An introduction to arithmetic dynamics

Franco Vivaldi

School of Mathematical Sciences,
Queen Mary, University of London, London E1 4NS, UK.

Course presented at the Summer School on Dynamical Systems
at the Mathematisches Institut, Georg-August Universität Göttingen
July 2011

Last updated: August 8, 2011

Preface

Arithmetic dynamics is discrete-time dynamics (function iteration) over arithmetical sets, such as algebraic number rings and fields, finite fields, p-adic fields, polynomial rings, algebraic curves, etc. This rapidly growing area of research lies at the interface between dynamics and number theory. It is rich in history and motivations, and is a fertile ground for the development of algorithmic and computer-oriented theories.

Some constructs of arithmetic dynamics (periodic orbits and their stability), are straightforward adaptations of dynamical concepts. Others (entropy, bifurcations), expose unexpected connections. The probabilistic phenomena are the most intriguing, as they originate from fluctuations of arithmetical origin. There one finds at the outset problems of considerable difficulty.

Some ideas of arithmetic dynamics are simple and compelling. By exploiting this circumstance, it is possible to introduce this subject while keeping the pre-requisite material to a minimum. This is the aim of the present course. I assume some familiarity with dynamical systems ideas, although little specific knowledge is actually used. The necessary background in arithmetic and algebra will be reviewed briefly, mostly omitting the proofs.

For advanced texts on arithmetic dynamics, see [4, 13, 2].

Franco Vivaldi
London, July 2011.

Contents

1 Gauss and the digits of rationals

We begin with some observations about digits of fractions. The decimal fraction $1/7$ is periodic, with period length 6

$$\frac{1}{7} = 0.142857\,142857\ldots.$$

The period of the fraction $1/11$ is only 2; if we change the numerator, the digits change, but the period remains the same

$$\frac{1}{11} = 0.09\,09\ldots \qquad \frac{8}{11} = 0.72\,72\ldots$$

By contrast, the digits of $11/12$ are not periodic: there is a transient of length 2, followed by period 1

$$\frac{11}{12} = 0.91\,6\,6\,6\ldots.$$

These problems were first studied by Gauss, in 1801 [5, art. 316].

Consider a rational number $x_0 = n/m$, with $0 \leqslant x_0 < 1$. Let $d_1, d_2, \ldots$ be its decimal digits.

$$\frac{n}{m} = \sum_{k \geqslant 1} \frac{d_k}{10^k} = 0.d_1 d_2 \ldots \qquad d_k \in \{0, \ldots, 9\}. \tag{1}$$

The first digit d_1 is computed as the integer part of $10x_0$

$$10x_0 = d_1.d_2 d_3 \ldots \qquad d_1 = \lfloor 10x_0 \rfloor$$

where the symbol $\lfloor \cdot \rfloor$ denotes the floor function. Let now $x_1 = 10d_0 - d_1 = 0.d_2 d_3 \ldots$. We obtain d_2 as the integer part of $10x_1$, etc. This process leads to the following recursive sequence of rational numbers $x_k \in [0, 1)$

$$x_0 = x \qquad x_{k+1} = 10x_k - \lfloor 10x_k \rfloor, \quad k \geqslant 0. \tag{2}$$

Each element of this sequence has denominator m (ignoring simplifications); there are m such rational numbers, hence, by Dirichlet's pigeon hole principle, the sequence (x_k) must be eventually periodic. But then so must the sequence (d_k) of the decimal digits of x_0.

Dynamically speaking, there are two perspectives on this problem. On the one hand, we may clear the denominators of our rationals, to obtain a dynamics over a finite set of integers. For instance, the first few steps in the recursive construction of the digits of $1/7$ are as follows

$$10 \times \frac{1}{7} = 1 + \frac{3}{7}, \qquad 10 \times \frac{3}{7} = 4 + \frac{2}{7}, \qquad 10 \times \frac{2}{7} = 2 + \frac{6}{7}.$$

The numerators $(1, 3, 2, \ldots)$ of the fractions form a recursive sequence of integers, determined by multiplication by 10 modulo 7. This construct clearly extends to any integer base $\omega > 1$, with digits $d_k \in \{0, 1, \ldots, \omega - 1\}$. So, for each denominator m, we have a dynamical system over the set of remainders (residues classes) modulo m

$$f_{\omega,m}(x) = \omega x \,(\mathrm{mod}\ m).$$

On the other hand, we may embed the rational dynamics —defined by equation (2)— on the continuum, namely the unit interval $I = [0,1)$

$$f_\omega : I \to I \qquad x \mapsto \omega x \,(\mathrm{mod}\ 1). \tag{3}$$

The dynamical system f_ω has strong statistical properties (ergodic, mixing, positive entropy). It is not difficult to see that map $f_{\omega,m}$ is conjugate to the restriction of f_ω to the rational numbers with denominator m in the unit interval. (Two maps $f : X \to X$ and $g : Y \to Y$ are conjugate if there exists a one-to-one map $L : X \to Y$ such that $f = L^{-1} \circ g \circ L$.)

If $x \in I \cap \mathbb{Q}$, then x is eventually periodic under f_ω. The converse is also true. Indeed, if x is periodic, then so are its digits in base ω. From a periodic digit sequence $(\overline{d_0, d_1, \ldots, d_{t-1}})$, we compute x explicitly as (see exercises)

$$x = \sum_{k=0}^{\infty} d_k \omega^{-(k+1)} = \frac{1}{\omega^t - 1} \sum_{k=0}^{t-1} d_k \omega^{t-1-k}. \tag{4}$$

The point x is clearly rational. The digits may be chosen arbitrarily, so periodic orbits of any period exist. They are precisely the rationals with denominator co-prime to ω, which are dense in I and all unstable (since $|f'_\omega| = |\omega| > 1$). If the denominator of x is not co-prime to ω, we observe irreversible pre-periodic behaviour.

Some natural questions arise, none of which has an easy answer:

- If $x_0 = n/m$, then the period is at most $m-1$; what is the actual period?
- Which rationals n/m have period equal to $m-1$?
- The denominator of a periodic point is a divisor of $\omega^t - 1$, where t is the period. What is the smallest denominator a point with period t can have?

These problems lead to the study of the linear map $x \mapsto \omega x$, first over the finite rings of modular arithmetic, and then over the p-adic fields. It will be instructive to compare and contrast these dynamics with those of the analogous map over the complex numbers.

1.1 Exercises

The map f_ω is defined in (3).

Problem 1. Let X be a finite set and let $f : X \to X$ be a map. Show that all orbits of f are periodic if and only if f is invertible.

Problem 2. Prove that a point in the unit interval is eventually periodic for the map f_ω iff it is rational, and periodic iff its denominator is co-prime to ω.

Problem 3. Consider the 'doubling map' f_2.

(a) By looking at periodic binary digits, show that there are three orbits of minimal period 4. How many orbits are there of minimal period 6? (To answer, you do not need to compute all 6-strings!).

(b) Divide the unit interval in four equal sub-intervals, hence determine the density histogram with respect to this partition[1], for the periodic orbit with initial condition $1/51$. Do the same with the initial condition $1/13$.

(c) Divide the unit interval in 16 equal sub-intervals, whence determine the binary digits of a 16-cycle whose density histogram is uniform (i.e., the cycle has one point in each sub-interval).

Problem 4. Consider the doubling map f_2.

(a) Determine all points of the 3-cycle with initial condition

$$x_0 = 0.001\,001\,001\,001\ldots = 0.\overline{001}$$

as rational numbers.
[*The number x_0 is the sum of a geometric series.*]

(b) Do the same for the 6-cycle

$$x_0 = 0.001101\,001101\,001101\ldots = 0.\overline{001101}.$$

[1] The fraction of the points that belong to each sub-interval.

2 Modular arithmetic

A background reference for this section is [7].

We recall some facts about modular arithmetic.

1. Let m be a positive integer, and let a and b be integers. If m divides $b-a$ we say that a is **congruent** to b modulo m, and we write $a \equiv b \pmod{m}$. This notation is due to Gauss. The integer m is called the **modulus** of the congruence.

2. A congruence relation is an equivalence relation over $\mathbb{Z}$. The equivalence class $[a]_m$ of an integer a is the set of integers that differ from a by a multiple of m, namely

$$[a]_m = \{\ldots, a-2m, a-m, a, a+m, a+2m, \ldots\} = a + m\mathbb{Z}.$$

There are m such **residue classes** modulo m. A set of m representatives, one from each class, is called a **complete set of residues** modulo m. Common choices are $0, 1, \ldots, m-1$, or the numerically least residues, e.g., for odd m

$$-\frac{m-1}{2}, \ldots, -2, -1, 0, 1, 2, \ldots, \frac{m-1}{2}.$$

3. Addition and multiplication of residue classes to the same modulus are defined as

$$[x]_m + [y]_m = [x+y]_m \qquad [x]_m \cdot [y]_m = [x \cdot y]_m$$

or, equivalently,

$$(x+m\mathbb{Z}) + (y+m\mathbb{Z}) = x+y+m\mathbb{Z} \qquad (x+m\mathbb{Z})(y+m\mathbb{Z}) = xy+m\mathbb{Z}.$$

These operations give the set $\mathbb{Z}/m\mathbb{Z}$ of residue classes the structure of a **finite commutative ring with identity**. The additive and multiplicative identities of the ring are the classes $[0]_m$ and $[1]_m$, respectively.

4. For sum, subtraction, and multiplication, congruences to the same modulus behave like equations. Thus if $a \equiv a' \pmod{m}$ and $b \equiv b' \pmod{m}$, then $a \pm b \equiv a' \pm b' \pmod{m}$ and $ab \equiv a'b' \pmod{m}$. Division requires care. If $ab \equiv ac \pmod{m}$, and $d = \gcd(a,m)$, then $b \equiv c \pmod{m/d}$. In particular, if $m = p$ is prime, then the congruence $ab = ac \pmod{p}$ implies either $a \equiv 0 \pmod{p}$ or $b \equiv c \pmod{p}$.

5. A solution of the linear congruence $ax \equiv b \pmod{m}$ exists iff $d = \gcd(a,m)$ divides b, in which case, if $x = s$ is one solution, then

$$x = s + k\frac{m}{d} \qquad k \in \mathbb{Z}$$

gives all solutions (d incongruent solutions modulo m). The solution s can be found, for instance, by using Euclid's algorithm. Thus if $b = 1$ and a is co-prime to m, then s is a **modular inverse** of a, that is, $[s]_m = [a]_m^{-1}$.

6. In particular, for p prime and $a \not\equiv 0 \pmod{p}$, the congruence $ax \equiv 1 \pmod{p}$ always has a solution. Indeed the finite ring $\mathbb{Z}/m\mathbb{Z}$ is a **finite field** iff m is a prime number.

For each positive integer m, we let $\phi(n)$ be the number of integers in the range $1, \ldots, n$, which are relatively prime to n. The function ϕ is called **Euler's ϕ-function**. Thus $\phi(5) = 4, \phi(6) = 2$.

