2004－ＣＳＥＣ－26　（１）
2004／7／20

$(\#E-1)/2$の偶奇の一判定法

小原真由美† 野上 保之† 森川 良孝†

† 岡山大学通信ネットワーク工学科, 岡山県
E-mail: †{obara,nogami,morikawa}@trans.cne.okayama-u.ac.jp

あらまし CM 法を用いて特定の位数をもつ楕円曲線を生成する場合，その候補として 2 つの曲線が得られるため，この候補曲線のどちらが真に目的とする位数をもつ楕円曲線であるのかを判別する必要がある．そこで本稿では，候補となる 2 曲線の位数をそれぞれ $\#E_+$，$\#E_-$ として，$(\#E_+-1)/2$，$(\#E_--1)/2$ の偶奇が相反関係にあることに着目し，この特性をに基づいた判別法を提案する．

キーワード CM 法，3 次既約多項式，平方剰余判定

A Method for Checking the Parity of $(\#E-1)/2$

Mayumi OBARA†, Yasuyuki NOGAMI†, and Yoshitaka MORIKAWA†

† Communication Network Engineering, Okayama University, 3–1–1, Tsushimanaka, Okayama, 700–8530 Japan
E-mail: †{obara,nogami,morikawa}@trans.cne.okayama-u.ac.jp

Abstract When we try to generate a certain order elliptic curve by using CM method, we have two candidate curves at the last step of the calculations; the one is given from the j-invariant, and the other is its twisted elliptic curve. In this paper, we propose a method for distinguishing these two candidate curves. This method is based on the fact that the parities of $(\#E_+-1)/2$ and $(\#E_--1)/2$ are reciprocal to each other, where $\#E_+$ and $\#E_-$ denote the orders of the two candidate curves.

Key words CM method, irreducible cubic polynomial, quadratic power residue/non residue

1. はじめに

近年，RSA 暗号に代わって楕円曲線暗号（ECC）が注目を集めている．その一方で，ECC に対するいくつかの攻撃法も研究されている [1]- [3]．とくに素数位数の楕円曲線はセキュリティ面の観点からだけでなく，実装の簡便性の面においても優れているため，ECC に素数位数の楕円曲線を用いることが推奨される．素数位数楕円曲線を生成するアルゴリズムがいくつか提案されているが，これらを大別すると，一方は位数計算アルゴリズムを用いる方法 [4], [5]，もう一方は虚数乗法（CM 法）を用いる方法 [6], [7] となる．

本稿では，後者の方法を取り扱う．CM 法に基づく方法（CM-Based：以下 CMB 法）では，一般に次のようにして処理が進められる [8]．まず，楕円曲線の定義体の標数（素数）p に対して，楕円曲線のトレースと呼ばれる量 t およびクラスパラメータと呼ばれる量 D を決定する．次に $p+1\pm t$ のいずれかが素数であれば，それを目標位数 X に定める．そして，D に応じてクラス多項式と呼ばれる多項式 $H_D(x)$ を求め，$H_D(x)$ の零点を計算する．この零点が j-不変量となり，j-不変量から目標位数をもつ曲線の候補として，2 つの曲線を得るが，j-不変量からのみではこれを一意に決定することはできない．そこで最後に，これらの候補のどちらが目標位数をもつかどうかを判別して出力する．既存の CMB 法に関する研究では，クラス多項式 $H_D(x)$ と j-不変量をそれぞれ高速に計算するアルゴリズムが取り扱われてきた．しかし，最後の処理である位数判別では，曲線上の適当な有理点を選び，その有理点の目標位数によるスカラー倍点を計算することによりこれを行っている．暗号に用いられる標数や位数は 160 ビット程度の大きさであるため，スカラー倍算による位数判別も重い処理となる．本稿ではこの位数判定の高速化を提案する．

楕円曲線とは $E(x,y)\equiv x^3+ax+b-y^2=0$ を満たす有理点 $(x,y)\in {F_p}^2$ の集合で，無限遠点も含めたこの集合を $E(F_p)$ で表し，$E(F_p)$ の総数を $\#E(F_p)$ で表す．この曲線が位数 2 の有理点をもたない場合，$E(x,0)$ は 3 次既約多項式であり，$E(i,0)(E(i,0)\neq 0, \forall i\in F_p)$ が平方剰余であるとき，$(i,\pm\sqrt{E(i,0)})$ が有理点となり，平方非剰余ならば有理点とならない．したがって $E(i,0)$ の平方剰余な個数を N とすれば，楕円曲線の位数は $\#E(F_p)=2N+1$ となる．位数

