MATHEMATICS OF COMPUTATION
VOLUME 44, NUMBER 170
APRIL 1985, PAGES 483-494

Elliptic Curves Over Finite Fields and the Computation of Square Roots mod p

By René Schoof

Abstract. In this paper we present a deterministic algorithm to compute the number of $\mathbf{F}_q$-points of an elliptic curve that is defined over a finite field $\mathbf{F}_q$ and which is given by a Weierstrass equation. The algorithm takes $O(\log^9 q)$ elementary operations. As an application we give an algorithm to compute square roots mod p. For fixed $x \in \mathbf{Z}$, it takes $O(\log^9 p)$ elementary operations to compute $\sqrt{x}$ mod p.

1. Introduction. In this paper we present an algorithm to compute the number of $\mathbf{F}_q$-points of an elliptic curve defined over a finite field $\mathbf{F}_q$, which is given by a Weierstrass equation. We restrict ourselves to the case where the characteristic of $\mathbf{F}_q$ is not 2 or 3. The algorithm is deterministic, does not depend on any unproved hypotheses and takes $O(\log^9 q)$ elementary operations (bit operations).

As an application, we give an algorithm to compute the square root of $x \in \mathbf{Z}$ mod p, whenever x is a square mod p. This algorithm is deterministic and for fixed $x \in \mathbf{Z}$ it takes $O(\log^9 p)$ elementary operations; here the O-symbol depends on x; in general, the algorithm takes $O((|x|^{1/2+\varepsilon} \log p)^9)$ elementary operations for any $\varepsilon > 0$. If one applies fast multiplication techniques, the algorithm will take $O((|x|^{1/2} \log p)^{6+\varepsilon})$ elementary operations for any $\varepsilon > 0$.

Let E be an elliptic curve defined over the prime field $\mathbf{F}_p$ and let an affine model of it be given by a Weierstrass equation

$$Y^2 = X^3 + AX + B \quad (A, B \in \mathbf{F}_p).$$

An explicit formula for the number of $\mathbf{F}_p$-points on E is given by

$$\#E(\mathbf{F}_p) = 1 + \sum_{x \bmod p} \left(\left(\frac{x^3 + Ax + B}{p} \right) + 1 \right).$$

Here $(\frac{a}{p})$ denotes the Legendre symbol. Computing $\#E(\mathbf{F}_p)$ by evaluating this sum in a straightforward way takes $O(p^{1+\varepsilon})$ elementary operations; this is the way Lang and Trotter do it in their paper [6]; see also [1], [2]. For small p, this method is practical. Another method which works well in practice, even for primes of moderate size (up to 20 decimal digits say), was suggested to me by Lenstra and is based on an algorithm of Shanks to compute the class groups of complex quadratic orders.

Received November 26, 1983.

1980 *Mathematics Subject Classification*. Primary 12C05, 14G15, 14K07, 68C25.

Key words and phrases. Elliptic curves, finite fields, factorization, polynomials, computational number theory.

© 1985 American Mathematical Society
0025-5718/85 $1.00 + $.25 per page

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use

It runs as follows: one tries to compute a point $P = (x, y)$ in $E(\mathbf{F}_q)$; in practice there is no problem in finding a point P, but I do not know how to prove that computing a point in $E(\mathbf{F}_q)$ is easy. Next, one searches for a number r satisfying $rP = 0$ and $q + 1 - 2\sqrt{q} \leqslant r \leqslant q + 1 + 2\sqrt{q}$. Here we use the—additivity written —group structure on $E(\mathbf{F}_q)$ and the estimate

$$|\#E(\mathbf{F}_q) - (q + 1)| \leqslant 2\sqrt{q};$$

these matters are explained in the next section. The searching for the number r may be done by means of Shanks' baby-step-giant-step techniques. If r is the only number satisfying the conditions above, we have that $\#E(\mathbf{F}_q) = r$. If not, we can easily compute the subgroup generated by P, which is of order $\leqslant 4\sqrt{q}$, and we pick a new point Q and compute an integer r such that $rQ = 0$ as we did before; we determine the group generated by the points P and Q and so on, until the group generated by the points we picked has its order s satisfying $q + 1 - 2\sqrt{q} \leqslant s \leqslant q + 1 + 2\sqrt{q}$; if $q \geqslant 37$, we must have that $\#E(\mathbf{F}_q) = s$. For details concerning these strategies see [10]. The computations in the group $E(\mathbf{F}_q)$ can be done using the addition formulas given in the next section. In practice, this algorithm runs in time $O(q^{1/4})$.

Computing square roots mod p can be done using Berlekamp's probabilistic method to find zeros of polynomials mod p; this algorithm is expected to take $O(\log^3 p)$ elementary operations [4]. Computing $\sqrt{q}$ mod p using the deterministic algorithm given by Shanks in [11] takes $O(\log^4 p)$ elementary operations; however, since in this algorithm one needs a quadratic nonresidue mod p, an unproved hypothesis, viz. the Riemann hypothesis for the L-function attached to the quadratic character mod p, is needed to prove this.

Note that both of these algorithms to compute $\sqrt{x}$ mod p have running times independent of x.

2. Elliptic Curves Over Finite Fields. Let $\mathbf{F}_q$ be a finite field with q elements of characteristic p not equal to 2 or 3; let E be an elliptic curve over $\mathbf{F}_q$. An affine equation for E can be given as follows:

$$Y^2 = X^3 + AX + B \tag{1}$$

with $A, B \in \mathbf{F}_q$ and $4A^3 + 27B^2 \neq 0$.

