The Canonical Lift of an Ordinary Elliptic Curve over a Finite Field and its Point Counting

Dedicated to the memory of Dr. Kenji Koyama

Takakazu Satoh.
Dept. Math. Fac. Sci.
Saitama University,
Urawa, Saitama, 338-8570 JAPAN
tsatoh@rimath.saitama-u.ac.jp

Abstract.

This paper is concerned with the problem of counting the number of points on an elliptic curve over a field $\mathbf{F}_{p^N}$ in the case where p is a small prime and N is a large integer. For simplicity we restrict to the case of $p \geq 5$. Our idea is different to the method of Schoof, Elkies and Atkin. We lift E to its canonical lift and compute the trace of Verschiebung (i.e. the dual of the Frobenius morphism) directly in characteristic zero. Define $\mu > 0$ so that the complexity of multiplication of two n-bit objects is $O(n^{\mu})$ bit operations. The method of Elkies with Couveignes' isogeny finding algorithm runs in heuristically $O((N \log p)^{2\mu+2})$ bit operations while our algorithm runs in $O(N^{2\mu+1})$ bit operations where the O-constant depends (badly) on p.

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

1. Introduction

Let p be a prime, $N \in \mathbf{N}$, $q := p^N$. We denote by $\mathbf{F}_q$ the finite field with q elements. Suppose E is an elliptic curve over $\mathbf{F}_q$. Our goal is to compute the number of $\mathbf{F}_q$-rational points on E in the case where p is small and N is large. This is an important problem in computational number theory and it has applications in cryptography. For elliptic curves over fields of large characteristic the algorithm due to Schoof, Elkies and Atkin is widely known (see Schoof[19], Elkies[7]). This algorithm has been modified to the case of fields of small characteristic by Couveignes[4] (also see Lercier and Morain[12]).

The idea behind to their method is to calculate $\mathrm{Tr}\,\mathrm{Fr}_q \bmod l$ for various primes l. Here, for each $n \geq 1$, we denote by Fr_{p^n} the p^n-th power Frobenius map. By Hasse's inequality $|\mathrm{Tr}\,\mathrm{Fr}_q| \leq 2\sqrt{q}$, we can recover $\mathrm{Tr}\,\mathrm{Fr}_q$ using the Chinese remainder theorem. Let $\mu \in \mathbf{R}$ be such that we can multiply two n-bit integers (resp. two polynomials of degree n) with $O(n^\mu)$ bit operations (resp. $O(n^\mu)$ arithmetic operations over coefficient rings). So, $\mu = 2$ for naive multiplication, $\mu = \log_2 3$ for the Karatsuba method, and $\mu = 1+\varepsilon$ for FFT based multiplication. The time complexity of Schoof's algorithm is $O((\log q)^{3\mu+2})$ bit operations. That of Elkies' algorithm is $O((\log q)^{2\mu+2})$ under the assumption that among primes of size $O(\log q)$, approximately half of them split in the endomorphism ring of a given elliptic curve. This assumption is not proved but it seems to hold for most elliptic curves. Due to the methods of Couveignes[4] for finding isogenies and Dewaghe[6] for finding eigenvalues, the most time consuming step is the computation of the action of Frobenius for each l about $O(\log q)$ times. So, to obtain a faster algorithm, the problem is how to avoid the Frobenius endomorphism of E.

Our method is totally different. We work with the characteristic zero lifting and obtain $\mathrm{Tr}\,\mathrm{Fr}_q$ directly, *not* via $\mathrm{Tr}\,\mathrm{Fr}_q \bmod l$. (Although Couveignes[4] paid attention to the Verschiebung and the p-torsion, his method still repeatedly computes $\mathrm{Tr}\,\mathrm{Fr}_q \bmod l$ for $O(\log q)$ primes l.) Our algorithm is efficient for small $p \geq 5$ and large N. The time complexity of our algorithm is $O(N^{2\mu+1})$ bit operations where O-constant depends on p. Unfortunately, behavior with respect to p is very bad as we need to use the p-th modular polynomial.

Let $E/\mathbf{F}_q$ be an elliptic curve. In Proposition 4.2 we show the case $j(E) \in \mathbf{F}_{p^2}$ is easily handled. So, in what follows, we can assume $j(E) \notin \mathbf{F}_{p^2}$ and, in particular, that E is ordinary. Instead of the Frobenius morphism Fr_p, we use the Verschiebung V_p which is the dual isogeny of Fr_p. For an ordinary elliptic curve $E/\mathbf{F}_q$, we denote its canonical lift by $E^\uparrow$, which is an elliptic curve over some unramified extension of $\mathbf{Q}_p$. The canonical lift of E is characterized by the following two properties: the modulo p reduction of $E^{\uparrow}$ is E, and $\mathrm{End}(E) \cong \mathrm{End}(E^{\uparrow})$ as a ring. A classical result of Deuring[5] shows that $E^{\uparrow}$ exists and is unique up to isomorphism. This notion is reformulated in the context of modern algebraic geometry by Lubin, Serre and Tate[13] (see also Messing[14]). If E and E' are ordinary elliptic curves over $\mathbf{F}_q$, then $\mathrm{Hom}(E, E') \cong \mathrm{Hom}(E^{\uparrow}, E'^{\uparrow})$. Cf. Messing[14, Corollary V.3.4]. Let $E^{(i)} := \mathrm{Fr}_p^i E$. Since E is ordinary, the elliptic curves $E^{(i)}$ for $i = 0, \ldots, N-1$ are also ordinary and $V_p: E^{(i)} \to E^{(i-1)}$ is separable. This implies that we can explicitly lift V_p to $V_p^{\uparrow}: E^{(i)\uparrow} \to E^{(i-1)\uparrow}$ by lifting the kernel of V_p, i.e. the group $E[p]$ of p-torsion points of E. By looking at the action of $V_p^{\uparrow N}: E^{\uparrow} \to E^{\uparrow}$ on formal group of $E^{\uparrow}$, we obtain the trace of $V_p^{\uparrow N}$, which is equal to the trace of Fr_q.

$$\begin{tikzcd}
E^{\uparrow} \arrow[r, "V_p^{\uparrow}"] & E^{(N-1)\uparrow} \arrow[r, "V_p^{\uparrow}"] & E^{(N-2)\uparrow} \arrow[r] & \cdots \arrow[r, "V_p^{\uparrow}"] & E^{\uparrow} \\
E = E^{(N)} \arrow[u] \arrow[r, shift left, "V_p"] & E^{(N-1)} \arrow[u] \arrow[l, shift left, "\mathrm{Fr}_p"] \arrow[r, shift left, "V_p"] & E^{(N-2)} \arrow[u] \arrow[l, shift left, "\mathrm{Fr}_p"] \arrow[r, shift left] & \cdots \arrow[l, shift left] \arrow[r, shift left, "V_p"] & E \arrow[u] \arrow[l, shift left, "\mathrm{Fr}_p"]
\end{tikzcd}$$

The above method is based on the following observations:

- The prime p is a priori an Elkies prime in the sense that $E[p]$ is an Fr_q invariant subgroup of order p.
- The algebraization of lifting of Verschiebung seems to be much easier than that of Frobenius. All we have to do is to lift $E[p]$.
- Assume that $f \in \mathrm{End}(E^{\uparrow})$ is "explicitly" given and that reduction modulo p of f is separable. Then it is easy to determine the characteristic polynomial of f by looking at the formal group of $E^{\uparrow}$ since $E^{\uparrow}$ is of characteristic zero. (See Proposition 4.1.)

