NOTES ON DIOPHANTINE APPROXIMATION

Jan-Hendrik Evertse

January 29, 2010

9 $p$-adic Numbers

Literature:

9.1 Absolute values.

Let $p$ be a prime number. The $p$-adic absolute value $|\cdot|_p$ on $\mathbb{Q}$ is defined as follows: if $a \in \mathbb{Q}$, $a \neq 0$ then write $a = p^m b/c$ where $b, c$ are integers not divisible by $p$ and put $|a|_p = p^{-m}$; further, put $|0|_p = 0$.

Example. Let $a = 2^{-7}3^85^{-3}$. Then $|a|_2 = 2^7$, $|a|_3 = 3^{-8}$, $|a|_5 = 5^3$, $|a|_p = 1$ for $p \geq 7$.

We give some properties:

\begin{align*}
|ab|_p &= |a|_p |b|_p \text{ for } a, b \in \mathbb{Q}^*; \\
|a + b|_p &\leq \max(|a|_p, |b|_p) \text{ for } a, b \in \mathbb{Q}^* \text{ (ultrametric inequality).}
\end{align*}

Notice that the last property implies that

\[ |a + b|_p = \max(|a|_p, |b|_p) \text{ if } |a|_p \neq |b|_p. \]

It is common to write the ordinary absolute value $|a| = \max(a, -a)$ on $\mathbb{Q}$ as $|a|_\infty$, to call $\infty$ the ‘infinite prime’ and to define $M_\mathbb{Q} := \{\infty\} \cup \{\text{primes}\}$. Then we have the important product formula:

\[ \prod_{p \in M_\mathbb{Q}} |a|_p = 1 \text{ for } a \in \mathbb{Q}, a \neq 0. \]
We define more generally absolute values on fields. Let $K$ be any field. An absolute value on $K$ is a function $|\cdot| : K \to \mathbb{R}_{\geq 0}$ with the following properties:

\[
|ab| = |a| \cdot |b| \text{ for } a, b \in K;
\]
\[
|a + b| \leq |a| + |b| \text{ for } a, b \in K \text{ (triangle inequality)};
\]
there is $a \in K$ with $|a| \notin \{0, 1\}$.

Notice that these properties imply that $|0| = 0$, $|1| = 1$ and $|a| \neq 0$ if $a \neq 0$. The absolute value $|\cdot|$ is called non-archimedean if the triangle inequality can be replaced by the stronger ultrametric inequality

\[
|a + b| \leq \max(|a|, |b|) \text{ for } a, b \in K.
\]

An absolute value not satisfying the ultrametric inequality is called archimedean.

If $K$ is a field with absolute value $|\cdot|$ and $L$ an extension of $K$, then an extension or continuation of $|\cdot|$ to $L$ is an absolute value on $L$ whose restriction to $K$ is $|\cdot|$.

**Examples.**

1) The ordinary absolute value $|\cdot|$ on $\mathbb{Q}$ is archimedean, while the $p$-adic absolute values are all non-archimedean.

2) Let $K$ be any field, and $K(t)$ the field of rational functions of $K$. For a polynomial $f \in K[t]$ define $|f| = 0$ if $f = 0$ and $|f| = e^{\deg f}$ if $f \neq 0$. Further, for a rational function $f/g$ with $f, g \in K[t]$ define $|f/g| = |f|/|g|$. Verify that this defines a non-archimedean absolute value on $K(t)$.

Two absolute values $|\cdot|_1, |\cdot|_2$ on $K$ are called equivalent if there is $\alpha > 0$ such that $|x|_2 = |x|^\alpha_1$ for all $x \in K$. We state without proof the following result:

**Theorem 9.1.1 (Ostrowski)** Every absolute value on $\mathbb{Q}$ is equivalent to either the ordinary absolute value or a $p$-adic absolute value for some prime number $p$.

### 9.2 Completions.

Let $K$ be a field, $|\cdot|$ an absolute value on $K$, and $\{a_k\}_{k=0}^{\infty}$ a sequence in $K$.

We say that $\{a_k\}_{k=0}^{\infty}$ converges to $\alpha$ with respect to $|\cdot|$ if $\lim_{k \to \infty} |a_k - \alpha| = 0$.

Further, $\{a_k\}_{k=0}^{\infty}$ is called a Cauchy sequence with respect to $|\cdot|$ if $\lim_{m,n \to \infty} |a_m - a_n| = 0$.

Notice that any convergent sequence is a Cauchy sequence.

We say that $K$ is complete with respect to $|\cdot|$ if every Cauchy sequence w.r.t. $|\cdot|$ in $K$ converges to a limit in $K$.

J.-H. Evertse, Diophantine Approximation
For instance, \( \mathbb{R} \) and \( \mathbb{C} \) are complete w.r.t. the ordinary absolute value. Ostrowski proved that any field complete w.r.t. an archimedean absolute value is isomorphic to \( \mathbb{R} \) or \( \mathbb{C} \). Every field \( K \) with an absolute value can be extended to an up to isomorphism complete field, the completion of \( K \).

**Theorem 9.2.1** Let \( K \) be a field with absolute value \( |\cdot| \). There is an up to isomorphism unique extension field \( \tilde{K} \) of \( K \), called the completion of \( K \), having the following properties:

(i) \( |\cdot| \) can be continued to an absolute value on \( \tilde{K} \), also denoted \( |\cdot| \), such that \( \tilde{K} \) is complete w.r.t. \( |\cdot| \);

(ii) \( K \) is dense in \( \tilde{K} \), i.e., every element of \( \tilde{K} \) is the limit of a sequence from \( K \).

