Implementation of the Schoof-Atkin-Elkies Algorithm

François Morain
École Polytechnique

March, 7, 1994

[summary by Daniel Augot]

After the definitions introduced in the previous talk, algorithms are presented for computing the number points of an elliptic curve on $\mathbb{F}_p$, $p > 3$ a prime number. Three authors have contributed to the problem, Schoof, Atkin and Elkies. The basic ideas are from Schoof and Atkin, Elkies gives a refinement of Schoof's method. A merge of Elkies and Schoof's methods, due to Atkin, is finally adopted.

1. Elliptic Curves

1.1. Group Law. The abelian group structure of an elliptic curve can be used in cryptography, using the difficulty of the discrete logarithm problem. One has to find a generator, and thus must compute the number of points on the elliptic curve over $\mathbb{F}_p$.

An elliptic curve $E(\mathbf{k})$ over a field $\mathbf{k}$ is defined by its (projective) equation

$$y^2z = x^3 + Axz^2 + Bz^3.$$

The group law on $E(\mathbf{k})$ (restricted to the affine plane) is

$$(x_3, y_3) = (x_1, y_1) + (x_2, y_2).$$

where

$$\begin{cases} x_3 &= \lambda^2 - x_1 - x_2 \\ y_3 &= \lambda(x_1 - x_3) - y_1 \end{cases} \quad \text{and } \lambda = \begin{cases} (y_2 - y_1)(x_2 - x_1)^{-1} \text{ if } x_2 \neq x_1, \\ (3x_1^2 + A)(2y_1)^{-1} \text{ otherwise.} \end{cases}$$

The neutral element if $0_E = (0 : 1 : 0)$; the invariant is $j(E) = 2^8 3^3 \frac{A^3}{4A^3+27B^2}$.

THEOREM 1. *$\#E(\mathbb{F}_p) = p + 1 - t$, $|t| \leq 2\sqrt{p}$. $E(\mathbb{F}_p)$ is isomorphic to $E_1 \times E_2$, where $\#E_1 = m_1$, $\#E_2 = m_2$, $m_1 \mid m_2$ and $m_1 \mid p - 1$.*

1.2. Counting points, old. The "Lang-Trotter" method uses the quadratic character:

$$\#E(\mathbb{F}_p) = p + 1 + \sum_{x=0}^{p-1} \left(\frac{x^3 + Ax + B}{p} \right).$$

The cost of computation is $O(p)$, thus convenient for small p only.

Shanks' technique of "Baby Steps, Giant Steps", valid for general groups, can be applied here, at cost $O(p^{\frac{1}{4}})$.

2. (Full) Schoof

2.1. Division polynomials. One can see that the coordinates of nP can be expressed in terms of polynomials in the coordinates of P a point of the elliptic curve:

$$n(X,Y) = \left(\frac{\phi_n(X,Y)}{\psi_n^2(X,Y)}, \frac{\omega_n(X,Y)}{\psi_n^3(X,Y)}\right).$$

DEFINITION 1. The division polynomial $f_n(X,Y)$ is

$$f_n(X,Y) = \begin{cases} \psi_n(X,Y) & \text{for } n \text{ odd,} \\ \psi_n(X,Y)/(2Y) & \text{for } n \text{ even.} \end{cases}$$

The first division polynomials are $f_{-1} = -1$, $f_0 = 0$, $f_1 = 1$, $f_2 = 1$, $f_3(X,Y) = 3X^4 + 6AX^4 + 12BX - A^2$.

The division polynomials can be computed with recurrence relations. They are in fact univariate polynomials, and their degree is of order $\approx n^2/2$. The points $P = (x,y) \in E$ of order ℓ in $E(\overline{\mathbb{F}_p})$ are the points such that $f_\ell(x) = 0$; these points can be described in the algebra $\mathbb{F}_p[X,Y]/(Y^2 - (X^3 + AX + B), f_\ell(X))$.

