LECTURE 13, MONDAY 22.03.04

FRANZ LEMMERMEYER

1. Hensel's Lemma

Now let us talk a little bit about the structure of p-adic fields. We will interpret $\mathbb{Z}_p$ as the projective limit of the rings $\mathbb{Z}/p^n\mathbb{Z}$, and $\pi_n : \mathbb{Z}_p \longrightarrow \mathbb{Z}/p^n\mathbb{Z}$ as the projection onto its n-th component. Thus we will write $x \in \mathbb{Z}_p$ as sequences $x = (x_1, x_2, x_3, \ldots)$ with $x_n \in \mathbb{Z}/p^n\mathbb{Z}$. If you want to think of p-adic integers as power series $a_0 + a_1p + a_2p^2 + \ldots$ in p, then $x_1 = a_0$, $x_2 = a_0 + a_1p$, $x_3 = a_0 + a_1p + a_2p^2$, etc.

Our first claim is

Proposition 1. *The sequence*

$$0 \longrightarrow \mathbb{Z}_p \xrightarrow{p^n} \mathbb{Z}_p \xrightarrow{\pi_n} \mathbb{Z}/p^n\mathbb{Z} \longrightarrow 0$$

is exact. In particular, $\mathbb{Z}_p/p^n\mathbb{Z}_p \simeq \mathbb{Z}/p^n\mathbb{Z}$.

Proof. Let us first show that multiplication by p is injective; by induction, this will show that multiplication by p^n is injective.

Assume therefore that $x = (x_1, x_2, \ldots) \in \mathbb{Z}_p$ satisfies $px = 0$. Then $px_{n+1} = 0$ in $\mathbb{Z}/p^{n+1}\mathbb{Z}$, which implies that x_{n+1} is divisible by p^n. But then so is $x_n = \pi_n^{n+1}x_{n+1}$, hence $x_n = 0$. Since this is valid for any n, we cnclude that $x = 0$.

Since π_n is clearly surjective, it remains to prove that $\ker \pi_n = p^n\mathbb{Z}_p$. It is clear that $p^n\mathbb{Z}_p \subseteq \ker \pi_n$, so assume that $x \in \mathbb{Z}_p$ satisfies $x_n = \pi_n(x) = 0$. Then $x_k = \pi_k^n(x_n) = 0$ for all $k \le n$, hence we have $x = (0, 0, \ldots, 0, x_{n+1}, x_{n+1}, \ldots)$. But for $m > n$ we have $0 = x_n = \pi_n^m x_m$, hence x_m is in the kernel of reduction modulo p^n, in other words, x_m is represented by an integer divisible by p^n. This means that $x = p^n x'$ for some $x' \in \mathbb{Z}_p$, hence $\ker \pi_n \subseteq p^n\mathbb{Z}_p$. □

Proposition 2. *A p-adic integer $u \in \mathbb{Z}_p$ is a unit if and only if $p \nmid u$.*

Proof. If u is a unit, then $uv = 1$ for some $v \in \mathbb{Z}_p$. Reducing modulo p show that $\pi_1(u)\pi_1(v) = 1$ in $\mathbb{Z}/p\mathbb{Z}$, hence $\pi_1(u)$ is a unit in $\mathbb{Z}/p\mathbb{Z}$ and thus not divisible by p. Conversely, assume that $u = (u_1, u_2, \ldots)$ is not divisible by p. Then $u_1 = \pi_1^n u_n$ is not divisible by p, and this shows that u_n is a unit in $\mathbb{Z}/p^n\mathbb{Z}$. But then $u^{-1} = (u_1^{-1}, u_2^{-1}, u_3^{-1}, \ldots)$ is an inverse of u in $\mathbb{Z}_p$. □

Proposition 3. *Every nonzero element $x \in \mathbb{Z}_p$ has a unique representation of the form $x = up^n$, where $u \in \mathbb{Z}_p^\times$ and $n \ge 0$.*

Proof. Since $x = (x_1, x_2, \ldots) \ne 0$, there is a minimal $n \ge 0$ with $x_{n+1} \ne 0$. Then $x = p^n u$ for the unit $u = p^{-n}(x_{n+1}, x_{n+2}, \ldots)$. Uniqueness is clear. □

More generally, every p-adic number $x \in \mathbb{Q}_p^\times$ can be written uniquely as $x = up^n$ for some unit $u \in \mathbb{Z}_p^\times$ and an integer $n \in \mathbb{Z}$. This shows that, as abelian groups, we have $\mathbb{Q}_p^\times \simeq \mathbb{Z} \cdot \mathbb{Z}_p^\times$.