**Proof.** Basically one has to mimic the construction of \( \mathbb{R} \) from \( \mathbb{Q} \) or the construction of a completion of a metric space in topology. We give a sketch. Cauchy sequences, limits, etc. are all with respect to \( |\cdot| \).

Call two Cauchy sequences \( \{a_k\} = \{a_k\}_{k=0}^{\infty} \) and \( \{b_k\} \) in \( K \) equivalent if

\[
\lim_{k \to \infty} |a_k - b_k| = 0.
\]

Denote the equivalence class of \( \{a_k\} \) by \( [\{a_k\}] \). Let \( \tilde{K} \) denote the collection of equivalence classes of Cauchy sequences.

We define addition and multiplication on \( \tilde{K} \) by

\[
[\{a_k\}] + [\{b_k\}] = [\{a_k + b_k\}], \quad [\{a_k\}] \cdot [\{b_k\}] = [\{a_k b_k\}].
\]

One can show that these operations are well-defined and that with these operations, \( \tilde{K} \) is a field, with zero-element \( [\{0\}] \) and one-element \( [\{1\}] \) (equivalence classes of constant sequences).

The absolute value \( |\cdot| \) on \( \tilde{K} \) is defined by \( |[\{a_k\}]| = \lim_{k \to \infty} |a_k| \) (limit in \( \mathbb{R} \)). This limit exists since \( |a_m - a_n| \to 0 \) as \( m, n \to \infty \) (where the outer absolute value is the one on \( \mathbb{R} \)). Further, it is independent of the choice of the representative, and satisfies the conditions of an absolute value.

We may view \( K \) as a subfield of \( \tilde{K} \) by identifying \( a \in K \) with the equivalence class of the constant sequence \( \{\{a_k\}\} \). Thus, the absolute value \( |\cdot| \) on \( \tilde{K} \) just defined is an extension of the absolute value on \( K \).

With the absolute value on \( \tilde{K} \) defined above, and with the identification of \( a \) with \( \{\{a\}\} \), one has \( \lim_{n \to \infty} |[\{a_k\}] - a_n| = 0 \). So \( K \) is dense in \( \tilde{K} \).

To prove that \( \tilde{K} \) is complete, one takes a Cauchy sequence \( \{\alpha_k\} \) in \( \tilde{K} \), constructs from this a Cauchy sequence \( \{b_k\} \) in \( K \) by taking a very good approximation \( b_k \) of \( \alpha_k \), takes the limit in \( \tilde{K} \) of \( \{b_k\} \), and shows that this is also the limit of \( \{\alpha_k\} \).

J.-H. Evertse, Diophantine Approximation
Finally, if $K'$ is another complete field with absolute value extending that on $K$ such that $K$ is dense in $K'$ one obtains an isomorphism from $\tilde{K}$ to $K'$ as follows: Take $\alpha \in \tilde{K}$. Choose a sequence $\{a_k\}$ in $K$ converging to $\alpha$; this is necessarily a Cauchy sequence. Then map $\alpha$ to the limit of $\{a_k\}$ in $K'$.

9.3 $p$-adic Numbers and $p$-adic integers

Let $p$ be a prime number.

The completion of $\mathbb{Q}$ with respect to $|\cdot|_p$ is called the field of $p$-adic numbers, notation $\mathbb{Q}_p$.

The continuation of $|\cdot|_p$ to $\mathbb{Q}_p$ is also denoted by $|\cdot|_p$.

Convergence, limits, Cauchy sequences and the like will all be with respect to $|\cdot|_p$.

Lemma 9.3.1 (i) The absolute value $|\cdot|_p$ is non-archimedean on $\mathbb{Q}_p$.

(ii) The value set of $|\cdot|_p$ on $\mathbb{Q}_p$ is $\{0\} \cup \{p^m : m \in \mathbb{Z}\}$.

Proof. (i) Let $x, y \in \mathbb{Q}_p$. Take sequences $\{x_k\}, \{y_k\}$ from $\mathbb{Q}$ converging to $x, y$, respectively. Then

$$|x + y|_p = \lim_{k \to \infty} |x_k + y_k|_p \leq \lim_{k \to \infty} \max(|x_k|_p, |y_k|_p) = \max(|x|_p, |y|_p).$$

(ii) Let $x \in \mathbb{Q}_p$, $x \neq 0$. Choose again a sequence $\{x_k\}$ in $\mathbb{Q}$ converging to $x$. Then $|x|_p = \lim_{k \to \infty} |x_k|_p$. For $k$ sufficiently large we have $|x_k|_p = p^{m_k}$ for some $m_k \in \mathbb{Z}$. Since the sequence of numbers $p^{m_k}$ converges we must have $m_k = m \in \mathbb{Z}$ for $k$ sufficiently large. Hence $|x|_p = p^m$.

The set $\mathbb{Z}_p := \{x \in \mathbb{Q}_p : |x|_p \leq 1\}$ is called the ring of $p$-adic integers.

Notice that if $x, y \in \mathbb{Z}_p$ then $|x - y|_p \leq \max(|x|_p, |y|_p) \leq 1$. Hence $x - y \in \mathbb{Z}_p$. Further, if $x, y \in \mathbb{Z}_p$ then $|xy|_p \leq 1$ which implies $xy \in \mathbb{Z}_p$. So $\mathbb{Z}_p$ is indeed a ring.

For $\alpha, \beta \in \mathbb{Q}_p$ we write $\alpha \equiv \beta$ (mod $p^m$) if $(\alpha - \beta)/p^m \in \mathbb{Z}_p$. This is equivalent to $|\alpha - \beta|_p \leq p^{-m}$.

For $p$-adic numbers, “very small” means “divisible by a high power of $p$”, and two $p$-adic numbers $\alpha$ and $\beta$ are $p$-adically close if and only if $\alpha - \beta$ is divisible by a high power of $p$.