The set of $\overline{\mathbf{F}}_q$-points of E will be denoted by $E(\overline{\mathbf{F}}_q)$ and consists of the solutions (x, y) of (1) and the point at infinity which will be denoted by 0. In general, for any field K with $\mathbf{F}_q \subset K \subset \overline{\mathbf{F}}_q$, we denote by $E(K)$ the set of K-points of E, i.e., the solutions (x, y) of (1) with $x, y \in K$ and the point at infinity. It is well-known that $E(\overline{\mathbf{F}}_q)$ carries the structure of an Abelian group; the point at infinity plays the role of the zero element of the group and all subsets $E(K)$, where K is a field satisfying $\mathbf{F}_q \subset K \subset \overline{\mathbf{F}}_q$, are, in fact, subgroups. The addition laws can be given very explicitly as follows:

$$\text{If } P = (x, y) \in E(\overline{\mathbf{F}}_q) \quad \text{then } -P = (x, -y).$$

Let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2) \in E(\overline{\mathbf{F}}_q)$ both not equal to 0 and assume that $P_1 + P_2 \neq 0$. If $P_1 \neq P_2$, we have that $x_1 \neq x_2$ and we put $\lambda = (y_2 - y_1)/(x_2 - x_1)$,

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use

otherwise we have that $y_1 \neq 0$ and we put $\lambda = (3x_1^2 + A)/2y_1$. Put $P_3 = (x_3, y_3) = P_1 + P_2$.We have that

$$(2) \qquad x_3 = -x_1 - x_2 + \lambda^2, \qquad y_3 = -y_1 - \lambda(x_3 - x_1),$$

see Lang [5].

The ring of endomorphisms of E that are defined over $\mathbf{F}_q$ is denoted by $\operatorname{End}_{\mathbf{F}_q} E$ and is either an order in a complex quadratic number field of a noncommutative ring of $\mathbf{Z}$-rank = 4. The same holds for $\operatorname{End}_{\overline{\mathbf{F}}_q} E$, the ring of endomorphisms that are defined over $\overline{\mathbf{F}}_q$; we call an elliptic curve E over $\mathbf{F}_q$ super-singular, if $\operatorname{End}_{\overline{\mathbf{F}}_q} E$ is a noncommutative ring.

By ϕ we denote the Frobenius endomorphism of an elliptic curve E that is defined over $\mathbf{F}_q$; this endomorphism acts on $E(\overline{\mathbf{F}}_q)$ as

$$(x, y) \overset{\phi}{\mapsto} (x^q, y^q).$$

In $\operatorname{End}_{\mathbf{F}_q} E$ the Frobenius endomorphism satisfies a unique relation

$$(3) \qquad \phi^2 - t\phi + q = 0 \qquad (t \in \mathbf{Z}).$$

We call t the trace of the Frobenius endomorphism. It holds that

$$(4) \qquad |t| \leqslant 2\sqrt{q} \qquad \text{(Riemann hypothesis)}$$

and that

$$(5) \qquad E(\mathbf{F}_q) = q + 1 - t.$$

For all these facts see, for instance, [12]. The absolute value of t is obviously bounded by $q + 1$ as is easily seen from the covering $E \to \mathbf{P}^1$ via $(x, y) \mapsto x$ of degree two. For our applications the latter bound is sufficient.

Next, we study the structure of $E(\overline{\mathbf{F}}_q)$ as an Abelian group and as a $\operatorname{Gal}(\overline{\mathbf{F}}_q/\mathbf{F}_q)$-module in more detail. The group $E(\overline{\mathbf{F}}_q)$ is infinite torsion; if $n \in \mathbf{Z}$ is not divisible by p, then $E[n]$, the subgroup of points in $E(\overline{\mathbf{F}}_q)$ that are killed by n or the n-torsion points, is isomorphic to $\mathbf{Z}/n\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z}$. The group of points in $E(\overline{\mathbf{F}}_q)$ killed by p, that is $E[p]$, is either zero or cyclic of order p, depending on whether the curve is super-singular or not.

We introduce polynomials $\Psi_n(X, Y) \in \mathbf{F}_q[X, Y]$ for $n \in \mathbf{Z}_{\geqslant -1}$; cf. [5].

$$\Psi_{-1}(X, Y) = -1, \quad \Psi_0(X, Y) = 0, \quad \Psi_1(X, Y) = 1, \quad \Psi_2(X, Y) = 2Y,$$
$$\Psi_3(X, Y) = 3X^4 + 6AX^2 + 12BX - A^2,$$
$$\Psi_4(X, Y) = 4Y(X^6 + 5AX^4 + 20BX^3 - 5A^2X^2 - 4ABX - 8B^2 - A^3),$$
$$\Psi_{2n}(X, Y) = \Psi_n(\Psi_{n+2}\Psi_{n-1}^2 - \Psi_{n-2}\Psi_{n+1}^2)/2Y \quad (n \in \mathbf{Z}_{\geqslant 1}),$$
$$\Psi_{2n+1}(X, Y) = \Psi_{n+2}\Psi_n^3 - \Psi_{n+1}^3\Psi_{n-1} \quad (n \in \mathbf{Z}_{\geqslant 1}).$$

On E, the polynomial Ψ_n vanishes precisely at the nonzero n-torsion points. We define the polynomials $f_n(x) \in \mathbf{F}_q[X]$ as follows. First we eliminate all Y^2-terms from Ψ_n using the relation (1); the resulting polynomial $\Psi_n'(X, Y)$ is either in $\mathbf{F}_q[X]$ or in $Y\mathbf{F}_q[X]$. Define

$$(6) \qquad \begin{aligned} f_n(X) &= \Psi_n'(X, Y) && \text{if } n \text{ is odd,} \\ f_n(X) &= \Psi_n'(X, Y)/Y && \text{if } n \text{ is even.} \end{aligned}$$

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use

From the recursive formulas for Ψ_n given above, one easily deduces that

$$\deg f_n = \tfrac{1}{2}(n^2-1) \quad \text{if } n \text{ is odd}, p \nmid n,$$
$$\deg f_n = \tfrac{1}{2}(n^2-4) \quad \text{if } n \text{ is even}, p \nmid n.$$

PROPOSITION (2.1). *Let $P = (x, y) \in E(\overline{\mathbf{F}}_q)$ with $P \notin E[2]$ and let $n \in \mathbf{Z}_{\geqslant -1}$; then*

$$nP = 0 \Leftrightarrow f_n(x) = 0.$$

Proof. See Lang [5].

