René Schoof's Algorithm for Computing $\sharp E(\mathbb{F}_p)$ for an elliptic curve $E : y^2 \equiv x^3 + A\,x + B \pmod p$

John McGee   Radford University
10-Aug-2007

"A four-year-old child could understand that.
Run out and find me a four-year-old child, I can't make head or tail out of it."
- Groucho Marx (Duck Soup-1933)

René Schoof's 1985 paper entitled "Elliptic curves over finite fields and the computation of square roots mod p", details a polynomial time algorithm for determining $\sharp E(\mathbb{F}_p)$ [3]. The following steps outline Schoof's method.

Let E be an elliptic curve over $\mathbb{F}_p$ given by

(1) $E : y^2 = x^3 + A\,x + B$, where $A, B \in \mathbb{F}_p$.

Hasse's Theorem tells us that the cardinality of the group of points is

(2) $\sharp E(\mathbb{F}_p) = p + 1 - t$, for some t with $|t| \le 2\sqrt{q}$.

Let $\phi_p : E(\overline{\mathbb{F}}_p) \to E(\overline{\mathbb{F}}_p)$ such that $\phi_p((x, y)) = (x^p, y^p)$. Note that this is map of points with coordinates in the algebraic closure of $\mathbb{F}_p$. Then ϕ_p is an endomorphism called the Frobenius map. It has the following property, crucial to Schoof's algorithm [5]

(3) $\phi_p{}^2 - t\,\phi_p + p = 0 \quad \forall\, P \in E(\overline{\mathbb{F}}_q)$

We can use (3) to compute $t \pmod{p_i}$ for a set of L primes $l_1, l_2, \ldots, l_L$ such that

(4) $K = \prod_{i=1}^{L} l_i > 4\sqrt{p}$,

The Chinese Remainder Theorem is then applied to the resulting set of congruences to compute the unique

$t \bmod K$ such that $|t| \le 2\sqrt{q}$.

The order of the group is then given by $\sharp E(\mathbb{F}_q) = q + 1 - t$. Schoof showed that this algorithm will run time proportional to $\log^9 q$, based on analysis of the number of elementary operations required [1,4] Details of the algorithm follow.

The division polynomials ψ_n of an elliptic curve E are elements of $\mathbb{F}_p[x, y]$ with the property that $\psi_n(x, y) = 0$ if and only if $(x, y) \in E[n] = \{P \in E(\overline{\mathbb{F}}_p) \mid n P = \mathcal{O}\}$. These polynomials are defined recursively as follows [5]

$$\psi_0 = 0, \quad \psi_1 = 1, \quad \psi_2 = 2y$$

$$\psi_3 = 3x^4 + 6ax^2 + 12bx - a^2$$

$$\psi_4 = 4y\left(x^6 + 5ax^4 + 20bx^3 - 5a^2x^2 - 4abx - 8b^2 - a^3\right)$$

$$\psi_{2n} = \psi_n\left(\psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2\right) \qquad n \in \mathbb{Z}, n > 2$$

$$\psi_{2n+1} = \psi_{n+2}\psi_n^3 - \psi_{n+1}^3\psi_{n-1} \qquad n \in \mathbb{Z}, n > 1$$

The following polynomials, based on these division polynomials, are used in Schoof's algorithm. Note that during the execution of the algorithm all of the polynomial arithmetic takes place modulo ψ_l for small primes l. Note also that these polynomials turn out to be univariate in x only by computing modulo the relation $y^2 = x^3 + ax + b$. The numbering refers to the equation numbers in [2]. The derivation of these polynomials [2] is based on the point multiplication formula (5).

(5) $$nP = \left(x - \frac{\psi_{n-1}\psi_{n+1}}{\psi_n^2}, \frac{\psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2}{4y\psi_n^3}\right)$$

$$\alpha = \psi_{k+2}\psi_{k-1}^2 - \psi_{k-2}\psi_{k+1}^2 - 4\psi_k^3 y^{p^2+1}$$

$$\beta = 4y\psi_k\left(\psi_k^2\left(x - x^{p^2}\right) - \psi_{k-1}\psi_{k+1}\right)$$

$$p_{16}(x, y) = \left(x^{q^2} - x\right)\psi_k^2 - \psi_{k-1}\psi_{k+1}$$

$$p_{17}(x, y) = (x^p - x)\psi_w^2 - \psi_{w-1}\psi_{w+1}$$

$$p_{18}(x, y) = 4\,\psi_w^3 y^{p+1} - \psi_{w+2}\psi_{w-1}^2 - \psi_{w-2}\psi_{w+1}^2$$

