Hasse-Minkowski theorem, lec 3: p-adic numbers

3.0) Introduction

p-adic numbers (a full name should be "p-adic rational numbers") relative to p-adic integers are like usual rational numbers relative to integers. Recall that a rational number can be thought of as a fraction: $\frac{a}{b}$ ($a \in \mathbb{Z}$, $b \in \mathbb{Z} \setminus \{0\}$). Two such fractions $\frac{a}{b}$ & $\frac{c}{d}$ are equal if $ad = bc$, they can be added & multiplied

$$\frac{a}{b} + \frac{c}{d} := \frac{ad+bc}{bd}, \quad \frac{a}{b}\frac{c}{d} := \frac{ac}{bd}.$$

Moreover, any $\frac{a}{b} \in \mathbb{Q}$ with $a \neq 0$ can be inverted: $\left(\frac{a}{b}\right)^{-1} = \frac{b}{a}$.

3.1) Definition of $\mathbb{Q}_p$

We can do the same for p-adic integers. We define p-adic numbers as fractions, i.e. expressions of the form $\frac{a}{b}$ ($a \in \mathbb{Z}_p$, $b \in \mathbb{Z}_p \setminus \{0\}$) where, by definition, $\frac{a}{b} = \frac{c}{d}$ if $ad = bc$. They can be added (& subtracted), multiplied & inverted just as fractions representing rational numbers.

But in a way p-adic numbers behave easier than

rational numbers: it's enough to consider denominators of the form p^k. To see this we need a lemma:

Lemma: Any $b \in \mathbb{Z}_p \setminus \{0\}$ can be written as $p^k b'$, where $k \geq 0$ & $b' \in \mathbb{Z}_p$ is invertible

Proof:

Write $b = \sum_{i=k}^{\infty} b_i p^i$ w. $b_k \neq 0$. Set $b' = \sum_{i=0}^{\infty} b_{i+k} p^i$. Note that: b' is invertible by Sec 2.3. Then $b = p^k b'$: this boils down to: $\sum_{i=k}^{m} b_i p^i \equiv p^k \sum_{i=0}^{k} b_{i+k} p^i \bmod p^m \; \forall \; m > k$, which is easy to see. □

Corollary: Any nonzero $a \in \mathbb{Q}_p$ can be uniquely written as $p^k c'$, where $k \in \mathbb{Z}$ & c' is an invertible element of $\mathbb{Z}_p$ (for $k<0$, by definition, $p^k c' = \frac{c'}{p^{-k}}$).

Proof:

Existence: Write $a = \frac{a}{b}$ w. $a, b \in \mathbb{Z}_p$. By Lemma, $a = p^\ell a'$; $b = p^k b'$ with invertible $a', b' \in \mathbb{Z}_p \Rightarrow \exists \; c' \in \mathbb{Z}_p$ with $c'b' = a'$; so $\frac{p^\ell a'}{p^k b'} = p^{\ell - k} c'$ & $(c')^{-1} = (a')^{-1} b'$.

Uniqueness: Assume $p^{k_1} c' = p^{k_2} c''$ in $\mathbb{Q}_p$ & $k_1 \leq k_2$. Then

$c' = p^{k_2-k_1} c''$ in $\mathbb{Z}_p$. Let $c' = \sum_{i=0}^{\infty} c_i p^i$ w. $c_0 \neq 0 \Rightarrow c'' = \sum_{i=0}^{\infty} c_i p^{i+k_2-k_1}$.
Since c'' is invertible, $k_2 = k_1$ & $c' = c''$. □

Writing $c' = \sum_{i=0}^{\infty} c_i p^i$ we get $\alpha = \sum_{i=k}^{\infty} c_{i-k} p^i$, which is how one usually writes p-adic numbers. The number k is called the order of α & denoted by $\mathrm{ord}(\alpha)$.

Example: $p=3$, then $\frac{1}{6} = \frac{1}{3}\cdot\frac{1}{2} = \frac{1}{3}(2 + \sum_{i=1}^{\infty} 3^i) = 2\cdot 3^{-1} + \sum_{i=0}^{\infty} 3^i \in \mathbb{Q}_3$, $\mathrm{ord}(\frac{1}{6}) = -1$.

Remarks

1) We have $\mathrm{ord}(\alpha\beta) = \mathrm{ord}(\alpha) + \mathrm{ord}(\beta)$ $\forall\, \alpha, \beta \in \mathbb{Q}_p \setminus \{0\}$:
$\alpha = p^{\ell} \sum_{i=0}^{\infty} a_i p^i$, $\beta \in p^{k} \sum_{i=0}^{\infty} b_i p^i$ w. $a_0, b_0 \in \{1, \dots p-1\} \Rightarrow$
$\alpha\beta = p^{\ell+k} \sum_{i=0}^{\infty} c_i p^i$ & $c_0 \equiv a_0 b_0 \bmod p \Rightarrow c_0 \neq 0$.

2) $\mathbb{Q}$ can be viewed as a subset of $\mathbb{Q}_p$ compatibly with all arithmetic operations (just as $\mathbb{Z} \subset \mathbb{Z}_p$).

Exercise*: $\mathbb{Q} = \{\sum_{i=k}^{\infty} a_i p^i \mid \exists\, \ell \text{ s.t. } (a_i)_{i \geq \ell} \text{ is periodic}\}$ ($\supset$ is easier & $\subset$ is a *-part).

3.2) Complete squares in $\mathbb{Q}_p$

We will need to study quadratic forms with coefficients in $\mathbb{Q}_p$. Our first step is to determine complete squares – elements α^2 for $\alpha \in \mathbb{Q}_p \setminus \{0\}$.

