2005－CSEC－31（11）
2005／12／9

準離散対数問題の提起

五十嵐 育弘　　児玉　英一郎　　高田　豊雄
ikuiga64@msn.com　kodama@iwate_pu.ac.jp　takata@iwate_pu.ac.jp

岩手県立大学　ソフトウエア情報学研究科

素数を法とする乗法群上の離散対数問題を，単純で，等価な準離散対数問題に還元したので，この問題を提起する．

Raising the Semi-discrete Logarithm Problem

Ikuhiro Igarashi　Eiichiro Kodama　Toyoo Takata

Iwate Prefectural University

Because the discrete logarithm problem was converted into a simpler problem, more equivalent semi-discrete logarithm problem we discuss this problem.

１．はじめに

「準離散対数問題」は筆者の造語である．準離散対数問題に多項式時間計算量の解法アルゴリズムが存在するならば、素数を法とする乗法群上の離散対数問題（以後「離散対数問題」と記述する）は、その解法アルゴリズムを利用して多項式時間計算量で解くことができる．また、準離散対数問題に多項式時間計算量の解法アルゴリズムが存在しないならば、離散対数問題にも多項式時間計算量の解法アルゴリズムが存在しないことになる．

離散対数問題が未解決であるため、準離散対数問題も未解決であり、離散対数問題より準離散対数問題の方が表面上、易しくみえる．そのため、離散対数問題の還元問題である準離散対数問題を提起することにした．

２．離散対数問題とは

素数 p を法とする乗法群の生成元を g 、乗法群の任意の元を y とした場合、(1)式を満たす自然数 x が一意に存在する．

$$y = g^x \bmod p \quad \cdots \quad (1)$$

(1)式において y, g, p が与えられ、これより x を求める問題を離散対数問題と呼ぶ．

(1)式を別の記法で表現をすれば、

$$x = Ind_g y$$

となる．これは、「x は原始元 g を底とする y の指数」という意味で整数論の用語である．’対数’と’指数’が y に対して混同しているが、あくまで表現上の問題である．

離散対数問題の代表的な解法アルゴリズムには、Shanks のベビーステップ・ジャイアントステップアルゴリズム、Pollard の ρ アルゴリズム、Pohlig-Hellman アルゴリズム、指数計算法などがある．これらのアルゴリズムは準指数計算量アルゴリズムである．

２．準離散対数問題の定義

準離散対数問題を３つのタイプで定義する．どのタイプが解決しても離散対数問題の解法に直結する．

タイプ１の定義

２つの集合 A, B を定義する、

$$A \equiv \{x \mid 1 \le x \le \frac{p-1}{2}\}, B \equiv \{x \mid \frac{p+1}{2} \le x \le p-1\}$$

(1)式で、y, g, p が与えられたとき、$x \in A$ か $x \in B$ を決定する問題を、準離散対数問題タイプ１と定義する．

タイプ２の定義

素数 p を法とする乗法群の生成元 g と任意の元 y が与えられたとき $(n, p-1)=1$ である n に対し、$n \mid Ind_g y$ の真偽を判定する問題を、離散対数問題タイプ２と定義する.

タイプ３の定義

$p = a^n(am-l)+1$ 型の素数（$0<l<a$）を法とする乗法群の生成元 g と任意の元 y が与えられたとき、$a^{n+1} \mid Ind_g y$ の真偽を判定する問題を準離散対数問題タイプ３と定義する.

３．離散対数問題への利用

準離散対数問題の解決がどのように離散対数問題の解法に利用できるかを示す.

