Stepanov's Method for Elliptic Curves

March 28, 2007

Consider the points $(x, y) \in \mathbb{F}_p \times \mathbb{F}_p$ on the curve

$$y^2 \;=\; f(x) \;:=\; x^3 + ax + b.$$

Hasse's and Weil's theorems imply that the number of such pairs (x, y) is

$$p + O(\sqrt{p}),$$

which is equivalent to saying that

$$|\{x \;:\; f(x) = y^2, \text{ for some y}\}| \;=\; \frac{p}{2} + O(\sqrt{p}).$$

(Actually, they give the sharper upper bound $2\sqrt{p}$ on the size of the error term.)

Let

$$g_1(x) \;:=\; f(x)^{(p-1)/2} - 1,\; g_2(x) \;:=\; f(x)^{(p-1)/2} + 1.$$

Then, to prove our theorem, it suffices to show that both $g_1(x)$ and $g_2(x)$ have at most $p/2 + O(\sqrt{p})$ roots mod p; and, to prove this, we will produce polynomials $r_1(x)$ and $r_2(x)$ such that

$$\deg(r_i(x)) \;\leq\; \frac{pM}{2} + O(M\sqrt{p}),$$

and $r_i(x)$ vanishes to order M at all the mod p roots of $g_i(x)$, at least when

$$M \;\sim\; c\sqrt{p}.$$

Since the case of producing $r_1(x)$ is nearly identical to that of producing $r_2(x)$, we will just work with $r(x) := r_1(x)$ and $g(x) := g_1(x)$.

1 The polynomial $r(x)$

We will try to find $r(x)$ having the special form

$$r(x) \;=\; f(x)^M(g(x)U(x)+V(x)),$$

where $U(x)$ and $V(x)$ are polynomials of degree about $Mp/2$. Notice that if we can find such an $r(x)$, we will get that for $M \sim c\sqrt{p}$,

$$\deg(r(x)) \;\lesssim\; 3M + \frac{3(p-1)}{2} + Mp/2 \;=\; \frac{Mp}{2} + O(M\sqrt{p}), \tag{1}$$

just as we need.

The reason for choosing this form for $r(x)$, especially the factor $f(x)^M$ out front, is that it allows us to take advantage of the fact that $g(x)$ is one less than a high power of $f(x)$. Roughy, the reason this is so is that in the middle of our calculations of the successive derivatives of $r(x)$, we will need to simplify expressions of the type $f(x)^{M-j}g'(x)$; and, these simplifications can be carried out as follows

$$\begin{aligned} f(x)^{M-j}g'(x) &= f(x)^{M-j}f(x)^{(p-3)/2}f'(x)(p-1)/2 \\ &= f(x)^{M-j-1}f(x)^{(p-1)/2}f'(x)(p-1)/2 \\ &= f(x)^{M-j-1}(g(x)+1)f'(x)(p-1)/2. \end{aligned}$$

It follows (after some work), that if $r(x)$ has the above form, then its successive derivatives take the form

$$\frac{d^j r(x)}{dx^j} \;=\; f(x)^{M-j}(g(x)U_j(x)+V_j(x)), \tag{2}$$

where $U_j(x)$ and $V_j(x)$ are polynomials of degree at most

$$\deg(U(x))+2j \;=\; \deg(V(x))+2j. \tag{3}$$

In order that $r(x)$ vanish to order M at all mod p roots of $g(x)$, it suffices to require [1]

$$\text{For all } j=0,1,...,M-1,\; \frac{d^j r(x)}{dx^j} \;\equiv\; 0 \pmod{p, x^p-x, g(x)}.$$

[1] Note that the ideal $(p, g(x), x^p-x)$ is the same as $(p, \Pi(x))$, where $\Pi(x)$ is the product $(x-\xi)$ over all the mod p roots ξ of $g(x)$.

One thing that would guarantee this is

$$\text{For all } j = 0, 1, ..., M-1,\ V_j(x) \ \equiv\ 0 \pmod{p, x^p - x}. \tag{4}$$

If we consider the single congruence

$$V_j(x) \ \equiv\ 0 \pmod{p, x^p - x},$$

we note that since the coefficients of V_j are linear combinations of the coefficients of $U(x)$ and $V(x)$, this single congruence determines p different linear equations in these coefficients of U and V. [2] So, in total, the M congruences determines Mp linear equations in the coefficients of U and V. These equations are homogeneous; and so, as long as the number of coefficients exceeds the number of equations, we are guaranteed a solution to (4).

Since the U and V have degree about $Mp/2$, the number of free coefficients in both U and V is about Mp, and in fact can be made a tiny bit bigger, so that all the V_j vanish mod $p, x^p - x$.