$\#E(F_p)$ を $\#E(F_p) = p+1 \pm t$ と表したときの t を $E(F_p)$ のトレースという．$\#E(F_p)$ が素数であり，標数 p は 3 より大きい素数であることから，t は奇数であることが必要であり，$N_{\pm} = (\#E_{\pm}(F_p) - 1)/2 = (p \pm t)/2$（複合同順）は符号 $\pm$ に対して両者の偶奇が一致することはない．すなわち，$N_{\pm}$ のいずれかが奇数で、残りが偶数となる．

ところで，筆者らは既約多項式の自動生成を目的として既約多項式の変換に興味をもっている．その一つにシフト積に基づく多項式変換（Shift Product-based Polynomial Transform；以下 SPPT）がある．$E(x,0)$ の SPPT を $\tilde{E}(x,0)$ と記せば $\tilde{E}(x^p - x, 0) = \prod_{i=0}^{p-1} E(x+i,0)$ となる．$x = 0$ とおけば $\tilde{E}(0,0) = \prod_{i=0}^{p-1} E(i,0)$ となる．p 個の $E(i,0)$ のうち，N 個が平方剰余，$p - N$ 個は平方非剰余なので，$\tilde{E}(0,0)^{(p-1)/2} = (-1)^{p-N} = -(-1)^N$ が得られる．つまり，N の偶奇により $\tilde{E}(0,0)$ が平方剰余であるか否かが決定できるため，$\tilde{E}(0,0)$ の平方剰余判定を実行することで N の偶奇が判別できる．$\tilde{E}(x,0)$ の定数項は容易に計算でき，また平方剰余判定も高速に実行できるため，スカラー倍算を行う方法に比べて高速になることが期待できる．加えて本稿では，4 が p-1 を割り切るとき，提案法は SPPT すら必要とせず，平方剰余の判定のみで位数の偶奇判定が可能となることを示す．

実際に提案法を用いた位数の判別を行ったところ，4 が p-1 を割り切らないときも，4 が p-1 を割り切るときも，提案法は従来法より高速に位数判定を行うことができた．とくに 4 が p-1 を割り切るとき，提案法は従来法の 20〜30 倍の速さで判別を行うことができた．

本稿ではとくに位数 2 の点をもたない楕円曲線を扱い，有限体 F_q の標数 p は 3 より大きい素数とする．また，$X \mid Y$ と $X \nmid Y$ はそれぞれ，X は Y を割り切る，X は Y を割り切らないことを意味し，$X \| Y$ は X は Y を割り切るが，X^2 は Y を割り切らないことを意味する．

2. 数学的準備

本節では，平方剰余／非剰余，楕円曲線に関する基礎的な事柄，CM 法を用いた素数位数楕円曲線の生成法とその問題点について簡単に紹介する．

2.1 平方剰余／非剰余

任意の非零元 $c \in F_q$ に対し，F_q において $x^2 = c$ となる x が存在するとき，c を平方剰余（Quadratic residue; QR）といい，存在しないとき，平方非剰余（Quadratic non-residue; QNR）という．この平方剰余判定は次式により行うことができる．

$$c^{(q-1)/2} = \begin{cases} 1 & \text{平方剰余} \\ -1 & \text{平方非剰余} \end{cases} \tag{1}$$

また，非零である 2 つの平方剰余元の積と，2 つの平方非剰余元の積は F_q において平方剰余元となる．一方，平方剰余元と平方非剰余元の積は F_q において平方非剰余元となる．

2.2 定 義 式

標数 p が 3 より大きい有限体 F_q（$q = p^m$）における楕円曲線は次式で定義される．

$$E(x,y) = x^3 + ax + b - y^2 = 0, \quad a,b \in F_q \tag{2}$$

式 (2) の解 $(x,y) \in {F_q}^2$ は，F_q 上の有理点と呼ばれ，この F_q を定義体という．楕円曲線上の有理点は幾何学的に定義された加法に関して可換群を成し，これを $E(F_q)$ で表す．その位数，すなわち曲線上の有理点の総数を $\#E(F_q)$ で表す．次式で与えられるパラメータ t（$t < 0$ も含む）は楕円曲線 $E(F_q)$ のトレースと呼ばれる．