For $n > 1$, we have $1 \leqslant \phi(n) \leqslant n - 1$. We have $\phi(n) = n - 1$ precisely if n is prime.

The following theorem, due to Euler, generalises an earlier result by Fermat [7, theorem 72].

Theorem 1 *If a and m are co-prime, then $a^{\phi(m)} \equiv 1 \pmod{m}$.*

Theorem 2 *The function ϕ is multiplicative, i.e., if m and n are co-prime, then $\phi(mn) = \phi(m)\phi(n)$.*

For a proof, see [7, theorem 60].

Let $m > 1$ have the prime factorisation

$$m = \prod_{k=1}^{r} p_k^{e_k}$$

where the p_k are distinct primes and $e_k \geqslant 1$. Using theorem 2, we can compute the value of $\phi(n)$ from the knowledge of $\phi(p^e)$, where p is a prime number, and e is a positive integer. Clearly

$$\phi(p^e) = \#\{1, 2, 3, \ldots, p^e\} - \#\{p, 2p, 3p, \ldots, p^e\} = p^e - p^{e-1}.$$

From this we obtain the formula

$$\phi(m) = \prod_{k=1}^{r} p_k^{e_k - 1}(p_k - 1) = m \prod_{k=1}^{r} \left(1 - \frac{1}{p^k}\right). \tag{5}$$

The divisor sum of Euler's ϕ-function is very tidy [7, theorem 63].

Theorem 3 *Let $m > 1$ be an integer. Then*

$$\sum_{d|m} \phi(d) = m.$$

2.1 Primitive roots

Let ω and m be co-prime integers, and $m > 1$. The (multiplicative) **order** of ω modulo m is the smallest positive integer t such that $\omega^t \equiv 1 \pmod{m}$. We write $\mathrm{ord}_m(a) = t$. From Euler's theorem, we have $\omega^{\phi(m)} \equiv 1 \pmod{m}$, so the order of ω modulo m exists, and does not exceed $\phi(m)$.

If ω and m are not co-prime, then $\omega^t \not\equiv 1 \pmod{m}$, for all positive t (since $\omega^t = 1 + km$ implies that ω and m are co-prime); so the order is undefined.

Theorem 4 *Let ω and $m > 1$ be co-prime integers, and let t be the multiplicative order of ω modulo m. The following holds:*

(i) $\omega^i \equiv 1 \pmod{m} \Leftrightarrow t \mid i$

(ii) $t \mid \phi(m)$

(iii) *If* $i, j, \in \mathbb{Z}$ *and* $i > j$, *then*

$$\omega^i \equiv \omega^j \pmod{m} \quad \Leftrightarrow \quad i \equiv j \pmod{t}.$$

Hence $\omega, \omega^2, \ldots, \omega^t$ *are distinct modulo m.*

(iv) *For all* $k > 0$, *we have* $\mathrm{ord}_m(\omega^k) = t/\mathrm{gcd}(k,t)$.

(v) *If* $d|t$, *then there are* $\phi(d)$ *values of* ω^k *modulo m for which* $\mathrm{ord}_m(\omega^k) = d$.

The most important item is (ii), which can be justified as follows. From remark 5 above, it follows that the congruence classes co-prime to the modulus m form a multiplicative group. The order of this group is $\phi(m)$, by definition of ϕ. Then the order of an element of this group divides $\phi(m)$, from Lagrange's theorem. The proof of the remaining items in theorem 4 is left as an exercise.

Let ω and m be co-prime integers, with $m > 1$. We say that ω is a **primitive root** modulo m if $\mathrm{ord}_m(\omega) = \phi(m)$.

Some remarks

1. Given m, a primitive root modulo m does not necessarily exist; the existence of a primitive root is equivalent to the multiplicative group of $\mathbb{Z}/m\mathbb{Z}$ being cyclic.
2. If a primitive root ω exists, then $\omega, \omega^2, \ldots, \omega^{\phi(m)}$ are all co-prime to m and distinct modulo m, from theorem 4 (iii). Hence these integers constitute a reduced residue system modulo m.
3. If a primitive root ω exists, then there are $\phi(\phi(m))$ distinct ones modulo m, by 2 above and theorem 4 (iv).

Theorem 5 *Let p be a prime. Then for each divisor d of* $p-1$ *there are* $\phi(d)$ *numbers of order d, which are incongruent modulo p.*

Letting $d = p-1$, we deduce that there are $\phi(p-1)$ primitive roots modulo a prime p.

2.2 Dynamical interpretation

Let m and ω be positive integers. We consider the dynamical system

$$f_{\omega,m} : \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \qquad x \mapsto \omega x \pmod{m} \tag{6}$$

where ω is an integer. The phase space has m elements. From observation 5, section 2 we see that the dynamics is invertible if and only if $\gcd(\omega, m) = 1$, in which case $x_t \equiv \omega^{-1} x_{t+1} \pmod{m}$, and all orbits are periodic.

In what follows we assume that ω and m are co-prime. For periodicity, we require $x_t \equiv x_0 \pmod{m}$. Now, $x_t \equiv \omega^t x_0 \pmod{m}$, giving

$$x_0 \omega^t \equiv x_0 \pmod{m}.$$

Dividing by x_0, we obtain (observation 4, section 2)

$$\omega^t \equiv 1 \pmod{m'} \qquad\qquad m' = \frac{m}{\gcd(x_0, m)}.$$

Thus the minimal period t is the **multiplicative order** of ω modulo m'. Such a quantity is well-defined, since ω and m' are co-prime by assumption (see remark in section 2.1).

Thus the period depends on the initial condition x_0 via $\gcd(x_0, m)$. From the formula for $\phi(m)$ (5), we see that if $m' \mid m$, then $\phi(m') \mid \phi(m)$. This fact, together with theorem 4 (ii) implies that if $\gcd(\omega, m) = 1$, then the period of any orbit of f is a divisor of $\phi(m)$.

The simplest case is $m = p$, a prime. Then $\gcd(x_0, p)$ is either p or 1. The former case corresponds to a fixed point at the origin. For all other initial conditions, the period is the same, and is equal to $\mathrm{ord}_p(\omega)$. The period is maximal precisely when ω is a primitive root modulo p.

The following lemma will allow us to reduce the computation of the period of the orbits of (6) to the case in which m is a prime power.

Lemma 6 *Let ω, m_1, m_2 be pairwise co-prime integers, with $m_1, m_2 > 1$. Then*

$$\mathrm{ord}_{m_1 m_2}(\omega) = \mathrm{lcm}(\mathrm{ord}_{m_1}(\omega), \mathrm{ord}_{m_2}(\omega)).$$

The case in which m and ω are not co-prime is left as an exercise.

2.3 An unsolved problem

We pointed out that the period of any non-zero point in $\mathbb{Z}/m\mathbb{Z}$ is maximal precisely if $m = p$ is a prime number, and ω is a primitive root modulo p. In dynamical terms, if ω is a primitive root modulo p, then the orbit of a rational point with denominator p under the map f_ω consists of $p - 1$ equally spaced points in the unit interval. This is an extraordinary degree of spatial uniformity, which most periodic orbits of f_ω do not have.

Fix an integer $\omega \neq 0, \pm 1$. What is the probability that ω is a primitive root modulo p? More precisely, let $\mathscr{P}_\omega$ be the set of all the primes co-prime to ω, and let us consider the quantity

$$A(\omega, x) = \frac{\#\{p \in \mathscr{P}_\omega \,:\, p \leqslant x, \, \mathrm{ord}_p(\omega) = p - 1\}}{\#\{p \in \mathscr{P}_\omega \,:\, p \leqslant x\}}. \tag{7}$$

(If $p \notin \mathscr{P}_\omega$, then $\mathrm{ord}_p(\omega)$ is undefined.) Then we take the limit

$$A(\omega) = \lim_{x \to \infty} A(\omega, x).$$

The quantity $A(\omega)$ —if it exists— is the fraction of prime numbers co-prime to ω for which the period is maximal. Does this limit exist? It is not difficult to see that if $\omega = n^2$ is a square, then such a limit is zero. Indeed, from Euler's theorem, we have

$$\omega^{\frac{p-1}{2}} = n^{p-1} \equiv 1 \,(\mathrm{mod}\ p)$$

and so the order of ω divides $(p-1)/2$, and it can never be maximal. Let us thus assume that ω is not a square in $\mathbb{Z}$.

In 1927, E Artin put forward the following conjecture.

Conjecture 1 *Let ω be an integer which is not the power of any integer. Then*

$$A(\omega) = \prod_p \left(1 - \frac{1}{p(p-1)}\right) = 0.3739558\ldots \tag{8}$$

independent of ω.

The number appearing in this formula is known as **Artin's constant**. Subsequent computations revealed that some adjustments are required in the above formulation (the square-free kernel of ω must not be congruent to 1 modulo 4).

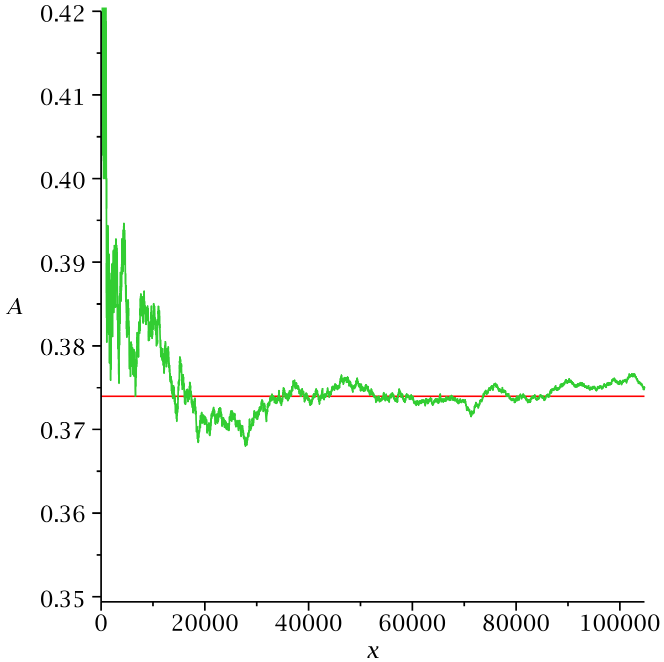

Figure 1: Behaviour of the quantity $A(2,x)$ defined in equation (7), as a function of x. The horizontal line represents Artin's constant (8). This computation was performed over the first 10,000 odd primes.

Artin's conjecture is still unresolved; it has been proved under the assumption of the so-called generalised Riemann hypothesis [11]. The convergence of the quantity (7) to Artin's constant is illustrated in figure 1, for $\omega = 2$.

In summary, linear dynamics modulo a prime p has a simple structure: there is a fixed point at the origin, and the remaining $p-1$ points are subdivided into N periodic orbits of period $(p-1)/N$, for some divisor N of $p-1$. The computation of N is conceptually simple, but hard in practice. (There is no known algorithm that will output N in a time which is polynomial in the input size. The latter is of order $\log_2(p)$, the number of bits needed to specify p.) However, an underlying probabilistic phenomenon is at work. Artin's conjecture states that the chances that $N = 1$ are about 37%.

