係数が固定されている Pairing-friendly 楕円曲線

白勢 政明 ‡

† 公立はこだて未来大学
041-8655 北海道函館市亀田中野町 116-2

あらまし 本稿は，$p(z) = 46656z^4 + 69984z^3 + 39744z^2 + 10116z + 973$($z$ は整数) で与えられる素数に対して，素体 $F_p(z)$ 上の $y^2 = x^3 + 432$ が埋込み次数 12 を持つ pairing-friendly 楕円曲線であることを示す．本稿の結果より，CM 法を必要とせず $p(z)$ が素数となる z の探索のみで pairing-friendly 楕円曲線を得ることができる．

Pairing-friendly Elliptic Curves with Fixed Coefficients

Masaaki Shirase‡

†Future University Hakodate
116-2 Kamedanakano, Hakodate, Hokkaido 041-8655, Japan

Abstract This paper shows that an elliptic curve $y^2 = x^3 + 432$ over $\mathbb{F}_{p(z)}$ having the embedding degree 12 is a pairing-friendly elliptic curve, where $p(z) = 46656z^4 + 69984z^3 + 39744z^2 + 10116z + 973$ for any integer z such that $p(z)$ is a prime number. Due to this paper, we can have a pairing-friendly elliptic curve only by search of integer z such that $p(z)$ is a prime number.

1 はじめに

ペアリングを用いることで，ID ベース鍵交換 [21]，ID ベース暗号 [5]，ID ベース署名 [14]，リング署名 [26]，キーワード検索暗号 [4]，効率的な放送型暗号 [7]，墨塗り署名 [6] といった新しい暗号プロトコルが可能となるため，ペアリング暗号の研究が盛んになっている．ペアリングは (超) 楕円曲線上の双線形写像として定義され，ペアリングに適した (pairing-friendly) 楕円曲線の構成がペアリング暗号の研究の大きなテーマの一つとなっている．E を有限体 $\mathbb{F}_q$ 上定義された楕円曲線とし，r を $\#E(\mathbb{F}_q)$ の最大素因数とすると，E が pairing friendly であるための条件は，1) r が大きな素数，2) $r|(q^k - 1)$ を満たす最小の k が適切な値，3) $\rho = \log q/\log r$ が 1 に近い，を満たすことである．

超特異楕円曲線に対しては，自動的に埋込み次数 k が定まり，定義体の標数が $2, 3, p \geq 5$ のとき，それぞれ $k = 4, 6, 2$ となる [18]．特に定義体の標数が 2,3 の時，k はペアリングに適切な値である．

素体上の通常楕円曲線による pairing-friendly 楕円曲線の構成法は，Miyaji, Nakabayashi, and Tanaka によって最初に研究され，$k = 3, 4, 6$ の場合を扱った [19]．その後，pairing-friendly の通常曲線の構成法として，Cocks-Pinch 法 [9]，Barreto 等の方法 [2]，Brezing-Weng 法 [8]，Dupont 等の方法 [10]，Galbraith 等の方法 [13]，Barreto-Naehrig 法 [3]，Freeman 法 [11]，Tanaka-Nakamula 法 [24, 25] 等が知られている．

これらの手法は，素体 $\mathbb{F}_p$ 上の楕円曲線が pairing-friendly の条件を満たすような素数 p，位数 $n = \#E(F_p)$ 及び $DV^2 = 4p - t^2$ (t は $t = p + 1 - n$ と定義されトレースという) を満たす平方因子を持たない整数 D を与えるのみである．従って，これらの値から CM 法 [1] により楕円曲線を構成する必要がある．

本稿では，$p(z) = 46656z^4 + 69984z^3 + 39744z^2 + 10116z + 973$ と $n(z) = 46656z^4 + 69984z^3 + 39528z^2 + 9972z + 949$($z$ は整数) が素数となるとき $y^2 = x^3 + 432$ が埋込み次数 12 を持ち位数が $n(z)$ となる pairing-friendly 楕円曲線であることを，Gauss の定理 [23, IV 章] と Barreto-Naehrig 法を利用して示す．これは，係数が明示的に示されているため，CM 法を必要としない pairing-friendly 楕円曲線を与える方法であり，従来手法より効率的に pairing-friendly 楕円曲線を構成できる．

2 楕円曲線とペアリング

本節では，楕円曲線，ツイスト，ペアリングの定義や性質を説明し，楕円曲線が pairing-friendly であるための条件を説明する．

2.1 楕円曲線

$p \geq 5$ を素数，q を素数 p のべきとする．有限体 $\mathbb{F}_q$ 上の楕円曲線

$$E : y^2 = x^3 + ax + b \tag{1}$$

に対して，E の $\mathbb{F}_q$ 上有理点の集合 $E(\mathbb{F}_q)$ を

$$E(\mathbb{F}_q)=\{(x,y)\in\mathbb{F}_q\times\mathbb{F}_q : y^2=x^3+ax+b\}\cup\{\mathcal{O}\}$$