$$t = q + 1 - \#E(F_q) \tag{3}$$

2.3 楕円曲線の位数

式 (2) を次のように書き直す．

$$y^2 = E(x,0) = x^3 + ax + b, \quad a,b \in F_q \tag{4}$$

任意の元 $i \in F_q$ に対して，$E(i,0)$ が F_q 上で平方剰余となるならば，曲線上の 2 つの有理点が以下のように与えられる．

$$\left(i, \pm\sqrt{E(i,0)}\right) \tag{5}$$

本稿では $E(F_q)$ を位数 2 の有理点をもたない楕円曲線としているため，$E(i,0) \neq 0$ であることに注意する．ここで，N を以下で表される平方剰余の集合の個数とする．

$$N = \left| \{ E(i,0) \mid E(i,0)^{(q-1)/2} = 1, \quad \forall i \in F_q \} \right| \tag{6}$$

この N を用いれば，$\#E(F_q)$ は次のように表される．

$$\#E(F_q) = 2N + 1 \quad \text{或は} \quad N = \frac{\#E(F_q) - 1}{2} \tag{7}$$

ここで，式 (7) に現れる 1 は無限遠点 $\mathcal{O}$ に対応している．位数 2 の有理点をもつための必要十分条件は，式 (2) から与えられる $E(x,0)$ が F_q 上の 3 次非既約多項式となることである．

2.4 CM 法を用いた素数位数楕円曲線生成法とその問題点

以下に，素体 F_p を定義体として，素数位数の楕円曲線を生成する CMB 法を示す [8]．

入力： 標数 p

出力： F_p 上の素数位数の楕円曲線 $E(x,y)$

Step1： $4p = t^2 + Ds^2, D, t, s \in Z$ を満たす，できるだけ小さい D とそれに付随する t の組を 1 つ求める．

Step2： $p + 1 \pm t$ が素数となるか否かを判定し，素数となる方を目標位数 X として設定する．$p + 1 \pm t$ が共に素数でなければ，Step1 に戻り，別の D と t を求める．

Step3： クラス多項式 $H_D(x)$ を求める．

Step4： $H_D(x)$ の零点 $j \in F_p$ を求め，次式の k を求める．

$$k = j/(1728 - j) \in F_p \tag{8}$$

Step5： Step4 で得た k を用い，$E(x,y)$ を次式で定める．

$$E(x,y) = x^3 + 3kx + 2k - y^2 \tag{9}$$

$E(x,y)$ 上の有理点 P を選び，$XP = \mathcal{O}$ が成立するか否かを判定する．成立する場合は式 (9) を出力し，成立しない場合は，これをツイストした次の曲線を出力する．

$$E'(x,y) = x^3 + 3kc^2x + 2kc^3 - y^2 \tag{10}$$

ただし，c は F_p における平方非剰余元である．

上記のアルゴリズムにおいて，Step1 から Step4 までの計算のうち，クラス多項式 $H_D(x)$ や j の計算に対しては，いくつかの高速なアルゴリズムが提案されている [6], [9]．一方，Step5 に必要な位数計算については，式 (9) 上の有理点 P をランダムに選び，スカラー倍演算を用いて $XP = \mathcal{O}$ を満たすか否かを調べている．そのため，Step5 の検査には楕円スカラー倍算を必要とする．言い換えれば，j の値からのみでは，式 (9) が所望の位数 X をもつか否か，すなわち $p+1\pm t$ のいずれを位数とするかが判別できない．以下では $\#E_{\pm}(F_p) = p+1\pm t$ として，Step5 の新たな検査方法を提案する．

3. シフト積に基づく多項式変換

以下では，素体 F_p を楕円曲線の定義体とした場合について議論する．まず，シフト積に基づく多項式変換 (SPPT) を導入する．次に，楕円曲線の定義式から与えられる 3 次多項式 $E(x,0)$ と SPPT との関係について述べる．

3.1 SPPT

次式で与えられる F_p 上の m 次単位既約多項式を考える．

$$g(x) = \sum_{i=0}^{m} \tilde{g}_i x^i, \quad g_i \in F_p, g_m = 1, g_{m-1} = 0 \tag{11}$$

付録 1 に示すように $p \nmid m$ ならば，次式を満たす m 次単位既約多項式 $g(x)$ が決まる．

$$\tilde{g}(x^p - x) = \prod_{i=0}^{p-1} g(x+i) \tag{12a}$$

$$\tilde{g}(x) = \sum_{i=0}^{m} \tilde{g}_i x^i, \quad \tilde{g}_i \in F_p, \tilde{g}_m = 1, \tilde{g}_{m-1} = 0 \tag{12b}$$

