有限体上の楕円曲線の位数計算について
–標数が小さい場合の漸近的高速算法–

埼玉大学理学部数学科
佐藤孝和

概要

本論文では素数 p が小さいときに $\mathbf{F}_{p^N}$ 上定義された楕円曲線 E の有理点の個数を求める漸近的高速アルゴリズムを考察する。簡単のため、ここでは $p \geq 5$ の場合を扱う。この場合、我々のアルゴリズムは deterministic なものとなる。($p=2$ の場合は注意 3.9 参照) n bit の object の乗算が $O(n^\mu)$ (bit operation, 以下同じ) で済むアルゴリズムを用いた場合、いわゆる Schoof-Elkies-Atkin アルゴリズムの計算量は $O((N\log p)^{2\mu+2})$ であるが、我々のアルゴリズムは $O(N^{2\mu+1})$ である。ただし O-constant は p に (残念ながら非常に悪く) 依存する。我々の方法は SEA とは全く異なる：E を canonical lift に持ち上げ、そこでの Verschiebung (Frobenius 準同型の双対 isogeny) の trace を標数 0 での情報から直接計算する。

1. はじめに

p を素数、$N \in \mathbf{N}$, $q := p^N$ とする。位数 q の有限体を $\mathbf{F}_q$ と書く。与えられた楕円曲線 $E/\mathbf{F}_q$ の $\mathbf{F}_q$ 有理点の数を速く求めることが我々の目的である。この方法として今日ではいわゆる Schoof-Elkies-Atkin algorithm が広く知られている。これに関しては Schoof[18] に要領の良い解説がある。また Elkies 自身による [7] も関連する多くの興味深い問題を交えながら SEA アルゴリズムを解説している。これらの方法に共通なアイデアはいろいろな素数 l に対して $\mathrm{Tr}\mathrm{Fr}_q \bmod l$ を求めるということである。ここで各 $n \geq 1$ に対して p^n 乗 Frobenius 写像を Fr_{p^n} と書く。Hasse の不等式から $|\mathrm{Tr}\mathrm{Fr}_q| \leq 2\sqrt{q}$ である。したがって Chinese Remainder Theorem (以下 CRT) を使って様々な l に対する $\mathrm{Tr}\mathrm{Fr}_q \bmod l$ の値から $\mathrm{Tr}\mathrm{Fr}_q$ を復元できる。ここで n-bit の object の乗算が $O(n^\mu)$ でできるとしよう。従って素朴な乗算アルゴリズムでは $\mu=2$, Karatsuba 法では $\mu=\log_2 3$, FFT を応用とした高速乗算では $\mu=1+\varepsilon$ である。このとき Schoof の algorithm の時間計算量は $O((\log q)^{3\mu+2})$, Elkies の algorithm では $O(\log q)$ 程度の素数の約半分が $\mathrm{End}(E)$ で分解するという (未だ証明されていないがもっともらしい) 仮定の基で $O((\log q)^{2\mu+2})$ である。isogeny を見つける Couveignes[4] の方法、Frobenius の固有値を見つける Dewaghe[6] の方法などが開発された結果、計算量の主要項 (の一つ) は $O(\log q)$ 個の素数 l に対して Frobenius の $E[l]$ (Elkies の方法では $E[l]$ の位数 l の部分群) 上の action を計算する部分となった。しかし、この部分はいかんともし難く、より速いアルゴリズムを構築するためにはいかにして Frobenius 写像そのものを避けて有理点の個数を求めるかということが

Mathematics Subject Classification (1991): 11G20, 11G07, 11T71
Keywords: elliptic curve, finite field, local field, canonical lift, order counting

真の問題であるように思える。

我々のアルゴリズムは SEA とは根本的に異なる。我々は $\mathrm{Tr}\mathrm{Fr}_q \bmod l$ を介するのではなく E の標数 0 への持ち上げから直接 $\mathrm{Tr}\mathrm{Fr}_q$ を計算する。このとき Frobenuius 写像ではなくその双対 Verschiebung を用いる。(Couveignes[4] も Verschiebung と p 分点の挙動に注目しているが彼の方法は結局のところ $\mathrm{Tr}\mathrm{Fr}_q \bmod l$ の計算を $O(\log q)$ 個の素数について計算する。) 我々の方法は $p \geq 5$ が十分小さく N が大きな時に有効でありその計算量は $O(N^{2\mu+1})$ である。ただしここの O-constant は p に依存する。残念ながら p に関する振舞いは極めて悪い。我々の方法では p-th modular polynomial を扱わなければならない。まず楕円曲線 $E/\mathbf{F}_q$ が $j(E) \in \mathbf{F}_{p^2}$ を満たす場合、この $\mathbf{F}_q$ 有理点の個数は簡単に求まることに注意する (命題 4.2)。よって以下 $j(E) \notin \mathbf{F}_{p^2}$ である楕円曲線のみを考える。特に E は ordinary である。ordinary な楕円曲線 $E/\mathbf{F}_q$ に対してその canonical lift を $E^{\uparrow}$ により表す。これは $\mathbf{Q}_p$ のある不分岐拡大体上定義された楕円曲線であり以下の 2 条件で特徴付けられる：(i) $E^{\uparrow}$ の $\bmod p$ reduction は E であり、(ii) かつ環として $\mathrm{End}(E) \cong \mathrm{End}(E^{\uparrow})$ である。そのような持ち上げは常に存在し、しかも同型を除けば一意的である。これは Deuring[5] による古典的な結果である。この考え方は Lubin, Serre, Tate[12] により現代的な代数幾何の文脈で再構成された。(Messing[13] も参照。) E と E' が ordinary な $\mathbf{F}_q$ 上の楕円曲線の時 $\mathrm{Hom}(E, E') \cong \mathrm{Hom}(E^{\uparrow}, E'^{\uparrow})$ である (Messing[13, Corollary V.3.4])。ここで $E^{(i)} := \mathrm{Fr}_p^i E$ とおこう。E は ordinary だから $i = 0, \ldots, N-1$ に対して $E^{(i)}$ も ordinary であり $V_p : E^{(i)} \to E^{(i-1)}$ は分離的である。これは V_p の核 (すなわち $E^{(i)}$ の p 分点の群 $E^{(i)}[p]$) さえ標数 0 に持ち上げることができれば V_p は $V_p^{\uparrow} : E^{(i)\uparrow} \to E^{(i-1)\uparrow}$ に明示的に持ち上げられることを意味する。$V_p^{\uparrow N} : E^{\uparrow} \to E^{\uparrow}$ の $E^{\uparrow}$ の形式群への作用を見て $V_p^{\uparrow N}$ の trace を得るがこの値は $\mathrm{Tr}\mathrm{Fr}_q$ に他ならない：

$$\begin{array}{ccccccccccc}
 & & E^{\uparrow} & \xrightarrow{V_p^{\uparrow}} & E^{(N-1)\uparrow} & \xrightarrow{V_p^{\uparrow}} & E^{(N-2)\uparrow} & \longrightarrow & \cdots & \xrightarrow{V_p^{\uparrow}} & E^{\uparrow} \\
 & & \uparrow & & \uparrow & & \uparrow & & & & \uparrow \\
E & = & E^{(N)} & \underset{\mathrm{Fr}_p}{\overset{V_p}{\rightleftarrows}} & E^{(N-1)} & \underset{\mathrm{Fr}_p}{\overset{V_p}{\rightleftarrows}} & E^{(N-2)} & \rightleftarrows & \cdots & \underset{\mathrm{Fr}_p}{\overset{V_p}{\rightleftarrows}} & E
\end{array}$$

上で説明した方法は以下のような考察に基づく。

- $E[p]$ は Fr_q stable な位数 p の群であるという意味において素数 p は a priori に Elkies 素数である。($j(E) \notin \mathbf{F}_{p^2}$ であるから E は ordinary であることに注意する。)
- Verschiebung の代数化は Frobenius のそれと比べて易しいと思われる。やるべきことは点集合としての $E[p]$ を持ち上げだけである。
- $f \in \mathrm{End}(E^{\uparrow})$ が "explicit" に与えられ、その reduction mod p が分離的であるとする。このとき f の特性多項式は (標数 0 の object である) $E^{\uparrow}$ の形式群への作用を見ることにより容易に分かる。(命題 4.1 参照)

本稿の内容であるが、§2 は準備であり、ある種の非分離多項式の因子をどのようにしてとり出すか述べる。§3 において $j(E) \notin \mathbf{F}_{p^2}$ を満たす与えられた楕円曲線 $E/\mathbf{F}_q$ の canonical lift の Weierstrass model を構成する。§4 では canonical lift がどのように位数計算に用いられるかを解説する。