THEOREM 2. *Let $E[\ell] = \{P \in \mathbb{P}_2(\overline{\mathbb{F}_p}), \ell P = 0_E\}$ denotes the set of points of ℓ-division. Then $E[\ell]$ is isomorphic to $\mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$.*

2.2. The algorithm. Let $\phi : E \to E$ denote the map $(x,y) \mapsto (x^p, y^p)$. It is known that ϕ satisfies the equation $\phi^2 - t\phi + p = 0$, where t is defined in theorem 1.

One works with the equation

$$\left(X^{p^2}, Y^{p^2}\right) + p\,(X,Y) = t\,(X^p, Y^p),$$

in the field $\mathbb{F}_p[X,Y]/(Y^2 - (X^3 + AX + B), f_\ell(X))$, finding the value of $t \bmod \ell$ by trial and error.

For different values of ℓ, $t \bmod \ell$ is obtained, and t is found by the Chinese remainder theorem, knowing that $|t| \leq 2\sqrt{p}$.

3. Atkin

The trouble with division polynomials is their important degree, $\approx \ell^2/2$ for points of ℓ-division. Atkin's approach does not use the division polynomials, and is related to the modular equation $\Phi_\ell(j(q^\ell), j(q))$.

3.1. The factorization of a modular equation. The (canonical) modular equation for $j(q^\ell)$ is in strong correspondence with the points of ℓ-division.

It is known from the literature that a modular equation $\Phi_\ell(X, j(E))$ admits one of four types of factorization modulo p:

(1) Φ_ℓ factors into s irreducible polynomials of degree r. Then the equation $X^2 - tX + p \equiv 0 \bmod \ell$ has two roots α and β in $\mathbb{F}_{\ell^2} \setminus \mathbb{F}_\ell$, such that the multiplicative order of α/β is r, and $\ell + 1 = rs$;
(2) Φ_ℓ has a factorization of type $(1)(1)(r)\cdots(r)$. Then the equation $X^2 - tX + p \equiv 0 \bmod \ell$ has two roots α and β in $\mathbb{F}_\ell$, such that the multiplicative order of α/β is r, and $\ell - 1 = rs$;
(3) Φ_ℓ has a factorisation of type $(1)(\ell)$. Then $t^2 \equiv 4p \bmod \ell$;
(4) Φ_ℓ has a factorisation of type $(1)^{\ell+1}$, and $t^2 \equiv 4p \bmod \ell^2$.

3.2. Matching. Having computed the equation Φ_ℓ, the type of the factorization of $\Phi_\ell(X, j(E))$ is found by computing $X^p, X^{p^2}, \ldots$ modulo $\Phi_\ell(X, j(E))$, until the degree of the splitting field of $\Phi_\ell(X, j(E))$ is found.

Then values of t are obtained such that the equation $X^2 - tX + p$ has roots corresponding to types of factorization. Note that, for a given ℓ, many values of $t \bmod \ell$ may be found. This is done for several ℓ_i, $i \in [1, n]$ (say), and then a "matching" is done to get the values of $t \bmod \ell_i$, as follows.

Let $K_i = (\prod \ell_j)/\ell_i$, $i \in [1, n]$. Compute and store the values $(p + 1 - \sum_{i=2}^{n} K_i t_i)P$, and compare with $t_1 K_1 P$ for the values at t_1, P being some point of E. This will match for one set of values $t_i \bmod \ell_i$, then t is recovered by the Chinese remainder theorem.

4. Elkies

The idea of Elkies is to work with polynomials $g_\ell(X)$ with lower degree than the ℓ-division polynomials f_ℓ.

4.1. Subsets of points of ℓ-division. We recall that E is isomorphic to $\mathbb{C}/\mathbb{L}(\omega_1, \omega_2)$. Let us consider $x_r = \wp(r\omega_1/\ell)$, for $1 \leq r \leq d = (\ell - 1)/2$. Let p_1 be the sum $p_1 = x_1 + \cdots + x_d$.

