Proc. Sci. Seminar
Faculty of Physics and Mathematics, Šiauliai University,
5, 2002, 90–107

THE WORLD OF p-ADIC NUMBERS AND p-ADIC FUNCTIONS

Jörn STEUDING

Institut für Algebra und Geometrie, Fachbereich Mathematik, Johann Wolfgang Goethe-Universität Frankfurt, Robert-Mayer-Str. 10, D-60054 Frankfurt, Germany
e-mail: steuding@math.uni-frankfurt.de

Abstract. We give a brief and elementary introduction to p-adic numbers and p-adic functions. Some of the topics are: non-archimedean valuations and the ultrametric topology, completions of $\mathbb{Q}$, the Hasse principle, p-adic analysis and, in particular, p-adic L-functions. Besides we prove the existence of *universal* p-adic power series (in the sense of Fekete).

Key words: non-archimedean valuation, p-adic numbers, Hasse principle, p-adic functions.

Mathematics Subject Classification: 11E12, 11S80, 12J25 .

Everyone knows the set of positive integers $\mathbb{N}$, including the infinite set of prime numbers

$$2, 3, 5, 7, \ldots,$$

the ring of integers $\mathbb{Z}$, the field of rational numbers $\mathbb{Q}$, its completion, the field of real numbers $\mathbb{R}$, and its algebraically closed extension, the field of complex numbers $\mathbb{C}$. But mathematics has much more to offer than this. One example are the p-adic numbers with their astonishing properties. p-adic numbers were discovered (or created, but this is a philosophical question) by Kurt Hensel[1] about hundred years ago; see [6]. Meanwhile the theory of p-adic numbers has a plenty of applications and impacts in various mathematical fields as number theory, algebra, topology and analysis. The aim of this talk is to give a survey on p-adic numbers and p-adic analysis. However, in Section 9 we prove a new result, namely a p-adic analogue of a variant of Fekete's remarkable universality theorem. In footnotes we give some brief historical remarks on the founders of the theory of p-adic numbers.

There are different possibilities to construct p-adic numbers. Our first construction follows the ideas of Kürschák[2] and uses the theory of valuations.

1. Valuations

By the prime factorization of the integers every rational number $\alpha \neq 0$ has a unique representation

[1] Kurt Hensel, ∗29.12.1861, Königsberg/Kaliningrad, - †1.6.1941, Marburg; student of Kronecker and Weierstrass in Berlin; professor in Marburg; editor of Crelle's Journal.

[2] József Kürschak, ∗14.3.1864, Budapest, - †26.3.1933, Budapest; teacher of von Neumann.

$$\alpha = \pm \prod_p p^{\nu(\alpha;p)} \quad \text{with } \nu(\alpha;p) \in \mathbb{Z};$$

here the product is taken over all prime numbers p, but in fact only finitely many of the p-exponents $\nu(\alpha;p)$ are non-zero. Thus, if we fix a prime p, then we may write

$$\alpha = \frac{a}{b} \cdot p^{\nu(\alpha;p)} \qquad \text{with } 0 \neq a, b \in \mathbb{Z},\ p \not| ab;$$

here and in the sequel we write $d|n$ if the integer d divides the integer n, and $d \not| n$ otherwise. We define the *p-adic absolute value* on $\mathbb{Q}$ by setting

$$|\alpha|_p = \begin{cases} p^{-\nu(\alpha;p)} & \text{if } \alpha \neq 0, \\ 0 & \text{if } \alpha = 0; \end{cases}$$

the function $\alpha \mapsto \nu(\alpha;p)$ is called *p-adic valuation*. An *absolute value* on a field $\mathbb{K}$ is a function $|\ | : \mathbb{K} \to \mathbb{R}$ satisfying the axioms

- $|x| \geqslant 0$ for all $x \in \mathbb{K}$, and $|x| = 0$ if and only if $x = 0$;
- $|x \cdot y| = |x| \cdot |y|$ for all $x, y \in \mathbb{K}$;
- $|x + y| \leqslant |x| + |y|$ for all $x, y \in \mathbb{K}$.

If the last axiom can be replaced by

$$|x + y| \leqslant \max\{|x|, |y|\} \qquad \text{for all } x, y \in \mathbb{K}, \tag{1}$$

the absolute value is said to be *non-archimedean*; otherwise the absolute value is called *archimedean*. The well-known absolute value

$$|\alpha|_\infty = \begin{cases} \alpha & \text{if } \alpha \geqslant 0, \\ -\alpha & \text{if } \alpha < 0, \end{cases}$$

is the standard example of an archimedean absolute value on $\mathbb{K}$; the notation $|\ |_\infty$ is traditional in the context of p-adic valuations. An example of a non-archimedean absolute value is the *trivial* absolute value which is constant 1 on all non-zero elements, but this is boring. More interesting is the fact that the p-adic absolute value, defined above, is a non-archimedean absolute value on $\mathbb{Q}$. It is easy to check that for each prime p the absolute value $|\ |_p$ is indeed an absolute value, and it is not much more difficult to prove that even (1) is satisfied; the main idea for the proof can be found by studying the following example

$$|3 \cdot 5 + 2 \cdot 3^2|_3 = |3(5 + 2 \cdot 3)|_3 = \frac{1}{3} = \max\{|3 \cdot 5|_3, |2 \cdot 3^2|_3\}.$$

A more practical characterization gives the following equivalence: an absolute value $|\ |$ on a field $\mathbb{K}$ is non-archimedean if and only if

$$\sup\{|n| : n \in \mathbb{N}\} < \infty \tag{2}$$

(since any positive integer n has a representation $n = 1 + \ldots + 1$, $\mathbb{N}$ has a natural embedding into any field $\mathbb{K}$). So we see that the notion of an archimedean absolute value has its origin in Archimedes' lemma which states that for all non-zero rationals x, y there exists a positive integer m with

$$|mx|_\infty > |y|_\infty.$$

Here we do a break to show in the following section that non-archimedean absolute values imply a curious topology.