有限体上定義された楕円曲線の有理点の数を求める問題は Miller[14] と Koblitz[9] により独立に提案された楕円曲線暗号と深い関連がある。応用上は $p=2$ の場合が極めて重要である。しかしながら技術的な問題からここでは $p\geq 5$ である場合のみ考える。これに関しては注意 3.9 も合わせて参照されたい。

記号

特に断りのない限り $p\geq 5$ は素数、$N\in\mathbf{N}$, $q:=p^N$ とする。K を $\mathbf{Q}_p$ 上 N 次不分岐拡大体とする。K の付値環を R と書く。p は K においても素元であるから R の剰余体は $\mathbf{F}_q$ である。K の最大不分岐拡大とその付値環をそれぞれ K^{ur}, R^{ur} と表すことにする。一般に $\mathcal{O}$ により楕円曲線の無限遠点を、π により reduction modulo p 写像を表す。楕円曲線 E_1 と E_2 に対し E_1 から E_2 への isogeny 全体のなす集合を $\mathrm{Isog}(E_1,E_2)$ と書く。p 番めの modular 多項式は Φ_p と書かれる。X および Y 座標を与える座標関数をそれぞれ ξ, η と書く。モデルに依存する若干の記号が定理 3.1 の前で導入される。

2. ある種の非分離的多項式の因数分解

本節ではある種の非分離的多項式の $\bmod p$ での因子を持ち上げる方法について考える。具体的には $U\in R[X]$ とし、$\pi(U)$ の因子 $f\in\mathbf{F}_q[X]$ が与えられたとする。この f を、$\pi(U)$ が既約多項式の冪乗になるような場合も含めて、U の因子 g に持ち上げたい。これは Hensel の補題 [8] の拡張である。しかしながら、我々は同時にその計算量も考慮しなければならない。ここで考える方法は Zassenhaus[22, Lemma 2] による 2 次持ち上げ (quadratic lift) の拡張である。なお、Cohen[3, Sect. 3.5.3] も合わせて参照されたい。それを用いて ordinary な楕円曲線の canonical lift の構成法について考える。Voloch and Walker[21] は canonical lift $\bmod p^2$ を考察している。以下の方法は $\bmod p^2$ lift だけを構成するのであれば彼らの方法よりは遅いが、canonical lift を任意の精度で近似できるという利点がある。これらの結果を用いて $E[p]$ を E の canonical lift の R^{ur} 有理点に持ち上げる。

f, $g\in R[X]$ を $\gcd(\pi(f),\pi(g))=1$ を満たす多項式とする。このとき任意の $u\in\mathbf{N}$ に対して $A_uf+B_ug\equiv 1 \bmod p^u$ となる A_u, $B_u\in R[X]$ が存在する。しかも、f が monic ならばそのような B_u で $\deg B_u<\deg f$ を満たすものを R/p^uR の算術演算高々 $O((\deg f+\deg g)^2)$ 回で構成することができる。$u=1$ ならばこれは Euclid の互除法を使えば良い。$u\geq 2$ のときは、まず再帰的に $A_{[(u+1)/2]}$ と $B_{[(u+1)/2]}$ を求めそれらを A_u と B_u に持ち上げれば良い。ここで $R/p^{[(u+1)/2]}R$ の算術演算は R/p^uR の算術演算よりも速く行なえることに注意する。また $u\geq 2$ のとき、Euclid の互除法を直接適用するのは疑除算が必要となり得策ではない。

補題 2.1. p を奇素数、$U\in R[X]$ とする。$t:=\mathrm{ord}_p\partial U$ (ここで $\partial=\frac{d}{dX}$) とおく。$f\in R[X]$ は以下の条件を満たすものとする：

(i)　f は monic

(ii)　$\pi(f)$ は square free

(iii)　$\pi(f)$ は $\pi(p^{-t}\partial U)$ と互いに素

(iv)　$Q_0 \in R[X]$ と $u \in \mathbf{N}$ で $\mathrm{ord}_p(U - fQ_0) \geq u+t$ となるものが存在する。

簡単のため $v := 2u + \min(t, u)$ とおく。このとき、以下が成立する。

(v)　$g,\ Q_1 \in R[X]$ が $g \equiv f \bmod p$ かつ $\mathrm{ord}_p(U - gQ_1) \geq v$ を満たしているとする。このとき $h \equiv g \bmod p^{2u}$ となる任意の $h \in R[X]$ に対して（h に依存する）$Q_2 \in R[X]$ で $\mathrm{ord}_p(U - hQ_2) \geq v$ を満たすものが存在する。

(vi)　$Q_3 \in R[X]$ と monic な $g \in R[X]$ で

$$\mathrm{ord}_p(U - gQ_3) \ \geq \ v \tag{2.1}$$

かつ $g \equiv f \bmod p^u$ となるものが存在する。（このとき、必然的に $\pi(g) = \pi(f)$ かつ $\deg g = \deg f$ となる。）このような g を $R/p^{2u}R$ の算術演算 $O((\deg f + \deg U)^2)$ 回で構成することができる。

証明．　(v): $\delta := p^{-2u}(h-g) \in R[X]$ とおく。$g \equiv f \bmod p$ だから $\pi(g)$ もまた square free である。前述したことから多項式 $A,\ B \in R[X]$ で

$$A\partial g + Bg \ \equiv \ \delta \mod p^{v-2u}.$$

となるものがある。他方、$U \equiv gQ_1 \bmod p^v$ だから

$$U(X + p^{2u}A(X)) \ \equiv \ g(X + p^{2u}A(X))Q_4(X) \mod p^v, \tag{2.2}$$

ここで $Q_4(X) := Q_1(X + p^{2u}A(X))$, となる。左辺を展開して

$$U(X) + p^{2u}A(X)\partial U(X) \ \equiv \ U(X) \mod p^v$$

を得る。$Q_5(X) := (1 - p^{2u}B(X))Q_4(X)$ とおく。$(1+p^{2u}B)(1-p^{2u}B) \equiv 1 \bmod p^v$ ゆえ (2.2) の右辺は

$$\begin{aligned} & (g(X) + p^{2u}A(X)\partial g(X))(1 + p^{2u}B(X))Q_5(X) \\ \equiv \ & (g(X) + p^{2u}(A(X)\partial g(X) + g(X)B(X)))Q_5(X) \mod p^v \\ \equiv \ & h(X)Q_5(X) \mod p^v. \end{aligned}$$

ゆえに Q_2 としてこの Q_5 がとれる。

(vi): Y を不定元とする。$r_0 := p^{-u-t}(U - fQ_0),\ \ r_1 := p^{-t}\partial U$ とおく。必要ならば Q_0 を置き換えて $\deg_X r_0(X) < \deg_X f(X)$ であるとしても一般性を失わない。つまり、$r_0 = p^{-u-t}(U \bmod f)$ としてよい。すると

$$U(X + p^u Y) \ = \ U(X) + p^u Y\partial U(X) + \frac{p^{2u}}{2}Y^2\partial^2 U(X) + \sum_{i=3}^{\infty}\frac{p^{iu}}{i!}Y^i\partial^i U(X)$$

となる。ここで $p \neq 2$ だから $\mathrm{ord}_p\left(\dfrac{p^{2u}}{2}\partial^2 U(X)\right) \geq 2u+t$ である。最後の項に関しては $\dfrac{\partial^i U(X)}{i!} \in R[X]$ だから $\mathrm{ord}_p\left(\dfrac{p^{iu}}{i!}Y^i\partial^i U(X)\right) \geq 3u$ である。ゆえに

$$U(X + p^u Y) \ \equiv \ f(X)Q_0(X) + p^{u+t}(r_0(X) + Yr_1(X)) \mod p^v.$$

(iii) により $A(X),\ B(X) \in R[X]$ で

$$A(X)f(X)+r_1(X)B(X) \equiv r_0(X) \mod p^u \quad \text{かつ} \quad \deg_X B(X) < \deg_X f(X)$$

を満たすものがある。従って

$$U(X+p^uY) \equiv f(X)Q_0(X)+p^{u+t}(A(X)f(X)+r_1(X)(Y+B(X))) \mod p^v. \tag{2.3}$$

(2.3) において X に $X+p^uB(X)$ を、Y に $-B(X)$ を代入すると

$$U(X) \equiv f(X+p^uB(X))Q_6(X) \mod p^v,$$

ただし $Q_6(X):=Q_0(X+p^uB(X))+p^{u+t}A(X+p^uB(X))\in R[X]$, となる。他方、

$$f(X+p^uB(X)) \equiv f(X)+p^uB(X)\partial f(X)+\frac{p^{2u}}{2}B(X)^2\partial^2 f(X) \mod p^{3u}.$$

