標数２の体上での楕円曲線の位数計算

福 士 広 大† 一 條 健 司† 吉 岡 良 雄†

楕円曲線暗号システムの構築の際に重要となるのは，楕円曲線の有理点群の位数である．総当り的方法で位数を計算することは有限体のサイズが大きくなると現実的に不可能となるため，現在様々な位数計算アルゴリズムが考案されている．本研究では C++による標数 2 の有限体上の楕円曲線用計算ライブラリを開発し，位数計算アルゴリズムである Schoof のアルゴリズムと Schoof-Elkies-Atkin(SEA) アルゴリズムを実装した．作成したプログラムを用いてランダムな曲線に対する位数を計算し，現実的な時間内に位数が計算できるかどうか検証する．

Calculating Rational Points over Elliptic Curve on $\mathbb{F}_{2^n}$

Kodai Fukushi,† Kenji Ichijo† and Yoshio Yoshioka†

The number of rational points on an elliptic curve becomes important in the case of construction of an elliptic curve cryptosystem. If the size of a finite field is large, it will be impossible actually to calculate the number of points by the round-robin method. Therefore various algorithms to count the number of points now is proposed. We developed the calculation library for elliptic curves over a finite field which has characteristic 2 by C++, and implemented Schoof algorithm and Schoof-Elkies-Atkin(SEA) algorithm – the counting points algorithm. Counting the number of points on random elliptic curves using these program, we verifies whether the number of points can be computed within a possible time.

1. はじめに

強固な暗号強度を持つものとして，ここ数年注目されている暗号化方法が，1985 年に N.Koblitz と V.S.Miller によりそれぞれ独立に提唱された楕円曲線暗号である．楕円曲線暗号は，同じ公開鍵暗号方式である Rivest-Shamir-Adleman(RSA) 暗号に対し，より短い鍵長で同等の暗号強度を持つことができ，より小さい計算パワーやメモリ領域での実装を可能にする．楕円曲線暗号を効率よく実装することで，小型 IC 搭載カードを利用した個人認証システムなどの実用化が期待できる．

楕円曲線暗号は，従来の有限アーベル群上での暗号プロトコルにおいて，楕円曲線上の点が為す加法群を使用する方法である．暗号用途の場合，楕円曲線上の有理点の個数 (有理点群の位数) が重要となる．楕円曲線群の位数は曲線のパラメータとともに暗号攻撃法に対する強固性を決定する重要な鍵となる．位数計算は総当りで計算すると事実上計算不可能なので，高速に計算するためのアルゴリズムやテクニックが次々と考えられている．

本研究では C++による標数 2 の有限体上の楕円曲線の計算用ライブラリの開発と，位数計算アルゴリズムのベースとなった Schoof のアルゴリズム [1, p.111–116]，およびその改良である SEA アルゴリズム [1, p.116–150][3] の実装を行う．そして，実行可能な時間内に位数計算ができるかどうかを調べる．

2. 有限体 $\mathbb{F}_{2^n}$

2 元体 $\mathbb{F}_2 = \{0, 1\}$ を係数とした多項式環 $\mathbb{F}_2[x]$ に対して，n 次既約多項式 $m(x) \in \mathbb{F}_2[x]$ の単項イデアル $\langle m(x) \rangle$ による剰余環 $\mathbb{F}_2[x]/\langle m(x) \rangle$ は体となり，$\mathbb{F}_2$ の n 次拡大体 $\mathbb{F}_{2^n}$ と同型になる．よって $\mathbb{F}_{2^n}$ の元は $n-1$ 次の多項式，

$$b_{n-1}x^{n-1} + \cdots + b_1 x + b_0,\ b_i \in \mathbb{F}_2$$

として表される．係数が 0 と 1 しか取り得ないので，$\mathbb{F}_{2^n}$ の元は n 個の係数ビット列 $[b_{n-1}, \ldots, b_1, b_0]$ として一意に表現できる．体を $\mathbb{F}_{2^n}$ に取ると元がビット列で表現できるため，計算機上での元の表現と体演算が高速に出来る利点が生じる．

