Hensel's Analogy and the p-adic Numbers

MATH6007/AMSI ACE Algebraic Number Theory

Declan Fletcher

Overview of the talk

1. Hensel's Analogy.
2. p-adic valuations and absolute values.
3. Ostrowski's theorem.
4. The p-adic numbers.
5. Series in $\mathbb{Q}_p$.
6. Hensel's lemma.
7. The Local–Global Principle.

Hensel's Analogy

$\mathbb{C}[t]$	$\mathbb{Z}$
$\mathrm{Frac}(\mathbb{C}[t]) = \mathbb{C}(t)$	$\mathrm{Frac}(\mathbb{Z}) = \mathbb{Q}$
Prime ideals $(t-\alpha)$	Prime ideals (p)
$\displaystyle\sum_{i=0}^{m} a_i (t-\alpha)^i$	$\displaystyle\sum_{i=0}^{m} a_i p^i$
$\displaystyle\sum_{i \geq i_0} a_i (t-\alpha)^i$	$\displaystyle\sum_{i \geq i_0} a_i p^i$

Valuations

Fix a prime p. For $x \in \mathbb{Z}$ define

$$v_p(x) = \begin{cases} n & \text{if } x = p^n x' \text{ and } p \nmid x', \\ \infty & \text{if } x = 0. \end{cases}$$

Extend to $\mathbb{Q}$ by

$$v_p\left(\frac{a}{b}\right) = v_p(a) - v_p(b).$$

This function $v_p : \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$ is the p-adic valuation.

It satisfies the following properties:

1. $v_p(xy) = v_p(x) + v_p(y)$.
2. $v_p(x + y) \geq \min\{v_p(x), v_p(y)\}$.

Absolute values

Recall: an absolute value on a field k is a function

$$|\cdot| : k \to \mathbb{R}_{\geq 0}$$

such that

1. $|x| = 0$ if and only $x = 0$;
2. $|xy| = |x|\,|y|$;
3. $|x + y| \leq |x| + |y|$.

We call $|\cdot|$ non-archimedian if it satisfies the strong inequality:

4. $|x + y| \leq \max\{|x|, |y|\}$ for all $x, y \in k$;

otherwise we say $|\cdot|$ is archimedian.

The p-adic absolute value

Define the p-adic absolute value on $\mathbb{Q}$ by

$$|x|_p = p^{-v_p(x)}.$$

Examples:

$$|35|_7 = 7^{-v_7(5 \cdot 7)} = \frac{1}{7}$$

$$\left|\frac{11}{18}\right|_3 = 3^{-v_3\left(\frac{11}{2 \cdot 3^2}\right)} = 9$$

$|\cdot|_p$ is a non-archimedean absolute value on $\mathbb{Q}$.

Convergence with respect to $|\cdot|_p$

Recall absolute values induce metrics: $d_p(x, y) = |x - y|_p$.

Example:

$$\lim_{n\to\infty} p^n = 0,$$

since

$$\lim_{n\to\infty} |p^n - 0|_p = \lim_{n\to\infty} p^{-v_p(p^n)} = \lim_{n\to\infty} p^{-n} = 0.$$

Example:

$$\sum_{n\geq 0} p^n = \frac{1}{1-p},$$

since $1 - p^n = (1-p)\sum_{k=0}^{n-1} p^k$, so

$$\sum_{n\geq 0} p^n = \lim_{n\to\infty} \frac{1-p^n}{1-p} = \frac{1}{1-p} - \frac{1}{1-p}\lim_{n\to\infty} p^n = \frac{1}{1-p}.$$

Absolute values on a field are considered equivalent if they define the same topology.

Theorem (Ostrowski)

Every non-trivial absolute value on $\mathbb{Q}$ is equivalent to either $|\cdot|_\infty$ or $|\cdot|_p$, for some prime p.

Recall: $\mathbb{R}$ is the completion of $\mathbb{Q}$ with respect to $|\cdot|_\infty$.

$\mathbb{Q}_p$ is the completion of $\mathbb{Q}$ with respect to $|\cdot|_p$.

This means $\mathbb{Q}_p$ is a field with an absolute value $|\cdot|_p$ such that:

1. There is an inclusion $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$, and the absolute value induced on $\mathbb{Q}$ is the p-adic absolute value;
2. The image of $\mathbb{Q}$ under this inclusion is dense in $\mathbb{Q}_p$;
3. $\mathbb{Q}_p$ is complete with respect to the absolute value $|\cdot|_p$.

The p-adic integers

With respect to $|\cdot|_p$, the set of integers has bounded norm:

$$|1|_p = 1, \qquad |1+1|_p \leq \max\{|1|_p, |1|_p\} = 1,$$

$$|2+1| \leq \max\{|1|_p, |2|_p\} \leq 1, \ \ldots$$

The ring of *p-adic integers* is

$$\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p \leq 1\}.$$

Claim: The series $\sum_{n \geq 0} a_n$ converges if and only if $\lim_{n \to \infty} a_n = 0$.

