Schoof's Algorithm for the Size of an Elliptic Curve

Eric Bach

April 2000

INTRODUCTION.

The goal of these notes is to explain the main results of [1], which has two parts:

1) A poly-time algorithm for computing the number of points on an elliptic curve mod p.
2) An algorithm (polynomial-time for fixed a), for computing the square root of a mod p. This uses part 1) as a subroutine.

NOTATION.

$p =$ odd prime
$\mathbf{F}_p =$ finite field w/ p elements
$E =$ elliptic curve defined by some equation with coordinates in $\mathbf{F}_p$. This has a group structure, where the group operations are given by rational operations. For this see, e.g. [4].
$(p|l)$ denotes the Legendre symbol (we only care about l prime).
If N is the number of points on E with coordinates in $\mathbf{F}_p$, then

$$N = p + 1 - t$$

for some number t with $|t| \leq 2\sqrt{p}$. This was proved by Hasse in the 1930's. Roughly, it says that the "predicted" number of points is $p+1$, to within a small error t that is $O(\sqrt{p})$. The error term t is called the "trace of Frobenius" – the reason for this peculiar name is that if ϕ denotes the map

$$(x, y) \mapsto (x^p, y^p)$$

(here x and y are coordinates of any point of E in the algebraic closure of $\mathbf{F}_p$) then ϕ satisfies

$$\phi^2 - t \cdot \phi + p = 0. \qquad (*)$$

To make sense of this, use additive notation for the group operation on E. We can speak of multiplication by n, which is just adding a point to itself n times. Then ϕ is a linear operator, in the sense that $\phi(aP + bQ) = a\phi(P) + \phi(Q)$. The above equation is like the characteristic equation for a matrix – it says that if you take any point P, and apply the above operator, i.e.

$$(\phi^2 - t\phi + p)(P) = \phi(\phi(P)) - t\phi(P) + pP$$

(pP denotes P added to itself p times), then you get the identity element of the group.

[Note: the idea of "endomorphism ring" may be useful to introduce here.]

COUNTING THE NUMBER OF POINTS ON AN ELLIPTIC CURVE

The basic idea for finding N is to compute t mod l for lots of small prime values of l, and recombine the results using the Chinese remainder theorem.

This is done by "reducing (*) mod l." We have to think a little about what this might mean. We want to cook up some operator ϕ_l (which you should think of as "ϕ mod l") with the property that

$$(\phi_l)^2 - (t \bmod l)\phi_l + (p \bmod l) = 0 \tag{**}$$

But what will this "operate" on? Since the coefficients are only defined mod l, a reasonable choice to use is

$$E[l] := \{P \in E : l \cdot P = 0\}$$

This will work because the Frobenius map ϕ clearly preserves $E[l]$. If you let $E[l]$ be as large as possible (throwing in points whose coordinates are in extension fields of $\mathbf{F}_p$), then it's known that

$$E[l] = \mathbf{F}_l \times \mathbf{F}_l$$

($\mathbf{F}_l$ = the finite field of l elements). Granting this, then, ϕ_l will be a 2×2 matrix of entries from $\mathbf{F}_l$, and its characteristic equation is

$$(\phi_l)^2 - t\phi_l + p = 0$$

[Is this also the minimal polynomial?]

The idea is now to search for a t satisfying the property (**). The search process is not fancy – it just tries all t, of $0 \leq t < l$. However, there are some rather clever "data structures" involved.

The basic idea is the following: a set S of points is represented by a polynomial that vanishes on S and nowhere else. Various operations on set of points (union, intersection, etc.) translate into operations on the polynomials. Using this "representation" of $E[l]$, we will check whether or not something like (**) holds.

DIVISION POLYNOMIALS

We'll restrict attention to curves that are presented in Weierstrass form:

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

(So $p \neq 2, 3$.)

It's known that there are polynomials ϕ_n, ω_n, and ψ_n (computable by recursion on n) such that:

1) If (x, y) is an affine point of E, then

$$(x, y) \in E[n] \Leftrightarrow \psi_n(x, y) = 0.$$

In this sense ψ_l "represents" $E[l]$.

