LECTURE 10, WEDNESDAY 10.03.04

FRANZ LEMMERMEYER

Today we will go through Manin's version of Hasse's proof that

$$|\#E(\mathbb{F}_q) - (p+1)| \le 2\sqrt{p}.$$

Let $\mathbb{F}_q$ be a finite field with $q = p^f$ elements and assume that $p \ge 5$. Manin's proof introduces elliptic curves over the function field $K = \mathbb{F}_q(t)$: given an elliptic curve

$$E : Y^2 = X^3 + aX + b \tag{1}$$

defined over $\mathbb{F}_q$ (in particular, the right hand side polynomial does not have multiple roots in $\mathbb{F}_q$) we introduce its quadratic twist

$$E_\lambda : \lambda Y^2 = X^3 + aX + b, \tag{2}$$

where $\lambda = \lambda(t) = t^3 + at + b \in \mathbb{F}_q[t]$. Multiplying through by λ^3 and introducing new coordinates $y = \lambda^2 Y$ and $x = \lambda X$ we see that (2) can be written in Weierstrass form

$$y^2 = x^3 + \lambda^2 ax + \lambda^3.$$

According to Tate's formulas, this curve has discriminant $\lambda^6\Delta$, where $\Delta \ne 0$ is the discriminant of the original curve E. Thus E_λ is an elliptic curve defined over K.

Let me recall the addition formulas for E_λ: for points $P = (x, y) \ne \mathcal{O}$, $P_j = (x_j, y_j)$ on E_λ, we have

$$x(P_1 + P_2) = \lambda\Big(\frac{y_1 - y_2}{x_1 - x_2}\Big)^2 - (x_1 + x_2), \tag{3}$$

and moreover, if $y \ne 0$,

$$x(2P) = \frac{(3x^2 + a)^2}{4(x^3 + ax + b)} - 2x. \tag{4}$$

The group $E_\lambda(K)$ clearly contains the points $(t, 1)$ and $(t, -1)$, as well as $P_0 = (t^q, (t^3 + at + b)^{(q-1)/2})$: in fact we have $(t^q)^3 + at^q + b = (t^3 + at + b)^q$ over $\mathbb{F}_q$.

We now define a sequence of points

$$P_n = P_0 + n(t, 1), \quad n \in \mathbb{Z} \tag{5}$$

in $E_\lambda(K)$. Our first claim is

Lemma 1. *If $P_n = (x_n, y_n) \ne \mathcal{O}$, then $x_n \ne 0$. Writing $x_n = f_n/g_n$ with $f_n, g_n \in \mathbb{F}_q[t]$, we have $\deg f_n > \deg g_n$.*

Since $\mathbb{F}_q[t]$ is Euclidean we may assume that f_n and g_n are coprime. This allows us to define a function $d : \mathbb{Z} \longrightarrow \mathbb{N}_0$ by

$$d_n = \begin{cases} 0 & \text{if } P_n = \mathcal{O}; \\ \deg f_n & \text{otherwise.} \end{cases}$$

The function d_n satisfies the following basic relation:

$$d_{n-1} + d_{n+1} = 2d_n + 2. \tag{6}$$

Now what has d_n got to do with the number $N_q = \#E(\mathbb{F}_q) - 1$ of $\mathbb{F}_q$-rational points $\neq \mathcal{O}$ on E? The answer is given by the equation

$$\#E(\mathbb{F}_q) = N_q + 1 = d_{-1}. \tag{7}$$

This relation yields

Lemma 2. *The function $d(n) := d_n$ is quadratic in n:*

$$d(n) = n^2 - (d_{-1} - d_0 - 1)n + d_0.$$

The proof of the Hasse bounds is now very simple: according to Lemma 2, the quadratic polynomial $d(x) = x^2 - (d_{-1} - d_0 - 1)x + d_0$ attains only nonnegative values for all $n \in \mathbb{Z}$.

We now claim that $d(x) \geq 0$ for all $x \in \mathbb{R}$. If not, then d has two simple roots (or a double root, but then the claim is trivial), say $\xi_1 < \xi_2$. The interval (ξ_1, ξ_2) does not contain any integer, since otherwise we would have $d(n) < 0$. Thus $n \leq \xi_1 < \xi_2 \leq n + 1$ for some $n \in \mathbb{Z}$.

If we had equality on both sides, then we would have $d_n = d_{n+1} = 0$; this in turn implies $P_n = P_{n+1} = \mathcal{O}$, from which we deduce $(t, 1) = P_{n+1} - P_n = \mathcal{O}$: contradiction. Thus at least one of the inequalities is sharp, hence $0 < \xi_2 - \xi_1 < 1$. But since $(\xi_1 - \xi_2)^2$ is the discriminant of d and therefore integral, this is a contradiction.

We have seen that $d(x) \geq 0$ for all $x \in \mathbb{R}$; this implies that the discriminant of d is nonpositive, and we find

$$0 \geq \operatorname{disc} d = (d_{-1} - d_0 - 1)^2 - 4d_0 = (N_q - q)^2 - 4q,$$

where we have used $d_0 = \deg t^q = q$. This yields our claim if we observe that N_q counts only the affine points.