PROPOSITION (2.2). *Let $P = (x, y) \in E(\overline{\mathbf{F}}_q)$; let $n \in \mathbf{Z}_{\geqslant 1}$ with $nP \neq 0$; then*

$$nP = \left(x - \frac{\Psi_{n-1}\Psi_{n+1}}{\Psi_n^2}, \frac{\Psi_{n+2}\Psi_{n-1}^2 - \Psi_{n-2}\Psi_{n+1}^2}{4Y\Psi_n^3}\right). \tag{7}$$

(*By Ψ_k we mean $\Psi_k(x, y)$.*)

Proof. See Lang [5].

These explicit formulas will enable us to do the computations on l-torsion points of $E(\overline{\mathbf{F}}_q)$ that we need in our algorithm.

Finally, we relate endomorphisms of E and $\mathrm{Gal}(\overline{\mathbf{F}}_q/\mathbf{F}_q)$-endomorphisms of torsion points. Let l be a prime different from p. We have a map

$$\mathrm{End}_{\mathbf{F}_q} E \to \mathrm{End}_{\mathrm{Gal}(\overline{\mathbf{F}}_q/\mathbf{F}_q)} E[l].$$

Let ϕ_l denote the image of ϕ in the right-hand side group. By (3) we have the following relation holding on $E[l]$:

$$\phi_l^2 - t\phi_l + q = 0. \tag{8}$$

On the other hand, suppose that the relation

$$\left(\phi_l^2 - t'\phi_l + q\right)P = 0 \tag{9}$$

holds for all $P \in E[l]$ and some $t' \in \mathbf{Z}$; using (8), we deduce that $(t' - t)\phi_l P = 0$ for all $P \in E[l]$. Since $\phi_l \in \mathrm{End}_{\mathrm{Gal}(\overline{\mathbf{F}}_q/\mathbf{F}_q)} E[l]$ is invertible, we find $t \equiv t' (\mathrm{mod}\ l)$. So we see that

(10) we can compute the trace of the Frobenius endomorphism mod l by checking which of the relations (9) hold on $E[l]$.

3. Computation of the Number of $\mathbf{F}_q$-Points on an Elliptic Curve Over $\mathbf{F}_q$. In this section we give a deterministic algorithm to compute the number of points on an elliptic curve E over $\mathbf{F}_q$ which is given by a Weierstrass equation (1).

Let E be an elliptic curve over $\mathbf{F}_q$; let char $\mathbf{F}_q \neq 2$ or 3. We make this assumption to be able to use the polynomials Ψ_n from Section 2; it should be possible to obtain polynomials like these if the characteristic is 2 or 3.

To compute $E(\mathbf{F}_q)$, we may as well compute the trace t of the Frobenius endomorphism $\phi \in \mathrm{End}_{\mathbf{F}_q} E$ by (5). Since we have a bound on the size of t by (4), we can compute t by computing t (mod l) for sufficiently many small prime numbers l: if we compute t (mod l) for $l = 3, 5, 7, 11, \ldots, L$ such that

$$\prod_{\substack{l \leqslant L \\ l \neq 2, p}} l > 4\sqrt{q}, \tag{11}$$

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use

we can unambiguously determine t by applying the Chinese Remainder Theorem. So we need only describe how to compute $t \pmod{l}$ for l a prime not equal to 2 or p. We will first give a sketch of these computations.

By the remark (10) at the end of Section 2, we can compute $t \pmod{l}$ by checking which of the relations

$$(12) \qquad \phi_l^2 + q = \tau\phi_l \qquad (\tau \in \mathbf{Z}/l\mathbf{Z})$$

holds on $E[l]$. These tests can be effected by computations with polynomials in $\mathbf{F}_q[X, Y]$: let l be a prime not equal to 2 or p and let $P = (x, y) \in E[l]$ not equal to 0. By Proposition (2.2) the relation (12) holds for (x, y) if and only if

$$(13) \qquad \left(x^{q^2}, y^{q^2}\right) + \left(x - \frac{\Psi_{q-1}\Psi_{q+1}}{\Psi_q^2}, \frac{\Psi_{q+2}\Psi_{q-1}^2 - \Psi_{q-2}\Psi_{q+1}^2}{4y\Psi_q^3}\right) = \begin{cases} 0 & \text{if } \tau \equiv 0 \pmod{l}, \\ \left(x^q - \left(\dfrac{\Psi_{\tau-1}\Psi_{\tau+1}}{\Psi_\tau^2}\right)^q, \left(\dfrac{\Psi_{\tau+2}\Psi_{\tau-1}^2 - \Psi_{\tau-2}\Psi_{\tau+1}^2}{4y\Psi_\tau^3}\right)^q\right) & \text{otherwise.} \end{cases}$$