2) Multiplication by n is given in affine coordinates by

$$n(x, y) = (\frac{\phi_n}{\psi_n^2}(x, y), \frac{\omega_n}{\psi_n^3}(x, y))$$

3) The degree of ψ_n is $< n^2$

4) If n is odd, then

$$\phi_n, \psi_n, \omega_n/y$$

are polynomials in x; if n is even, then

$$\phi_n, \psi_n/y, \omega_n$$

are polynomials in x.

The first few of the ψ_n are

$$\psi_1 = 1$$

$$\psi_2 = 2y$$

$$\psi_3 = 3x^4 + 6Ax^2 + 12Bx - A^2$$

$$\psi_4 = 4y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3)$$

After that we can use the recursion formulas

$$\psi_{2n+1} = \psi_{n+2}\psi_n^3 - \psi_{n-2}\psi_{n+1}^3$$

$$\psi_{2n} = \frac{1}{2y}\psi_n(\psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2)$$

Finally,

$$\phi_n = x\psi_n^2 - \psi_{n+1}\psi_{n-1}$$

$$\omega_n = \frac{1}{4y}(\psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2)$$

(For proofs see [4] p. 33.)

Classically the division polynomials have integer coefficients, but for our purposes we can think of them as living in $\mathbf{F}_p[x, y]$.

FINDING THE CHARACTERISTIC EQUATION MOD l

Assume that $2 < l < p$. There are two cases, depending on whether or not $(p|l) = 1$. Only the first is used by the point counting algorithm.

CASE 1: p is not a square mod l.

In this case, (**) has to be the minimal polynomial of ϕ on $E[l]$. [Proof: otherwise ϕ acts like a scalar, call it $c \neq 0$. But the characteristic polynomial of c times the identity matrix is $X^2 - 2cX + c^2$; it follows that $p \equiv c^2 \bmod l$.]

The unknown coefficient t may be zero or not. We first attempt to find a nonzero t that works; if none is found, then $t \equiv 0 \bmod l$.

To prove that $\phi^2 - t\phi + p$ annihilates $E[l]$, it is enough that it annihilate "most" of $E[l]$, as the following shows.

Remember that $E[l] = \mathbf{F}_l \times \mathbf{F}_l$. We want to find the magic t for which

$$\phi^2 - t\phi + p = 0$$

that is, the t for which the kernel of the left-hand side is 2-dimensional.

For $P \in E[l]$, let A, B, C denote the following points:

$$A = \phi^2(P)$$

$$B = -t\phi(P)$$

$$C = p(P)$$

(they are thus functions of P). For "most" points in $E[l]$, A, B, C are distinct, as can be seen by counting the number of P for which distinctness fails.

1) $A = B$ holds iff $P \in \ker(\phi - t)$. This kernel is at most 1-dimensional, since ϕ's minimal polynomial has degree 2. Therefore at most l points P make $A = B$.
2) $B = C$ is similar: count the kernel of $\phi - p/t$ to get at most l points.
3) For $A = C$, recall that $t \neq 0$. Then since $\phi^2 - p$ is the "wrong" polynomial, its kernel has size at most l too.

Therefore there are at most $3l$ points P for which A, B, C are not distinct. If $l \geq 5$, $l^2 - 3l > l$. Hence if we show that

$$\forall P \in E[l], (A, B, C \text{distinct} \Rightarrow A + B + C = 0) \qquad (+)$$

then we know that

$$\#(\ \ker\ (\phi^2 - t\phi + p)) > l^2/2$$

so it must be all of $E[l]$.

Recall the condition for three points to be on a line in the projective plane: $(x_1 : y_1 : z_1)$, $(x_2 : y_2 : z_2)$, $(x_3 : y_3 : z_3)$ are collinear iff

$$\det \begin{pmatrix} x_1 & y_1 & z_1 \\ x_2 & y_2 & z_2 \\ x_3 & y_3 & z_3 \end{pmatrix} = 0.$$

Assume that t and p are reduced mod l. Then if A, B, C are distinct,

$$(\phi^2 t - t\phi + p)(x, y) = 0$$

is equivalent to the collinearity of $A = \phi^2(x, y)$, $B = -t\phi(x, y)$, and $C = p(x, y)$ (sometimes this is taken as the definition of elliptic curve addition).