$\mathbb{F}_{2^n}$ の体演算の実装は，次のような方法で実現した．

- **加減算** 加減算は元である係数ビット列の排他的論理和 (XOR) で表現できる．
- **法還元** 既約多項式を用いた多項式基底で体を表現する．拡大次数に応じて 3 項か 5 項の既約多項式を用いることで，効率的に法還元でき $O(n)$ で計算できる．
- **乗算** Karatsuba 法による再帰的計算によって実現

† 弘前大学大学院理工学研究科電子情報システム工学専攻
Dept. of Electirical and Infomation System Eng, Graduate School of Science and Technology, Hirosaki University

する．さらなる高速化のために 8bit の乗算テーブルを参照する方法を採っている．

● **逆元**　拡張 Euclid の互除法によって逆元を計算する．

3. 楕 円 曲 線

体 $\mathbb{F}$ 上の楕円曲線 $E(\mathbb{F})$ とは，Weierstrass 方程式

$$E : Y^2+a_1XY+a_3Y = X^3+a_2X^2+a_4X+a_6$$

を満たす有理点の集合と無限遠点$\mathcal{O}$を加えたもの，

$$E(\mathbb{F}) = \{(x,y) \in \mathbb{F}^2 |\ \text{上定義式}\ \} \cup \{\mathcal{O}\}$$

となる．ここで $a_i \in \mathbb{F}$ である．実数体上では無限遠点$\mathcal{O}$は y 軸上はるか遠方にあるものとして解釈される．$\mathbb{F}_{2^n}$ 上の楕円曲線は定義式が簡略化されて，

$$E_{a_2,a_6} : Y^2 + XY = X^3 + a_2X^2 + a_6$$

となる．ここで $a_2 \in \{0,1\}$，$a_6 \in \mathbb{F}_{2^n}^* = \mathbb{F}_{2^n} - \{0\}$ である．

曲線の判別式 $\Delta \neq 0$ のとき，曲線の j **不変量**が，

$$j(E) = \{(a_1^2+4a_2)^2 - 24(a_1a_3+2a_4)\}^3/\Delta$$

で定義される．j 不変量は楕円曲線の同型に関係している．標数 2 のとき，j 不変量は $j(E) = a_1^{12}/\Delta$ と簡略化される．

4. 群　法　則

楕円曲線上の有理点に対して適切に群演算を与えることで，有理点集合は加法群となる．実数体上の楕円曲線は，次に挙げる幾何学的な定義によって群演算をもつ．

(1)　$P = \mathcal{O}$ のとき，$-P = \mathcal{O}$ とする．任意の Q に対して $\mathcal{O}+Q = Q$ とする．

(2)　$P, Q \neq \mathcal{O}$ とする．P の負の点 $-P$ は，無限遠点$\mathcal{O}$から P を通る直線が，楕円曲線と交わるもう 1 つの交点である．$\mathcal{O}$は y 座標のはるか遠くにあるものとしたので，この場合 P を通る y 軸に平行な直線と楕円曲線との交点である．

(3)　$P \neq Q$ とする．2 点 P, Q を通る直線と楕円曲線との交点を R とする．点の加法は，$P+Q = -R$ となる．

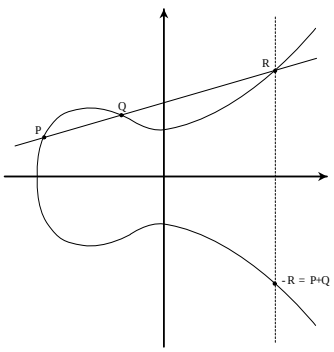

図 1　楕円曲線上の 2 点の加法，$P+Q$

(4)　$P = Q$ とする．このとき $P+P = [2]P$ は P の 2 倍点である．P における接線と楕円曲線との交点を R としたとき，2 倍点は $[2]P = -R$ とする．接線が垂直なとき，接線は無限遠点で交わるので $[2]P = \mathcal{O}$ となる．つまり，このとき P は位数 2 の点となる．

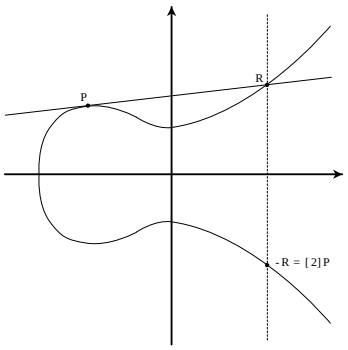

図 2　楕円曲線上の点の 2 倍，$[2]P$

群法則は代数的操作によっても定義できる．点 $P = (x_1, y_1)$，$Q = (x_2, y_2)$ を $E_{a_2,a_6}(\mathbb{F}_{2^n})$ 上の$\mathcal{O}$でない点とする．

