論文の内容の要旨

論文題目　On The Discrete Logarithm Problem in Finite Fields
(有限体上の離散対数問題について)

氏　名　張　祺智

位数nの巡回群G、その生成元gとGの元bを与えて、$g^x = b$であるような整数xを求める問題を離散対数問題と言う。

Gが有限体の乗法群や有限体上の楕円曲線の有理点の群の場合において離散対数問題の多項式時間アルゴリズムは知られていない。これらの群上の離散対数問題の困難性は暗号系の構築によく利用されている。だからこれらの群上の離散対数問題の計算量の下限を評価するのは重要かつ難しい問題である。この論文はこの問題を調べる。

第2節で一般的な巡回群における離散対数問題に対する指数時間アルゴリズムを三つ紹介する。2.1節で中国の剰余定理を利用する自然なアルゴリズムを紹介する。群の指数のすべての素因子が小さい場合にこのアルゴリズムは有効である。2.2節でShanksのアルゴリズム（[Shanks 1971]）を紹介する。このアルゴリズムの時間計算量と空間計算量はともに$O(\sqrt{n})$である。2.3節でPollardのアルゴリズム（[Pollard 1978]）を紹介する。このアルゴリズムの時間計算量は$O(\sqrt{n})$であり、空間計算量は$O(1)$である。

第3節で有限体の乗法群における離散対数問題に対する準指数時間アルゴリズムを三つ紹介する。セクション3.1でIndex Calculusアルゴリズムを紹介する。Index Calculusアルゴリズムは1922年にKraitchik氏[Kraitchik 1992]によって提案されて、有限素体の乗法群上の離散対数問題を解くアルゴリズムである。素体$\mathbb{F}_p$の乗法群上の離散対数問題を解く場合にこのアルゴリズムの計算量は$exp(c(\log p)^{\frac{1}{2}}(\log\log p)^{\frac{1}{2}})$である（$c$は正の実数定数である）。3.2節で代数体篩い法を紹介する。代数体篩い法は最初1993年に因数分解アルゴリズムとして提案された。後その類似としての離散対数アルゴリズムが発見された（[Gordon 1993]）。素体$\mathbb{F}_p$の乗法群上の離散対数問題を解く場合にこのアルゴリズムの計算量は$exp((\frac{64}{9}+o(1))(\log p)^{\frac{1}{2}}(\log\log p)^{\frac{1}{2}})$と予想される。3.3節で関数体篩い法を紹介する。関数体篩い法は1994年にAdleman氏によって提案されて、1999年にAdleman氏とHuang氏によって改良された（[Adleman and Huang 1999]）。有限体$\mathbb{F}_q$の乗法群上の

離散対数問題を解く場合にこのアルゴリズムの計算量は$exp(c(\log q)^{\frac{1}{2}}(\log\log q)^{\frac{1}{2}})$と予想される。

離散対数問題の計算量下限を評価するため、直接この問題を解くアルゴリズムを探す他にこの問題と同値な問題を探す手法もある。2009年にHuang氏とRaskind氏は有限素体上の離散対数問題を実2次体と結びつけた（[Huang-Raskind 2009]）。彼らは実2次体に対してramification signatureというものを定義し、ある二つの仮定の下で、有限素体上の離散対数問題と実2次体上のramification signatureの計算問題の同値性を証明した。仮定の一つは実2次体の類数に関するもので、もう一つは実2次体のある単数に関する仮定である。この仕事を第4節で紹介する。

この論文の主要部である第5節では実二次体のramification signatureを一般化する。もとのramification signatureは「pとlは両方分解する」という場合に定義されたが、このセクションでは「pが不分岐でlが分解する」という場合へ一般化する。それから有限素体と位数が素数の平方であるような有限体上の乗法群上の離散対数問題と実2次体上のramification signatureの計算問題の同値性をある仮定の下で証明する。この仮定は実2次体の類数に関する仮定である。特に、Huang氏とRaskind氏の証明から単数に関する仮定を削除してもよいということを示す。具体的には、実2次体と単数を構成するアルゴリズムを改良し（本文の5.3節のStep 4）、[Huang-Raskind 2009]の中の4.1節の命題2の条件(2), (3)が自動的に満たされるようにする。

References

[Adleman and Huang 1999] L.M. Adleman, M.-D. Huang, Function field method for discrete logarithms over finite fields, Inform. and Comput. 151:1-2 (1999), 5-16.

[Buhler 1993] J.P. Buhler, H.W. Lenstra, Jr., C. Pomerance, Factoring Integers with the Number Field Sieve, in A.K. Lenstra and H.W. Lenstra, Jr. (eds), The Development of the Number Field Sieve, Lecture Notes in Mathematics 1554, Springer-Verlag, New York, 1993, pp. 50-94

[Gordon 1993] D.M.Gordon, "Discrete logarithms in GF(p) using the number field sieve", SIAM J. Discrete Math. 6:1 (1993), 124-138

[Huang-Raskind 2009] Ming-Deh Huang and Wayne Raskind , Global Duality, Signature Calculus and the Discrete Logarithm Problem, LMS Journal of Computation and Mathematics , Volume 12 , Jan 2009 , pp 228-263.

[Kraitchik 1992] M. Kraitchik, Thorie des nombres, Gauthier–Villards, 1922

[Pollard 1978] Pollard, J. M. (1978). "Monte Carlo methods for index computation (mod p)". Mathematics of Computation 32 (143): 918924. JSTOR 2006496.

[Shanks 1971] D. Shanks. Class number, a theory of factorization and genera. In Proc. Symp. Pure Math. 20, pages 415440. AMS, Providence, R.I., 1971.