である。(v) により $Q_7\in R[X]$ で

$$U(X) \equiv (f(X)+p^uB(X)\partial f(X))Q_7(X) \mod p^v$$

を満たすものがある。$Q_8,\ r_2\in K[X]$ を $B\partial f=Q_8f+r_2$ かつ $\deg r_2<\deg f$ により定める。すると (i) により Q_8 と r_2 は $R[X]$ に属する。

$$(1-p^uQ_8+p^{2u}Q_8^2)(1+p^uQ_8) \equiv 1 \mod p^{3u},$$

であるから $Q_9:=Q_8^2f-Q_8B\partial f\ \ (=-Q_8r_2),\ \ Q_{10}:=(1+p^uQ_8)Q_7$ とおけば

$$U \equiv (f+p^ur_2+p^{2u}Q_9)Q_{10} \mod p^v$$

を得る。$g:=f+p^ur_2$ とおく。すると g は monic かつ $g\equiv f \bmod p^{2u}$ である。この g に対する Q_3 の存在は (v) から従う。計算量に関する主張は明らかである。■

補題 2.2. p を素数、$U\in R[X],\ \{a_n\in\mathbf{N}\}_{n=1}^{\infty}$ を狭義単調増加数列とする。$\{h_n\in R[X]\}_{n=1}^{\infty}$ を以下の条件を満たす monic な多項式列とする：

(i) $h_{n+1}\equiv h_n \bmod p^{a_n}$.

(ii) 各 n に対して $\mathrm{ord}_p(U-h_nS_n)\geq a_n$ となる $S_n\in R[X]$ が存在する。

(iii) $\pi(h_0)$ は square free.

このとき $h:=\lim_{n\to\infty}h_n\in R[X]$ が存在し $\deg h=\deg h_n$ が (任意の n に対して) 成立する。h の全ての零点は R^{ur} に属し、それらは U の零点である。特に h は U を割り切る。

証明． $R[[X]]$ は p 進付値に関して完備だから (i) により $R[[X]]$ において $\lim_{n\to\infty}h_n$ が存在する。(i) と h_n が monic であることを用いて全ての $n\geq 1$ に対して $\deg h_n=\deg h_1$ となる。ゆえに実は h は $R[X]$ に属し任意の $n\geq 1$ に対して $\deg h=\deg h_n$ が成立する。θ を $h(X)=0$ の根とする。$\pi(h)=\pi(h_0)$ は square free だから $\theta\in R^{\mathrm{ur}}$ である。後は $U(\theta)=0$ を示せば良い。$n\geq 1$ に対して

$$U = (U-h_nS_n)+(h_n-h)S_n+hS_n$$

だから $\mathrm{ord}_pU(\theta)\geq a_n$ であることが分かる。これが任意の n に対して成立しているのだから $U(\theta)=0$ でねばならない。■

3. Canonical Lift の構成

$E/\mathbf{F}_q$ を $j(E)\notin\mathbf{F}_{p^2}$ となる楕円曲線とする。本節では E の canonical lift に p adic に十分近い楕円曲線を素早く求める algorithm を構成する。Voloch and Walker[21] は canonical lift $\bmod p^2$ を考察している。以下の方法は $\bmod p^2$ lift だけを構成するのであれば彼らの方法よりは遅いが、canonical lift を任意の精度で近似できるという利点がある。これらの結果を用いて $E[p]$ を E の canonical lift の R^{ur} 有理点に持ち上げる。

k を体、S を k の代数閉包の部分環とする。k 上定義された楕円曲線 $E\colon Y^2=X^3+AX+B$ に対して

$$E(S) := \{\,(x,y)\in S^2 : y^2 = x^3+Ax+B\,\}\cup\{\,\mathcal{O}\,\}.$$

とおく。ここで S が体でない場合には $E(S)$ は一般的には群にならないことに注意する。我々は $\tau(X,Y):=-X/Y$ を $\mathcal{O}$ における local parameter とする。E の n-torsion point の群は $E[n]$ と書く。$\mathscr{P}\subset E$ に対して k に $\mathscr{P}-\{\mathcal{O}\}$ に属する全ての点の座標値を添加した体を $k(\mathscr{P})$ と書く。

不定元 α, β に対して $\Psi_p(X,\alpha,\beta)\in\mathbf{Z}[X,\alpha,\beta]$ を p-th division polynomial とする。従って $P:=(x,y)\in E-\{\mathcal{O}\}$ は $\Psi_p(x,A,B)=0$ となるときかつそのときに限り $E[p]$ に属する。さらに $P\notin E[p]$ に対して

$$pP = \left(\frac{\varphi_p(x,A,B)}{\Psi_p(x,A,B)^2},\ y\frac{\Omega_p(x,A,B)}{\Psi_p(x,A,B)^3}\right)$$

となる φ_p, $\Omega_p\in\mathbf{Z}[X,\alpha,\beta]$ がある。$\Psi_p(X,A,B)$ は $k[X]$ において $\varphi_p(X,A,B)$ と互いに素である。division polynomial の基本的な事柄については Silverman[19, Exercise 3.7] 参照のこと。(p が奇数という条件の基でここの Ψ_p と Ω_p は Silverman の記号でそれぞれ ψ_p と $y^{-1}\omega_p$ である。)

ここで $E\colon Y^2=X^3+AX+B$ を ordinary かつ $AB\neq0$ であるような $\mathbf{F}_q$ 上の楕円曲線、$\widetilde{E}\colon Y^2=X^3+\widetilde{A}X+\widetilde{B}$ をその K への持ち上げとする。

定理 3.1. E と $\widetilde{E}$ を上の通りとする。以下の条件 (i)-(iv) は同値である。

(i) $\widetilde{E}[p]\cap\widetilde{E}(R^{\mathrm{ur}})\neq\{\mathcal{O}\}$

(ii) $\tau(pP)\in p^2R^{\mathrm{ur}}$ となるような $P\in\widetilde{E}(R^{\mathrm{ur}})-\{\mathcal{O}\}$ が存在する。

(iii) $\Psi_p(x,\widetilde{A},\widetilde{B})\equiv0\bmod p^2$ となるような $P:=(x,y)\in\widetilde{E}(R^{\mathrm{ur}})-\{\mathcal{O}\}$ が存在する。

(iv) $j(\widetilde{E})\equiv j(E^{\uparrow})\bmod p^2$.

証明． 証明は [16, Cor. 3.4] や [17, Th. 3.7] とほぼ同様である。しかしながらこの定理は我々のアルゴリズムにとって非常に重要であるので証明をきちんと記述する。

(i)→(ii),(iii): 明らか。(ii)→(i): 仮定から $\tau(Q)=\frac{1}{p}\tau(pP)\in pR^{\mathrm{ur}}$ を満たす $Q\in\widetilde{E}(K^{\mathrm{ur}})\cap\mathrm{Ker}\,\pi$ が存在する。$\tau\colon\mathrm{Ker}\,\pi\cap\widetilde{E}(K^{\mathrm{ur}})\to pR^{\mathrm{ur}}$ は同型であるから (Silverman[19, Th. IV.6.3]), $P-Q\in\widetilde{E}[p]\cap\widetilde{E}(R^{\mathrm{ur}})$ を得る。(iii)→(ii): $pP=\mathcal{O}$ であれば証明すべきことは何もない。そうでないときには $(x',y'):=pP$ とおく。仮定 (iii) から $\varphi_p(x,\widetilde{A},\widetilde{B})\not\equiv0\bmod p$ (もしそうでなければ $\varphi_p(X,A,B)$ は $\mathbf{F}_q[X]$ で $\Psi_p(X,A,B)$

と互いに素でなくなり矛盾である。) ゆえに

$$\begin{aligned}\mathrm{ord}_p x' &= \mathrm{ord}_p \varphi_p(x, \widetilde{A}, \widetilde{B}) - 2\mathrm{ord}_p \Psi_p(x, \widetilde{A}, \widetilde{B}) \\ &\leq -4\end{aligned}$$

および $\mathrm{ord}_p y' = \frac{3}{2}\mathrm{ord}_p x'$ が成立する。したがって $\tau(pP) = -x'/y' \equiv 0 \bmod p^2$ である。

(i)→(iv): $H := \widetilde{E}[p] \cap \widetilde{E}(R^{\mathrm{ur}})$ とおく。p は素数であるから H は位数 p の巡回群である。$G := \widetilde{E}[p] \cap \mathrm{Ker}\,\pi$ とおく。$\pi : \widetilde{E}[p] \to E[p]$ は単射ではあり得ないから G は自明ではない。ゆえに G もまた位数 p の巡回群である。したがって群として $\widetilde{E}[p] = H \oplus G$ である。Q が $G - \{\mathcal{O}\}$ のどの点であっても $K(G) = K(\xi(Q), \eta(Q))$ である。G も H も K 上定義されていることに注意する。特に $\xi(Q)$ の共役の数は $G - \{\mathcal{O}\}$ の点の X-座標の数を越えない。すなわち

$$[K(G) : K] \;=\; [K(\xi(Q), \eta(Q)) : K(\xi(Q))][K(\xi(Q)) : K] \;\leq\; 2 \cdot \frac{p-1}{2}.$$

