LECTURE 14, MONDAY 29.03.04

FRANZ LEMMERMEYER

1. Lifting Points

Let $\mathcal{C}$ be the plane curve defined by the polynomial $F(X,Y) \in \mathbb{Z}[X,Y]$ and fix a prime p. Hensel's Lemma deals with the following situation: assume you have a pair of integers (x,y) such that $F(x,y) \equiv 0 \bmod p^k$ (in other words: (x,y) is a $\mathbb{Z}/p^k\mathbb{Z}$-point on $\mathcal{C}$). Do there exist integers x', y' such that $F(x',y') \equiv 0 \bmod p^{k+1}$, and if yes, how many?

To get an answer, write $x' = x + rp^k$, $y' = y + sp^k$, and $F(x,y) = p^k t$; we have to count the number of residue classes $r, s \bmod p$ for which $F(x',y') \equiv 0 \bmod p^{k+1}$.

The Taylor expansion of F shows that

$$F(x+h, y+i) = F(x,y) + hF_X(x,y) + iF_Y(x,y) + \text{ terms of higher order,}$$

where $F_X = \frac{\partial F}{\partial X}$ and $F_Y = \frac{\partial F}{\partial Y}$. Thus

$$F(x',y') \equiv p^k(t + rF_X(x,y) + sF_Y(x,y)) \bmod p^{k+1}$$

and $F(x',y') \equiv 0 \bmod p^{k+1}$ if and only if $t + rF_X(x,y) + sF_Y(x,y) \equiv 0 \bmod p$. If $p \nmid F_X(x,y)$ or $p \nmid F_Y(x,y)$, there are clearly p solutions $(r,s) \in \mathbb{F}_p \times \mathbb{F}_p$, each one defining a point $(x',y') \in \mathcal{C}(\mathbb{Z}/p^{k+1}\mathbb{Z})$. If $p \mid F_X(x,y)$ and $p \mid F_Y(x,y)$, on the other hand, then either $p \mid t$ and every pair $(r,s) \in \mathbb{F}_p \times \mathbb{F}_p$ is a solution, or $p \nmid t$, in which case the point does not have any lift at all.

The congruences $F_X(x,y) \equiv F_Y(x,y) \equiv 0 \bmod p$, together with the congruence $F(x,y) \equiv 0 \bmod p$, are equivalent to (x,y) being a singular point over $\mathbb{Z}/p\mathbb{Z}$. Let us call a point $(x,y) \in \mathcal{C}(\mathbb{Z}/p^k\mathbb{Z})$ regular if its reduction $(x \bmod p, y \bmod p)$ is nonsingular over $\mathbb{Z}/p\mathbb{Z}$. Then we have proved:

Theorem 1. *Let $\mathcal{C}$ be an affine curve defined over $\mathbb{Z}$, and let p be a prime. Then every regular point $P \in \mathcal{C}(\mathbb{Z}/p^k\mathbb{Z})$ can be lifted to exactly p different points in $\mathcal{C}(\mathbb{Z}/p^{k+1}\mathbb{Z})$. Non-regular points either do not have a lift at all, or can be lifted in p^2 different ways.*

2. Reduction

Let $E : y^2 = x^3 + ax + b$ be an elliptic curve defined over $\mathbb{Q}$. Using simple transformations we can make sure that a, b are actually integers: if t is the common denominator of a and b, then multiplication by t^6 gives $(t^3y)^2 = (t^2x)^3 + t^5a(tx) + t^6b$; now put $Y = t^3y$ and $X = t^2X$.

For elliptic curves $y^2 = x^3 + ax + b$ with $a, b \in \mathbb{Z}$ we can define its reduction $\overline{E} : y^2 = x^3 + \overline{a}\,x + \overline{b}$ over $\mathbb{F}_p$ (the bar represents reduction modulo p).

Actually we can define this reduction not only from $\mathbb{Q}$ to $\mathbb{F}_p$, but more generally from $\mathbb{Q}_p$ to $\mathbb{F}_p$. To this end, let $E : y^2 = x^3 + ax + b$ be an elliptic curve defined over $\mathbb{Q}_p$, with coefficients $a, b \in \mathbb{Z}_p$. By sending every $a = a_0 + a_1p + a_2p^2 + \ldots \in \mathbb{Z}_p$ to $\overline{a} = a_0 \in \mathbb{F}_p$, we get a reduction map $^- : \mathbb{Z}_p \longrightarrow \mathbb{F}_p : a \longmapsto \overline{a}$.

Next let us recall the reduction map on general projective spaces $\mathbb{P}^n\mathbb{Q}$. Given $P = [x_0 : x_1 : \cdots : x_n] \in \mathbb{P}^n\mathbb{Q}_p$, we may rescale to get $x_j \in \mathbb{Z}_p$, and we may assume that not all coordinates are divisible by p. We will call such a representation of P "standard". Let $\overline{x} = x \bmod p$ be the reduction modulo p of the p-adic number; the point $\overline{P} = [\overline{x}_0 : \overline{x}_1 : \cdots : \overline{x}_n]$ is called the reduction of P (with respect to p).

