日本応用数理学会論文誌
Vol. 13, No. 2, 2003, pp. 273～288

有限体上の楕円曲線の位数計算アルゴリズム

佐藤 孝和*
* 埼玉大学理学部数学科

On Algorithms for Computing Order of Elliptic Curves over Finite Fields

Takakazu Satoh*
* Saitama University

Abstract. This paper surveys recent advances of algorithms for computing order of elliptic curves over finite fields. Let p be the characteristic of the base field of a given elliptic curve. Following a usual convention, we denote a prime different from p by l. Then, for fields of large characteristic, l-adic method known as the SEA algorithm is efficient. Whereas, p-adic method runs much faster for fields of small characteristic.

1 はじめに

p を素数，$q := p^N$ とし，$\mathbf{F}_q$ を q 個の要素を持つ有限体とする．我々の目標は $\mathbf{F}_q$ 上定義された楕円曲線 E が与えられたときその $\mathbf{F}_q$ 有理点のなす群 $E(\mathbf{F}_q)$ の位数を求めるなるべく速いアルゴリズムを求めることである．数論の立場からはこの問題はこれだけで取り組む価値の多いものである．他方，この問題は楕円曲線暗号 (Miller[39], Koblitz[27]) の安全性と密接な関連があり，応用サイドからも速いアルゴリズムが必要とされている．

この問題に対して最初に多項式時間アルゴリズムを与えたのは Schoof[48] である．(本稿では多項式時間とは「$\log q$ に関して多項式時間」と解するものとし，時間計算量は特に断りのない限り bit 演算の数とする．) それ以来，位数計算アルゴリズムの研究は大きく進展した．今では $p = 2$ なら $N = 239$ でも 700MHz の Pentium を使ってわずか 0.4 秒で位数が求まるし (Gaudry[18])，$N = 50021$ に対して Alpha EV6(750Mhz) を使って 63 時間 7 分で位数が求まったとの報告 (Harley[21]) もある．本稿では近年研究が進んだ位数計算の二つの方法：標数が大きいときに用いられる l 進的方法と標数が小さいときに用いられる p 進的方法のそれぞれについて全体像・基本となる考え方を概説する．いずれの方法でも Hasse の関係式を用いて位数を求める問題を Frobenius 写像の trace の値 t を求めることに帰着させる．

l 進的方法では様々な小さい素数 l に対して $t \bmod l$ を求め，それから t を復元する．Schoof のアルゴリズムもこの範疇に属する．Schoof のアルゴリズムは E の l 分点のなす群全体から $t \bmod l$ を読みとるのであるが，Elkies[13] はある種の l に対してはその部分群から $t \bmod l$ を求めるアルゴリズムを与えた．また，Atkin は Elkies の方法が適用できない l に対して $t \bmod l$ の候補を効率良く絞り込む方法を与えた．今日，このアルゴリズムは三人の名前を冠して SEA アルゴリズムと呼ばれる．この時間計算量は，素朴な乗算アルゴリズムを用いたとすると，$O((\log q)^6)$ である．本稿では l 進的方法としてこの SEA アルゴリズムを解説する．

これに対して p 進的方法では Frobenius 写像を標数 0 の完備離散的付値体上の何らかの意味での作用素に持ち上げる．小さい素数 p が固定されていて $N \to \infty$ としたときの計算量は $O(N^5)$ であり，この状況下では l 進的方法よりも p 進的方法のほうが速い．(ただし，O-constant は p に依存する．) SEA アルゴリズムよりも速い p 進的方法は Satoh[44]($p \geq 5$), Fouquet, Gaudry, Harley[15]($p = 2, 3$), Skjernaa[52]($p = 2$) などにより構成された．この方法は与えられた有限体上の楕円曲線を標準持ち上げと呼ばれる p 進体の不分岐拡大体上定義された特別な曲線に持ち上げる．当初はこのアルゴリズムの領域計算量は $O(N^3)$ であったが Vercauteren, Preneel, Vandewalle[54] により $O(N^2)$ にまで削減された．(領域計算量の厳密な定義については Aho, Hopfcroft, Ullman[1] を参照されたい．ただ，本稿を通して

領域計算量は計算終了までに必要となるメモリーの量と解して差し支えない.) これらの方法は §7で解説される. また, §8 では応用上重要な $p = 2$ の場合に有効である算術幾何平均 (Arithemtic Geometric Mean, AGM) を使うアルゴリズムを解説する. これは Eurocrypt 2001 に於いて Harley[20] によりアナウンスされた非常に速いアルゴリズムである.(詳細は Harley et al.[22] に発表予定とのことである.) p 進的方法にはこのほかにも Frobenius 写像を Monsky-Washnizer cohomology 群へ持ち上げる Kedlaya[25] の方法, 指標和を用いる Lauder, Wang[31, 32] の方法が知られている. これらは楕円曲線よりも広いクラス (超楕円曲線, あるいは一般の代数多様体) に適用可能であるが楕円曲線の位数計算に対してはいまのところ標準持ち上げや AGM を用いる方が速い模様である. これらの方法がどこまで速くできるのかは今後の研究が待たれるところである.

なお, p 進的方法を記述するには完備離散的付値体を避けて通ることはできない. これは数論では極めて基本的な道具であるにもかかわらず数論以外の分野の方には遺憾ながらまったくと言っていいほど知られていない. このため, p 進的方法の解説に先立ち §6 に完備離散的付値体の基本的性質をまとめた.

2 楕円曲線論

ここで楕円曲線の基本的な性質を手短にまとめておこう. 厳密な定義や証明は Silverman[50, 51], Blake, Seroussi, Smart[3], Enge[14] などを参照されたい. k を (必ずしも有限とは限らない) 完全体とする. k 係数の二変数三次式

$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6 \tag{2.1}$$

により定義される代数曲線は一つの無限遠点 $\mathcal{O}$ を持つ. このとき

$$E := \{\,(x,y) \in (k^a)^2 : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\,\} \cup \{\,\mathcal{O}\,\}$$

(ここで k^a は k の代数閉包) が特異点を持たなければ E を (2.1) により k 上定義された楕円曲線というのであった. (2.1) を E の Weierstrass 方程式という. E 上の有理関数 $\tau_E := -X/Y$ は $\mathcal{O}$ における局所 parameter である. 本稿では特に断りのない限り $\mathcal{O}$ における局所 parameter として τ_E を用いる. E には $\mathcal{O}$ を単位元とする可換群の構造が入る. k の代数拡大体 K に対して集合

$$E(K) := \{\,(x,y) \in E : x, y \in K\,\} \cup \{\mathcal{O}\}$$

は E の部分群となる. $E(K)$ を E の K 有理点のなす群, その要素を E の K 有理点という. また $n \in \mathbf{N}$ に対して $nP = \mathcal{O}$ となる $P \in E$ を E の n 分点といい, それらがなす集合を $E[n]$ と書く. これは n 倍写像の核に他ならないから E の部分群であるが, より詳しく k の標数 $\mathrm{char}(k)$ が n を割らなければ Abel 群として $E[n] \cong \mathbf{Z}/n\mathbf{Z} \oplus \mathbf{Z}/n\mathbf{Z}$ となる. 他方, $p := \mathrm{char}(k) > 0$ のときは全ての $e \in \mathbf{N}$ に対して $E[p^e] = \{\mathcal{O}\}$ となるか全ての $e \in \mathbf{N}$ に対して $E[p^e] \cong \mathbf{Z}/p^e\mathbf{Z}$ となるかのいずれかである. 前者の場合 E は超特異, 後者の場合 E は非超特異であるという.

$\mathrm{char}(k) \neq 2$ とする. 簡単のため $a_1 = a_3 = 0$ の場合を考え, $B(X) := X^3 + a_2X^2 + a_4X + a_6$ とおく. $n \in \mathbf{N}$ に対して E 上の n 倍写像はある多項式 $\Psi_n, \Theta_n, \Omega_n$ により

$$(x,y) \to \begin{cases} \left(\frac{\Theta_n(x)}{\Psi_n(x)^2}, \frac{y\Omega_n(x)}{\Psi_n(x)^3}\right) & (n : \text{odd}) \\ \left(\frac{\Theta_n(x)}{B(x)\Psi_n(x)^2}, \frac{\Omega_n(x)}{yB(x)\Psi_n(x)^3}\right) & (n : \text{even}) \end{cases}$$

(ここで Ψ_n と Θ_n は互いに素) と書き表せる. 多項式 $\Psi_n, \Theta_n, \Omega_n$ を n 次等分多項式という.(文献によっては多少定義が異なるものもある.) $P \in E[n] - E[2]$ となる必要十分条件は