(1)　無限遠点$\mathcal{O}$は加法群の単位元として扱う．即ち，$-\mathcal{O} = \mathcal{O}$，$P+\mathcal{O} = \mathcal{O}+P = P$ である．

(2)　負の点 $-P$ は (x_1, x_1+y_1) として定義される．

(3)　$P \neq Q$ とする．このとき $P+Q = (x_3, y_3)$ を

$$\lambda = (y_1+y_2)/(x_1+x_2)$$
$$x_3 = \lambda^2+\lambda+x_1+x_2+a_2$$
$$y_3 = (x_1+x_3)\lambda+x_3+y_1$$

と定義する．

(4)　2 倍点 $P+P = [2]P = (x_3, y_3)$ を

$$\lambda = y_1/x_1+x_2$$
$$x_3 = \lambda^2+\lambda+a_2$$
$$y_3 = (x_1+x_3)\lambda+x_3+y_1$$

と定義する．

これらの群演算の定義により有理点集合は有限アーベル群となる．演算が簡単な代数的操作によって表されるので計算機上に実装が可能となる．

ここで点 P の整数 m による m 倍点 $[m]P$ を，

$$[m]P = \begin{cases} \underbrace{P+P+\cdots+P}_{m\ 個} & (m>0) \\ -(\underbrace{P+P+\cdots+P}_{m\ 個}) & (m<0) \\ \mathcal{O} & (m=0) \end{cases}$$

と定義する．

楕円曲線に対して加法と m 倍点が定義できたので，**楕円曲線上の離散対数問題**を考えることができる．楕円曲線上の離散対数問題 (ECDLP) とは，楕円曲線 $E(\mathbb{F}_q)$ の元 P と，与えられた元 $Q \in \langle P \rangle$ に対し，

$$Q = [m]P$$

を満たす整数 m を見つける問題である．楕円曲線暗号は ECDLP をベースとした暗号なので，楕円曲線暗号に対する攻撃法は ECDLP に対する指数・準指数時間で無い解法となっている．攻撃法のうち幾つかは楕円曲線の位数に依存した計算量を持つので，楕円曲線群の位数は重要な要素となる．また，ECDLP で取り得る Q は P の張る巡回群の元なので，P を大きな素数位数を持つ楕円曲線群の部分群の生成元に選ぶ必要がある．

5. 等分多項式

前節の群法則から，楕円曲線上の 2 点の和 $P+Q$ の座標が 2 点 P, Q の座標の有理関数となることはすぐに分かる．公式の適用を繰り返すことで，m 倍写像

$$(x, y) \mapsto [m](x, y)$$

は x と y の有理関数となることが分かる．m 倍点 $[m]P$ に対して次のような結果が得られている．

• E を K 上で定義された楕円曲線とし，m を正整数とする．多項式 $\psi_m, \theta_m, \omega_m \in K[x, y]$ で，$P = (x, y) \in E(\overline{K})$ に対して $[m]P \neq \mathcal{O}$ となるものが存在し，

$$[m]P = \left(\frac{\theta_m(x, y)}{\psi_m(x, y)^2}, \frac{\omega_m(x, y)}{\psi_m(x, y)^3} \right) \tag{1}$$

と表せる．

多項式 $\psi_m(x, y)$ を E の m **等分多項式**と呼ぶ．θ_m, ω_m は ψ_m の式で表すことができる．また，等分多項式 ψ_m は漸化式で定義でき，x と y の有理式として表現できる．

非負の整数 m について，E の m **ねじれ点** $E[m]$ を，

$$E[m] = \{P \in E \mid [m]P = \mathcal{O}\}$$

と定義する．K が有限体のとき，$E(\overline{K})$ は曲線 E 上の位数有限の点全てである**ねじれ群**であるが，ねじれ点 $E[m]$ が $E(\overline{K})$ の部分群であることは容易に確かめられる．m 等分多項式 ψ_m と m ねじれ点を関連付ける次の定理がある．