Section 2 is somewhat technical. We study lifting of a factor of a certain polynomial whose reduction modulo p is inseparable. In Section 3, we construct the Weierstrass model of the canonical lift of given elliptic curve $E/\mathbf{F}_q$ with $j(E) \notin \mathbf{F}_{p^2}$. In Section 4, we explain how to utilize the canonical lift in our point counting algorithm.

The problem of point counting of elliptic curves over finite fields has a connection to the elliptic curve cryptography independently proposed by Miller[15] and Koblitz[9]. In the application, the case $p=2$ is very important. However, to avoid technical difficulties, we limit ourselves to the case $p\geq 5$. See also Remark 3.9.

The result of this paper was announced at the conference "Algebra and Computation 99", held on 18-22, Oct., 1999 at Tokyo Metropolitan university.

Acknowledgement: The author would like to thank Dr. S. Galbraith and Ms. B. Skjernaa who read and commented on an earlier version of this paper.

Notation

Unless otherwise explicitly specified, $p\geq 5$ is a prime, $N\in\mathbf{N}$, and $q:=p^N$. We choose and fix an unramified extension $K/\mathbf{Q}_p$ of degree N. We denote its valuation ring by R. Since $K/\mathbf{Q}_p$ is unramified, p remains prime, and the residue field of R is $\mathbf{F}_q$. We denote the maximal unramified extension of K and its valuation ring by K^{ur} and R^{ur}, respectively. In general, $\mathcal{O}$ stands for the point at infinity of elliptic curves, and π is the reduction modulo p map. For elliptic curves E_1 and E_2, the set of isogenies from E_1 to E_2 is denoted by $\mathrm{Isog}(E_1,E_2)$. The p-th modular polynomial is denoted by $\boldsymbol{\Phi}_p$. We denote the X-coordinate function and the Y-coordinate function by ξ and η, respectively. Some other symbols are introduced in Sect. 3.

2. Lifting of a Factor of Polynomials

In this section, we consider a method to lift a factor of certain polynomials. More precisely, let $U\in R[X]$ and suppose we have a factor $f\in\mathbf{F}_q[X]$ of $\pi(U)$. We want to lift f to a factor g of U even if $\pi(U)$ is a power of a irreducible polynomial. This is a variant of Hensel's lemma[8], however we need to consider the computational complexity. Our algorithm is based on the quadratic lifting by Zassenhaus[23, Lemma 2]. See also Cohen[3, Sect. 3.5.3].

Let f, $g\in R[X]$ with $\gcd(\pi(f),\pi(g))=1$. Then, for each $u\in\mathbf{N}$, there exist A_u, $B_u\in R[X]$ satisfying $A_uf+B_ug\equiv 1 \bmod p^u$. Moreover, if f is monic, we can construct such B_u satisfying $\deg B_u<\deg f$ in time $O((\deg f+\deg g)^2)$ arithmetic operations over

R/p^uR. For $u=1$, this is done by Euclid's algorithm. For $u>1$, we first compute $A_{[(u+1)/2]}$ and $B_{[(u+1)/2]}$ by recursion and lift them to A_u and B_u, respectively. We note that arithmetic over $R/p^{[(u+1)/2]}R$ requires less time than over R/p^uR. Note that, for $u \geq 2$, a direct application of Euclid's algorithm to f and g may require much more time because in this case we need pseudo divisions.

Lemma 2.1. *Let p be an odd prime, $U \in R[X]$. Put $t := \operatorname{ord}_p \partial U$ where $\partial = \frac{d}{dX}$. Let $f \in R[X]$ be a monic polynomial satisfying the following conditions:*

(i) *f is monic.*

(ii) *$\pi(f)$ is square free.*

(iii) *$\pi(f)$ is relatively prime to $\pi(p^{-t}\partial U)$.*

(iv) *There exists $Q_0 \in R[X]$ and $u \in \mathbf{N}$ such that $\operatorname{ord}_p(U - fQ_0) \geq u+t$.*

Put $v := 2u + \min(t, u)$ for simplicity. Then we have the following:

(a) Assume there exist g, $Q_1 \in R[X]$ satisfying $g \equiv f \bmod p$ and $\operatorname{ord}_p(U - gQ_1) \geq v$. Then for all $h \in R[X]$ such that $h \equiv g \bmod p^{2u}$, there exists $Q_2 \in R[X]$ (which depends on h) satisfying $\operatorname{ord}_p(U - hQ_2) \geq v$.

(b) There exist $Q_3 \in R[X]$ and a monic $g \in R[X]$ satisfying

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

and $g \equiv f \bmod p^u$. (Note necessarily $\pi(g) = \pi(f)$ and $\deg g = \deg f$.) We can construct g with $O((\deg f + \deg U)^2)$ arithmetic operations over $R/p^{2u}R$.

Proof. (a): Put $\delta := p^{-2u}(h-g) \in R[X]$. Since $g \equiv f \bmod p$, the reduction $\pi(g)$ is also square free. By the above remark, there are polynomials A, $B \in R[X]$ such that

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

On the other hand, $U \equiv gQ_1 \bmod p^v$ implies

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

with $Q_4(X) := Q_1(X + p^{2u}A(X))$. Expanding the left hand side, we obtain

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

Put $Q_5(X) := (1 - p^{2u}B(X))\,Q_4(X)$. Since $(1+p^{2u}B)(1-p^{2u}B) \equiv 1 \bmod p^v$, the right hand side of (2.2) is

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

Hence we can take Q_5 as Q_2.