2. Ultrametric topology

An absolute value on a field $\mathbb{K}$ induces a topology. Since an absolute value $|\ |$ is a norm, we may define a metric by setting

$$\mathrm{d}(x, y) = |x - y| \qquad \text{for } x, y \in \mathbb{K}$$

with which we can measure distances on $\mathbb{K}$. If $|\ |$ is a non-archimedean absolute value, then we call the corresponding metric *ultrametric* and $\mathbb{K}$ together with this ultrametric is said to be an *ultrametric space*. Obviously, with view to (1), a metric is ultrametric if and only if

$$\mathrm{d}(x, y) \leqslant \max\{\mathrm{d}(x, z), \mathrm{d}(y, z)\} \qquad \text{for all } x, y, z \in \mathbb{K}$$

holds; the latter inequality is called the *ultrametric inequality*. In the special case of a p-adic absolute value on $\mathbb{Q}$ we see for a rational number α that

$$|\alpha|_p \text{ is small} \quad \Longleftrightarrow \quad \alpha \text{ is divisible by a large power of } p.$$

This was the underlying idea for Hensel in introducing p-adic numbers. Divisibility properties of the integers are one of the fundamentals in number theory!

In the sequel we will consider only the case of a non-archimedean absolute value and the topology which the corresponding ultrametric induces. It is easily seen that if $|\ |$ is a non-archimedean absolute value on $\mathbb{K}$, and if $|x| \neq |y|$, then the equality

$$|x + y| = \max\{|x|, |y|\}$$

holds. This has several surprising consequences: in an ultrametric space

- all triangles are isosceles, i.e. two sides have equal length;
- all balls are both open and closed;
- each point inside a ball is center of the ball;
- any two open balls are either disjoint or contained in one another;

here an ultrametric *triangle* is given by three points $x, y, z \in \mathbb{K}$ whereas the ultrametric open, resp. closed, *ball* (resp. *disc*) with center z and radius $r > 0$ is the set

$$\mathcal{B}_{<r}(z) := \{x \in \mathbb{K} : \mathrm{d}(x, z) < r\}\ , \quad \text{resp.}$$
$$\mathcal{B}_{\leqslant r}(z) := \{x \in \mathbb{K} : \mathrm{d}(x, z) \leqslant r\}.$$

We leave the proofs as an exercise to the interested reader. One may consider these facts as curiosities. Nevertheless, since in ultrametric spaces many sets are *clopen*, i.e. *closed* and o*pen*, they are interesting objects in general topology. By standard arguments one can show that an ultrametric space is *totally disconnected*, that means the connected component of any point is the point itself. Here we see an interesting analogy to the Cantor set. The Cantor set $\mathcal{C}$ can be constructed as follows: delete from the unit interval $[0,1] \subset \mathbb{R}$ the open middle third. Then remains the compact set

$$\mathcal{C}_1 := \left[0, \frac{1}{3}\right] \cup \left[\frac{2}{3}, 1\right].$$

Deleting again the open middle third of each interval of $\mathcal{C}_1$, we get a compact subset $\mathcal{C}_2$ consisting of four closed intervals each of length $\frac{1}{9}$. Iterating this process, we get a decreasing sequence of nested compact subsets of $[0,1]$. Then, the *Cantor set* $\mathcal{C}$ is the intersection of all:

$$\mathcal{C} = \bigcap_{n=1}^{\infty} \mathcal{C}_n.$$

One can show that $\mathcal{C}$ consists precisely of the points

$$\alpha = \sum_{n=1}^{\infty} \alpha_n \cdot 3^{-n} \qquad \text{with digits } \alpha_n \in \{0, 2\}; \tag{3}$$

note that this representation is not unique but this causes no difficulties here. It is well known that $\mathcal{C}$ is an uncountable, totally disconnected set; see [11].

We return to the field of rational numbers and its p-adic absolute values.

3. Absolute values on the rationals

A natural question occurs: what are the absolute values of a given field? If $\mathbb{K}$ is a finite field, say with q elements, then criterion (2) implies immediately that $\mathbb{K}$ can only have non-archimedean absolute values. Obviously, we have $|0| = 0$ for any absolute value $|\ |$ on $\mathbb{K}$ by definition. Now take an element $0 \neq x \in \mathbb{K}$. Since $\mathbb{K}$ is finite, we have $x^q = x$, which gives $|x|^q = |x|$. Thus, $|x| = 1$, which shows that the only absolute value on a finite field is the trivial one.

More difficult but much more interesting is the case of the field of rational numbers. Here the answer was found by Ostrowski[3]. If we call two absolute values *equivalent* if they induce the same topology, then

THEOREM 1 (Ostrowski). *Every non-trivial absolute value on $\mathbb{Q}$ is equivalent to one of the absolute values $|\ |_p$, where either p is a prime number or $p = \infty$.*

[3] Alexander Ostrowski, ∗25.9.1893, Kiew, - †20.11.1986, Montagnola(Lugano); student of Hensel in Marburg, of Klein, Hilbert and Landau in Göttingen and of Hecke in Hamburg; solved Hilbert's 18th problem; professor in Basel.

The proof is not difficult but tricky. With view to (2) one can decide whether an absolute value is archimedean or not. Furthermore, if $|\ |$ is a non-archimedean value, then

$$\min\{n \in \mathbb{N} : |n| < 1\}$$

has to be prime, say p, which yields that $|\ |$ is equivalent to the p-adic absolute value. For details we refer the reader to [5] (which is a very good introduction to p-adic numbers).

Moreover, Ostrowski's theorem is to see as the justification for Hensel's approach in introducing p-adic numbers to number theory. Further, it fits very good to the *product formula* which states that

$$\prod_{p \leqslant \infty} |\alpha|_p = 1 \qquad \text{for any } 0 \neq \alpha \in \mathbb{Q}.$$

This follows easily from the definition of the p-adic absolute value and the unique prime factorization. The primes p are also called *places* and $p = \infty$ is the *infinite place*.

p-adic absolute values imply a strange convergence. Consider the sequence of rational numbers

$$\alpha_m = 1 + p + \ldots + p^m = \frac{1 - p^{m+1}}{1 - p}.$$

Since

$$\left|\frac{p^{m+1}}{1-p}\right|_p = |p^{m+1}|_p \cdot |1-p|_p^{-1} = p^{-m-1}$$

tends to zero as $m \to \infty$, we see that the sequence (α_m) is p-adically convergent. This yields the curious formula

$$\sum_{n=0}^{\infty} p^n = \frac{1}{1-p}, \tag{4}$$

which is with respect to the usual absolute value divergent! With this formula one can solve the diophantine equation

$$X = p(X+1)$$

by iteration (since the solution, resp. the limit, is rational). However, the same reasoning as for (4) can be applied to more general sequences (α_m) given by

$$\alpha_m = \sum_{n=0}^{m} \alpha_n p^n \qquad \text{with } \alpha_n \in \mathbb{Z},\ 0 \leqslant \alpha_n < p. \tag{5}$$

