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 any finite extension $k'$ 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 $\alpha$ and $\beta$ are the roots of $X^2 - aX + q$ then

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

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

The subcase we’re interested in is when $a$ is prime to $p$. Then $\pi \overline{\pi} = q$ and $\pi + \overline{\pi} = a$ so $\pi$ and $\overline{\pi}$ are coprime. Because $Q(\pi)$ is imaginary quadratic and $|\pi| > 1$, $\pi$ can’t be a unit. An easy check now shows that $p$ must split in $Q(\pi)$, and $\pi$ is coprime to one of the primes above $p$, but $\pi = \nu^j$ 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 $E = Q$, so $c = 1$ (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 $\pi$ is a root of $X^2 - p^2X + p^{10}$ so the slopes of $\pi$ are 2 and 8, so $p$ splits, and the ords of $\pi$ 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 $Q(\pi) = Q(\sqrt{-p})$ 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.