と定義する．ここで $\mathcal{O}$ は無限遠点である．変換 $x=X/Z, y=Y/Z$ によって得られる射影座標系では，E の式 (1) は $Y^2Z=X^3+aXZ^2+bZ^3$ で与えられ，射影点 $[X,Y,Z]=[0,1,0]$ が $\mathcal{O}$ に対応する[1]．

$$t=q+1-\#E(\mathbb{F}_q)$$

を $E(\mathbb{F}_q)$ のトレースという．

E の係数 a,b に対して，E の判別式は $\Delta(E)=-16(a^3+27b^2)$ で定義され，E の j 不変数 $j(E)$ は $j(E)=-12^3a^3/\Delta(E)$ で定義される．また $j_0\in\mathbb{F}_q$ が与えられると，j_0 を j 不変数とする楕円曲線を構成できる [22, III.1.4]．特に標数 5 以上では

$$j(E)=0\Leftrightarrow E: y^2=x^3+b,\ b\in\mathbb{F}_q^* \qquad (2)$$

が成り立つ．

2.2 ツイスト

$\mathbb{F}_q$ 上定義されているの楕円曲線 E,E' に対して，$\mathbb{F}_{q^d}$ 上同型写像 $\psi_d : E'\to E$ があり d が最小の時，E' は E の d 次のツイストであると言う[2]．このような同型写像があるならば，d の値は 1, 2, 3, 4, 6 のどれかになることが知られている [22, Proposition X.5.4]．E' が E の (次数に関係なく) ツイストであることと $j(E')=j(E)$ が成り立つことは同値である．E' が E の 1 次のツイストならば $\#E(\mathbb{F}_q)=\#E'(\mathbb{F}_q)$ となるが，E' が E の d 次 ($d>1$) のツイストならば $\#E(\mathbb{F}_q)\neq\#E'(\mathbb{F}_q)$ となる．$\#E(\mathbb{F}_q)=p+1-t$(t はトレース) とすると，$\#E'(\mathbb{F}_q)$ は以下のように書ける [3]．

	$\#E'(\mathbb{F}_q)$	f が満たす関係式
$d=2$	$q+1+t$	
$d=3$	$q+1-(3f-t)/2$	$(t^2-4q=-3f^2)$
	$q+1-(-3f-t)/2$	$(t^2-4q=-3f^2)$
$d=4$	$q+1+f$	$(t^2-4q=-f^2)$
	$q+1-f$	$(t^2-4q=-f^2)$
$d=6$	$q+1-(-3f+t)/2$	$(t^2-4q=-3f^2)$
	$q+1-(3f+t)/2$	$(t^2-4q=-3f^2)$

2.3 ペアリング

r を素数とすると，写像 $e: G_1\times G_2\to G_3$ (G_1, G_2 は位数 r の加群，G_3 は位数 r の乗法群) が，双線形性 (整数 a,b に対して $e(aP,bQ)=e(P,Q)^{ab}$ が成り立つ) と非退化性 ($e(P,Q)\neq1$ を満たす P,Q が存在する) とき，e をペアリングという．

本稿が扱う素体上の通常楕円曲線を用いる場合は Ate ペアリング [15] が高速実装に適している．Ate ペアリング $e(P,Q)$ は，$P\in G_1=E(\mathbb{F}_p)$，$Q\in G_2=Ker([p]-\phi)$ (ϕ は p 乗 Frobenius 写像) に対して，因子が $(f_{t,Q})=t(Q)-(tQ)-(t-1)\mathcal{O}$ となる関数 $f_{t,Q}$ を使って，$e(P,Q)=f_{t,Q}(P)^{(q^k-1)/r}\in\mathbb{F}_{p^k}^*$ と定義される．但し，$\#E(\mathbb{F}_p)$ の最大素因数 r に対して，k は

$$r|(q^k-1)$$

を満たす最小の自然数であり埋込み次数と呼ばれる．また，Ate ペアリングの改良版として，optimized Ate ペアリング [17]，R-ate ペアリング [16]，Xate ペアリング [20] 等もあり，より高速に計算できる．

2.4 Pairing-friendly 楕円曲線

ペアリング暗号に適した楕円曲線を pairing-friendly 楕円曲線と言う．E を有限体 $\mathbb{F}_q$ 上定義された楕円曲線とし，r を $\#E(\mathbb{F}_q)$ の最大素因数とすると，$\mathbb{F}_q$ 上の E が pairing-friendly であるための条件は

条件 1 (*Pairing-friendly* の条件)
($c1$) r が大きな素数．($\#E(\mathbb{F}_q)=r$ が最良)
($c2$) 埋込み次数 k が適切な値．($4\le k\le 30$)
($c3$) $\rho=\log q/\log r$ が 1 に近い．($\rho=1$ が最良)