(By Ψ_k we denote $\Psi_k(x, y)$ as before.) By Proposition (2.1) the point $P = (x, y)$ is in $E[l]$ if and only if $\Psi_l(x, y) = 0$ or, equivalently, $f_l(x) = 0$. Using formula (1) and the addition formulas (2), the relation (13) can be transformed into relations of the form

$$H_1(x) = 0 \quad \text{and} \quad H_2(x) = 0$$

for some polynomials in $\mathbf{F}_q[X]$. This comes from the fact that $P = (x, y)$ satisfies (13) if and only if $-P = (x, -y)$ does. The final test boils down to testing whether

$$(14) \qquad H_1 \equiv 0 \pmod{f_l} \quad \text{and} \quad H_2 \equiv 0 \pmod{f_l}$$

in $\mathbf{F}_q[X]$. This test is done for every $\tau \in \mathbf{Z}/l\mathbf{Z}$, until a value of τ is encountered for which (15) holds; then we have that $t \equiv \tau \pmod{l}$. Note that testing (12) is equivalent to testing whether $\phi_l^2 + k = \tau\phi_l$ holds on $E[l]$, where $k \equiv q \pmod{l}$ and $1 \leqslant k < l$.

Next, we give a detailed description of the algorithm. The first step consists of computing a number L for which (11) holds and of making a list of the polynomials f_n for $n = 1, 2, \ldots, L$. The second step is the computation of $t \pmod{l}$ for every prime $l \leqslant L$ not equal to 2 or p. This is done as follows:

We will use formula (13); since we use the addition formulas (2) to evaluate (13), we distinguish the cases where the points are distinct or not: First test whether there is a nonzero point $P = (x, y)$ in $E[l]$ for which $\phi_l^2 P = \pm kP$ holds. Here $k \equiv q \pmod{l}$ and $1 \leqslant k < l$. So we must test whether

$$x^{q^2} = x - \frac{\Psi_{k-1}\Psi_{k+1}}{\Psi_k^2}(x, y)$$

holds or, using $f_m(X)$ rather than $\Psi_m(X, Y)$

$$(15) \qquad x^{q^2} = \begin{cases} x - \dfrac{f_{k-1}(x)f_{k+1}(x)}{f_k^2(x)(x^3 + Ax + B)} & (\text{if } k \text{ even}), \\ x - \dfrac{f_{k-1}(x)f_{k+1}(x)(x^3 + Ax + B)}{f_k^2(x)} & (\text{if } k \text{ odd}). \end{cases}$$

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use

Note that the denominators in the above expressions do not vanish on $E[l]$. We find that $\phi_l^2 P = \pm kP$ if and only if

$$(x^{q^2} - x) f_k^2(x)(x^3 + Ax + B) + f_{k-1}(x) f_{k+1}(x) = 0 \quad (k \text{ even}),$$
$$(x^{q^2} - x) f_k^2(x) + f_{k-1}(x) f_{k+1}(x)(x^3 + Ax + B) = 0 \quad (k \text{ odd}),$$

and we can test whether a point like P exists in $E[l]$ by computing

$$\begin{aligned} &\gcd\big((X^{q^2} - X) f_k^2(X)(X^3 + AX + B) + f_{k-1}(X) f_{k+1}(X), f_l(X)\big) \\ (16) \qquad &\qquad (k \text{ even}), \\ &\gcd\big((X^{q^2} - X) f_k^2(X) + f_{k-1}(X) f_{k+1}(X)(X^3 + AX + B), f_l(X)\big) \\ &\qquad (k \text{ odd}). \end{aligned}$$

If this gcd $\neq 1$ we have that a point P exists in $E[l]$ with $\phi_l^2 P = \pm qP$; we will return to this case. If, on the other hand, this gcd equals 1, we have that $\tau \neq 0$ in (11). In testing (11) for other values of τ, we can, when adding $\phi_l^2(x, y)$ and $q(x, y)$, apply the version of the addition formulas where the two points have distinct X-coordinates.

Case 1. This is the case where for some nonzero $P \in E[l]$ we have that $\phi_l^2 P = -qP$. If $\phi_l^2 P = -qP$, for some nonzero P, we have by (3) that $t\phi_l P = 0$, whence, since $\phi_l P \neq 0$, that $t \equiv 0 \pmod{l}$. If $\phi_l^2 P = qP$ for some nonzero P, we have by (3) that

$$(2q - t\phi_l)P = 0 \quad \text{and} \quad \phi_l P = \frac{2q}{t} P.$$

(Note that $t \not\equiv 0 \pmod{l}$ since $l \neq 2$ or p.) From this we deduce that $t^2 \equiv 4q \pmod{l}$. Let $w \in \mathbf{Z}$ with $0 < w < l$ denote a square root of $q \pmod{l}$; this number may be computed by successively trying $1, 2, \ldots$. Since $(\phi_l - \frac{1}{2}t)^2 = 0$, the eigenvalues of ϕ_l acting on $E[l]$ are w or $-w$. We can decide Case 1 by the following computations:

If $(\frac{q}{l}) = -1$ we clearly have that $t \equiv 0 \pmod{l}$; if not, we compute w, a square root of $q \pmod{l}$ with $0 < w < l$ and we test whether w or $-w$ is an eigenvalue of ϕ_l; if this is not the case, we conclude that $t \equiv 0 \pmod{l}$ and if indeed a nonzero point P exists with $\phi_l P = \pm wP$, we test whether either $\phi_l P = wP$ or $\phi_l P = -wP$ holds. In the first case we have $t \equiv 2w \pmod{l}$; in the second case, $t \equiv -2w \pmod{l}$. Explicitly (with $w^2 \equiv q \pmod{l}$):

If

$$\begin{aligned} &\gcd\big((X^q - X) f_w^2(X)(X^3 + AX + B) + f_{w-1}(X) f_{w+1}(X), f_l(X)\big) \\ (17) \qquad &\qquad (w \text{ even}), \\ &\gcd\big((X^q - X) f_w^2(X) + f_{w-1}(X) f_{w+1}(X)(X^3 + AX + B), f_l(X)\big) \\ &\qquad (w \text{ odd}) \end{aligned}$$

