Schoof’s Algorithm (Basic Ideas)

Given: An elliptic curve $E: y^2 = f(x)$ over $\mathbb{F}_q$, $q = p^r$.

Find: $\#E(\mathbb{F}_q)$ or, equivalently, $a_E = q + 1 - \#E(\mathbb{F}_q)$.

First reduction: By Hasse’s theorem and the Chinese Remainder Theorem it is enough to determine $a_E \pmod{\ell}$, for all primes $\ell \leq B$, where $B$ is such that $\prod_{\ell \leq B} \ell > 4\sqrt{q}$.

Thus: We need to consider only primes $\ell$ with $\ell = O(\log q)$.

Main Idea: For each $\ell$, consider the action of Frobenius $\varphi = \varphi_q$ on the group

$$E[\ell] = \{ P \in E(\overline{\mathbb{F}}_q) : \ell P = O \},$$

where $\overline{\mathbb{F}}_q$ denotes the algebraic closure of $\mathbb{F}_q$. This action is given by

$$\varphi_q((x, y)) = (x^q, y^q).$$

Basic fact: If $\ell \neq p$, then $\varphi_q : E[\ell] \rightarrow E[\ell]$ is an $\mathbb{F}_\ell$-linear map with characteristic polynomial

$$ch(t) = X^2 - a_E X + q \in \mathbb{F}_\ell[X];$$

in particular (by Cayley-Hamilton) we have $\varphi^2 - q \text{id} = a_E \varphi$. This leads to the following

Strategy: Test successively $t = 0, 1, \ldots, \ell - 1$ to find a $t$ for which

$$(1) \quad \varphi^2 - q \text{id} = t\varphi \quad \text{on} \ E[\ell].$$
To test that condition (1) holds, use the following:

**Fact:** For each (odd) \( n \), there is a polynomial \( \psi_n(X) \in \mathbb{F}_q[X] \) of degree \((n^2 - 1)/2\) such that:

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

Moreover, this polynomial \( \psi_n(X) \) (called the \( n \)-th division polynomial of \( E \)) can be computed recursively.

**Example:** If \( E : y^2 = x^3 + ax + b \), then

\[
\psi_3(X) = 3X^4 + 6ax^2 + 12bX - a^2.
\]

**Thus:** Condition (1) can be translated into the following polynomial identity/congruence:

\[
(X^{q^2}, Y^{q^2}) - [q](X, Y) = [t](X^q, Y^q) \mod (\psi_\ell, Y^2 - f(X)).
\]

**Note:** In the above, \([q](X, Y)\), the \( q \)-th multiple of the (abstract) point \((X, Y)\), is computed by the addition law on the elliptic curve (and hence is actually a pair of rational functions in \(X, Y\)), and the same is true for \([t](X^q, Y^q)\). Moreover, the \(-\) in the above expression is subtraction on the elliptic curve.

**Main difficulty:** The degree of \( \psi_\ell \) is quite large, and grows quadratically with \( \ell \).

For example, if \( q \approx 10^{200} \approx 2^{650} \), then we need \( \ell \approx 250 \); in this case \( \deg(\psi_\ell) \approx 250^2/2 = 31,250 \).

**Remark:** The refinements of Schoof’s Algorithm (due to N. Elkies and A. Atkins) avoid the use of the division polynomials and use instead certain polynomials of degree \( \approx \ell \).