As a very modest Local-Global Principle, let us prove

Proposition 4. *A rational number a is a square in $\mathbb{Q}$ if and only if it is a square in every completion $\mathbb{Q}_p$ (including $\mathbb{R} = \mathbb{Q}_\infty$).*

Proof. A rational number can be written as $a = up^m$ in $\mathbb{Q}_p$, where $u \in \mathbb{Z}_p^\times$ is a unit and m an integer. If a is a square in $\mathbb{Q}_p$, then m must be even, and this shows that the prime factor p occurs in a to an even power. Since a is a square in $\mathbb{R}$, we must have $a > 0$. But then a is a product of squares, hence a square in $\mathbb{Q}$. □

Our next goal will be showing that the p-adic number fields $\mathbb{Q}_p$ contain a lot more "irrationalities" than their common subfield $\mathbb{Q}$. We start with

Theorem 5. *For any integer a not divisible by the prime p, the sequenc a, a^p, a^{p^2}, ... converges in $\mathbb{Z}_p$ to some element $\omega(a) = (a, a^p, a^{p^2}, \dots)$ with the property that $\omega^{p-1} = 1$.*

What this result tells us is that $\mathbb{Q}_p$ contains the $p-1$-th roots of unity.

Proof. Consider the element $(a, a^p, a^{p^2}, \dots) \in \prod \mathbb{Z}/p^n\mathbb{Z}$; in order to show that it is in $\mathbb{Z}_p$, we have to show that the sequence is compatible, i.e., that $a^{p^{n+1}} \equiv a^{p^n} \bmod p^{n+1}$. For $n = 0$ this is just Fermat's Little Theorem. Now use induction. □

Corollary 6. *If p is an odd prime, then $\mathbb{Z}_p^\times \simeq \mathbb{Z}/(p-1)\mathbb{Z} \oplus H$, where $H = \{u \in \mathbb{Z}_p : u \equiv 1 \bmod p\}$ is the group of principal units.*

In fact, given any unit u with $u \equiv a \bmod p$, the unit $v = u\omega(a)^{-1}$ is in H. Using the p-adic logarithm, it is easy to verify that $H \simeq \mathbb{Z}_p$ as an abelian group.

Proposition 7. *The group $\mathbb{Z}_p$ is torsion free.*

Proof. This is trivial: $nx = 0$ for some integer $n \in \mathbb{N}$ and $x \in \mathbb{Z}_p$ implies $n = 0$ or $x = 0$ since $\mathbb{Z}_p$ is a domain. Here we have used the fact that $\mathbb{Z} \hookrightarrow \mathbb{Z}_p$. □

Exercise: Consider the ring homomorphism $\mathbb{Z} \hookrightarrow \mathbb{Z}_p$. Show that it induces a ring homomorphism $\mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}_p/n\mathbb{Z}_p$. Determine kernel and image.

Next we will explain why $\sqrt{2} \in \mathbb{Q}_{17}$ but $\sqrt{2} \notin \mathbb{Q}_5$ (here $\sqrt{2}$ does *not* stand for the real number $1.414\dots$, since this number is not contained in any $\mathbb{Q}_p$: it simply does not converge there. Rather, $\sqrt{2}$ denotes a solution of $x^2 = 2$ in $\mathbb{Q}_p$.)

It is in fact easy to see why $\mathbb{Q}_5$ does not contain a square root of 2: assume that $x^2 = a$ in $\mathbb{Q}_p$ for some odd prime $p \nmid a$; then $1 = |a|_p = |x^2|_p = |x|_p^2$, hence $|x|_p = 1$ and x is a unit in $\mathbb{Q}_p$, in particular an element of $\mathbb{Z}_p$ (observe that $\mathbb{Z}_p$ consists of all $x \in \mathbb{Q}_p$ with $|x|_p \le 1$). Now if $x^2 = a$ in $\mathbb{Z}_p$, then we can project this equality down to $\mathbb{Z}/p\mathbb{Z}$ using π_1, and we get $x^2 \equiv a \bmod p$. Thus if $x^2 = a$ in $\mathbb{Q}_p$, then we necessarily must have $(a/p) = +1$.

We now prove the converse; theorems of this kind (giving conditions modulo p for solvability of equations in $\mathbb{Z}_p$) are called Hensel's lemma.

Theorem 8. *For odd primes $p \nmid a$ and $a \in \mathbb{Z}$, the equation $x^2 = a$ has a solution in $\mathbb{Z}_p$ if and only if $(a/p) = +1$.*

Proof. Assume that $(a/p) = +1$; then there is some integer $0 < x_0 < p$ with $x_0^2 \equiv a \bmod p$. Now we use Newton's method: given an approximation x_n, we construct a better approximation using $x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)} = x_{n+1} - \frac{x_n^2 - a}{2x_n}$.

