アルゴリズム B 第 15 回

2024 年 1 月 29 日

15　離散対数問題

p を素数とする．p と互いに素な整数 a, b が与えられたとき，

$$a \equiv b^n \pmod{p}$$

を満たす整数 n を（もし存在すれば）求める問題を，**離散対数問題** (discrete logarithm problem, DLP) という．このとき，n を b を底とする a の**離散対数** (discrete logarithm) という．

より一般に，G を群として，与えられた $a, b \in G$ に対して，$a = b^n$ を満たす整数 n を求める問題を離散対数問題という．上の問題は $G = (\mathbb{Z}/p\mathbb{Z})^\times$ の場合である．

以下では，$a = b^n$ を満たす n が存在することは既知として，n を求めるアルゴリズムを考える．b の位数を N とすると，b が生成する G の部分群 $\langle b \rangle = \{b^k \mid k \in \mathbb{Z}\}$ は位数 N の巡回群である．G を $\langle b \rangle$ と置き換えることで，G は位数 N の巡回群，b は G の生成元であり，$a \in G$ と仮定してよい．このとき，$a = b^n$ を満たす整数 n は N を法としてただ 1 つ定まることに注意する．また，e を G の単位元とする．

素朴な方法

$b, b^2, b^3, \ldots$ と計算していき，a に一致するまで続ける．$N = \#G$ なので，$n \leq N$ で $a = b^n$ となり n が見つかる．最悪の場合 $N - 1$ 回の群演算が必要である．この方法は G が有限群であれば，b の位数が不明な場合や，$a = b^n$ かどうか事前に分からない場合も使用できる．

ρ 法

一様に $a^{m_i} b^{n_i} \in G$ を生成することで離散対数問題を解くことを考える．群 G を 3 個の同程度の大きさの集合 S, T, U に分割する．すなわち，$G = S \cup T \cup U$, $S \cap T = T \cap U = U \cap S = \emptyset$ とする．写像 $f \colon G \times (\mathbb{Z}/N\mathbb{Z})^2 \to G \times (\mathbb{Z}/N\mathbb{Z})^2$ を

$$f(g, x, y) = \begin{cases} (ag, x+1, y) & (g \in S) \\ (g^2, 2x, 2y) & (g \in T) \\ (bg, x, y+1) & (g \in U) \end{cases}$$

で定義する．初期値を $(c_1, m_1, n_1) = (e, 0, 0)$ として，$(c_{i+1}, m_{i+1}, n_{i+1}) = f(c_i, m_i, n_i)$ と定める．このとき，$c_i = a^{m_i} b^{n_i}$ $(i = 1, 2, \ldots)$ である．もし $i \neq j$ に対して $c_i = c_j$ となり，$\gcd(m_i - m_j, N) = 1$ ならば，$(m_i - m_j)n \equiv n_j - n_i \pmod{N}$ から n を求めることができる．この方法によって，高確率で $O(\sqrt{N})$ 回の群演算で n が求まる．フロイドの周期発見法を用いることで比較回数を $O(\sqrt{N})$ 回とし，記憶領域の大きさを $O(1)$ にすることができる．

BSGS 法 (baby-step giant-step method)

$m = \lceil \sqrt{N} \rceil$ とする．$a = b^n$ となる n を $0 \leq n < N$ の範囲で取ったとすると，$n = mq + r$ となる整数 $0 \leq q, r < m$ が存在する．このとき，$ab^{-r} = (b^m)^q$ となっている．逆に，この式を満たす q と r が見つかれば n が求まる．

そこで，まず集合 $S = \{ab^{-r} \mid 0 \leq r < m\}$ を計算する．次に，$q = 0, 1, \ldots, m-1$ に対して，$(b^m)^q$ を計算して S 内で探す．一致するとき，$ab^{-r} = (b^m)^q$ より，$n = mq + r$ を得る．

この方法は $O(\sqrt{N})$ 回の群演算と，大きさ $O(\sqrt{N})$ の記憶領域を必要とする．また，S 内での探索にソートと 2 分探索，またはハッシュ表が用いられる．ソートと 2 分探索を用いる場合は G 上の全順序が，ハッシュ表を用いる場合は G 上定義されたハッシュ関数がそれぞれ必要である．

BSGS 法は，b の位数そのものではなく，b の位数の上界 N が既知である場合も同様に使用できる．この性質から，群 G の位数計算に BSGS 法を用いることもある．

ポーリッヒ・ヘルマンのアルゴリズム

ポーリッヒ・ヘルマンのアルゴリズム (Pohlig-Hellman algorithm) では，N の素因数分解 $N = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ が既知であるとする．まず b の位数が素数冪である場合に問題を帰着する．これは次の定理により行われる．

定理 15.1. $i = 1, 2, \ldots, r$ に対して，$q_i = p_i^{e_i}$, $c_i = a^{N/q_i}$, $d_i = b^{N/q_i}$ とおき，整数 y_i は $c_i = d_i^{y_i}$ を満たすとする．このとき，$a = b^n$ であるための必要十分条件は，$n \equiv y_i \pmod{q_i}$ $(i = 1, 2, \ldots, r)$ である．

定理 15.1 より，y_i を計算できれば，中国剰余定理により n を計算できる．

そこで，b の位数が素数冪 $N = p^e$ である場合を考える．$n \equiv \sum_{i=0}^{e-1} x_i p^i \pmod{p^e}$, $x_i \in \{0, 1, \ldots, p-1\}$ として，$x_0, x_1, \ldots, x_{e-1}$ を順に決定する．

$d = b^{N/p}$ として，集合 $T = \{e, d, d^2, \ldots, d^{p-1}\}$ を計算しておく．$a = b^n$ の両辺を N/p 乗すると，$a^{N/p} = d^{x_0}$ となる．$a^{N/p}$ を T から探すことで，x_0 が求められる．

$a = b^n$ より，$ab^{-x_0} = b^{x_1 p + x_2 p^2 + \cdots x_{e-1} p^{e-1}}$ である．両辺を N/p^2 乗すると，$(ab^{-x_0})^{N/p^2} = d^{x_1}$ となる．$(ab^{-x_0})^{N/p^2}$ を T から探すことで x_1 が求められる．

以下同様に繰り返すと $x_0, x_1, \ldots, x_{e-1}$ を計算することができる．アルゴリズムは次のように書ける．

1: DiscreteLogarithmPrimePower(b, a, N, p, e)
2: $L = N/p$, $d = b^L$, $T = \{e, d, d^2, \ldots, d^{p-1}\}$, $f = a$, $g = b^{-1}$
3: **for** $i = 0$ **to** $e - 1$
4: f^L を計算し，T 内で探すことで，$f^L = d^{x_i}$ となる整数 $0 \leq x_i < p$ を求める
5: $L = L/p$, $f = fg^{x_i}$, $g = g^p$
6: **return**$(\sum_{i=0}^{e-1} x_i p^i)$

ポーリッヒ・ヘルマンのアルゴリズムは $O(\sum_{i=1}^{r}(e_i \log N + p_i))$ 回の群演算，中国剰余定理の計算などの整数の計算と，群の要素の比較を必要とする．$p_1, p_2, \ldots, p_r$ が小さいとき，これは非常に高速である．

注意. 以上のアルゴリズムはどんな群でも適用できる方法であるが，指数計算法 (index calculus method) のように，特定の群（例えば $(\mathbb{Z}/p\mathbb{Z})^\times$）に有効な方法も知られている．