よって $[K(G) : K]$ の分岐指数は p 未満である。他方、$K(H)/K$ は不分岐である。よって $K(\widetilde{E}[p])$ は K 上 tamely ramified である。(iv) は Nakamura[15, Theorem] から従う。

(iv)→(iii): 最初に $E^{\uparrow}[p] \cap E^{\uparrow}(R^{\mathrm{ur}}) \neq \{\mathcal{O}\}$ を示す。V_p を E の Verschiebung とし $V_p^{\uparrow} \in \mathrm{End}(E^{\uparrow})$ をその $\mathrm{End}(E^{\uparrow})$ への持ち上げとする。V_p は分離的だから $\pi(\mathrm{Ker}\, V_p^{\uparrow}) = \mathrm{Ker}\, V_p = E[p]$ である。これは $\prod_{P \in (\mathrm{Ker}\, V_p^{\uparrow} - \{\mathcal{O}\})/\pm 1} (X - \xi(P)) \in R[X]$ を $\bmod p$ した多項式が square free であることを意味する。したがって Lang[11, Prop. II.4.7] により $P \in \mathrm{Ker}\, V_p^{\uparrow} - \{\mathcal{O}\}$ に対しては $\xi(P) \in R^{\mathrm{ur}}$ となる。p は奇数だから $\mathrm{ord}_p \eta(P) = 0$ である。これと $\eta(P)^2 \in R^{\mathrm{ur}}$ から $\eta(P) \in R^{\mathrm{ur}}$ を得る。ゆえに $\widetilde{E} = E^{\uparrow}$ であれば (i) が成立し、従って (iii) も成立する。次に $Y^2 = X^3 + A^{\uparrow}X + B^{\uparrow}$ を $E^{\uparrow}$ の Weierstrass model とする。$u := \dfrac{\widetilde{A}B^{\uparrow}}{A^{\uparrow}\widetilde{B}} \in R^{\times}$ とおくと $j(\widetilde{E}) \equiv j(E^{\uparrow}) \bmod p^2$ は $\widetilde{A} \equiv u^2 A^{\uparrow} \bmod p^2$ と $\widetilde{B} \equiv u^3 B^{\uparrow} \bmod p^2$ を意味する。(iii) の成否は $\widetilde{A} \bmod p^2$ と $\widetilde{B} \bmod p^2$ のみに依存するから $\widetilde{E}$ に対しても (iii) が成立する。■

注意 **3.2.** Nakamura[15] によればこの論文中の定理は Serre の未刊行の結果であり、その証明には local Serre-Tate parameter が使われている。しかしながら Nakamura[15] の証明法は初等的である (そして出版されている)。

さて、p-th modular polynomial を Φ_p と書くことにする。今までは $j(E) \notin \mathbf{F}_{p^2}$ という仮定を使ってこなかった。この仮定を使う次の命題は $0, 1728$ 以外の non-supersingular j に対して成立するであろうと予想されるがその証明は著者には分からない。小池 [10, Prop. 1] に $\Phi_p \bmod p^2$ の性質がいくつか述べられている。我々の方法の idea は基本的に Lubin-Serre-Tate[12, Sect. 8] のものであるが、計算量を極力減らすように工夫しなければならない。特に、R 上の Frobenius 置換は R 上全微分不可能なのでこれを陽に使うと Newton 法が使えなくなってしまう。

命題 **3.3.** $m \in \mathbf{N}$ とする。$z_0, \ldots, z_{N-1} \in R$ は全ての $0 \leq i < N$ に対して以下を満たすものとする：

(i) $z_i \equiv z_{i+1}^p \bmod p$,

(ii) $\pi(z_i) \notin \mathbf{F}_{p^2}$

(iii) $\Phi_p(z_i, z_{i+1}) \equiv 0 \bmod p^m$

ここで $z_N = z_0$ と解する。このとき全ての $0 \le i < N$ に対して

(iv) $\zeta_i \equiv z_i \bmod p^m$,

(v) $\Phi_p(\zeta_i, \zeta_{i+1}) \equiv 0 \bmod p^{2m}$

を満たす $\zeta_0, \ \dots, \ \zeta_{N-1} \in R$ が $\bmod p^{2m}$ を除いて一意的に存在する。(ここでも $\zeta_N = \zeta_0$と解する。) さらに (二変数多項式 $\Phi_p \bmod p^{2m}$ が計算されていれば) 全ての $\zeta_i \bmod p^{2m}$ $(0 \le i < N)$ を $R \bmod p^{2m}$ 上の算術演算 $O(N)$ 回で求めることができる。

証明 . まず Kronecker の合同式

$$\Phi_p(U, V) \ \equiv \ (U^p - V)(U - V^p) \ \bmod \ p.$$

に注意する。よって (i) により

$$\frac{\partial \Phi_p}{\partial U}(z_i, z_{i+1}) \ \equiv \ z_{i+1}^{p^2} - z_{i+1} \ \bmod \ p, \tag{3.1}$$

$$\frac{\partial \Phi_p}{\partial V}(z_i, z_{i+1}) \ \equiv \ 0 \ \bmod \ p \tag{3.2}$$

となる。$\mathscr{F} \in \mathrm{Map}(R^N, R^N)$ を

$$\mathscr{F}({}^t(x_0 \ \dots \ x_{N-1})) \ := \ {}^t(\Phi_p(x_0, x_1) \quad \Phi_p(x_1, x_2) \ \dots \ \Phi_p(x_{N-1}, x_0)).$$

に定める。$z := {}^t(z_0 \ \dots \ z_{N-1})$ とする。ここで

$$(D\mathscr{F})(z) \ := \begin{pmatrix} \frac{\partial \Phi_p}{\partial U}(z_0, z_1) & \frac{\partial \Phi_p}{\partial V}(z_0, z_1) & 0 & \dots & 0 \\ 0 & \frac{\partial \Phi_p}{\partial U}(z_1, z_2) & \frac{\partial \Phi_p}{\partial V}(z_1, z_2) & & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \dots & \frac{\partial \Phi_p}{\partial V}(z_{N-2}, z_{N-1}) \\ \frac{\partial \Phi_p}{\partial V}(z_{N-1}, z_0) & 0 & 0 & \dots & \frac{\partial \Phi_p}{\partial U}(z_{N-1}, z_0) \end{pmatrix}$$

とおくと $\delta \in R^N$ に対して

$$\mathscr{F}(z + p^m\delta) \ \equiv \ \mathscr{F}(z) + (D\mathscr{F})(z)p^m\delta \ \bmod \ p^{2m} \tag{3.3}$$

である。(3.1) と (3.2) により $(D\mathscr{F})(z) \bmod p$ は対角行列でありその (ii) より対角成分は 0 ではない。よって $\det(D\mathscr{F})(z) \in R^\times$ であり $\delta := -p^{-m}(D\mathscr{F})(z)^{-1}\mathscr{F}(z)$ ととると (iii) を用いて $\delta \in R^N$ であることが分かる。このとき ${}^t(\zeta_0 \ \dots \ \zeta_{N-1}) := z + p^m\delta$ が求めるものである。実際、(iv) は $\delta \in R^N$ から、(v) は (3.3) と ζ_i, δ の定義から従う。一意性は $(D\mathscr{F})(z)$ が正則だから明らかである。

計算量に関してであるが、$R \bmod p^{2m}$ 上の算術演算 $O(p^2N)$ 回で $\mathscr{F}(z)$ と $(D\mathscr{F})(z)$ の 0 でない成分が計算できる。さらに $2N$ 回の行基本変形 (すなわち算術演算 $O(N)$ 回) で $(D\mathscr{F})(z)^{-1}\mathscr{F}(z)$ が出る。$(R \bmod p^{2m})^N$ の引き算が後一回必要であるがこれは明らかに $R \bmod p^{2m}$ の引き算 N 回でできる。■

系 3.4. E を $j(E)\notin\mathbf{F}_{p^2}$ であるような楕円曲線とする。$\mathrm{Fr}_p^i E$ を $E^{(i)}$ と書きその canonical lift を $E^{(i)\uparrow}$ により表す。$\{a_n\in\mathbf{N}\}_{n=0}^{\infty}$ を $a_0=1$ である狭義単調増加数列とする。$0\le i<N$ と $n>0$ に対して $z_{i,n}\in R$ が以下の条件を満たすとする。

(i) $\pi(z_{i,0})=\mathrm{Fr}_p^i j(E)$.