を満たすことである [12]．

3 従来の楕円曲線の構成法

この節では，指定した位数を持つ楕円曲線を構成するための Complex Multiplication(CM) 法と，現在知られている pairing-friendly 楕円曲線の構成法について簡単に説明する．

3.1 CM 法 [1]

CM 法は，素数 p，トレース t 及び

$$DV^2=p^2-4t \qquad (3)$$

を満たす平方因数を持たない整数 D から，位数が $n=p+1-t$ となる楕円曲線を構成するアルゴリズムである．CM 法は，初めに $\#E_0(\mathbb{F}_p)=n$ となる楕円曲線 E_0 の j 不変数 j_0 を与え，次に j 不変数が j_0 となる楕円曲線 E を構成する．2.2 節で説明したように E は E_0 のツイストであるが，E の位数 $\#E(\mathbb{F}_p)$ が n になるとは限らない．位数チェックのため $\mathcal{O}$ でない点 $G\in E(\mathbb{F}_p)$ をとり，nG が $\mathcal{O}$ となるかどうかをチェックする必要がある．つまり，CM 法は以下のプロセスを持つ．

CM 法のプロセス	
(a)	j 不変数 j_0 の決定
(b)	j 不変数 j_0 を持つ楕円曲線 E を構成し $\mathcal{O}$ でない 1 点 $G\in E(\mathbb{F}_p)$ を見つける
(c)	$nG=\mathcal{O}$ ならば E を返す，そうでなければ (b) へ戻る

[1]本稿では，曲線の無限遠点の個数が重要となるため，射影座標系が必要となる．射影座標標系の点 $[X_0,Y_0,Z_0]$ と $[X_1,Y_1,Z_1]$ に対して，$X_1=rX_0, Y_1=rY_0, Z_1=rZ_0$ ($r\neq0$) となるならば，$[X_0,Y_0,Z_0]=[X_1,Y_1,Z_1]$ となる．

[2]d=1 の時はツイストと呼ばない場合があるが，本稿では $d=1$ の場合もツイストであるとする．

(a) が CM 法のメインの部分でありコストも最大である．

$D=3$ のとき，CM 法は j 不変数 0 を返すことが知られている．従って Barreto-Naehrig 法 [3] のように $D=3$ の場合のみを扱うならば，CM 法のメインの部分 (a) が不要となる．

3.2 従来の pairing-friendly 楕円曲線の構成法

素体 $\mathbb{F}_p$ 上の pairing-friendly の通常曲線の構成法については，Miyaji, Nakabayashi and Tanaka が最初に研究し，$k=3,4,6$ の場合を扱った [19]．その後，pairing-friendly の通常曲線の構成法として，Cocks と Pinch の方法 (任意の k に対して $\rho\approx 2$ となるよう構成法)[9]，Barreto 等の方法 [2]($\rho\approx 2$ となるよう構成法)，Brezing と Weng の方法 (任意の k に対する構成法)[8]，Dupont 等の方法 ($\rho\approx 2$ となる構成法)[10]，Galbraith 等の方法 ($k=5,10,12$ に対する構成法)[13]，Barreto と Naehrig の方法 ($k=12$ に対する構成法)[3]，Freeman の方法 ($k=10$ に対する構成法)[11]，Tanaka と Nakamula の方法 ($k=8$ に対する構成法)[24, 25] 等が提案された．

これらの通常曲線の構成方法は，2.4 節の pairing-friendly の**条件 1** を満たすような p，トレース t，式 (3) 満たす平方因子を持たない整数 D をどのように見つけるかを論じている．これらのパラメータを見つけた後は，CM 法により目的の楕円曲線を構成する (3.1 節参照)．

4 Gauss の定理と Barreto-Naehrig の曲線構成法

本節では，5 節の提案手法で用いる，素体 $\mathbb{F}_p$ 上の曲線 $u^3+v^3+1=0$ の点の個数についてを述べる Gauss の定理 [23] と，埋込み次数 12 の楕円曲線の構成についての Barreto-Naehrig 法 [3] について説明する．

4.1 Gauss の定理

定理 1 (Gauss の定理)

$\mathcal{P}$ を $\mathcal{P}\equiv 1\ (mod\ 3)$ を満たす素数とし，$M_{\mathcal{P}}$ を有限体 $\mathbb{F}_{\mathcal{P}}$ での

$$C: u^3+v^3+1=0$$

の射影点の個数を表すとする．すると，

$$4\mathcal{P}=A^2+27B^2 \tag{4}$$

を満たす整数 A と B が正負の符号を無視すると一意に定まり，$A\equiv 1\ (mod\ 3)$ となるように A を選ぶと，

$$M_{\mathcal{P}}=\mathcal{P}+1+A$$

を満たす．

証明) [23] を参照．□

4.2 Barreto-Naehrig の曲線構成法

Barreto と Naehrig は埋込み次数 12 で $\rho\approx 1$ となる pairing-friendly 楕円曲線の構成法を与えている [3]．

z を変数とする多項式 $t'(z), n'(z), p'(z)$ を

$$\left.\begin{aligned} t'(z) &= 6z^2+1\\ n'(z) &= 36z^4+36z^3+18z^2+6z+1\\ p'(z) &= n'(z)+t'(z)-1\\ &= 36z^4+36z^3+24z^2+6z+1 \end{aligned}\right\} \tag{5}$$