We have to study how rational points on E behave with respect to this reduction. First we can reduce line equations in the same way: lines $aX+bY+cZ = 0$ in $\mathbb{P}^2\mathbb{Q}_p$ correspond to triples $[a : b : c] \in \mathbb{P}^2\mathbb{Q}_p$, and if $[\overline{a} : \overline{b} : \overline{c}]$ is the reduced point, the corresponding equation $\overline{a}X + \overline{b}Y + \overline{c}Y = 0$ is called the reduction of the line. The same goes for conics, which correspond to points in $\mathbb{P}^5\mathbb{Q}_p$, or to curves of higher degree.

We now prove the fact that this reduction map respects the group law; at first this may seem surprising, but a second thought shows that this is what one should expect. After all, if P, Q, R are collinear points on an elliptic curve (i.e. if $P+Q+R = 0$), then they remain collinear after reduction modulo p. The only accident that could happen is that the reduced curve vanishes everyhwere or contains the line PQ: in these cases, there would not be a group law over $\mathbb{F}_p$. The proof that reduction is a group homomorphism basically has to make sure these cases do not occur.

Proposition 2. *Let $E : y^2 = x^3 + ax + b$ be an elliptic curve with coefficients $a, b \in \mathbb{Z}_p$; if $P_1, P_2, P_3 \in E(\mathbb{Q}_p)$ are collinear, then so are the reductions $\overline{P}_1, \overline{P}_2$ and $\overline{P}_3$. Moreover, the reduction of the tangent to E at P_1 is a tangent to $\overline{E}$ at $\overline{P}_1$.*

Proof. Let us more generally consider an arbitrary cubic curve $F(X, Y, Z) = 0$, where F is a homogeneous polynomials in standard form. Moreover, let $\ell : l_1X + l_2Y + l_3Z = 0$ be a line in standard form. We may assume without loss of generality that $p \nmid l_3$. Dividing the line equation through by the p-adic unit $-l_3$ we find that it can be written in the form $\ell : Z = lX + mY$. The points of intersection of ℓ with C are given by the roots of $G(X, Y) := F(X, Y, lX + mY) = 0$; reduction yields $\overline{G}(X, Y) = \overline{F}(X, Y, \overline{l}X + \overline{m}Y) = 0$.

If $\overline{G}$ vanishes identically, then the reduced curve contains a line. An example is given by the cubic Fermat curve $C : X^3 + Y^3 = Z^3$, whose reduction modulo 3 can be written in the form $(X + Y - Z)^3 = 0$ and hence is just a triple line $Z = X + Y$)in particular, all points on the Fermat cubic over $\mathbb{F}_3$ are singular). For Weierstrass equations, this can not happen: curves $Y^2Z = X^3 + aXZ + bZ^3$, and more generally any curve of the form $y^2 = f(x)$, where f is a monic polynomial of odd degree, are still irreducible after reduction.

Thus we may assume that $\overline{G}$ is not identically zero. Now consider the points $P_j = (x_j : y_j : z_j)$ with $j = 1, 2, 3$; we assume that they are in standard form. Note that we cannot have $(\overline{x}_j, \overline{y}_j) = (0, 0)$, since this would imply $\overline{z}_j = \overline{l}\,\overline{x}_j + \overline{m}\,\overline{y}_j = 0$, which contradicts our assumptions.

Since the points P_j lie on the line and the equation, there is some $\lambda \in \mathbb{Q}_p$ with $F(X, Y, lX + mY) = \lambda H(X, Y)$ and $H(X, Y) = (y_1X - x_1Y)(y_3X - x_3Y)(y_3X - x_3Y)$. We have just seen that the reduction of H cannot vanish identically, and this implies that $\lambda \in \mathbb{Z}_p$: if not, then $\lambda^{-1} \in p\mathbb{Z}_p$ and hence $0 = \overline{\lambda F} = \overline{H}$: contradiction. Thus $\lambda \in \mathbb{Z}_p$ and $\overline{F}(X, Y, \overline{l}X + \overline{m}Y) = \overline{\lambda}\overline{H}(X, Y)$; since $\overline{F}$ does not vanish completely, we have $\overline{\lambda} \neq 0$, hence $\lambda \in \mathbb{Z}_p^\times$.

Thus $\overline{F} = c\overline{H}$ for some $c = \overline{\lambda} \in \mathbb{F}_p^\times$. This shows that the reduced points $\overline{P}_j$ are collinear and satisfy $\overline{P}_1 + \overline{P}_2 + \overline{P}_3 = \overline{\mathcal{O}}$; it also shows that tangents at P_1 reduce to tangents at $\overline{P}_1$. □

Thus the reduction map $E^{(0)} \longrightarrow E_{\mathrm{ns}}(\mathbb{F}_p)$ is a group homomorphism; it is surjective by Hensel's Lemma:

Proposition 3. *Let E be as above; if Q is a point on the nonsingular part $\overline{E}_{ns}$ of the reduction, then there is a $P \in E(\mathbb{Q}_p)$ with $Q = \overline{P}$.*