Correct Limit: show that $|x_{n+1}^2 - a|_p < |x_n^2 - a|_p$. This is easy since $x_{n+1}^2 - a = \left(\frac{x_n^2 - a}{2x_n}\right)^2$.

Convergence: show that $|x_{n+1} - x_n|_p < |x_n - x_{n-1}|_p$. This follows from preceding claim. Details are left as homework. □

Similarly, it can be proved that an odd integer a is a square in $\mathbb{Z}_2$ if and only if $a \equiv 1 \bmod 8$.

These results have drastic consequences. Consider e.g. the field $\mathbb{Q}_5$ of 5-adic numbers and look at all its quadratic extensions $\ldots$, $\mathbb{Q}_5(\sqrt{-1})$, $\mathbb{Q}_5(\sqrt{2})$, $\mathbb{Q}_5(\sqrt{3})$, $\mathbb{Q}_5(\sqrt{5})$, $\ldots$; then the fact that $(-1/p) = +1$ shows that $\mathbb{Q}_5(\sqrt{-1}) = \mathbb{Q}_5$, and similarly $(6/5) = +1$ implies $\mathbb{Q}_5(\sqrt{2}) = \mathbb{Q}_5(\sqrt{3})$. Going on like this one very soon discovers that $\mathbb{Q}_5$ has at most three quadratic extensions, namely $\mathbb{Q}_5(\sqrt{2})$, $\mathbb{Q}_5(\sqrt{5})$, and $\mathbb{Q}_5(\sqrt{10})$.

This surprising fact generalizes to all $\mathbb{Q}_p$ with odd p: if a is a nonsquare modulo p, then the only quadratic extensions of $\mathbb{Q}_p$ are $\mathbb{Q}_p(\sqrt{a})$, $\mathbb{Q}_p(\sqrt{p})$, and $\mathbb{Q}_p(\sqrt{ap})$. The prime 2 behaves differently: there are exactly 7 quadratic extensions of $\mathbb{Q}_2$, and they are generated by $\sqrt{-1}$, $\sqrt{5}$, and $\sqrt{2}$.

You should view this as part of the simplicity of p-adic numbers: theorems on quadratic extensions of these fields can be proved almost by inspection!

2. Torsion Points and p-adic Numbers

Recall that our goal is to study torsion points in $E(\mathbb{Q})$. So where do the p-adic fields $\mathbb{Q}_p$ come in? Here's how. First of all, the inclusion $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$ for every prime p implies that $E(\mathbb{Q}) \hookrightarrow E(\mathbb{Q}_p)$; the reason why $E(\mathbb{Q}_p)$ is important for understanding torsion points is that the image of $E(\mathbb{Q})$ in $E(\mathbb{Q}_p)$ can be located rather precisely. The tool for doing so is the reduction map, which will be defined on the whole projective plane.

In fact, consider a point P in the projective plane $\mathbb{P}^2\mathbb{Q}$. Rescaling if necessary we may assume that $P = [x : y : z]$ for $x, y, z \in \mathbb{Z}_p$, and if we assume in addition that not all three coordinates are divisible by p, then this representation is unique up to multiplication by units. Let $\overline{x} = x \bmod p$ be the reduction modulo p of the p-adic number; the point $\overline{P} = [\overline{x} : \overline{y} : \overline{z}]$ is called the reduction of P (with respect to p).

Now consider an elliptic curve $E : y^2 = x^3 + ax + b$ with $a, b \in \mathbb{Z}$. Reduction modulo p of points on $E(\mathbb{Q}_p)$ yield points defined over $\mathbb{F}_p$; note, however, that E might be singular over $\mathbb{F}_p$. If E is an elliptic curve over $\mathbb{F}_p$, that is, if $p \nmid \Delta$, then we say that E has good reduction at p; otherwise we talk about bad reduction. In any case, the inverse image E_0 of $E_{\mathrm{ns}}(\mathbb{F}_p)$ under the reduction map is a subgroup of $E(\mathbb{Q}_p)$, and the reduction map induces a surjective group homomorphism $E_0 \longrightarrow E_{\mathrm{ns}}(F_p)$. The kernel of this map is called the kernel of redeuction and denoted by E_1. By definition, we have the exact sequence

$$0 \longrightarrow E_1 \longrightarrow E_0 \longrightarrow E_{\mathrm{ns}}(\mathbb{F}_p) \longrightarrow 0.$$

One of the theorems we will prove is

Theorem 9. $E_1 \simeq \mathbb{Z}_p$.

