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 $\neq 1$ 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 $\tau \neq 0$ in **(12)**. In testing **(12)** for ther values of τ, 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 $\phi_l^2 P = \pm qP$. If $\phi_l^2 P = -qP$, for some nonzero P, we have by (3) that $t\phi_l P = 0$, whence, since $\phi_l P \neq 0$, that $t \equiv 0 \pmod{l}$. 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
>
> $$\text{(17)} \quad \begin{array}{l} \gcd\left((X^q - X)f_w^2(X)(X^3 + AX + B) + f_{w-1}(X)f_{w+1}(X), f_l(X)\right) \text{ (w even)}, \\ \gcd\left((X^q - X)f_w^2(X) + f_{w-1}(X)f_{w+1}(X)(X^3 + AX + B), f_l(X)\right) \text{ (w odd)} \end{array}$$

- p. 489, top:

equals 1, we have that $t \equiv 0 \pmod{l}$ otherwise, if

$$(18)\quad \begin{array}{l} \gcd\left(4(X^3+AX+B)^{(q-1)/2} f_w^3(X) - f_{w+2}(X) f_{w-1}^{\mathbf{2}}(X) + f_{w-2}(X) f_{w+1}^{\mathbf{2}}(X), f_l(X)\right), \\ \gcd\left(4(X^3+AX+B)^{(q+3)/2} f_w^3(X) - f_{w+2}(X) f_{w-1}^{\mathbf{2}}(X) + f_{w-2}(X) f_{w+1}^{\mathbf{2}}(X), f_l(X)\right) \end{array}$$

(for w **odd**, resp. **even**) equals 1, we have that $t \equiv -2w \pmod{l}$ else $t \equiv 2w \pmod{l}$.

Case 2. This is the case where we know that $\phi_l^2 P$ and qP are neither equal nor opposite for any $P \in E[l]$. In this case we will test which of the relations (**12**) holds with $\tau \in \mathbb{Z}/l\mathbb{Z}^x$. We have with $P = (x, y)$ and $k \equiv q \pmod{l}$ and $0 < k < l$, that

$$\phi_l^2 P + qP = \left(-x^{q^2} - x + \frac{\Psi_{k-1}\Psi_{k+1}}{\Psi_k^2} + \lambda^2, -y^{q^2} - \lambda\left(-2x^{q^2} - x + \frac{\Psi_{k-1}\Psi_{k+1}}{\Psi_k^2} \boldsymbol{+\lambda^2}\right)\right),$$

where

$$\lambda = \frac{\Psi_{k+2}\Psi_{k-1}^2 - \Psi_{k-2}\Psi_{k+1}^2 - 4y^{q^2+1}\Psi_k^3}{4\Psi_k y\left(\left(x - x^{q^2}\right)\Psi_k^2 - \Psi_{k-1}\Psi_{k+1}\right)}.$$

Note that the denominator of λ does not vanish on $E[l]$ since Ψ_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

$$\tau\phi_l P = \left(x^q - \left(\frac{\Psi_{\tau+1}\Psi_{\tau-1}}{\Psi_\tau^2}\right)^q, \left(\frac{\Psi_{\tau+2}\Psi_{\tau-1}^2 - \Psi_{\tau-2}\Psi_{\tau+1}^2}{4y\Psi_\tau^3}\right)^q\right).$$

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 $\phi_l^2 + q = \tau\phi_l$ holds on $E[l]$ boils down to testing whether

$$(19)\quad \begin{array}{r} \left(\left(\Psi_{k-1}\Psi_{k+1} - \Psi_k^{\mathbf{2}}\left(X^{q^2} + X^q + X\right)\right)\beta^2 + \Psi_k^2\alpha^2\right)\Psi_\tau^{2q} + \Psi_{\tau-1}^q\Psi_{\tau+1}^q\beta^2\Psi_k^2 \text{ and,} \\ 4Y^q\Psi_\tau^{3q}\left(\alpha\left(\left(2X^{q^2} + X\right)\boldsymbol{\beta^2}\Psi_k^2 - \Psi_{k-1}\Psi_{k+1}\boldsymbol{\beta^2 + \Psi_k^2\alpha^2}\right) - Y^{q^2}\beta^{\mathbf{3}}\Psi_k^2\right) \\ -\beta^{\mathbf{3}}\Psi_k^2\left(\Psi_{\tau+2}\Psi_{\tau-1}^2 - \Psi_{\tau-2}\Psi_{\tau+1}^2\right)^q \end{array}$$

are zero mod $f_l(X)$. Here

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

and

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

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 $F_q[X]$. This completes the description of the second step of our algorithm.