タイプ１の結果を利用する場合

もし、タイプ１が解決したならば、それを利用して乗法群上の相異なる２つの任意の元の指数の大小を比較できることになる. つまり、$a, b (a \neq b)$ に対して、

$$Ind_g a < Ind_g b$$

の真偽が決定できることなる.
まず、その決定方法を示す.
与えられた $a, b (a \neq b)$ に対して、a の乗法逆元を求める．求め方は、$aX - pY = 1$ を拡張ユークリッドの互除法を用いて X を解く． X が a の乗法逆元 a^{-1} である． a の乗法逆元 a^{-1} と b を掛け合わせたものをタイプ１の解法で判定にかける．つまり、

$$c = a^{-1} \times b \bmod p$$

$$A \equiv \{x \mid 1 \leq x \leq \frac{p-1}{2}\}, B \equiv \{x \mid \frac{p+1}{2} \leq x \leq p-1\}$$

$c \in A$ なのか $c \in B$ なのかを決定する.
もし、$c \in A$ であるなら、$Ind_g a < Ind_g b$ であり、$c \in B$ ならば、$Ind_g a > Ind_g b$ である.
次に、この指数の大小比較可能性を利用して探索対象となる指数 $x = Ind_g y$ を二分探索の手法を用いて探索する．その手順は、

１． $i = 0, m_i = n_i = \dfrac{p-1}{2}$ とおく.
２． $y = g^{n_i}$ であれば n_i が解である.
３． $m_{i+1} = \left\lceil \dfrac{m_i}{2} \right\rceil$ とする.
４． $y < g^{n_i}$ の場合、$n_{i+1} = n_i - m_{i+1}$ とし、
　　$y > g^{n_i}$ の場合、$n_{i+1} = n_i + m_{i+1}$ とする.
５． i を１増やして２．に戻る.

以上の探索回数は、最悪でも $\lceil \log_2(p-1) \rceil$ となり、タイプ１の解法アルゴリズムが多項式時間計算量であるなら、この手法も多項式時間計算量となる.

タイプ２の結果を利用する場合

素数 p を法とする乗法群の任意の元は、$(n, p-1)=1$ となる n で一意の n 乗根をもつ. その求め方は、$nX - (p-1)Y = 1$ を前記同様に拡張ユークリッドの互除法をもちいて X を求める．乗法群上の任意の元を X 乗することにより、その元の n 乗根を求めることができる．この n 乗根演算を活用するために、n を因子にもつ指数を探さなければならない．それは、$n \mid Ind_g y$ の真偽をタイプ２の解法を用いて判定し、これが真になるまで y を g^{-1} 倍することを繰り返して、n を因子にもつ指数を探すことができる.
探索回数は最大 $n-1$ であり、n 乗根演算の最大回数は $\lceil \log_n(p-1) \rceil$ である．タイプ２が多項式時間計算量の解法アルゴリズムであるなら、この手法も多項式時間計算量となる.

タイプ３の結果を利用する場合

$$p = a^n(am-l)+1 \text{ より } m = \frac{(p-1)+a^n l}{a^{n+1}}$$

であるため、$a^{n+1} \mid Ind_g y$ である y に対して m 乗することにより、y の $\dfrac{a}{l}$ 乗根を求めることができる．さらに、$(l, p-1)=1$ であるならば l 乗根を前記の方法で求めることができる.

一般的に a^n+1 型以外は全てこの $a^n(am-l)+1$ 型である．$a^{n+1}\left|Ind_g\, y\right.$ となる指数を探索するための最大探索回数は $a^{n+1}-1$ 回であるため、a^{n+1} の計算可能な上限値がタイプ３の計算量に依存する．タイプ３だけ多項式時間計算量で解ける乗法群が限定されるが、大部分の乗法群に対して有効な解法である．

４．まとめ

素数を法とする乗法群上の離散対数問題を３つの準離散対数問題に還元した．
準離散対数問題タイプ１とタイプ２は離散対数問題と等価であり、タイプ１かタイプ２に多項式時間計算量アルゴリズムが存在するならば離散対数問題にも存在し、タイプ１とタイプ２に多項式時間計算量アルゴリズムが存在しなければ、離散対数問題にも存在しない．
タイプ３だけは離散対数問題と完全に等価ではないが、大部分の乗法群に適用できる．

５．参考文献

1) J.A.ブーフマン著、林芳樹訳「暗号理論入門」シュプリンガー・フェアラーク東京
2) ジョセフ．H．シフヴァーマン著　鈴木治郎訳「はじめての数論」ピアソン・エヂュケーション