とする．すると，$p'(z)$ と $t'(z)$ は

$$4p'(z)-t'(z)^2=3\underbrace{(5z^2+4z+1)}_{V'(z)}{}^2 \tag{6}$$

という関係を満たす．よって，$p'(z)$ 及び $n'(z)$ が素数となる整数 z を選ぶと，素数 $p'(z)$，トレース $t'(z)$，$D=3$ が得られる．これら $p'(z), t'(z), D=3$ を CM 法の入力とすると，3.1 節で説明したように CM 法は j 不変数 0 を返すため，CM 法のプロセス (a) が不要となる．従って Barreto-Naehrig 法は最も効率的な pairing-friendly 楕円曲線の構成法の一つである．Barreto-Naehrig 法で使用する改良 CM 法 ([3] の Algorithm 1) は平均 12 回の $\mathbb{F}_p$ の元の平方剰余であるかどうかのチェックと平均 6 回の nG の計算で，埋込み次数 $k=12$ の pairing-friendly 楕円曲線を構成できる．

5 提案手法

Barreto-Naehrig 法では CM 法の j 不変数決定プロセスが不要なため pairing-friendly 楕円曲線の最も効率的な構成法の一つであるが，それでも CM 法は平均 12 回の $\mathbb{F}_p$ の元の平方剰余であるかどうかのチェックと平均 6 回のスカラー倍算が必要である．

本節では，Gauss の定理と Barreto-Naehrig 法の式 (5)，(6) を用いて，係数が明示的に与えられるため CM 法が不要な埋込み次数 12 を持ち $\rho\approx 1$ となる楕円曲線を構成する方法 (定理 2) を提案する．なお，2 つの楕円曲線 E_+ と E_- を

$$E_+: y^2=x^3+432,$$
$$E_-: y^2=x^3-432,$$

と定義する．

定理 2（提案定理）

$$t(z)=216z^2+144z+25$$
$$p(z)=46656z^4+69984z^3+39744z^2+10116z+973$$
$$n(z)=46656z^4+69984z^3+39528z^2+9972z+949$$

とする．$p=p(z)$ が素数となる自然数 z に対して，$E_+(\mathbb{F}_p)=n(z)$ が成り立ち，$E_+(\mathbb{F}_p)$ は埋込み次数 *12* を持ち $\rho\approx 1$ となる．

定理 2 の証明の概略は以下のようになる．初めに Gauss の定理の条件 (4) を満たしかつ埋込み次数が $k=12$ となる A, B, p を与える多項式を，BN 法を用いて構成する．すると，Gauss の定理より 3 次曲線 $C: u^3+v^3+1=0$ の射影点の個数 $\#C(\mathbb{F}_p)$ が求まる．次に $C(\mathbb{F}_p)$ と $E_-(\mathbb{F}_p)$ との間の (ほぼ) 一対一の写像の存在と両者の無限遠点の個数を正確に数えることで，$\#C(\mathbb{F}_p)=\#E_-(\mathbb{F}_p)$ を示すことができる．$\#E_-(\mathbb{F}_p)$ は必ず 27 の倍数なるため，$\#E_-(\mathbb{F}_p)$ はあまり pairing-friendly でない．そこで E_- の 2 次のツイスト E_+ を考えると，定理 2 が得られる．

定理 2 の正確な証明は次の補題を使って得られる．

補題 1

$$t_0(z) = 54z^2+72z+25$$
$$p_0(z) = 2916z^4+8748z^3+9936z^2+5058z+973$$
$$n_0(z) = 2916z^4+8748z^3+9990z^2+5130z+999$$

とする．曲線 C を *Gauss* の定理 (定理 1) で定義したように $C: u^3+v^3+1=0$ とする．すると，次が成り立つ．

(1) $A(z), B(z)$ を

$$\begin{array}{rcl} A(z) & = & 54z^2+72z+25 \\ B(z) & = & 45z^2+72z+29 \end{array}$$

と定義すると，$p_0(z)$ が素数となる整数 z に対して，$A(z), B(z), \mathcal{P}=p_0(z)$ は *Gauss* の定理の条件 *(4)* を満たす．従って，*Gauss* の定理より $\#C(\mathbb{F}_{p_0})=n_0(z)$ となる．

(2) $p_0=p_0(z)$ が素数となる整数 z を選ぶと次が成り立つ．

(2-i) $C(\mathbb{F}_{p_0})$ は *3* 個の無限遠点をもつ．

(2-ii) $\#C(\mathbb{F}_{p_0})=\#E_-(\mathbb{F}_{p_0})$．つまり，$\#E_-(\mathbb{F}_{p_0})=n_0(z)$，$\#E_-(\mathbb{F}_{p_0})$ のトレース $=-t_0(z)$．