It is easily seen that all these sequences (α_m) are not only p-adically convergent but even Cauchy sequences. On the other side, one can show the following irrationality criterion: if $\nu, \alpha_k \in \mathbb{Z}$ with $0 \leqslant \alpha_k < p$, then

$$\alpha = \sum_{k \geqslant \nu}^{\infty} \alpha_k p^k \in \mathbb{Q} \qquad \Longleftrightarrow \qquad (\alpha_k) \text{ is eventually periodic;} \tag{6}$$

the proof of this equivalence is absolutely similar to the well-known criterion for real numbers with regard to their decimal expansion. This shows that there exist p-adically convergent series with an irrational limit. As we all know the same is true for rational sequences with respect to the absolute value; for example, it is well-known that

$$\exp(1) = \sum_{k=0}^{\infty} \frac{1}{k!} \notin \mathbb{Q}.$$

4. Completions of the rationals

We have seen that $\mathbb{Q}$ is not complete to any of its absolute values. The next step is obvious: in the same way as Cantor constructed the set of real numbers as completion of $\mathbb{Q}$ by *adding* all Cauchy-sequences (modulo the classes of sequences with limit zero), we may complete the set of rational numbers with respect to the p-adic absolute values. Putting

$$\mathcal{R}_p = \{(\alpha_m) \,:\, (\alpha_m) \text{ is a Cauchy sequence with respect to } |\ |_p\}$$

and

$$\mathcal{M}_p = \{(\alpha_m) \in \mathcal{R}_p \,:\, \lim_{m\to\infty} \alpha_m = 0 \ p\text{-adically}\},$$

the completion of $\mathbb{Q}$ with respect to the p-adic absolute value is given by

$$\mathbb{Q}_p = \mathcal{R}_p \,\Big/\, \mathcal{M}_p.$$

Since $\mathcal{R}_p$ is a ring with 1 and since $\mathcal{M}_p$ is a maximal ideal in $\mathcal{R}_p$, we obtain

THEOREM 2 (Hensel). *$\mathbb{Q}_p$ is a field.*

Therefore, to each prime number p we have constructed *the field of p-adic numbers* $\mathbb{Q}_p$. In addition with the real numbers,

$$\mathbb{Q} \quad \overset{\text{completion}}{\longrightarrow} \quad \mathbb{Q}_2, \mathbb{Q}_3, \mathbb{Q}_5, \cdots \quad \text{and} \quad \mathbb{Q}_\infty = \mathbb{R}.$$

This shows that beside the world of real numbers exist *equally important* for each prime p a world of p-adic numbers. Note that two distinct p-adic fields are non-isomorphic since they are by Ostrowski's theorem different topological spaces. One can even show that

$$\mathbb{Q}_p \cap \mathbb{Q}_q = \mathbb{Q} \qquad \text{if } p, q \in \mathbb{P},\ p \neq q.$$

We note some further properties of the field of p-adic numbers:

- $\mathbb{Q}_p$ is uniquely determined (up to isomorphisms);
- $\mathbb{Q}$ lies dense in $\mathbb{Q}_p$;
- $\mathbb{Q}_p$ is complete with respect to $|\ |_p$;

- $\mathbb{Q}_p$ is a locally compact, totally disconnected Hausdorff space, consisting of uncountable many elements.

But how do p-adic numbers look like? In view of (4) and (5) (also (3) in a certain sense) it is not surprising that we already know p-adic numbers. One can show that any p-adic number α has a unique *p-adic expansion*

$$\alpha = \sum_{n \geqslant \nu}^{\infty} \alpha_n p^n \qquad \text{with } \alpha_n \in \mathbb{Z},\ 0 \leqslant \alpha_n < p, \tag{7}$$

where ν is an integer which coincides with $\nu(\alpha; p)$ if $\alpha \in \mathbb{Q}$. Moreover, setting $\nu(\alpha; p) = \nu$ for all $\alpha \in \mathbb{Q}_p$, gives the continuation of the p-adic absolute value to $\mathbb{Q}_p$. Since we have a lot of experience to calculate with the decimal expansions of real numbers or the binary expansions which a computer uses, we do believe that it is an easy task to do computations with p-adic numbers. Note that Hensel started with the expansions (7) when he constructed $\mathbb{Q}_p$ (having in mind to apply the fruitful method of power series from analysis to number theory). This representation of p-adic numbers has a plenty of applications as there is to mention error-free computing (see [14] for the *Hensel code*), modelling memory retrieval by a p-adic dynamical system [1] or in elementary number theory. For example, if $d|p-1$, then

$$d \mid n = \sum_{k \geqslant 0} \alpha_k p^k \qquad \Longleftrightarrow \qquad d \mid \sum_{k \geqslant 0} \alpha_k;$$

we leave the simple proof to the interested reader. Note that for each d such a prime p exists by Dirichlet's prime number theorem for arithmetic progressions. However, we shall give a more advanced example.

THEOREM 3 (Joint approximation). *If $p_1, \ldots, p_n$ are distinct primes and $\beta_1, \ldots, \beta_n$ are arbitrary rational numbers, then for any given $\varepsilon > 0$ there exists $\alpha \in \mathbb{Q}$ such that*

$$|\alpha - \beta_k|_{p_k} < \varepsilon \qquad \text{for } 1 \leqslant k \leqslant n.$$

A proof of this remarkable result can be found in [4]. In view of the definition of the p-adic absolute value we obtain as an immediate consequence the chinese remainder theorem from elementary number theory which states that any system of congruences

$$X \equiv \beta_k \bmod p_k^{\nu_k} \qquad \text{for } 1 \leqslant k \leqslant n,$$

with distinct primes $p_1, \ldots, p_n$ and positive integers $\nu_1, \ldots, \nu_n$ has a solution.

However, we may interpret the above theorem a little bit different, namely that $\mathbb{Q}$ lies not only dense in one $\mathbb{Q}_p$ but also in a collection of distinct p-adic fields. That means: if $p_1, \ldots, p_n$ are distinct primes, then to any collection of p_k-adically convergent sequences with limit β_k, where $1 \leqslant k \leqslant n$, there exists a divergent sequence (α_m) of rational numbers such that

$$\alpha_m \quad \longrightarrow \quad \beta_k \qquad \text{for } 1 \leqslant k \leqslant n.$$

In a sense, this is a joint universality property. But the importance of the joint approximation theorem becomes only clear in the context of adéles in algebraic number theory; see [16].