P の X 座標が Ψ_n の零点であることである．等分多項式は漸化式を用いて効率良く計算できる．n が奇数なら $\deg \Psi_n = (n^2-1)/2$ となる．$\mathrm{char}(k) = 2$ のときにも同様な結果が成立する (Koblitz[28])．

k 上の楕円曲線 E_1, E_2 が与えられたとき E_1 から E_2 への有理写像 f で $f(\mathcal{O}) = \mathcal{O}$ （$\mathcal{O}$ が二箇所で用いられているが，左辺の $\mathcal{O}$ は E_1 の無限遠点，右辺の $\mathcal{O}$ は E_2 の無限遠点である）を満たすものを E_1 から E_2 への isogeny といい，その全体のなす集合を $\mathrm{Hom}(E_1, E_2)$ と書く．$f \in \mathrm{Hom}(E_1, E_2)$ は k 係数の有理写像であるときに k 上定義されているという．$\mathrm{Hom}(E_1, E_2)$ は E_2 の加法から導かれた演算により群となる．また isogeny は E_1 から E_2 への群準同型写像でもある．特に $\mathrm{Hom}(E, E)$ はこの和と写像の合成に関して（必ずしも可換とは限らない）環になる．これを E の自己準同型環といい $\mathrm{End}(E)$ と書く．k の標数に関わらず $\mathrm{End}(E)$ は常に標数 0 である．よって $m \in \mathbf{Z}$ を $\mathrm{End}(E)$ の元である m 倍写像と同一視できる．(特に E 上の m 倍写像として見ていることを強調するときには m_E と書く．) また $\mathrm{End}(E)$ が標数 0 ということは $m \in \mathbf{Z}$, $m \neq 0$, $f \in \mathrm{End}(E)$ に対して $mf = 0$ ならば $f = 0$ であることを意味する．

通常の代数方程式の根に対して「根の重複度」という概念が定義されたように $f \in \mathrm{Hom}(E_1, E_2)$, $f \neq 0$ に対して $f(P) = \mathcal{O}$ となる P の「重複度」ともいうべき概念が定義される．これは全ての $\mathrm{Ker} f$ の元 (≒“f の根”) P について同じ値となる．これを非分離次数といい，この値が 1 であるとき f は分離的であるという．$f \neq 0$ のとき，$f(P) = \mathcal{O}$ となる P の重複を込めた個数は有限である．これを f の次数といい $\deg f$ と書く．この定義の下で $\hat{f} \circ f = \deg(f)_{E_1}$ かつ $f \circ \hat{f} = \deg(f)_{E_2}$ となる $\hat{f} \in \mathrm{Hom}(E_2, E_1)$ がただ一つ存在する．これを f の双対 isogeny という．便宜上，零写像の次数は 0, 零写像の双対は零写像自身と定める．定義から

$$\hat{\hat{f}} = f. \tag{2.2}$$

さらに $f \in \mathrm{End}(E)$ なら $f + \hat{f} \in \mathrm{End}(E)$ となるが実は $f + \hat{f} = t_E$ となる $t \in \mathbf{Z}$ が存在する．これを f の trace といい $\mathrm{Tr}(f)$ と書く．このとき

$$f^2 - \mathrm{Tr}(f) f + \deg(f) = 0 \tag{2.3}$$

が成立する．また (2.2) から

$$\mathrm{Tr}(\hat{f}) = \mathrm{Tr}(f) \tag{2.4}$$

である．

$f \in \mathrm{Hom}(E_1, E_2)$ で $\deg f = 1$ となるものがあるとき E_1 と E_2 は同型であるという．ところで k 上定義された楕円曲線 E に対して E の j 不変量 $j(E)$ という k の元が $a_1 \sim a_6$ の有理式を用いて定義される．この一般の形は繁雑であるが $a_1 = a_2 = a_3 = 0$ ならば

$$j(E) = 1728 \frac{4a_4^3}{4a_4^3 + 27a_6^2}$$

となる．k 上定義された二つの楕円曲線 E_1, E_2 が同型となる（同型写像は必ずしも k 上定義されなくともよい）必要十分条件は $j(E_1) = j(E_2)$ である．

l を $\mathrm{char}(k)$ と異る素数とする．(数論幾何では考えている曲線（あるいはもっと高次元の代数多様体）の定義体の標数を p, それと異る素数を l により表す慣習がある．) k 上の二つの楕円曲線 E_1, E_2 の間にその次数が l である isogeny が存在する必要十分条件が $\Phi_l(j(E_1), j(E_2)) = 0$ となるような**整数係数**二変数多項式 Φ_l が存在する．これを l 次 modular 多項式という（$\mathbf{C}$ 上の場合は Silverman[51], 一般の場合は Lang[30] 参照.) $\Phi_l(t_1, t_2)$ は変数 t_1, t_2 についてそれぞれ $l+1$ 次式であり，また $\Phi_l(t_1, t_2) = \Phi_l(t_2, t_1)$ を満たす．Φ_l の係数は巨大ではあるが

(Cohen[8]) これらはただ一度だけ計算すれば良い．実際の計算にあたっては種々の方法が知られているが l が数十以上の場合には Lehmann, Maurer, Müller[33] のような方法が効率が良い．また p 進的方法では（小さな素数 p に対して）ただ一つの modular 多項式 Φ_p が用いられるだけなので実用上の問題はない．

G を E の有限部分群とする．このとき楕円曲線 E_0 と分離的な $f \in \mathrm{Hom}(E, E_0)$ でちょうど $\mathrm{Ker} f = G$ となるものが存在する．また E_0 は同型を除いて一意的に定まる．この同型類を E/G と表す．E の Weierstrass 方程式が与えられまた G の各点の座標が分かっている，あるいは

$$g_G(X) := \prod_{P \in G - \{\mathcal{O}\}} (X - \xi(P))$$

（$\xi(P)$ は P の X 座標）が既知であるとき E/G（の一つの）Werierstrass 方程式が Vélu [53] により具体的に与えられている．（なお，G の位数が奇数のときは g_G の代わりに $\tilde{g}_G(X) := \prod_{P \in (G-\{\mathcal{O}\})/\{\pm 1\}} (X - \xi(P))$ の方が良く用いられる．このとき $g_G = \tilde{g}_G^2$ となる．）$P := (x, y) \in (k^a)^2$ に対して $F(P) := y^2 + a_1 xy + a_3 y - x^3 - a_2 x^2 - a_4 x - a_6$ とおき，F_x, F_y をそれぞれ F の x, y に関する偏微分とする．さらに

$$T_G := -\sum_{P \in G - \{\mathcal{O}\}} F_x(P), \qquad W_G := \sum_{P \in G - \{\mathcal{O}\}} \left(\frac{F_y(P)^2}{2} - \xi(P) F_x(P) \right)$$

とおく．このとき E/G として

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + (a_4 - 5T_G)x + a_6 - (a_1^2 + 4a_2)T_G - 7W_G \tag{2.5}$$

がとれ，しかも $\mathrm{Ker} f = G$ となる $f \in \mathrm{Hom}(E, E/G)$ で $\tau_{E/G} \circ f = \tau_E + O(\tau_E)$ となるものがとれる．特に E が短 Weierstrass 形式で与えられている（すなわち $a_1 = a_2 = a_3 = 0$ である）ならば (2.5) もやはり短 Weierstrass 形式となる．また G が各点の座標ではなく $g_G(X)$（あるいは $\tilde{g}_G(X)$）により与えられている場合（p 進位数計算法で Vélu の公式を使うときはこの場合に該当する），T_G, W_G を計算するためには $g_G(X)$（あるいは $\tilde{g}_G(X)$）の最高次から順に 3 次下がったところまでの係数が分かれば十分である．逆に楕円曲線 E_1, E_2 の間に分離的な $f \in \mathrm{Hom}(E_1, E_2)$ で $\deg f$ が奇素数 l $(\neq p)$ かつ $\tau_{E_2} \circ f = \tau_{E_1} + O(\tau_{E_1}^2)$ となるものがあることが分かっているときには E_1 と E_2 の Weierstrass 方程式から $\tilde{g}_{\mathrm{Ker} f}$ を復元できる．l が p よりも十分小さいときに $\tilde{g}_{\mathrm{Ker} f}$ を求める方法は Schoof[49], Elkies[13] などで得られた．これらのアルゴリズムは l 進位数計算法の実行時間を大幅に向上させる鍵とる．

R を k の部分環，M を R の極大イデアル，R_M を R の M に於ける局所化とし R から剰余体 R/M への標準的全射を π とおく．（有限体上の楕円曲線の位数計算で使われるのは k が代数体，R がその整数環，M が R の素イデアルの場合および §6 で説明する k が完備離散的付値体，R がその付値環，M が k の素元で生成されるイデアルの場合である．）楕円曲線 E を定義する Weierstrass 方程式 (2.1) において a_i が全て R に属しているとする．このとき

$$Y^2 + \pi(a_1)XY + \pi(a_3)Y = X^3 + \pi(a_2)X^2 + \pi(a_4)X + \pi(a_6) \tag{2.6}$$

が再び楕円曲線となる（すなわち R/M 上の曲線として特異点を持たない）とき，(2.6) を E の M を法とする還元といい $\pi(E)$ と表す．特に k が R の商体のとき $\pi(\mathcal{O}) = \mathcal{O}$,

$$\pi(x, y) := \begin{cases} \mathcal{O} & (x \notin R_M) \\ (\pi(x), \pi(y)) & (x \in R_M) \end{cases}$$

により $\pi : E(k) \to (\pi(E))(R/M)$ なる群準同型が定義される．（同じ π という関数記号がいろいろな意味で用いられているが C++ などの関数名の多重定義と同じで引数の“型”によ

り区別できるので紛れはない.) 逆に R/M 上の楕円曲線 E_0 が与えられたとき k 上の楕円曲線 E で $\pi(E) = E_0$ となるものを E_0 の持ち上げという. 広義には E と k 上同型な楕円曲線をすべて E_0 の持ち上げという.