2.4 Exercises

The map $f_{\omega,m}$ is defined in (6).

Problem 1. Calculate the value of the Euler ϕ-function $\phi(m)$ for the following values of m

$$a)\quad 512; \qquad\qquad b)\quad 1155; \qquad\qquad c)\quad 10!.$$

Problem 2. For the following values of m, characterize the integers ω such that map $f_{\omega,m}$ has precisely two orbits.

$$a)\quad 13; \qquad\qquad b)\quad 23.$$

[*Consider primitive roots.*]

Problem 3. Compute the quantity

$$\frac{7}{13} \pmod{23}$$

by determining $1/13$ as $13^{-1} = 13^{t-1}$, where t is the order of 13 modulo 23.
[*To compute t, consider the computations of part (a) of previous problem.*]

Problem 4. Show that the number of distinct periods the orbits of the map $f_{\omega,m}$ (with $\gcd(\omega,m) = 1$) cannot be greater than the number of divisors of m. Identify conditions under which the number of distinct periods is equal to the number of divisors of m.

Problem 5. Determine the maximum transient length an orbit of $f_{\omega,m}$ can have.

Problem 6. Let ω, m_1, m_2 be pairwise co-prime integers, with $m_1, m_2 > 1$. Prove that

$$\mathrm{ord}_{m_1,m_2}(\omega) = \mathrm{lcm}\big(\mathrm{ord}_{m_1}(\omega), \mathrm{ord}_{m_2}(\omega)\big).$$

(Using this formula, the computation of the periods of the orbits of the map f_{ω,m_1m_2} is reduced to that of the maps f_{ω,m_1} and f_{ω,m_2}.)

Problem 7. Prove that the product of all the squares modulo p is congruent to $(-1)^{(p+1)/2}$ modulo p.
[*Use a primitive root.*]

Problem 8*. Show that if p and $q = 4p + 1$ are both primes, then 2 is a primitive root modulo q. Give a dynamical interpretation of this result.
[*Some knowledge of quadratic residues is required.*]

Problem 9. Write a computer program to reproduce the data of figure 1.

3 *p*-adic numbers

A background reference for this section is [6].

Linear dynamics modulo a prime-power is highly organised. There is a rather surprising theory, that will allow us to describe it using the tools of analysis. This is the theory of ***p*-adic numbers.**

The familiar absolute value function $|\cdot|$ is first defined in $\mathbb{Z}$,

$$|\cdot|:\mathbb{Z}\to\mathbb{Z}\qquad\qquad |x| = \begin{cases} x & \text{if } x\geqslant 0\\ -x & \text{if } x<0.\end{cases}$$

and then extended to the field $\mathbb{Q}$ of rational numbers via the equation

$$\left|\frac{a}{b}\right| = \frac{|a|}{|b|}\qquad\qquad a,b\in\mathbb{Z},\quad b\neq 0.$$

We wish to define other absolute value functions on $\mathbb{Q}$.

Fix a prime p. The ***p*-adic valuation** v_p is the function

$$v_p:\mathbb{Z}\smallsetminus\{0\}\to\mathbb{Z}$$

defined as follows. For each $n\in\mathbb{Z}$, let $v_p(n)$ be the unique non-negative integer v such that

$$n = p^v\cdot n'\qquad\qquad \gcd(p,n') = 1.$$

If $x = a/b\in\mathbb{Q}\smallsetminus\{0\}$, then letting

$$v_p(x) = v_p(a) - v_p(b)$$

we extend v_p to non-zero rationals. For example

$$v_5(900) = 2\qquad v_7(91) = 1\qquad v_3(2/3) = -1\qquad v_p(2/3) = 0,\quad p>3.$$

Lemma 7 *For all $x,y\in\mathbb{Q}\smallsetminus\{0\}$, we have*

i) $v_p(xy) = v_p(x) + v_p(y)$.

ii) $v_p(x+y)\geqslant \min(v_p(x),v_p(y))$.

The proof is left as an exercise.

Let $x\in\mathbb{Q}$. The ***p*-adic absolute value** $|x|_p$ is defined as follows

$$|x|_p = \begin{cases} p^{-v_p(x)} & \text{if } x\neq 0\\ 0 & \text{if } x=0.\end{cases}\tag{9}$$

Theorem 8 *The function $x \mapsto |x|_p$ satisfies the following conditions, for all $x, y \in \mathbb{Q}$.*

i) $|x|_p = 0 \Leftrightarrow x = 0$

ii) $|xy|_p = |x|_p |y|_p$

iii) $|x+y|_p \leqslant \max(|x|_p, |y|_p)$.

The proof is an immediate consequence of lemma 7. Since $\max(|x|_p, |y|_p) \leqslant |x|_p + |y|_p$, property *iii)* implies the triangle inequality

iv) $|x+y|_p \leqslant |x|_p + |y|_p$.

Let F be a field. A function $|\cdot| : F \longrightarrow \mathbb{R}^+$ satisfying $i), ii), iv)$ is called an **absolute value**. If $iv)$ is replaced by the stronger $iii)$, then the absolute value is said to be **non-archimedean.**

Lemma 9 *Let F be a field. Any absolute value on F satisfies the following conditions, for all $x \in F$.*

i) $|1| = 1$

ii) *If* $|x^n| = 1$, *then* $|x| = 1$

iii) $|-1| = 1$

iv) $|-x| = |x|$.

PROOF. By definition, if $x \neq 0$, then $|x|$ is a positive real number. Then

$$|1| = |1 \times 1| = |1|\,|1| \Rightarrow |1| = 1; \qquad |x^n| = |x|^n = 1 \Rightarrow |x| = 1;$$

etc. □

Let F be a field, let $|\cdot|$ be an absolute value on F, and let $x, y \in F$. Define a distance d on F as

$$d(x,y) = |x-y|.$$

We mainly consider $F = \mathbb{Q}$, and $|\cdot| = |\cdot|_p$. It is customary to associate the ordinary absolute value $|\cdot|$ with the 'prime at infinity', and write

$$|\cdot|_\infty := |\cdot|.$$

Proposition 10 *Let F be a field, and let $|\cdot|$ be a non-archimedean absolute value on F. If $x, y \in F$, and $|x| \neq |y|$, then $|x+y| = \max(|x|, |y|)$.*

PROOF. Without loss of generality, we suppose that $|x| > |y|$. Then

$$|x+y| \leqslant |x| = \max(|x|,|y|).$$

On the other hand, $x = (x+y) - y$, and hence

$$|x| \leqslant \max(|x+y|,|y|)$$

and since $|x| > |y|$, this inequality can hold only if

$$\max(|x+y|,|y|) = |x+y|.$$

Thus $|x+y| \leqslant |x| \leqslant |x+y|$, which proves our assertion. □

For example, if $F = \mathbb{Q}$, with absolute value $|\cdot|_2$, then $|1024+1023|_2 = |1023|_2 = 1$.

Consider now finite expansions in base p.

$$x = \sum_{k=n_0}^{n} d_k p^k \qquad d_k \in \{0,1,\ldots,p-1\}, \qquad d_{n_0} \neq 0. \tag{10}$$

If $d_k \neq 0$, then $|d_k p^k|_p = |d_k|_p |p|_p^k = p^{-k}$, so the non-zero terms in the above sum become smaller as k increases. Consequently, from proposition 10 and an easy induction, we obtain

$$|x|_p = p^{-n_0}.$$

Therefore, in the p-adic metric, sums of the type (10) are bounded.

To make these observations concrete, let us examine the sequence of non-negative powers of 2, measuring their size with the absolute value $|\cdot|_3$. We have $|2|_3 = 1$, and hence $|2^k|_3 = 1$ for all $k \in \mathbb{Z}$. We represent 2^k to the base 3 as in equation (10), and then write the 3-ary digits of 2^k backwards, so that the digit which is most significant with respect to $|\cdot|_3$ appears on the left.

k	2^k	3-adic digits
0	$1 = 1\cdot 3^0$	.1
1	$2 = 2\cdot 3^0$	.2
2	$4 = 1\cdot 3^0 + 1\cdot 3^1$	.11
3	$8 = 2\cdot 3^0 + 2\cdot 3^1$	.22
4	$16 = 1\cdot 3^0 + 2\cdot 3^1 + 1\cdot 3^2$	.121
5	$32 = 2\cdot 3^0 + 1\cdot 3^1 + 1\cdot 3^3$	.2101
$2\cdot 3$	$64 = 1\cdot 3^0 + 1\cdot 3^2 + 2\cdot 3^3$	.1012
$\vdots$		
$2\cdot 3^2$	$2^{2\cdot 3^2} = 1\cdot 3^0 + 1\cdot 3^3 + 2\cdot 3^4 + \cdots$	.1001212...
$\vdots$		
$2\cdot 3^3$	$2^{2\cdot 3^3} = 1\cdot 3^0 + 1\cdot 3^4 + 2\cdot 3^5 + \cdots$	.100012101...
$\vdots$		
$2\cdot 3^4$	$2^{2\cdot 3^4} = 1\cdot 3^0 + 1\cdot 3^5 + 2\cdot 3^6 + \cdots$	.1000012102...
$\vdots$		

Let us inspect the data. The sequence of integers

$$4^3, 4^{3^2}, \ldots, 4^{3^k}, \ldots$$

appears to 'converge' to 1, in the sense that the terms of the sequence differ from 1 by an increasing power of 3. This phenomenon need not be completely mysterious. If you consider that in the 3-adic metric, increasing powers of 3 become smaller and smaller, then the convergence of the sequence above seems justified by the limit

$$\lim_{\varepsilon \to 0} 4^{\varepsilon} = 1.$$

There also seems to be convergence for the integer sequence

$$\frac{4^{3^k} - 1}{3^k}, \qquad k = 0, 1, \ldots.$$

What is the limit in this case? Analogy with complex analysis would suggest that

$$\lim_{\varepsilon \to 0} \frac{4^{\varepsilon} - 1}{\varepsilon} = \log(4).$$

These heuristic observations can be made rigorous, as we shall see in the next sections.

3.1 Completion

The process of completion generalises the construction of the real numbers from the rationals, familiar from real analysis.

Let F be a field, and let $|\cdot|$ be an absolute value on F. A sequence (x_k) in F is a **Cauchy sequence** if $\forall \varepsilon > 0\ \exists N \in \mathbb{N}$ such that $|x_n - x_m| < \varepsilon$ whenever $m, n \geqslant N$. A field F is **complete** with respect to $|\cdot|$ if every Cauchy sequence in F has a limit.

The field $\mathbb{Q}$ is not complete with respect to $|\cdot|_{\infty}$. This can be seen, for instance, by constructing a rational Cauchy sequence whose limit is $\sqrt{2}$, which is irrational. Then this sequence does not converge in $\mathbb{Q}$. Likewise $\mathbb{Q}$ is not complete with respect to $|\cdot|_p$ for any p. This will be shown later.