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use

equals 1, we have that $t \equiv 0 \pmod{l}$ otherwise, if

$$\begin{aligned}(18)\qquad &\gcd\bigl(4(X^3 + AX + B)^{(q-1)/2} f_w^3(X) - f_{w+2}^2(X) f_{w-1}(X)\\ &\qquad + f_{w-2}^2(X) f_{w+1}(X), f_l(X)\bigr),\\ &\gcd\bigl(4(X^3 + AX + B)^{(q+3)/2} f_w^3(X) - f_{w+2}^2(X) f_{w-1}(X)\\ &\qquad + f_{w-2}^2(X) f_{w+1}(X), f_l(X)\bigr)\end{aligned}$$

(for w even, resp. odd) equals 1, we have that $t \equiv -2w \pmod{l}$ else $t \equiv 2w \pmod{l}$.

Case 2. This is the case where we know that $\phi_l^2 P$ and qP are neither equal nor opposite for any $P \in E[l]$. In this case we will test which of the relations (11) holds with $\tau \in \mathbf{Z}/l\mathbf{Z}^\times$. We have with $P = (x, y)$ and $k \equiv q \pmod{l}$ and $0 < k < l$, that

$$\phi_l^2 P + qP = \left(-x^{q^2} - x + \frac{\Psi_{k-1}\Psi_{k+1}}{\Psi_k^2} + \lambda^2, -y^{q^2} - \lambda\left(-2x^{q^2} - x + \frac{\Psi_{k-1}\Psi_{k+1}}{\Psi_k^2}\right)\right),$$

where

$$\lambda = \frac{\Psi_{k+2}\Psi_{k-1}^2 - \Psi_{k-2}\Psi_{k+1}^2 - 4y^{q^2+1}\Psi_k^3}{4\Psi_k y\bigl((x - x^{q^2})\Psi_k^2 - \Psi_{k-1}\Psi_{k+1}\bigr)}.$$

Note that the denominator of λ does not vanish on $E[l]$ since Ψ_k has no zeros on $E[l]$ and since we are in Case 2. Let $\tau \in \mathbf{Z}$ with $0 < \tau < l$; we have

$$\tau\phi_l P = \left(x^q - \left(\frac{\Psi_{\tau+1}\Psi_{\tau-1}}{\Psi_\tau^2}\right)^q, \left(\frac{\Psi_{\tau+2}\Psi_{\tau-1}^2 - \Psi_{\tau-2}\Psi_{\tau+1}^2}{4y\Psi_\tau^3}\right)^q\right).$$

In a way analogous to the computations above one can test, by computations in $\mathbf{F}_q[X]$, which of the relations (11) holds by trying $\tau = 1, \ldots, l-1$. The computations involve evaluating polynomials modulo $f_l(X)$ and testing whether they are zero mod $f_l(X)$. We do not give all the details; testing whether $\phi_l^2 + q = \tau\phi_l$ holds on $E[l]$ boils down to testing whether

$$\begin{aligned}(19)\qquad &\Bigl(\bigl(\Psi_{k-1}\Psi_{k+1} - \Psi_k(X^{q^2} + X^q + X)\bigr)\beta^2 + \Psi_k^2\alpha^2\Bigr)\Psi_\tau^{2q} + \Psi_{\tau-1}^q\Psi_{\tau+1}^q\beta^2\Psi_k^2, \text{ and}\\ &4Y^q\Psi_\tau^{3q}\Bigl(\alpha\bigl((2X^{q^2} + X)\Psi_k^2 - \Psi_{k-1}\Psi_{k+1}\bigr) - Y^{q^2}\beta\Psi_k^2\Bigr)\\ &\qquad - \beta\Psi_k^2\bigl(\Psi_{\tau+2}\Psi_{\tau-1}^2 - \Psi_{\tau-2}\Psi_{\tau+1}^2\bigr)^q\end{aligned}$$

are zero mod $f_l(x)$. Here

$$\alpha = \Psi_{k+2}\Psi_{k-1}^2 - \Psi_{k-1}\Psi_{k+1}^2 - 4Y^{q^2+1}\Psi_k^3$$

and

$$\beta = \bigl((X - X^{q^2})\Psi_k^2 - \Psi_{k-1}\Psi_{k+1}\bigr)4Y\Psi_k.$$

By the expressions (19) we understand the polynomials in $\mathbf{F}_q[X]$ one gets after eliminating Y using (19) and, if necessary, by dividing the expressions by Y. The result is a polynomial in $\mathbf{F}_q[X]$. This completes the description of the second step of our algorithm.

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use

The third step is the computation of t from the values of $t \pmod{l}$ obtained using the Chinese Remainder Theorem and the estimate (4). This is straightforward. This completes the description of the algorithm.

Next we estimate the number of elementary operations involved in these computations. It is well-known that there exists an effectively computable universal constant C_1 for which

$$\prod_{\substack{l \leqslant L,\ \text{prime} \\ l \neq 2, p}} l > C_1 e^L \tag{20}$$

holds for every $L > 0$; see [8] for instance. So we can take L to be $O(\log q)$ and all primes $l \leqslant L$ are $O(\log q)$ as well. The number of primes occurring in (20) is also $O(\log q)$.

To compute in $\mathbf{F}_q$ we assume that we are provided with an irreducible polynomial f of degree $[\mathbf{F}_q : \mathbf{F}_p]$ a zero of which generates $\mathbf{F}_q$ over $\mathbf{F}_p$; we compute in $\mathbf{F}_q$ by computing in $\mathbf{F}_p[X]/(f)$.