再び有限体上 $\mathbf{F}_q$ 上の楕円曲線について考える. Fr_q で q 乗 Frobenius 写像を表す:

$$\mathrm{Fr}_q(a,b) := (a^q, b^q)$$

容易に分かるように $\mathrm{Fr}_q \in \mathrm{End}(E)$ となる. よって $\mathrm{Tr}(\mathrm{Fr}_q)$ が意味を持つが, これに対して Hasse により

$$\#E(\mathbf{F}_q) = 1 + q - \mathrm{Tr}(\mathrm{Fr}_q) \tag{2.7}$$

$$|\mathrm{Tr}(\mathrm{Fr}_q)| \leq 2\sqrt{q} \tag{2.8}$$

であることが証明されている. これから $\#E(\mathbf{F}_q)$ を求めるには $\mathrm{Tr}(\mathrm{Fr}_q)$ を求めれば十分であることが分かる. $\deg(\mathrm{Fr}_q) = q$ であり, (2.3) は

$$\mathrm{Fr}_q^2 - \mathrm{Tr}(\mathrm{Fr}_q)\mathrm{Fr}_q + q = 0 \tag{2.9}$$

となる. これは $\mathrm{End}(E)$ に於ける等式であり, E の等式に翻訳すると

$$\forall P \in E\,[\mathrm{Fr}_q^2 P - \mathrm{Tr}(\mathrm{Fr}_q)\mathrm{Fr}_q P + qP = \mathcal{O}] \tag{2.10}$$

(ここの $+, -$ は E の点の加減算) と同値であることに注意する.

3 l 進位数計算法のアイディア

$q := p^N$ を前節の通りとする. l 進位数計算法の基本的なアイディアは $\mathrm{Tr}\,\mathrm{Fr}_q \bmod l$ をたくさんの小さな奇素数 l (ただし $l \neq p$) に対して求めてそれから $\mathrm{Tr}\,\mathrm{Fr}_q$ を Chinese Reminer Theorem (CRT) で復元しようとすることである. この点をもっとも基本的な Schoof の方法 [48] により見てみよう. (2.10) を使うと整数 t に対して

$$\forall P \in E\,[\mathrm{Fr}_q^2 P + qP = t\mathrm{Fr}_q P]$$

ならば $t = \mathrm{Tr}\,\mathrm{Fr}_q$ でねばならないことが分かる. しかし E の全ての点 P (無限個ある) に対してこれを直接確かめるのではアルゴリズムにならない. すこし条件を弱くして

$$\exists P \in E[l] - \{\mathcal{O}\}\,[\mathrm{Fr}_q^2 P + qP = t\mathrm{Fr}_q P] \tag{3.1}$$

が成立していたらどうであろうか. (2.10) は成立しているのであるから $\mathrm{Fr}_q((t - \mathrm{Tr}\,\mathrm{Fr}_q)P) = \mathcal{O}$ がこの $P \in E[l] - \{\mathcal{O}\}$ に対して成り立つ. Fr_q は明らかに単射だから $(t - \mathrm{Tr}\,\mathrm{Fr}_q)P = \mathcal{O}$. l が素数だから P の位数も素数 l である. ゆえに $t \equiv \mathrm{Tr}\,\mathrm{Fr}_q \bmod l$ でなければならない. また, これから (3.1) は

$$\forall P \in E[l] - \{\mathcal{O}\}\,[\mathrm{Fr}_q^2 P + qP = t\mathrm{Fr}_q P] \tag{3.2}$$

とも同値であることが分かる. (3.2) は l 次等分多項式 Ψ_l を用いて結局のところ $\mathbf{F}_q$ 係数の $O(l^2)$ 次の一変数多項式の等式が成立するかということに帰着される. ここで $t = 0, t = \pm 1, \ldots, t = \pm(l-1)/2$ に対して (3.2) が成立しているかどうかを順次確かめれば $\mathrm{Tr}\,\mathrm{Fr}_q \bmod l$ を得る. 他方, Chebyshev[7] による素数分布の評価からある定数 $c > 0$ があり十分大きな実数

L に対しては$\sum_{l<L}\log l > cL$ となる．最初の $O(\log q)$ 個の奇素数（但し p は除く）に対して上述のようなプロセスを行えばHasse の不等式 (2.8) から $\mathrm{Tr}\,\mathrm{Fr}_q$ が求まる．時間計算量を評価するため $\mathbf{F}_{p^N}$ 係数の二つの ν 次式の乗算が

$$O((N\nu\log p)^{\mu}) \tag{3.3}$$

回の bit 演算で実行できると仮定しよう．(従って素朴乗算では $\mu=2$, Karatsuba 法 [24] なら $\mu=\log_2 3$, 整数に対する Schönhage-Strassen 乗算 [47] あるいは多項式に対する Cantor-Kaltofen 乗算 [5], Schönhage 乗算 [46] を使えば任意の正の ε に対して $\mu=1+\varepsilon$ ととれる.) すると Schoof のアルゴリズムの時間計算量は $O((\log q)^{3\mu+2})$ bit 演算，領域計算量は $O((\log q)^3)$ bit と評価される．なお，Schoof の原論文に忠実にこのアルゴリズムをインプリメントすると時間計算量は $O((\log q)^{3\mu+3})$ となってしまう．このあたりの事情については Enge[14, §5.2] 参照.

4 Elkies の方法

Schoof のアルゴリズムは確かに $\log q$ に関して多項式時間アルゴリズムであるがその計算量はまだだいぶ大きい．ところで $E[l]$ は $\mathrm{Tr}\,\mathrm{Fr}_q$ の $\bmod l$ での情報しか与えないのにその位数は l^2 であり，この点に改善の余地がある．Elkies は p が十分大きく $E[l]$ がもし位数 l の部分群 V で $\mathbf{F}_q$ 上定義されている（すなわち $\mathrm{Fr}_q V=V$ となる；これは V の各点が Fr_q の不動点ということと同値ではない）ものがあるときに $\mathrm{Tr}\,\mathrm{Fr}_q \bmod l$ を時間計算量 $O((\log q)^{1+\mu}l^{\mu})$ で求めるアルゴリズムを与えた（Elkies[13], なおSchoof[49] も合わせて参照されたい）．このような V が存在するような素数 l を E に対する Elkies 素数という．l が E の Elkies 素数であるためには (2.9) を $\bmod l$ でみたときに二つの一次式に分解する（すなわち (2.9) の判別式が $\mathbf{F}_l$ の平方元である）ことが必要十分である．従って l が与えられたときにそれが E に対する Elkies 素数である“確率”はおおよそ 1/2 であることが期待される．従って E の Elkies 素数 $l_1, l_2, \ldots, l_m$ で $\prod_{i=1}^{m} l_i > 4\sqrt{q}$ となる最小の l_m はやはり $O(\log q)$ 程度であると推測される．もちろん，上述のような議論は $\mathrm{Tr}\,\mathrm{Fr}_q$ を計算するのに必要な Elkies 素数の大きさの評価を何ら与えない．実際，一般化された Riemann 予想 (GRH) を仮定しても筆者の知る限り位数計算に於いて現れる Elkies 素数の評価は R. Murty, K. Murty による $O((\log q)^{2+\varepsilon})$ が最善である.(Frey[16, Th. 3.8] 参照；なお，同じオーダーの評価が Ankey[2] から初等的に従う.) これでは Elkies の方法の時間計算量の上限は Schoof の方法以上となってしまう．また，GRH の下では最初の $O(\log q \log\log q)$ 個の素数が全て Elkies 素数ではない楕円曲線が無数に存在する（Montgomery[40, Th. 13.5] の証明に自明な変更を加えれば分かる）．しかし，経験則としてほとんどの楕円曲線に対して $O(\log q)$ 程度の範囲であっても概ね半数の素数が Elkies 素数であるので，以下これが成り立っているとして話を進める．この仮定のもとで Elkies の方法の時間計算量は $O((\log q)^{2\mu+2})$ bit 演算となる．このアイディアを実現するには次の問題点を解決せねばならない.

(1) l が Elkies 素数になるかならないかをどうやって判定するか．先ほど l が Elkies 素数であるための判定条件を (2.9) を使って与えたが実際には $\mathrm{Tr}\,\mathrm{Fr}_q$ はこれから求めようとする値に他ならず我々の目的にはこの判定方法は使えない.

(2) l が Elkies 素数であることが分かったとしてどうやって V を求めるのか.

(3) V が求まったとしてどうやって $\mathrm{Tr}\,\mathrm{Fr}_q \bmod l$ を得るか.