The process of completion amounts to adjoining to $\mathbb{Q}$ the set of limits of Cauchy sequences. Canonical sets of representatives for such sequences are the decimal expansion for $|\cdot|_{\infty}$, and their analogue (10) for $|\cdot|_p$.

Let $\mathscr{C}_p$ be the set of all sequences in $\mathbb{Q}$ which are Cauchy with respect to $|\cdot|_p$.

Proposition 11 *Defining*

$$(x_k) + (y_k) = (x_k + y_k) \qquad\qquad (x_k) \times (y_k) = (x_k \times y_k) \tag{11}$$

where $(x_k), (y_k) \in \mathscr{C}_p$, makes $\mathscr{C}_p$ into a commutative ring with identity.

All that needs to be checked is that the sequences on the RHS are Cauchy. The rest is easy.

The set $\mathscr{C}_p$ contains a 'copy' of $\mathbb{Q}$, which is the set of constant sequences of rational numbers. Formally, this means that the map

$$\tau : \mathbb{Q} \to \mathscr{C}_p \qquad\qquad x \mapsto (x,x,x,\ldots)$$

is injective. In particular, the sequences $(0,0,\ldots)$ and $(1,1,\ldots)$ are, respectively, the additive and multiplicative identities of the ring $\mathscr{C}_p$.

We recall some definitions from commutative algebra. An **ideal** in a commutative ring R is an additive subgroup $I \subset R$, which is also closed under multiplication by any ring element, that is

$$\forall r \in R,\ \forall x \in I,\ \ rx \in I.$$

An ideal of the form

$$(x) = xR = \{xr \,:\, r \in R\}$$

is called a **principal ideal.** Thus $R = (1)$. An ideal $I \neq R$ which is not contained in any other ideal different from R is called a **maximal ideal**.

The sum of two ideals is defined naturally, as the (Minkowsky) sum of two sets, namely

$$I + J = \{x + y \,:\, x \in I, y \in J\}.$$

In this context, we use the notation

$$(x,y) = xR + yR.$$

For example, if $R = \mathbb{Z}$, then $(x,y) = x\mathbb{Z} + y\mathbb{Z} = \gcd(x,y)\mathbb{Z}$. (Think about it.)

Regarding a ring R and an ideal I as additive groups, we form the factor group R/I, whose elements are represented by the sets

$$x + I = \{x\} + I = \{x + y \,:\, y \in I\}.$$

Addition and multiplication in R/I are defined as

$$(x+I)+(y+I) = (x+y)+I \qquad\qquad (x+I)(y+I) = xy+I.$$

The importance of maximal ideals stems from the following result.

Theorem 12 *Let R be a commutative ring with identity, and let I be an ideal in R. Then R/I is a field if and only if I is maximal.*

For a proof, see, e.g., [14, chapter 3].

We return to our Cauchy sequences. We define

$$\mathscr{N} = \{(x_k) \in \mathscr{C}_p \,:\, \lim_{k\to\infty} |x_k|_p = 0\}.$$

The set $\mathscr{N}$ is an ideal in $\mathscr{C}_p$, as easily verified from (11).

Theorem 13 *The ideal $\mathscr{N}$ is maximal.*

PROOF. Let $(x_k) \in \mathscr{C}_p \setminus \mathscr{N}$, and let $\mathscr{I} = ((x_k), \mathscr{N})$. We will show that $\mathscr{I} = \mathscr{C}_p$, that is, that $(1) \in \mathscr{I}$.

Since $(x_k) \not\to 0$, then $\exists c > 0$ and N such that $|x_k|_p > c > 0$ for all $k \geqslant N$. In particular, for $k \geqslant N$ we have $x_k \neq 0$, so we define the sequence (y_k) where

$$y_k = \begin{cases} 0 & \text{if} \quad k < N \\ 1/x_k & \text{if} \quad \geqslant N. \end{cases}$$

Next we show that (y_k) is Cauchy. Indeed for $k \geqslant N$, we have

$$|y_{k+1} - y_k|_p = \left| \frac{1}{x_{k+1}} - \frac{1}{x_k} \right|_p = \left| \frac{x_k - x_{k+1}}{x_k x_{k+1}} \right|_p \leqslant \frac{|x_k - x_{k+1}|_p}{c^2} \to 0.$$

Since $|\cdot|$ is non-archimedean, we have, letting $j = k + r > k$

$$\begin{aligned} |y_j - y_k|_p &= |y_{k+r} - y_{k+r-1} + y_{k+r-1} - y_{k+r-2} + \cdots + y_{k+1} - y_k|_p \\ &\leqslant \max(|y_{k+r} - y_{k+r-1}|_p, |y_{k+r-1} - y_{k+r-2}|_p, \ldots, |y_{k+1} - y_k|_p) \to 0 \end{aligned}$$

which establishes the Cauchy property. Now

$$x_k y_k = \begin{cases} 0 & \text{if} \quad k < N \\ 1 & \text{if} \quad k \geqslant N \end{cases}$$

and therefore $(1) - (x_k)(y_k) \in \mathscr{N}$.

This shows the the sequence (1) can be written as a multiple of (x_k) plus an element of $\mathscr{N}$, and hence $(1) \in \mathscr{I}$, as desired. □

We have also proved

Lemma 14 *A rational sequence (y_k) is Cauchy with respect to $|\cdot|_p$ if and only if $|y_{k+1} - y_k|_p \to 0$.*

From theorems 12 and 13, we conclude that the quotient

$$\mathbb{Q}_p = \mathscr{C}_p / \mathscr{N}$$

is a field. This is the **field p-adic numbers**. Thus $\mathbb{Q}_p$ is the set of all equivalence classes of rational sequences which are Cauchy with respect to $|\cdot|_p$, and where the equivalence identifies sequences whose difference converges to zero.

Consider the rational sequence (x_n), where

$$x_n = \sum_{k=n_0}^{n} d_k p^k \qquad d_k \in \{0, 1, \ldots, p-1\}, \quad d_{n_0} \neq 0 \tag{12}$$

and (d_k) is a given sequence. This is a Cauchy sequence, since $|x_{n+1}-x_n|_p \to 0$ (lemma 14), and so we can consider its limit

$$x = \sum_{k=n_0}^{\infty} d_k p^k. \tag{13}$$

Accordingly, we define

$$|x|_p = \lim_{n\to\infty} |x_n|_p = p^{-n_0}. \tag{14}$$

We want to show that every equivalence class in $\mathscr{C}_p$ contains a sequence of the type (13) —an infinite expansion to the base p. It will then follow that (14) defines a non-archimedean absolute value in $\mathbb{Q}_p$. The image of $\mathbb{Q}_p$ under $|\cdot|_p$ is a discrete set of rational numbers:

$$|\mathbb{Q}_p|_p = \{p^n : n \in \mathbb{Z}\}.$$

Such a range of values does not change going from $\mathbb{Q}$ to $\mathbb{Q}_p$.

Lemma 15 *Let $(y_n) \in \mathscr{C}_p \setminus \mathscr{N}$. Then $|y_n|_p$ is eventually stationary.*

PROOF. By assumption, there is $c > 0$ such that $|y_n|_p > c$ for all sufficiently large n, say, $n \geqslant N_1$. There is also N_2 such that $|y_{n+1}-y_n|_p < c$ for all $n \geqslant N_2$. Let $N = \max(N_1, N_2)$. For all $n \geqslant N$ we have

$$|y_n|_p = |y_n - y_{n+1} + y_{n+1}|_p \leqslant \max(|y_n - y_{n+1}|_p, |y_{n+1}|_p) = |y_{n+1}|_p$$
$$|y_{n+1}|_p = |y_{n+1} - y_n + y_n|_p \leqslant \max(|y_{n+1} - y_n|_p, |y_n|_p) = |y_n|_p$$

and so $|y_n|_p \leqslant |y_{n+1}|_p \leqslant |y_n|_p$ giving $|y_{n+1}|_p = |y_n|_p$, as desired. □

Theorem 16 *Every equivalence class in $\mathscr{C}_p$ contains a sequence of the type* (13).

PROOF. Let $(y_n) \in \mathscr{C}_p$. If $(y_n) \in \mathscr{N}$, then $(y_n) \sim (0,0,\ldots)$, which is of the type (13).

Otherwise, let p^{-n_0} be the stationary value of $|y_n|_p$, according to lemma 15. Without loss of generality, we replace (y_n) with a sequence for which $|y_n|_p = p^{-n_0}$, for all n.

Define y'_n via $y_n = p^{n_0} y'_n$, so that $|y_n|_p = 1$. Choose a sub-sequence (z_n) of (y'_n) such that $|z_{n+1} - z_n|_p \leqslant p^{-n}$ for all n. Since $|z_n|_p = 1$, we can choose $d'_0, d'_1, \ldots, d'_n \in \{0,\ldots,p-1\}$ such that $x'_n = \sum_{k=0}^{n} d'_k p^n$ has the property $z_n \equiv x'_n \pmod{p^n}$. The condition $z_n \equiv z'_n \pmod{p^n}$ ensures that there exists d'_{n+1} such that $z_{n+1} \equiv x'_{n+1} \pmod{p^{n+1}}$, and so on. We obtain $(x'_n) \sim (z_n) \sim (y'_n)$, and therefore the sequence (13) with coefficients $d_k = d'_{k+n}$ is equivalent to (y_n). □

Real numbers are often identified with decimal expansions. From theorem 16, we can do an analogous thing with the p-adics, which we identify with the infinite expansion in base p

$$x = \sum_{k=n_0}^{\infty} d_k p^k \qquad d_k \in \{0,\ldots,p-1\}, \quad d_{n_0} \neq 0 \tag{15}$$

with non-archimedean absolute value

$$|x|_p = p^{-n_0}.$$

This representation is *unique*, unlike decimal expansions.

3.2 p-adic integers

The set $\mathbb{Z}_p$ of **p-adic integers** is defined as

$$\mathbb{Z}_p = \left\{x \in \mathbb{Q}_p \,:\, |x|_p \leqslant 1\right\}.$$

Thus $\mathbb{Z}_p$ is the **closed unit disc** in $\mathbb{Q}_p$. Since $|\cdot|_p$ is discrete —its values are the integer powers of p— the set $\mathbb{Z}_p$ is also open, because $|x_n|_p \leqslant 1$ could be replaced by $|x|_p < p$.

The set $\mathbb{Z}_p$ is a **ring**. indeed it contains 0 and 1, it is closed under addition and multiplication (theorem 8) and change of sign (lemma 9 (*iv*)).

The set

$$p\mathbb{Z}_p = \{x \in \mathbb{Q}_p \,:\, |x|_p < 1\}$$

is an **ideal** in $\mathbb{Z}_p$. Indeed it is closed under addition, it contains 0, and if $x \in \mathbb{Z}_p$ and $y \in p\mathbb{Z}_p$, then $xy \in p\mathbb{Z}_p$, since $|xy|_p = |x|_p|y|_p$.