(b): Let Y be an indeterminate. Put $r_0 := p^{-u-t}(U - fQ_0)$ and $r_1 := p^{-t}\partial U$. Replacing Q_0 if necessary, we may assume $\deg_X r_0(X) < \deg_X f(X)$ without loss of generality. That is, we may assume $r_0 = p^{-u-t}(U \bmod f)$. Then,

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

Since $p \neq 2$, we see $\mathrm{ord}_p\left(\frac{p^{2u}}{2}\partial^2 U(X)\right) \geq 2u+t$. Regarding the last term, the fact that $\frac{\partial^i U(X)}{i!} \in R[X]$ implies that $\mathrm{ord}_p\left(\frac{p^{iu}}{i!}Y^i\partial^i U(X)\right) \geq 3u$. Therefore,

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

By (iii), there exist $A(X)$, $B(X) \in R[X]$ satisfying

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

Therefore,

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

Setting X to be $X+p^uB(X)$ and Y to be $-B(X)$ in (2.3), we obtain

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

with $Q_6(X) := Q_0(X+p^uB(X)) + p^{u+t}A(X+p^uB(X))$. Obviously, we have

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

By (a), there exists $Q_7 \in R[X]$ satisfying

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

Define Q_8, $r_2 \in K[X]$ by $B\partial f = Q_8 f + r_2$ with $\deg r_2 < \deg f$. Then Q_8 and r_2 belong to $R[X]$ by (i). Since

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

we see

$$U \equiv (f + p^u r_2 + p^{2u} Q_9) Q_{10} \bmod p^v$$

where $Q_9 := Q_8^2 f - Q_8 B \partial f \quad (= - Q_8 r_2)$. and $Q_{10} := (1 + p^u Q_8) Q_7$. Put $g := f + p^u r_2$. Then g is monic and $g \equiv f \bmod p^{2u}$. The existence of Q_3 for this g follows from (a). The assertion on the computational complexity is clear. $\square$

Lemma 2.2. *Let p be a prime and $U \in R[X]$ and $\{a_n \in \mathbf{N}\}_{n=1}^{\infty}$ a strictly increasing sequence. Let $\{h_n \in R[X]\}_{n=1}^{\infty}$ be a sequence of monic polynomials for which the following conditions hold.*

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

(ii) *For each n, there exists $S_n \in R[X]$ such that* $\mathrm{ord}_p(U - h_n S_n) \geq a_n$.

(iii) $\pi(h_0)$ is square free.

Then, $h := \lim_{n \to \infty} h_n \in R[X]$ exists and $\deg h = \deg h_n$ (for all n). All the zeros of h lie in R^{ur} and they are zeros of U. In particular, h is a factor of U.

Proof. Since $R[[X]]$ is complete with respect to the p-adic valuation, $\lim_{n \to \infty} h_n$ exists in $R[[X]]$ by (i). Moreover, (i) together with the fact that h_n is monic implies $\deg h_n = \deg h_1$ for all $n \geq 1$. Therefore, h belongs in fact to $R[X]$ and $\deg h = \deg h_n$ for all $n \geq 1$. Let θ be a root of $h(X) = 0$. Since $\pi(h) = \pi(h_0)$ is square free, $\theta \in R^{\mathrm{ur}}$. It remains to show $U(\theta) = 0$. Using

$$U = (U - h_n S_n) + (h_n - h) S_n + h S_n,$$

we see $\mathrm{ord}_p U(\theta) \geq a_n$. This holds for any n, so $U(\theta) = 0$. $\square$

3. Construction of the Canonical Lifting

Let E be an elliptic curve over $\mathbf{F}_q$ with $j(E) \notin \mathbf{F}_{p^2}$. In this section, we develop a fast algorithm to construct an elliptic curve which is p-adically close enough to the canonical lift of E. Voloch and Walker[22] studied an algorithm to construct canonical lifts $\bmod p^2$. Although our algorithm needs more time to construct the $\bmod p^2$ lift than Voloch and Walker's algorithm, ours can construct the canonical model $\bmod p^m$ for an arbitrary m. Using these results, we lift $E[p]$ to R^{ur}-valued points of the canonical lift of E.

Let k be a field, S a subring of the algebraic closure of k. For an elliptic curve $E: Y^2 = X^3 + AX + B$ defined over k, we put

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

Note that if S is not a field, $E(S)$ is not a group in general. We use $\tau(X, Y) := -X/Y$ as a local parameter at $\mathscr{O}$. The group of n-torsion points is denoted by $E[n]$. For $\mathscr{P} \subset E$, we denote by $k(\mathscr{P})$ the extension field of k generated by coordinates of all the points belonging to $\mathscr{P} - \{\mathscr{O}\}$.

Let $\Psi_p(X, \alpha, \beta) \in \mathbf{Z}[X, \alpha, \beta]$ be the p-th division polynomial where α and β are indeterminates. Thus, $P := (x, y) \in E - \{\mathscr{O}\}$ belongs to $E[p]$ if and only if $\Psi_p(x, A, B) = 0$. There exist φ_p and $\Omega_p \in \mathbf{Z}[X, \alpha, \beta]$ such that

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

for $P \notin E[p]$ and that $\Psi_p(X, A, B)$ is prime to $\varphi_p(X, A, B)$ in $k[X]$. For the fundamental properties of division polynomials, see Silverman[20, Exercise 3.7]. (Under the condition that p is odd, our Ψ_p and Ω_p are Silverman's ψ_p and $y^{-1}\omega_p$, respectively.)

Now, let $E: Y^2 = X^3 + AX + B$ be an ordinary elliptic curve over $\mathbf{F}_q$ satisfying $AB \neq 0$ and $\widetilde{E}: Y^2 = X^3 + \widetilde{A}X + \widetilde{B}$ its lifting to K.

Theorem 3.1. *Let E and $\widetilde{E}$ as above. The following conditions (i)-(iv) are equivalent.*

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

(ii) *There exists* $P \in \widetilde{E}(R^{\mathrm{ur}}) - \{\mathscr{O}\}$ *such that* $\tau(pP) \in p^2 R^{\mathrm{ur}}$.

(iii) *There exists* $P := (x, y) \in \widetilde{E}(R^{\mathrm{ur}}) - \{\mathscr{O}\}$ *such that* $\Psi_p(x, \widetilde{A}, \widetilde{B}) \equiv 0 \bmod p^2$.

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

Proof. The proof is similar to [17, Cor. 3.4] and [18, Th. 3.7] however, since this theorem is crucial to our method, we recall it here.