The number of elementary operations needed to compute f_1 up to f_L is $O(\log^7 q)$; this follows from the fact that $L = O(\log q)$ and that $\deg f_m = O(m^2)$. Evaluating the expressions (19) modulo f_l and the gcd's (16), (17) and (18) can be done using $O(d^2 \log^3 q)$ elementary operations; here d denotes the degree of f_l. Since $\deg f_l = O(\log^2 q)$ we see that we need $O(\log^7 q)$ elementary operations to do this. If we happen to be in Case 2 for some l, we have to repeat these computations $O(l) = O(\log q)$ times. So for each l, the second step of the algorithm takes $O(\log^8 q)$ elementary operations. We conclude that the entire Step 2 takes $O(\log^9 q)$ elementary operations.

The computations of L and the computations involving the application of the Chinese Remainder Theorem are easily seen to be dominated by $O(\log^9 q)$. This proves the result stated in the first section.

In the algorithm we precompute the polynomials f_n; it takes $O(\log^5 q)$ bits to store these polynomials. The amount of memory used in the rest of the algorithm is dominated by $O(\log^5 q)$.

We believe that this algorithm may work well in practice. In this paper no effort has been made to be economic from the practical point of view. For instance, in practice one should also consider the prime $l = 2$ and in fact work on $E[l^k]$ for prime powers l^k.

We do not find the group structure of $E(\mathbf{F}_q)$. We know that the l-parts of $E(\mathbf{F}_q)$ need at most two generators for any prime l and we have that the l-part can only be noncyclic if $l | q - 1$ and $l^2 | \#E(\mathbf{F}_q)$. So sometimes it is easy to find the group structure as well, but in general we do not know how to compute the group structure in time polynomial in $\log q$.

4. Square roots mod p. In this section, we describe a deterministic algorithm to compute the square roots of $x \in \mathbf{Z}$ modulo a prime p, provided that $(\frac{x}{p}) = +1$. The algorithm takes $O((|x|^{1/2+\varepsilon} \log p)^9)$ elementary operations for all $\varepsilon > 0$. The amount of work involved to compute $(\frac{x}{p})$ is dominated by this.

Let $x \in \mathbf{Z}$ and let p be a prime not equal to 2 or 3 with $(\frac{x}{p}) = +1$; we may and do assume that $p \equiv 1 \pmod 4$, because, if $p \equiv -1 \pmod 4$ and $(\frac{x}{p}) = +1$, a square root

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use

of x (mod p) is given by $x^{(p+1)/4}$ and this number can be evaluated mod p in $O(\log^3 p \cdot \log|x|)$ elementary operations. We also assume that x is the discriminant of a complex quadratic order; for, if it is not, either $4x$ or $-4x$ is, and we compute either $\sqrt{4x}$ or both $\sqrt{4x}$ and $\sqrt{-4x}$. All these numbers are in $\mathbf{F}_p$ since $p \equiv 1$ (mod 4).

Briefly, the algorithm runs as follows: we write down a Weierstrass equation of an elliptic curve E over $\mathbf{F}_q$, a suitable extension of $\mathbf{F}_p$, which has complex multiplication by $\mathcal{O}$, i.e., its ring of $\mathbf{F}_q$-endomorphisms contains $\mathcal{O}$. Next we compute the Frobenius endomorphism ϕ in $\mathcal{O}$ by means of the algorithm given in Section 2. We have that

$$\phi = \frac{a + b\sqrt{x}}{2} \qquad (a, b \in \mathbf{Z};\ a \equiv b (\operatorname{mod} 2))$$

and $4q = a^2 - b^2x$. So, $(a/b)^2 \equiv x$ (mod p). We shall see later that the fact that $(\frac{x}{p}) = 1$ implies that $b \not\equiv 0$ (mod p); for definitions and facts concerning elliptic curves, their endomorphism rings etc., see for instance [12].

Let $j(z)$ denote the modular function

$$(21) \qquad j(z) = e^{-2\pi i z} + 744 + 196884e^{2\pi i z} + \dots, \qquad (\operatorname{Im} z > 0)$$

or, more precisely,

$$j(z) = 12^3 G_2(z)^3 / \left(G_2(z)^3 - G_3(z)^2\right),$$

where

$$G_2(z) = 1 + 240 \sum_{k=1}^{\infty} \sigma_3(k) e^{2\pi i k z} \quad (\operatorname{Im} z > 0),$$

$$G_3(z) = 1 - 504 \sum_{k=1}^{\infty} \sigma_5(k) e^{2\pi i k z} \quad (\operatorname{Im} z > 0),$$

$$\sigma_m(k) = \sum_{0<d\,|\,k} d^m.$$

Define the integers $c(k)$ by

$$j(z) = e^{-2\pi i z} + \sum_{k=0}^{\infty} c(k) e^{2\pi i k z}.$$

We have that

$$\lim_{n\to\infty} c(n)^{-1} \frac{e^{4\pi\sqrt{n}}}{\sqrt{2}\cdot n^{3/4}} = 1;$$

this is due to Petersson [7]; the result is effective and we deduce: there exists an effectively computable constant C_1, such that

$$|c(n)| \leqslant C_1 \frac{e^{4\pi\sqrt{n}}}{\sqrt{2}\cdot n^{3/4}}$$

for all $n \in \mathbf{Z}_{\geqslant 1}$. From this estimate one easily deduces that for $z \in \mathbf{Z}$ with $|\operatorname{Re} z| \leqslant \frac{1}{2}$ and $|z| \geqslant 1$ (i.e., z is in the standard fundamental domain for the action of $\mathrm{SL}_2(\mathbf{Z})$ on the upper half-plane), we have

$$(22) \qquad \left|j(z) - e^{\pi \operatorname{Im} z}\right| \leqslant C_2$$

for some universal, effectively computable constant C_2.

