LECTURE 15, WEDNESDAY 31.03.04

FRANZ LEMMERMEYER

1. The Filtration of $E^{(1)}$

Let us now see why the kernel of reduction $E^{(1)}$ is torsion free. Recall that $E^{(1)}$ is defined by the exact sequence

$$0 \longrightarrow E^{(1)} \longrightarrow E^{(0)} \longrightarrow E_{\rm ns}(\mathbb{F}_p) \longrightarrow 0$$

The following result will be needed again when we discuss the theorem of Mordell-Weil; it is formulated for arbitrary Unique Factorization Domains, but we will need it only for $R = \mathbb{Z}$ and $R = \mathbb{Z}_p$ (which, like any local ring, is a UFD).

Lemma 1. *Let R be a unique factorization domain with quotient field K, and let Let $P = (x, y)$ be a K-rational point on the elliptic curve $E : y^2 = x^3 + ax^2 + bx + c$ with $a, b, c \in R$. Then there exist $m, n, e \in R$ such that $x = m/e^2$, $y = n/e^3$, and $(m, e) = (n, e) = 1$.*

Proof. Write $x = m/M$ und $y = n/N$ with $m, n \in R$, $M, N \in R \setminus \{0\}$, and $(m, M) = (n, N) = 1$. We want to show that $M^3 \mid N^2$ and $N^2 \mid M^3$; this will imply that $M^3 = uN^2$ for some unit $u \in R^\times$, which in turn gives $(uM)^3 = (u^2N)^2$. Replacing M by uM and N by u^2N then shows that $M^3 = N^2$, and unique factorization gives $M = e^2$ and $N = e^3$ for some $e \in R$.

From $y^2 = x^3 + ax^2 + bx + c$ we get

$$M^3n^2 = N^2m^3 + aN^2Mm^2 + bN^2M^2m + cN^2M^3.$$

Since the right hand side is divisible by N^2, and since we know that $(n, N) = 1$, we conclude that $N^2 \mid M^3$. On the other hand we have $M \mid N^2m^3$ and $(m, M) = 1$, hence $M \mid N^2$. This implies $M^2 \mid N^2m^3$, that is, $M \mid N$, and running through this argument once more we find $M^3 \mid N^2$. □

We now define a function $\ell : E^{(0)} \longrightarrow \mathbb{N}$ as follows: write (x, y) projectively as $[x : y : 1] = [me : n : e^3]$ and let $\ell(x, y) = l$ if $p^l \parallel e$. Using the p-adic valuation $|\cdot| = |\cdot|_p$ we have $|x| = p^{2l}$.

Note that $\ell(x, y) = 0$ if and only if the reduction of (x, y) is an affine point, and that $\ell(x, y) \geq 1$ for points in $E^{(0)}$ if and only if $(x, y) \in E^{(1)}$. This allows us to define a filtration of $E^{(1)}$ by setting

$$E^{(N)} = \{(x, y) \in E^{(1)} : \ell(x, y) \geq N\}.$$

It is immediately clear that

$$\ldots \subseteq E^{(N+1)} \subseteq E^{(N)} \subseteq \ldots \subseteq E^{(1)} \subseteq E^{(0)}.$$

It can be proved directly that the $E^{(N)}$ are actually groups; it is more convenient, however, to reduce this to the proof that the reduction is a group homomorphism.

To this end we write the equation of our elliptic curve in homogeneous form $E : Y^2Z = X^3 + aXZ^2 + bZ^3$. For any natural number $N \geq 1$ we put $X_N =$

$p^{2N}X$, $Y_N = p^{3N}Y$ and $Z_N = Z$; these integers give points on the elliptic curve $E^N : Y_N^2 Z_N = X_N^3 + p^{4N} a X_N Z_N^2 + p^{6N} B Z_N^3$ (the corresponding map $E \longrightarrow E^N$ is a projective transformation and in fact a group homomorphism, since it preserves lines). Reducing E^N modulo p gives $\overline{E}^N : Y_N^2 Z_N = X_N^3$; we denote this reduction $E(K) \longrightarrow \overline{E}^N(\mathbb{F}_p)$ by π^N.