(2-iii) E_- (と C) は埋込み次数 *12* を持ち，$\#E_-(\mathbb{F}_{p_0})$ $(=\#C(\mathbb{F}_{p_0}))$ は *27* で割れる．(つまり $\#E_-(\mathbb{F}_{p_0})$ は素数に成り得ない．)

(2-iv) z が奇数ならば，$\#E_+(\mathbb{F}_{p_0})=p_0(z)+1-t_0(z)$．$z$ が偶数ならば，$\#E_+(\mathbb{F}_{p_0})=\#E_-(\mathbb{F}_{p_0})$．

証明) **(1)** Barreto-Naehrig の手法の式 (6) において，$V'(z)$ が 3 の倍数であるならば，$4p'(z)=t'(z)^2+27(\frac{V'(z)}{3})^2$ と書ける．つまり，Gauss の定理において $A=t'(z), B=V'(z)/3$ とおくことができる．また $z \equiv 2 \pmod 3$ の時 $V'(z)$ が 3 の倍数となることはすぐに確かめられる．従って，

$$A(z) = t'(3z+2) = 54z^2+72z+25$$
$$B(z) = V'(3z+2) = 45z^2+72z+29$$
$$\begin{aligned} \mathcal{P}(z) &= p'(3z+2) \\ &= 2916z^4+8748z^3+9936z^2+5058z+973 \end{aligned}$$

とすると Gauss の定理の条件 (4) を満たす．ここで，$p_0(z)=\mathcal{P}(z)$ となっている．$p_0(z)$ が素数となる全ての整数 z に対して，$p_0(z)\equiv 1 \pmod 3$ かつ $A(z)\equiv 1 \pmod 3$ が常に成り立つから，Gauss の定理より $\#C(\mathbb{F}_{p_0})=p_0(z)+1+A(z)=n_0(z)$ となる．

(2-i) 曲線 C の式を射影座標系で表現すると，

$$U^3+V^3+W^3=0$$

となる．C には $W=0$ を満たす射影点が 3 つ $[-1,1,0]$, $[-1,\omega,0]$, $[-1,\omega^2,0]$ あり，これらが C の無限遠点である．ここで ω は 1 の原始 3 乗根．これらの 3 点が $C(\mathbb{F}_{p_0})$ に含まれるかどうか調べる必要がある．

明らかに $-1,1,0\in\mathbb{F}_{p_0}$ であるから $[-1,1,0]\in C(\mathbb{F}_p)$ である．$p_0=p_0(z)\equiv 1 \pmod 3$ を満たすため，$\omega\in\mathbb{F}_{p_0}$ である．よって，$[-1,\omega,0]\in C(\mathbb{F}_{p_0})$ である．同様に，$[-1,\omega^2,0]\in C(\mathbb{F}_{p_0})$ である．従って，$C(\mathbb{F}_{p_0})$ の無限遠点は $[1,-1,0]$, $[1,\omega,0]$, $[1,\omega^2,0]$ の 3 点である．

(2-ii) $E_-: y^2=x^3-432$ と $C: u^3+v^3+1=0$ に対して写像 $\zeta: E_-(\mathbb{F}_{p_0})\to C(\mathbb{F}_{p_0})$ と写像 $\xi: C(\mathbb{F}_{p_0})\to E_-(\mathbb{F}_{p_0})$ を以下のように定義する．

$$\zeta: E_-(\mathbb{F}_{p_0})\to C(\mathbb{F}_{p_0})\ :\ (x,y)\to\left(\frac{-36+y}{6x},\frac{-36-y}{6x}\right)$$

$$\xi: C(\mathbb{F}_{p_0})\to E_-(\mathbb{F}_{p_0})\ :\ (u,v)\to\left(\frac{-12}{u+v},\frac{u-v}{u+v}\right)$$

ここで $p_0\geq 5$ であるため $\mathbb{F}_{p_0}$ では 6 での除算が可能であることに注意. 正確には, ζ は $E_-(\mathbb{F}_{p_0})$ の無限遠点と $x=0$ となる点に対しては定義されないが, その他の点 $(x,y)\in E_-(\mathbb{F}_{p_0})$ に対して，$\zeta(x,y)\in C(\mathbb{F}_p)$ となる．同様に，ξ は $C(\mathbb{F}_{p_0})$ の無限遠点と $u+v=0$ となる点 (u,v) に対しては定義されないが，その他の点 $(u,v)\in C(\mathbb{F}_{p_0})$ に対して，$\xi(x,y)\in E_-(\mathbb{F}_{p_0})$ となる．従って，集合 $E_-^{\mathcal{O}}, E_-^{x=0}, C^{\mathcal{O}}, C^{u+v=0}$ を

$$\begin{array}{rcl} E_-^{\mathcal{O}} & = & \{E_-(\mathbb{F}_{p_0})\text{ の無限遠点の全体 }\} \\ E_-^{x=0} & = & \{(x,y)\in E_-(\mathbb{F}_{p_0}): x=0\} \\ C^{\mathcal{O}} & = & \{C(\mathbb{F}_{p_0})\text{ の無限遠点の全体 }\} \\ C^{u+v=0} & = & \{(u,v)\in C(\mathbb{F}_{p_0}): u+v=0\} \end{array}$$