Lemma 9.3.2 For every $\alpha \in \mathbb{Z}_p$ and every positive integer $m$ there is a unique $a_m \in \mathbb{Z}$ such that $|\alpha - a_m|_p \leq p^{-m}$ and $0 \leq a_m < p^m$.

J.-H. Evertse, Diophantine Approximation
There is a rational number $a/b$ (with coprime $a, b \in \mathbb{Z}$) such that $|\alpha - (a/b)|_p \leq p^{-m}$ since $\mathbb{Q}$ is dense in $\mathbb{Q}_p$. At most one of $a, b$ is divisible by $p$ and it cannot be $b$ since $|a/b|_p \leq 1$. Hence there is an integer $a_m$ with $ba_m \equiv a \pmod{p^m}$ and $0 \leq a_m < p^m$. Thus, $|\alpha - a_m|_p \leq \max(|\alpha - (a/b)|_p, |(a/b) - a_m|_p) \leq p^{-m}$.

This shows the existence of $a_m$. As for the unicity, if $a'_m$ is another integer with the properties specified in the lemma, we have $|a_m - a'_m|_p \leq p^{-m}$, hence $a_m \equiv a'_m \pmod{p^m}$, implying $a_m = a'_m$.

We prove some algebraic properties of the ring $\mathbb{Z}_p$.

**Theorem 9.3.3** (i) The unit group of $\mathbb{Z}_p$ is $\mathbb{Z}_p^* = \{ x \in \mathbb{Q}_p : |x|_p = 1 \}$.

(ii) The non-zero ideals of $\mathbb{Z}_p$ are $p^m\mathbb{Z}_p$ ($m = 0, 1, 2, \ldots$) and $\mathbb{Z}_p/p^m\mathbb{Z}_p \cong \mathbb{Z}/p^m\mathbb{Z}$.

**Proof.** We have $x \in \mathbb{Z}_p^* \iff x, x^{-1} \in \mathbb{Z} \iff |x|_p \leq 1, |x^{-1}|_p \leq 1 \iff |x|_p = 1$.

To prove (ii), let $I$ be a non-zero ideal of $\mathbb{Z}_p$ and choose $\alpha \in I$ for which $|\alpha|_p$ is maximal. Let $|\alpha|_p = p^{-m}$. Then $p^{-m} \alpha \in \mathbb{Z}_p^*$, hence $p^m \in I$. Further, for $\beta \in I$ we have $|\beta p^{-m}|_p \leq 1$, hence $\beta \in p^n\mathbb{Z}_p$. Hence $I \subseteq p^n\mathbb{Z}_p$. This implies $I = p^m\mathbb{Z}_p$.

The homomorphism $\mathbb{Z}/p^m\mathbb{Z} \rightarrow \mathbb{Z}/p^m\mathbb{Z}$: $a \pmod{p^m} \mapsto a \pmod{p^m}$ is clearly injective and also surjective in view of Lemma ???. Hence $\mathbb{Z}/p^m\mathbb{Z} \cong \mathbb{Z}/p^m\mathbb{Z}_p$.

**Lemma 9.3.4** Let $\{a_k\}_{k=0}^{\infty}$ be a sequence in $\mathbb{Q}_p$. Then $\sum_{k=0}^{\infty} a_k$ converges in $\mathbb{Q}_p$ if and only if $\lim_{k \to \infty} a_k = 0$.

Further, every convergent series in $\mathbb{Q}_p$ is unconditionally convergent, i.e., neither the convergence, nor the value of the series, are affected if the terms $a_k$ are rearranged.

**Proof.** Suppose that $\alpha := \sum_{k=0}^{\infty} a_k$ converges. Then $a_n = \sum_{k=0}^{n} a_k - \sum_{k=0}^{n-1} a_k \rightarrow \alpha - \alpha = 0$. Conversely, suppose that $a_k \rightarrow 0$ as $k \rightarrow \infty$. Let $\alpha_n := \sum_{k=0}^{n} a_k$. Then for any integers $m, n$ with $0 < m < n$ we have

$$|\alpha_n - \alpha_m|_p = \left| \sum_{k=m+1}^{n} a_k \right|_p \leq \max(|a_{m+1}|_p, \ldots, |a_n|_p) \rightarrow 0 \text{ as } m, n \to \infty.$$ 

So the partial sums $\alpha_n$ form a Cauchy sequence, hence must converge to a limit in $\mathbb{Q}_p$.

To prove the second part of the lemma, let $\sigma$ be a bijection from $\mathbb{Z}_{\geq 0}$ to $\mathbb{Z}_{\geq 0}$. We have to prove that $\sum_{k=0}^{\infty} a_{\sigma(k)} = \sum_{k=0}^{\infty} a_k$. Equivalently, we have to prove that $\sum_{k=0}^{M} a_k - \sum_{k=0}^{M} a_{\sigma(k)} \rightarrow 0$ as $M \to \infty$, i.e., for every $\varepsilon > 0$ there is $N_{\varepsilon}$ such that

$$\left| \sum_{k=0}^{M} a_k - \sum_{k=0}^{M} a_{\sigma(k)} \right|_p < \varepsilon \text{ for every } M > N_{\varepsilon}.$$ 

J.-H. Evertse, Diophantine Approximation
Let \( \varepsilon > 0 \). There is \( N \) such that \( |a_k|_p < \varepsilon \) for all \( k \geq p \). Choose \( N_\varepsilon \) such that \( \{\sigma(0),\ldots,\sigma(N_\varepsilon)\} \) contains \( \{0,\ldots,N\} \) and let \( M > N_\varepsilon \). Then in the sum \( S := \sum_{k=0}^M a_k - \sum_{k=0}^M a_{\sigma(k)} \), only terms \( a_k \) with \( k > N \) and \( a_{\sigma(k)} \) with \( \sigma(k) > N \) occur. Hence each term in \( S \) has \( p \)-adic absolute value \( \varepsilon \) and therefore, by the ultrametric inequality, \( |S|_p < \varepsilon \). \( \square \)

We now show that every element of \( \mathbb{Z}_p \) has a “Taylor series expansion,” and every element of \( \mathbb{Q}_p \) a “Laurent series expansion” where instead of powers of a variable \( X \) one takes powers of \( p \).

