Notes on elliptic curves over finite fields.

Kevin Buzzard

February 7, 2012

Last modified 16/01/2004.

Just a few notes on elliptic curves over finite fields. Let k be a fixed finite field, of cardinality $q = p^f$. If E/k is an elliptic curve, then $\#E(k) = 1 + q - a$ where $a = a(E)$ is an integer which tells you a lot about E (note that $a^2 \leq 4q$, and equality really can occur). For example if $l \neq p$ is a prime then the l-adic Tate module of E has an action of Frobenius with characteristic polynomial $X^2 - aX + q$. Because of this, and the Tate conjecture or whatever, which is certainly a theorem in this setting, two elliptic curves E and F over k are isogenous iff $a(E) = a(F)$.

The number a tells you the number of k-points of E. It also tells you the number of k'-points for k' any finite extension of k, for the following reason: if k' is an extension of k of degree n then Frobenius on the l-adic Tate module of E/k' is just the n'th power of Frobenius on the Tate module of E/k. Hence if α and β are the roots of $X^2 - aX + q$ then

$$\#E(k') = 1 + q^n - \alpha^n - \beta^n.$$

An elliptic curve is *supersingular* if it has no point of order p over $\overline{k}$, that is, if $\#E(k')$ is prime to p for all finite extensions k' of k. One checks easily that this is true iff a is prime to p.

Given an integer a with $a^2 \leq 4q$, is there an elliptic curve over k with $a = a(E)$? I don't think so! In fact I guess I can prove that this isn't the case. It's true if $p \nmid a$ or if $a^2 = 4q$, and probably in some other cases too. But I think that in the general case there is trouble. Here's why.

Let a be an arbitrary integer with $a^2 \leq 4q$. Let π be a root of $X^2 - aX + q$. Then either π is a quadratic irrational with norm $\sqrt{q}$, or $q = p^f = p^{2g} = r^2$ is the square of an integer and $a = \pm 2r$ and $\pi = \pm r = \pm p^g$. In either case, Theorem 5.1(c) of Milne's Corvalis article (where he explains Honda-Tate theory) applies, and we deduce the existence of a simple abelian variety $A = A_\pi$ with some property or other. What's the dimension of this variety? One has to do two calculations, which I'll sketch here.

Easy case: $a^2 = 4q$. Then $f = 2g$ is even, $q = p^{2g} = r^2$ with $r = p^g$, and $a = \pm 2r$, so $\pi = \pm r$. By Milne Theorem 5.1(a) we have $\mathbf{Q}(\pi) = \mathbf{Q}$, and e is the least common multiple of 2 and 2, so it's 2. Hence the dimension of A is 1, and A is a supersingular elliptic curve over k with either as few points as possible, or as many as possible, depending on the sign of a. Note that one of these forms will be a quadratic twist of the other, at least if $p > 2$. Note also that the endomorphism ring of A *over* k is already an order in the quaternion algebra over $\mathbf{Q}$ of discriminant p.

Messier case: $|a| < 2\sqrt{q}$. Then π is a quadratic irrational, so $\mathbf{Q}(\pi)$ is an imaginary quadratic field $\mathbf{Q}(\sqrt{a^2 - 4q})$.

The subcase we're interested in is when a is prime to p. Then $\pi\overline{\pi} = q$ and $\pi + \overline{\pi} = a$ so π and $\overline{\pi}$ are coprime. Because $\mathbf{Q}(\pi)$ is imaginary quadratic and $|\pi| > 1$, π can't be a unit. An easy check now shows that p must split in $\mathbf{Q}(\pi)$, and π is coprime to one of the primes above p, but $\pi = v^f$ for the other one. Milne's result about invariants of division algebras shows that the invariants of the division algebra $End(A)$ are all integers, so $E = \mathbf{Q}$, so $e = 1$ (in Milne's notation) and A is 1-dimensional and hence an elliptic curve, and the endomorphism ring is an order in an imaginary quadratic field.

Perhaps one can do something when $q|a^2$ in some cases (I think p has to not split in this case if one wants an elliptic curve?). But here is an example to show that there can be problems in general: consider $q = p^{10}$ and $a = p^2$. Then π is a root of $X^2 - p^2X + p^{10}$ so the slopes of π are 2 and 8, so p splits, and the ords of π wrt the two primes above p are 2 and 8, and the ord of q is 10, so the invariants of the division algebra are 1/5 and 4/5 and it has dimension 25. So A is 5-dimensional.

Note that if $q|a^2$ then one could get examples of supersingular elliptic curves where the endomorphism ring gets bigger if one extends the ground field. For example if $a = 0$ and q is an odd power of p then $\mathbf{Q}(\pi) = \mathbf{Q}(\sqrt{-p})$ and in this case I guess we have a supersingular elliptic curve whose endomorphism ring over the ground field is just an order in an imaginary quadratic field.