What happens to an affine point $P = (x, y) \in E(K)$ under this map? Writing $x = n/e^2$ and $y = m/e^3$ we find that the above transformation π^N corresponds to dividing e through by p^N. Writing P projectively as $[x : y : 1] = [me : n : e^3]$ we find that π^N maps P to the reduction modulo p of $Q = [p^{2N}me : p^{3N}n : e^3]$. Thus the reduction of $\pi^N(P)$ is

- the singular point $(0, 0)$ on $E^N(\mathbb{F}_p)$ if $\ell(x, y) < N$;
- some smooth affine point on $E^N(\mathbb{F}_p)$ if $\ell(x, y) = N$;
- the point at infinity on $E^N(\mathbb{F}_p)$ if $\ell(x, y) > N$.

In fact:

- if $l \le N$, then the standard form of Q is given by
$$Q = [p^{2N}me : p^{3N}n : e^3] = [p^{2N-3l}me : p^{3N-3l}n : p^{-3l}e^3],$$
where the last coordinate is a p-adic unit; thus the reduction of Q is the singular point $[0 : 0 : 1]$ if $l < N$, and some nonsingular affine point if $l = N$.
- if $l > N$, then Q has standard form
$$Q = [p^{2N}me : p^{3N}n : e^3] = [p^{-N}me : n : p^{-3N}e^3],$$
hence reduces to the point $[0 : 1 : 0]$ at infinity.

Thus $E^{(N+1)}$ is exactly the kernel of $\pi^N : E^N \longrightarrow E_{\rm ns}^N(\mathbb{F}_p)$, and therefore a group. Since the reduction is surjective by Hensel's Lemma, we have an exact sequence

$$0 \longrightarrow E^{(N+1)} \longrightarrow E^{(N)} \longrightarrow E_{\rm ns}^N(\mathbb{F}_p) \longrightarrow 0$$

for each $N \ge 0$. Moreover we know that $\overline{E}^N : y^2 = x^3$ is singular over $\mathbb{F}_p$ for $N \ge 1$, and that $E_{\rm ns}^N(\mathbb{F}_p) \simeq \mathbb{Z}/p\mathbb{Z}$. Finally, we clearly have $\bigcap E^{(N)} = \{\mathcal{O}\}$, since the only integer divisible by arbitrarily high powers of p is 0. Thus we have proved

Theorem 2. *The group $E^{(0)}$ has a filtration of subgroups*

$$E^{(0)} \supset E^{(1)} \supset \ldots \supset E^{(N)} \supset \ldots$$

with $\bigcap E^{(N)} = \{\mathcal{O}\}$, and the homomorphisms π_N induce exact sequences

$$0 \longrightarrow E^{(1)} \longrightarrow E^{(0)} \longrightarrow E_{\rm ns}(\mathbb{F}_p) \longrightarrow 0$$

for $N = 0$ and

$$0 \longrightarrow E^{(N+1)} \longrightarrow E^{(N)} \longrightarrow \mathbb{Z}/p\mathbb{Z} \longrightarrow 0$$

for $N \ge 1$.

This immediately implies

Corollary 3. *Let $(x, y) \in E(\mathbb{Q}_p)$ be a point with finite order n, where $(n, p) = 1$. Then $x, y \in \mathbb{Z}_p$.*

Proof. If not, then $\ell(x,y) \geq 1$. Since $\bigcap_N E^{(N)} = \{\mathcal{O}\}$ there is some $N \in \mathbb{N}$ with $(x,y) \in E^{(N)} \setminus E^{(N+1)}$. The map $E \longrightarrow E^{(N)} \longrightarrow E^{(N)}/E^{(N+1)}$ sends (x,y) to some element of order > 1 (hence of order p) in $E^{(N)}/E^{(N+1)}$; but group homomorphisms cannot map an element of order coprime to p to an element of order p: contradiction! □

2. $E^{(1)}$ is torsion free

Corollary 3 is almost all we need to prove the Theorem of Nagell-Lutz. It only remains to get rid of the assumption that $(n,p) = 1$. To this end we define a map $u : E^{(1)} \longrightarrow \mathbb{Z}_p$ by $u(P) = x/y$ for $P = (x,y)$, and $u(\mathcal{O}) = 0$. In fact, if $l = \ell(x,y) \geq 1$, then $p^l \mid \frac{x}{y}$, so the right hand side is a p-adic integer with $|u(P)| = p^{-l}$.