[定理 1] *$P \in E(\overline{K}) - \mathcal{O}$, $m \geq 1$ とする．このとき*

$$P \in E[m] \iff \psi_m(P) = 0.$$

が成り立つ．

ここで，標数 2 の場合の楕円曲線についての等分多項式をとりあげる．曲線の定義方程式は，

$$Y^2 + XY = X^3 + a_2X^2 + a_6$$

である．標数 2 の場合の等分多項式 ψ_m は一般の場合と比べて簡略化されて次の漸化式で表される．

$$\begin{aligned}
\psi_0 &= 0, \\
\psi_1 &= 1, \\
\psi_2 &= x, \\
\psi_3 &= x^4 + x^3 + a_6, \\
\psi_4 &= x^6 + a_6x^2, \\
\psi_{2m+1} &= \psi_{m+2}\psi_m^3 + \psi_{m-1}\psi_{m+1}^3, \ m \geq 2, \\
\psi_{2m} &= (\psi_{m+2}\psi_{m-1}^2 + \psi_{m-2}\psi_{m+1}^2)\psi_m/x, \\
&\qquad m \geq 3.
\end{aligned}$$

漸化式から ψ_m は全て x のみの多項式となっている．そのため，$f_m(x) = \psi_m(x, y)$ と x のみの変数であることを強調しておく．$m \geq 2$, $P = (x, y) \in E(\overline{K}) - E[m]$ に対し，(1) 式の x 座標，y 座標は，

$$([m]P)_X = x + \frac{f_{m-1}f_{m+1}}{f_m^2} \tag{2}$$

$$\begin{aligned}
([m]P)_Y = x + y &+ \left\{(x^2 + x + y)f_{m-1}f_{m+1}\right\}/xf_m^2 \\
&+ \left(f_{m-2}f_{m+1}^2\right)/xf_m^3
\end{aligned}$$

となる．Schoof のアルゴリズムでは等分多項式 f_m が重要な役割をもっている．

6. Schoof のアルゴリズム

Schoof のアルゴリズムは一般の有限体上の楕円曲線に対して有効なものであるが，本研究では標数 2 の有限体 $\mathbb{F}_{2^n}$ 上の楕円曲線 $E(\mathbb{F}_{2^n})$ に限定して述べる．取り扱う曲線の定義式は，

$$Y^2 + XY = X^3 + a_6, \ a_6 \in \mathbb{F}_{2^n}^*$$

でよい．

$E(\mathbb{F}_q)$, $q = 2^n$ の群準同型写像の 1 つに q 乗 Frobenius 自己準同型写像 φ がある．φ は

$$\varphi : \begin{cases} E(\overline{\mathbb{F}}_q) & \longrightarrow & E(\overline{\mathbb{F}}_q) \\ (x, y) & \longmapsto & (x^q, y^q) \\ \mathcal{O} & \longmapsto & \mathcal{O} \end{cases}$$

で定義される写像である．$\overline{\mathbb{F}}_q$ は $\mathbb{F}_q$ の代数的閉包である．ここで φ は特性方程式

$$\varphi^2 - [t]\varphi + [q] = [0]$$

を持ち，曲線上の任意の点 $P = (x, y)$ について

$$(x^{q^2}, y^{q^2}) - [t](x^q, y^q) + [q](x, y) = \mathcal{O}$$

が成り立つ．位数計算アルゴリズムである Schoof のアルゴリズムではこの方程式が重要となる．

曲線の位数を $\sharp E(\mathbb{F}_q)$ とする．$\sharp E(\mathbb{F}_q) = q + 1 - t$ を満たす t を Frobenius のトレースと呼ぶ．t は Hasse の定理から $|t| \leq 2\sqrt{q}$ を満たす．