このうち実は (3) が一番簡単である．l が素数だから $\mathbf{Z}/l\mathbf{Z}\cong\mathbf{F}_l$ は体で $E[l]$ は 2 次元 $\mathbf{F}_l$ 線形空間であり，Fr_q は $E[l]$ から $E[l]$ への $\mathbf{F}_l$ 線形写像である．V が $\mathbf{F}_q$ 上定義された位数 l

の部分群というのは V が Fr_q の1次元固有空間であるということにほかならない．Fr_q の V に対する固有値を $\lambda \in \mathbf{F}_l$ とする．Fr_q を $E[l]$ 上の線形写像と見たときの特性方程式は (2.9) を mod l したものだから二次方程式の根と係数の関係を使って $\mathrm{Tr}\,\mathrm{Fr}_q \equiv \lambda + q/\lambda \bmod l$ を得る．λ を求めるには $P \in V - \{\mathcal{O}\}$ に対して $\mathrm{Fr}_q P = \lambda P$ が成立するかどうかを $\lambda = 0, \pm 1, \ldots, \pm(l-1)/2$ に対して順次調べれば良い．なお，いわゆる Baby-Step-Giant-Step (BSGS) のアイディアを乗法的に適用してこの部分を高速化する手法が Dewaghe[12] にある．

Elkies 素数の判定法について考えよう．l が Elkies 素数で V が $\mathbf{F}_q$ 上定義された部分群なら E から E/V への $\mathbf{F}_q$ 上定義された次数 l の isogeny がある．ゆえに $j(E/V) \in \mathbf{F}_q$ かつ $\Phi_l(j(E), j(E/V)) = 0$ でねばならない．この逆は成立するとは限らないが E が非超特異かつ $j(E) \neq 0, 1728$ のときは $\Phi_l(j(E), z) = 0$ となる $z \in \mathbf{F}_q$ があるならば E の $\mathbf{F}_q$ 上定義された位数 l の部分群 V で $j(E/V) = z$ となるものが存在する (Schoof[49, Prop. 6.1])．従って上記の例外を除けば $\deg \gcd(\Phi_l(j(E), Z), Z^q - Z) > 0$ のとき l は Elkies 素数である．(実際に必要なのは Z^q ではなく $Z^q \bmod \Phi_l(j(E), Z)$ であることに注意．よって上記 gcd を求めるときに現れる多項式は高々 l 次式である．)

問題 (1)(3) に比べると (2) は遥かに難しく，そのアルゴリズムを詳細に説明するには保型形式論（黒川，栗原，斎藤 [29] 参照）や虚数乗法論を必要とする．$n, k \in \mathbf{N}$ に対して $d_k(n) := \sum_{m|n, m>0} m^k$ とおき $\omega \in \mathbf{C}, \mathrm{Im}\,\omega > 0, c \in \mathbf{C}^\times$ に対して $\mathbf{C}$ 上の楕円曲線 $E_{\omega,c}$ を

$$Y^2 = X^3 - \frac{c^2 \mathbf{E}_4(\omega)}{48} X + \frac{c^3 \mathbf{E}_6(\omega)}{864}$$

ここで $\mathbf{E}_4(\omega) = 1 + 240 \sum_{n \geq 1} d_3(n) \exp(2\pi i n \omega)$, $\mathbf{E}_6(\omega) = 1 - 504 \sum_{n \geq 1} d_5(n) \exp(2\pi i n \omega)$ により定義する．($\mathbf{E}_4$ や $\mathbf{E}_6$ は保型形式の一例である．) (2) を解く鍵はある ω と c があり $E_{\omega,c}$, $E_{l\omega,c}$ がともにある代数体上定義されてしかも適当な素イデアルによる還元 π により E が $\pi(E_{\omega,c})$ と，E/V が $\pi(E_{l\omega,c})$ と同型になることである．このとき isogeny $E \to E/V$ に対応する isogeny $E_{\omega,c} \to E_{l\omega,c}$ を Weierstrass の $\wp$ 関数で引き戻したものが l 倍写像という具体的に書き下せる写像であることから V を求めることができるのである．詳しくは Elkies[13] や Blake, Seroussi, Smart[3, VII.4] を参照されたい．ここでは以下の点を注意するにとどめる．

(a) Elkies 自身の方法では p は $\log q$ に比して十分大きくなければならない．これは計算の途中で現れる漸化式の係数が $\mathbf{F}_q$ に於いて 0 にならないために必要である．p が小さいときには Couveignes[9, 10], 特に $p = 2$ に対しては Lercier[34] などの方法でこの問題は回避できる．また Lercier, Morain[36] のような実装上の工夫もある．p が十分小さいのならこのような方法に依らずとも p 進的方法を使う方が位数計算は速くできる．しかしながら計算数論の立場からは Weierstrass 方程式だけから V をいかにして効率良く復元するかということはなお興味深い問題である．

(b) Elkies のアイディアを拡張して $\mathrm{Tr}\,\mathrm{Fr}_q \bmod l^n$ を l^n があまり大きくないところまで求めることができる．Couveignes, Morain[11] 参照．これが SEA アルゴリズムが l“進”的方法といわれるゆえんである．

5 Atkin の方法

Atkin は l が Elkies 素数ではないときに $O(l \log q)$ の領域計算量で $\mathrm{Tr}\,\mathrm{Fr}_q \bmod l$ の情報をある程度得る方法を見つけた．Elkies 素数ではない素数は Atkin 素数と呼ばれる．l が Atkin 素数のときは Z の多項式 $\Phi_l(Z, j(E))$ の $\mathbf{F}_q$ 上のすべての既約因子の次数は互いに等しい．この値を r とする．このとき r は $l+1$ の約数でしかも 1 の原始 r 乗根 $\zeta \in \mathbf{F}_{l^2}$ で $(\mathrm{Tr}\,\mathrm{Fr}_q)^2 = q(\zeta + 2 + \zeta^{-1})$ となるものが存在する．すなわち $\mathrm{Tr}\,\mathrm{Fr}_q \bmod l$ の値を一意に定めることはできないがその可能な値を大幅に絞り込むことができる (cf. Schoof[49, Prop. 6.2])．

ただ，Atkin 素数 l を動かすとき $\mathrm{Tr}\,\mathrm{Fr}_q$ の可能な値の個数は用いた Atkin 素数の個数に関して指数関数的に増加する．よって Atkin の方法だけで楕円曲線の位数計算を行うのは多項式時間アルゴリズムではない．しかし，Elkies の方法と組み合わせることにより必要となる Elkies 素数の最大値を小さくすることができる．BSGS と組み合わせることによりさらに必要となる Elkies 素数・Atkin 素数の個数を減らすことができる．これについては Lehmann, Maurer, Müller[33, §6] を参照されたい．

6 完備離散的付値体の性質

p 進的方法の解説に先立ち，本節では完備離散的付値体の性質に関して必要となることをまとめておく．厳密な定義・証明は森田[41]，斎藤[43] を参照されたい．k を体とする．$v \in \mathrm{Map}(k, \mathbf{R})$ は以下の条件を満たすとき k 上の付値であるという：

(V1) 任意の $x \in k$ に対して $v(x) \geq 0$. また $v(x) = 0$ ならば $x = 0$.

(V2) 任意の $x, y \in k$ に対して $v(x+y) \leq v(x) + v(y)$.

(V3) 任意の $x, y \in k$ に対して $v(xy) = v(x)v(y)$.

v が条件 (V2) よりも強い

(V4) 任意の $x, y \in k$ に対して $v(x+y) \leq \max(v(x), v(y))$

を満たすとき v は非アルキメデス的，そうでなければアルキメデス的といわれる．たとえば $x \in \mathbf{Q}$ に対して $v_\infty(x) := |x|$ とおくと v_∞ は $\mathbf{Q}$ 上のアルキメデス的付値である．また k がどのような体であれ，$v_0(0) := 0$, $v_0(x) := 1$ $(x \neq 0)$ と定めると v_0 は k 上の付値である．これを自明な付値という．もともと付値は実数の絶対値の一般化なのであるが，付値論の立場からいうとアルキメデス的付値は例外的であり，圧倒的“多数”の付値は非アルキメデス的である．体とその上の付値の複合概念を付値体というが，どの付値が用いられているかが前後関係から分かるときは単に「付値体 k」などという言い方をする．非アルキメデス的付値のもっとも基本的なものが p 進付値 v_p（ここに p は素数）である．これは $\mathbf{Q}$ 上の付値であり，$v_p(0) := 0$, $v_p(x) := p^{-m}$（ここで $x = p^m \frac{a}{b}$, a, b は p と互いに素な整数）により定義される．

(V3) から $v(k^\times)$ は $\mathbf{R}^\times$ の部分群となる．v が自明ではなくかつ $\mathcal{P} \in k$ で $v(k^\times)$ が $v(\mathcal{P})$ により生成される無限巡回群である（すなわち $v(k^\times) = \{v(\mathcal{P})^n : n \in \mathbf{Z}\}$ となっている）ようなものがあるとき，v は離散的であると言う．またこのような $\mathcal{P}$ で $v(\mathcal{P}) < 1$ であるものを (k, v) の素元という．たとえば素数 p に対して m が p で割れない整数ならば mp は $(\mathbf{Q}, v_p)$ の素元である．他方，$(\mathbf{Q}, v_\infty)$ は離散的ではない．

ところで k に付値 v が定義されているとこれから k 上の距離 d_v が $d_v(x, y) := v(x-y)$ により定義される．実際，これが k 上の距離になることは付値の定義から従う．ゆえに (k, d_v) は距離空間であり，距離空間としての完備化 $(\widehat{k}, d_v)$ が定義される．k の加法・乗法も $\widehat{k}$ 上の連続な二項演算に一意的に延長され，これらの演算に対して $\widehat{k}$ は体になる．v も $\widehat{k}$ 上の連続関数に一意的に延長され（したがって同じ記号 v で書いてもよい），$\widehat{k}$ 上の付値になることが分かる．付値体 $(\widehat{k}, v)$ を付値体 (k, v) の完備化という．たとえば $(\mathbf{Q}, v_\infty)$ の完備化は $(\mathbf{R}, v_\infty)$ である．距離空間を完備化する際には Cauchy 列が重要な役割を果たしていたことを思い出そう．$\mathbf{Q}$ から $\mathbf{R}$ を構成するにはいろいろな方法があるが切断とか縮小閉区間列を使う方法は有理数の順序構造に依存するため v_∞ 以外の付値に対しては無力である．