Observe that there are no problems with points that have $y = 0$: if $y = 0$, then (x,y) is a point of order 2, and if we already knew that $E^{(1)}$ is torsion free, we could conclude that $(x,y) \notin E^{(1)}$. A direct argument goes like this: from $0 = y^2 = x^3 + ax + b$ we deduce that x must be a p-adic root of $x^3 + ax + b$. Since $a, b \in \mathbb{Z}$, we find that x must be a p-adic integer: if p^m is the exact power of p dividing the denominator of x, then p^{3m} is the power of p dividing the denominator of x^3; but the denominator of $ax + b$ is divisble by at most p^m, hence $x^3 + ax + b$ could not be 0. Now $E^{(1)}$) is the kernel of reduction modulo p, hence its elements reduce to the point at infinity over $\mathbb{F}_p$. On the other hand, since x is a p-adic integer, $[x : y : 1]$ is in standard form, hence its reduction has z-coordinate $\neq 0$. Thus $(x,0) \in E(\mathbb{Q}_p) \setminus E^{(1)}$.

We are now in the following situation:

$$\begin{array}{ccccccccccc} E(\mathbb{Q}_p) & \longleftarrow & E^{(0)} & \longleftarrow & E^{(1)} & \longleftarrow & E^{(2)} & \longleftarrow & E^{(3)} & \longleftarrow & \dots \\ & & & & \downarrow u & & \downarrow u & & \downarrow u & & \\ & & & & p\mathbb{Z}_p & \longleftarrow & p^2\mathbb{Z}_p & \longleftarrow & p^3\mathbb{Z}_p & \longleftarrow & \dots \end{array}$$

The horizontal maps are inclusions, the vertical maps are induced by u.

Now consider a point $P \in E^{(n)} \setminus E^{(n+1)}$; then $sP \in E^{(n)} \setminus E^{(n+1)}$ for all $s \in \mathbb{Z}$ with $p \nmid s$: this is because the quotient group $E^{(n)}/E^{(n+1)}$ has order p. Thus $\ell(sP) = n$, and we have $|u(sP)| = |u(P)|$. For $s = p$, on the other hand, we have $pP \in E^{(n+1)}$, hence $\ell(pP) \geq n + 1$ and therefore $|u(pP)| \leq |p| \cdot |u(P)|$. Using induction we see that $|u(sP)| \leq |s| \cdot |u(P)|$ for all $s \in \mathbb{Z}$.

If we knew that we have equality here, in other words that we have $pP \in E^{(n+1)} \setminus E^{(n+2)}$, then we could deduce that $E^{(n)}/E^{(n+2)} \simeq \mathbb{Z}/p^2\mathbb{Z}$, and using induction it would follow that $E^{(n)}/E^{(n+m)} \simeq \mathbb{Z}/p^m\mathbb{Z}$ for all $m, n \geq 1$. In particular, $E^{(1)}$ could not contain a point of p-power order, and we would have shown that $E^{(1)}$ is torsion free. In fact, we do have equality:

Lemma 4. *For all $P \in E^{(1)}$ and all $s \in \mathbb{Z}$ we have $|u(sP)| = |s| \cdot |u(P)|$.*

Now everything is easy: if $P \in E^{(1)}$ is torsion, say $sP = \mathcal{O}$ with $s \in \mathbb{N}$, then the lemma shows that $0 = |u(sP)| = |s| \cdot |u(P)|$; since $s \geq 1$ we have $|s| \neq 0$, hence $P = \mathcal{O}$. In other words: $E^{(1)}$ is torsion free.

The lemma would be trivial if u was a group homomorphism; in this case u would also be injective, and it would follow that $E^{(1)}$ is isomorphic to a subgroup of $p\mathbb{Z}_p$. In particular, $E^{(1)}$ would be torsion free because $p\mathbb{Z}_p$ is.

Unfortunately, however, u is not a group homomorphism: the difference $u(P_1+P_2)-u(P_1)-u(P_2)$ is in general not equal to 0. On the other hand, the difference is p-adically small, and this is all we need for proving the lemma. In fact we claim that we have the inequality

$$|u(P_1+P_2)-u(P_1)-u(P_2)| \le \max\{|u(P_1)|^5, |u(P_2)|^5\} \tag{1}$$

for all $P_1, P_2 \in E^{(1)}$, and this will imply Lemma 4.

The inequality (1) is clearly correct if one of the points is $\mathcal{O}$; for example, if $P_1+P_2=\mathcal{O}$, then $P_2=-P_1$, hence $u(P_1+P_2)-u(P_1)-u(P_2) = u(\mathcal{O})-u(P_1)-u(-P_1)=0$.