ℓ を素数とする．$q_\ell \equiv q \pmod{\ell}$, $t_\ell \equiv t \pmod{\ell}$ とするとき，$\tau \in \{0, 1, \ldots, \ell - 1\}$ と点 $P = (x, y) \in E[\ell]^*$ において，

$$(x^{q^2}, y^{q^2}) + [q_\ell](x, y) = [\tau](x^q, y^q) \tag{3}$$

を満たす τ が見つかったならば，$\tau = t_\ell$ とならなければならない．各素数 ℓ に対して上式を満たす τ を調べ，$t \pmod{\ell}$ の情報を得る．

$$\prod_{\ell:\text{素数},\ 2\le\ell\le\ell_{max}} \ell > 4\sqrt{q}$$

を満たす最小の素数 ℓ_{max} 以下の全素数に対して $t \pmod{\ell}$ を得て，中国剰余定理によって一意に t が決定でき，群位数がわかる．

(3) 式を満たす τ の値を決定するため，$\tau \in \{0, 1, \ldots, \ell-1\}$ の値が順に試されるものとする．

• (3) 式の x 座標の計算

与えられた ℓ と τ の値に対して，倍点 $[q_\ell](x,y)$ と $[\tau](x^q, y^q)$ の x 座標は x の有理関数となり，(2) 式で計算される．$(x^{q^2}, y^{q^2}) + [q_\ell](x,y)$ の x 座標の計算には，曲線の点の加法公式を記号的に適用する．(3) 式の両辺の x 座標をそれぞれ $((x^{q^2}, y^{q^2}) + [q_\ell](x,y))_X$，$([\tau](x^q, y^q))_X$ とすると，

$$((x^{q^2}, y^{q^2}) + [q_\ell](x,y))_X = ([\tau](x^q, y^q))_X \quad (4)$$

を計算することになる．(4) 式の分母を払い，y の 2 次以上の冪があったならば曲線の方程式 $y^2 = xy + x^3 + a_6$ を法として還元する．記号的操作により $a(x) - yb(x) = 0$ または $y = b(x)/a(x)$ の形の式を得る．この式を曲線の方程式に代入することで y を消去でき，$h(x)_X = 0$ の形の方程式を得る．

ここで，$h(x)_X$ と等分多項式 f_ℓ の最大公約数 (gcd) を計算することで，$h(x)_X = 0$ が解をもつかどうか，即ち，(3) 式を満たす点が $E[\ell]^*$ にあるかどうか判別できる．$\gcd(h(x)_X, f_\ell) = 1$ のとき，$E[\ell]^*$ を満たす点に対して $h(x)_X = 0$ が解を持たないので次の τ の値をテストする．gcd$\neq 1$ のとき，

$$(x^{q^2}, y^{q^2}) + [q_\ell](x,y) = \pm[\tau](x^q, y^q) \quad (5)$$

を満たす点が $E[\ell]^*$ に存在する．右辺が正負どちらの符号であっても (5) 式の x 座標は同じであるので，この段階では右辺の符号は不定である．

• (5) 式の y 座標の計算

(5) 式の符号決定のため，右辺を正符号と仮定する．両辺の y 座標を計算して，x 座標の計算と同様に分母を払い，y の 2 次以上の冪を 1 次以下に落として，$h(x)_Y = 0$ の形の式を得る．再び $\gcd(h(x)_Y, f_\ell)$ を計算し，gcd$\neq 1$ なら，式を満たす点が存在して正符号となる．gcd=1 なら正符号なら存在しないので負符号となる．τ に対しては正負の場合をテストするので，実際には $0 \le \tau \le (\ell-1)/2$ の範囲をテストすればよいことが分かる．

計算では，(3) 式を満たす点 P が $E[\ell]^*$ に属すると仮定していることから，全て f_ℓ を法として計算され，多項式の次数は $O(\ell^2)$ となる．アルゴリズム中のボトルネックとなる部分は $x^q, y^q, x^{q^2}, y^{q^2}$ の計算である．$x^q, y^q, x^{q^2}, y^{q^2}$ は f_ℓ と曲線の定義式により，$\log q$ の指数的サイズから $O(\ell^2)$ 以下の多項式サイズとなる．アルゴリズム全体の計算量は $O(\log^8 q)$ となる．

PentiumII 266Mhz, メモリ 64MB 上で作成したプログラムにおいて計算したところ，$n = 40$ 次で約 10 分，80 次で 6 時間ほど掛かった．暗号として使用できる鍵サイズが約 160 次以上であるので，位数計算にはこのアルゴリズムでも効率が悪いことは明らかである．