The set

$$\mathbb{Z}_p \smallsetminus p\mathbb{Z}_p = \{x \in \mathbb{Q}_p \,:\, |x|_p = 1\}$$

is the **unit circle**. It consists of the **invertible elements**[2] in $\mathbb{Z}_p$. It follows that any ideal in $\mathbb{Z}_p$ properly containing $\mathbb{Z}_p$ must contain an invertible element, and hence it contains 1, that is, it is $\mathbb{Z}_p$ itself. This shows that $p\mathbb{Z}_p$ is maximal, and hence $\mathbb{Z}_p/p\mathbb{Z}_p$ is a **field**, from theorem 12.

Proposition 17 *The field $\mathbb{Z}_p/p\mathbb{Z}_p$ has p elements.*

PROOF. Among the expressions (15) with $n_0 \geqslant 0$ we identify those that differ by expressions with $n_0 \geqslant 1$. This leaves p possibilities, given by the values of the first digit d_0. □

The following result is known as **Hensel's lemma**

Theorem 18 *Let $f(x)$ be a polynomial with coefficients in $\mathbb{Z}_p$. If there exists a p-adic integer α_1 such that*

$$f(\alpha_1) \equiv 0 \,(\text{mod } p)$$

and its derivative

$$f'(\alpha_1) \not\equiv 0 \,(\text{mod } p),$$

then there exists a unique p-adic integer α such that

$$i) \quad f(\alpha) = 0 \qquad\qquad ii) \quad \alpha \equiv \alpha_1 \,(\text{mod } p).$$

PROOF. We shall construct a Cauchy sequence of integers $\alpha_1, \alpha_2, \ldots$ converging to α, and such that, for all $n \geqslant 1$

$$f(\alpha_n) \equiv 0 \,(\text{mod } p^n) \qquad\qquad \alpha_{n+1} \equiv \alpha_n \,(\text{mod } p^n).$$

This 'coherent' sequence is Cauchy because $|\alpha_{n+1} - \alpha_n|_p \leqslant p^{-n}$ (lemma 14). Also, its limit α will satisfy $f(\alpha) = 0$ (by continuity of f), and $\alpha \equiv \alpha_1 \,(\text{mod } p)$ (by construction).

[2] The invertible elements in a ring are called **units**.

The first term α_1 exists by assumption. To construct α_2 we require (to satisfy *ii*)) that

$$\alpha_2 = \alpha_1 + d_1 p.$$

Substituting and expanding, we get

$$f(\alpha_2) = f(\alpha_1) + f'(\alpha_1) d_1 p + O(p^2)$$

giving the congruence

$$d_1 p f'(\alpha_1) + f(\alpha_1) \equiv 0 \,(\mathrm{mod}\ p^2).$$

Now, $f(\alpha_1) \equiv 0 \,(\mathrm{mod}\ p)$, so that $f(\alpha_1) = p\beta$, for some $\beta \in \mathbb{Z}_p$. After division by p, we obtain

$$d_1 f'(\alpha_1) + \beta \equiv 0 \,(\mathrm{mod}\ p)$$

and hence

$$d_1 \equiv -\beta f'(\alpha_1)^{-1} \,(\mathrm{mod}\ p)$$

which is legitimate since $f'(\alpha_1)$ is invertible modulo p. Exactly the same calculation will work to get α_{n+1} from α_n, as easily checked. □

EXAMPLE. Let $f(x) = x^2 + 1$, and $p = 5$.

$$f(2) = 2^2 + 1 \equiv 0 \,(\mathrm{mod}\ 5) \qquad f'(2) = 2 \cdot 2 \not\equiv 0 \,(\mathrm{mod}\ 5).$$

Because $f(2) \equiv 5 \cdot 1 \,(\mathrm{mod}\ 5^2)$, we have $\beta = 1$ (using the notation introduced in the proof of Hensel's lemma). Thus

$$d_1 \equiv -1 \cdot \frac{1}{4} \equiv -4 \equiv 1 \,(\mathrm{mod}\ 5) \qquad \alpha_2 = 2 + 1 \cdot 5 = 7.$$

Now

$$f(7) = 50 = 2 \cdot 5^2 \,(\mathrm{mod}\ 5^2) \qquad \Rightarrow \qquad \beta = 2$$

and hence

$$d_2 \equiv -2 \cdot \frac{1}{14} \equiv -\frac{1}{7} \equiv -\frac{1}{2} \equiv 2 \,(\mathrm{mod}\ 5) \qquad \alpha_3 = 7 + 2 \cdot 5^2 = 57.$$

We write

$$\alpha = \sqrt{-1} = \sum_{k=0}^{\infty} d_k 5^k.$$

Regarding (d_k) as the sequence of 'digits' of α, we have

$$\sqrt{-1} = .21213423\ldots \qquad \text{in} \quad \mathbb{Q}_5.$$

Let us consider the following approximation to the root $\sqrt{-1}$ of $f(x)$, given by the first five digits

$$\sqrt{-1} \approx 2 + 1 \cdot 5 + 2 \cdot 5^2 + 1 \cdot 5^3 + 3 \cdot 5^4 \equiv 2057 \,(\mathrm{mod}\ 5^5).$$

We find

$$f(2057) = 4231250 = 5^5 \cdot 1354 \equiv 0 \,(\mathrm{mod}\ 5^5).$$

3.3 Sequences and series

We have seen that the elements of $\mathbb{Q}_p$ can be identified with the limits of sequences (x_n) of the type

$$x_n = \sum_{k=n_0}^{n} d_k p^k \qquad d_k \in \{0,1,\ldots,p-1\}, \quad d_{n_0} \neq 0$$

and it is natural to consider infinite sequences and series of elements of $\mathbb{Q}_p$.

We recall that a **metric space** is a set equipped with a **distance function**; in our case this function is given by the absolute value $d_p(x,y) = |x-y|_p$. A metric space is **complete** if every Cauchy sequence converges. The most important fact about analysis on $\mathbb{Q}_p$ is the following.

Theorem 19 *The set $\mathbb{Q}_p$ is a complete metric space.*

For a proof, see [6, section 3.2].

The following result highlights a significant difference between analysis in $\mathbb{R}$ or $\mathbb{C}$ and in $\mathbb{Q}_p$.

Lemma 20 *A sequence (a_n) in $\mathbb{Q}_p$ is Cauchy if and only if*

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

This is a generalisation of lemma 14 given for rational sequences. Its proof can be repeated verbatim for this case. This lemma gives us the following important result:

Corollary 21 *An infinite series in $\mathbb{Q}_p$ converges if and only if its general terms goes to zero.*

PROOF. A series converges if the sequence of partial sums converges. The difference between the nth and the $(n-1)$th partial sums is equal to the nth term of the series. If the latter tends to zero, it follows from lemma 20 that the sequence of partial sums is Cauchy, hence converges. □

The above corollary is plainly false in $\mathbb{R}$ or $\mathbb{C}$, due to the well-know counterexample

$$\sum_{k\geqslant 1} \frac{1}{k}.$$

The general term k^{-1} approaches zero, but the series diverges.

EXAMPLE. The series $\sum_{k\geqslant 0} p^k$ converges in $\mathbb{Q}_p$, since $|p^n|_p \to 0$. For its nth partial sum, we find

$$\sum_{k=0}^{n} p^k = \frac{1-p^{n-1}}{1-p} \to \frac{1}{1-p}.$$

We also obtain

$$-1 = \sum_{k\geqslant 0} (p-1)p^k.$$

So, in $\mathbb{Q}_5$ we have

$$-\frac{1}{4} = \frac{1}{1-5} = 1+5+5^2+5^3+\cdots \qquad -1 = 4+4\cdot 5+4\cdot 5^2+4\cdot 5^3+\cdots.$$

3.4 Exercises

Problem 1. Prove that, for all non-zero rational numbers x and y, we have

i) $v_p(xy) = v_p(x) + v_p(y)$

ii) $v_p(x+y) \geqslant \min(v_p(x), v_p(y))$.

[*To prove the first property, write out the prime factorization of x and y; for the second, factor out common powers of p from the sum.*]

Problem 2. Compute

$$|35|_7, \qquad |12/56|_7, \qquad |2400|_7, \qquad |2400/2401|_7.$$

Problem 3. Let F be a field. Prove that the function

$$|\cdot| : x \mapsto \begin{cases} 1 & \text{if } x \neq 0 \\ 0 & \text{if } x = 0 \end{cases}$$

is an absolute value on F (called the *trivial* absolute value). Prove that, for every prime p, this is the only absolute value that can be defined on $F = \mathbb{Z}/p\mathbb{Z}$.
[*Use lemma 9 and Euler's theorem.*]

Problem 4. Let $d(x,y) = |x-y|_p$. Prove that for all $x, y, z \in \mathbb{Q}$

i) $d(x,y) = 0$ iff $x = y$;

ii) $d(x,y) = d(y,x)$;

iii) $d(x,z) \leqslant \max(d(x,y), d(y,z))$.

Problem 5. Let $x \in \mathbb{Q} \setminus \{0\}$. Then

$$\prod_{p \leqslant \infty} |x|_p = 1$$

where the product is taken over all primes, including the prime at infinity (ordinary absolute value).
[*Begin with x being a positive integer.*]

Problem 6. Decide if the following sequences converge in $\mathbb{Q}_p$, and find the limit of those that do

$$1)\ p^n \qquad 2)\ n! \qquad 3)\ n \qquad 4)\ 1/n \qquad 5)\ (1+p)^{p^n}.$$

Problem 7. Let the radius of convergence ρ of the p-adic power series $\sum_{k\geqslant 0} a_k x^k$ be determined by the equation

$$\rho^{-1} = \limsup \sqrt[n]{|a_n|_p}.$$

Prove that, for the p-adic exponential function

$$\exp(x) = \sum_{k=0}^{\infty} \frac{x^k}{k!}$$

we have $\rho \geqslant p^{-1/(p-1)}$.

Problem 8. Prove that, for any odd prime p, the field $\mathbb{Q}$ is not complete with respect to $|\cdot|_p$, namely there exists a Cauchy sequence of rational numbers that does not converge to a rational number.
[*Choose an integer a such that: a is not a square in $\mathbb{Q}$; a is not divisible by p; a is a square modulo p. (Why does such an integer exist?) Then use Hensel's lemma for the polynomial $x^2 - a$.*]

Problem 9. Same as previous problem, for $p = 2$.
[*Try cube roots.*]

4 Linear dynamics in $\mathbb{Q}_p$

We have seen that the computation of the period of orbits of the linear map

$$f_\omega : \quad x \mapsto \omega x \,(\mathrm{mod}\, m) \qquad \gcd(\omega, m) = 1$$

can be reduced to the case in which

$i)$ the initial condition is co-prime to the modulus;

$ii)$ the modulus is a prime power.