と定義すると，ζ と ξ が正確に定義できる．

$$\begin{aligned} \zeta: E_-(\mathbb{F}_{p_0})\backslash(E_-^{\mathcal{O}}\cup E_-^{x=0}) &\to C(\mathbb{F}_{p_0}) \\ (x,y) &\mapsto \left(\frac{-36+y}{6x},\frac{-36-y}{6x}\right) \\ \xi: C(\mathbb{F}_{p_0})\backslash(C^{\mathcal{O}}\cup C^{u+v=0}) &\to E_-(\mathbb{F}_{p_0}) \\ (u,v) &\mapsto \left(\frac{-12}{u+v},\frac{u-v}{u+v}\right) \end{aligned}$$

すべての $(x,y)\in E_-(\mathbb{F}_{p_0})\backslash(E_-^{\mathcal{O}}\cup E_-^{x=0})$ に対して，$\xi\circ\zeta(x,y)=(x,y)$ が成り立ち，すべての $(u,v)\in C(\mathbb{F}_{p_0})\backslash(C^{\mathcal{O}}\cup C^{u+v=0})$ に対して $\zeta\circ\xi(u,v)=(u,v)$ が成り立つ．つまり，ζ と ξ は一対一写像であり

$$\begin{aligned} &\#E_-(\mathbb{F}_{p_0})\backslash(E_-^{\mathcal{O}}\cup E_-^{x=0}) \\ &\quad=\#C(\mathbb{F}_{p_0})\backslash(C^{\mathcal{O}}\cup C^{u+v=0}) \end{aligned} \tag{7}$$

となる．従って，$\#E_-(\mathbb{F}_{p_0})$ と $\#C(\mathbb{F}_{p_0})$ の関係を知るには，$\#E_-^{\mathcal{O}}, \#E_-^{x=0}, \#C^{\mathcal{O}}, \#C^{u+v=0}$ を調べれ

ば良い．**(2-i)** で述べたように，$\#C^{\mathcal{O}}=3$ であり，$\#E_-^{\mathcal{O}}=1$ である．

次に $\#E_-^{x=0}$ を調べる．$x=0$ を E_- の式 $y^2=x^3-432$ に代入すると $y=\pm\sqrt{-432}=\pm12\sqrt{-3}$ となる．z が奇数のとき $p_0=p_0(z)\equiv 3 \pmod 4$ より，ルジャンドル記号の式

$$\left(\frac{-1}{p_0}\right)=-1,\ \left(\frac{3}{p_0}\right)=-\left(\frac{p_0}{3}\right)=-\left(\frac{1}{3}\right)=-1$$

が成り立ち，z が偶数のとき $p_0=p_0(z)\equiv 1 \pmod 4$ より

$$\left(\frac{-1}{p_0}\right)=1,\ \left(\frac{3}{p_0}\right)=\left(\frac{p_0}{3}\right)=\left(\frac{1}{3}\right)=1$$

が成り立つ．従って，z が偶数，奇数どちらの場合でも

$$\left(\frac{-3}{p_0}\right)=\left(\frac{-1}{p_0}\right)\left(\frac{3}{p_0}\right)=1$$

となる．つまり，$\pm12\sqrt{-3}\in\mathbb{F}_{p_0}$ であり，$E_-^{x=0}=\{(0,12\sqrt{-3}),\ (0,-12\sqrt{-3})\}$ となる．従って，$\#E_-^{x=0}=2$ である．

最後に $\#C^{u+v=0}$ を調べる．$v=-u$ を C の式 $u^3+v^3+1=0$ に代入すると，矛盾した式 $1=0$ が得られる．これは $\#C^{u+v=0}=0$ を意味する．

以上から $\#E_-^{\mathcal{O}}=1$, $\#E_-^{x=0}=2$, $\#C^{\mathcal{O}}=3$, $\#C^{u+v=0}=0$ であるため，式 (7) より $\#C(\mathbb{F}_{p_0})=\#E_-(\mathbb{F}_{p_0})$ が得られる．

(2-iii) $n_0|(p_0^{12}-1)$, $n_0\nmid(p_0^i-1)\ (1\le i\le 11)$ より $E_-(\mathbb{F}_{p_0})$ と $C(\mathbb{F}_{p_0})$ は埋込み次数 12 を持つ．また，**(1)** より $\#C(\mathbb{F}_{p_0})=\#E_-(\mathbb{F}_{p_0})=n_0=27(108z^4+324z^3+370z^2+190z+37)$ となるため $\#E_-(\mathbb{F}_{p_0})$ は 27 で割れる．