Proof: A sequence (x_n) is Cauchy in $\mathbb{Q}_p$ if and only if

$$\lim_{n \to \infty} |x_{n+1} - x_n|_p = 0.$$

Suppose for $n \geq N$ that $|x_{n+1} - x_n| < \varepsilon$. Then for $m > n$,

$$\begin{aligned}
&|x_m - x_n|_p \\
&= |(x_m - x_{m-1}) + (x_{m-1} - x_{m-2}) + \ldots + (x_{n+1} - x_n)|_p \\
&\leq \max\{|x_m - x_{m-1}|_p, \ldots, |x_{n+1} - x_n|_p\} < \varepsilon.
\end{aligned}$$

For $x_n = \sum_{k=0}^{n} a_k$, we need

$$\lim_{n \to \infty} |x_{n+1} - x_n| = \lim_{n \to \infty} |a_n| = 0.$$

Representing p-adic numbers

The claim implies

$$\sum_{i \geq i_0} a_i p^i, \qquad i_0 \in \mathbb{Z},\ 0 \leq a_i \leq p-1,$$

always converges!

Every p-adic number has a unique expression of the above form. In particular,

$$\mathbb{Z}_p = \left\{ \sum_{i \geq 0} a_i p^i : 0 \leq a_i \leq p-1 \right\}.$$

It follows that $\mathbb{Z}_p / p\mathbb{Z}_p \cong \mathbb{Z}/p\mathbb{Z}$.

Hensel's lemma

Theorem

Let $F(X) \in \mathbb{Z}_p[X]$. Suppose there exists $\alpha_1 \in \mathbb{Z}_p$ such that

$$F(\alpha_1) \equiv 0 \mod p\mathbb{Z}_p, \qquad F'(\alpha_1) \not\equiv 0 \mod p\mathbb{Z}_p.$$

Then there exists $\alpha \in \mathbb{Z}_p$ such that $\alpha \equiv \alpha_1 \mod p\mathbb{Z}_p$ and $F(\alpha) = 0$.

Sketch: Construct a sequence $(\alpha_n) \subseteq \mathbb{Z}_p$ such that for all $n \geq 1$,

$$F(\alpha_n) \equiv 0 \mod p^n\mathbb{Z}_p, \qquad \alpha_{n+1} \equiv \alpha_n \mod p^n\mathbb{Z}_p.$$

The sequence is then Cauchy and there is a limit α. By continuity, $F(\alpha) = 0$. By construction, $\alpha \equiv \alpha_1 \mod p\mathbb{Z}_p$.

Sketch, continued

Goal:

$$(1)\ F(\alpha_n) \equiv 0 \mod p^n\mathbb{Z}_p \qquad (2)\ \alpha_{n+1} \equiv \alpha_n \mod p^n\mathbb{Z}_p$$

Write $\alpha_{n+1} = \alpha_n + ap^n$ so (2) holds. We want to solve for $a \in \mathbb{Z}_p$ so (1) holds:

$$F(\alpha_{n+1}) = F(\alpha_n + ap^n) \equiv 0 \mod p^{n+1}\mathbb{Z}_p.$$

By Taylor expansion,

$$F(\alpha_n) + F'(\alpha_n)ap^n \equiv 0 \mod p^{n+1}\mathbb{Z}_p.$$

Our assumptions imply there is a unique solution

$$a \equiv -\frac{F(\alpha_n)}{p^n F'(\alpha_n)} \mod p\mathbb{Z}_p.$$

An application of Hensel's lemma

Let

$$F(X) = X^{p-1} - 1.$$

Since $\mathbb{F}_p^\times$ is cyclic of order $p-1$, for each $\alpha_1 = 1, 2, \ldots, p-1$,

$$F(\alpha_1) \equiv 0 \mod p\mathbb{Z}_p.$$

Also,

$$F'(\alpha_1) \equiv (p-1)(\alpha_1)^{p-2} \not\equiv 0 \mod p\mathbb{Z}_p.$$

The theorem implies each α_1 lifts to a distinct $(p-1)^{\text{th}}$ root of unity in $\mathbb{Z}_p$.

Local-Global Principle

$$\begin{array}{c} \text{Global} \\ \text{solutions} \\ \text{in } \mathbb{Q} \end{array} \quad \leftrightsquigarrow \quad \begin{array}{c} \text{Local} \\ \text{solutions} \\ \text{in } \mathbb{Q}_p,\ p \leq \infty \end{array}$$

The Hasse–Minkowski Theorem

Let $F(X_1, \ldots, X_n)$ be a quadratic form with rational coefficients. Then $F(X_1, \ldots, X_n) = 0$ has nontrivial solutions in $\mathbb{Q}$ if and only if it has nontrivial solutions in $\mathbb{Q}_p$ for each $p \leq \infty$.

References

M. Baker, *Algebraic Number Theory Course Notes*,
https://sites.google.com/view/mattbakermath/publications

F. Q. Gouvêa, *p-adic Numbers*, Springer-Verlag, Berlin, 1997.