Now we will give one more but last construction of p-adic numbers; the following pure algebraic approach is rather simple and elegant but does not give any information on the links to $\mathbb{R}$.

5. An algebraic approach

Define

$$\mathbb{Z}_p = \{\alpha \in \mathbb{Q}_p \,:\, \nu(\alpha; p) \geqslant 0\};$$

obviously, in view of (7) the appearance of $\mathbb{Q}_p$ can be ommitted. It is easily seen that $\mathbb{Z}_p$ is a subring of $\mathbb{Q}_p$, the *ring of p-adic integers*

$$\alpha = \sum_{n=0}^{\infty} \alpha_n p^n \qquad \text{with } \alpha_n \in \mathbb{Z},\ 0 \leqslant \alpha_n < p.$$

Denoting by $\mathbb{Z}/p^n\mathbb{Z}$ the ring of residue classes $\bmod p^n$ for $n \in \mathbb{N}$, we may define the sequence of maps

$$\ldots \to \mathbb{Z}/p^{n+1}\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z} \to \ldots \to \mathbb{Z}/p^2\mathbb{Z} \to \mathbb{Z}/pZ,$$

where each map is the natural projection

$$\pi_n \,:\, \mathbb{Z}/p^{n+1}\mathbb{Z} \to \mathbb{Z}/p^n Z\ , \quad a \mapsto a \bmod p^n.$$

Then we can define the *inverse limit*

$$\lim_{\leftarrow} \mathbb{Z}/p^n\mathbb{Z} = \left\{ (a_n) \in \prod_{n \geqslant 1} \mathbb{Z}/p^n\mathbb{Z} \,:\, \pi_n(a_{n+1}) = a_n \right\}.$$

As a matter of fact we see that each $(a_n) \in \lim_{\leftarrow} \mathbb{Z}/p^n\mathbb{Z}$ gives raise to a sequence of integers x_n such that

$$a_n = x_n \bmod p^n,$$

and (x_n) is a Cauchy sequence with respect to the p-adic absolute value. This gives now easily

THEOREM 4. $\lim_{\leftarrow} \mathbb{Z}/p^n\mathbb{Z} \cong \mathbb{Z}_p$.

Thus we obtained $\mathbb{Z}_p$ by letting $n \to \infty$ in $\mathbb{Z}/p^n\mathbb{Z}$. Since $\mathbb{Z}_p$ is (as an inverse limit) an integral domain, that is a ring without zero divisors, we may construct $\mathbb{Q}_p$ as the quotient field of $\mathbb{Z}_p$. The observation $\mathbb{Z}_p \cap \mathbb{Q} = \mathbb{Z}$ shows that it makes sense to call $\alpha \in \mathbb{Z}_p$ a p-adic integer. We note further:

- $\mathbb{Z}$ lies dense in $\mathbb{Z}_p$ and $\mathbb{Z}_p$ is clopen in $\mathbb{Q}_p$;
- for every positive integer n the set

$$p^n\mathbb{Z}_p := \{\alpha \in \mathbb{Z}_p \,:\, \nu(\alpha; p) \geqslant n\}$$

  is an ideal in $\mathbb{Z}_p$, isomorphic to $\mathbb{Z}/p^n\mathbb{Z}$;
- $p\mathbb{Z}_p$ is a maximal ideal in $\mathbb{Z}_p$ and, thus, $\mathbb{Z}_p$ is a local ring; the group of units is given by

$$\mathbb{Z}_p^* := \mathbb{Z}_p \setminus p\mathbb{Z}_p := \{\alpha \in \mathbb{Z}_p \,:\, |\alpha|_p = 1\}.$$

We see an interesting link between topological objects and algebraic structures: on the algebraic side we have

$$\mathbb{Z}_p = \mathbb{Z}_p^* \cup p\mathbb{Z}_p,$$

whereas we have in one-one correspondence on the topological side

$$\mathcal{B}_{\leqslant 1}(0) \;= \text{boundary of } \mathcal{B}_{\leqslant 1}(0) \;\cup\; \text{interior of } \mathcal{B}_{\leqslant 1}(0).$$

Thus, the group of units can be regarded as 1-sphere. This is the starting point to introduce algebraic features into topology and leads to the theory of valuations.

In the next section we have a look on one of the most important properties of $\mathbb{Q}_p$, namely that under some circumstances one can easily decide whether a polynomial equation is soluble in $\mathbb{Q}_p$.

6. Newton approximation

We consider quadratic equations. For example, does the equation

$$X^2 + a = 0 \qquad \text{with } p \not| a \in \mathbb{Z}$$

have solutions in $\mathbb{Z}_5$? Setting

$$\begin{aligned} 0 &= a + (\alpha_0 + \alpha_1 \cdot 5 + \alpha_2 \cdot 5^2 + \ldots)^2 \\ &= a + \alpha_0^2 + 2\alpha_0\alpha_1 \cdot 5 \mod 5^2\mathbb{Z}_5, \end{aligned} \tag{8}$$

we see that $-a$ has to be a quadratic residue mod 5, i. e. the congruence

$$X^2 \equiv -a \bmod 5$$

is soluble. In the case $a = -2$ this congruence has no solution, which gives, since $\mathbb{Q} \subset \mathbb{Q}_5$, a new and simple proof for the irrationality of $\sqrt{2}$. Now lets take $a = 1$. Since $2^2 = 4 \equiv -1 \bmod 5$, we are in the position to continue our search for a root

of X^2+1 in $\mathbb{Z}_5$. Substituting $\alpha_0 = 2$ (resp. $\alpha_0 = 3$) in (8), we now have to solve the congruence

$$1 + 4 \cdot \alpha_1 \equiv 0 \bmod 5,$$

but this is a linear congruence, which is always soluble. Since in all consecutive steps we always have to solve only linear equations, we have

$$\sqrt{-1} = 2 + 1 \cdot 5 + 2 \cdot 5^2 + \dots \tag{9}$$

as a solution of $X^2+1 = 0$ in $\mathbb{Z}_5$; this is not the complex $i = \sqrt{-1}$. Since the solution is irrational, we see in view of (6) that the sequence of its digits is aperiodic (though there are only finitely many possible congruences for the digits) but *does there exist a distribution law for the p-adic digits of algebraic irrationals?*