THEOREM 3. *The polynomial $g_\ell(X) = \prod_{r=1}^{d}(X - x_r)$ is in $\mathbb{Q}(A, B, p_1)[X]$.*

The polynomial $g_\ell(X)$ obviously divides the division polynomial $f_\ell(X)$; we have the following tower of extensions: $[\mathbb{Q}(A, B, x_1) : \mathbb{Q}(A, B, p_1)] = d$ and $[\mathbb{Q}(A, B, p_1) : \mathbb{Q}(A, B)] = \ell + 1$.

The polynomial $g_\ell(X)$ describes a subset of $E[\ell]$. The following theorem describes what happens modulo p, and states an interesting case of the factorization of $\Phi_\ell(X, j(E))$.

THEOREM 4. (1) *If $\Phi(X, j(E))$ has a root mod p, then $E[\ell]$ has a cyclic subgroup of order ℓ, whose points have coordinates in $\mathbb{F}_p$. This is equivalent to saying that $t^2 - 4p$ is a square mod ℓ.*

(2) *Then if $t^2 - 4p$ is a square mod ℓ, there is at least one 1-dimensional $\mathbb{F}_\ell$-subspace of $E[\ell]$, which is invariant by ϕ, hence $p_1 \in \mathbb{F}_p$, and $g_\ell(X) \in \mathbb{F}_p[X]$.*

In the hypothesis of theorem 4, $g_\ell(X) \in \mathbb{F}_p[X]$, and we search for an eigenvalue k of ϕ, that is, $k \in [1, \ell]$ such that

$$(X^p, Y^p) = k\,(X, Y) \text{ in } \mathbb{F}_p[X, Y]/\left(Y^2 - (X^3 + AX + B), g_\ell(X)\right).$$

This gives an unique value of $t \bmod \ell$, namely $t \equiv (k^2 + p)/k \bmod \ell$.

4.2. The whole algorithm. The main steps of the algorithm are

(1) Compute *a* modular equation $\Phi_\ell(F, J)$, where F is a function on $\Gamma_0(\ell)$ (may not be the canonical modular equation).

(2) **If** $\Phi_\ell(F, j(E)) \bmod p$ has at least one root **then** *(Elkies' way)*
   (a) compute a factor $g_\ell(X)$ of $f_\ell(X)$ modulo p, having degree $d = (\ell - 1)/2$.
   (b) fink k such that $(X^p, Y^p) = k(X, Y)$ in $\mathbb{F}_p[X, Y]/\left(Y^2 - (X^3 + AX + B), g_\ell(X)\right)$, and deduce $t \equiv (k^2 + p)/k \bmod \ell$.

   else *(Atkin's way)* $\lambda^2 - t\lambda + p \equiv 0 \bmod \ell$ has two roots α and β such that α/β has order r, r defined by the splitting of $\Phi(F, j(E)) \bmod p$ into r' factors of degree r, with $rr' = \ell + 1$. Eventually do some "matching", and deduce the value of $t \bmod \ell$.

Atkin has described an ingenious way for computing p_1, and the value of $g_\ell(X)$.

5. Conclusion

The implementation is now using fast polynomial arithmetic, which has proven to be superior. The operations includes fast multiplication (with FFT, done by R. Lercier), fast division, gcd, ...

Modular equations for $\ell \leq 500$ can be found, with Chinese remainder theorem on 64 bits. Two curves are studied as examples:

- the INRIA curve: $y^2 = x^3 + 105x + 78153$;
- the POLYTECHNIQUE curve: $y^2 = x^3 + 4589x + 91128$.

Morain's record is POLYTECHNIQUE for a prime of 350 digits, using improvements of Couveignes, for computing values of $t \mod l^n$.

Bibliography

[1] Morain (François). – Calcul du nombre de points sur une courbe elliptique dans un corps fini : aspects algorithmiques. – March 1994. Submitted for publication of the Actes des Journées Arithmétiques 1993.

[2] Schoof (R.). – Elliptic curves over finite fields and the computation of square roots mod p. *Mathematics of Computation*, vol. 44, 1985, pp. 483–494.

[3] Schoof (René). – Counting points on elliptic curves over finite fields. – February 1994. Submitted for publication of the Actes des Journées Arithmétiques 1993.