これらの既約多項式 $g(x)$ と $\tilde{g}(x)$ は 1 対 1 の関係にある．このようなことから，$g(x)$ および $\tilde{g}(x)$ を用いて SPPT を式 (13) のように定義できる．以降では，SPPT により得られる多項式に対して ˜ を付して表記する．

$$\text{SPPT}: g(x) \to \tilde{g}(x) \tag{13}$$

3.2 $E(x,0)$ に対する SPPT の性質

前節に紹介した SPPT において，$g(x) = E(x,0)$ を考える．$E(x,0)$ は 2.3 で述べたように F_p 上の 3 次単位既約多項式となることに注意する．このとき，次式を満たす F_p 上の 3 次単位多項式 $\tilde{g}(x)$ が存在し，その 2 次の係数 g_2 は 0 となる．

$$\tilde{g}(x^p - x) = \tilde{E}(x^p - x, 0) = \prod_{i=0}^{p-1} E(x+i, 0) \tag{14}$$

式 (14) に $x = 0$ を代入し両辺を $(p-1)/2$ 乗して，次式を得る．

$$\tilde{g}(0) = \tilde{E}(0,0)^{(p-1)/2} = \prod_{i=0}^{p-1} E(i,0)^{(p-1)/2} \tag{15}$$

2.3 で定義した値 N を用いれば，p 個の $E(i,0)$, $\forall i = 0 \in F_p$ のうち，N 個が平方剰余，$p-N$ 個が平方非剰余であることから，式 (1) を用いて次式が成り立つことが分かる．

$$\tilde{E}(0,0)^{(p-1)/2} = 1^N(-1)^{p-N} = (-1)^{p-N} = -(-1)^N \tag{16}$$

上式の最後の等号では，本稿で取り扱っている標数 p が奇素数であることを用いた．これより次の性質が得られる．

性質 1 式 (14) を満たす F_p 上の 3 次単位既約多項式 $\tilde{E}(x,0)$ の定数項を $\tilde{E}(0,0)$ とする．N を式 (6) で与えられる平方剰余元の個数として，N が奇数であることは $\tilde{E}(0,0)$ が F_p において平方剰余であることの必要十分条件である．

3.3 SPPT の求め方

性質 1 により，3 次既約多項式 $\tilde{E}(x,0)$ の定数項 $\tilde{E}(0,0)$ が求まれば，$\tilde{E}(0,0)$ が F_p 上において平方剰余か否かを判定することにより N の偶奇が判定できることとなる．そこで本節では，SPPT の簡単な求め方について述べる．

3.1 で導入した $g(x)$ と $\tilde{g}(x)$ の零点をそれぞれ ω と τ とすると，付録 1 より $\tau = \omega^p - \omega$ が成り立つ．すなわち $\tilde{g}(x)$ は $\omega^p - \omega$ の F_p に関する最小多項式である．ここで，ω と τ は F_{p^3} の元であり，F_p には属さないことに注意する．このとき，付録 2 で示すように，$m = 3$ のとき式 (12b) で与えられる $g(x)$ から，以下に示す 2 つの候補式 $\tilde{g}_{\pm}(x)$ を得ることができる．

$$\tilde{g}_{\pm}(x) = x^3 + 3g_1x \pm \sqrt{-(4g_1^3 + 27g_0^2)} \quad \text{(複合同順)} \tag{17}$$

ただし，g_0, g_1 はそれぞれ，$g(x)$ の 0 次および 1 次の係数である．$g(x)$ が既約であるとき，式 (17) 中の $-(4g_1^3 + 27g_0^2)$ は F_p において必ず平方剰余となることに注意する [10]．$\tilde{g}(x)$ が $\tilde{g}_+(x)$ であるか $\tilde{g}_-(x)$ であるかは，$\tilde{g}(x)$ と $g(x)$ が式 (12a) の関係を満たすことを用いて，次式により判定できる．

$$\tilde{g}(x) = \begin{cases} \tilde{g}_+(x) & g(x) \mid \tilde{g}_+(x^p - x) \\ \tilde{g}_-(x) & g(x) \mid \tilde{g}_-(x^p - x) \end{cases} \tag{18}$$

式 (18) を検証するには，$\tilde{g}_+(x^p - x)$ が $g(x)$ により割り切られるか否かを調べればよく，これには $O(\log p)$ 程度の計算量の多項式除算を必要とする．