It remains to prove Lemma 1 and Lemma 2, as well as the equations (6) and (7).

Proof of Equation (7). We observe that $d_0 = q$ since $P_0 = (x_0, y_0)$ with $x_0 = t^q$. A little calculation shows

$$x_{-1} = \frac{(t^3 + at + b)[(t^3 + at + b)^{(q-1)/2} + 1]^2}{(t^q - t)^2} - (t^q + t).$$

Since $\lambda = t^3 + at + b$, the numerator becomes

$$\begin{aligned} f_{-1} &= \lambda(\lambda^{(q-1)/2} + 1)^2 - (t^q + t)(t^q - t)^2 \\ &= \lambda^q + 2\lambda^{(q+1)/2} + \lambda - (t^{2q} - t^2)(t^q - t); \end{aligned} \tag{8}$$

since we work in characteristic p, we have $\lambda^q = t^{3q} + at^q + b$ (note that $a^q = a$ since $a \in \mathbb{F}_q$), hence the numerator of x_{-1} has the form $t^{2q+1} + h(t)$ for some polynomial $h(t)$ of degree $\leq 2q$.

Now we have to check whether we numerator and denominator have any common factors. To this end we observe that the denominator can be written in the form $t^q - t = \prod(t - \alpha)$, where the product is over all $\alpha \in \mathbb{F}_q$. Now there for each factor $t - \alpha$ are two cases:

i) The numerator is divisible by $(t - \alpha)^2$;
ii) The numerator is exactly divisible by $(t - \alpha)$.

In case i) formula (8) shows that

$$(t-\alpha)^2 \mid \lambda(\lambda^{(q-1)/2}+1)^2;$$

since $\lambda = t^3+at+b$ does not have any multiple roots in $\mathbb{F}_q$ (the curve is nonsingular), it follows that $(t-\alpha) \mid (\lambda^{(q-1)/2}+1)$. In case ii), on the other hand, we find that $t-\alpha$ must divide t^3+at+b.

Now let m denote the number of all factors $t-\alpha$ dividing $(\lambda^{(q-1)/2}+1)$, and n the number of all those dividing λ. Then we clearly have

$$d_{-1} = \deg f_{-1} = 2q+1-2m-n. \tag{9}$$

Next we count $\#E(\mathbb{F}_q)$. Assume first that $(t-\alpha) \mid \lambda$, i.e., $\alpha^3+a\alpha+b=0$. Then for each of these $n \leq 3$ different α the equation (1) has exactly one solution. In the other case where $t-\alpha$ divides $(\lambda^{(q-1)/2}+1)$ we have $(\alpha^3+a\alpha+b)^{(q-1)/2} = -1$, hence Euler's criterion tells us that $\alpha^3+a\alpha+b$ is a nonsquare in $\mathbb{F}_q$; for these m values of α the equation (1) does not have solutions.

Thus among the q values of α there are m, n and $q-m-n$ values for which (1) has none, exactly one, and two solutions, respectively. This shows that the number of all solutions equals $N_q = 2(q-m-n)+n = 2q-2m-n$. Plugging this into (9) yields the desired equality (7).

Proof of Lemma 2. Lemma 2 now follows easily from the basic relation (6): for $n=-1$ and $n=0$ the claim is trivial; if it holds for $n-1$ and n, then

$$\begin{aligned} d_{n+1} &= 2d_n - d_{n-1} + 2 \\ &= 2[n^2 - (d_{-1}-d_0-1)n + d_0] \\ &\quad -[(n-1)^2 - (d_{-1}-d_0-1)(n-1)+d_0] + 2 \\ &= (n+1)^2 - (d_{-1}-d_0-1)(n+1)+d_0. \end{aligned}$$

Similarly we can prove the claim for all $n \leq -1$.

The Proof of Lemma 1 is next and consists essentially of calculations with the values of polynomials at infinity. Let us therefore first explain what this means.

In order to be able to evaluate an expression $x(t) = \frac{f(t)}{g(t)}$ at $t=\infty$, we observe that $[x:1] = [f(t):g(t)]$ and then substitute $t = r/s$; we can interpret x as a map from the projective line $\mathbb{P}^1\mathbb{F}_p \longrightarrow \mathbb{P}^1\mathbb{F}_p$ and find that x maps $[t:1] = [r:s]$ to $[s^jF(r,s) : G(r,s)]$, where F and G are the homogenizations of f and g, and where $j = \deg g - \deg f$. Now we define $x(\infty) = x(t)|_\infty$ to be the value of $[s^jF(r,s):G(r,s)]$ at $[1:0]$. Thus $x(\infty)=0$ if $\deg f = \deg g$, and $x(\infty) = a_n/b_n$ if $\deg f = \deg g = n$ and $f(t) = a_nt^n + \ldots$, $g(t) = b_nt^n + \ldots$.

Evaluation at $t=\infty$ satisfies the familiar properties: for rational functions x, y we have $(x+y)|_\infty = x|_\infty + y|_\infty$, $(xy)|_\infty = x|_\infty \cdot y|_\infty$, etc. as long as all the "limits" involved exist.