7. Schoof-Elkies-Atkin アルゴリズム

Schoof のアルゴリズムを改良したものが Schoof-Elkies-Atkin(SEA) アルゴリズムである．Schoof のアルゴリズムにおける各素数 ℓ のステップにおいて，Frobenius 自己準同型 φ の特性方程式

$$\mathcal{F}_\ell(u) = u^2 + t_\ell u + q_\ell = 0$$

の判別式 $\Delta_{\mathcal{F}_\ell} = t^2 - 4q$ が，ℓ を法として平方数なら ℓ を Elkies 素数，そうでないなら Atkin 素数と呼ぶ．Elkies 素数の場合，Elkies が考案したアルゴリズムを用いて Schoof のアルゴリズムと同様 $t \pmod{\ell}$ を得る．Atkin 素数なら Atkin のアルゴリズムから $t \pmod{\ell}$ と成り得る可能性のある値の集合を得る．Schoof のアルゴリズムと同様に，各素数における t の情報が十分に集まったら，中国剰余定理と BabyStep/GiantStep 法 (有限アーベル群上の離散対数問題を解くアルゴリズム)[1, p.94–96] により t が決定できる．

7.1 モジュラー多項式による判別

Elkies 素数と Atkin 素数の判別では $t^2 - 4q$ が ℓ を法として平方数かどうかを調べなければならないが，t そのものが求めたい値であるので直接調べることはできない．そのため，素数の判別においてはモジュラー多項式が重要な役割を演じる．各素数 ℓ に対して，ℓ 次**モジュラー多項式**と呼ばれる多項式が導入できる．モジュラー多項式は，整数係数をもつ 2 変数の対称式 $\Phi_\ell(x,y) \in \mathbb{Z}[x,y]$ であり，

$$x^{\ell+1} - x^\ell y^\ell + y^{\ell+1}$$

の形式の項に

$$a_{ij} x_i y_j,\ \ i,j \le \ell,\ i+j < 2\ell,\ a_{ij} \in \mathbb{Z}$$

の形をした項を足したものに等しくなる．モジュラー多項式には，Kronecker の合同関係式により

$$\Phi_\ell(x,y) \equiv (x^\ell - y)(x - y^\ell) \pmod{\ell}$$

が成り立つ．モジュラー多項式 $\Phi_\ell(x,y)$ の次数は各変数に対して $\ell+1$ であり，各項の整係数は ℓ が大きくなるにつれて非常に大きくなる．モジュラー多項式の特性としては次のものが挙げられる．任意の体 $\mathbb{F}$, $\mathrm{char}(\mathbb{F}) \neq \ell$ と j 不変量 $j \in \mathbb{F}$ に対して，方程式 $\Phi_\ell(x,j) = 0$ の $\ell+1$ 個の零点 $\tilde{j} \in \overline{\mathbb{F}}$ は，ちょうど同種な曲線 E/C の j 不変量となる．ここで E は j 不

変量 j を持つ楕円曲線であり，C は $E[\ell]$ の $\ell+1$ 個の巡回部分群のどれかとなる．同種な曲線とは，同種写像 (楕円曲線 E_1, E_2 に対し，E_1 上の単位元 (無限遠点) を E_2 上の単位元に写すような写像) によって写された曲線のことをいう．この性質は，Elkies のアルゴリズムにおける等分多項式 f_ℓ の因子 $\mathrm{F}_\ell(x)$ の決定の際に使われる．

例として，$\ell=3$ のときのモジュラー多項式 $\Phi_3(x,y)$ は次のようになる．

$$\begin{aligned}\Phi_3(x,y) = {} & x^4 - x^3y^3 + y^4 + 2232(x^3y^2 + x^2y^3) \\ & -1069956(x^3y + xy^3) \\ & +36864000(x^3 + y^3) \\ & +2587918086x^2y^2 \\ & +8900222976000(x^2y + xy^2) \\ & +452984832000000(x^2 + y^2) \\ & -770845966336000000xy \\ & +1855425871872000000000(x + y)\end{aligned}$$