(2-iv) E_+ と E_- には以下のような写像が存在する．

$$\begin{array}{rcl}\psi: E_+ & \to & E_- \\ (x,y) & \mapsto & (-x,\sqrt{-1})\end{array}$$

$\sqrt{-1}\notin\mathbb{F}_{p_0}$ のとき (つまり z が奇数のとき) ψ は $\mathbb{F}_{p_0^2}$ 上同型となり，E_+ は E_- の 2 次のツイストとなる．E_- のトレースは $-t_0(z)$ であるため，$E_+(\mathbb{F}_{p_0})=p_0(z)+1+(E_-\text{のトレース})=p_0(z)+1-t_0(z)$ となる．

$\sqrt{-1}\in\mathbb{F}_{p_0}$ のとき (つまり z が偶数のとき) ψ は $\mathbb{F}_{p_0}$ 上同型となり，E_+ は E_- の 1 次のツイストとなる．従って $E_+(\mathbb{F}_{p_0})=E_-(\mathbb{F}_{p_0})$ となる．(ツイストの元の個数については 2.2 節を参照)．□

定理 2 の証明:
補題 1 の **(2-iv)** より $p_0(2z+1)$ が素数となる整数 z に対して，$\#E_+(\mathbb{F}_{p_0(2z+1)})=p_0(2z+1)+1-t_0(2z+1)$ となる．$p(z)=p_0(2z+1)$, $n(z)=p_0(2z+1)+1-t_0(2z+1)$ であるから，$p=p(z)$ が素数となる整数 z に対して，$\#E_+(\mathbb{F}_p)=n(z)$ となることが示された．$\rho\approx1$ となることと $\#E_+$ が埋込み次数 12 を持つことは簡単に確かめられる．□

定理 2 は次のように言い換えることができる．

系 1 *Barrto-Naehrig* 法 (*3.2* 節) において，$z\equiv 5$ (*mod 6*) を満たす整数に対して $p'(z)$ が素数となるならば，楕円曲線 $E: y^2=x^3+432$ は $\#E(\mathbb{F}_{p'(z)})=n'(z)$ を満たす．

5.1 例

定理 2 において，$z=62909388675$ を選ぶと $p=p(z)$ と $n=n(z)$ は共に 160 ビットの素数となる．

$p=730750905261752415441280784953441175457046356931$
$n=730750905261752415441279930113745524970523218781$

よって $\mathbb{F}_p$ 上の $y^2=x^3+432$ は埋込み次数 12 の pairing-friendly 楕円曲線である．

5.2 提案手法と従来手法の比較

従来の pairing-friendly 曲線の構成手法では，素数 p，トレース t，式 (3) の平方因子を持たない整数 D を決定し，これらのパラメータを CM 法の入力とし，その出力が目的の楕円曲線となる．CM 法は j 不変数の決定，曲線構成，位数チェックからなっており，j 不変数の決定が CM 法のメインの部分であり，コストもこの三者の中では最も大きい．$D=3$ の場合，j 不変数の決定を省け，曲線構成も式 (2) よりほぼ計算コスト 0 で行うことができる．そのため，Barreto-Naehrig 法のように $D=3$ となる楕円曲線構成法は，効率的な手法である．しかしながら，位数チェックも無視できないコストを要する (3.1 節参照)．

これに対して提案手法は CM 法を全く用いずに pairing-friendly 楕円曲線を構成できる効率的な手法である．

		従来手法		**提案手法**
		$D\neq3$	$D=3$	
素数と位数の決定		必要	必要	必要
CM 法	j 不変数の決定	必要	**不要**	**不要**
	曲線構成	必要	必要 *	**不要**
	位数チェック	必要	必要	**不要**

* 計算コストはほぼ 0

6 まとめ

本稿では $p=p(z)=46656z^4+69984z^3+39744z^2+10116z+973$ が素数となる整数 z と楕円曲線

$$E: y^2=x^3+432$$

に対して位数 $\#E(\mathbb{F}_p)$ が $n(z)=46656z^4+69984z^3+39528z^2+9972z+949$ となり，埋込み次数が 12 かつ $\rho\approx1$ となることを示した．従って，CM 法を用いず，$p(z)$ と $n(z)$ が共に素数となる z の探索のみで pairing-friendly 楕円曲線を得ることができる．今後

は $p(z)$ と $n(z)$ が素数となる整数 z を効率的に見つけることが課題となる．

従来は平方因子を持たない D を用いて pairing-friendly 楕円曲線を構成していたが，本稿では $D = 27$ の場合を扱い，係数が固定されている pairing-friendly 楕円曲線が得られた．D の平方因子，あるいは立方因子に楕円曲線の係数の情報があるのかも知れない．

参考文献

[1] A. Atkin and F. Morain, "Elliptic Curves and Primality Proving," *Math. Comp.* Vol.61, No.203, pp.29-68, 1993.