(i)$\to$(ii),(iii): trivial. (ii)$\to$(i): By assumption, there exists $Q \in \widetilde{E}(K^{\mathrm{ur}}) \cap \mathrm{Ker}\,\pi$ satisfying $\tau(Q) = \frac{1}{p}\tau(pP) \in pR^{\mathrm{ur}}$. Since $\tau: \mathrm{Ker}\,\pi \cap \widetilde{E}(K^{\mathrm{ur}}) \to pR^{\mathrm{ur}}$ is an isomorphism (Silverman[20, Th. IV.6.3]), we obtain $P - Q \in \widetilde{E}[p] \cap \widetilde{E}(R^{\mathrm{ur}})$. (iii)$\to$(ii): In the case where $pP = \mathcal{O}$, there is nothing more to prove. Otherwise, put $(x', y') := pP$. By assumption (iii), $\varphi_p(x, \widetilde{A}, \widetilde{B}) \not\equiv 0 \bmod p$ (otherwise, $\varphi_p(X, A, B)$ is not prime to $\Psi_p(X, A, B)$ over $\mathbf{F}_q[X]$, which is a contradiction). Therefore

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

and $\mathrm{ord}_p y' = \frac{3}{2} \mathrm{ord}_p x'$. Hence $\tau(pP) = -x'/y' \equiv 0 \bmod p^2$.

(i)→(iv): Let $H := \widetilde{E}[p] \cap \widetilde{E}(R^{\mathrm{ur}})$. Since p is a prime, H is a cyclic group of order p. Let $G := \widetilde{E}[p] \cap \mathrm{Ker}\,\pi$. Since $\widetilde{E}[p] \to E[p]$ cannot be injective, G is nontrivial. So, G is also a cyclic group of order p. Therefore, $\widetilde{E}[p] = H \oplus G$ as a group. It follows that $K(G) = K(\xi(Q), \eta(Q))$ where Q is an any point in $G - \{\mathcal{O}\}$. Note both G and H are defined over K. In particular, the number of conjugates of $\xi(Q)$ cannot exceeds the number of X-coordinates of points of $G - \{\mathcal{O}\}$. Hence

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

On the other hand $K(H)/K$ is unramified. Thus, $K(\widetilde{E}[p])$ is tamely ramified over K. This yields (iv) by the main result of Nakamura[16].

(iv)→(iii): First we show $E^{\uparrow}[p] \cap E^{\uparrow}(R^{\mathrm{ur}}) \neq \{\mathcal{O}\}$. Let V_p be the Verschiebung of E and let $V_p^{\uparrow} \in \mathrm{End}(E^{\uparrow})$ be its lift to $\mathrm{End}(E^{\uparrow})$. Since V_p is separable, $\pi(\mathrm{Ker}\, V_p^{\uparrow}) = \mathrm{Ker}\, V_p = E[p]$. This implies the reduction modulo p of $\prod_{P \in (\mathrm{Ker}\, V_p^{\uparrow} - \{\mathcal{O}\})/\pm 1} (X - \xi(P)) \in R[X]$ is square free. Thus $\xi(P) \in R^{\mathrm{ur}}$ for $P \in \mathrm{Ker}\, V_p^{\uparrow} - \{\mathcal{O}\}$ by Lang[11, Prop. II.4.7]. Since p is odd, $\mathrm{ord}_p \eta(P) = 0$. This together with $\eta(P)^2 \in R^{\mathrm{ur}}$ yields $\eta(P) \in R^{\mathrm{ur}}$. Hence (i) holds when $\widetilde{E} = E^{\uparrow}$, and so does (iii). Next, let $Y^2 = X^3 + A^{\uparrow} X + B^{\uparrow}$ be a Weierstrass model of $E^{\uparrow}$. Then $j(\widetilde{E}) \equiv j(E^{\uparrow}) \bmod p^2$ implies $\widetilde{A} \equiv u^2 A^{\uparrow} \bmod p^2$ and $\widetilde{B} \equiv u^3 B^{\uparrow} \bmod p^2$ where $u := \dfrac{\widetilde{A} B^{\uparrow}}{A^{\uparrow} \widetilde{B}} \in R^{\times}$. (Note $\widetilde{A}$, $\widetilde{B}$, $A^{\uparrow}$ and $B^{\uparrow}$ belong to $R^{\times}$.) Since validity of (iii) depends only on $\widetilde{A} \bmod p^2$ and $\widetilde{B} \bmod p^2$, we see (iii) also holds for $\widetilde{E}$. □

Remark 3.2. According to [16], the above mentioned theorem is due to Serre's unpublished work, where the proof uses a local Serre-Tate parameter. However, Nakamura's proof is fairly elementary (and published).

From now on, Φ_p is the p-th modular polynomial. So far we did not use assumption $j(E) \notin \mathbf{F}_{p^2}$. The next proposition, which is a reason of this restriction, should be hold with minor modification for any ordinary j other than $0, 1728$. However, $\Phi_p \bmod p^n$ for $n \geq 2$ is somewhat complicated. See Koike[10, Prop. 1] for the case $n = 2$. Our method is implicit in Lubin-Serre-Tate[13, Sect. 8] however we focus on optimizing the performance of the algorithm.

Proposition 3.3. *Let $m \in \mathbf{N}$. Let $z_0, \ldots, z_{N-1} \in R$ be such that*
(i) $z_i \equiv z_{i+1}^p \bmod p$,
(ii) $\pi(z_i) \notin \mathbf{F}_{p^2}$, *and*
(iii) $\Phi_p(z_i, z_{i+1}) \equiv 0 \bmod p^m$
for all $0 \leq i < N$. Here, we understand $z_N = z_0$. Then there exist $\zeta_0, \ldots, \zeta_{N-1} \in R$, unique up to modulo p^{2m} satisfying conditions for all $0 \leq i < N$ (again we understand $\zeta_N = \zeta_0$):
(a) $\zeta_i \equiv z_i \bmod p^m$,
(b) $\Phi_p(\zeta_i, \zeta_{i+1}) \equiv 0 \bmod p^{2m}$
Moreover (once $\Phi_p \bmod p^{2m}$ is computed), we obtain $\zeta_i \bmod p^{2m}$ for all $0 \leq i < N$ with $O(N)$ arithmetic operations over $R \bmod p^{2m}$.

Proof. Recall the Kronecker relation

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

Therefore, by (i), we see

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

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

Define $\mathscr{F} \in \mathrm{Map}(R^N, R^N)$ by

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

Let $z := {}^t(z_0 \ \ldots \ z_{N-1})$. For $\delta \in R^N$,

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

where

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

By (3.1) and (3.2), $(D\mathscr{F})(z) \bmod p$ is a diagonal matrix and its diagonal entries are non-zero by (ii). Thus $\det(D\mathscr{F})(z) \in R^\times$ and letting $\delta := -p^{-m}(D\mathscr{F})(z)^{-1}\mathscr{F}(z)$, we see that $\delta \in R^N$ by (iii). Then, we can take ${}^t(\zeta_0 \ \ldots \ \zeta_{N-1}) := z + p^m\delta$. In fact, (a) follows from $\delta \in R^N$ and (b) follows from (3.3) and the definitions of ζ_i and δ. Uniqueness is also trivial by the regularity of $(D\mathscr{F})(z)$.