(ii) $z_{i,n+1}\equiv z_{i,n}\bmod p^{a_n}$.

(iii) $\Phi_p(z_{i,n},z_{i+1,n})\equiv 0\bmod p^{a_n}$.

このとき各 $0\le i<N$ に対して極限 $z_i:=\lim_{n\to\infty} z_{i,n}$ が存在し $z_i=j(E^{(i)\uparrow})$ となる。さらに $z_{i,n}\equiv j(E^{(i)\uparrow})\bmod p^{a_n}$ が成立する。

証明 . 前命題と同様な議論で $(Z_0,\ldots,Z_{N-1})$ に関する連立方程式

$$\begin{aligned}&\Phi_p(Z_0,Z_1)\;=\;0,\;\ldots,\;\Phi_p(Z_{N-2},Z_{N-1})\;=\;0,\;\Phi_p(Z_{N-1},Z_0)\;=\;0,\\&\pi(Z_0)\;=\;j(E),\;\ldots,\;\pi(Z_{N-1})\;=\;j(E^{(N-1)})\end{aligned}\tag{3.4}$$

の解は $j(E)\notin\mathbf{F}_{p^2}$ という条件の基で高々一組である。$E^{(i)\uparrow}$ と $E^{(i+1)\uparrow}$ は p-isogenous だから $(j(E^{(0)\uparrow}),\ldots,j(E^{(N-1)\uparrow}))$ は (3.4) の解である。他方、(ii) から $\{z_{n,i}\}_{n=1}^{\infty}$ は Cauchy 列であり (iii) から $(z_1,\ldots,z_{N-1})$ は (3.4) の解である。よって解の一意性から $z_i=j(E^{(i)\uparrow})$ である。最後の主張は非アルキメデス的付値の性質から容易に従う。■

注意 3.5. 実際の計算に於いては $(D\mathscr{F})(z)$ を表すのに疎行列表現 (あるいは単にサイズ N の一次元配列を二つ) 用いる。この技法を用いたとしても領域計算量は $O(N^3)$ であり、これは残念ながら (漸近的には) 非常に大きい。Galois 群の性質を利用して領域計算量が、例えばこの $1/N$ 程度ですむようなアルゴリズムが望まれる。すぐ思いつく方法として $K=\mathbf{Q}_p(\omega)$ であるようにとり $\sigma\in\mathrm{Gal}(K/\mathbf{Q}_p)$ を Frobenius 置換とする。$x\in R$ は $x=\sum_{i=0}^{N-1} x_i\omega^i$ $(x_0,\ \ldots,\ x_{N-1}\in\mathbf{Q}_p)$ と表される。そこで $\Phi_p(x,\sigma x)=0$ を $x_0,\ \ldots,\ x_{N-1}$ に関して解くことが考えられる。しかしこの場合 $(D\mathscr{F})(z)$ の替わりに $\mathrm{Mat}(N,\mathbf{Z}/p^m\mathbf{Z})$ に属する密行列の逆行列を計算せねばならず、かえって遅くなってしまう。

注意 3.6. $M\in\mathbf{N}$ に対して $j(E^{\uparrow})\bmod p^M$ の値を求めようとする場合、以下の手順による：

- $\nu:=[\log_2(M-1)]+1,\ 0\le n\le\nu$ に対して $a_n:=[2^{-(\nu-n)}M]$ とおく。
- $0\le i\le N-1$ に対して $z_{i,0}:=j(E^{(i)})\in\mathbf{F}_q=R/pR$ とおく。
- $n=1\sim\nu$ に対して命題 3.3 の手順により $z_{i,n}\equiv z_{i,n-1}\bmod p^{a_{n-1}}$ かつ $\Phi_p(z_{i,n},z_{i+1,n})\equiv 0\bmod p^{a_n}$ となる $z_{i,n}\in R/p^{a_n}R$ を $z_{i,n-1}$ より計算する。

このとき $z_{0,\nu}$ が求める値となる。これは単純に R/p^MR 上で Newton 法を実行するより速い。なぜなら m が小さくなるにつれ R/p^mR での計算が速くなるからである。

補題 3.7. $\widetilde{E}:Y^2=X^3+\widetilde{A}X+\widetilde{B}$ が定理 3.1 の (i)-(iv) のいずれかの条件を満たすとする。このとき任意の $P\in\widetilde{E}[p]\cap\widetilde{E}(R^{\mathrm{ur}})-\{\mathcal{O}\}$ に対して

$$\mathrm{ord}_p(\partial\Psi_p)(\xi(P),\widetilde{A},\widetilde{B})\;=\;1$$

が成立する。ここで $\partial=d/dX$.

証明． $Q\in\widetilde{E}[p]\cap\mathrm{Ker}\pi-\{\mathcal{O}\}$ とする。すると P と Q はそれぞれ $\widetilde{E}[p]\cap\widetilde{E}(R^{\mathrm{ur}})$ と $\widetilde{E}[p]\cap\mathrm{Ker}\pi$ を生成する。よって p-th division polynomial は K の代数閉包において

$$\Psi_p(X,\widetilde{A},\widetilde{B}) = p\prod_{j=1}^{(p-1)/2}(X-\xi(jQ))\prod_{i=1}^{(p-1)/2}(X-\xi(iP))\prod_{i=1}^{(p-1)/2}\prod_{j=1}^{p-1}(X-\xi(iP+jQ))$$

と因数分解する。(例えば Cassels[2, Formulary, (I)] あるいは Silverman[19, Exer. 3.7(b)] 参照。) ゆえに

$$\partial\Psi_p(\xi(P),\widetilde{A},\widetilde{B}) = p\prod_{j=1}^{(p-1)/2}(\xi(P)-\xi(jQ))\prod_{i=2}^{(p-1)/2}(\xi(P)-\xi(iP))\prod_{i=1}^{(p-1)/2}\prod_{j=1}^{p-1}(\xi(P)-\xi(iP+jQ))$$

である。$t_j:=-\xi(jQ)/\eta(jQ)$ を $\mathcal{O}$ における local parapeter の jQ での値とする。ここで

$$\xi(jQ) = t_j^{-2}-\widetilde{A}t_j^2+O(t_j^3) \quad \text{および} \quad \eta(jQ) = -t_j^{-3}+\widetilde{A}t_j+O(t_j^2)$$

であることを使うと

$$\begin{aligned}\xi(iP+jQ) &= \left(\frac{-t_j^{-3}-\eta(iP)+O(t_j)}{t_j^{-2}-\xi(iP)-O(t_j^2)}\right)^2-(t_j^{-2}+O(t_j^2))-\xi(iP)\\ &= \xi(iP)+2\eta(iP)t_j+O(t_j^2)\end{aligned}$$

を得る。p は奇数で $P\in\widetilde{E}[p]\cap\widetilde{E}(R^{\mathrm{ur}})$ であることを思いだそう。これは $1\le i\le p-1$ に対して $\mathrm{ord}_p(\eta(iP))=0$ であることを意味する。他方、$1\le i<j\le(p-1)/2$ に対して $\mathrm{ord}_p(\xi(iP)-\xi(jP))=0$ である。従って

$$\begin{aligned}\mathrm{ord}_p(\xi(P)-\xi(jQ)) &= -2\mathrm{ord}_p t_j,\\ \mathrm{ord}_p(\xi(P)-\xi(P+jQ)) &= \mathrm{ord}_p t_j,\\ \mathrm{ord}_p(\xi(P)-\xi(iP+jQ)) &= 0 \quad (i\ge 2\text{のとき})\end{aligned}$$

となる。$1\le j\le p-1$ に対して $t_j=-t_{p-j}$ なのだから

$$\begin{aligned}\mathrm{ord}_p((\partial\Psi_p)(\xi(P),\widetilde{A},\widetilde{B})) &= 1+\sum_{j=1}^{(p-1)/2}(-2\mathrm{ord}_p t_j)+0+\sum_{j=1}^{p-1}\mathrm{ord}_p t_j\\ &= 1.\end{aligned}$$

■

定理 3.8. $E/\mathbf{F}_q$ を Weierstrass 方程式 $Y^2=X^3+AX+B$ により定義される $j(E)\notin\mathbf{F}_{p^2}$ であるような楕円曲線とする。$E^{(i)}$ をその $\mathbf{F}_p$ 上の共役 $Y^2=X^3+(\mathrm{Fr}_p^i A)X+\mathrm{Fr}_p^i B,\ M\ge 2$ を整数とする。このとき $R \bmod p^M$ 上の算術演算 $O(N\log M)$ 回と $\mathbf{F}_q$ 上の算術演算 $O(N^2)$ 回で $0\le i<N$ 全てに対して以下の条件を満たす出力を求めるアルゴリズムがある。(証明中も含めて O-constant は p に依存する。)：

出力：

$0\le i<N$ に対する以下の値：

- 楕円曲線 $E^{\langle\langle i\rangle\rangle}: Y^2=X^3+A^{\langle\langle i\rangle\rangle}X+B^{\langle\langle i\rangle\rangle}$.
- 多項式

$$h^{\langle\langle i\rangle\rangle}(X) := \prod_{P\in(G^{\langle\langle i\rangle\rangle}-\{\mathcal{O}\})/\pm 1}(X-\xi(P)) \in R[X]$$

の $\bmod p^{M-1}$. ここで $G^{\langle\langle i\rangle\rangle}:=E^{\langle\langle i\rangle\rangle}[p]\cap E^{\langle\langle i\rangle\rangle}(R^{\mathrm{ur}})$ である。

条件：

(i) $j(E^{\langle\langle i\rangle\rangle})\equiv j(E^{(i)\uparrow})\bmod p^M$.