[2] P. Barreto, B. Lynn, and M. Scott, "Constructing elliptic curves with prescribed embedding degrees," *SCN 2002*, LNCS 2576, pp.263-273, 2002.

[3] P. Barreto and M. Naehrig, "Pairing-friendly elliptic curves of prime," *SAC 2005*, LNCS 3897, pp.319-331, 2006.

[4] D. Boneh, G. Crescenzo, R. Ostrovsky, and G. Persiano, Public Key Encryption with Keyword Search *EUROCRYPT 2004*, LNCS 3027, pp.506-522, 2004.

[5] D. Boneh and M. Franklin, "Identity based encryption from the Weil pairing," *SIAM Journal of Computing*, Vol. 32, No. 3, pp. 586-615, 2003.

[6] D. Boneh, C. Gentry, B. Lynn, and H. Shacham, H, "Aggregate and Verifiably Encrypted Signatures from Bilinear Maps," *EUROCRYPT 2003*, LNCS 2656, pp.416-432, 2003.

[7] D. Boneh, G. Gentry, and B. Waters, "Collusion resistant broadcast encryption with short ciphertexts and private keys", *CRYPTO 2005*, LNCS 3621, pp.258-275, 2005.

[8] F. Brezing and A. Weng, "Elliptic curves suitable for pairing based cryptography," *Designs, Codes and Cryptography*, Springer–Verlag, Vol.37, No.1, pp 133-141, 2005.

[9] C. Cocks and R. Pinch, "Identity-based cryptosystems based on the Weil pairing," Unpublished manuscript, 2001.

[10] R. Dupont, A. Enge, and F. Morain, "Building curves with arbitrary small MOV degree over finite prime fields," *Journal of Cryptology*, Vol. 18, No. 2, pp. 79-89, 2005.

[11] D. Freeman, "Constructing pairing-friendly elliptic curves with embedding degree 10," *Algorithmic Number Theory*, LNCS 4076, pp.452-465, 2006.

[12] D. Freeman, M. Scott, E. Teske, "A taxonomy of pairing-friendly elliptic curves," `http://theory.stanford.edu/~dfreeman/papers/taxonomy.pdf` .

[13] S. Galbraith, J. McKeea, and P. Valença, "Ordinary abelian varieties having small embedding degree," newblock *Finite Fields and Their Applications*, Vol.13, Iss.4, pp.800-814, 2007.

[14] F. Hess, "Exponent group signature schemes and efficient identity based signature schemes based on pairings", *SAC 2002*, LNCS 2595, pp.310-324, 2002.

[15] F. Hess, N. P. Smart, and F. Vercauteren, "The Eta pairing revisited", *IEEE Transactions on Information Theory*, Vol. 52, pp.4595-4602, 2006.

[16] E. Lee, H. Lee, and C. Park, "Efficient and generalized pairing computation on abelien varieties," IEEE Transactions of Information Theory, Vol.55, No.4, pp.1793-1803, 2009.

[17] S. Matsuda, N. Kanayama, F. Hess, and E. Okamoto, "Optimized versions of the Ate and twisted Ate pairings," *Cryptography and Coding*, LNCS 4887, pp.302-312, 2007.

[18] A. Menezes, T. Okamoto, and S. A. Vanstone, "Reducing elliptic curve logarithms to logarithms in a finite field," *IEEE Transactions on Information Theory*, Vol. 39, pp.1639-1646, 1993.

[19] A. Miyaji, M. Nakabayashi, and S. Takano, "New explicit conditions of elliptic curve traces for FR-reduction," *IEICE Transactions on Fundamentals*, Vol.E84-A, No.5, pp.1234-1243, 2001.

[20] Y. Nogami, M. Akane, Y. Sakemi, H. Kato, and Y. Morikawa, "Integer variable χ-based Ate pairing," *Pairing 2008*, LNCS 5209, pp.178-191, 2008.

[21] R. Sakai, K. Ohgishi, and M. Kasahara, "Cryptosystems based on pairing," *SCIS 2000*, pp. (2000)

[22] J. Silverman, *The arithmetic of elliptic curves*, Springer–Verlag, 1986.

[23] J. Silverman and J. Tate, *Rational points on elliptic curves*, Springer–Verlag, 1992.

[24] S. Tanaka and K. Nakamula, "More constructing pairing-friendly elliptic curves for cryptography," *Transactions of the Japan Society for Industrial and Applied Mathematics*, Vol.17, No.4, pp.595-606, 2007. (in Japanese)

[25] S. Tanaka and K. Nakamula, "Constructing Pairing-Friendly Elliptic Curves Using Factorization of Cyclotomic Polynomials," *Pairing 2008*, LNCS 5209, pp.136-145. 2008.

[26] F. Zhang and K. Kim, "ID-Based Blind Signature and Ring Signature from Pairings," *ASIACRYPT 2002*, LNCS 2501, pp.629-637, 2002.