In a sense, solving these linear congruences step by step can be understood as applying the Newton iteration method to the polynomial $F(X) = X^2+1$. We define the *formal* derivative of a polynomial as usual via

$$(cX^n)' = ncX^{n-1} \qquad \text{for } n \in \mathbb{N} \cup \{0\}.$$

Then the iteration

$$x_{n+1} = x_n - \frac{F(x_n)}{F'(x_n)} = x_n - \frac{x_n^2+1}{2x_n} \qquad \text{with } x_0 = 2$$

gives

$$x_1 = 2 - 5 \cdot \frac{F(2)}{5}(F'(2))^{-1} = 2 + 1 \cdot 5,$$

which should be compared with (9). In fact, this idea leads to

THEOREM 5 (Hensel's lemma). *Let $F \in \mathbb{Z}_p[X]$ be a polynomial and suppose that there is a p-adic integer x_1 such that*

$$F(x_1) \equiv 0 \bmod p\mathbb{Z}_p \qquad \text{and} \qquad F'(x_1) \not\equiv 0 \bmod p\mathbb{Z}_p.$$

Then there exists a p-adic integer x such that

$$x \equiv x_1 \bmod p\mathbb{Z}_p \qquad \text{and} \qquad F(x) = 0.$$

The main idea for the proof is the formal identity

$$F(X+h) = F(X) + F'(X)h + \dots + F^{(d)}(X)\frac{h^d}{d!},$$

where $F(X)$ is a polynomial of degree d. We omit the technical details (for a proof see [5]) but give an example. An immediate consequence of Hensel's lemma is: if m is a positive integer which is not divisible by p, then there exists a primitive m-th root of unity ζ_m in $\mathbb{Q}_p$, i. e.

$$\zeta_n^m - 1 = 0 \qquad \text{and} \qquad \zeta_m^n \neq 1 \quad \text{for } 1 \leqslant n < m,$$

if and only if m divides $p-1$. This shows that $\mathbb{Q}_p$ is not algebraically closed.

In the next section we get some insights to a philosophy connecting classical number theoretical questions with its p-adic analogues.

7. The Hasse principle

Extending the example of the previous section, we see that a positive integer α is a square in $\mathbb{Z}_p$ if and only if α is a quadratic residue mod 5. We can even get a sufficient condition, namely: for a rational number α,

$$\alpha \text{ is a square} \quad \Longleftrightarrow \quad \alpha \text{ is a square in all } \mathbb{Q}_p,\ p \leqslant \infty.$$

One implication of this equivalence follows easily from $\mathbb{Q} \subset \mathbb{Q}_p$, whereas the other implication follows immediately from the prime factorization of α. This was rather simple but the idea of *putting together local information at all places $p \leqslant \infty$ should give global information* is extraordinary successful and seems to go back to Hensel but was first clearly stated by Hasse[4]. With this concept Hasse was able to solve around 1920 one of Hilbert's problems posed at the International Congress of Mathematicians in Paris 1900. We call a homogeneous quadratic polynomial in n variables *quadratic form*; we say that a quadratic form $F \in \mathbb{K}[X_1, \ldots, X_n]$ is *isotropic* over $\mathbb{K}$ if there exist $x_1, \ldots, x_n \in \mathbb{K}$, not all $x_k = 0$, such that

$$F(x_1, \ldots, x_n) = 0.$$

It can be shown that if F is an isotropic quadratic form, all equations

$$F(X_1, \ldots, X_n) = \beta \qquad \text{with } \beta \in \mathbb{K}$$

have a solution. The most important problem in the theory of quadratic forms is the characterization of isotropic quadratic forms. A first but complicated characterization was given by Minkowski[5] in 1890. But the mathematical truth behind is of p-adic nature as Hasse showed.

THEOREM 6 (Hasse-Minkowski). *A quadratic form is isotropic over $\mathbb{Q}$ if and only if it is isotropic over all $\mathbb{Q}_p, p \leqslant \infty$.*

The proof of this so-called *Hasse-principle* is far beyond the scope of this survey and uses deeper knowledge on the theory of quadratic forms, the multiplicative structure of $\mathbb{Q}_p$, its subgroup of squares, and even Dirichlet's prime number theorem for arithmetic progressions; we refer the interested reader to [3] or [15]. An important lemma for the proof, and also for concrete applications, is the fact that if p is an odd prime, then any quadratic form in more than three variables which has at least three coefficients in $\mathbb{Z}_p^*$ is isotropic over $\mathbb{Q}_p$. We shall give an example: the equation

$$3X^2 - 5Y^2 - 7Z^2 = 0$$

[4] Helmut Hasse, ∗25.8.1898, Kassel, - †26.12.1979, Ahrendsburg (Hamburg); student of Landau, Hilbert, Noether and Hecke in Göttingen and Hensel in Marburg; lecturer in Kiel and Halle, professor in Göttingen, Berlin and Hamburg; editor of Crelle's Journal.

[5] Hermann Minkowski, ∗22.6.1864, Aleksotas/Kaunas, - †12.1.1909, Göttingen; student of Hilbert; lecturer in Bonn, Königsberg and Zürich; professor in Göttingen; teacher of Einstein.

has a non-trivial solution $(x, y, z) \in \mathbb{Q}^3$, i. e. solutions with $xyz \neq 0$ while it fails to have a non-trivial solution when we change the sign by $7Z^2$. This follows simply only by studying the quadratic forms $3X^2 - 5Y^2 \pm 7Z^2$ in $\mathbb{Q}_p$ with $p = 2, 3, 5, 7, \infty$, which is an easy task. Furthermore, we have to mention some well-known consequences as there is Lagrange's theorem that every positive integer can be written as a sum of at most four squares, and Gauss' theorem which states that every positive integer has a representation as a sum of at most three triangle numbers.

However, the idea to use information from the local fields $\mathbb{Q}_p, p \leqslant \infty$, to solve a problem in the global field $\mathbb{Q}$, sometimes called *local-global principle*, has also limits. For example, it is easily seen that the equation

$$(X^2 - 2)(X^2 - 17)(X^2 - 34) = 0$$

has solutions in all $\mathbb{Q}_p, p \leqslant \infty$, but has no solution in $\mathbb{Q}$. A further example is the Fermat equation

$$X^n + Y^n = Z^n \qquad \text{with } n \in \mathbb{N},$$

which has non-trivial solutions in all $\mathbb{Q}_p$, $p \leqslant \infty$, but has only trivial solutions in $\mathbb{Q}$ whenever $n \geqslant 3$ as Wiles proved (after important work in advance by Shimura, Taniyama, Frey, Mazur, Ribet et al.). Nevertheless, Wiles' celebrated proof of Fermat's last theorem used p-adic theory.