First of all, $\text{ord}(\alpha^2) = 2\,\text{ord}(\alpha)$ must be even. Now take $\beta \in \mathbb{Q}_p \setminus \{0\}$ with $\text{ord}(\beta) = 2l$ ($l \in \mathbb{Z}$). It's a complete square if and only if $p^{-2l}\beta$ is so. Note that $p^{-2l}\beta$ is of the form $\sum_{i=0}^{\infty} b_i p^i$ w. $b_0 \in \{1, \dots p-1\}$ & if $\beta = \alpha^2$, then $\text{ord}(\alpha) = 0$ so $\alpha = \sum_{i=0}^{\infty} a_i p^i$ w. $a_0 \in \{1, \dots p-1\}$. In particular, $b_0 = a_0^2$ in $\mathbb{Z}/p\mathbb{Z}$.

For $p > 2$, there exactly $\frac{p-1}{2}$ complete squares in $\mathbb{Z}/p\mathbb{Z}$ (called quadratic residues, the remaining $\frac{p-1}{2}$ nonzero elements are quadratic non-residues). Note that if $b_0 = a_0^2$, then $x^2 = b_0$ for $x \in \mathbb{Z}/p\mathbb{Z} \Rightarrow x_0 = \pm a_0$.

Lemma 1: Assume $p \neq 2$. Let $\beta = \sum_{i=0}^{\infty} b_i p^i \in \mathbb{Z}_p$ w. $b_0 \neq 0$. If $b_0 = a_0^2$ in $\mathbb{Z}/p\mathbb{Z}$, then there is unique α of the form

$$\alpha = \sum_{i=0}^{\infty} a_i p^i \text{ w. } \beta = \alpha^2.$$

Proof: We apply the general algorithm for finding p-adic solutions to polynomial equations from Sec. 2.3: we find $a_k \in \{0,1,..,p-1\}$ recursively from

(*) $b_0 + b_1 p + ... + b_k p^k \equiv (a_0 + ... + a_{k-1} p^{k-1} + a_k p^k)^2 \mod p^{k+1}$

The base of recursion is our assumption that $b_0 \equiv a_0^2 \mod p$.

Now suppose $K \geq 1$ & (*) holds for $K-1 \Leftrightarrow \exists\, c \in \mathbb{Z}$ s.t. $b_0 + .. + b_{K-1} p^{K-1} + p^K c = (a_0 + ... + a_{K-1} p^{K-1})^2$. Then mod p^{K+1} we have

$(a_0 + .. + a_{k-1} p^{k-1} + a_k p^k)^2 = (a_0 + ... + a_{k-1} p^{k-1})^2 + 2(a_0 + ... + a_{k-1} p^{k-1}) a_k p^k +$

$a_k^2 p^{2k} \equiv [2k \geq k+1]\, b_0 + ... + b_{k-1} p^{k-1} + p^k c + 2 a_0 a_k p^k \mod p^{k+1}$

Then (*) reduces to

$$2 a_0 a_k \equiv b_k - c \mod p$$

that has a unique solution $a_k \in \mathbb{Z}/p\mathbb{Z}$ b/c $2a_0 \not\equiv 0 \mod p$ - here we used that $p \neq 2$ □

Now we proceed to the case $p=2$, which is more difficult. As before, the order of a complete square must be even. It remains to determine complete squares of order 0, i.e. $\beta = 1 + \sum_{i=1}^{\infty} b_i p^i$. If $\beta = y^2$, then $ord(y) = 0 \Rightarrow y = 1 + 2x$ for $x \in \mathbb{Z}_p$.

Then the equation becomes

$$\beta = (1+2x)^2 = 1 + 4(x+x^2) \iff \sum_{i=1}^{\infty} b_i p^i = 4(x+x^2)$$

In order for this to have solution we need to have $b_1 = b_2 = 0$ (b/c ord(x) or ord(x+1) > 0). Arguing as in the proof of Lemma 1, we arrive at the following (the proof is an exercise)

Lemma 2: The equation $x + x^2 = \sum_{i=3}^{\infty} b_i p^{i-3}$ has exactly one order 0 ("odd") solution & exactly one order > 0 ("even") solution. In particular, $b = 1 + \sum_{i=1}^{\infty} b_i p^i$ is a complete square $\iff b_1 = b_2 = 0$.

Side remark: In both lemmas we have the same pattern: we have a polynomial $f \in \mathbb{Z}_p[x]$ with the property that ∀ solution, say, a_0, to $f(a_0) = 0$ in $\mathbb{Z}/p\mathbb{Z}$, there is a unique solution $\alpha = \sum_{i=0}^{\infty} a_i p^i$ to $f(\alpha) = 0$ in $\mathbb{Z}_p$. There's a general result in this direction known as the Hensel Lemma (Hensel was a German mathematician who first formally defined p-adic numbers in 1893).

To state it note that to a polynomial $f(x) \in \mathbb{Z}_p[x]$ we can formally assign its derivative $f'(x)$: if $f(x) = \sum_{j=0}^{n} a_j x^j$, then $f'(x) = \sum_{j=1}^{n} j a_j x^{j-1}$. The Hensel lemma states

if $a_0 \in \{0, 1, \ldots p-1\}$ satisfies $f(a_0) \equiv 0 \bmod p$, $f'(a_0) \not\equiv 0 \bmod p$, then there's unique $\alpha = \sum_{i=0}^{\infty} a_i p^i \in \mathbb{Z}_p$ s.t. $f(\alpha) = 0$ in $\mathbb{Z}_p$

Exercise*: • prove this (hint: "Taylor decomposition": $f(x) = \sum_{j=0}^{\infty} \frac{f^{(j)}(\alpha)}{j!} (x-\alpha)^j \quad \forall \alpha \in \mathbb{Z}_p$, where $f^{(j)}$ is the jth iterated derivative).

• Google "Newton method."