4. CMB 法の改良

本節では，性質 1 を用いて，2.4 に示した Step5 の改良法を示す．以下において，楕円曲線の定義体は素体 F_p とする．

4.1 提 案 法

$\#E(F_p)$ の位数が $\#E_+(F_p)$ であるか $\#E_-(F_p)$ であるかを判別するため，$(\#E_{\pm}(F_p) - 1)/2$ の偶奇について調べる．

$(\#E_{\pm}(F_p) - 1)/2$ の偶奇性

本稿では定義式 $E(x,y)$ が位数 2 の有理点をもたない場合を考

えているので，位数 $\#E(F_p)$ とトレース t の両者は奇数となる．加えて，p が奇数であることに注意すれば，$(\#E_+(F_p)-1)/2$ が奇数であることと $(\#E_-(F_p)-1)/2$ が偶数であることが必要十分の関係になる．このことは，次式より理解できる．

$$\begin{cases} 2||(p-t) & \text{ならば} \quad 4|\{(p-t)+2t\} \\ 4|(p-t) & \text{ならば} \quad 2||\{(p-t)+2t\} \end{cases} \tag{19}$$

まとめると，以下のような性質となる．

性質 2 $(\#E_+(F_p)-1)/2$ と $(\#E_-(F_p)-1)/2$ の偶奇は相反関係にある．

この事実を用いて，2.4 で紹介した CMB 法の Step5 の代わりに Step5' を提案する．Step5' においては，3 次単位既約多項式 $E(x,0)=x^3+3kx+2k$ に対して，3.3 で示した SPPT 計算により式 (14) を満たす $\tilde{E}(x,0)$ を求め，以下に示す値 $T\in F_p$ を計算する．

$$T=\tilde{E}(0,0)^{(p-1)/2}=\left(\pm\sqrt{-(108k^3+108k^2)}\right)^{(p-1)/2} \tag{20}$$

ただし，符号の選択は式 (18) の多項式除算の結果行う．$\#E(F_p)$ を式 (9) の位数とすると，式 (16) より次式を得る．

$$N=\frac{\#E(F_p)-1}{2}=\begin{cases} odd & T=1 \text{ の場合} \\ even & T=-1 \text{ の場合} \end{cases} \tag{21}$$

性質 1 と性質 2 により，T の値から N の偶奇が分かり，$\#E(F_p)$ の位数が $\#E_+(F_p)$ であるか $\#E_-(F_p)$ であるかを判定する．$\#E(F_p)$ が Step2 で設定した位数 X でなかった場合は，ツイストした楕円曲線式 (10) が目的の位数をもつこととなる．

Step5': 式 (20) により得た T の値により，式 (21) を用いて N の偶奇が分かるので，これにより $\#E(F_p)$ が $\#E_+(F_p)$ であるか $\#E_-(F_p)$ であるかを判定する．Step2 で設定した $(X-1)/2$ と $(\#E(F_p)-1)/2$ の偶奇が一致しなかった場合にはツイストした曲線を出力する．

4 が $p-1$ を割り切る場合

2.4 の Step5 では，有理点に対するスカラー倍演算が必要であった．一方，Step5' は $\tilde{E}(0,0)$ が F_p において平方剰余であるか否かのみで判定できるものの，SPPT のための多項式除算を必要とする．しかしながら，4 が $p-1$ を割り切る場合，$(p-1)/2$ は必ず偶数となるため，$\tilde{E}(0,0)$ が F_p において平方剰余か否かは次式のように簡単に判定できる．

$$\begin{aligned} \tilde{E}(0,0)^{(p-1)/2} &= \left(\pm\sqrt{-(108k^3+108k^2)}\right)^{(p-1)/2} \\ &= \left(\left(\pm\sqrt{-(108k^3+108k^2)}\right)^2\right)^{(p-1)/4} \\ &= (-108k^3-108k^2)^{(p-1)/4} \end{aligned} \tag{22}$$

つまり，式 (22) の結果は符合 $\pm$ に依存しない．それゆえ，4 が $(p-1)$ を割り切る場合には，N の偶奇を SPPT を実際に行うことなく簡単に判定できる．有理点のスカラー倍演算および多項式演算と比較して，式 (22) の計算は格段に速い．