モジュラー多項式の整係数は指数的☆に増えるため，計算機上でのモジュラー多項式を使った計算には大きな負担が付きまとう．一般の場合は，異なる定義によりモジュラー多項式の係数の小さな変種を与えることでこの問題を解決する．しかし，標数 2 の体上での計算ではモジュラー多項式の各係数に対し 2 を法としたものを取ればよく，モジュラー多項式を予め計算しておき 2 を法としたものを表に保存すればよい．例えば，標数 2 の体上では $\Phi_3(x,y), \Phi_5(x,y), \Phi_7(x,y)$ は，

$$\Phi_3(x,y) = x^4 + x^3y^3 + y^4 \pmod 2$$
$$\Phi_5(x,y) = x^6 + x^5y^5 + x^4y^2 + x^2y^4 + y^6 \pmod 2$$
$$\Phi_7(x,y) = x^8 + x^7y^7 + x^6y^6 + y^8 \pmod 2$$

となり，これらを表に保存したもの用いて計算する．ここで，ℓ が Elkies 素数か Atkin 素数かどうかの判別に $\Phi_\ell(x,j)$ の分解型が利用できることを示す次の命題がある．

[命題 1] **E を $\mathbb{F}_q$ 上の supersingular でない楕円曲線とし，この曲線の j 不変量 j が $j \neq 0, 1728$ とする．$\Phi_\ell(x,j) = f_1, f_2, \ldots, f_s$ を $\Phi_\ell(x,j) \in \mathbb{F}_q[x]$ の既約多項式の積としての分解とする．このとき，$f_1, f_2, \ldots, f_s$ の次数として次の可能性がある．**

(1) **1 と ℓ(このとき $r = \ell$ とおく)，もしくは $1, 1, \ldots, 1$(このとき $r=1$ とおく)；線形因子と ℓ 次の既約因子の積，もしくは線形因子のみの積として表された場合，ℓ は曲線の判別式 $\Delta_t = t^2 - 4q$ について ℓ を法として割り切る．**

(2) **$1, 1, r, r, \ldots, r$；この場合，$t^2 - 4q$ は ℓ を法として平方数であり，r は $\ell-1$ を割り切り，Frobenius 自己準同型 φ は，$E[\ell]$ 上で**

$$\begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix}$$

として作用する．ここで，$\lambda, \mu \in \mathbb{F}_\ell^*$ である．

(3) **ある $r > 1$ において，$r, r, \ldots, r$：この場合，$t^2 - 4q$ は ℓ を法として平方数でなく，r は $\ell+1$ を割り切り，φ は $E[\ell]$ 上で，$\mathbb{F}_\ell$ 上既約な特性多項式を持った 2×2 行列として作用する．**

全ての場合において r は $\mathbb{F}_\ell$ 上の射影一般線形群 $PGL_2(\mathbb{F}_\ell)$ の位数であり，φ のトレース t は，1 のある原始 r 乗根 $\zeta \in \overline{\mathbb{F}}_\ell$ に存在して，

$$t^2 = q(\zeta + 2 + \zeta^{-1}) \tag{6}$$

を満たす．

この命題により，ℓ が Elkies 素数であるのか Atkin 素数であるのかを判別する方法が $\Phi_\ell(x,j)$ の分解型によって与えられる．命題の **1,2** の場合は，素数 ℓ が Elkies 素数のときであり，**1** のときは $\mathcal{F}_\ell$ が重根を持つ場合に対応する．**3** の場合は Atkin 素数に対応している．Atkin 素数のとき，(6) 式からトレース t の取り得る値の個数が分かり，オイラーの関数 $\varphi_{\mathrm{Euler}}(r)$ つまり 1 の原始 r 乗根の個数となる．r は $\ell+1$ を割るので，$\mathcal{F}_\ell$ の根は全て $\mathbb{F}_{\ell^2} - \mathbb{F}_\ell$ に属する．

Elkies 素数と Atkin 素数の判別では，実際には正確な分解型は必要とならない．なぜなら

$$\gcd\left(x^q - x, \Phi_\ell(x,j)\right)$$

を計算することで判別できるためである．gcd の次数は 0,1,2,$\ell+1$ のどれかであって，次数が 1,2,$\ell+1$ の場合は Elkies 素数に対応し，次数 0 の場合が Atkin 素数に対応している．