$$p_{19_x}(x, y) = \psi_\tau^{2p}\left(\beta^2\left(\psi_{k-1}\psi_{k+1} - \psi_k^2\left(x^{p^2} + x^p + x\right) + \alpha\psi_k^2\right)\right) + \psi_k^2\beta^2(\psi_{\tau-1}\psi_{\tau-1})^p$$

$$p_{19_y}(x, y) = 4y^p\psi_t^{3p}\left(\alpha\beta^2\left(\psi_k^2\left(2x^{p^2} + x\right) - \psi_{k-1}\psi_{k+1}\right) - \psi_k^2\left(\alpha^3 + \beta^3 y^{p^2}\right)\right) - \beta^3\psi_k^2\left(\psi_{t+2}\psi_{t-1}^2 - \psi_{t-2}\psi_{t+1}^2\right)^p$$

We can now gives the details of Schoof's algorithm for $E : y^2 = x^3 + ax + b$ over $\mathbb{F}_p$ as follows.

1. If $\gcd\left(x^3 + ax + b,\ x^p - x\right) = 1$ then $t \equiv 0 \pmod 2$, else $t \equiv 1 \pmod 2$

2. Create a set of small primes $S = \{l_i\}$ such that $\prod_{i=1}^{L} l_i > 4\sqrt{p}$.

3. Compute the first $L+2$ division polynomials ψ_k.

4. For each $l \in S$, compute $k \equiv p(\bmod l)$

5. If $\gcd(p_{16}, \psi_l) \neq 1$ then there exists $P \in E[l]$ such that $\phi_l^2 P = \pm k P$.

6. If k is not a quadratic residue mod l, then $t \equiv 0 \pmod{l}$ else

7. Compute w such that $w^2 \equiv k \pmod{l}$

8. If $\gcd(p_{17}, \psi_l) = 1$ then $t \equiv 0 \pmod{l}$, else

9. If $\gcd(p_{18}, \psi_l) \neq 1$ then $t \equiv 2w (\bmod l)$, else $t \equiv -2w (\bmod l)$.

10. else we are in case two

11. For each $\tau \leq (l+1)/2$

12. If $\gcd\left(p_{19_x}, \psi_l\right) \neq 1$ then

13. $\phi_p{}^2 + k \equiv \pm \tau \phi_p \pmod{l}$ for some point in $E[l]$ so we test

14. If $\gcd\left(p_{19_y}, \psi_l\right) \neq 1$ then $t \equiv \tau (\bmod l)$ else $t \equiv -\tau \pmod{l}$

15. Next τ

16. Next l

17. At this point we have computed $t \pmod{l_i}$ for all $l_i \in S$,

18. so we can use the Chinese Remainder Theorem to compute

19. $T \equiv t \pmod{N}$ where $N = \prod_{i=1}^{L} l_i$.

20. If T is within Hasse's bounds then $t = T$, else $t \equiv -T (\bmod N)$ and

21. $\# E\left(\mathbb{F}_p\right) = p + 1 - t$.

This completes the description of Schoof's algorithm.

A version of this algorithm has been developed in *Mathematica* [2] and tested for elliptic curves over fields as large as
$\mathbb{F}_p$ with $p \sim$ 10^30.

References

[1] Lercier, R. and Morain, F., *Counting the number of points on elliptic curves over finite fields: strategies and performances*, Advances in Cryptology, Proc. Eurocrypt'95, LNCS 921, L.C. Guillou and J.J. Quisquater, Eds., Springer-Verlag, 1995, pp. 79--94.

[2] McGee, John - *René Schoof's Algorithm for Determining the Order of the Group of Points on an Elliptic Curve over a Finite Field* - Master's Thesis at Virginia Tech

[3] Schoof, René - *Elliptic curves over finite fields and the computation of square roots mod p*, Mathematics of Computation, Vol. 44, No 170 (1985), 482-494

[4] Schoof, René - *Counting points on elliptic curves over finite fields*, Journal de Téorie des Nombres de Bordeaux 7 (1995), 219-254

[5] Washington, Lawrence - *Elliptic Curves - Number Theory and Cryptography*, Chapman & Hall (2003)