As to the computational complexity, $O(p^2N)$ arithmetic over $R \bmod p^{2m}$ is sufficient to compute $\mathscr{F}(z)$ and the non-zero entries of $(D\mathscr{F})(z)$. A further $2N$ row operations (i.e. $O(N)$ arithmetic operations) yields $(D\mathscr{F})(z)^{-1}\mathscr{F}(z)$. One more subtraction in $(R \bmod p^{2m})^N$ is necessary, which is clearly done with N subtractions in $R \bmod p^{2m}$. $\square$

Corollary 3.4. *Let E be an elliptic curve satisfying $j(E) \notin \mathbf{F}_{p^2}$. Denote $\mathrm{Fr}_p^i E$ by $E^{(i)}$ and its canonical lift by $E^{(i)\uparrow}$. Let $\{a_n \in \mathbf{N}\}_{n=0}^\infty$ be a strictly increasing sequence with $a_0 = 1$. For $0 \le i < N$ and $n \ge 0$, assume $z_{i,n} \in R$ satisfy following conditions: (We understand $z_{N,n} = z_{0,n}$.)*

(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) $\boldsymbol{\Phi}_p(z_{i,n}, z_{i+1,n}) \equiv 0 \bmod p^{a_n}$.

Then $z_i := \lim_{n\to\infty} z_{i,n}$ exists and we have $z_i = j(E^{(i)\uparrow})$ for each $0 \le i < N$. Moreover $z_{i,n} \equiv j(E^{(i)\uparrow}) \bmod p^{a_n}$ for all $n \ge 0$.

Proof. By a similar argument to the proof of the preceding proposition, the system of equations

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

has at most one solution under the condition $j(E)\notin \mathbf{F}_{p^2}$. Since $E^{(i)\uparrow}$ and $E^{(i+1)\uparrow}$ are p-isogenous, $(j(E^{(0)\uparrow}),\ldots,j(E^{(N-1)\uparrow}))$ is a solution of (3.4). On the other hand, $\{z_{n,i}\}_{n=1}^{\infty}$ is a Cauchy sequence by (ii) and $(z_1,\ldots,z_{N-1})$ is a solution of (3.4) by (iii). By the uniqueness of the solution it follows that $z_i=j(E^{(i)\uparrow})$. The last assertion follows easily from properties of a non-Archimedean valuation. □

Remark 3.5. In actual computation, we use a sparse matrix representation (or simply use two one-dimensional arrays of size N) for $(D\mathscr{F})(z)$. Even if this technique is adopted, the space requirement is $O(N^3)$ which is still considerably huge. It would be desirable to reduce the space requirement to $O(N^2)$. This could be achieved by using the Galois action as follows. Take $\omega\in R$ such that $K=\mathbf{Q}_p(\omega)$ and let $\sigma\in \mathrm{Gal}(K/\mathbf{Q}_p)$ be the Frobenius substitution. One may try to solve $\varPhi_p(x,\sigma x)=0$ as an equation with respect to $x_0,\ \ldots,\ x_{N-1}\in\mathbf{Q}_p$ where $x=\sum_{i=0}^{N-1}x_i\omega^i$. However, instead of $(D\mathscr{F})(z)$, we may obtain a dense matrix of size N whose inversion may need much more time.

Remark 3.6. Let $M\in\mathbf{N}$ and assume we need $j(E^{\uparrow}) \bmod p^M$. In this case, we proceed as follows:

- Put $\nu:=[\log_2(M-1)]+1$, $a_n:=[2^{-(\nu-n)}M]$ for $0\le n\le \nu$.
- Put $z_{i,0}:=j(E^{(i)})\in\mathbf{F}_q=R/pR$ for $0\le i\le N-1$.
- For $n:=1\sim\nu$, compute $z_{i,n}\in R/p^{a_n}R$ for $0\le i<N$ from $z_{i,n-1}$ such that $z_{i,n}\equiv z_{i,n-1} \bmod p^{a_{n-1}}$ and $\varPhi_p(z_{i,n},z_{i+1,n})\equiv 0 \bmod p^{a_n}$ by Proposition 3.3.

Then $z_{0,\nu}$ gives the desired value. This runs much faster than the naive quadratic lift over R/p^MR because the smaller m is, the faster we can perform arithmetic operations over R/p^mR.

Lemma 3.7. *Assume $\widetilde{E}\colon Y^2=X^3+\widetilde{A}X+\widetilde{B}$ satisfies one of conditions (i)-(iv) in Theorem 3.1. Then, for any $P\in\widetilde{E}[p]\cap\widetilde{E}(R^{\mathrm{ur}})-\{\mathscr{O}\}$, we have*

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

where $\partial=d/dX$.

Proof. Let $Q\in\widetilde{E}[p]\cap\mathrm{Ker}\,\pi-\{\mathscr{O}\}$. Then P and Q generate $\widetilde{E}[p]\cap\widetilde{E}(R^{\mathrm{ur}})$ and $\widetilde{E}[p]\cap\mathrm{Ker}\,\pi$, respectively. Therefore the p-th division polynomial factors as

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

in the algebraic closure of K (see e.g. Cassels[2, Formulary, (I)] or Silverman[20, Exer. 3.7(b)]). Hence

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

Let $\tau:=-\xi/\eta$ be the local parameter at $\mathcal{O}$ and put $t_j:=\tau(jQ)$. Using

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

we have

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

Recall that p is odd and that $P\in\widetilde{E}[p]\cap\widetilde{E}(R^{\mathrm{ur}})$. This implies $\mathrm{ord}_p(\eta(iP))=0$ for $1\le i\le p-1$. On the other hand, $\mathrm{ord}_p(\xi(iP)-\xi(jP))=0$ for $1\le i<j\le(p-1)/2$. Therefore,

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

Because $t_j=-t_{p-j}$ for $1\le j\le p-1$ we have

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

□

Theorem 3.8. *Let $E/\mathbf{F}_q$ be an elliptic curve with $j(E)\notin\mathbf{F}_{p^2}$ given by the Weierstrass equation $Y^2=X^3+AX+B$. Let $E^{(i)}$ be its conjugate over $\mathbf{F}_p$ defined by $Y^2=X^3+(\mathrm{Fr}_p^iA)X+\mathrm{Fr}_p^iB$. Let $M\ge 2$ be an integer. Then there is an algorithm to produce the following: For all $0\le i<N$,*

- *An elliptic curve* $E^{\langle\langle i\rangle\rangle}: Y^2 = X^3 + A^{\langle\langle i\rangle\rangle}X + B^{\langle\langle i\rangle\rangle}$.
- *A polynomial* $h^{\langle\langle i\rangle\rangle} \in R[X]$ *such that*

$$h^{\langle\langle i\rangle\rangle}(X) \equiv \left(\prod_{P \in (G^{\langle\langle i\rangle\rangle} - \{\mathcal{O}\})/\pm 1} (X - \xi(P))\right) \bmod p^{M-1}$$

where $G^{\langle\langle i\rangle\rangle} := E^{\langle\langle i\rangle\rangle}[p] \cap E^{\langle\langle i\rangle\rangle}(R^{\mathrm{ur}})$.

which satisfy the following conditions:

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

(ii) The group $G^{\langle\langle i\rangle\rangle}$ *is a cyclic group of order* p *whose reduction modulo* p *is* $E^{(i)}[p]$.