Since $p, t \not\equiv 0(\bmod l)$, we know that $\phi^2(x, y)$, $-t\phi(x, y)$, $p(x, y)$ will all be in the affine plane when $(x, y) \in E[l]$. Denoting the affine coordinates of these three points by (x_1, y_1), (x_2, y_2), and (x_3, y_3) checking $(+)$ is the same as checking whether

$$\det \begin{pmatrix} x_1 & y_1 & 1 \\ x_2 & y_2 & 1 \\ x_3 & y_3 & 1 \end{pmatrix} = 0.$$

Let $\Delta(x,y)$ denote this determinant; if t is correct then we will have

$$\forall (x,y) \in E[l], \quad \Delta(x,y) = 0$$

The idea now is to rewrite this condition so as not to involve y. Since l is odd, we see that $(x,y) \in E[l]$ iff $(x,-y) \in E[l]$; put another way, membership in $E[l]$ does not involve y, so we can reduce the above criterion to

$$\forall (x,y) \in E, \psi_l(x) = 0 \Longrightarrow \Delta(x,y) = 0$$

Now notice that if (x,y) is contained in $E[l]$, then y cannot be 0 (for otherwise $2(x,y)$ would be the identity). We will factor y out of Δ as follows. We know that Δ has the form

$$\det \begin{pmatrix} x^{p^2} & y^{p^2} & 1 \\ \frac{\phi_t(x^p)}{\psi_t(x^p)^2} & \frac{\omega_t(x^p)}{\psi_t(x^p)^3} & 1 \\ \frac{\phi_p(x)}{\psi_p(x)^2} & \frac{\omega_p(x)}{\psi_p(x)^3} & 1 \end{pmatrix} = 0.$$

Now

1. $\forall n$, ϕ_n/ψ_n^2 is in $\mathbf{F}_p(x)$
2. n even $\Longrightarrow \omega_n/\psi_n^3$ is in $\mathbf{F}_p(x)/y$
3. n odd $\Longrightarrow \omega_n/\psi_n^3$ is in $y\mathbf{F}_p(x)$

The first column of Δ contains only functions in $\mathbf{F}_p(x)$; and when multiplied by y, the second column of Δ contains only functions in $\mathbf{F}_p(x) \cdot y^2$ (because p is odd). This last operation (multiplication by y) will not affect whether or not Δ is zero, since we know that $y \neq 0$. After multiplying the last column by y, we can replace all y^2's by $x^3 + Ax + B$, and clear fractions to get a new determinant $\Delta'(x)$. Our criterion now is

$$\forall x \in \bar{\mathbf{F}}_p, \psi_l(x) = 0 \Longrightarrow \Delta'(x) = 0$$

This is equivalent to

$$\Delta'(X) \equiv 0 (\mathrm{mod} \psi_l(X))$$

which is what the algorithm actually tests.

CASE 2: $(p|l) = +1$.

We now want to run the above algorithm, but we must first test if $\phi - c$ is zero on $E[l]$ (there are only two choices for c, as $c^2 \equiv p (\mathrm{mod} l)$). Let c denote one of these values. Then we have to check whether for all $(x,y) \in E[l]$, the pair

$$(x^p, y^p)$$

is equal to

$$(\phi_c/\psi_c^2, \omega_c/\psi_c^3)$$

i.e.

$$x^p - \phi_c/\psi_c^2 \equiv 0(\psi_l)$$

and

$$y^p - \omega_c/\psi_c^3 \equiv 0(\psi_l)$$

The first one is easy to check. For the second, we can again divide or multiply by y, then substitute $x^3 + Ax + B$ for y^2, yielding an equation in x only.

If this preliminary check gives a good value of c, then we know that $t \equiv 2c \bmod l$. Otherwise, we have shown that (**) is the minimal polynomial of ϕ, and we continue as in case 1.