In the sequel we will do the first steps towards p-adic analysis. As we have seen above $\mathbb{Q}_p$ is *too small* for deeper analytic studies. It turns out that we have to do some gymnastics to find the right extension for this aim.

8. Mahler's theorem

Some problems for doing p-adic analysis are obvious:

- $\mathbb{R}$ is an ordered field, which gives a notion of *bigger than* which fits perfectly together with the standard operations, but this does not hold for $\mathbb{Q}_p$;
- since $\mathbb{Q}_p$ is totally disconnected, we do not have intervals, so we cannot expect that an analogue of the mean-value theorem holds;

But we should not be too pessimistic, some things are much easier: if $a_n \in \mathbb{Q}_p$, then one can prove

$$\sum_n a_n \quad \text{converges } p\text{-adically} \qquad \Longleftrightarrow \qquad |a_n|_p \to 0 \quad \text{as } n \to \infty.$$

This statement is false over $\mathbb{R}$ where, for example, the harmonic series $\sum_n \frac{1}{n}$ diverges. Further, notions like continuity, differentiability and analyticity remain unchanged since they depend only on the metric structure.

$\mathbb{Q}_p$ is not algebraically closed as we have seen above. Hence, analogously to the real case, we add all algebraic irrationals and obtain the *algebraic closure* $\overline{\mathbb{Q}}_p$; the p-adic absolute value extends uniquely without any problems. But whereas the field of complex numbers has only degree two over the field of real numbers, the

p-adic situation is more complicated: $\overline{\mathbb{Q}}_p$ is much larger than $\mathbb{Q}_p$; it has infinite degree over $\mathbb{Q}_p$. Unfortunately, $\overline{\mathbb{Q}}_p$ is not complete, and thus, it cannot be the right field for doing analysis. But the trip ends after the next step: the completion of $\overline{\mathbb{Q}}_p$ is complete and algebraically closed; we denote it by $\mathbb{C}_p$, in analogy to $\mathbb{C}$. It is obvious that again the p-adic absolute value extends uniquely to $\mathbb{C}_p$. There are several unsolved questions concerning the structure of $\mathbb{C}_p$, e.g. characterizing $\mathbb{Q}_p$-linear field automorphisms.

We follow Mahler's[6] approach to p-adic analysis; see [13]. If

$$n = \alpha_0 + \alpha_1 p + \alpha_2 p^2 + \dots \quad \text{and} \quad k = \beta_0 + \beta_1 p + \beta_2 p^2 + \dots$$

are the p-adic expansions of the integers n and k, then one can show that

$$\binom{n}{k} \equiv \binom{\alpha_0}{\beta_0}\binom{\alpha_1}{\beta_1} \cdot \dots \bmod p.$$

In view of the binomic inversion formula one gets for any continuous functions $f : \mathbb{Z}_p \to \mathbb{C}_p$ the representation

$$f(n) = \sum_{k=0}^{n} \binom{n}{k} a_k(f) \qquad \text{with} \qquad a_k(f) = \sum_{j=0}^{k} \binom{k}{j} (-1)^{k-j} f(j).$$

Defining the *finite difference operator* by

$$\Delta^k f(x) = \sum_{j=0}^{k} (-1)^{k-j} \binom{k}{j} f(x+j) \qquad \text{for } k \in \mathbb{N} \cup \{0\},$$

one can prove the celebrated

THEOREM 7 (Mahler). *Let $f : \mathbb{Z}_p \to \mathbb{C}_p$ be a continuous function and put $a_k = \Delta^k f(0)$ for $n \in \mathbb{N}$. Then $a_k \to 0$ as $k \to \infty$, and*

$$\sum_{k=0}^{n} a_k \binom{x}{k} \quad \longrightarrow \quad f(x) \qquad \text{uniformly on } \mathbb{Z}_p \text{ as } n \to \infty.$$

In particular, there is a sequence of polynomials $f_n \in \mathbb{Z}_p[X]$ that converges uniformly to f.

---

[6] Kurt Mahler,∗26.7.1903, Krefeld, - †25.2.1988, Canberra; left school because of health problems after four classes only; student of Siegel and Dehn in Frankfurt and of Noether, Courant, Landau, Heisenberg and Hilbert in Göttingen; emigrated from Germany to Manchester, invited by Mordell; professor in Canberra.

This is a remarkable and very useful representation; an analogue for continuous real functions does not exist. However, it gives also the p-adic analogue of the well-known Weierstrass' approximation theorem which states that every continuous function on a closed interval is the limit of a uniformly convergent sequence of polynomials.

Further applications of Mahler's theorem are the construction of p-adic anlogues of classical functions like the exponential function, the logarithm or the Gamma-function. But be careful! Not any classical function has a p-adic relative: for example, there do not exist non-constant periodic p-adic functions.

In the next section we will give a new and curious application of Mahler's theorem.

9. A p-adic monster

The first in the mathematical literature appearing *universal* object was discovered by Fekete in 1914/15 (see [12]); he proved the existence of a real power series $\sum_n a_n x^n$ with the property that for any(!) continuous function on the interval $[-1,1]$ with $f(0)=0$ there is a sequence of positive integers (m_k) such that the partial sums $\sum_{1\leqslant n\leqslant m_k} a_n x^n$ converge to f uniformly on $[-1,1]$. In [9] Luh proved the existence of a real power series $\sum_n a_n x^n$ with the property that for any(!) interval $[a,b]$ with $0\notin[a,b]$ and any(!) continuous function f on $[a,b]$ there exists a sequence of positive integers (m_k) such that

$$\sum_{n=0}^{m_k} a_n x^n \quad\longrightarrow\quad f(x) \qquad \text{uniformly on } [a,b] \quad \text{as } k\to\infty.$$

