

## Algorithms for Finite Fields

October 3, 2006

Notes by: Mark Rothlisberger

We will apply Schoof's algorithm, previously discussed, to compute the number of points of  $y^2 = x^3 + 1$  over  $\mathbb{F}_5$  and  $\mathbb{F}_7$ .

### 1. SCHOOF'S ALGORITHM

Recall the following:  $\#E(\mathbb{F}_q) = q + 1 - t$ , where  $|t| \leq 2q^{1/2}$ . Furthermore, if

$$(x^{q^2}, y^{q^2}) + [q](x, y) = \tau(x^q, y^q)$$

in  $E[\ell]$  for some  $\ell$ , then  $t \equiv \tau \pmod{\ell}$ .

We have defined the Frobenius morphism, for  $P = (x, y)$ , to be  $Fr(P) = (x^q, y^q)$ , and so the previous equation could also be written, for  $P \in E[\ell]$ ,  $P \neq 0$ , that  $Fr^2(P) + qP = \tau Fr(P)$ .

If  $P \in E[\ell] \cap E(\mathbb{F}_q)$ ,  $P \neq 0$ , then  $Fr(P) = P$  and  $Fr^2(P) = P$ , so in calculations we will check to see if  $P + qP = \tau P$ , i.e.  $\tau \equiv (q + 1) \pmod{\ell}$ , or  $t \equiv (q + 1) \pmod{\ell}$ . This is the same as saying that if  $E(\mathbb{F}_q)$  has a point of order  $\ell$ , then  $\ell | \#E(\mathbb{F}_q)$ .

With our given curve,  $y^2 = x^3 + 1$ , it is trivial to see that  $(-1, 0) \in E[2]$  and  $(0, 1) \in E[3]$ . Also, since  $t \equiv (q + 1) \pmod{6}$ , if  $q = 5$ , then  $t \equiv 6 \equiv 0 \pmod{6}$ . Since  $|t| \leq 2\sqrt{5}$ , this implies that  $t = 0$ , so  $y^2 = x^3 + 1$  has six points over  $\mathbb{F}_5$ , including the point at infinity. Note, of course, that there are other ways to calculate the number of points of this curve over  $\mathbb{F}_5$ .

However, things become less trivial over  $\mathbb{F}_7$ : When  $q = 7$ , then  $t \equiv 8 \equiv 2 \pmod{6}$ . Since  $|t| \leq \lfloor 2\sqrt{7} \rfloor$ , it follows that  $t = 2$  or  $t = -4 \equiv 3 \pmod{7}$ . This means that we can't decide between these options just considering points mod 2 and mod 3, so we must attempt to calculate  $t \pmod{5}$ , which requires that we work in  $E[5]$ . (Note that  $\#E[5] = 25$ , including one zero point). It is too cumbersome to carry out these calculations by hand, so we resort to a Pari script, which can be found at <http://www.ma.utexas.edu/users/voloch/FFnotes/schoof.gp>.

### 2. NOTES ABOUT THE PARI SCRIPT

Note that

$$5(x, y) = \left( \frac{u_5(x)}{f_5(x)^2}, \frac{v_5(x)}{f_5(x)^3 y} \right),$$

and by reading the denominators in the output of the script, we see that  $\deg f_5(x) = 12$ ; its roots are the  $x$ -coordinates of the non-zero points of  $E[5]$ . We can check that  $f_5$  is irreducible mod 7.

As a matter of notation, the script has a variable  $a$ , which is given by  $a = \bar{t} \in \mathbb{F}_7[t]/(f_5(t)) = \mathbb{F}_{7^{12}}$ , which gives some indication of why it would be unreasonable to carry out these calculations by hand.

Furthermore,  $P = (a, v) \in E[5]$ , where  $v = \sqrt{a^3 + 1}$ . So  $v = \bar{x}$ , the image of  $x$  in the field  $\mathbb{F}_{7^{12}}[x]/(x^2 - (a^3 + 1)) = \mathbb{F}_{7^{24}}$ .

After running the script, we find that  $t \equiv 1 \pmod{5}$ , which allows us to decide that  $t = -4$ .

Now we know  $t \pmod{30}$ . Moreover, this will work not only for 7: For any prime  $q$  such that  $4\sqrt{q} < 30$ , or, solving for  $q$ , for any prime  $q < 50$ . we can find  $t$  once we know  $t \pmod{2}$ ,  $t \pmod{3}$ , and  $t \pmod{5}$ .

## 3. INCIDENTAL COMMENTS

There is one point to consider that is incidental to the calculation: one step includes factoring a polynomial with integer coefficients. How do we do this?

Note that

$$\begin{aligned} f(x) &= f_1 \cdots f_r && \in \mathbb{Z}[x] \\ f(x) &\equiv g_1 \cdots g_k \pmod{p} && \in \mathbb{F}_p[x], \end{aligned}$$

We can factor in  $\mathbb{F}_p[x]$ , but we don't know how to lift factorizations to  $\mathbb{Z}[x]$ , besides trying all combinations. Applying Hensel's lemma allows us to find the factorization mod  $p^n$ , given the factorization mod  $p$ , for all  $n$ . This provides congruences modulo  $p^n$  for the coefficients of the unknown  $f_i$ . However, this isn't quite enough. Additionally, we must infer a bound for the size of the coefficients of the  $f_i$ , based on the size of the coefficients of  $f$ . To find such a bound, we must use the Mahler measure, specifically the property that  $\mu(fg) = \mu(f)\mu(g)$ , and the fact that there are bounds for the coefficients based on the Mahler measure.