(ii) 群 $G^{\langle\langle i\rangle\rangle}:=E^{\langle\langle i\rangle\rangle}[p]\cap E^{\langle\langle i\rangle\rangle}(R^{\mathrm{ur}})$ は位数 p の巡回群であり、その $\bmod p$ は $E[p]$ である。

(iii) $\pi(A^{\langle\langle i\rangle\rangle})=A^{(i)}$ and $\pi(B^{\langle\langle i\rangle\rangle})=B^{(i)}$.

証明．最初に $\mathbf{F}_q$ 上の乗算 $O(N)$ 回で $A^{(i)}:=\mathrm{Fr}_p^i A$ と $B^{(i)}:=\mathrm{Fr}_p^i B$ を計算する。$z_i\in R$ を $\pi(z_i)=j(E^{(N-i)})$ が満たされるようにとる。命題 3.3 を $O(\log M)$ 回繰り返して使って $\Phi_p(\zeta_i,\zeta_{i+1})\equiv 0\bmod p^M$ かつ $\pi(\zeta_i)=j(E^{(N-i)})$ となる $\zeta_i\in R$ を $R\bmod p^M$ 上の算術演算 $O(N\log M)$ 回で求めることができる。$A^{\langle\langle i\rangle\rangle},\ B^{\langle\langle i\rangle\rangle}\in R$ を $\pi(A^{\langle\langle i\rangle\rangle})=A^{(i)},\ \pi(B^{\langle\langle i\rangle\rangle})=B^{(i)},\ j(E^{\langle\langle i\rangle\rangle})=\zeta_{N-i}$ となるように選ぶ。これは $\mathbf{F}_q$ において $\dfrac{\partial j}{\partial A}(A^{(i)},B^{(i)})\neq 0$ だから確かに可能であり、$O(N\log M)$ 回の算術演算で十分である。また、これは (iii) が成立していることも意味する。他方、$\Phi_p(j(E^{(N-i)\uparrow}),j(E^{(N-i+1)\uparrow}))=0$ と $\pi(j(E^{(N-i)\uparrow}))=j(E^{(N-i)})$ が成立している。系 3.4 より条件 (i) が満たされることが分かる。そうすると定理 3.1(iv)→(i) により条件 (ii) も満たされる。$h^{\langle\langle i\rangle\rangle}$ を求めるために p-th division polynomial Ψ_p を調べる。ここで $\pi(\Psi_p(X,A^{\langle\langle i\rangle\rangle},B^{\langle\langle i\rangle\rangle}))=cf(X)^p$, ただし $f\in\mathbf{F}_q[X]$ は *monic square free*, $c\in\mathbf{F}_q^\times$, と因数分解することに注意する。Cf. Cassels[1, Theorem I]. 具体的には $f(X)=\sum_{k=0}^{(p-1)/2}\dfrac{u_k}{u_{(p-1)/2}}X^k$, ここで u_k は $\Psi_p(X,A^{(i-1)},B^{(i-1)})$ の X^{pk} の係数、となる。いずれにせよ、$\mathrm{ord}_p(\partial\Psi_p)(X,A^{\langle\langle i\rangle\rangle},B^{\langle\langle i\rangle\rangle})\geq 1$ である。他方、$E^{\langle\langle i\rangle\rangle}$ は定理 3.1 の仮定 (iv) を満たす。補題 3.7 を適用して $\mathrm{ord}_p(\partial\Psi_p)(X,A^{\langle\langle i\rangle\rangle},B^{\langle\langle i\rangle\rangle})=1$ であることおよび f は $\pi\left(\dfrac{1}{p}(\partial\Psi_p)(X,A^{\langle\langle i\rangle\rangle},B^{\langle\langle i\rangle\rangle})\right)$ と互いに素であることが分かる。すると $U(X):=\Psi_p(X,A^{\langle\langle i\rangle\rangle},B^{\langle\langle i\rangle\rangle}),\ t:=1$ に対して補題 2.1 を最初は $u:=1$ として繰り返し使えば補題 2.2 により $\Psi_p(X,A^{\langle\langle i\rangle\rangle},B^{\langle\langle i\rangle\rangle})$ の monic factor $h(X)$ が求まる。R^{ur} 内の $\Psi_p(X,A^{\langle\langle i\rangle\rangle},B^{\langle\langle i\rangle\rangle})$ の根は $G^{\langle\langle i\rangle\rangle}$ の点の X-座標であることに注意する。h は R^{ur} 内に $(p-1)/2$ 個の異なる根を持つから $h=h^{\langle\langle i\rangle\rangle}$ である。よって補題 2.1 を $O(\log M)$ 回使い $h^{\langle\langle i\rangle\rangle}\bmod p^{M-1}$ を得る。このとき必要な計算量は各 i に対して $R\bmod p^M$ 上の算術演算 $O(\log M)$ 回である。■

注意 3.9. $p=2$ のときは補題 3.7 が成立しないので補題 2.1 を用いることができない。これが我々の方法を $p=2$ に適用しようとするときの最も大きな障壁である。これをどのように回避するかの方針を少し考えてみよう。$M\geq 3$ とする。R を $\mathbf{Q}_2$ の N 次不分岐拡大の付値環とする。$\widetilde{a_2}\in R,\ \widetilde{a_6}\in R^\times$ とし楕円曲線 $\widetilde{E}/R$ を

$$\widetilde{E}:\ Y^2+XY\ =\ X^3+\widetilde{a_2}X^2+\widetilde{a_6}$$

により定義する。その reduction $\bmod 2$ を E と書く。$U(X):=4X^3+(1+4\widetilde{a_2})X^2+4\widetilde{a_6}$ とおく。$\widetilde{E}[2]-\{\mathcal{O}\}$ の点の X-座標は U の根として特徴付けられる。$(x,y)\in\widetilde{E}[2]\cap\widetilde{E}(R^{\mathrm{ur}})-\{\mathcal{O}\}$ とする。このとき $\mathrm{ord}_2 x=1$ でありそのような点は $-\dfrac{\widetilde{a_6}}{1+4\widetilde{a_2}}$ が R の平方元であるとき、かつそのときに限り存在する。この条件は $\widetilde{a_2}\bmod 2$ と $\widetilde{a_6}\bmod 8$ のみに依存する。$j(\widetilde{E})\equiv -1/\widetilde{a_6}\bmod 8$ だから $\widetilde{a_6}$ を $j(\widetilde{E})\equiv j(E^\uparrow)\bmod p^{M+2}$ となるように選ぶことができる。このとき $\widetilde{E}[2]\cap\widetilde{E}(R^{\mathrm{ur}})\neq\{\mathcal{O}\}$ であり $x\bmod 8$ を $R/8R$ の演算 $O(1)$ 回と $\mathbf{F}_{2^N}[X]$ の因数分解 (確率的アルゴリズム) 1 回で求めることができる。ところで我々が持ち上げる必要があるのは E の自明でない 2 分点 1 点のみであることに注意する。

よって $j(E^{\uparrow}) \bmod 2^{M+2}$ が計算できれば Newton 法を用いて $\widetilde{a_6} \bmod 2^{M+2}$ と $x \bmod 2^M$ を $R/2^{M+2}R$ 上の算術演算 $O(N \log M)$ 回で求めることができる。