If $m = p^k$ is a prime power, the p-adic formalism developed above will allow us to treat the infinite sequence of maps

$$x \mapsto \omega x \,(\mathrm{mod}\, p^k) \qquad k = 1, 2, \ldots \tag{16}$$

as a single map over $\mathbb{Q}_p$.

The idea is that, by increasing k, we increase the accuracy with which we represent the exact (infinite k) p-adic dynamics. In this perspective, the periodicity observed for any finite k in the map (16), corresponds to orbits that return close to the initial condition, within a distance p^{-k}. If the p-adic motion is not periodic, then the sequence of periods modulo p^k, for increasing k, is a sequence **Poincaré recurrence times**.

We shall generalise the map f_ω to the case in which ω is a p-adic integer, as opposed to an ordinary integer. This generalisation presents no additional difficulty, but brings substantial benefits. Thus we consider the linear map

$$f_\omega : \mathbb{Q}_p \to \mathbb{Q}_p \qquad x \mapsto \omega x \qquad |\omega|_p = 1, \qquad \forall k \in \mathbb{N} \quad \omega^k \neq 1.$$

The last condition (which can be expressed by saying that ω is not a **root of unity**) ensures that the p-adic motions are not periodic. We have

$$|f_\omega(x)|_p = |\omega x|_p = |\omega|_p |x|_p = |x|_p$$

and therefore the absolute value of every point of an orbit is the same. Indeed, all circles in $\mathbb{Q}_p$ centred at 0, namely

$$\{x \in \mathbb{Q}_p \;\; |x|_p = p^n\} \qquad n \in \mathbb{Z}$$

are invariant under f_ω. (In what follows, we shall omit the subscript ω, whenever appropriate.)

Because $|omega|_p = 1$, we have the p-adic expansion

$$\omega = d_0 + d_1 p + d_2 p^2 + \cdots \qquad d_0 \neq 0.$$

Let r be the multiplicative order of ω modulo p, that is,

$$\omega^r \equiv 1 \,(\mathrm{mod}\, p)$$

and r is the smallest positive integer with that property. (This is the same as the multiplicative order of d_0 modulo p.) We define $s \in \mathbb{N}$ and $\beta, \mu \in \mathbb{Z}_p$ via the equations

$$\mu = \omega^r = 1 + p^s\beta \qquad |\beta|_p = 1. \tag{17}$$

To justify the existence and uniqueness of such quantities, we note that, since ω is not a root of unity, then $\omega^r - 1 \neq 0$. To compute s, we consider the equation

$$p^s = \frac{\omega^r - 1}{\beta}$$

and since $|\beta|_p = 1$, we find, taking the absolute value,

$$|p^s|_p = p^{-s} = |\omega^r - 1|_p = p^{-\nu_p(\omega^r - 1)},$$

from which we find that

$$s = \nu_p(\omega^r - 1).$$

By definition of multiplicative order, we know that $\omega^r - 1$ is divisible by p, hence s is a positive integer. Finally

$$|\mu|_p = |\omega^r|_p = |\omega|_p^r = 1.$$

A unit μ with the property that $\mu \equiv 1 \pmod{p}$ is called a **one-unit**.

EXAMPLE. We compute the value of the parameters r, μ, s, β is some cases.

i) Let $p = 5, \omega = 2$; then $r = 4$, and $\mu = 2^4 = 16 = 1 + 3 \cdot 5^1$ so that $s = 1, \beta = 3$.

ii) Let

$$p = 3, \omega = -\frac{1}{2} = 1 + 3 + 3^2 + \cdots = 1 + 3(1 + 3 + 3^2 + \cdots).$$

We find $r = 1, s = 1, \beta = -\frac{1}{2}$.

iii) Let $p = 7$ and $\omega = \sqrt{2}$. Then ω is a root of $f(x) = x^2 - 2$. We find

$$f(3) = 7 \equiv 0 \pmod{7} \qquad f'(3) \not\equiv 0 \pmod{7}.$$

From Hensel's lemma, we know that a root ω of $f(x)$ exists in $\mathbb{Q}_7$, and is determined uniquely by the condition $\omega \equiv 3 \pmod{7}$. Computation gives

$$\omega = .312612\ldots$$

Check:

$$\sqrt{2} \equiv 3 + 1 \cdot 7 + 2 \cdot 7^2 + 6 \cdot 7^3 \equiv 2166 \pmod{7^4} \qquad 2166^2 = 4691556 = 2 + 7^4 \cdot 1954 \equiv 2 \pmod{7^4}.$$

The first digit of ω is $d_1 = 3$, and 3 is a primitive root modulo 7, so $r = 6$. We find $\omega^6 = (\sqrt{2})^6 = 8 = 1 + 7$, so $s = 1, \beta = 1$. Note that if we had chosen the other root of f modulo 7, namely $-3 \equiv 4 \pmod{7}$, we would have obtained different parameter values.

We now determine the period of the orbits of the map f_ω reduced modulo p^k, by considering p-adic approximations. For initial conditions co-prime to p, such a period is equal to the order of ω modulo p^k. This quantity is well-defined, since $|\omega|_p = 1$ implies that any integer in the residue class of ω modulo p^k is co-prime to p. We have

Theorem 22 *Let ω, r and s be as above. Then*

$$\mathrm{ord}_{p^k}(\omega) = \begin{cases} r & \text{if } 1 \leqslant k \leqslant s \\ rp^{k-s} & \text{if } k > s. \end{cases}$$

PROOF. The case $k \leqslant s$ is an immediate consequence of equation (17) and the definition of r. We proceed by induction on $k \geqslant s$, and we have just verified that the base case $k = s$ holds. Assume that our statement is true for some $k \geqslant s$, that is,

$$\omega^{rp^{k-s}} = \mu^{p^{k-s}} = 1 + p^k \beta_k \qquad k \geqslant s$$

where β_k is an appropriate unit.

Let $u = rp^{k-s}$. Then $\mathrm{ord}_{p^{k+1}}(\omega)$ must be a multiple tu of u, for some $t \geqslant 1$ (lest the inductive assumption is violated). The binomial theorem gives

$$\begin{aligned} \omega^{ut} &= \left(1 + p^k\beta_k\right)^t = \sum_{n=0}^{t} \binom{t}{n} p^{nk}\beta_k^n \\ &= 1 + tp^k\beta_k + \frac{t(t-1)}{2} p^{2k}\beta_k^2 + \cdots . \end{aligned}$$

Clearly $v_p\left((p^k\beta_k)^n\right) = nk$. Furthermore for all $n \leqslant t$, we have

$$v_p\left(\binom{t}{n}\right) = \begin{cases} 0 & \text{if } 1 \leqslant t < p \\ 1 & \text{if } t = p \end{cases}$$

and therefore

$$\omega^{ut} \not\equiv 1 \,(\mathrm{mod}\ p^{k+1}) \qquad t = 1, 2, \ldots, p-1.$$

On the other hand, we have

$$\omega^{up} = 1 + p^{k+1}\beta_k + O(p^{2k+1}) = 1 + p^{k+1}\beta_{k+1}$$

where $O(p^{2k-1})$ represents an unspecified element of $p^{2k+1}\mathbb{Z}_p$ and β_{k+1} is a unit. The last two expressions ensure that $\mathrm{ord}_{p^{k+1}}(\omega) = up = rp^{k+1-s}$, completing the induction. □

The dynamical interpretation of theorem 22 is the following. We consider the orbit $x_t = f_\omega^t(x_0)$ of a point $x_0 \in \mathbb{Q}_p$. After r iterates of the map, the point x_r returns, for the first time, in a small neighbourhood of the initial point, a disc of radius p^{-s}. All previous iterates remained at unit distance from x_0. To return to a smaller neighbourhood of x_0, we must iterate the map rp times, whereby the distance from x_0 becomes p^{-s-1} for the first time, etc. At these recurrence times, the corresponding iterate of the map becomes closer and closer to the identity. The orbit never returns exactly to the initial point, because we have assumed that ω is not a root of unity.

EXAMPLE. We have seen that the decimal digits of $1/7$ have period 6. What is the period of the decimals of $1/7^k$ for $k \geqslant 1$?

We have $p = 7, \omega = 10, r = 6$. We compute

$$10^6 = 1 + 7 \cdot 142857 \qquad 142857 = 3^3 \cdot 11 \cdot 13 \cdot 37.$$

So $s = 1$, and $\beta = 142857$. We find $\mathrm{ord}_{7^k}(10) = 6 \cdot 7^{k-1}$, for $k \geqslant 1$.

4.1 One units: recurrence and renormalisation

We are interested in characterising the aperiodic motion of f_ω in greater detail. Recall that a one-unit is a unit which is congruent to 1 modulo p. We will show that the dynamics generated by one-units is regular, in a sense to be made precise below.

We denote by H the set of one-units. Then $H = 1 + p\mathbb{Z}_p$. More generally, we denote by $H_s = 1 + p^s\mathbb{Z}_p$ the set of one-units of **level** $\geqslant s$. Geometrically, H_s is a closed disc of radius p^{-s} centred at 1. Algebraically, H_s is a multiplicative group, since $1 \in H_s$ and

$$(1+p^k\beta)^{-1} = 1 - p^k\beta + p^{2k}\beta^2 + \cdots$$

which shows that the inverse of a one-unit is a one-unit of the same level. Then $\mu \in H_s$ if and only if $z = (\mu - 1)/p^s$ is a p-adic integer. So we define

$$z_t = \frac{\mu^t - 1}{p^s}$$

which yields

$$z_{t+\tau} = \mu^t z_t + z_\tau. \tag{18}$$

Letting $\tau = 1$ in the above formula, we obtain the invertible recursion

$$z_{t+1} = \mu z_t + z_1 \qquad t \geqslant 1. \tag{19}$$

If we let $z_1 = \beta$ (cf. (26)), then the digits of z_t are the digits of ω^{rt} that are not fixed. Thus the map (19) is relevant to our problem if the initial condition z_1 is a unit.

From the discussion above, it follows that the point z_t is periodic modulo p^k with period p^k, so it visits each residue class modulo p^k exactly once. It follows that the orbit (z_t) is not only dense in $\mathbb{Z}_p$, but is also ergodic with respect to the Haar measure. The ergodicity of (19) is associated to a logarithmic problem, namely the solution for t of the equation $z_t = x$. The computation of this logarithm is much simpler that that of the discrete logarithm modulo the prime p, because one can exploit the analytic structure of the p-adic logarithmic function.

From equation (26) it also follows that for the mapping (19) the recurrence times for an orbit to visit a circle of radius p^{-t} about the origin is exactly p^t, and this value is independent from the unit chosen within a given level. This is in sharp contrast with the case of linear maps $x \mapsto \omega x$ over $\mathbb{C}$ (with $|\omega| = 1$, and ω not a root of unity), where recurrence times depend on the continued fractions expansion of the rotational angle being considered.