Thus we may assume that all points occurring in the inequality are in the affine plane. Moreover we may assume that $|u(P_2)| \le |u(P_1)| = p^{-N}$. Now consider the line L_N through P_1, P_2 and $-P_1-P_2$ in the projective $X_N-Y_N-Z_N$ plane. Since the reductions of P_1 and P_2 are not singular, the line through the reductions of P_1, P_2 and $-P_1-P_2$ does not go through the origin, hence can be written in the form $Z=rX+sY$ with $r,s\in\mathbb{F}_p^\times$. Thus the line L through P_1, P_2 and $-P_1-P_2$ has the form $Z=rX+sY$ with p-adic numbers r,s such that $|r|\le 1$ and $|s|\le 1$, that is, they are p-adic integers.

Intersecting the line L_N with E_N gives

$$\begin{aligned} 0 &= X_N^3 + p^{4N}aX_N(rX_N+sY_N)^2 + p^{6N}b(rX_N+sY_N)^3 - Y_N^2(rX_N+sY_N) \\ &= c_3X_N^3 + c_2X_N^2Y_N + c_1X_NY_N^2 + c_0Y_N^3, \end{aligned}$$

where $c_3 = 1+p^{4N}ar^2+p^{6N}br^3$ and $c_2 = 2p^{4N}ars+3p^{6N}br^2s$. In particular, we have $|c_3|=1$ and $|c_2|\le p^{-4N}$. The roots X_N/Y_N of the equation are $-p^{-N}u(P_1+P_2)$, $p^{-N}u(P_1)$ and $p^{-N}u(P_2)$; since their sum equals $-c_2/c_3$, we get $p^{5N} \mid p^Nc_2/c_3 = u(P_1+P_2)-u(P_1)-u(P_2)$, and this is what we needed to prove.

Lemma 4 is now a formal consequence of this inequality:

Lemma 5. *Let u be a map from a group G to $p\mathbb{Z}_p$ satisfying*

- $u(-g)=-u(g)$,
- $|u(ag)| \le |a|\cdot|u(g)|$,
- $|u(g+h)-u(g)-u(h)| \le \max\{|u(g)|^5, |u(h)|^5\}$

for all $g,h\in G$. Then

$$|u(ag)| = |a|\cdot|u(g)|$$

for all $a\in\mathbb{Z}$ and $g\in G$.

Proof. As a first step we prove that

$$|u(ag)-au(g)| \le |u(g)|^5. \tag{2}$$

Since the claim is invariant under the transformation $a\longmapsto -a$, it is sufficient to prove it for $a\ge 0$. Let $|u(g)|=p^{-l}$; then we have to show that $p^{5l} \mid (u(ag)-au(g))$. We do this by induction; the cases $a=0$ and $a=1$ are clearly trivial (note that $u(0)=0$ from the first or the second property of u). Assume therefore that the relation holds for some $a\ge 1$. Using (1) we find that

$$|u((a+1)g)-u(ag)-u(g)| \le \max\{|u(ag)|^5, |u(g)|^5\}.$$

Since $|u(ag)|\le|u(g)|$ this implies that $p^{5l} \mid [u((a+1)g)-u(ag)-u(g)]$. Adding the induction assumption shows that $p^{5l} \mid [u((a+1)g)-au(g)-u(g)]$.

Now let us prove the actual claim. Recall that $|u(g)|=p^{-l}<1$; if $p\nmid a$, then $p^l \parallel au(g)$, whereas $p^{5l} \mid [u(ag)-au(g)]$. This is possible only if $p^l \parallel u(ag)$. This

proves the lemma for all integers a coprime to p (actually for all a that are not divisible by p^{4l}).

Now if the claim is true for some integer a, then it also holds for pa. In fact, setting $g = ag$ and $a = p$ in (2) gives $|u(pag) - pu(ag)| \leq |u(ag)|^5$, and this implies that $u(pag) - pu(ag)$ is divisible by $u(aP)^5$, which is only possible if $|u(pag)| = |pu(ag)|$. The induction assumption shows that $|u(ag)| = |a| \cdot |u(g)|$, hence we have $|u(pag)| = |pu(ag)| = |pa| \cdot |u(g)|_g$. The claim follows. □