**Theorem 9.3.5 (i)** Every element of \( \mathbb{Z}_p \) can be expressed uniquely as \( \sum_{k=0}^{\infty} b_k p^k \) with \( b_k \in \{0,\ldots,p-1\} \) for \( k \geq 0 \) and conversely, every such series belongs to \( \mathbb{Z}_p \).

(ii) Every element of \( \mathbb{Q}_p \) can be expressed uniquely as \( \sum_{k=-k_0}^{\infty} b_k p^k \) with \( k_0 \in \mathbb{Z} \) and \( b_k \in \{0,\ldots,p-1\} \) for \( k \geq -k_0 \) and conversely, every such series belongs to \( \mathbb{Q}_p \).

**Proof.** We first prove part (i). First observe that by Lemma ??, a series \( \sum_{k=0}^{\infty} b_k p^k \) with \( b_k \in \{0,\ldots,p-1\} \) converges in \( \mathbb{Q}_p \). Further, it belongs to \( \mathbb{Z}_p \), since \( |\sum_{k=0}^{\infty} b_k p^k|_p \leq \max_{k \geq 0} |b_k p^k|_p \leq 1 \).

Let \( \alpha \in \mathbb{Z}_p \). Define sequences \( \{\alpha_k\}_{k=0}^{\infty} \) in \( \mathbb{Z}_p \), \( \{b_k\}_{k=0}^{\infty} \) in \( \{0,\ldots,p-1\} \) inductively as follows:

\[
\alpha_0 := \alpha;
\]

For \( k = 0,1,\ldots, \) let \( b_k \in \{0,\ldots,p-1\} \) be the integer with \( \alpha_k \equiv b_k \pmod{p} \) and put

\[
\alpha_{k+1} := (\alpha_k - b_k)/p.
\]

By induction on \( k \), one easily deduces that for \( k \geq 0 \),

\[
\alpha_k \in \mathbb{Z}_p, \quad \alpha = \sum_{j=0}^{k} b_j p^j + p^{k+1} \alpha_k.
\]

Hence \( |\alpha - \sum_{j=0}^{k} b_j p^j|_p \leq p^{-k-1} \) for \( k \geq 0 \). It follows that

\[
\alpha = \lim_{k \to \infty} \sum_{j=0}^{k} b_j p^j = \sum_{j=0}^{\infty} b_j p^j.
\]

Notice that the integer \( a_m \) from Lemma ?? is precisely \( \sum_{k=0}^{m-1} b_k p^k \). Since \( a_m \) is uniquely determined, so must be the integers \( b_k \).

We prove part (ii). As above, any series \( \sum_{k=-k_0}^{\infty} b_k p^k \) with \( b_k \in \{0,\ldots,p-1\} \) converges in \( \mathbb{Q}_p \). Let \( \alpha \in \mathbb{Q}_p \) with \( \alpha \neq 0 \). Suppose that \( |\alpha|_p = p^{k_0} \). Then \( \beta := p^{-k_0} \alpha \) has \( |\beta|_p = 1 \), so it belongs to \( \mathbb{Z}_p \). Applying (i) to \( \beta \) we get

\[
\alpha = p^{-k_0} \beta = p^{-k_0} \sum_{k=0}^{\infty} c_k p^k.
\]

J.-H. Evertse, Diophantine Approximation
9.3 \( p \)-adic Numbers and \( p \)-adic integers

with \( c_k \in \{0, \ldots, p - 1\} \) which implies (ii).

\[ \square \]

Theorem 9.3.6 Let \( \alpha = \sum_{k=-k_0}^{\infty} b_k p^k \) with \( b_k \in \{0, \ldots, p - 1\} \) for \( k \geq -k_0 \). Then
\[
\alpha \in \mathbb{Q} \iff \{b_k\}_{k=-k_0}^{\infty} \text{ is ultimately periodic.}
\]

Proof. \( \iff \) Exercise.

\( \implies \) Without loss of generality, we assume that \( \alpha \in \mathbb{Z}_p \) (if \( \alpha \in \mathbb{Q}_p \) with \( |\alpha|_p = p^{k_0} \), say, then we proceed further with \( \beta := p^{k_0} \alpha \) which is in \( \mathbb{Z}_p \)).

Suppose that \( \alpha = A/B \) with \( A, B \in \mathbb{Z} \), \( \gcd(A, B) = 1 \). Then \( p \) does not divide \( B \) (otherwise \( |\alpha|_p > 1 \)). Let \( C := \max(|A|, |B|) \). Let \( \{\alpha_k\}_{k=0}^{\infty} \) be the sequence defined in the proof of Theorem ??.

Claim. \( \alpha_k = A_k/B \) with \( A_k \in \mathbb{Z} \), \( |A_k| \leq C \).