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use

Next, we will explain how to compute a Weierstrass equation of an elliptic curve over $\mathbf{F}_q$ that has complex multiplication by $\mathcal{O}$. Here $\mathcal{O}$ denotes the unique complex quadratic order of discriminant x. If $x = -3 \cdot$ square or $-4 \cdot$ square we may as well assume that $x = -3$ resp. $x = -4$. It is easy to test whether x is of this form and $\sqrt{x}$ is easily determined from $\sqrt{-3}$ resp. $\sqrt{-4}$.

If $x = -3$ we take as a Weierstrass equation for E: $Y^2 = X^3 - 1$; if $x = -4$ we take $Y^2 = X^3 - X$. If x is not -3 or -4 times a square, we compute all invertible ideal classes of the ring $\mathcal{O}$; since these classes are, in a way which is well-known, in one-to-one correspondence with the set of triples

$$\big\{(a, b, c) \in \mathbf{Z}^3 \colon a > 0; \gcd(a, b, c) = 1; |b| \leqslant a \leqslant c;$$
$$b^2 - 4ac = x;\ b > 0 \text{ whenever } |b| = a \text{ or } a = c\big\},$$

we compute these triples instead. For a triple (a, b, c) in the above set it holds that $|b| \leqslant a \leqslant \sqrt{(|x|/3)}$ and one can compute all these triples in time $O(|x|^{1+\varepsilon})$.

Let $h(x)$ denote the cardinality of the set of triples. For every triple (a, b, c) we approximate $j((b + i\sqrt{|x|})/2a)$ using the Fourier expansion (21), such that the absolute error is smaller than $\exp(-C_3|x|^{1+\varepsilon})$ for some constant C_3 depending on ε only. We need $[C_4|x|^{1+\varepsilon}]$ terms of the expansion to accomplish this. The numbers $j((b + i\sqrt{|x|})/2a)$ are conjugate algebraic integers; they are precisely the j-invariants of elliptic curves over $\mathbf{C}$ with complex multiplication by $\mathcal{O}$. These numbers are the zeros of an irreducible polynomial $F \in \mathbf{Z}[X]$ of degree $h(x)$. We have that $h(x) = O(|x|^{1/2+\varepsilon})$ for every $\varepsilon > 0$.

We approximate the coefficients of this polynomial by evaluating symmetric functions of the approximations of its roots. We leave it to the reader to verify that for every $\varepsilon > 0$, one can determine constants C_3 and C_4, independent of x, such that the coefficients of F can be deduced unambiguously from these approximations. All computations can be done using $O(|x|^{2.5+\varepsilon})$ elementary operations, for every $\varepsilon > 0$.

Proposition (4.1). *Let $\mathcal{O}$ be the unique complex quadratic order having discriminant x, which is not -3 or -4 times a square. Let $F \in \mathbf{Z}[X]$ denote the irreducible polynomial having the j-invariants of the elliptic curves with complex multiplication by $\mathcal{O}$ as its roots. Let p be a prime which splits in $\mathcal{O}$, i.e., for which $(\frac{x}{p}) = 1$. Then, it holds that $v(\zeta) = v(\zeta - 1728) = 0$ for every zero of F and every valuation v of $\overline{\mathbf{Q}}$ that extends the p-adic valuation of $\mathbf{Q}$.*

Proof. Let v extend the p-adic valuation of $\mathbf{Q}$; let $\mathfrak{p}$ be a prime ideal of some finite extension L of $\mathbf{Q}$ that corresponds to v. Let $F(\zeta) = 0$ and let E denote an elliptic curve defined over $\mathbf{Q}(\zeta)$ that has its j-invariant equal to ζ. The curve E has potentially good reduction at $\mathfrak{p}$, i.e., it has good reduction over some finite extension of $\mathbf{Q}(\zeta)$. Since we may replace L by any finite extension and $\mathfrak{p}$ by any prime over it in that extension, we enlarge L such that E is defined over L and has good reduction at $\mathfrak{p}$. Let $\mathbf{F}_q$ denote the residue class field of $\mathfrak{p}$.

We have

$$\mathcal{O} \hookrightarrow \operatorname{End}_L E \quad \text{and} \quad \operatorname{End}_L E \hookrightarrow \operatorname{End}_{\mathbf{F}_q}(E \bmod \mathfrak{p})$$

by a result of Deuring [3, Section 4]. If $\zeta \in \mathfrak{p}$ or $\zeta - 1728 \in \mathfrak{p}$ we have that

$$\mathbf{Z}[\zeta_3] \hookrightarrow \operatorname{End}_{\mathbf{F}_q}(E \bmod \mathfrak{p}) \quad \text{resp.} \quad \mathbf{Z}[\zeta_4] \hookrightarrow \operatorname{End}_{\mathbf{F}_q}(E \bmod \mathfrak{p})$$

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use

by the same argument. This implies, by the assumption that $x \neq -3$ or -4 times a square, that $\mathrm{End}_{\mathbf{F}_q}(E \bmod \mathfrak{p})$ cannot be a quadratic order; so $\mathrm{End}_{\mathbf{F}_q}(E \bmod \mathfrak{p})$ is noncommutative and $E \bmod \mathfrak{p}$ is a super-singular curve. This is impossible since $\mathfrak{p}$ splits in $\mathrm{Frac}(\mathcal{O})$. This proves the proposition.

For the facts concerning reduction of elliptic curves used in the proof, see [9].

