アルゴリズム B 演習 No. 13 2013 年 1 月 25 日配布

13. 離散対数問題

G を群とする．**離散対数問題**とは，与えられた $a, b \in G$ に対して，$a = b^n$ を満たす整数 n を（もし存在すれば）求める問題である．n を b を底とする a の**離散対数**という．

離散対数問題の難しさは群 G の性質に依存する．例えば，$G = \mathbb{Z}/N\mathbb{Z}$（加法群）のときは，拡張ユークリッドの互除法によって容易に解くことができる．もとの意味での離散対数問題は，$G = (\mathbb{Z}/p\mathbb{Z})^\times$（$p$ は素数）の場合であり，これは一般には難しい（計算に時間がかかる）問題である．

以下，G は有限巡回群，b は G の生成元であるとして，$N = |G|$ とする．離散対数問題を解くアルゴリズムとして，以下のようなものが知られている．

- **（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 が見つかるか，$n = N$ で $b^n = e$（単位元）となり，$a^n = b$ となる整数 n は存在しないことがわかる．最悪の場合 $N - 1$ 回の群演算が必要である．
- **（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（問題 13-1）．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（問題 12-6）を用いることで比較回数を減らすことができる．）
- **（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，$n + Q = mR$ となる整数 $0 \leq Q < m$, $0 \leq R \leq m$ が存在する．このとき，$ab^Q = (b^m)^R$ 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，ab^Q $(Q = 0, 1, \ldots, m-1)$

と $(b^m)^R$ $(R = 0, 1, \ldots, m)$ を求め，一致するものを探せばよい．この方法では，$O(\sqrt{N})$ 回の群演算が必要である．また，一致するものを探すためにソートと 2 分探索が用いられる．

- 以上のアルゴリズムはどんな有限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．

問題

13-1. ρ 法において，確かに $c_i = a^{m_i} b^{n_i}$ $(i = 1, 2, \ldots)$ となっていることを示せ．

以下では，$G = (\mathbb{Z}/p\mathbb{Z})^\times$, $p = 23$, $b = 5$, $a = 3$ とする．

13-2. 素朴な方法によって $a = b^n$ となる n を求めよ．

13-3. ρ 法によって $a = b^n$ となる n を求めよ．ただし，$S = \{1, 2, \ldots, 7\}$, $T = \{8, 9, \ldots, 14\}$, $U = \{15, 16, \ldots, 22\}$ とする．

13-4. BSGS 法によって $a = b^n$ となる n を求めよ．