This is proved by induction on \( k \). For \( k = 0 \) the claim is obviously true. Suppose the claim is true for \( k = m \) where \( m \geq 0 \). Then
\[
\alpha_{m+1} = \frac{\alpha_m - b_m}{p} = \frac{(A_m - b_mB)/p}{B}.
\]

Since \( \alpha_m \equiv b_m \pmod{p} \) we have that \( A_m - b_mB \) is divisible by \( p \). So \( A_{m+1} := (A_m - b_mB)/p \in \mathbb{Z} \). Further,
\[
|A_{m+1}| \leq \frac{C + (p - 1)B}{p} \leq C.
\]

This proves our claim.

Now since the integers \( A_k \) all belong to \( \{-C, \ldots, C\} \), there must be indices \( l < m \) with \( A_l = A_m \), that is, \( \alpha_l = \alpha_m \). But then, \( b_{k+m-l} = b_k \) for all \( k \geq l \), proving that \( \{b_k\}_{k=0}^{\infty} \) is ultimately periodic. \( \square \)

Examples.

(i) We determine the 3-adic expansion of \( -\frac{2}{5} \). Notice that \( \frac{1}{5} \equiv 2 \pmod{3} \).

\[
\begin{array}{ccccccc}
  k & 0 & 1 & 2 & 3 & 4 \\
  \alpha_k & -\frac{2}{5} & -\frac{4}{5} & -\frac{3}{5} & -\frac{1}{5} & -\frac{2}{5} \\
  b_k & 2 & 1 & 0 & 1 & 2
\end{array}
\]

It follows that the sequence of 3-adic digits \( \{b_k\}_{k=0}^{\infty} \) of \( -\frac{2}{5} \) is periodic with period 2, 1, 0, 1 and that
\[
-\frac{2}{5} = 2 \times 3^0 + 1 \times 3^1 + 0 \times 3^2 + 1 \times 3^3 + 2 \times 3^4 + 1 \times 3^5 + 0 \times 3^6 + 1 \times 3^7 + \cdots
\]

J.-H. Evertse, Diophantine Approximation
(ii) We determine the 2-adic expansion of $\frac{1}{56}$. Notice that $\frac{1}{56} = 2^{-3} \times \frac{1}{7}$. We start with the 2-adic expansion of $\frac{1}{7}$.

<table>
<thead>
<tr>
<th>$k$</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\alpha_k$</td>
<td>$\frac{1}{7}$</td>
<td>$-\frac{3}{7}$</td>
<td>$-\frac{5}{7}$</td>
<td>$-\frac{6}{7}$</td>
<td>$-\frac{2}{7}$</td>
</tr>
<tr>
<td>$b_k$</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

So

$$\frac{1}{7} = 1 \times 2^0 + 1 \times 2^1 + 1 \times 2^2 + 0 \times 2^3 + 1 \times 2^4 + 1 \times 2^5 + 0 \times 2^6 + \cdots,$$

$$\frac{1}{56} = 1 \times 2^{-3} + 1 \times 2^{-2} + 1 \times 2^{-1} + 0 \times 2^0 + 1 \times 2^1 + 1 \times 2^2 + 0 \times 2^3 + \cdots$$

The next result, which is a special case of Hensel’s Lemma, gives a method to compute roots of polynomials in $\mathbb{Q}_p$ (if such roots exist).

**Theorem 9.3.7** Let $f(X) \in \mathbb{Z}_p[X]$ be a non-zero polynomial. Suppose there is $a \in \mathbb{Z}$ such that $f(a) \equiv 0 \pmod{p}$, $f'(a) \not\equiv 0 \pmod{p}$.

Then there is a unique $\alpha \in \mathbb{Z}_p$ such that $f(\alpha) = 0$ and $\alpha \equiv a \pmod{p}$.

**Proof.** We define a sequence of integers $\{a_k\}_{k=0}^\infty$ such that for $k = 0, 1, 2, \ldots$,

$$0 \leq a_k < p^{2^k}, \quad f(a_k) \equiv 0 \pmod{p^{2^k}}, \quad f'(a_k) \not\equiv 0 \pmod{p}, \quad a_{k+1} - a_k \equiv 0 \pmod{p^{2^k}}.$$

Take $a_0 \in \{0, \ldots, p-1\}$ such that $a_0 \equiv a \pmod{p}$. Then $f(a_0) \equiv 0 \pmod{p}$, $f'(a_0) \not\equiv 0 \pmod{p}$.

Assume that $k \geq 0$ and that $a_k$ has been constructed. Let $a_{k+1}$ be the (necessarily unique) solution to the congruence

$$f'(a_k)(x - a_k) \equiv -f(a_k) \pmod{p^{2^{k+1}}}, \quad 0 \leq x < p^{2^{k+1}}.$$

Thus, $a_{k+1} - a_k \equiv 0 \pmod{p^{2^k}}$, implying that $f'(a_k) \not\equiv 0 \pmod{p}$.

Considering the Taylor expansion of $f$ around $x_k$, noting that the polynomials $f^{(k)}(X)/k!$ (divided derivatives) have their coefficients in $\mathbb{Z}_p$,

$$f(a_{k+1}) = f(a_k) + f'(a_k)(a_{k+1} - a_k) + \frac{f^{(2)}(a_k)}{2!}(a_{k+1} - a_k)^2 + \cdots \equiv 0 \pmod{p^{2^{k+1}}}.$$

Now

$$\lim_{k \to \infty} a_k = a_0 + \sum_{j=0}^\infty (a_{j+1} - a_j) =: \alpha$$

J.-H. Evertse, Diophantine Approximation
converges in \( \mathbb{Q}_p \) and \( f(\alpha) = \lim_{k \to \infty} f(a_k) = 0 \). It is clear that \( \alpha \equiv a \pmod{p} \).