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

The algorithm requires $O(N \log M)$ *operations over* $R \bmod p^M$ *and* $O(N^2)$ *operations over* $\mathbf{F}_q$. *(Here and during the proof, O-constants depends on p.)*

Proof. First we compute $A^{(i)} := \mathrm{Fr}_p^i A$ and $B^{(i)} := \mathrm{Fr}_p^i B$, which are obtained with $O(N)$ multiplications over $\mathbf{F}_q$. Take $z_i \in R$ so that $\pi(z_i) = j(E^{(N-i)})$. By the $O(\log M)$ times repeated use of Proposition 3.3, we have $\zeta_i \in R$ satisfying $\Phi_p(\zeta_i, \zeta_{i+1}) \equiv 0 \bmod p^M$ and $\pi(\zeta_i) = j(E^{(N-i)})$ with $O(N \log M)$ operations over $R \bmod p^M$. Take $A^{\langle\langle i\rangle\rangle}$, $B^{\langle\langle i\rangle\rangle} \in R$ satisfying $\pi(A^{\langle\langle i\rangle\rangle}) = A^{(i)}$, $\pi(B^{\langle\langle i\rangle\rangle}) = B^{(i)}$ and $j(E^{\langle\langle i\rangle\rangle}) = \zeta_{N-i}$. This is possible and in fact can be done in $O(N \log M)$ operations since $\dfrac{\partial j}{\partial A}(A^{(i)}, B^{(i)}) \neq 0$ in $\mathbf{F}_q$. This also implies (iii). On the other hand, $\Phi_p(j(E^{(N-i)\uparrow}), j(E^{(N-i+1)\uparrow})) = 0$ and $\pi(j(E^{(N-i)\uparrow})) = j(E^{(N-i)})$. By Corollary 3.4 we have (i). Then Theorem 3.1(iv)$\to$(i) proves that condition (ii) holds. To obtain $h^{\langle\langle i\rangle\rangle}$, we investigate the p-th division polynomial Ψ_p. Note that $\pi(\Psi_p(X, A^{\langle\langle i\rangle\rangle}, B^{\langle\langle i\rangle\rangle}))$ factors as $cf(X)^p$ with *monic square free* $f \in \mathbf{F}_q[X]$ and $c \in \mathbf{F}_q^{\times}$. Cf. Cassels[1, Theorem I]. Actually, $f(X) = \sum_{k=0}^{(p-1)/2} \dfrac{u_k}{u_{(p-1)/2}} X^k$ where u_k is the coefficient of X^{pk} in $\Psi_p(X, A^{(i-1)}, B^{(i-1)})$. Anyway, $\mathrm{ord}_p(\partial \Psi_p)(X, A^{\langle\langle i\rangle\rangle}, B^{\langle\langle i\rangle\rangle}) \geq 1$. On the other hand, $E^{\langle\langle i\rangle\rangle}$ satisfies condition (iv) of Theorem 3.1. Applying Lemma 3.7, we see that $\mathrm{ord}_p(\partial \Psi_p)(X, A^{\langle\langle i\rangle\rangle}, B^{\langle\langle i\rangle\rangle}) = 1$ and that f is prime to $\pi\left(\frac{1}{p}(\partial \Psi_p)(X, A^{\langle\langle i\rangle\rangle}, B^{\langle\langle i\rangle\rangle})\right)$. Thus we can use Lemma 2.1 repeatedly with $U(X) := \Psi_p(X, A^{\langle\langle i\rangle\rangle}, B^{\langle\langle i\rangle\rangle})$, $t := 1$, and initially $u := 1$. By Lemma 2.2, we obtain a monic factor $h(X)$ of $\Psi_p(X, A^{\langle\langle i\rangle\rangle}, B^{\langle\langle i\rangle\rangle})$. Note that roots of $\Psi_p(X, A^{\langle\langle i\rangle\rangle}, B^{\langle\langle i\rangle\rangle})$ in R^{ur} are X-coordinates of points of $G^{\langle\langle i\rangle\rangle}$. Since h has $(p-1)/2$ distinct roots in R^{ur}, we conclude that $h = h^{\langle\langle i\rangle\rangle}$. Hence $O(\log M)$ applications of Lemma 2.1 is enough to obtain $h^{\langle\langle i\rangle\rangle} \bmod p^{M-1}$. This amounts to $O(\log M)$ arithmetic operations over $R \bmod p^M$ for each i. $\square$

Remark 3.9. In the case of $p=2$, we cannot use Lemma 2.1 since a $p=2$ version of Lemma 3.7 no longer holds. This is the most serious obstacle when we apply our method to the case $p=2$. We sketch how to avoid this difficulty. Let $M \geq 3$. Let R be the valuation ring of a degree N unramified extension field of $\mathbf{Q}_2$. For $\tilde{a}_2 \in R$ and $\tilde{a}_6 \in R^\times$, define $\tilde{E}/R$ by

$$\tilde{E} : Y^2 + XY \ = \ X^3 + \tilde{a}_2 X^2 + \tilde{a}_6.$$

We denote its reduction $\tilde{E} \bmod 2$ by E. Put $U(X) := 4X^3 + (1+4\tilde{a}_2)X^2 + 4\tilde{a}_6$. Then an X-coordinate of a point in $\tilde{E}[2] - \{\mathcal{O}\}$ is a root of U. Assume $(x, y) \in \tilde{E}[2] \cap \tilde{E}(R^{\mathrm{ur}}) - \{\mathcal{O}\}$. Then $\mathrm{ord}_2 x = 1$ and such a point exists if and only if $-\dfrac{\tilde{a}_6}{1+4\tilde{a}_2}$ is a square in R. This condition depends only on $\tilde{a}_2 \bmod 2$ and $\tilde{a}_6 \bmod 8$. Since $j(\tilde{E}) \equiv -1/\tilde{a}_6 \bmod 8$, we can choose $\tilde{a}_6$ so that $j(\tilde{E}) \equiv j(E^\uparrow) \bmod p^{M+2}$. Then $\tilde{E}[2] \cap \tilde{E}(R^{\mathrm{ur}}) \neq \{\mathcal{O}\}$ and we obtain $x \bmod 8$ with $O(1)$ arithmetic operations over $R/8R$ and a probabilistic factoring algorithm over $\mathbf{F}_{2^N}[X]$. Note we have only to lift one point (i.e. the unique non-trivial 2-torsion point of E). Therefore, once we have computed $j(E^\uparrow) \bmod 2^{M+2}$, we can obtain $\tilde{a}_6 \bmod 2^{M+2}$ and $x \bmod 2^M$ with $O(N \log M)$ arithmetic operations over $R/2^{M+2}R$ by Newton's iterated root finding algorithm.