RUNNING TIME ANALYSIS

Recall that the idea of the algorithm is to compute $t \bmod l$ for lots of small l, where $(p|l) = +1$.

Since $|t| \leq 2\sqrt{p}$, we need the product of these l's to be at least $4\sqrt{p}$. So we must choose B to make

$$\sum_{\substack{4 \leq l \leq B \\ (l|p)=+1}} \log l = 1/2 \log p + O(1).$$

Half of all primes are quadratic residues of p, so by the prime number theorem $B \sim \log p$ should be enough. So we need $O(\log p/\log\log p)$ values of ℓ. (This hand-waving should be replaced by something rigorous.)

We must now make ψ_n, ϕ_n, ω_n modulo $y^2 = x^2 - Ax - B$ for $n \leq B$. We use the recurrence formulas, taking care to do the reduction at each step. The polynomials for n each have degree $\leq n^2$ (why?), so the bit complexity will be

$$\sum_{n \leq B} O((n^2)^2) O(\log p)^2 = O(\log p)^7.$$

Now consider an individual prime l. We work in the ring $R = \mathbf{F}_p[x]/(\psi_l(x))$ (remember l is odd here). Operations in R cost $O(l^4(\log p)^2)$, which is $O((\log p)^6)$.

We need:

1. x^{p^2} – costs $O((\log p)^7)$.
2. $y^{p^2+1} = (x^3 + Ax + B)^{(p^2+1)/2}$ – ditto.
3. ϕ_p/ψ_p^2 and ω_p/ψ_p^3 with p reduced mod l – costs $O((\log p)^6)$.
4. x^p, then powers of this in R up to $O(l^2)$ – costs $O((\log p)^8)$.

And then for each $t \leq l$:

5. ϕ_t/ψ_t^2 and ω_t/ψ_t^3 evaluated at x^p – each polynomial a linear combination of $O(l^2)$ elements of R, hence $O((\log p)^6)$ operations.

Since there are at most l values of t, the total work for a given l is $O((\log p)^8)$.

Since there are $O(\log p/\log\log p)$ values of ℓ, the total work for this part of the algorithm is $O((\log p)^9/\log\log p)$.

Recovery of t using the Chinese remainder theorem can be done with $O(\log p)^2$ bit operations [5].

This gives a complexity estimate of $O((\log p)^9/\log\log p)$ bit operations. A reduced bound of $O((\log p)^8)$ is claimed in [6], which (presumably) results from streamlining the algorithm somewhat.

COMPUTING SQUARE ROOTS MOD p

Only the case $p \equiv 3 \bmod 4$ is of interest, for other p see [4].

Suppose we have a quadratic field K with discriminant Δ. (General Δ can be reduced to this case.) Skipping some details here, an elliptic curve E can be found that has complex multiplication by A, the ring of integers in K. Use the ideas of the previous sections to express the Frobenius on E as

$$\phi = \frac{a + b\sqrt{\Delta}}{2}$$

Since $\phi^2 - t\phi + p = 0$, we must have

$$p = \phi\bar{\phi} = a^2 - \Delta b^2$$

and so in $\mathbf{F}_p$

$$\sqrt{\Delta} = a/b.$$

REFERENCES.

[1] R. Schoof, Elliptic curves over finite fields and the computation of square roots mod p, Math. Comp. v. 44, pp. 483-494, 1985.

[2] B. Mazur, Eigenvalues of Frobenius acting on algebraic varieties over finite fields, AMS Proceedings of Symposia in Pure Mathematics vol 29, 1975 ["Algebraic Geometry, Arcata 1974"]

[3] W. Waterhouse and J. S. Milne, Abelian varieties over finite fields, AMS Proceedings of Symposia in Pure Mathematics vol. 20, 1969.

[4] S. Lang, Elliptic Curves: Diophantine Analysis, Springer 1978.

[5] E. Bach and J. Shallit, Algorithmic Number Theory, vol. 1: Efficient Algorithms, MIT Press 1996.

[6] I. Blake, G. Seroussi, and N. Smart, Elliptic Curves in Cryptography, Cambridge Univ. Press, 1999.