Suppose that there are two distinct elements \( \alpha, \beta \in \mathbb{Z}_p \) such that \( f(\alpha) = f(\beta) = 0 \) and \( \alpha \equiv \beta \equiv a \pmod{p} \). Then \( f(X) = (X - \alpha)(X - \beta)g(X) \) with \( g \in \mathbb{Z}_p[X] \). Hence \( f'(X) = (X - \alpha)g(X) + (X - \beta)g(X) + (X - \alpha)(X - \beta)g'(X) \). Substituting \( X = a \) gives \( f'(a) \equiv 0 \pmod{p} \), against our assumption. \( \Box \)

The ball with center \( a \in \mathbb{Q}_p \) and radius \( r \) in the value set \( \{0\} \cup \{p^m : m \in \mathbb{Z}\} \) of \( | \cdot |_p \) is defined by \( B(a, r) := \{x \in \mathbb{Q}_p : |x - a|_p \leq r\} \). Notice that if \( b \in B(a, r) \) then \( |b - a|_p \leq r \). So by the ultrametric inequality, for \( x \in B(a, r) \) we have \( |x - b|_p \leq \max(|x - a|_p, |a - b|_p) \leq r \), i.e. \( x \in B(b, r) \). So \( B(a, r) \subseteq B(b, r) \). Similarly one proves \( B(b, r) \subseteq B(a, r) \). Hence \( B(a, r) = B(b, r) \). In other words, any point in a ball can be taken as center of the ball.

We define the \( p \)-adic topology on \( \mathbb{Q}_p \) as follows. A subset \( U \) of \( \mathbb{Q}_p \) is called open if for every \( a \in U \) there is \( m > 0 \) such that \( B(a, p^{-m}) \subseteq U \). We prove some peculiar properties of this topology.

**Theorem 9.3.8** Let \( a \in \mathbb{Q}_p, m \in \mathbb{Z} \). Then \( B(a, p^{-m}) \) is both open and compact in the \( p \)-adic topology.

**Proof.** The ball \( B(a, p^{-m}) \) is open since for every \( b \in B(a, p^{-m}) \) we have \( B(b, p^{-m}) = B(a, p^{-m}) \).

To prove the compactness we modify the proof of the Heine-Borel theorem stating that every closed bounded set in \( \mathbb{R} \) is compact. Assume that \( B_0 := B(a, p^{-m}) \) is not compact. Then there is an infinite open cover \( \{U_\alpha\}_{\alpha \in A} \) of \( B_0 \) no finite subcollection of which covers \( B_0 \). Take \( x \in B(a, p^m) \). Then \( |(x - a)/p^m|_p \leq 1 \). Hence there is \( b \in \{0, \ldots, p - 1\} \) such that \( \frac{x - a}{p^m} \equiv b \pmod{p} \). But then, \( x \in B(a + bp^m, p^{-m-1}) \). So \( B(a, p^m) = \bigcup_{b=0}^{p-1} B(a + bp^m, p^{-m-1}) \) is the union of \( p \) balls of radius \( p^{-m-1} \). It follows that there is a ball \( B_1 \subset B(a, p^{-m}) \) of radius \( p^{-m-1} \) which can not be covered by finitely many sets from \( \{U_\alpha\}_{\alpha \in A} \). By continuing this argument we find an infinite sequence of balls \( B_0 \supset B_1 \supset B_2 \supset \cdots \), where \( B_i \) has radius \( p^{-m-i} \), such that \( B_i \) can not be covered by finitely many sets from \( \{U_\alpha\}_{\alpha \in A} \).

We show that the intersection of the balls \( B_i \) is non-empty. For \( i \geq 0 \), choose \( x_i \in B_i \). Thus, \( B_i = B(x_i, p^{-m-i}) \). Then \( \{x_i\}_{i \geq 0} \) is a Cauchy sequence since \( |x_i - x_j|_p \leq p^{-m-\min(i,j)} \to 0 \) as \( i, j \to \infty \). Hence this sequence has a limit \( x^* \) in \( \mathbb{Q}_p \). Now we have \( |x_i - x^*|_p = \lim_{j \to \infty} |x_i - x_j|_p \leq p^{-m-i} \), hence \( x^* \in B_i \), and so \( B_i = B(x^*, p^{-m-i}) \) for \( i \geq 0 \).

The point \( x^* \) belongs to one of the sets, \( U \), say, of \( \{U_\alpha\}_{\alpha \in A} \). Since \( U \) is open, for \( i \) sufficiently large the ball \( B_i \) must be contained in \( U \). This gives a contradiction. \( \Box \)

J.-H. Evertse, Diophantine Approximation
Corollary 9.3.9 Every non-empty open subset of \( \mathbb{Q}_p \) is disconnected.

Proof. Let \( U \) be an open non-empty subset of \( \mathbb{Q}_p \). Take \( a \in U \). Then \( B := B(a, p^{-m}) \subset U \) for some \( m \in \mathbb{Z} \). By increasing \( m \) we can arrange that \( B \) is strictly smaller than \( U \). Now \( B \) is open and also \( U \setminus B \) is open since \( B \) is compact. Hence \( U \) is the union of two non-empty disjoint open sets. \( \square \)

9.4 Algebraic extensions of \( \mathbb{Q}_p \).

Let again \( p \) be a prime number. We state without proof some results concerning extensions of \( |·|_p \) to field extensions of \( K \). We denote by \( \overline{\mathbb{Q}}_p \) an algebraic closure of \( \mathbb{Q}_p \).

Theorem 9.4.1 (i) Let \( K \) be a finite extension of \( \mathbb{Q}_p \). Then \( |·|_p \) has a unique continuation to \( K \) and \( K \) is complete with respect to this continuation.

(ii) \( |·|_p \) has a unique continuation to \( \overline{\mathbb{Q}}_p \) and \( \overline{\mathbb{Q}}_p \) is not complete with respect to this continuation.