We continue the description of our algorithm. After computing the polynomial F, we write down an elliptic curve defined over $\overline{\mathbf{F}}_p$ which has its j-invariant equal to a zero of F. This curve has complex multiplication by $\mathcal{O}$ and is elliptic by Proposition (4.1):

$$Y^2 + YX = X^3 - \frac{36}{\zeta - 1728}X - \frac{1}{\zeta - 1728}.$$

Here ζ denotes a zero of F in $\overline{\mathbf{F}}_p$; the j-invariant of this curve is ζ.

We let $\mathbf{F}_q = \mathbf{F}_q(\zeta)$; the field $\mathbf{F}_q$ does not depend on the choice of ζ, since F is in $\mathbf{F}_p[X]$ a product of irreducible factors that all have the same degree. It is not difficult to deduce an equation

$$Y^2 = X^3 + AX + B$$

with $A, B \in \mathbf{F}_p(\zeta)$ for the curve E from the equation given above.

Now, there is only one problem to solve before we can apply the algorithm of Section 2 to compute the Frobenius endomorphism of E and the square root of $x \bmod p$. The problem is that we do not necessarily have an irreducible polynomial G, a zero of which generates $\mathbf{F}_q$ over $\mathbf{F}_p$. We only have F, a polynomial which may be reducible.

We compute in $\mathbf{F}_q$ by computing with expressions

$$x = \sum_{k=0}^{d-1} a_k \zeta^k \quad (d = \deg F;\ a_k \in \mathbf{F}_p);$$

it is obvious how to compute sums and products of these numbers and these computations are as hard as the analogous computations in $\mathbf{F}_{p^d}$. Essentially, the only problem is how to test whether

$$x = \sum_{k=0}^{d-1} a_k \zeta^k = 0?$$

We will perform this test by testing whether

$$G = \gcd\left(\sum_{k=0}^{d-1} a_k T^k,\ F(T)\right) = 1;$$

if this $\gcd = 1$, we have that $x \neq 0$, independent of our choice of ζ; if this $\gcd = F(T)$, we always have that $x = 0$; if the gcd is a proper divisor G of F, we may replace F by G and we may take $x = 0$ or we do it the other way around: we replace F by F/G and we take $x \neq 0$. We will always do the former. Computing in $\mathbf{F}_p(\zeta)$ in this way, is not harder than computing in $\mathbf{F}_{p^{\deg F}}$. Since initially $\deg F = h(x)$ and since $h(x) = O(|x|^{1/2+\varepsilon})$, we find that computing $x \bmod p$ takes $O(\log^9(p^{h(x)}))$ $= O((|x|^{1/2+\varepsilon} \log q)^9)$ elementary operations for any $\varepsilon > 0$.

Finally, we give one further application.

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use

PROPOSITION (4.2). *There exists a deterministic polynomial time algorithm to compute* $\sqrt{x} \bmod p$ *if* $p \not\equiv 1 \pmod{16}$. *This algorithm has a running time independent of* x *for* $x < p$.

Proof. In view of the algorithm presented by Shanks in [11], it suffices to show how to compute a generator of the 2-part of $\mathbf{Z}/p\mathbf{Z}^{\times}$ in time polynomial in $\log p$. If $p \not\equiv 1 \pmod{16}$, either $\zeta_2 = -1$, $\zeta_4 = \sqrt{-1}$ or $\zeta_8 = \frac{1}{2}\sqrt{2}(1 + \sqrt{-1})$ is a generator. Since we can compute these numbers in time polynomial in $\log p$ by means of our deterministic algorithm, the proposition is proved.

Universiteit van Amsterdam
Mathematisch Instituut
Roetersstraat 15
1018 WB Amsterdam
The Netherlands

1. I. BOROSH, C. MORENO & H. PORTA, "Elliptic curves over finite fields. I," *Proc.* 1972 *Number Theory Conference* (University of Colorado), Boulder, 1972, pp. 147–155.

2. I. BOROSH, C. MORENO & H. PORTA, "Elliptic curves over finite fields, II," *Math. Comp.*, v. 29, 1975, pp. 951–964.

3. M. DEURING, "Die Typen der Multiplikatorenringe elliptischer Funktionenkörper," *Abh. Math. Sem. Hamburg*, v. 14, 1941, pp. 197–272.

4. D. KNUTH, *The Art of Computer Programming*, vol. II (*Seminumerical Algorithms*), Addison-Wesley, Reading, Mass., 1981.

5. S. LANG, *Elliptic Curves; Diophantine Analysis*, Springer-Verlag, Berlin and New York, 1978.

6. S. LANG AND H. TROTTER, *Frobenius Distributions in GL_2-Extensions*, Lecture Notes in Math., vol. 504, Springer-Verlag, Berlin and New York, 1976.

7. H. PETERSSON, "Über die Entwicklungskoeffizienten der automorphen Formen," *Acta Math.*, v. 58, 1932, pp. 169–215.

8. J. B. ROSSER & L. SCHOENFELD, "Approximate formulas for some functions of prime numbers," *Illinois J. Math.*, v. 6, 1962, pp. 64–94.

9. J.-P. SERRE & J. TATE, "Good reduction of abelian varieties," *Ann. of Math.*, v. 88, 1968, pp. 492–517.

10. D. SHANKS, *Class Number, A Theory of Factorization and Genera*, Proc. Sympos. Pure Math., vol. 20, Amer. Math. Soc., Providence, R. I., 1970, pp. 415–440.

11. D. SHANKS, "Five number-theoretic algorithms," *Congressus Numerantium* No. VII; *Proc.* 2*nd Manitoba Conf. on Numerical Math.* (University of Manitoba), 1972, pp. 51–70.

12. J. TATE, "The arithmetic of elliptic curves," *Invent. Math.*, v. 23, 1974, pp. 179–206.

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use