4. 位数計算への応用

本節では前節に述べた結果をどのようして楕円曲線の位数計算に応用するかを考える。E を $\mathbf{F}_q$ 上定義された楕円曲線とする。$j(E) \in \mathbf{F}_{p^2}$ の場合は位数が簡単に求まることを命題 4.2 においておいて示す。一旦これが示されてしまえばあとは $j(E) \notin \mathbf{F}_{p^2}$ の場合だけを考えれば良い。すると前節で述べた方法が適用できる。我々は E の canonical lift に Verschiebung がどのように作用するかを見、そこからその trace を計算する。まず楕円曲線の自己準同型から導かれた formal group の自己準同型に関する簡単な考察から始める。多かれ少なかれこれは知られていることと思われるが、著者にはこの証明が書かれた文献を見つけることができなかった。

命題 4.1. $\mathscr{E}/K$ を楕円曲線、$f \in \mathrm{End}_K(\mathscr{E})$ の次数が d であるとする。f の modulo p での reduction $\pi(f)$ が分離的で $f(\mathrm{Ker}\pi) \subset \mathrm{Ker}\pi$ であるとする。f から $\mathscr{E}$ の formal group $\widehat{\mathscr{E}}$ に導かれた自己準同型を $\widehat{f}$ とする。$\widehat{f}$ の $\mathscr{O}$ における τ によるベキ級数展開を $\widehat{f}(\tau) = \sum_{n=1}^{\infty} c_n \tau^n$ とする。このとき

$$\mathrm{Tr}(f) \;=\; c_1 + \frac{d}{c_1} \tag{4.1}$$

が成立する。

証明． $\mathrm{End}(\mathscr{E})$ において f は $f \circ f - \mathrm{Tr}(f) f + d = 0$ を満たす。よって $\widehat{\mathscr{E}}$ 上で

$$(c_1^2 - \mathrm{Tr}(f) c_1 + d)\tau + O(\tau^2) \;=\; 0$$

が成立するから τ の係数は 0 でねばならない。他方 $\pi(f)$ は分離的だから $\pi(c_1) \neq 0$ とくに $c_1 \neq 0$ である。(Cf. Silverman[19, Cor. IV.7.5] の case 2 の証明。) ゆえに (4.1) は成立する。■

命題 4.2. $q := p^N$ とし $E : Y^2 = X^3 + AX + B$ を $\mathbf{F}_q$ 上定義された楕円曲線とする。$j(E) \in \mathbf{F}_{p^2}$ と仮定する。このとき ${}^{\#}E(\mathbf{F}_q)$ は $\mathbf{F}_q$ 上の算術演算 $O(N)$ 回と bit 演算 $O(N^{1+\mu})$ 回で求まる。

証明． $m \in \mathbf{N}$ を $p^m = {}^{\#}\mathbf{F}_p(j(E))$ により定める。仮定 $j(E) \in \mathbf{F}_{p^2}$ から $m = 1$ か $m = 2$ である。このとき E と $\mathbf{F}_q$ 上同型である $\mathbf{F}_{p^m}$ 上定義された楕円曲線 $E' : Y^2 = X^3 + A'X + B'$ がある。実際に E' を見つけるには以下のようにすればよい。E と E' が $\mathbf{F}_q$ 上同型であるかどうかは $\mathbf{F}_q$ 上の算術演算 $O(N)$ 回で判定できる。例えば $AB \neq 0$ の場合は $j(E) = j(E')$ かつ $\left(\dfrac{A/B}{A'/B'}\right)^{(q-1)/2} = 1$ であるかを確かめれば良い。他の場合も同様である。ゆえに $A' \in \mathbf{F}_{p^m}$ と $B' \in \mathbf{F}_{p^m}$ の可能な値を全て試せば E' が見つかる。${}^{\#}E(\mathbf{F}_q) = {}^{\#}E'(\mathbf{F}_q)$ であることは自明であろう。ゆえに $T_i := \mathrm{Tr}\mathrm{Fr}_{p^m}^i|_{E'}$. とおくと $T_{N/m}$ を求めれば良い。(m は常に N を割り切ることに注意。) T_1 $(= 1 + p^m - {}^{\#}E'(\mathbf{F}_{p^m}))$ は例えば全数探索により (N に関して) $\mathbf{F}_{p^m}$ の算術演算 $O(1)$ 回分の計算量で求まる。$T_{N/m}$ は良く知られた漸化式 $T_{i+2} - T_1 T_{i+1} + p^m T_i = 0$ (ここで $T_0 = 2$) により求まる。$|T_i| \leq 2p^{im/2}$ だから T_1 から $T_{N/m}$ を求めるに計算量は $O(N^{1+\mu})$ の bit operation で十分である。■

以下、$j(E)\notin\mathbf{F}_{p^2}$ し、定理 3.8 と同じ記号を用いる。さらに $E^{(i)\uparrow}$ を $E^{(i)}$ の canonical lift とする。一般性を失うことなく $E^{(i)\uparrow}$ は適当な $A^{(i)\uparrow}\in R$ を用いて $Y^2=X^3+A^{(i)\uparrow}X+B^{\langle\langle i\rangle\rangle}$ により与えあられているとして良い。便宜上 $B^{(i)\uparrow}:=B^{\langle\langle i\rangle\rangle}$ とおく。$G^{(i)}:=E^{(i)\uparrow}[p]\cap E^{(i)\uparrow}(R^{\mathrm{ur}})$ とおく。これは位数 p の巡回群である。

$V_p^{(i)}$ を $\mathrm{Fr}_p\in\mathrm{Isog}(E^{(i-1)},E^{(i)})$ の dual isogeny とする。Messing[13, Corollary V.3.4]. により $V_p^{(i)}$ は $V_p^{(i)\uparrow}\in\mathrm{Isog}(E^{(i)\uparrow},E^{(i-1)\uparrow})$ に持ち上げられる。これが formal group 上でどのように見えるか調べる。

命題 4.3. $\tau_i(X,Y):=-X/Y$ を $E^{(i)\uparrow}$ の $\mathcal{O}$ における local parameter とする。$A^{(i)\uparrow}$, $B^{(i)\uparrow}$ と

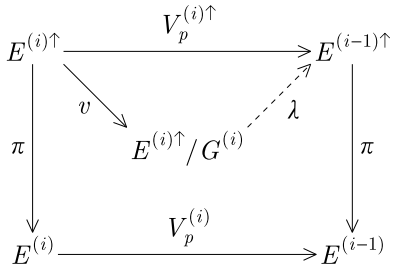
$$h^{(i)\uparrow}(X)\ :=\prod_{g\in(G^{(i)}-\{\mathcal{O}\})/\pm1}(X-\xi(g))$$

が与えられたと仮定する。$c_1^{(i)}\in R$ を

$$\tau_{i-1}\circ V_p^{(i)}\ =\ c_1^{(i)}\tau_i+O(\tau_i^2)$$

によって定める。このとき $c_1^{(i)2}$ の値は R の算術演算 $O(1)$ 回で求まる。

証明． $V_p^{(i)\uparrow}$ は $V_p^{(i)}$ の持ち上げであるから次の図式の長方形の部分は可換である。



$v\in\mathrm{Isog}(E^{(i)\uparrow},E^{(i)\uparrow}/G^{(i)})$ を Vélu[20] により構成された isogeny とする。具体的には

$$v(X,Y)\ :=\ \left(X+\sum_{g\in G^{(i)}-\{\mathcal{O}\}}(\xi((X,Y)+g)-\xi(g)),\ \sum_{g\in G^{(i)}}\eta((X,Y)+g)\right)$$

(ここで $(X,Y)+g$ のプラス記号は曲線上の加法を表す) である。Vélu の公式は $E^{(i)\uparrow}/G^{(i)}$ の Weierstrass model も与える。s_i を $h^{(i)\uparrow}$ の $X^{((p-1)/2)-i}$ の係数とする。すると $E^{(i)\uparrow}/G^{(i)}$ は $Y^2=X^3+\alpha_iX+\beta_i$, ただし

$$\begin{aligned}\alpha_i\ &:=\ A^{(i)\uparrow}-5\sum_{g\in G^{(i)}-\{\mathcal{O}\}}(3\xi(g)^2+A^{(i)\uparrow})\\ &=\ (6-5p)A^{(i)\uparrow}-30(s_1^2-2s_2),\\ \beta_i\ &:=\ B^{(i)\uparrow}-7\sum_{g\in G^{(i)}-\{\mathcal{O}\}}(5\xi(g)^3+3A^{(i)\uparrow}\xi(g)+2B^{(i)\uparrow})\\ &=\ (15-14p)B^{(i)\uparrow}-70(-s_1^3+3s_1s_2-3s_3)+42A^{(i)\uparrow}s_1\end{aligned}$$

