Elliptic curves over a finite field. For the rest of this section we shall let K be the finite field $\mathbf{F}_q$ of $q = p^r$ elements. Let E be an elliptic curve defined over $\mathbf{F}_q$. If $p = 2$ or 3, then E is given by an equation of the form (2) or (3), respectively.

It is easy to see that an elliptic curve can have at most $2q+1$ $\mathbf{F}_q$-points, i.e., the point at infinity along with $2q$ pairs (x, y) with $x, y \in \mathbf{F}_q$ which satisfy (1) (or (2) or (3) if $p = 2$ or 3). Namely, for each of the q possible x's there are at most 2 y's which satisfy (1).

But since only half of the elements of $\mathbf{F}_q^*$ have square roots, one would expect (if $x^3 + ax + b$ were random elements of the field) that there would be only about half that number of $\mathbf{F}_q$-points. More precisely, let χ be the quadratic character of $\mathbf{F}_q$. This is the map which takes $x \in \mathbf{F}_q^*$ to ± 1 depending on whether or not x has a square root in $\mathbf{F}_q$ (and we take $\chi(0) = 0$). For example, if $q = p$ is a prime, then $\chi(x) = (\frac{x}{p})$ is the Legendre symbol (see § II.2). Thus, in all cases the number of solutions $y \in \mathbf{F}_q$ to the equation $y^2 = u$ is equal to $1 + \chi(u)$, and so the number of solutions to (1) (counting the point at infinity) is

$$1 + \sum_{x \in \mathbf{F}_q} (1 + \chi(x^3 + ax + b)) = q + 1 + \sum_{x \in \mathbf{F}_q} \chi(x^3 + ax + b). \qquad (6)$$

We would expect that $\chi(x^3+ax+b)$ would be equally likely to be $+1$ and -1. Taking the sum is much like a "random walk": toss a coin q times, moving one step forward for heads, one step backward for tails. In probability theory one computes that the net distance traveled after q tosses is of the order of $\sqrt{q}$. The sum $\sum \chi(x^3 + ax + b)$ behaves a little like a random walk. More precisely, one finds that this sum is bounded by $2\sqrt{q}$. This result is Hasse's Theorem; for a proof, see § V.1 of Silverman's book on elliptic curves cited in the references.

Hasse's Theorem. *Let N be the number of $\mathbf{F}_q$-points on an elliptic curve defined over $\mathbf{F}_q$. Then*

$$|N - (q + 1)| \leq 2\sqrt{q}.$$

In addition to the number N of elements on an elliptic curve defined over $\mathbf{F}_q$, we might want to know the actual structure of the abelian group. This abelian group is not necessarily cyclic, but it can be shown that it is always a product of two cyclic groups. This means that it is isomorphic to a product of p-primary groups of the form $\mathbf{Z}/p^\alpha\mathbf{Z} \times \mathbf{Z}/p^\beta\mathbf{Z}$, where the product is taken over primes dividing N (here $\alpha \geq 1$, $\beta \geq 0$). By the *type* of the abelian group of $\mathbf{F}_q$-points on E, we mean a listing $(\ldots, p^\alpha, p^\beta, \ldots)_{p|N}$ of the orders of the cyclic p-primary factors (we omit p^β when $\beta = 0$). It is not always easy to find the type.

Example 4. Find the type of $y^2 = x^3 - x$ over $\mathbf{F}_{71}$.

Solution. We first find the number of points N. In (6) we notice that in the sum the term for x and the term for $-x$ cancel, because