(k, v) が非アルキメデス的付値体のとき $R_{k,v} := \{x \in k : v(x) \leq 1\}$ は k の部分環で $M_{k,v} := \{x \in k : v(x) < 1\}$ は $R_{k,v}$ の極大イデアルである．$R_{k,v}$ を (k, v) の付値環，$M_{k,v}$ を (k, v) の極大イデアル，$R_{k,v}/M_{k,v}$ を (k, v) の剰余体という．v が前後関係から分かると

きには (k,v) の剰余体を $\overline{k}$ と書く．v が離散的なら $M_{k,v}$ は素元 $\mathcal{P}$ で生成される単項イデアルで $M_{k,v}^n = \mathcal{P}^n R_{k,v}$ である．これを使うと完備離散的付値体の元がどのようなものであるかが分かる：S を $R_{k,v}/M_{k,v}$ の完全代表系とする．(k,v) の剰余体とその完備化 $(\hat{k},v)$ の剰余体は同型だからこれは $R_{\hat{k},v}/M_{\hat{k},v}$ の完全代表系でもある．$x \in R_{\hat{k},v}$ とすると $a_0 \in S$ で $x - a_0 \in M_{\hat{k},v} = \mathcal{P}R_{\hat{k},v}$ となるものがある．よって $x_1 := \mathcal{P}^{-1}(x - a_0) \in R_{\hat{k},v}$ である．同様に $a_1 \in S$ で $x_1 - a_1 \in M_{\hat{k},v}$ となるものがあるから $x_2 := \mathcal{P}^{-1}(x_1 - a_1) \in R_{\hat{k},v}$ となる．このプロセスを繰り返せば $a_0, a_1, \ldots \in S$ および $x_1, x_2, \ldots \in R_{\hat{k},v}$ が定まり任意の $m \in \mathbf{N}$ に対して

$$x = \sum_{n=0}^{m-1} a_n \mathcal{P}^n + x_m \mathcal{P}^m$$

となる．$v(\mathcal{P}^m x_m) \leq v(\mathcal{P})^m \to 0\ (m \to \infty)$ だから $\hat{k}$ において

$$x = \sum_{n=0}^{\infty} a_n \mathcal{P}^n$$

となる．特に $(\mathbf{Q}, v_p)$ に対しては $R_{\mathbf{Q},v_p} = \{a/b : a \in \mathbf{Z},\ b \notin p\mathbf{Z}\}$, $M_{\mathbf{Q},v_p} = \{a/b : a \in p\mathbf{Z},\ b \notin p\mathbf{Z}\}$ となり剰余体は $\mathbf{F}_p$ と同型で，その完全代表系として $\{0, \ldots, p-1\}$ がとれる．$\mathbf{Q}$ の v_p に関する完備化は p 進体と呼ばれ $\mathbf{Q}_p$ と書かれる．その要素を p 進数という．$\mathbf{Q}_p$ の付値環を p 進整数環といい $\mathbf{Z}_p$ と書く．($n \in \mathbf{Z}$ に対して $\mathbf{Z}/n\mathbf{Z}$ を $\mathbf{Z}_n$ と略記することは，初等整数論を除き，整数論ではまずない．) 上に述べたことから $x \in \mathbf{Z}_p$ は

$$x = \sum_{n=0}^{\infty} a_n p^n$$

と一意的に表示されることが分かる．(右辺の和は $\mathbf{Q}_p$ における極限に関して考えていることに注意．これを $\mathbf{R}$ に於ける極限と混同すると意味をなさなくなる．) これより

$$\mathbf{Z}_p/p^m\mathbf{Z}_p \cong \mathbf{Z}/p^m\mathbf{Z} \tag{6.1}$$

であることも分かる．実数が計算機上では有限精度の浮動小数点数として近似的に表現されているのと同じように p 進整数も適当な $m \in \mathbf{N}$ に対して誤差 $v(p)^m$ 迄を認める有限精度で実装するわけだが，(6.1) はこのとき保持すべきデーターが 0 以上 p^m 未満の整数であることを意味する．また一般に非アルキメデス的付値の付値環の元に対して四則演算（ただし，除算は可逆元による割算に限る）をいくら施しても誤差が積もり積もって増大するということはないことが (V4) より示される．これはアルゴリズムの実装という面からは非常に望ましい性質である．

以下 (k,v) を**完備離散的**付値体とし K を k の有限次ガロア拡大とする．(簡単のため K, k の付値環をそれぞれ R_K, R_k と書く．) このとき v は K に一意的に延びる．具体的には $x \in K$ に対して

$$v(x) := v(N_{K/k}(x))^{1/[K:k]}$$

により与えられる．ここで $N_{K/k}(x) := \prod_{g \in \mathrm{Gal}(K/k)} g(x)$ は K/k のノルムである．$v(k^\times)$ は $v(K^\times)$ の部分群である．これらが等しく，かつ，K の剰余体が k の剰余体上分離的なとき K/k は不分岐であるという．前半の条件は k の素元が K の素元でもあることに他ならない．また，k の剰余体が完全体のとき（特に $k = \mathbf{Q}_p$ のとき）後半の条件は常に満たされる．$N \in \mathbf{N}$ に対して $\mathbf{Q}_p$ 上の N 次不分岐拡大は以下のように構成される．$q := p^N$ とおく．$\mathbf{F}_q = \mathbf{F}_p(\overline{\theta})$ となる $\overline{\theta}$ があるが，この $\mathbf{F}_p$ 上の monic な最小多項式を $f(X)$ とおく．$F \in \mathbf{Z}[X]$ で monic かつ $F \bmod p = f$ となるものがある．(必然的に $\deg F = N$ である．)

このとき $\mathbf{Q}_p$ に $F(X)=0$ の根を添加した体 ($\cong \mathbf{Q}_p[X]/\langle F(X)\rangle$) は $\mathbf{Q}_p$ 上の N 次不分岐拡大である．これは常に Galois 拡大となる．さらに付値環は $R:=\mathbf{Z}_p[X]/\langle F(X)\rangle$ で与えられ $R/p^mR \cong (\mathbf{Z}/p^m\mathbf{Z})[X]/\langle F(X) \bmod p^m\rangle$ となる．R/p^mR を計算機上に実装するときはこの右辺を用いる．ここで $R/pR \cong \mathbf{F}_q$ に注意する．

再び一般論に戻り，K/k を完備離散的付値体の有限次不分岐 Galois 拡大とする．k の素元 $\mathcal{P}$ を一つ決める．明らかに $g \in \mathrm{Gal}(K/k)$ は K の（v から導かれた距離に関して）等長写像である．よって各 $m \in \mathbf{N}$ に対して $g_m : R_K/\mathcal{P}^mR_K \to R_K/\mathcal{P}^mR_K$ なる環準同型写像が導かれる．これは特に $m=1$ のとき

$$\mathrm{Gal}(K/k) \ni g \to g_1 \in \mathrm{Gal}(\overline{K}/\overline{k}) \tag{6.2}$$

なる群の準同型写像を与える．実はこれは同型となる．$K/\mathbf{Q}_p$ が不分岐 N 次拡大なら $\overline{K}=\mathbf{F}_{p^N}$, $\overline{\mathbf{Q}_p}=\mathbf{F}_p$ であり $\mathrm{Gal}(\mathbf{F}_{p^N}/\mathbf{F}_p)$ は p 乗写像 Fr_p で生成される巡回群である．ゆえに $\mathrm{Gal}(K/\mathbf{Q}_p)$ の元で (6.2) で Fr_p に写るものがある．これを Frobenius 置換といい，以下，σ により表す．なお $m>1$ のときは σ_m はもはや p 乗写像ではないことに注意しよう．

7 標準持ち上げによる位数計算

p を小さな素数とする．p 進的方法の計算量を考えるときは p を固定し $N\to\infty$ としたときの漸近的増大度を問題とする．K を $\mathbf{Q}_p$ 上の不分岐 N 次拡大とする．$\mathbf{F}_q$ 上の楕円曲線 E_1, E_2 に対してそれぞれの K への持ち上げ $\tilde{E}_1, \tilde{E}_2$ をとる．このとき $F \in \mathrm{Hom}(\tilde{E}_1, \tilde{E}_2)$ に対して $\pi\circ F = f\circ\pi$ となる $f \in \mathrm{Hom}(E_1, E_2)$ が一意的に定まる．これを F の p を法とする還元といい $\pi(F)$ と書く．$\pi : \mathrm{Hom}(\tilde{E}_1, \tilde{E}_2) \to \mathrm{Hom}(E_1, E_2)$ は単射群準同型であるが一般には全射ではない．特に $\pi : \mathrm{End}(\tilde{E}) \to \mathrm{End}(E)$ が全単射になるとき（このとき π は環同型写像となる）$\tilde{E}$ を E の標準持ち上げといい，本稿では $E^\uparrow$ により表す．これは同型を除いて一意的に定まり，

$$\pi : \mathrm{Hom}(E_1^\uparrow, E_2^\uparrow) \to \mathrm{Hom}(E_1, E_2) \tag{7.1}$$

