Corrections to Schoof 85

Nick Alexander
Janice Tytaneck

January 18, 2004

This document is meant to be a substitute for page 489 of Rene Schoof’s 1985 paper, *Elliptic Curves Over Finite Fields and the Computation of Roots mod p*. The motivation for this document is the number of typographical errors in Schoof’s original work. Corrections are noted in boldface. No responsibility is taken for the accuracy of this work!

• p. 488, middle (paragraph after equation (16):

If this gcd \( \not= 1 \) 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 \( \tau \not= 0 \) in (12). In testing (12) for their values of \( \tau \), we can, when adding \( \phi_l^2 (x, y) \) and \( q(x, y) \), apply the version of the addition formula 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 \( \phi_l^3 P = \pm qP \). If \( \phi_l^2 P = -qP \), for some nonzero \( P \), we have by (3) that \( t \phi_l P = 0 \), whence, since \( \phi_l P \not= 0 \), that \( t \equiv 0 \) (mod \( l \)). If \( \phi_l^2 P = qP \) for some nonzero \( P \) we have by (3) that

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

• p. 488, bottom (no corrections, but included for completeness since the text continues in the next box):

If

\[
\gcd \left( (X^q - X)f_w^2(X)(X^3 + AX + B) + f_{w-1}(X)f_{w+1}(X), f_l(X) \right) \quad (w \text{ even}),
\]

\[
\gcd \left( (X^q - X)f_w^2(X) + f_{w-1}(X)f_{w+1}(X)(X^3 + AX + B), f_l(X) \right) \quad (w \text{ odd})
\]

• p. 489, top:
the details; testing whether $f$ polynomials modulo $w$ of the relations $(12)$. In a way analogous to the computations above one can test, by computations in $\mathbb{F}_q[X]$ using (19) and, if necessary, by dividing the expressions by $Y$. The result is a polynomial $F(Y)$ and $f$ are zero mod $(19)$. Note that the denominator of $\lambda$ does not vanish on $E[l]$ since $\Psi_k$ has no zeros on $E[l]$ and since we are in Case 2. Let $\tau \in \mathbb{Z}$ with $0 < \tau < l$; we have

$$\tau \phi_t P = \left( x^q - \left( \frac{\Psi_{\tau+1} \Psi_{\tau-1}}{\Psi_{\tau}^2} \right) \right)^q \left( \Psi_{\tau+2} \Psi_{\tau-1}^2 - \Psi_{\tau-2} \Psi_{\tau+1}^2 \right)^q.$$}

In a way analogous to the computations above one can test, by computations in $\mathbb{F}_q[X]$, which of the relations $(12)$ 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 $\phi_t^2 + q = \tau \phi_t$ holds on $E[l]$ boils down to testing whether

$$\left( \left( \Psi_{k-1} \Psi_{k+1} - \Psi_k^2 \left( X^q + X^q + X \right) \right) \right)$$

are zero mod $f_l(X)$. Here

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

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

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