表 1　Step5, Step5', Step5" の計算時間

[単位:ms]

	characteristic p	Step5	Step5'	Step5"
$4\nmid(p-1)$	$2^{160}+7$	149	45.3	–
	$2^{160}+291$	116	45.3	–
	$2^{200}+235$	131	64.4	–
	$2^{200}+1027$	164	63.8	–
	$2^{240}+115$	177	88.4	–
	$2^{240}+751$	248	89.6	–
	$2^{280}+547$	303	126	–
	$2^{280}+651$	238	127	–
$4\mid(p-1)$	$2^{160}+357$	113	–	4.83
	$2^{160}+421$	115	–	4.77
	$2^{200}+687$	170	–	6.59
	$2^{200}+1285$	131	–	6.73
	$2^{240}+325$	180	–	8.99
	$2^{240}+897$	248	–	8.95
	$2^{280}+45$	301	–	12.3
	$2^{280}+633$	364	–	12.5

PentiumIII(846MHz)

そこで 4 が $p-1$ を割り切る場合には，3 次既約多項式 $\tilde{E}(x,0)=x^3+3kx+2k$ に対し，式 (22) より以下に示す値 $T\in F_p$ を計算する．

$$T=\tilde{E}(0,0)^{(p-1)/2}=(-108k^3-108k^2)^{(p-1)/4} \tag{23}$$

それ以降は Step5' と同様にして，T の値と N の偶奇の組み合わせから $\#E(F_p)$ が $\#E_+(F_p)$ であるか $\#E_-(F_p)$ であるかを判定する．$\#E(F_p)$ が Step2 で設定した位数 X でなかった場合は，曲線 $E(x,y)$ をツイストした曲線を出力する．これを Step5" として以下にまとめる．

Step5": 式 (23) により得た T の値から，式 (21) により N の偶奇が分かるので，これにより $\#E(F_p)$ が $\#E_+(F_p)$ であるか $\#E_-(F_p)$ であるかを判定する．Step2 で設定した X と $\#E(F_p)$ が一致しなかった場合にはツイストした曲線を出力する．

4.2 シミュレーション結果

表 1 は隣の Step5, Step5', Step5" の平均計算時間を示している．このシミュレーションは PentiumIII(846MHz) 上で C 言語と NTL を用いて行った．表より，Step5' と Step5" の計算時間は Step5 の計算時間より速いことが分かる．とくに，Step5" の計算時間は Step5 より 20〜30 倍も速い．この結果から，CM 法の入力においては $4\mid(p-1)$ を満たす標数 p を選ぶと良いことが分かる．Savas らによると，標数 p が 192 ビットのとき，PentiumIII(450MHz) を用いて，素数位数の楕円曲線が約 3 秒で生成できる [7]．このことから，4 が $p-1$ を割り切るとき，提案法を用いることで生成時間の 1〜2 割程度の削減が見込める．

5. ま と め

本稿ではまず，CM 法によって得られる 2 つの候補曲線の位数 $\#E_\pm$ から計算される $(\#E_\pm-1)/2$ の偶奇が互いに相反関

係にあることについて示した．次に，シフト積に基づく多項式変換；$(E(x,0) \to \tilde{E}(x,0))$ を導入し，$(\#E_{\pm}-1)/2$ の偶奇が $\tilde{E}(0,0)$ の平方剰余判定で決定できることを示した．4 が（標数-1）を割り切るとき，提案法は SPPT さえ必要とせず，平方剰余判定のみで位数の判定が可能となる．提案法では，偶奇の判定を従来の候補決定法に比べての 20〜30 倍の速さで実行可能であり，楕円曲線の生成時間の 1〜2 割程度の削減が見込まれる．

文　献

[1] T.Satoh and K.Araki, "Fermat Quotients and the Polynomial Time Discrete Log Algorithm for Anomalous Elliptic Curve," Commentarii Math. Univ. Sancti. Pauli, vol.47, no.1, pp.81-92, 1988.

[2] G.Frey and H.Rück,"A Remark Concerning m-Divisibility and the Discrete Logarithm in the Divisor Class Group of Curves," Math Comp. no.**62**, pp.865-874, 1994.

[3] P.Gaudry, F.Hess, ans N.Smart, "Constructive and Destructive Facets of Weil Descent on Elliptic Curves," Hewlett Packard Tech. Report, HPL-2000-10, 2000.

[4] K.Horiuchi et al., "Construction of Eliptic Curves with Prime Order and Estimation of Complexity," IEICE Trans A., vol.J82, no.8, pp.1269-1277, 1999.

[5] Y.Nogami and Y.Morikawa, "Fast Generation of Elliptic Curves with Prime Order over $F_{p^{2^c}}$," Proc. of Workshop on Coding and Cryptography 2003, pp.347-3, 2003.