The proof of this interesting variant of Fekete's universality theorem relies essentially on Weierstrass' approximation theorem. We have seen that this result holds also in the p-adic context, and hence it is natural to ask whether there is also a p-adic analogue of this universality theorem. The role of the intervals in the real world will be played by balls like

$$a+p^{\mu}\mathbb{Z}_p := \{\alpha\in\mathbb{Q}_p \,:\, |\alpha-a|_p\leqslant p^{-\mu}\} = \mathcal{B}_{\leqslant p^{-\mu}}(a) \qquad \text{with } \mu\in\mathbb{Z},\ a\in\mathbb{Q}_p.$$

Then

THEOREM 8. *There exists a p-adic power series $\sum_{n=0}^{\infty} a_n x^n$ with the property that for any ball $a+p^{-\nu}\mathbb{Z}_p$ with $a\in\mathbb{Z}_p^*, \nu\in\mathbb{N}$ and any continuous function f on $a+p^{-\nu}\mathbb{Z}_p$ there exists a sequence of positive integers (m_k) such that*

$$\sum_{n=0}^{m_k} a_n x^n \quad\longrightarrow\quad f(x) \quad \text{uniformly on } a+p^{-\nu}\mathbb{Z}_p \quad \text{as } k\to\infty.$$

Since this result is new, we have to prove it.

Proof. Let (Q_n) be the sequence of polynomials with integral coefficients. We construct a sequence of polynomials (P_n) as follows: let $P_0 = Q_0$ and assume that $P_0, \dots, P_{n-1}$ are known. Denote by d_n the degree of P_{n-1}. Now let ϕ_n be a continuous function on $\mathbb{Z}_p$ such that

$$\phi_n(x) = \left(Q_n(x) - \sum_{k=0}^{n-1} P_k(x) \right) x^{-d_n - 1} \qquad \text{for } x \in a + p^{-n}\mathbb{Z}_p.$$

With view to Mahler's theorem there exists a polynomial F_n with

$$\max_{x \in a + p^{-n}\mathbb{Z}_p} |F_n(x) - \phi_n(x)|_p \leqslant p^{-d_n}.$$

Setting $P_n(x)n(x)x^{d_n+1}$, the sequence (P_n) is constructed, and P_n satisfies

$$\max_{x \in a + p^{-n}\mathbb{Z}_p} \left| \sum_{k=0}^{n} P_k(x) - Q_n(x) \right|_p = \max_{x \in a + p^{-n}\mathbb{Z}_p} |(F_n(x) - \phi_n(x))x^{d_n+1}|_p \leqslant p^{-d_n}.$$

Obviously, distinct P_n have no powers in common. Thus we can rearrange the polynomial series into a formal power series:

$$\sum_{n=0}^{\infty} a_n x^n := \sum_{n=0}^{\infty} P_n(x).$$

Again by Mahler's theorem, for any continuous function f on $a + p^{-\nu}\mathbb{Z}_p$ exists a sequence of positive integers (n_k), tending to infinity, such that

$$\max_{x \in a + p^{-n_k}\mathbb{Z}_p} |f(x) - Q_{n_k}(x)|_p \leqslant p^{-n_k}.$$

For sufficiently large k the ball $a + p^{-\nu}\mathbb{Z}_p$ is contained in $a + p^{-n_k}\mathbb{Z}_p$. In view of the above estimates we obtain

$$\begin{aligned}
\max_{x \in a + p^{-n_k}\mathbb{Z}_p} \left| f(x) - \sum_{n=0}^{d_{n_k}+1} a_n x^n \right|_p &= \max_{x \in a + p^{-n_k}\mathbb{Z}_p} \left| f(x) - \sum_{n=0}^{n_k} P_n(x) \right|_p \\
&\leqslant \max_{x \in a + p^{-n_k}\mathbb{Z}_p} |f(x) - Q_{n_k}(x)|_p + \max_{x \in a + p^{-n_k}\mathbb{Z}_p} \left| Q_{n_k}(x) - \sum_{n=0}^{n_k} P_n(x) \right|_p \\
&\leqslant p^{-n_k} + p^{-d_{n_k}},
\end{aligned}$$

which tends to zero as $k \to \infty$. Thus, putting $m_k = d_{n_k} + 1$, the assertion of the theorem follows.

It would be interesting to lift other universality results from the *real* or *complex* world to its *p-adic* analogues (or even to find new).

We conclude with one of the most beautyful aspects of p-adic numbers and p-adic functions.

10. Bernoulli numbers and p-adic L-functions

The *Bernoulli polynomials* $B_n(X)$ are defined by the Taylor series expansion

$$\frac{z\exp(zX)}{\exp(z)-1} = \sum_{n=1}^{\infty} B_n(X)\frac{z^n}{n!},$$

and the *Bernoulli numbers* are given by $B_n = B_n(0)$. It is easy to compute that $B_{2k+1} = 0$ for $k \in \mathbb{N}$, and

$$B_1 = -\frac{1}{2}, \quad B_2 = \frac{1}{6}, \quad B_4 = -\frac{1}{30}, \ldots, B_{30} = \frac{861\,58412\,76005}{14322} \quad , \ldots \ .$$

For the Bernoulli numbers remarkable congruences are known by the work of von Staudt, Clausen and Kummer. As they were regarded as something *mysterious* in the 19-th century it turned out that they appear naturally in the context of p-adic numbers.

THEOREM 9 (von Staudt-Clausen). *Let n be an even positive integer, then*

$$B_n + \sum_{(p-1)|n} \frac{1}{p} \in \mathbb{Z},$$

and, hence, $pB_n \in \mathbb{Z}_p$.

The p-adic proof bases on the simple identity

$$\sum_{j=1}^{n-1} j^k = \sum_{r=0}^{k} \binom{k}{r} B_r \frac{n^{k+1-r}}{k+1-r},$$

but is quite tricky; see [4]. We shall give only an example for the von Staudt-Clausen theorem:

$$B_{30} + \frac{1}{2} + \frac{1}{3} + \frac{1}{7} + \frac{1}{11} + \frac{1}{31} = 6015\,80875.$$

Bernoulli numbers are not only interesting because of their relation to Fermat's last theorem, discovered by Kummer, but for algebraic number theory in general. They are the main ingredient for the construction of p-adic zeta-functions and p-adic L-functions as analogues of their classical relatives.

