overline{\beta} = 2$.
   Tedy $x_2 = 2 + 2 \cdot 3 = 8$.

4. Nyní zbývá vyřešit systém kongruencí

$$\begin{aligned} x &\equiv 2 \pmod{8}, \\ x &\equiv 8 \pmod{9}. \end{aligned}$$

Platí

$$\begin{aligned} x &= \left(x_1 \frac{d}{p_1^{e_1}} \left(\left(\frac{d}{p_1^{e_1}} \right)^{-1} \bmod p_1^{e_1} \right) \right. \\ &\quad + \left. x_2 \frac{d}{p_2^{e_2}} \left(\left(\frac{d}{p_2^{e_2}} \right)^{-1} \bmod p_2^{e_2} \right) \right) \bmod d \\ &= (2 \cdot 9 \cdot 1 + 8 \cdot 8 \cdot 8) \bmod 72 = 26, \end{aligned}$$

tedy $\log_{11} 19 = 26$.

Index Calculus

Buď G cyklická grupa řádu N, g její generátor a $h \in G$. Ve své nejjednodušší podobě algoritmus sestává z několika fází.

1. Zvolíme podmnožinu $S = \{p_1, \ldots, p_t\} \subset G$, zvanou *faktorová báze* tak, aby velkou část prvků G bylo možné vyjádřit jako součiny prvků S.
2. Náhodně vybereme ℓ, $0 < \ell < N$ a spočteme g^ℓ. Pokud lze g^ℓ vyjádřit jako součin prvků faktorové báze, najdeme $c_i, i = 1, \ldots, t$, taková, že
$$g^\ell = \prod_{i=1}^{t} p_i^{c_i}, \qquad c_i \geq 0, \tag{2}$$
spočteme logaritmus obou stran a dostaneme lineární kongruenci
$$\ell \equiv \sum_{i=1}^{t} c_i \log_g p_i \pmod{N}. \tag{3}$$
Pokud to nelze, zvolíme jiné ℓ. Tento krok opakujeme pro různé hodnoty ℓ tak dlouho, dokud nemáme dostatek rovnic (3), aby bylo možno vyjádřit všechny $\log_g p_i$ coby řešení soustavy kongruencí.
3. Vyřešíme soustavu kongruencí pro neznámé $\log_g p_i$.
4. Náhodně vybereme k, $0 < k < N$ a spočteme hg^{-k}. Je-li to možné, najdeme $d_i, i = 1, \ldots, t$, taková, že
$$hg^{-k} = \prod_{i=1}^{t} p_i^{d_i}, \qquad d_i \geq 0. \tag{4}$$
Pokud to nelze, zvolíme jiné k. Spočteme logaritmus obou stran (4) a dostaneme
$$\log_g h \equiv \sum_{i=1}^{t} d_i \log_g p_i + k \pmod{N}.$$

Index Calculus

V našem popisu jsme vynechali především postup výběru S, ale také způsob, jak hledat rozklady (2), (4) a řešit (3). Všechny tyto kroky jsou netriviální, především neexistuje způsob jak v obecné grupě G hledat rozklady (2), (4). Vhodné metody pro řešení těchto problémů jsou však známy pro $\mathbb{Z}_p^\times$ a $GF(p^m)^*$.

Index Calculus

Příklad

[Index calculus v $Z^{\times}_{18443}$] $g = 37$ je generátor řádu $N = 18442$ grupy $Z^{\times}_{18443}$. Pro $h = 211$ chceme najít $\log_{37} 211$. Za faktorovou bázi zvolíme první 3 prvočísla, tedy $S = \{2, 3, 5\}$. Po několika stovkách pokusů najdeme taková l, že se povede úspěšně rozložit g^l jako:

$$\begin{aligned} 37^{12708} &\equiv 2^3 \cdot 3^4 \cdot 5 \pmod{18443}, \\ 37^{11311} &\equiv 2^3 \cdot 5^2 \pmod{18443}, \\ 37^{15400} &\equiv 2^3 \cdot 3^3 \cdot 5 \pmod{18443}, \\ 37^{2731} &\equiv 2^3 \cdot 3 \cdot 5^4 \pmod{18443}. \end{aligned}$$

Označíme $\log_{37} 2 = x_2, \log_{37} 3 = x_3, \log_{37} 5 = x_5$. Odtud vychází soustava kongruencí (připomeňme, že $\log_g h$ je definován modulo $p - 1$)

$$\begin{aligned} 12708 &\equiv 3x_2 + 4x_3 + x_5 \pmod{18442}, \\ 11311 &\equiv 3x_2 + 2x_5 \pmod{18442}, \\ 15400 &\equiv 3x_2 + 3x_3 + x_5 \pmod{18442}, \\ 2731 &\equiv 3x_2 + x_3 + 4x_5 \pmod{18442}, \end{aligned}$$

jíž je potřeba řešit.