There is considerable regularity in the dynamics of the map (19). One sees immediately that the evolution of the low-order digits of z is determined by an additive, rather than multiplicative, algorithm. Indeed, if μ is a one-unit of level s, equation (18) becomes

$$z_{t+1} \equiv z_t + z_1 \pmod{p^s}.$$

To see that the motion possesses an overall additive nature, we introduce a renormalisation operator R, acting on maps over $\mathbb{Q}_p$,

$$R(f) = B^{-1} \circ f^p \circ B \tag{20}$$

which involves a p-fold composition with the affine scaling

$$B(x) = px + \overline{x} \qquad \overline{x} \in \mathbb{Q}_p,$$

whose effect is to magnify about the point $\overline{x}$. (The operator R is reminiscent of Feigenbaum's operator.)

The operator R possesses a one-parameter family of fixed point f^*_λ, namely, all translations in $\mathbb{Q}_p$,

$$f^*_\lambda(x) = x + \lambda \qquad R(f^*_\lambda) = f^*_\lambda.$$

We let f act on an affine map f

$$f(x) = \mu x + \gamma \qquad \mu \neq 1. \tag{21}$$

We have

$$\begin{aligned} (Rf)(x) &= \frac{1}{p}[f^p(px+\overline{x}) - \overline{x}] \\ &= \mu^p x + \frac{\mu^p - 1}{p}\left(\frac{\gamma}{\mu - 1} + \overline{x}\right), \end{aligned}$$

showing that the action of R corresponds to the following reparametrisation for f

$$\mu \mapsto \mu^p \qquad \gamma \mapsto \frac{\mu^p - 1}{p}\left(\frac{\gamma}{\mu - 1} + \overline{x}\right).$$

The asymptotics of the orbit of f under R are given by

$$\lim_{n\to\infty}(R^n f)(x) = \lim_{n\to\infty}\mu^{p^n}x + \frac{\mu^{p^n} - 1}{p^n}\left(\frac{\gamma}{\mu - 1} + \overline{x}\frac{1+p^n}{1-p}\right).$$

If μ is a one-unit, then

$$\lim_{n\to\infty}\mu^{p^n} = 1 \qquad \lim_{n\to\infty}\frac{\mu^{p^n} - 1}{p^n} = \log(\mu), \tag{22}$$

where the p-adic logarithmic function $\log(1+x)$ agrees in the open unit disc $|x|_p < 1$ with the sum of the familiar power series

$$\log(1+x) = \sum_{k\geqslant 1}\frac{(-1)^{k+1}x^k}{k}.$$

Noting that $p^n \to 0$, one sees that the second formula in (22) corresponds to the formula

$$\log(x) = \lim_{\varepsilon\to 0}\frac{x^\varepsilon}{\varepsilon}.$$

Thus an affine map f with a one-unit multiplier lies in the stable manifold of a translation f^*_λ. Letting $\gamma = z_1$ in (21), we see that the multiplicative mapping (19) under renormalisation about $\bar{z}$ converges to the translational fixed point of R

$$f(x) = \mu x + \lambda = z + \log(\mu)\left(\frac{1}{p^s} + \frac{\bar{z}}{1-p}\right).$$

We remark that by exploiting the $\mathbb{Z}_p$-module property of the group of one-units, we can interpret the relation $x_t = f^t(x_0)$ for a linear map $f(x) = \mu x$ with the one-unit multiplier μ as a flow with p-adic time. The vector field generated bu this flow is then given by

$$v(x) = \lim_{t\to 0} \frac{f^t(x) - x}{t} = \lim_{t\to 0} \frac{\mu^t - 1}{t} x = \log(\mu)x.$$

In this context, time measures recurrence distances, that is, $|t|_p$ is proportional to $|x_t - x_0|_p$.

4.2 Exercises

Problem 1. For $n \in \mathbb{Z}$, consider the circles, centred at zero.

$$\mathscr{C}_n = \{x \in \mathbb{Q}_p : v_p(x) = n\}$$

Prove that the restriction of f_ω to $\mathscr{C}_n$ is conjugate to the restriction of f to $\mathscr{C}_0$.

Problem 2. Compute the period of the orbit through the point $x = 1$ for the map $x \mapsto \omega x \,(\mathrm{mod}\ p^k)$, $k \geqslant 1$, in the following cases

$$\omega = 4,\ p = 5 \qquad\qquad \omega = 14,\ p = 29.$$

(In the second case, use Maple.)

Problem 3. Let $\omega = 1 + p^s$. Show that any orbits of the map $\mathbb{Q}_p \to \mathbb{Q}_p$, $x \mapsto \omega x$ with initial point x is contained in a disc of radius $|x|_p p^{-s}$ centred at x.

5 Linearisation

Let $f(x)$ be a polynomial with integer coefficients. We let f act on $\mathbb{Z}/p^k\mathbb{Z}$, where p is a prime. Can the dynamics be studied with p-adic methods?

We restrict our attention to motions in the vicinity of a fixed point of f. The latter is a solution of the equation $f(x)=x$, namely a root of the polynomial

$$\Phi(x) = f(x) - x.$$

Assume that Φ has a root a modulo p and that $\Phi'(a) \not\equiv 0 \pmod{p}$. From Hensel's lemma, it follows that Φ has a root θ in $\mathbb{Z}_p$, with $\theta \equiv a \pmod{p}$.

Furthermore, $f(\theta)=\theta$, namely θ is a fixed point of f in $\mathbb{Z}_p$. To study motions near θ, we consider the new variable $z = x - \theta$. We find

$$\begin{aligned} z \mapsto f(x) - \theta &= f(z+\theta) - \theta = f(\theta) + f'(\theta)z + O(z^2) - \theta \\ &= f'(\theta)z + O(z^2). \end{aligned}$$

The map $z \mapsto f'(\theta)z$ is the **linearisation** of the map f near the point θ. The quantity $f'(\theta)$ is called the **multiplier** of f' at θ.

EXAMPLE. Let $p=7$ and $f(x)=x^2+1$. Then $\Phi(x)=x^2-x+1$, and $\Phi'(x)=2x-1$. We find

$$\Phi(x) = (x-3)(x-5) \pmod{7} \qquad \Phi'(3) \equiv 5 \pmod{7}, \quad \Phi'(5) \equiv 2 \pmod{7}.$$

From Hensel's lemma, it follows that Φ has two distinct root $\theta, \overline{\theta}$ in $\mathbb{Z}_7$, with

$$\theta \equiv 3 \pmod{7} \qquad\qquad \overline{\theta} \equiv 5 \pmod{7}.$$

The map in the variable $z = x - \theta$ reads

$$\begin{aligned} z \mapsto f(z+\theta) - \theta &= (z+\theta)^2 + 1 - \theta = 2\theta z + z^2 + \theta^2 - \theta + 1 \\ &= 2\theta z + z^2 + \Phi(\theta) = 2\theta z + z^2 \end{aligned}$$

where we have used the fact the θ is a root of Φ. So the linearisation of f is $z \mapsto 2\theta z$, with multiplier $f'(\theta) = 2\theta$. In particular

$$\begin{aligned} &z \mapsto 6z \pmod{7} \qquad \text{near } \theta \\ &z \mapsto 4z \pmod{7} \qquad \text{near } \overline{\theta}. \end{aligned}$$

Let $f(x) = \omega x + O(x^2)$ be a polynomial with coefficients in $\mathbb{Q}_p$, (or, more generally, a p-adic power series over $\mathbb{Q}_p$, converging in some neighbourhood of the origin) which has a fixed point at 0 with multiplier ω. The linearisation problem is posed as follows: does there exist a smooth change of coordinates that turns f into its linear part?

Specifically, we look for a function $\mathscr{L}:\mathbb{Q}_p\to\mathbb{Q}_p$ which satisfies the equation

$$\mathscr{L}(f(x))=\omega\mathscr{L}(x). \tag{23}$$

This is called **Schröder functional equation**. We require $\mathscr{L}$ to be expressible as a power series, convergent in some non-empty disc about $x=0$, and invertible in some suitable (possibly smaller) disc

$$\mathscr{L}(x)=b_0+b_1x+b_2x^2+\cdots. \tag{24}$$

For the sake of concreteness, we consider the simplest non-trivial case, namely that of a quadratic polynomial over $\mathbb{Z}_p$, with an indifferent fixed point at the origin

$$f(x)=\omega x+ax^2 \qquad |\omega|_p=1.$$

Schröder equation reads

$$\mathscr{L}(\omega x+ax^2)=\sum_{n\geqslant 0}b_n(\omega x+ax^2)^n=\sum_{n\geqslant 0}\omega b_nx^n.$$

Using the binomial theorem, we obtain

$$\sum_{n\geqslant 0}b_n\sum_{k=0}^{n}\binom{n}{k}\omega^ka^{n-k}x^{2n-k}=\sum_{n\geqslant 0}\omega b_nx^n.$$

Equating the coefficients of the same powers of x, we obtain an infinite sequence of equations for the unknown coefficients b_n, to be solved recursively.

Let m denote the power of x under consideration. We obtain

$$\begin{array}{lrcl} m=0: & b_0=\omega b_0 & \Rightarrow & b_0=0 \\ m=1: & \omega b_1=\omega b_1 & \Rightarrow & b_1 \text{ arbitrary.} \end{array}$$

Noting that b_1 is the derivative of $\mathscr{L}$ at 0, for $\mathscr{L}$ to be invertible, we need $b_1\neq 0$. We choose $b_1=1$, for normalisation. Furthermore

$$m=2: \qquad b_1\binom{1}{0}+b_2\binom{2}{2}\omega^2=\omega b_2$$
$$\Rightarrow b_2=-\frac{ab_1}{\omega(\omega-1)}=-\frac{a}{\omega(\omega-1)}.$$

For $m\geqslant 2$ we obtain the recursion

$$b_m\left[\binom{m}{m}\omega^m-\omega\right]=b_m\omega(\omega^{m-1}-1)=-\sum_{n=\lceil m/2\rceil}^{m-1}b_m\binom{n}{2n-m}\omega^{2n-m}a^{m-n}$$

($\lceil\cdot\rceil$ is the ceiling function) which expresses b_m in terms of some coefficients of lower order. The lower bound of summation ensures that $\binom{n}{2n-m}\neq 0$.