4. Application to Point Counting

In this section, we state our point counting algorithm. Let E be an elliptic curve over $\mathbf{F}_q$. In Proposition 4.2, we observe that the case $j(E) \in \mathbf{F}_{p^2}$ is easily handled and so we may assume $j(E) \notin \mathbf{F}_{p^2}$. Under this condition, we can apply Theorem 3.8 to E. We compute the leading coefficient of Verschiebung on the formal group of the canonical lift of E, which yields the trace of Verschiebung. We begin with a simple observation on an endomorphism of a formal group induced by an endomorphism of an elliptic curve. This may be known however the author could not find a proof in the literature.

Proposition 4.1. *Let $\mathcal{E}/K$ be an elliptic curve and let $f \in \mathrm{End}_K(\mathcal{E})$ be of degree d. We denote its local parameter at $\mathcal{O}$ by τ. Assume that the reduction $\pi(f)$ of f*

modulo p *is separable and that* $f(\mathrm{Ker}\pi)\subset\mathrm{Ker}\pi$. *Let* $\widehat{f}$ *be the homomorphism induced from* f *over the formal group* $\widehat{\mathscr{E}}$ *of* $\mathscr{E}$. *Then,*

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

where $\widehat{f}(\tau)=\sum_{n=1}^{\infty} c_n\tau^n$.

Proof. Since f satisfies $f\circ f-\mathrm{Tr}(f)f+d=0$ in $\mathrm{End}(\mathscr{E})$ we have

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

on $\widehat{\mathscr{E}}$, and hence the coefficient of τ must vanish. On the other hand, separability of $\pi(f)$ implies $\pi(c_1)\neq 0$ hence $c_1\neq 0$. Cf. the proof of case 2 of Silverman[20, Cor. IV.7.5]. Therefore, (4.1) holds. □

Proposition 4.2. *Let* $q:=p^N$ *and let* $E: Y^2=X^3+AX+B$ *be an elliptic curve over* $\mathbf{F}_q$. *Assume* $j(E)\in\mathbf{F}_{p^2}$. *Then* $^{\#}E(\mathbf{F}_q)$ *is determined with* $O(N)$ *arithmetic operations over* $\mathbf{F}_q$ *and* $O(N^{1+\mu})$ *bit operations.*

Proof. Define $m\in\mathbf{N}$ so that $p^m={}^{\#}\mathbf{F}_p(j(E))$. By the assumption $j(E)\in\mathbf{F}_{p^2}$, we see either $m=1$ or $m=2$. There exists an elliptic curve $E': Y^2=X^3+A'X+B'$ defined over $\mathbf{F}_{p^m}$ which is isomorphic to E over $\mathbf{F}_q$. We can obtain such E' as follows. Note we can determine whether E is isomorphic to E' over $\mathbf{F}_q$ with $O(N)$ arithmetic operations over $\mathbf{F}_q$. For example, in case of $AB\neq 0$, we check whether $j(E)=j(E')$ and $\left(\dfrac{A/B}{A'/B'}\right)^{(q-1)/2}=1$. The remaining cases are similar. Let $E_0/\mathbf{F}_{p^m}$ be any elliptic curve satisfying $j(E_0)=j(E)$, which can be constructed with $O(1)$ operations over $\mathbf{F}_{p^m}$ (see e.g. the proof of Silverman[20, Prop. III.1.4(c)]). We can take E_0 as E' when E_0 is isomorphic to E over $\mathbf{F}_q$. Otherwise, we take the twist of E_0 over $\mathbf{F}_{p^m}$ as E', which is again constructed in $O(1)$. It is obvious that $^{\#}E(\mathbf{F}_q)={}^{\#}E'(\mathbf{F}_q)$. Therefore, it is enough to obtain $T_{N/m}$ where $T_i:=\mathrm{Tr}\,\mathrm{Fr}^i_{p^m}|_{E'}$. (Note m always divides N.) The value T_1 $(=1+p^m-{}^{\#}E'(\mathbf{F}_{p^m}))$ is obtained by $O(1)$ (with respect to N) arithmetic operations over $\mathbf{F}_{p^m}$ (say via exhaustive search). We obtain $T_{N/m}$ by the relation $T_{i+2}-T_1T_{i+1}+p^mT_i=0$ with $T_0=2$. Using $|T_i|\leq 2p^{im/2}$ we see that $O(N^{1+\mu})$ bit operation is sufficient for computing $T_{N/m}$ from T_1. □

In what follows, we assume $j(E) \notin \mathbf{F}_{p^2}$. We use same the notation as in Theorem 3.8. Moreover, let $E^{(i)\uparrow}$ be the canonical lift of $E^{(i)}$. Without loss of generality, we may assume $E^{(i)\uparrow}$ is given by $Y^2 = X^3 + A^{(i)\uparrow}X + B^{\langle\langle i\rangle\rangle}$ with some $A^{(i)\uparrow} \in R$. For notational convenience, we put $B^{(i)\uparrow} := B^{\langle\langle i\rangle\rangle}$. Let $G^{(i)} := E^{(i)\uparrow}[p] \cap E^{(i)\uparrow}(R^{\mathrm{ur}})$ which is a cyclic group of order p.

Let $V_p^{(i)}$ be the dual isogeny of $\mathrm{Fr}_p \in \mathrm{Isog}(E^{(i-1)}, E^{(i)})$. Recall that $V_p^{(i)}$ can be lifted to $V_p^{(i)\uparrow} \in \mathrm{Isog}(E^{(i)\uparrow}, E^{(i-1)\uparrow})$ by Messing[14, Corollary V.3.4]. We investigate how it looks on the formal groups.

Proposition 4.3. *Let $\tau_i(X, Y) := -X/Y$ be the local parameter of $E^{(i)\uparrow}$ at $\mathcal{O}$. Assume $A^{(i)\uparrow}$, $B^{(i)\uparrow}$ and*

$$h^{(i)\uparrow}(X) \;:=\; \prod_{g \in (G^{(i)} - \{\mathcal{O}\})/\pm 1} (X - \xi(g))$$

are given. Define $c_1^{(i)} \in R$ by

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

Then we can obtain the value of $c_1^{(i)2}$ with $O(1)$ arithmetic operations over R.