[6] E.Konstantinou et al., "On the Construction of Prime Order Elliptic Curves," Indocrypto2003, vol.LNCS 2904, pp.309-322, 2003.

[7] E.Savas, T.Schmidt, and C.Koc, "Generating Elliptic Curves of Prime Order," CHES2001, vol.LNCS2162, pp.142-158, 2001.

[8] I.Blake, G.Seroussi, and N.Smart, Elliptic Curves in Cryptography, LNS 265, Cambridge University Press, 1999.

[9] Class Polynomials of CM-fields, http://www.exp-math.uni-essen.de/zahlentheorie/classpol/class.html

[10] T.Hiramoto, Y,Nogami, and Y.Morikawa, "A Fast Algorithm to Test Irreducibility of Cubic Polynomial over GF(P)," IEICE Trans. vol.J84-A no.5, 2000.

[11] A Library for Number Theory, http://www.shoup.net/ntl/.

[12] R.Lidl amd H.Niederreiter, Finite Fields, Encyclopedia of Mathematics and Its Applications, Cambridge University Press, 1984.

付　録

1. 式 (12a)，式 (12b) の証明

$g(x)$ の零点 $\omega \in F_{p^m}$ は，$g_{m-1}=0$ より $\mathrm{Tr}(\omega)=0$ を満たす．$\prod_{i=0}^{p-1}(g+i)$ を零点 ω とその共役元を用いて因数分解し，これを ω の次数に注目してまとめると，次式が得られる．

$$\prod_{i=0}^{p-1} g(x+i) = \prod_{i=0}^{p-1}(x-\omega+i)\prod_{i=0}^{p-1}(x-\omega^p+i)\cdots\prod_{i=0}^{p-1}(x-\omega^{p^{m-1}}+i)$$
$$= \prod_{I=0}^{m-1}\left(x^p - x - (\omega^p-\omega)^{p^i}\right) \qquad \text{(A·1)}$$

ここで，$\tau=\omega^p-\omega$ が F_{p^m} の真部分体 F_{p^r} に属すると仮定すると次式を得る．

$$\tau+\tau^p+\cdots+\tau^{p^{r-1}}$$
$$=(\omega^p-\omega)+(\omega^{p^2}-\omega^p)+\cdots+(\omega^{p^r}-\omega^{p^{r-1}})$$
$$=\omega^{p^r}-\omega \qquad \text{(A·2)}$$

ω は真部分体 F_{p^r} には属していないので，式 (A·2) 右辺の $\omega^{p^r}-\omega$ は 0 ではない．一方，$\mathrm{Tr}(\tau)=\tau+\tau^p+\cdots+\tau^{p^{r-1}}$ は τ の共役元の総和であり，その結果は F_p に属するため，これを $\mathrm{Tr}(\tau)=c\in F_p$ とすれば，次式を得る．

$$c+c^{p^r}+c^{p^{2r}}+\cdots+c^{p^{m'r}}$$
$$=(\omega^{p^r}-\omega)+(\omega^{p^r}-\omega)^{p^r}$$
$$+(\omega^{p^r}-\omega)^{p^{2r}}+\cdots+(\omega^{p^r}-\omega)^{p^{m'r}} \qquad \text{(A·3)}$$

ここで，$c\in F_p$ より $c^p=c$ であることに注意すれば次式を得る．

$$(m'+1)c=\omega^{p^m}-\omega$$
$$(m'+1)c=0 \qquad \text{(A·4)}$$
$$\text{ただし，}m'=m/r-1$$

本稿では標数 p が拡大次数 m で割り切れない場合を扱う．$p\nmid m$ であるため，式 (A·4) を満たすには $c=0$ でなくてはならない．したがって，このことは式 (**??**) に矛盾する．よって τ は真部分体 F_{p^r} には属さないことが分かる．生成される $\tilde{g}(x)$ は F_p の m 次既約多項式になる．加えて，$\tilde{g}(x)$ の零点 $\tau=\omega^p-\omega$ は次式を満たすことから，その $m-1$ 次係数 $\tilde{g}_{m-1}$ は 0 となる．

$$-\tilde{g}_{m-1}=\mathrm{Tr}(\tau)=\mathrm{Tr}(\omega^p-\omega)=\mathrm{Tr}(\omega)^p-\mathrm{Tr}(\omega)=0 \qquad \text{(A·5)}$$