も全単射となる．(Lubin, Serre, Tate[37], Messing[38] 参照.) ゆえに $f \in \mathrm{Hom}(E_1, E_2)$ に対して $\pi(F)=f$ となる $F \in \mathrm{Hom}(E_1^\uparrow, E_2^\uparrow)$ が一意的に定まるが，これを f の持ち上げといい $f^\uparrow$ と書く．

V_q を Fr_q の双対 isogeny とする．$\mathrm{Tr}\, V_q = \mathrm{Tr}\,\mathrm{Fr}_q$ である．$\pi : \mathrm{End}(E^\uparrow) \to \mathrm{End}(E)$ は同型であったから

$$V_q^{\uparrow 2} - (\mathrm{Tr}\,\mathrm{Fr}_q)V_q^\uparrow + q = 0 \tag{7.2}$$

である．簡単のため，$\tau_{E^\uparrow}$ を τ と書くことにする．$\tau\circ V_q^\uparrow$ は $E^\uparrow$ 上の有理関数だから

$$\tau\circ V_q^\uparrow = c_1\tau + c_2\tau^2 + \cdots \qquad (c_i \in K) \tag{7.3}$$

という形に展開される．(7.2) から

$$\tau\circ(V_q^{\uparrow 2} - (\mathrm{Tr}\,\mathrm{Fr}_q)V_q^\uparrow + q) = 0$$

となるがこれに (7.3) を代入して τ の一次の係数を比べ $c_1^2 - (\mathrm{Tr}\,\mathrm{Fr}_q)c_1 + q = 0$ を得る．(このようなことを示すには E の形式群を使うと見通しが良くなる．Silverman[50, Chap. IV] などを参照.) ゆえに

$$\mathrm{Tr}\,\mathrm{Fr}_q = c_1 + \frac{q}{c_1}$$

となる．E が非超特異なら V_q は分離的であり $c_1 \in R^\times$ となる．Hasse の不等式から $\mathrm{Tr}\,\mathrm{Fr}_q$ を復元するには c_1 を $\bmod p^{N/2+O(1)}$ で求めれば良いことが分かる．(Fr_q ではなくその双対である V_q を持ち上げるのはこのためである．) ここに E を標数 0 に持ち上げた効果をはっきりと見てとれる．E を持ち上げなくても E の局所 parmeter τ_E を用いて $\tau_E \circ V_q$ を $\sum_{i=1}^{\infty} d_i \tau_E^i$ $(d_i \in \mathbf{F}_q)$ という形に展開できる．しかし，d_i は標数 p の値でありこれは $\mathrm{Tr}\,\mathrm{Fr}_q \bmod p$ しか与えない．他方，c_i は標数 0 の値だから $\mathrm{Tr}\,\mathrm{Fr}_q$ の真の値を与えることができるのである．

c_1 を効率良く求める方法を考えよう．$\deg V_q = q$ だから $V_q^\uparrow$ を書き下したり，直接 c_1 を求める効率の良い方法はありそうにない．そこで V_q を分解することを考える．$\mathbf{F}_q$ 上の楕円曲線 E が与えられたとき $E^{(i)} := \mathrm{Fr}_p^i E$ とおく．$\mathrm{Fr}_p \in \mathrm{Hom}(E^{(i-1)}, E^{(i)})$ の双対 isogeny を $V_p^{(i)}$ とおく．$\mathrm{Fr}_q = \mathrm{Fr}_p \circ \cdots \circ \mathrm{Fr}_p$ だから $V_q = V_p^{(N)} \circ \cdots \circ V_p^{(1)}$ である．これを持ち上げれば

$$V_q^\uparrow = V_p^{(N)\uparrow} \circ \cdots \circ V_p^{(1)\uparrow}$$

を得る．他方，$E^{(i)\uparrow}$ の $\mathcal{O}$ での局所 parameter を τ_i とおくと $\tau_{i-1} \circ V_p^{(i)\uparrow} = \sum_{m=1}^{\infty} c_m^{(i)} \tau_i^m$ と展開される．ゆえに

$$c_1 = c_1^{(1)} \cdots c_1^{(N)}$$

である．$E^{(i)\uparrow} = \sigma^i(E^\uparrow)$ となるようにとると $c_1^{(i)} = \sigma^{i-1}(c_1^{(1)})$ となることが証明できるので結局 $c_1 = N_{K/\mathbf{Q}_p}(c_1^{(1)})$ となる．ここで $\deg V_p^{(i)} = p$ で p は十分小さいと仮定したので $\mathrm{Ker}V_p^{(1)\uparrow}$ を求めることができ，これに Vélu の公式を使って $c_1^{(1)}$ を求めることができる．

以上が標準持ち上げによる位数計算の全体像である．各段階をもう少し詳しく見てみよう．

まず，標準持ち上げをどう構成するかである．(7.1) が同型だから $\Phi_p(j(E^{(i)\uparrow}), j(E^{(i+1)\uparrow})) = 0$ である．(ここで持ち上げた後の曲線は標数 0 の体上の楕円曲線であり Φ_p を使うことは問題がないことに注意する．) Vercauteren, Preneel, Vandewalle[54, §2] は $z \equiv j(E^{(i)\uparrow}) \bmod p^m$ となる $z \in R$ が求まったなら $\Phi_p(z, z') = 0$ かつ $z' \equiv z^p \bmod p$ となる $z' \in R$ は $z \equiv j(E^{(i+1)\uparrow}) \bmod p^{m+1}$ を満たすことを証明した．z が分かれば z' は Newton 法を使って求めることができる．よって $j(E)$ の R への任意の持ち上げを初期値として上述の方法を繰り返せば $j(E^{(m)\uparrow}) \bmod p^{m+1}$ が時間計算量 $O(N^\mu m^{\mu+1})$, 領域計算量 $O(N^2)$ で求まる．ここで μ は (3.3) において導入された定数である．実は $j(E^{(i)\uparrow}) \bmod p^{N/2+O(1)}$ が分かれば $\mathrm{Tr}\,\mathrm{Fr}_q$ を正しく復元できることが示される．(ただし，O-constant は $c_1^{(i)}$ の計算法にも依存する．) なお，最終的には norm をとってしまうのだから $E^\uparrow$ の代わりにどの $E^{(i)\uparrow}$ を求めても構わない．

$j(E^{(i)\uparrow})$, $j(E^{(i-1)\uparrow})$ が求まったとする．このとき $E^{(i)\uparrow}$, $E^{(i-1)\uparrow}$ の Weierstrass model で $\sigma(E^{(i-1)\uparrow}) = E^{(i)\uparrow}$ となっているものを R の四則演算 $O(1)$ 回で求めることができる．(たとえば $p = 2$ で E が $Y^2 + XY = X^3 + 1/j(E)$ で与えられているのなら $E^{(i)\uparrow}$ の Weierstrass model として $y^2 + xy = x^3 - \frac{36}{j(E^{(i)\uparrow})-1728} x - \frac{1}{j(E^{(i)\uparrow})-1728}$ ととることができる．) $\mathrm{Ker}V_p^{(i)\uparrow}$ が求まれば同型写像 $E^{(i)\uparrow}/\mathrm{Ker}V_p^{(i)\uparrow} \cong E^{(i-1)\uparrow}$ を用いて $c_1^{(i)}$ が計算される．この先は $p = 2$ と $p > 2$ で計算方法が異る．

$p > 2$ のときは

$$\mathrm{Ker}V_p^{(i)\uparrow} = E^{(i)\uparrow}[p] \cap E^{(i)\uparrow}(R^{\mathrm{ur}}) \tag{7.4}$$

(ここで R^{ur} は $\mathbf{Q}_p$ の最大不分岐拡大の付値環) が成立し，Ψ_p の因数分解をとおして $\mathrm{Ker}V_p^{(i)\uparrow}$ を求めることができる (Satoh[44, §3])．ここで標数 p では Ψ_p は p 重根を持つ (Cassels[6]) ので古典的な Hensel の補題では $\mathrm{Ker}V_p^{(i)\uparrow}$ を“取り出す”(正確には Ψ_p の $(p-1)/2$ 次の因子を求める) ことはできない．しかし Hensel の補題を多少修正することによりこの問題を回避できる．また時間計算量削減のため Zassenhaus[55] による 2 乗収束するアルゴリズムを使う必要がある．これに対して $p = 2$ のときは (7.4) は常に成立せず，$E^{(i)\uparrow}[2]$ から $\mathrm{Ker}V_p^{(i)\uparrow}$ を抽出するにはいろいろと工夫が必要である．これらについては Fouquet, Gaudry, Harley[15,

§4.3] や Skjernaa[52, §4] を参照されたい．両者の方法の漸近的な計算量は同じであり，どちらが速いかは実装に依存する．

残るは $c_1^{(i)}$ が求まった後，その norm を計算することである．一般的に $c \in R^\times$ の norm 計算について考えよう．K 上の c 倍写像（明らかに $\mathbf{Q}_p$ 線形写像である）の $K/\mathbf{Q}_p$ の基底 $\{1, \theta, \ldots, \theta^{N-1}\}$ に関する表現行列を求めてその行列式を計算する方法は時間計算量・領域計算量ともに大きすぎて実用的ではない．

$c \equiv 1 \bmod p$ が成立している場合には

$$\log(c) := \sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n}(c-1)^n \tag{7.5}$$