Let q be a positive integer. A Dirichlet character χ mod q is a non-vanishing, multiplicative group homomorphism from the group of prime residue classes mod q onto $\mathbb{C}$. Define

$$\chi(n) = \begin{cases} \chi(m \bmod q) & \text{if } \gcd(n,q) = 1, \\ 0 & \text{if } \gcd(n,q) > 1. \end{cases}$$

Then χ extends to a periodic and multiplicative arithmetical function; here $\gcd(n,q)$ is the greatest common divisor of q and n. Then the associated Dirichlet L-function is given by

$$L(s,\chi) = \prod_p \left(1 - \frac{\chi(p)}{p^s}\right)^{-1} = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} \qquad \text{for } \mathrm{Re}\, s > 1,$$

and by analytic continuation elsewhere except for at most one simple pole at $s = 1$ with residue 1. $L(s,\chi)$ has a pole at $s = 1$ if and only if χ is the principal character mod q, i. e. $\chi(n) = 1$ for all n coprime with q. The well-known Riemann zeta-function may be regarded as L-function to the principal character mod 1. Of special interest in number theory are the values of Dirichlet L-functions at the integers. It is remarkable that the values taken at the negative integers are rational:

$$L(1-n,\chi) = -\frac{B_{n,\chi}}{n} \qquad \text{with} \qquad B_{n,\chi} := q^{n-1}\sum_{a=1}^{q}\chi(a)B_n\left(\frac{a}{q}\right) \qquad \text{for } n \in \mathbb{N}.$$

The first construction of p-adic L-functions is due to Kubota and Leopoldt. Meanwhile, other constructions were found, e.g. the way via p-adic integration; see [7]. But any construction is beyond the scope of this survey; we can only quote the main result. If we define a character ω by setting $\omega(a) \equiv a \bmod p$ for $a \in \mathbb{Z}_p^*$, then

THEOREM 10 (Kubota+Leopoldt). *Let χ be a Dirichlet character of conductor q, and let F be any multiple of q and $P = p$ if $p \neq 2$, or $P = 4$ if $p = 2$. Then there exists a p-adic meromorphic function $L_p(s,\chi)$ on $\{s \in \mathbb{C}_p : |s|_p < Pp^{\frac{-1}{p-1}}\}$ such that*

$$L_p(1-n,\chi) = -(1-(\chi\omega^{-n})(p))\frac{B_{n,\chi\omega^{-n}}}{n} \qquad \text{for } n \in \mathbb{N}.$$

If χ is not the principle character, then $L_p(s,\chi)$ is analytic, otherwise $L_p(s,\chi)$ is analytic except for a simple pole at $s = 1$ with residue $1 - \frac{1}{p}$.

In particular,

$$L_p(1-n,\chi) = L(1-n,\chi)(1-\chi(p)p^{n-1}) \qquad \text{if } n \equiv 0 \bmod p-1;$$

here the factor on the right hand side is exactly the Euler factor at p for $L(s,\chi)$. The proof bases mainly on the theorem of von Staudt-Clausen; for details see [17] or [10]. One immediate consequence are the *Kummer congruences*

$$\frac{B_m}{m} \equiv \frac{B_n}{n} \bmod p \qquad \text{if } m \equiv n \not\equiv 0 \bmod p-1.$$

Moreover, there is a striking analogy between the behaviour of the classical Dirichlet L-functions and its p-adic relatives for the value taken at $s = 1$, which is of special interest for the class number problem; we refer the interested reader once more to [17].

We did not speak about the influence of p-adic numbers to class field theory (the p-adic proof of the celebrated Kronecker-Weber theorem; see [4]) or the impacts to diophantine equations and transcendence theory (the p-adic proof of the transcendence of exp(1) due to Bezivin and Robba [2] - a dream of Hensel). And there is much more what we left out, but we hope that during this short trip through the world of p-adic numbers the reader became interested into this field.

ACKNOWLEDGMENT . The author would like to express his deep gratitude to all members at the Department for Mathematics at Šiauliai University and the kind hospitality during his visits.

REFERENCES

[1] S. Albeverio, A. Khrennikov, P. E. Kloeden, Memory retrieval as a p-adic dynamical system, *BioSystems* **49,** 105–115 (1999).

[2] J. P. Bezivin, P. Robba, A new p-adic method for proving irrationality and transcendence results, *Ann. Math.* **129,** 151–160 (1989).

[3] S. I. Borewič, I. R. Šafarevič, *Zahlentheorie*, Birkhäuser (German translation of the Russian original) (1966).

[4] J. W. S. Cassels, *Local fields*, London Mathematical Society, Cambridge University Press (1986).

[5] F. Q. Gouvea, *p-adic numbers*, Springer (1993).

[6] K. Hensel, Über eine neue Begründung der Theorie der algebraischen Zahlen, *Jahresberichte Deutschen Mathematiker Vereinigung* **6,** 83–88 (1897).

[7] N. Koblitz, *p-adic numbers, p-adic analysis, and zeta-functions*, Springer (1977).

[8] T. Kubota, H. W. Leopoldt, Eine p-adische Theorie der Zetawerte I. Einführung der p-adischen Dirichletschen L-Funktionen, *J. reine angew. Math.* **214/215,** 328–339 (1964).

[9] W. Luh, Universalfunktionen in einfach zusammenhängenden Gebieten, *Aequationes Mathematicae* **19,** 183–193 (1979).

[10] M. R. Murty, *Introduction to p-adic Analytic Number Theory* http://www.mri.ernet.in/∼mathweb/lecture/murty-padic00/.

[11] I. P. Nathanson, *Theorie der Funktionen einer reellen Veränderlichen*, Verlag Harri Deutsch (1977).

[12] J. Pál, Zwei kleine Bemerkungen, *Tohoku Math. J.* **6,** 42–43 (1914/15).

[13] A. M. Robert, *A course in p-adic Analysis*, Springer (2000).

[14] M. R. Schroeder, *Number theory in Science and Communication*, Springer (1997).

[15] J. P. Serre, *A course in Arithmetic*, Springer (1973).

[16] H. P. F. Swinnerton-Dyer, *A brief guide to Algebraic Number Theory*, London Mathematical Society (2001).

[17] L. C. Washington, *Introduction to cyclotomic fields*, Springer (1982).

p-adityviųjų skaičių ir *p*-adityviųjų funkcijų pasaulis

J. Steuding

Pateiktas trumpas ir elementarus įvadas apie p-adityviuosius skaičius ir p-adityviąsias funkcijas. Pavyzdžiui, supažindinama su nearchimedine metrika, ultrametrine topologija ir panašiai. Be to įrodomas universlios p-adityvios laipsninės eilutės Fekete prasme egzistavimas.

Rankraštis gautas
2002 04 17