(iii) Denote the continuation of \( |·|_p \) to \( \overline{\mathbb{Q}}_p \) also by \( |·|_p \). Then the completion \( \mathbb{C}_p \) of \( \overline{\mathbb{Q}}_p \) with respect to \( |·|_p \) is algebraically closed.

Corollary 9.4.2 Let \( \alpha \in \overline{\mathbb{Q}}_p \) have minimal polynomial \( f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in \mathbb{Q}_p[X] \). Then \( |\alpha|_p = |a_0|_{p}^{1/n} \).

Proof. Let \( f(X) = (X - \alpha_1) \cdots (X - \alpha_n) \) with \( \alpha_1, \ldots, \alpha_n \in \overline{\mathbb{Q}}_p \). There are \( \mathbb{Q}_p \)-automorphisms \( \sigma_1, \ldots, \sigma_n \) of \( \overline{\mathbb{Q}}_p \) such that \( \alpha_i = \sigma_i(\alpha) \) for \( i = 1, \ldots, n \). Then \( |\sigma_i(·)|_p \) \( (i = 1, \ldots, n) \) also define continuations of \( |·|_p \) to \( \overline{\mathbb{Q}}_p \) which must be all equal to \( |·|_p \). Hence

\[ |a_0|_p = |\sigma_1(\alpha)|_p \cdots |\sigma_n(\alpha)|_p = |\alpha|_{p}^{n}. \]

We recall Eisenstein’s irreducibility criterion for polynomials in \( \mathbb{Z}_p \).

Lemma 9.4.3 Let \( f(X) = a_0X^n + a_1X^{n-1} + \cdots + a_{n-1}X + a_n \in \mathbb{Z}_p[X] \) be such that \( a_0 \not\equiv 0 \pmod{p} \), \( a_i \equiv 0 \pmod{p} \) for \( i = 1, \ldots, n \), and \( a_n \equiv 0 \pmod{p^2} \). Then \( f \) is irreducible in \( \mathbb{Q}_p[X] \).

Proof. Completely similar as the Eisenstein criterion for polynomials in \( \mathbb{Z}[X] \). \( \square \)

Example. Let \( \alpha \) be a zero of \( X^3 - 8X + 10 \) in \( \overline{\mathbb{Q}}_2 \). The polynomial \( X^3 - 8X + 10 \) is irreducible in \( \mathbb{Q}_2[X] \), hence it is the minimal polynomial of \( \alpha \). It follows that \( |\alpha|_2 = |10|_2^{1/3} = 2^{-1/3}. \)

J.-H. Evertse, Diophantine Approximation
9.5 Exercises.

In the exercises below, $p$ always denotes a prime number and convergence is with respect to $|\cdot|_p$.

Exercise 9.5.1 (1) Determine the $2$-adic expansion of $-\frac{9}{7}$.

(2) Determine the $p$-adic expansion of $-1$.

Exercise 9.5.2 Let $\alpha \in \mathbb{Q}_p$. Prove that $\alpha$ has a finite $p$-adic expansion if and only if $\alpha = a/p^r$ where $a$ is a positive integer and $r$ a non-negative integer.

Exercise 9.5.3 Prove that $\mathbb{Z}_p$ is not enumerable.

Exercise 9.5.4 Let $\{a_k\}_{k=0}^\infty$ be a sequence in $\mathbb{Q}_p$. Prove that $\prod_{k=0}^{\infty}(1+a_k)$ converges if and only if $\lim_{k \to \infty} a_k = 0$.

Exercise 9.5.5 Let $x \in \mathbb{Z}_p$, $|x|_p < 1$.

(1) Prove that $\frac{1}{1-x} = \sum_{k=0}^{\infty} x^k$.

(2) Prove that $\frac{1}{(1-x)^m} = \sum_{k=0}^{\infty} \binom{m+k-1}{k} x^k$.

Hint. Recall that all convergent series in $\mathbb{Q}_p$ are unconditionally convergent. So you may freely manipulate with products of convergent series, rearrange terms etc. without having to bother about convergence.

Exercise 9.5.6 Let $\alpha = \sum_{k=-k_0}^{\infty} b_k \alpha^k$ where $b_k \in \{0, \ldots, p-1\}$ for $k \geq -k_0$. Suppose that the sequence $\{b_k\}_{k=-k_0}^{\infty}$ is ultimately periodic, i.e., there exist $r, s$ with $s > 0$ such that $a_{k+s} = a_s$ for all $k \geq r$. Prove that $\alpha \in \mathbb{Q}$.

Exercise 9.5.7 Let $\alpha = \sum_{k=0}^{\infty} b_k p^k$ with $b_k \in \{0, \ldots, p-1\}$ for $k \geq 0$. Determine the $p$-adic expansion of $-\alpha$.

Exercise 9.5.8 Let $\alpha \in \mathbb{Z}_p$ with $|\alpha - 1|_p \leq p^{-1}$. In this exercise you are asked to define $\alpha^x$ for $x \in \mathbb{Z}_p$ and to show that this exponentiation has the expected properties. You may use without proof that the limit of the sum, product etc. of two sequences in $\mathbb{Z}_p$ is the sum, product etc. of the limits.

(1) Prove that $\left| \frac{\alpha^{p-1}}{\alpha - 1} \right|_p \leq p^{-1}$. 

J.-H. Evertse, Diophantine Approximation
(2) Let \( u \) be a positive integer. Prove that \( |\alpha^u - 1|_p \leq |u|_p |\alpha - 1|_p \).

**Hint.** Write \( u = p^mb \) where \( b \) is not divisible by \( p \) and use induction on \( m \).

(3) Let \( u, v \) be positive integers. Prove that \( |\alpha^u - \alpha^v|_p \leq |u - v|_p |\alpha - 1|_p \).