7.2 Elkies のアルゴリズム

ℓ が Elkies 素数のとき，φ の特性多項式 $\mathcal{F}_\ell$ は $\mathbb{F}_\ell$ において 2 根 λ, μ を持つ．よって特性多項式は $\mathcal{F}_\ell(u) = u^2 - tu + q = (u-\lambda)(u-\mu)$ と分解される．これから，

$$t \equiv \lambda + q/\lambda \pmod \ell$$

より，根の 1 つ λ を決定することで $t \pmod \ell$ が得られる．そのような λ を見つけるために，点 $P=(x,y)$ および $\lambda \in \{1, 2, \ldots, \ell-1\}$ に対して，$u = \lambda$ から

$$(x^q, y^q) = [\lambda](x,y)$$

を満たすかどうか調べることで λ を決定できる．

ここで計算上のボトルネックとなるのは Schoof のアルゴリズムと同様 x^q, y^q の計算である．Elkies 素数の場合多項式計算の法として，次数 $O(\ell^2)$ である $f_\ell(x)$ の代わりに f_ℓ の次数 $(\ell-1)/2$ の因子 $\mathrm{F}_\ell(x)$ を

☆ $\Phi_\ell(x,y)$ の最大の係数の絶対値に対する自然対数を $h(\Phi_\ell)$ とすると，

$$h(\Phi_\ell) = 6(\ell+1)\left((1-\frac{2}{\ell})\log\ell + O(1)\right)$$

となるのが分かっている．

使用する．計算量による制約から直接 f_ℓ を分解して $\mathrm{F}_\ell(x)$ を導くことはできない．そのため，$\mathrm{F}_\ell(x)$ を得る方法として，同種写像から得られる情報を利用して $\mathrm{F}_\ell(x)$ を構成する方法がとられる．標数 2 の体上の楕円曲線 $E(\mathbb{F}_{2^n})$ では，Lercier の考案したアルゴリズム [4] を使用する．Lercier のアルゴリズムでは，ブール値変数の多変数非線形方程式系を解く必要が出てくる．

7.3 Atkin のアルゴリズム

ℓ が Atkin 素数のとき，Atkin のアルゴリズムが用いられる．モジュラー多項式 $\Phi_\ell(x, j)$ の分解型から得られる情報を利用する．$\Phi_\ell(x, j)$ の因子の次数 r から，Atkin のアルゴリズムによって $t \pmod{\ell}$ と成り得る値の集合が決定される．SEA アルゴリズムの最後の段階で，Elkies 素数から得られる情報と Atkin 素数から得られる情報から全ての t の候補が BabyStep/GiantStep 法によってテストされる．

7.4 計 算 結 果

PentiumII 266Mhz, メモリ 64MB 上で，$\mathbb{F}_{2^{161}}$ 上のランダムな楕円曲線 50 個について計算したところ次のようになった．

平均時間 (s)	最長時間 (s)	最短時間 (s)
3044	6507	803

161 次では平均時間で一時間以内に計算できているので，位数計算として SEA アルゴリズムが使用できる見込みが立った．計算時間に開きがあるのは，Atkin 素数が多かった曲線では計算時間が増大するためである．

8. まとめと今後の課題

今回の研究においては位数を実行時間内に計算できたが，まだ十分に速いとは言えない．速度向上のために楕円曲線ライブラリの改良や，現在考案されているさらに高速な位数計算アルゴリズムの実装が今後の課題として挙げられる．また，位数計算により安全だと思われる楕円曲線を用いた IC カード上での楕円曲線暗号システムの構築も興味深いテーマと言える．

参 考 文 献

[1] I.F.Blake,G.Seroussi,N.P.Smart 訳 : 鈴木 治郎 **楕円曲線暗号** *2001* ピアソン・エデュケーション

[2] J.H.Silverman,J.Tate 訳 : 足立 恒雄, 木田 雅成, 小松 啓一, 田谷 久雄 **楕円曲線論入門** *1995* シュプリンガー・フェアラーク東京

[3] R.Schoof **Counting points on elliptic curves over finite fields** *1995* J.Théorie des Nombres de Bordeaux, 7, 219-254

[4] R.Lercier **Computing isogenies in $\mathbb{F}_{2^n}$** *1996* ANTS-2: Algorithmic Number Theory.197-212 Springer-Verlag

[5] 奥村 晴彦 **C 言語による最新アルゴリズム事典** *1991* 技術評論社