In particular E_1 is torsion free. This implies that torsion points in $E(\mathbb{Q})$ cannot lie in E_1, hence $E(\mathbb{Q})_{\rm tors}$ must inject into $E(\mathbb{Q}_p) \setminus E_1$. Thus the reduction of some torsion point $[x:y:z]$ different from $\mathcal{O}$ must land on some point $[\overline{x}:\overline{y}:\overline{z}] \in E(\mathbb{F}_p)$ in the affine plane, which implies $p \nmid \overline{z}$. Thus the point P has affine coordinates $(X,Y) = (\frac{x}{z}, \frac{y}{z})$ with $p \nmid z$, in other words: $E(\mathbb{Q})_{\rm tors} \subseteq E(\mathbb{Z}_p)$ for every prime p. This implies that the coordinates of a torsion point are integers:

Theorem 10. *Let $E: y^2 = x^3 + ax + b$ be an elliptic curve with $a, b \in \mathbb{Z}$. Then any torsion point $P = (x,y) \in E(\mathbb{Q})_{\rm tors} \setminus \{\mathcal{O}\}$ has integral coordinates: $x, y \in \mathbb{Z}$.*

In a similar vein, we have

Theorem 11. *Let $E: y^2 = x^3 + ax + b$ be an elliptic curve with $a, b \in \mathbb{Z}$. If E has good reduction at p, then there is an injective group homomorphism $E(\mathbb{Q})_{\rm tors} \hookrightarrow E(\mathbb{F}_p)$.*

Proof. Since $p \nmid \Delta$, we have $E_{\rm ns}(\mathbb{F}_p) = E(\mathbb{F}_p)$. Thus $E_0 = E(\mathbb{Q}_p)$, and the composition of the maps $E(\mathbb{Q}_p)_{\rm tors} \longrightarrow E(\mathbb{Q}_p) \longrightarrow E_0/E_1 \simeq E(\mathbb{F}_p)$ is a group homomorphism with kernel $E(\mathbb{Q}_p)_{\rm tors} \cap E_1$. Since E_1 is torsion free, the map is injective. Composing this injection with the injective group homomorphism $E(\mathbb{Q})_{\rm tors} \longrightarrow E(\mathbb{Q}_p)_{\rm tors}$ proves the claim. □

This result is very useful for bounding the torsion groups of families of elliptic curves. For example, the curves $E_p: y^2 = x^3 + px$ for primes $p \ge 5$ have good reduction at 3, hence $\#E(\mathbb{Q})_{\rm tors} \le \#E(\mathbb{F}_3) \le 4$. Since $(0,0)$ is a point of order 2 (and the only one), we must have $E(\mathbb{Q})_{\rm tors} \simeq \mathbb{Z}/2\mathbb{Z}$ or $E(\mathbb{Q})_{\rm tors} \simeq \mathbb{Z}/4\mathbb{Z}$.

Finally, let us now derive the most famous result about torsion points; it was first proved by Nagell (a Scandinavian number theorist) in 1935 using Weierstrass $\wp$-functions; the investigation of elliptic curves over p-adic fields was started in 1937 by Elisabeth Lutz, a student of A. Weil.

Theorem 12 (Theorem of Nagell-Lutz)**.** *Let $E: y^2 = x^3 + ax + b$ be an elliptic curve with $a, b \in \mathbb{Z}$. If (x,y) is a torsion point on E, then $y = 0$ or $y^2 \mid (4a^3 + 27b^2)$.*

This allows us to determine the torsion subgroup of an elliptic curve with small discriminant very quickly. Note, however, that the theorem only says that torsion points are integral: not every integral point is a torsion point.

The Theorem of Nagell-Lutz is a simple consequence of Theorem 10. In fact, it is sufficient to prove the following

Lemma 13. *If $P = (x_P, y_P)$ is an affine point on $E: y^2 = x^3 + ax + b$, and if P and $2P$ have integral coordinates, then $y_P = 0$ or $y_P^2 \mid D = 4a^3 + 27b^2$.*

Proof. The addition formulas give

$$x_{2P} = \frac{\phi(x_P)}{4\psi(x_P)} \quad \text{with} \quad \begin{cases} \phi(X) &= X^4 - 2aX^2 - 8bX + a^2 \text{ and} \\ \psi(X) &= X^3 + aX + b \end{cases}$$

With $f(X) = 3X^2 + 4a$ and $g(X) = 3X^3 - 5aX - 27b$ we can immediately verify that $f(X)\phi(X) - g(X)\psi(X) = D$. Putting $X = x_P$ in this identity, and observing that $\phi(x_P) = 4x_{2P}\psi(x_P)$ and $\psi(x_P) = y_P$, we deduce

$$y_P^2[4x_{2P}f(x_P) - g(x_P)] = D.$$

Since x_P, y_P and x_{2P} are integers by assumption, this implies that $y_P^2 \mid D$. □

It remains to study the reduction map and prove that E_1 is torsion free.