は p 進付値に関して収束する．また $x \equiv 0 \bmod 4$ $(p=2)$, $x \equiv 0 \bmod p$ $(p>2)$ なら $\exp(x) := \sum_{n=0}^{\infty} \frac{1}{n!}x^n$ も収束する．すると

$$N_{K/\mathbf{Q}_p}(c) = \exp(\mathrm{Tr}_{K/\mathbf{Q}_p}(\log c))$$

である．(Norm 計算に現れるかけ算を対数を使って足し算に変換するところがポイントである．) $\log c \bmod p^M$ の値を求めるのに (7.5) 右辺を評価すると $O(M)$ 項が必要である．しかし，対数関数の性質を使って収束を加速し $O(\sqrt{M})$ 項で済ませることができる．(Satoh, Skjernaa, Taguchi[45, §3])

楕円曲線の位数計算に戻って $p=2$ なら $c_1^{(i)} \equiv 1 \bmod 4$ なので上のアルゴリズムがそのまま適用できる．$p>2$ のときは Teichmüller lift を使って $c \equiv 1 \bmod p$ の場合に帰着することができる．

以上を総合すると時間計算量 $O(N^{2\mu+1})$，領域計算量 $O(N^2)$ のアルゴリズムを得る．なお，N のみに依存する事前計算を認めると領域計算量を増やすことなしに時間計算量を $O(N^{2\mu+1/2})$ に減らすことができる (Satoh, Skjernaa, Taguchi[45])．また，$\mathbf{F}_q/\mathbf{F}_p$ に type の小さい Gaussian normal base が存在する場合は事前計算無しで $O(N^{2\mu+1/(\mu+1)})$ の時間計算量で位数を求めることができる (Kim et al.[26])．このような正規底があるならば Frobenius 置換の n 乗の評価を n に依存しない時間で行うことができる．Lercier, Lubciz[35] はこの条件下で $\sigma(x) = ax + b$ $(a, b \in R)$ の効率の良い解法を与え，任意の $\varepsilon > 0$ に対して時間計算量が $O(N^{2\mu+\varepsilon})$ となる位数計算アルゴリズム構成した．ごく最近 Harley[21] はこれらの方法を Newton 法と組み合わせることにより事前計算無しで全ての拡大次数に適用できる $O(N^{2\mu+\varepsilon})$ アルゴリズムをアナウンスした．

8 算術幾何平均法

数 a, b に対して

$$\mathcal{M}(a,b) := \left(\frac{a+b}{2}, \sqrt{ab}\right)$$

とおく．正の実数 a_0, b_0 が与えられたとき $(a_n, b_n) := \mathcal{M}(a_{n-1}, b_{n-1})$ により二つの数列 $\{a_n\}_{n=0}^{\infty}$, $\{b_n\}_{n=0}^{\infty}$ が定まる．このとき $\lim_{n\to\infty} a_n$, $\lim_{n\to\infty} b_n$ は存在して，その値は等しい．この共通の値を a_0, b_0 の算術幾何平均 (AGM) という．Henniart, Mestre[23] は完備離散的付値体 K の付値環 R の要素 a_0, b_0 （ただし $a_0 \equiv b_0 \bmod \mathcal{P}$）に対して $(a_n, b_n) := \mathcal{M}(a_{n-1}, b_{n-1})$ により定まる数列の性質を調べた．ここで K は実数体ではないから平方根の符号を合理的に定めねばならない．$\mathcal{P}$ を K の素元としたとき一般に $a, b \in R^\times$, $a \equiv b \bmod \mathcal{P}$ に対しては $\sqrt{ab} := a\sqrt{b/a}$ ここで $\sqrt{b/a} \equiv 1 \bmod \mathcal{P}$，と定義すると上記漸化式により $a_n \equiv b_n \bmod \mathcal{P}$ となる二つの数列 $\{a_n\}_{n=0}^{\infty}$, $\{b_n\}_{n=0}^{\infty}$ が定まる．彼らは $a_0 \equiv b_0 \bmod 4\mathcal{P}$ であればこの二つの数列は共通の極限値に収束することを示した．

さて，$p=2$ とし，K を $\mathbf{Q}_2$ 上の不分岐 N 次拡大，R をその付値環とする．$q:=2^N$ とおく，$a,b\in R^\times$ に対して $E_{a,b}$ を $Y^2=X(X-a^2)(X-b^2)$ による定まる楕円曲線とする．$\mathbf{F}_q$ 上の楕円曲線 $Y^2+XY=X^3+\alpha$ に対して $a_0,b_0\in R$ を E_{a_0,b_0} が E の持ち上げになっているようにとる．このとき $(a_n,b_n):=\mathcal{M}(a_{n-1},b_{n-1})$ により数列 $\{a_n\}_{n=0}^\infty$, $\{b_n\}_{n=0}^\infty$ を作ってもこの数列自体は収束しない．それにも関わらず Harley et al.[22] は $\{j(E_{a_n,b_n})-j(E^{(n)\uparrow})\}_{n=0}^\infty$ は 0 に収束することを証明した．ここでは E_{a_n,b_n} から $E_{a_{n+1},b_{n+1}}$ への写像 $(x,y)\to\left(\frac{y^2}{4x^2}+a_{n+1}^2,-\frac{y(b_{n+1}^4-x^2)}{8x^2}\right)$ が 2-isogeny であること，および $p=2$ であることが本質的に用いられる．このことを用いると次の驚くべきアルゴリズムを得る．

Input: $E:Y^2+XY=X^3+c,\ c\in\mathbf{F}_q^\times$
Output: E 上での $\mathrm{Tr}\,\mathrm{Fr}_q$
Procedure:
1: a_0, b_0 を求め，それらを a,b とする．
2: $M:=\lceil N/2\rceil+3$;
3: for $(i:=0\ ;\ i<M-2\ ;\ i:=i+1)$ {
4: $\quad(a,b):=\mathcal{M}(a,b)$;
5: }
6: $(c,d):=\mathcal{M}(a,b)$;
7: $|t|<2\sqrt{q}$ かつ $t\equiv N_{K/\mathbf{Q}_2}(a/c) \bmod 2^M$ となる t を返す．

この形でも十分速く $\mathrm{Tr}\,\mathrm{Fr}_q$ が求まるが，実装にあたっては種々の技巧を取り入れてさらに速くできる．詳細は Harley et al.[22] を参照されたい．なお，このアルゴリズムは ArgoTech 社の特許となっていることを付記しておく．また，Gaudry[18] は Satoh, Skjernaa, Taguchi[45] の方法を AGM 法と組み合わせ更に高速なアルゴリズムを得ている．

9 結びにかえて

本稿の目的の範囲を越えるが算術幾何平均法は標数 2 の有限体上定義された種数 2 の ordinary な超楕円曲線の位数計算にも適用できる (Harley et al.[22], Gaudry[17])．いまのところ cohomology に基づく方法が $O(N^3)$ の領域計算量を必要とするが算術幾何平均法の領域計算量は $O(N^2)$ ですむ．Harley らは実際に $N=4000$ に対してこのアルゴリズムを実行して見せた．要した時間は 144 時間である．それ以前の計算例（l 進的方法と BSGS の併用；Gaudry, Harley[19]）はせいぜい数十 bit の体上で数十日を要していた．標数が異るので単純は比較はできないものの，いかにこのアルゴリズムが速いかが分かる．ところで，種数 2 の算術平均法の正しさの証明では Richelet[42] が 1836 年（これは 1936 の誤植ではない）に発見した第一種超楕円積分の計算法の Bost, Mestre[4] による p 進版ともいうべき結果が本質的に重要である．このような経緯を見ると，やはり，数学の研究は 3 年とか 5 年とかの目先の成果を追い求めるのではなく，数学的対象が内在する固有の—時代と共にうつろうようなことのない—性質をじっくりと探求することが第一義的に肝要であり，ひいてはそれが有益な応用に結び付くと思うのであるがいかがであろうか．

参考文献

[1] Aho, A.V., Hopcroft, J.E., Ullman, J.D.: "The design and analysis of computer algorithms". Reading, Mass.: Addison-Wesley pub. 1974 (邦訳：アルゴリズムの設計と解析（野崎昭弘、野下浩平共訳）サイエンス社).

[2] Ankeny, N.C.: The least quadratic non residue. *Ann. of Math.* **55** (1952) 65-72.

[3] Blake, I.F., Seroussi, G., Smart, N.P.: "Elliptic curves in cryptography". London Math. Soc. Lecture Note Series, 265. Cambridge: Cambridge U.P. 1999 (邦訳：楕円曲線暗号（鈴木治郎訳）ピアソン・エデュケーション).

[4] Bost, J.-B., Mestre, J.-F.: Moyenne arithmético-géométrique et périodes des courbes de genre 1 et 2. *Gaz. Math.* **38** (1988) 36-64.

[5] Cantor, D. G., Kaltofen, E.: On fast multiplication of polynomials over arbitrary algebras. *Acta Inform.* **28** (1991) 693-701.

[6] Cassels, J. W. S.: A note on the division values of $\wp(u)$. *Proc. Cambridge Philos. Soc.* **45** (1949) 167-172.

[7] Chebyshev, P.L.: Mémoire sur les nombres premiers. *J. Math. Pures Appl.* **17** (1852) 366-390 (Œuvres, I-5).

[8] Cohen, P.: On the coefficients of the transformation polynomials for the elliptic modular function. *Math. Proc. Cambridge Philos. Soc.* **95** (1984) 389-402.