(4) We now define \( \alpha^x \) for \( x \in \mathbb{Z}_p \) as follows. Take a sequence of positive integers \( \{a_k\}_{k=0}^\infty \) such that \( \lim_{k \to \infty} a_k = x \) and define

\[
\alpha^x := \lim_{k \to \infty} \alpha^{a_k}.
\]

Prove that this is well-defined, i.e., the limit exists and is independent of the choice of the sequence \( \{a_k\}_{k=0}^\infty \).

(5) Prove that for \( x, y \in \mathbb{Z}_p \) we have \( |\alpha^x - \alpha^y|_p \leq |x - y|_p |\alpha - 1|_p \). (**Hint.** Take sequences of positive integers converging to \( x, y \).) Then show that if \( \{x_k\}_{k=0}^\infty \) is a sequence in \( \mathbb{Z}_p \) such that \( \lim_{k \to \infty} x_k = x \) then \( \lim_{k \to \infty} \alpha^{x_k} = \alpha^x \) (so the function \( x \mapsto \alpha^x \) is continuous).

(6) Prove the following properties of the above defined exponentiation:

(i) \( (\alpha \beta)^x = \alpha^x \beta^x \) for \( \alpha, \beta \in \mathbb{Z}_p \), \( x \in \mathbb{Z}_p \) with \( |\alpha - 1|_p \leq p^{-1}, |\beta - 1|_p \leq p^{-1} \);

(ii) \( \alpha^{x+y} = \alpha^x \alpha^y \), \( (\alpha^x)^y = \alpha^{xy} \) for \( \alpha \in \mathbb{Z}_p \) with \( |\alpha - 1|_p \leq p^{-1} \), \( x, y \in \mathbb{Z}_p \).

**Remark.** In 1935, Mahler proved the following \( p \)-adic analogue of the Gel’fond-Schneider Theorem: let \( \alpha, \beta \) be elements of \( \mathbb{Z}_p \), both algebraic over \( \mathbb{Q} \), such that \( |\alpha - 1|_p \leq p^{-1} \) and \( \beta \not\in \mathbb{Q} \). Then \( \alpha^\beta \) is transcendental over \( \mathbb{Q} \).

**Exercise 9.5.9** This exercise is about the \( p \)-adic logarithm.

(1) Prove that the series \( \log_p(x) := \sum_{k=1}^\infty \frac{(-1)^{k-1}}{k} (x - 1)^k \) converges for all \( x \in \mathbb{Q}_p \) with \( |x - 1|_p < 1 \) and diverges for all \( x \in \mathbb{Q}_p \) with \( |x - 1|_p \geq 1 \).

(2) Prove that for \( x \in \mathbb{Z}_p \) with \( |x - 1|_p < 1 \) we have \( |\log_p(x)|_p \leq |x - 1|_p \).

(3) (Tricky). Prove that \( \log_p(xy) = \log_p x + \log_p y \) for \( x, y \in \mathbb{Z}_p \) with \( |x - 1|_p < 1 \) and \( |y - 1|_p < 1 \).

**Hints.** You need a few facts on \( p \)-adic power series.

1) Let \( f(X) = \sum_{n=0}^\infty a_n X^n \), \( g(X) = \sum_{n=0}^\infty b_n X^n \) be power series with coefficients in \( \mathbb{Q}_p \) and \( h(X) = \sum_{n=0}^\infty (\sum_{k=0}^n a_{n-k} b_k) X^n \) their Cauchy product. Then for all \( v \in \mathbb{Q}_p \) for which both \( f(v), g(v) \) converge, we have \( h(v) = f(v)g(v) \). This follows in the same manner as for power series over \( \mathbb{C} \), using unconditional convergence.

J.-H. Evertse, Diophantine Approximation
9.5 Exercises.

2) For any positive integer \( l \) we have a formal power series expression \((1+X)^{-l} = \sum_{n=0}^{\infty} (-1)^n \binom{n+l-1}{l-1} X^n\), i.e.,

\[
(1 + X)^l \cdot \sum_{n=0}^{\infty} (-1)^n \binom{n + l - 1}{l - 1} X^n = 1.
\]

The power series converges for all \( v \in \mathbb{Q}_p \) with \(|v|_p < 1\) since the binomial coefficients are integers. So we may substitute \( X = v \) for any \( v \in \mathbb{Q}_p \) with \(|v|_p < 1\).

3) Let \( x = u + 1, y = v + 1 \), view \( v \) as a constant and \( u \) as a variable. Then it has to be shown that

\[
\log_p(xy) = \sum_{n=1}^{\infty} (-1)^{n-1} \frac{(yu+v)^n}{n} = \sum_{n=1}^{\infty} (-1)^{n-1} \frac{u^n}{n} + \sum_{n=1}^{\infty} (-1)^{n-1} \frac{v^n}{n}.
\]

You have to rewrite the left-hand side as a power series in \( u \), and use Newton’s binomial formula, interchange of summation, and 2). Since convergence of series is always unconditional, such manipulations do not affect convergence or the values of the series involved.

(4) Prove that \( \log_p(x^u) = u \log_p(x) \) for \( x \in \mathbb{Z}_p \) with \(|x-1|_p < 1, u \in \mathbb{Z}_p\).

**Hint.** First prove that \( \log_p \) is continuous by showing that \(|\log_p x - \log_p y|_p \leq |x - y|_p \) for \( x, y \in \mathbb{Z}_p \) with \(|x-1|_p < 1 \) and \(|y-1|_p < 1\). Then prove (4) first in the special case that \( u \) is a positive integer.