以上により SPPT を得る．

2. 式 (17) の証明

$g(x)$ と $\tilde{g}(x)$ の零点をそれぞれ ω，τ とする．まず，$g(x)$ の根と係数の関係より ω に関して次式が成り立つ．

$$\begin{cases} \omega+\omega^p+\omega^{p^2}=0 \\ \omega\omega^p+\omega^p\omega^{p^2}+\omega^{p^2}\omega=g_1 \\ \omega\omega^p\omega^{p^2}=-g_0 \end{cases} \qquad \text{(A·6)}$$

同様に τ に関しても次式が成り立つ．

$$\begin{cases} \tilde{g}_2=-\tau-\tau^p-\tau^{p^2} \\ \tilde{g}_1=\tau\tau^p+\tau^p\tau^{p^2}+\tau^{p^2}\tau \\ \tilde{g}_0=-\tau\tau^p\tau^{p^2} \end{cases} \qquad \text{(A·7)}$$

$\tau=\omega^p-\omega$ を式 (A·7) に代用し，式 (A·6) を用いれば，$\tilde{g}_2$，$\tilde{g}_1$，$\tilde{g}_0$ はそれぞれ次のようになる．

$$\tilde{g_2} = -(\tau + \tau^p + \tau^{p^2})$$
$$= (\omega - \omega^p) + (\omega^p - \omega^{p^2}) + (\omega^{p^2} - \omega) = 0 \qquad \text{(A·8a)}$$
$$\tilde{g_1} = \tau\tau^p + \tau^p\tau^{p^2} + \tau^{p^2}\tau$$
$$= (\omega^p - \omega)(\omega^{p^2} - \omega^p) + (\omega^{p^2} - \omega^p)(\omega - \omega^{p^2}) + (\omega - \omega^{p^2})(\omega^p - \omega)$$
$$= \omega\omega^p + \omega^p\omega^{p^2} + \omega^{p^2}\omega - \omega^2 - \omega^{2p} - \omega^{2p^2}$$
$$= 3(\omega\omega^p + \omega^p\omega^{p^2} + \omega^p\omega) - (\omega - \omega^p - \omega^{p^2})^2$$
$$= 3g_1 \qquad \text{(A·8b)}$$
$$\tilde{g_0} = -\tau\tau^p\tau^{p^2}$$
$$= (\omega - \omega^p)(\omega^p - \omega^{p^2})(\omega^{p^2} - \omega)$$
$$= A - B \qquad \text{(A·8c)}$$

ただし $\begin{cases} A = \omega\omega^{2p} + \omega^p\omega^{2p^2} + \omega^{p^2}\omega^2 \\ B = \omega^2\omega^p + \omega^{2p}\omega^{p^2} + \omega^{2p^2}\omega \end{cases}$

次に，$A - B$ を g_1 および g_0 で表現するため，A，B の和と積を計算する．

$$A+B = \omega\omega^p(\omega + \omega^p) + \omega^p\omega^{p^2}(\omega^p + \omega^{p^2}) + \omega^{p^2}\omega(\omega^{p^2} + \omega)$$
$$= (\omega + \omega^p + \omega^{p^2})(\omega\omega^p + \omega^p\omega^{p^2} + \omega^p\omega^{p^2}) - 3\omega\omega^p\omega^{p^2}$$
$$= 3g_0 \qquad \text{(A·9a)}$$
$$AB = \left((\omega\omega^p)^3 + (\omega^p\omega^{p^2})^3 + (\omega^{p^2}\omega)^3\right) + \omega\omega^p\omega^{p^2}\left((\omega^3 + \omega^{3p} + \omega^{3p^2}) + 3\omega\omega^p\omega^{p^2}\right)$$
$$= \left((\omega\omega^p + \omega^p\omega^p + \omega^{p^2}\omega) - 3\omega\omega^p\omega^{p^2}(A+B) - 6(\omega\omega^p\omega^{p^2})^2\right) + \omega\omega^p\omega^{p^2}\left((\omega + \omega^p + \omega^{p^2})^3 - 3(A+B) - 3\omega\omega^p\omega^{p^2}\right)$$
$$= (\omega\omega^p + \omega^p\omega p + \omega^{p^2}\omega)^3 + 9(\omega\omega^p\omega^{p^2})^2$$
$$= g_1^3 + 9g_0^2 \qquad \text{(A·9b)}$$

式 (A·9a)，式 (A·9b) を用いて次式のように $\tilde{g_0}$ を得る．

$$\tilde{g_0} = A - B = \pm\sqrt{(A+B)^2 - 4AB}$$
$$= \pm\sqrt{-(4g_1^3 + 27g_0^2)} \qquad \text{(A·10)}$$