[9] Couveignes, J.-M.: "Quelques calculs en théorie des nombres". Université de Bordeaux I: Thèse 1994 (available at http://www.ufr-mi.u-bordeaux.fr/ couveign/Publi/Cou94-5.ps).

[10] Couveignes, J.-M.: Computing l-isogenies using the p-torsion, Algorithmic number theory (Telence, 1996), Lecture Notes in Comput. Sci., **1122**, Berlin: Springer, 1996.

[11] Couveignes, J.-M., Morain, F.: Schoof's algorithm and isogeny cycles, Algorithmic number theory (Ithaca, NY, 1994), Lect. Notes in Comput. Sci., **877**, 43-58, Berlin: Springer, 1994.

[12] Dewaghe, L.: Remarks on the Schoof-Elkies-Atkin algorithm. *Math. Comp.* **67** (1998) 1247-1252.

[13] Elkies, N.D.: Elliptic and modular curves over finite fields and related computational issues, Computational perspectives on number theory (Chicago, IL, 1995), AMS/IP Stud. Adv. Math., **7**, 21-76, Providence, RI: AMS, 1998.

[14] Enge, A.: "Elliptic curves and their applications to cryptography: An introduction". Boston, Dordrecht, London: Kluwer Acad. Pub. 1999.

[15] Fouquet, M., Gaudry, P., Harley, R.: An extension of Satoh's algorithm and its implementation. *J. Ramanujan Math. Soc.* **15** (2000) 281-318.

[16] Frey, G.: Applications of arithmetical geometry to cryptographic constructions, Finite fields and applications (Augsburg, 1999), 128-161, Berlin: Springer, 2001.

[17] Gaudry, P.: Algorithms for counting points on curves, (2001) Slides at ECC2001, Waterloo, Oct. 31, 2001, Available at http://www.cacr.math.uwaterloo.ca/conferences/2001/ecc/slides.html.

[18] Gaudry, P.: A comparison and a combination of SST and AGM algorithms for counting points of elliptic curves in characteristic 2, Advances in Cryptology - ASIACRYPT 2002, Lect. Notes in Comput. Sci., **2501**, 311-327, ed. Zheng, Y., Berin, Heidelberg: Springer Verlag, 2002.

[19] Gaudry, P., Harley, R.: Counting points on hyperelliptic curves over finite fields, ANTS-IV, Lect. Notes in Comput. Sci., **1838**, 313-332, Springer, 2000.

[20] Harley, R.: Counting points with the arithmetic-geometric mean (joint work with J.-F. Mestre and P. Gaudry), Eurocrypt 2001, Rump session, 2001.

[21] Harley, R.: Asymptotically optical p-adic point counting, (2002) Post to NMBRTHRY list.

[22] Harley, R., et al.: On the generation of secure elliptic curves using an arithmetic-geometric mean iteration, (in preparation).

[23] Henniart, G., Mestre, J.-F.: Moyenne arithmético-géométrique p-adique. *C.R. Acad. Sci. Paris Sér. I Math.* **308** (1989) 391-395.

[24] Karatsuba, A., Ofman, Y.: Multiplication of multidigit numbers on automata. *Soviet physics doklady* **7** (1963) 595-596.

[25] Kedlaya, K.: Counting points on hyperelliptic curves using Monsky-Washnitzer cohomology. *J. Ramanujan Math. Soc.* **16** (2001) 323-338.

[26] Kim, H., Park, J., Cheon, J., Park, J., Kim, J., Hahn, S.: Fast elliptic curve point counting using Gaussian normal basis, Algorithmic number theory (Sydney, Australia, July 2002), Lect. Notes in Comput. Sci., **2369**, 292-307, ed. Fieker, C., Kohel, D., Berlin: Springer, 2002.

[27] Koblitz, N.: Elliptic curve cryptosystems. *Math. Comp.* **48** (1987) 203-209.

[28] Koblitz, N.: Constructing elliptic cryptosystems in characteristic 2, Advances in cryptology, CRYPTO 90, Lect. Notes in Comput. Sci., **537**, 156-167, ed. Menezes, A.J., Vanstone, S.A., Berin: Springer Verlag, 1991.

[29] 黒川信重, 栗原将人, 斎藤毅: "数論 3". 岩波講座、現代数学の基礎, 11. 岩波書店 2001.

[30] Lang, S.: "Elliptic functions". GTM, 112. Berlin, Heidelberg: Springer 1987.

[31] Lauder, A., Wan, D.: Counting points on varieties over finite fields of small characteristic, (2001) preprint.

[32] Lauder, A., Wan, D.: Computing zeta functions of Artin-Schreier curves over finite fields. *LMS J. Comput. Math.* **5** (2002) 34-55.

[33] Lehmann, F., Maurer, M., Müller, V.: Counting the number of points on elliptic curve curves over finite fields of characteristic greater than three, Algorithmic number theory (Ithaca, NY, 1994), Lect. Notes in Comput. Sci., **877**, 60-70, Berlin: Springer, 1994.

[34] Lercier, R.: Computing isogenies in $\mathbf{F}_{2^n}$, Algorithmic number theory II(Talence, 1996), Lecture Notes in Comput. Sci., **1122**, 197-212, Berlin: Springer, 1996.

[35] Lercier, R., Lubciz, D.: Counting points on elliptic curves over finite fields in quadratic time, (2002) preprint.

[36] Lercier, R., Morain, F.: Computing isogenies between elliptic curves over $\mathbf{F}_{p^n}$ using Couveignes's algorithm. *Math. Comp.* **69** (2000) 351-370.

[37] Lubin, J., Serre, J.-P., Tate, J.: Elliptic curves and formal groups, (1964) Mimeographed notes, available at http://www.ma.utexas.edu/users/voloch/lst.html.

[38] Messing, W.: "The crystals associated to Barsotti-Tate groups: with applications to Abelian schemes". Lect. Notes in Math., 264. Berin-Heidelberg-New York: Springer 1972.

[39] Miller, V. S.: Use of elliptic curves in cryptography, Advances in cryptology-CRYPTO '85 (Santa Barbara, Calif., 1985), Lecture Notes in Comput. Sci., **218**, 417-426, Berlin-Heidelberg-New York: Springer, 1986.

[40] Montgomery, H.L.: "Topics in multiplicative number theory". Lect. Notes in Math., 227. Berlin, Heidelberg: Springer 1971.

[41] 森田康夫: "整数論". 基礎数学, 13. 東京大学出版会 1999.

[42] Richelot, F.: Essai sur une méthode générale pour déterminer la valuer des intégrales ultra-elliptiques, fondée sur des transformations remarquables des ce transcendantes. *C.R. Acad. Sc. Paris* **2** (1836) 622-627.

[43] 斉藤秀司: "整数論". 共立講座 21 世紀の数学, 20. 共立出版 1997.

[44] Satoh, T.: The canonical lift of an ordinary elliptic curve over a finite field and its point counting. *J. Ramanujan Math. Soc.* **15** (2000) 247-270.

[45] Satoh, T., Skjernaa, B., Taguchi, Y.: Fast computation of canonical lifts of elliptic curves and its application to point counting. *Finite fields and their appl.* **9** (2003) 89-101.

[46] Schönhage, A.: Asymptotically fast algorithms for the numerical multiplication and division of polynomials with complex coefficients, Computer algebra (Marseille, 1982), Lect. Notes in Comput. Sci., **144**, 3-15, Berlin-New York: Springer, 1982.

[47] Schönhage, A., Strassen, V.: Schnelle Multiplikation grosser Zahlen. *Computing* **7** (1971) 281-292.

[48] Schoof, R.: Elliptic curves over finite fields and the computation of square roots mod *p*. *Math. Comp.* **44** (1985) 483-494.

[49] Schoof, R.: Counting points on elliptic curves over finite fields. *J. Théor. Nombres Bordeaux* **7** (1995) 219-254.

[50] Silverman, J. H.: "The arithmetic of elliptic curves". GTM, 106. Berlin-Heidelberg-New York: Springer 1985.

[51] Silverman, J.H.: "Advanced topics in the arithmetic of Elliptic curves". GTM, 151. Berlin: Springer 1994.

[52] Skjernaa, B.: Satoh's algorithm in characteristic 2. *Math. Comp.* **72** (2003) 477-487.

[53] Vélu, J.: Isogénies entre courbes elliptiques. *C.R. Acad. Sc. Paris.* **273** (1971) 238-241.

[54] Vercauteren, F., Preneel, B., Vandewalle, J.: A memory efficient version of Satoh's algorithm, Advances in Cryptology - Eurocrypt 2001 (Innsbruck, Austria, May 2001), Lect. Notes in Comput. Sci., **2045**, 1-13, ed. Pfitzmann, B., Berlin, Heidelberg: Springer Verlag, 2001.

[55] Zassenhaus, H.: On Hensel Factorization, I. *J. Number Theory* **1** (1969) 291-311.

佐藤孝和 (非会員) 〒 338-8570 さいたま市桜区下大久保 255 (招待論文)

1989 年東京工業大学大学院理工学研究科博士課程修了. 理学博士. 同年, 埼玉大学理学部数学科助手. 現在, 同大学助教授. 保型形式・解析的数論の研究に従事. 情報理論とその応用学会, AMS, IACR 各会員.

(2002年11月 7 日受付)

(2003年 4 月 7 日最終稿受付)