LECTURE 16, MONDAY 05.04.04

FRANZ LEMMERMEYER

1. Applications of Nagell-Lutz

As a first example consider the elliptic curve $E_c : y^2 = x^3 + cx$ over $\mathbb{F}_p$, where $p = 2m + 1$ is an odd prime and $c \in \mathbb{Z}$. We need to compute the cardinality of $E_c(\mathbb{F}_p)$ for some c. In general, counting points on the elliptic curve $y^2 = f(x)$ over $\mathbb{F}_p$ is done as follows (if p is small): for $a \in \mathbb{F}_p$, there are 0, 1 or 2 points in $E(\mathbb{F}_p)$ with x-coordinate a according as $f(a)$ is a quadratic nonresidue modulo p, divisible by p, or a quadratic residue modulo p. Thus

$$\#E(\mathbb{F}_p) = 1 + \sum_{a=0}^{p-1} \Big(\frac{f(a)}{p}\Big).$$

In our case we find

$$\begin{aligned} S &= \sum_{a=1}^{2m} \Big(\frac{a}{p}\Big)\Big(\frac{a^2+c}{p}\Big) \\ &= \sum_{a=1}^{m} \Big(\frac{a}{p}\Big)\Big(\frac{a^2+c}{p}\Big) + \sum_{a=1}^{m} \Big(\frac{p-a}{p}\Big)\Big(\frac{(p-a)^2+c}{p}\Big) \\ &= \sum_{a=1}^{m} \Big(\frac{a}{p}\Big)\Big(\frac{a^2+c}{p}\Big) + \sum_{a=1}^{m} \Big(\frac{-a}{p}\Big)\Big(\frac{a^2+c}{p}\Big). \end{aligned}$$

If m is odd, i.e., if $p \equiv 3 \bmod 4$, then $(-1/p) = -1$, hence $S = 0$; if m is even, on the other hand, that is if $p \equiv 1 \bmod 4$, then we only find that S must be even too.

Using the information that $\#E_c(\mathbb{F}_p) = p+1$ for primes $p \equiv 3 \bmod 4$ we now can prove

Theorem 1. *Let E be the elliptic curve $y^2 = x^3 + cx$, where $c \in \mathbb{Z}$ is not divisible by a fourth power $\neq 1$. Then*

$$E(\mathbb{Q})_{\text{tors}} \simeq \begin{cases} \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}, & \text{if } -a \text{ is a square;} \\ \mathbb{Z}/4\mathbb{Z}, & \text{if } a = 4; \\ \mathbb{Z}/2\mathbb{Z} & \text{otherwise.} \end{cases}$$

Proof. Note that the case $E(\mathbb{Q})_{\text{tors}} = \{\mathcal{O}\}$ does not occur since $P = (0, 0)$ is a rational point of order 2 on E.

The heart of the proof consists in showing that $E(\mathbb{Q})_{\text{tors}}$ has at most 4 points. This is achieved by a standard trick: according to Dirichlet's theorem there are infinitely many primes $p \equiv 3 \bmod 8$ (actually this special case can be proved along the lines of Euclid's theorem on the infinitude of primes). In particular there is one such prime that does not divide the discriminant $-64c^3$. For such a prime with

good reduction we know that $\#E(\mathbb{Q})_{\rm tors} \mid \#\overline{E}(\mathbb{F}_p)$; but from $p \equiv 3 \bmod 4$ we get $\#\overline{E}(\mathbb{F}_p) = p+1 \equiv 4 \bmod 8$, hence $\#E(\mathbb{Q})_{\rm tors}$ is not divisible by 8.

Next we show that there is no odd prime $q \ge 3$ with $q \mid \#E(\mathbb{Q})_{\rm tors}$. To this end we choose a prime $p \nmid \Delta$ with $p \equiv 1 \bmod q$ and $p \equiv 3 \bmod 4$ (Chinese Remainder Theorem and Dirichlet). As above we find $\#E(\mathbb{Q})_{\rm tors} \mid \#\overline{E}(\mathbb{F}_p) = p+1$, but now $p+1 \equiv 2 \bmod q$ shows that $q \nmid \#E(\mathbb{Q})_{\rm tors}$ as claimed.

Thus $\#E(\mathbb{Q})_{\rm tors} \mid 4$, and there are the following possibilities:

(1) There are three $\mathbb{Q}$-rational points of order 2: this happens if and only if $x^3 + ax = x(x^2+a)$ has three rational roots, i.e., if and only if $-a$ is a square.

(2) There is exactly one $\mathbb{Q}$-rational point of order 2: then either $\#E(\mathbb{Q})_{\rm tors} = 2$, or the unique point $(0,0)$ of order 2 is the double of some other rational point, say $(0,0) = 2(x,y)$ for some $x, y \in \mathbb{Z}$ (by Nagell-Lutz). The duplication formula shows that the x-coordinate of $2(x,y)$ has numerator $x^4 - 2ax^2 + a^2 = (x^2-a)^2$; this expression vanishes if and only if $x^2 = a$ ist, i.e., if a is a square. Since a is not divisible by fourth powers, x must be squarefree. Then $y^2 = x(x^2+a) = 2x^3$ implies that $x \mid 2$, which leads to $x = 2$, $a = 4$, and $y = \pm 4$.

This completes the proof. □

In a similar way we can prove the following

Theorem 2. *Let $E : y^2 = x^3 + b$ be an elliptic curve, where $b \in \mathbb{Z}$ is not divisible by a sixth power $\ne 1$. Then*

$$E(\mathbb{Q})_{\rm tors} \simeq \begin{cases} \mathbb{Z}/6\mathbb{Z}, & \text{if } b = 1; \\ \mathbb{Z}/3\mathbb{Z}, & \text{if } b = -432 \text{ or } 1 \ne b \text{ is a square}; \\ \mathbb{Z}/2\mathbb{Z} & \text{if } 1 \ne b \text{ is a cube}; \\ 0 & \text{otherwise.} \end{cases}$$

For a proof, one needs

Proposition 3. *Consider the elliptic curve $E : y^2 = x^3 + b$ with $b \in \mathbb{Z}$; For any odd prime $p \equiv 2 \bmod 3$ we have $\#E(\mathbb{F}_p) = p+1$.*