Proof. Since $V_p^{(i)\uparrow}$ is a lifting of $V_p^{(i)}$, the rectangle in the following diagram is commutative.

$$\begin{tikzcd}
E^{(i)\uparrow} \arrow[rr, "V_p^{(i)\uparrow}"] \arrow[dr, "v"] \arrow[dd, "\pi"'] & & E^{(i-1)\uparrow} \arrow[dd, "\pi"] \\
& E^{(i)\uparrow}/G^{(i)} \arrow[ur, dashed, "\lambda"'] & \\
E^{(i)} \arrow[rr, "V_p^{(i)}"] & & E^{(i-1)}
\end{tikzcd}$$

Let $v \in \mathrm{Isog}(E^{(i)\uparrow}, E^{(i)\uparrow}/G^{(i)})$ be the isogeny constructed by Vélu[21]. Explicitly,

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

where the plus sign in $(X, Y) + g$ is the curve addition. Vélu's formula also gives the Weierstrass model of $E^{(i)\uparrow}/G^{(i)}$. Let s_i be the coefficient of $X^{((p-1)/2)-i}$ in $h^{(i)\uparrow}$. Then $E^{(i)\uparrow}/G^{(i)}$ is $Y^2 = X^3 + \alpha_i X + \beta_i$ with

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

where we understand $s_3 = 0$ for $p = 5$. Since $\operatorname{Ker} v = \operatorname{Ker} V_p^{(i)\uparrow} = G^{(i)}$, there is a $\lambda \in \operatorname{Isog}(E^{(i)\uparrow}/G^{(i)}, E^{(i-1)\uparrow})$ which makes the triangle in the above diagram commutative by Silverman[20, Cor. III.4.11]. But $\deg(V_p^{(i)\uparrow}) = \deg(v)\deg(\lambda)$ implies that λ is an isomorphism. Hence λ is given by

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

with some $\gamma_i \in R$. The map v induces a homomorphism $\widehat{v}$ between formal groups with leading coefficient 1 by Vélu[21, (13)], whereas $\widehat{\lambda}(t) = t/\gamma_i$. By composition, we see $c_1^{(i)} = 1/\gamma_i$. Looking at coefficients of Weierstrass model, we have $B^{(i-1)\uparrow} = \beta_i \gamma_i^6$ and $A^{(i-1)\uparrow} = \alpha_i \gamma_i^4$, and thus $c_1^{(i)2} = \gamma_i^{-2} = \dfrac{\beta_i/\alpha_i}{B^{(i-1)\uparrow}/A^{(i-1)\uparrow}}$. □

Theorem 4.4. *Let $q := p^N$ and let $E/\mathbf{F}_q$ be an elliptic curve with $j(E) \notin \mathbf{F}_{p^2}$. There exists an algorithm to determine $^{\#}E(\mathbf{F}_q)$ whose time complexity is $O(N \log N)$ operations over $R \bmod p^N$ and $O(N)$ operations over $\mathbf{F}_q$.*

Proof. Let $c_1^{(i)}$ be as in Proposition 4.3. Then,

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

by (4.1) where $c := \prod_{i=0}^{N-1} c_1^{(i)}$. However, $|\operatorname{Tr}\mathrm{Fr}_q| \le 2\sqrt{q}$. So, $c \bmod p^{N/2+\alpha}$ ($\alpha := 3$, say) is enough to obtain $\operatorname{Tr}\mathrm{Fr}_q$. Hence instead of $A^{(i)\uparrow}$ and $h^{(i)\uparrow}$ we can use $A^{\langle\langle i\rangle\rangle}$ and $h^{\langle\langle i\rangle\rangle}$ given by Theorem 3.8 with $M := N/2 + \alpha + 1$. Computation of $A^{\langle\langle i\rangle\rangle}$ and $h^{\langle\langle i\rangle\rangle}$ requires $O(N \log M)$ operations. By Proposition 4.3, we obtain c^2 with $O(N)$ operations. On the other hand, let C_1 be the coefficient of X^{p-1} in $(X^3 + AX + B)^{(p-1)/2} \in \mathbf{F}_q[X]$ and define C_n for $n \ge 2$ by

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

Then as is shown in the proof of Silverman[20, Theorem V.4.1], $C_N \equiv c \bmod p$.

Clearly C_N is computed in $O(N)$ operations over $\mathbf{F}_q$. Thus, we obtain $c \bmod p^M$ from C_N and $c^2 \bmod p^M$ with $O(\log N)$ operations over $R/p^M R$. Let v be the unique integer satisfying $|v| \le 2\sqrt{q}$ and $v \equiv c \bmod p^M$. Then, as is well known, ${}^{\#}E(\mathbf{F}_q)$ is given by $q+1-v$. $\square$

Remark 4.5. One arithmetic operation over $R \bmod p^N$ amounts to $O(N^{2\mu})$ bit operations and one arithmetic operation over $\mathbf{F}_q$ amounts to $O(N^{\mu})$ bit operations. Adopting the device stated in Remark 3.6, we see in fact our algorithm runs within $O(N^{2\mu+1})$ bit operations. In practice, Karatusba method may be applicable. In this case, $2\mu+1 = 4.1699\ldots$.

Remark 4.6. In order to obtain c^2, one may be tempted to compute $N_{K/\mathbf{Q}_p}(c_1^{(0)2})$ instead of $\prod_{i=0}^{N-1} c_1^{(i)2}$. However, the norm computation is not so fast. Let $\sigma \in \mathrm{Gal}(K/\mathbf{Q}_p)$ be the Frobenius substitution. As far as the author knows, evaluation of $\sigma(x)$ for $x \in R/qR$ needs $O(N)$ operations over R/qR with $O(N^2)$ precomputation. Such a method is clearly inefficient. A better method is to compute the determinant of the representation matrix of the multiplication by $c_1^{(0)}$ map with respect to suitable base of $K/\mathbf{Q}_p$. However, this method is still slower than computing $\prod_{i=0}^{N-1} c_1^{(i)}$ at least with the FFT based implementation.

References

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. Lercier, R. and Morain, F.: Computing isogenies between elliptic curves over $\mathbf{F}_{p^n}$ using couveignes's algorithm. Math. Comp. (To apper.)

13. 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

14. 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

15. 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.

16. Nakamura, T.: A note on elliptic curves with ordinary reduction. Arch. Math. **60**, 440-445 (1980)

17. 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)

18. 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.

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

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

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

22. Voloch, J.F. and Walker, J.L.: Euclidean weights of codes from elliptic curves over rings. preprint

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