2 We are done, right ?

It would seem that this finishes the proof of our theorem; however, one thing that could happen, which is what makes the proof a little more complicated, is that we could have

$$g(x)U(x) + V(x) \ =\ 0, \tag{5}$$

even though the coefficients of U and V are not identically 0. For example, we could have $U(x) = x^p - x$ and $V(x) = -(x^p - x)g(x)$.

The way to keep this from happening is to restrict U and V to have a very special form, which disallows (5). You might think that by restricting U and V to have a special form, we would have fewer free coefficients to play with in our proof, and so we would not be able to satisfy all the Mp linear equations, and you'd be right if indeed we had Mp linear equations; however, it will turn out that the special form we work with will involve U and V having about $Mp/4$ free parameters each, or about $Mp/2$ in total, while the number of linear equations will only be $Mp/2$, not Mp as we had before.

[2] The reason it is p linear equations, and not $\deg(V_j)$ linear equations is that when we mod out by $x^p - x$ we are left with a polynomial of degree smaller than p.

Basically, what we do is choose U and V so that the highest power in $g(x)U(x)$ cannot be congruent mod p to the highest power in $V(x)$. One way to do this is require all the powers of x in both $U(x)$ and $V(x)$ to lie in the interval $[0,(p-5)/2]$ modulo p. For then, since the highest power of

$$g(x) \;=\; f(x)^{(p-1)/2} - 1$$

is $3(p-1)/2$, we have that the higest power of x in $g(x)U(x)$ must lie in the mod p interval

$$\frac{3(p-1)}{2} + [0,(p-5)/2] \;\equiv\; [(p-3)/2, p-4] \pmod{p},$$

while the highest power of x in $V(x)$ lies in the mod p interval $[0,(p-5)/2]$. It follows that

$$g(x)U(x) - V(x) \;\neq\; 0,$$

so long as $U(x)$ and $V(x)$ are not identically 0.

Another way of expressing the fact that all the powers of U and V lie in $[0,(p-5)/2]$ modulo p is to say that U and V have the following forms:

$$U(x) \;=\; k_0(x) + x^p k_1(x) + x^{2p} k_2(x) + \cdots + x^{Np} k_N(x),$$

and

$$V(x) \;=\; \ell_0(x) + x^p \ell_1(x) + x^{2p} \ell_2(x) + \cdots + x^{Np} \ell_N(x),$$

where

$$N \;=\; [M/2] + 2;\ \text{and, for } i = 0, ..., N,\ \deg(k_i),\ \deg(\ell_i) \leq \frac{(p-5)}{2}.$$

3 The Proof Proper

Even though we have restricted U and V to have the special form above, we still have that (1), (2) and (3), all hold. The final extra detail we need in order to complete our proof is to show that $V_j(x)$ mod $x^p - x$ (and p) has degree at most about $p/2$. If so, we will have only about half as many linear equations as we had before, which is good, since we also have only about half

the number of free coefficients in our $U(x)$ and $V(x)$ of special form. We will need to understand better what form $V_j(x)$ takes: First,

$$\begin{aligned} r'(x) &= Mf(x)^{M-1}f'(x)(g(x)U(x)+V(x)) \\ &\quad + f(x)^M(U'(x)g(x)+g'(x)U(x)+V'(x)). \end{aligned}$$

Using the aforementioned fact

$$f(x)^M g'(x) = f(x)^{M-1}(g(x)+1)f'(x)(p-1)/2,$$

we find that

$$r'(x) = f(x)^{M-1}(g(x)U_1(x)+V_1(x)),$$

where

$$V_1(x) = Mf'(x)V(x)+f'(x)U(x)(p-1)/2+f(x)V'(x).$$

So, the powers of x that appear in $V_1(x)$ will lie in the interval $[0,(p-5)/2+2] = [0,(p-1)/2]$ modulo p, [3] which means on modding out by x^p-x they will lie in $[0,(p-1)/2+N]$; and, in general, one can show that the powers of x that appear in $V_j(x)$ upon modding out by x^p-x, will lie in

$$[0,(p-5)/2+2j+N] \text{ modulo } p.$$

Having all the $V_j(x)$ be congruent to $0 \pmod{p, x^p-x}$ then gives us a system of

$$\sum_{j=0}^{M-1}((p-3)/2+2j+N) = \frac{M(p-3)}{2}+M(M-1)+MN.$$

homogeneous linear equations. Fortunately, the number of free variables we have among the $k_i(x)$ and $\ell_i(x)$ that make up $U(x)$ and $V(x)$ is

$$2(N+1)(p-3)/2 > \frac{M(p-3)}{2}+M(M-1)+MN,$$

for $M \sim \sqrt{p}/2$. So, the homogeneous system of equations can be satisfied, and our theorem is proved.

[3] Note that the powers appearing in $V'(x)$ lie in $[0,(p-7)/2]$ mod p, not $[-1,(p-7)/2]$, because the derivative of terms cx^{kp} is 0 mod p.