により与えられる。なお、$p=5$ のときは $s_3=0$ と解するものとする。$\mathrm{Ker}\,v=\mathrm{Ker}\,V_p^{(i)\uparrow}=G^{(i)}$ だから Silverman[19, Cor. III.4.11] により上の図式の三角形の部分を可換にする $\lambda\in\mathrm{Isog}(E^{(i)\uparrow}/G^{(i)},E^{(i-1)\uparrow})$ がある。しかし $\deg(V_p^{(i)\uparrow})=\deg(v)\ \ (=p)$ ということは $\deg(\lambda)=1$, すなわち λ が同型であるというこ

とである。よって λ は適当な定数 $\gamma_i \in R$ を用いて

$$\lambda(X,\, Y) \;=\; (\gamma_i^2 X, \gamma_i^3 Y)$$

となる筈である。Vélu[20, (13)] によって写像 v は一次の項が 1 であるような formal group 間の準同型 $\widehat{v}$ を導くが他方においては $\widehat{\lambda}(t) = t/\gamma_i$ である。合成写像をとって $c_1^{(i)} = 1/\gamma_i$ を得る。Weierstrass model の係数を見て $B^{(i-1)\uparrow} = \beta_i \gamma_i^6$, $A^{(i-1)\uparrow} = \alpha_i \gamma_i^4$ でねばならずこれから $c_1^{(i)2} = \gamma_i^{-2} = \dfrac{\beta_i/\alpha_i}{B^{(i-1)\uparrow}/A^{(i-1)\uparrow}}$ を得る。■

定理 4.4. $E/\mathbf{F}_q$ を $j(E) \notin \mathbf{F}_{p^2}$ であるような楕円曲線とする。時間計算量が $R \bmod p^N$ の算術演算 $O(N \log N)$ 回と $\mathbf{F}_q$ の算術演算 $O(N)$ 回分以下であるような $\#E(\mathbf{F}_q)$ を求めるアルゴリズムが存在する。

証明 . $c_1^{(i)}$ を命題 4.3 の通りとする。すると (4.1) から

$$\begin{aligned} \mathrm{Tr}(\mathrm{Fr}_q) \;&=\; \mathrm{Tr}\,(\, V_p^{(0)\uparrow} \circ V_p^{(N-1)\uparrow} \circ \;\cdots\; \circ V_p^{(2)\uparrow} \circ V_p^{(1)\uparrow}) \\ &=\; c + \frac{q}{c}, \end{aligned}$$

ただし $c := \prod_{i=0}^{N-1} c_1^{(i)}$ となる。しかしながら $|\mathrm{Tr}\mathrm{Fr}_q| \le 2\sqrt{q}$ である。よって $\mathrm{Tr}\mathrm{Fr}_q$ を得るには $c \bmod p^{[(N+3)/2]}$ が分かれば十分である。よって $A^{(i)\uparrow}$ と $h^{(i)\uparrow}$ の替りに定理 3.8 $M := [(N+5)/2]$ ととった $A^{\langle\langle i\rangle\rangle}$ と $h^{\langle\langle i\rangle\rangle}$ が分かれば十分である。これには $O(N \log M)$ 回の算術演算が必要である。命題 4.3 によって c^2 を $O(N)$ 回の算術演算により求めることができる。他方、C_1 を $(X^3 + AX + B)^{(p-1)/2} \in \mathbf{F}_q[X]$ の X^{p-1} の係数とし $n \ge 2$ に対して C_n を帰納的に

$$C_n \;:=\; C_{n-1} C_1^{p^{n-1}}$$

と定める。Silverman[19, Theorem V.4.1] の証明中に示されているように $C_N \equiv c \bmod p$ である。明らかに C_N は $\mathbf{F}_q$ 上 $O(N)$ 回の乗算で求まる。ゆえに C_N と $c^2 \bmod p^M$ から $c \bmod p^M$ を $R/p^M R$ 上の算術演算 $O(\log N)$ 回で求めることができる。v を $|v| \le 2\sqrt{q}$ かつ $v \equiv c \bmod p^M$ となる唯一の整数とする。すると良く知られているように $\#E(\mathbf{F}_q)$ は $q + 1 - v$ によって与えられる。■

注意 4.5. $R \bmod p^N$ の算術演算 1 回は $O(N^{2\mu})$ 回で実現できる。同様に $\mathbf{F}_q$ の算術演算の計算量は $O(N^{\mu})$ である。したがって我々のアルゴリズムの計算量は注意 3.6 の方法を援用すれば FFT 乗算を用いた場合 $O(N^3)$ の、素朴な乗算を用いた場合 $O(N^5)$ の計算量である。実装に当たっては Karatsuba 法の採用が現実的選択であろう。その場合は理論上 $O(N^{4.2})$ のアルゴリズムとなる。

注意 4.6. c^2 を求めるにあたって $\prod_{i=0}^{N-1} c_1^{(i)2}$ を計算するのではなく ($c^{(1)2}$, $\ldots$, $c^{(N-1)2}$ を求めず) $c^{(0)2}$ だけから $N_{K/\mathbf{Q}_p}(c_1^{(0)2})$ 計算する方が良いのではないかと思うかも知れない。しかしながら norm の計算はさほど速くはない。$\sigma \in \mathrm{Gal}(K/\mathbf{Q}_p)$ を Frobenius 置換とする。著者の知る限り $x \in R/p^M R$ に対して $\sigma(x)$ を計算するには $R/p^M R$ 上の算術演算を事前計算に $O(N^2)$ 回、x ごとに $O(N)$ 回必要とする。そのような方法は明らかに遅い。それよりはましな方法として適当な $K/\mathbf{Q}_p$ の基底に関して $c_1^{(0)}$ 倍写像の表現行列を求めその行列式を (漸近的高速アルゴリズムを用いて) 計算することが考

えられる。しかし、(かけ算に FFT を使うなら) この方法でもなお正直に $\prod_{i=0}^{N-1} c_1^{(i)}$ を計算するのにかなわない。

参考文献

1. Cassels, J. W. S.: A note on the division values of $\wp(u)$. Proc. Cambridge Philos. Soc. **45**, 167-172 (1949)
2. Cassels, J. W. S.: Lectures on elliptic curves. London Mathematical Society Student Texts, 24. Cambridge: Cambridge UP 1991
3. Cohen, H.: A course in computational algebraic number theory. GTM, 138. Berlin: Springer-Verlag 1993
4. Couveignes, J.-M.: Computing l-isogenies using the p-torsion, Algorithmic number theory (Telence, 1996), Lecture Notes in Comput. Sci., **1122**, Berlin: Springer, 1996.
5. Deuring, M.: Die Typen der Multiplikatorenringe elliptischer Funktionenkörper. Abh. Math. Sem. Univ. Hamburg **14**, 197-272 (1941)
6. Dewaghe, L.: Remarks on the Schoof-Elkies-Atkin algorithm. Math. Comp. **67**, 1247-1252 (1998)
7. 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.
8. Hensel, K.: Eine neue Theorie der algebraischen Zahlen. Math. Z. **2**, 433-452 (1918)
9. Koblitz, N.: Elliptic curve cryptosystems. Math. Comp. **48**, 203-209 (1987)
10. Koike, M.: Congruences between modular forms and functions and applications to the conjecture of Atkin. J. Fac. Sci. Univ. Tokyo **20**, 129-169 (1973)
11. Lang, S.: Algebraic number theory. Reading, Mass.: Addison-Wesley Pub. 1970
12. Lubin, J., Serre, J.-P. and Tate, J.: Elliptic curves and formal groups, (1964). Mimeographed notes, available at http://www.ma.utexas.edu/users/voloch/lst.html
13. 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
14. 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.
15. Nakamura, T.: A note on elliptic curves with ordinary reduction. Arch. Math. **60**, 440-445 (1980)
16. Satoh, T. and Araki, K.: Fermat Quotients and the Polynomial Time Discrete Log Algorithm for Anomalous Elliptic Curves. Commentarii Math. Univ. St. Pauli. **47**, 81-92 (1998)
17. Satoh, T. and Araki, K.: Errata to the paper "Fermat Quotients and the Polynomial Time Discrete Log Algorithm for Anomalous Elliptic Curves", (1999). to appear in Commentarii Math. Univ. St. Pauli.
18. Schoof, R.: Counting points on elliptic curves over finite fields. J. Théor. Nombres Bourdeaux **7**, 219-254 (1995)
19. Silverman, J. H.: The arithmetic of elliptic curves. GTM, 106. Berlin-Heidelberg-New York: Springer 1985
20. Vélu, J.: Isogénies entre courbes elliptiques. C.R. Acad. Sc. Paris. **273**, 238-241 (1971)
21. Voloch, J.F. and Walker, J.L.: Euclidean weights of codes from elliptic curves over rings. preprint
22. Zassenhaus, H.: On Hensel Factorization, I. J. Number Theory **1**, 291-311 (1969)