数学アルゴリズム問題の研究調査
Investigation on Mathematical Algorithmic Problems

佐藤孝和[1*]
Takakazu Satoh[1]

[1]埼玉大学　理学部数学科
Department of Mathematics, Faculty of Science, Saitama University

本研究調査は数学問題の中でも有限体上定義された楕円曲線の有理点のなす群上の離散対数問題（以下、楕円型離散対数問題という）および関連する緒問題に対して現在までにどのようなアルゴリズムが知られているかを調査することを目的とする。

このため、以下の項目に関して調査・考察を行った。

(a) 特定の曲線の性質に影響されずに楕円型離散対数問題を解くためのアルゴリズムの調査を行う。これらを考慮した上で楕円型離散対数問題が容易には解けなくなるようにするための留意点をまとめる。

(b) 特殊なクラスの楕円型離散対数問題（例えば Koblitz 曲線上での楕円型離散対数問題）で特に効率の良い解法があるかどうかを調査する。

(c) 有限体上の楕円曲線が与えられたときその有理点のなす群の位数を計算という問題について現在知られているアルゴリズムを調査する。

その結果、(a)(b) に関しては、Shanks 法（いわゆる Baby Step Giant Step, BSGS）、乗法群への埋め込み、加法群への埋め込み、自己同型法、Weil 降下法、Xedni 計算法などが調査対象となった。このうち、Shanks 法はどのような場合にも適用できる。乗法群への埋め込み、加法群への埋め込み、自己同型法は適用対象となる曲線がはっきり分かっている。これに対して残りの方法はそれらが有効となるための必要条件が得られていない。ただし Weil 降下法については必要条件が判明しつつある。位数が 160 bit を越える場合には調査時点において Shanks 法の実行は非現実的であると考えられているので Xedni 計算法を除き残りの解法を受け付けないような曲線の条件をまとめることができた。

(c) に関して、現在知られている方法は l-adic 法か p-adic 法に分類される。m を乗算指数、p を標数とし、q を係数体の位数、$q=p^N$ とおく。知られている最も速い l-adic 法が必要とする bit 演算の数は経験測として $O((\log q)^{2m+2})$ とされていたが、この経験則が成り立たない楕円曲線が頻度は少ないが無限にあることが知られていること、p-adic 法では実用上も理論上も $O(N^{2m})$ であることが分かった。

* 〒 338-8570 さいたま市桜区下大久保 255　電話：048-858-3346　FAX：048-858-3699
Email: cr3dsato@rimath.saitama-u.ac.jp