Index Calculus

Jedná se ale o soustavu kongruencí modulo $p-1 = 2 \cdot 9221$, takže standardní Gaussova eliminační metoda nemusí fungovat, protože některá čísla nemusí mít inverzi. Soustavu proto vyřešíme zvlášť modulo 2 a modulo 9221 Gaussovou eliminací jako

$$(x_2, x_3, x_5) = (1, 0, 1) \pmod 2, \qquad (x_2, x_3, x_5) = (5733, 6529, 6277) \pmod{9221},$$

a teprve potom složíme řešení pomocí CRT jako

$$(x_2, x_3, x_5) = (5733, 15750, 6277) \pmod{18442}.$$

Zvolíme-li $k = 9549$, pak

$$hg^{-k} = 211 \cdot 37^{-9549} \equiv 2^5 \cdot 3^2 \cdot 5^2 \pmod{18443}.$$

Odtud $\log_{37} 211 = (9549 + 5\log_{37} 2 + 2\log_{37} 3 + 2\log_{37} 5) \equiv 8500 \pmod{18442}$. Snadno se přesvědčíme, že se skutečně jedná o hledané řešení.

Definice [Hladká čísla, hladké polynomy]

Celé číslo N nazveme B-hladké, jestliže má všechny prvočíselné dělitele menší nebo rovny B. Polynom f nad konečným tělesem nazveme B-hladký, jestliže jej lze faktorizovat na ireducibilní polynomy stupně maximálně B.

Index Calculus

Za faktorovou bázi S pro řešení DLP v $\mathbb{Z}_p^\times$ se volí prvočísla p_i menší než předem zvolené B. Požadavek existence rozkladů (2), (4) je pak požadavkem, aby levé strany rovností byla B-hladká čísla. Pro malá B lze existenci rozkladů ověřovat efektivně zkusmo dělením. Nízké B umožňuje snáze řešit soustavy kongruencí a jelikož množina S neobsahuje mnoho prvků, není potřeba mnoho různých hodnot l. O to více pokusů je ale potřeba při hledání jednotlivých k a l, neboť pravděpodobnost, že g^l bude B-hladké číslo jistě s klesajícím B klesá. Nechť $\pi(B)$ označuje počet prvočísel menších, nebo rovných B. Potom pro určení řešení soustavy (3) je potřeba najít alespoň $\pi(B)$ čísel g^l která jsou B-hladká. Zároveň (3) musí být nezávislé rovnice, takže kongruencí (3) je zpravidla potřeba vygenerovat o něco více než $\pi(B)$.

Index Calculus

Příklad 44. Nechť $G = \mathbb{Z}_{101}^*$, $\alpha = 2$ generuje $\mathbb{Z}_{101}^*$ a $\beta = 69$. Prvek α má tedy řád $d = 100$. Pomocí algoritmu indexový kalkulus spočítáme $\log_2 69$ následovně:

1. Zvolíme $B = 5$ a naše báze tedy bude $S = \{2, 3, 5\}$.
2. Nyní můžeme postupovat tak, že pro náhodná k aplikujeme na 2^k zkusmé dělení prvky z báze. Zjistíme tak, jaký má 2^k rozklad

Index Calculus

nebo že není 5-hladké. Pokusíme se tak získat rozklad čtyř 5-hladkých čísel.

Pro patnáct z devatenácti náhodně vygenerovaných čísel k nebylo 2^k 5-hladké. Pro $k = 8,\ 5,\ 28,\ 69$ platí tyto rovnosti:

$$\begin{aligned}
2^8 \bmod 101 &= 54 = 2 \cdot 3^3,\\
2^5 \bmod 101 &= 32 = 2^5,\\
2^{28} \bmod 101 &= 80 = 2^4 \cdot 5,\\
2^{69} \bmod 101 &= 3.
\end{aligned}$$

Rovnosti upravíme na následující kongruence:

$$\begin{aligned}
8 &\equiv \log_2 2 + 3\log_2 3 \pmod{100},\\
5 &\equiv 5\log_2 2 \pmod{100},\\
28 &\equiv 4\log_2 2 + \log_2 5 \pmod{100},\\
69 &\equiv \log_2 3 \pmod{100}.
\end{aligned}$$

3. Vyřešení soustavy kongruencí nám dává tyto hodnoty: $\log_2 2 = 1$, $\log_2 3 = 69$ a $\log_2 5 = 24$.
4. Pro šest náhodně vygenerovaných k nebylo číslo $\beta\alpha^k$ 5-hladké. Jako sedmé se vygenerovalo $k = 71$, a tedy jsme získali rovnost

   $$\beta\alpha^k = 69 \cdot 2^{71} \bmod 101 = 20 = 2^2 \cdot 5.$$

   Z rovnosti plyne kongruence

   $$x + 71 \equiv 2\log_2 2 + \log_2 5 \pmod{100},$$

   a tedy $\log_2 69 = (2\log_2 2 + \log_2 5 - 71) \bmod 100 = 55.$