Recalling that

$$\left|\binom{n}{k}\right|_p \leqslant 1 \qquad |a|_p \leqslant 1 \qquad |\omega|_p = 1$$

an easy induction shows that

$$|b_m|_p \leqslant \frac{1}{|\mathscr{D}_{m-1}|_p}$$

where

$$\mathscr{D}_m = \prod_{i=1}^{m}(\omega^i - 1). \tag{25}$$

The quantity $\mathscr{D}_m$ appears at denominator of the expression defining b_m. How small is $\mathscr{D}_m$? As we did before, we let r be the order of ω modulo p, and we define the quantities μ, s and β via the equations

$$\mu = \omega^r = 1 + p^s\beta \qquad |\beta|_p = 1. \tag{26}$$

The only term in the product (25) that are smaller than 1 correspond to the values of i that are multiples of r. Letting $n = \lfloor m/r \rfloor$, we obtain

$$\begin{aligned} v_p(\mathscr{D}_m) &= \sum_{j=1}^{n} v_p(\mu^j - 1) \\ &= \sum_{j=1}^{n} v_p(\mu - 1) + \sum_{j=1}^{n} v_p(\mu^{j-1} + \mu^{j-2} + \cdots + 1) \\ &= ns + \sum_{j=1}^{n} v_p(j) \\ &= ns + \sum_{j\geqslant 1} \left\lfloor \frac{n}{p^j} \right\rfloor \leqslant ns + \sum_{j\geqslant 1} \frac{n}{p^j} \\ &= ns + n\frac{1}{p-1} = \left\lfloor \frac{m}{r} \right\rfloor \left(s + \frac{1}{p-1} \right). \end{aligned}$$

Thus $v_p(\mathscr{D}_m)$ is bounded above by a linear function of m. This means that $|\mathscr{D}_m|_p$ decreases no faster than exponentially, and hence $|b_m|_p$ increases no faster than exponentially, that is, the power series (24) has a non-zero radius of convergence. Using standard results on the invertibility of power series, we obtain

Theorem 23 *Let $f(x) = \omega x + ax^2$, with $a, \omega \in \mathbb{Z}_p$ and ω a p-adic unit which is not a root of unity. Then there exists a neighbourhood of the origin where f is conjugate to its linear part.*

This theorem can be generalised to the case of any p-adic function f analytic in a neighbourhood of the origin. The region surrounding an indifferent fixed point where the motion is conjugate to a rotation is called a p-adic **Siegel disc.** Siegel proved the existence of such discs for analytic maps over $\mathscr{C}$, where the question of convergence of the conjugacy function $\mathscr{L}$ is considerably more difficult.

5.1 Conjugacy and the logarithm

We consider the following one-parameter family of nonlinear maps

$$f_\theta(x) = (1+x)^\theta - 1 \qquad \theta \in \mathbb{Z}_p. \tag{27}$$

These maps illustrate clearly the main features of regular motions over the p-adics. These are the endomorphisms of the so-called multiplicative formal group, which in the specialised literature are usually denoted by $[\theta](x)$[8].

We are interested in the dynamics of these endomorphisms, over algebraic extensions K of $\mathbb{Q}_p$. If $\theta \in \mathbb{Z}$, then f_θ is defined over the whole of K, but if one restricts x to the domain $|x|_p < 1$ (the maximal ideal), then the exponent can be allowed to be an element of $\mathbb{Z}_p$, which is the case of interest to number theorists. Whenever we apply f_θ outside the maximal ideal, it will be understood that θ is a rational integer.

The study of f_θ illustrates the dynamical significance of the p-adic logarithmic and exponential functions, which provide analytic conjugacies to Siegel discs. These maps also exemplify the most salient dynamical features of the so-called **endomorphisms of formal groups**, which we briefly describe in the next section.

From (27), we obtain

$$\begin{aligned} f_\theta(f_\phi(x)) &= f_\theta((1+x)^\phi - 1) \\ &= (1+x)^{\theta\phi} - 1 = f_{\theta\phi}(x), \end{aligned}$$

that is, all elements of the family commute. In particular

$$f_\theta^t(x) = f_{\theta^t}(x),$$

which is valid for rational integers t, and if θ is a one-unit, then t may be taken to be any p-adic integer. Thus if x^* is a fixed point of f_θ, so is $f_\phi(x^*)$, and since the number of fixed points of f_θ is finite, x^* is also (pre)-periodic for f_ϕ.

The derivative (multiplier) of the map is given by

$$f_\theta'(x) = \theta(1+x)^{\theta-1}. \tag{28}$$

The periodic orbits of period dividing t are roots of the polynomial

$$\Phi_t(x) = f_{\theta^t}(x) - x = (1+x)\left[(1+x)^{\theta^t-1} - 1\right] \tag{29}$$

The first factor of Φ_t yields a fixed point at $x = -1$, which is superstable (the multiplier is equal to zero), and independent of θ.

Its basin of attraction is the set of x for which

$$\lim_{t\to\infty} f_\theta^t(x) + 1 = \lim_{t\to\infty}(1+x)^{\theta^t} = 0,$$

which implies $|1+x|_p < 1$, that is, the basin is the open unit disc centred at $x = -1$.

The second factor of (29) yields a fixed point at the origin, with multiplier θ, as well as infinitely many cycles x^* with the property that $1+x^*$ are the $(\theta^t - 1)$th roots of unity. Motions near these periodic points are the same as near the origin, apart from a linear scaling. Indeed let $x^* \neq 0, -1$ be a periodic point of minimal period t, and let $\eta = 1+x^*$. From (28) and (29), we find for the kth derivative

$$f_{\theta^t}^{(k)}(0) = f_{\theta^t}^{(k)}(x^*)\eta^{k-1} \qquad k \geqslant 1$$

so that, in terms of the local coordinate $y = x - x^*$ we have the linear conjugacy

$$\frac{1}{\eta} f_{\theta^t}(y\eta) = f_{\theta^t}(x), \tag{30}$$

which preserves the metric since $|\eta|_p = 1$. In particular, the multiplier of a t-cycle is the same as that at the origin, and therefore these periodic orbits are either all attractive, if θ is divisible by p, or indifferent, if θ is co-prime to p. (Here we exclude the trivial case $\theta = \pm 1$.)

In the former case the basin of attraction of the origin is the set of x for which

$$\lim_{t\to\infty} f_\theta^t = 0 \qquad \text{or} \qquad \lim_{t\to\infty} (1+x)^{\theta^t} = 1.$$

We have $\varepsilon = \theta^t \to 0$, p-adically, and the basin includes the open unit disc, because if ε is a p-adic integer, then the binomial theorem is valid in that domain, and $\binom{\varepsilon}{k}$ goes to zero with ε.

On the other hand, the basin of the origin cannot include the unit circle, because of the presence non only of the superstable cycle there, but also of the other roots of unity. The latter are attractive, and, by the conjugacy (30), have basins of the same size as that at the origin. Note that in this case all periodic points belong to the subgroup G of E, and the one-units H are all attracted to the origin. In particular, the p-power roots of unity are eventually fixed, that is, they reach the origin in a finite number of iterations.

If the map is invertible, that is, if θ is not divisible by p, then all cycles (apart from the superstable one) are surrounded by a Siegel disc, meaning that the map is analytically conjugate to its linear part in a neighbourhood of each cycle. The size of a disc is the maximal domain where the conjugacy function has an analytic inverse. It is sufficient to construct the Siegel disc at the origin. Conjugating f_θ to its linear part (which is just θx) amounts to solving Schröder functional equation (cf. 23)

$$\mathscr{L}(f_\theta(x)) = \theta \mathscr{L}(x) \tag{31}$$

for $\mathscr{L}$ analytic of the form

$$\mathscr{L}(x) = \sum_{k \geqslant 0} c_k x^k \tag{32}$$

which has solution

$$\mathscr{L}(x) = \log(1+x)$$

independently from θ. This solution is unique if we require that $\mathscr{L}(0) = 1$ and $l'(0) = 1$. The series (32) defining the p-adic logarithm converges in the open unit disc, and the superstable attractor at $x = -1$ gives a dynamical system justification for the exclusion of the unit circle from the domain of convergence.

On the other hand, the actual radius of the disc is somewhat smaller, for the inverse of the conjugacy function $\mathscr{L}$ —the exponential function— converges only over the smaller domain $\nu(x) > (p-1)^{-1}$. The dynamical reason for this phenomenon is that the disc at the origin must exclude the remaining periodic points, which now lie inside the maximal ideal (the numbers $1+x^*$ are one-units), each surrounded by its own disc, according to (30).

Dynamically speaking, the convergence of logarithmic series in a region which includes other discs depends on the concomitance of two facts. First, the logarithm vanishes at the centre of secondary discs, thereby mapping them into the primary one. Second, all discs have the same multiplier, which must be the case, as seen by differentiating (31) and noting that the derivative of the logarithm does not vanish in the secondary discs.

5.2 Remarks on endomorphisms of formal groups

The main features of the phase portrait of the map f_θ described in section 5.1 are shared by automorphisms of more general groups, which we describe informally in this section. We shall in no way attempt to do justice to such a vast realm of number theory, we merely explain some key concepts using the language of dynamics. We refer the reader to [9] for an advanced text.

A one-parameter **formal group** is given by a formal power series F in two indeterminates, over a ring R, with no constant term, and with unit linear coefficients

$$F(x,y) = x+y+\cdots$$

representing the group law. For this to be a group, we must have associativity

$$F(x,F(y,z)) = F(F(x,y),z),$$

and x must have a formal inverse $\iota(x)$:

$$F(x,\iota(x)) = F(\iota(x),x) = 0.$$

We take the ring R to be the ring of integers is some finite extension of $\mathbb{Q}_p$.

An **endomorphism** of F is a formal power series f without constant coefficient, which respects the group law, namely

$$f(F(x,y) = F(f(x),f(y)) \qquad f(x) = \omega x+\cdots.$$

The existence of endomorphisms is ensured by the commutativity of F, and they are parametrised by the coefficient ω.

Dynamically speaking, and endomorphism of a formal group is (in its domain of convergence) a nonlinear mapping with a fixed point at the origin, with multiplier ω. In our example (27), the mappings f_θ are the endomorphisms of the formal multiplicative group

$$F(x,y) = x+y+xy$$

which mimics the law of multiplication of one-units

$$(1+x)(1+y) = 1+x+y+xy = 1+F(x,y)$$

for x and y in the maximal ideal.

The **logarithm** L of a formal group is a formal power series $L(x) = x+\cdots$ that turns the group law into addition

$$L(F(x,y)) = L(x)+L(y).$$

The term-by-term construction of the logarithm yields a power series with coefficients in the field of fraction s of the ring A, which can be shown to converge in the entire maximal ideal.

For any endomorphism f of F one has

$$L(f(x)) = f'(0)L(x) = \omega L(x) \tag{33}$$

which conjugates the mapping f to its linearisation about the origin. Thus if f is an automorphism, then the logarithm of a formal group serves as a conjugacy function to a Siegel disc. If F is the multiplicative group, we have seen that $L(x) = \log(1+x)$.

It can be shown that the logarithm L of a formal group vanishes at all periodic points within the maximal ideal, and has non-vanishing derivative there. So one always has the same phase portrait as in multiplicative case, with full tiling by isochronous Siegel discs. In particular, the size of the disc at the origin is determined by the domain of convergence of L^{-1}, which is smaller than that of L, since the disc cannot include other periodic points.

5.3 Exercises

Problem 1. Let $f(x) = x^2 - x + 2$. Find the fixed points of f in $\mathbb{Z}_5$, with three digits accuracy. By computing the corresponding multipliers, determine the nature of such fixed points.

Problem 2. Let $f(x) = \omega x + ax^2$, with $a, \omega \in \mathbb{Z}_p$. Extend theorem 23 to the case $|\omega|_p < 1$.

6 An application: planar rotations with round-off errors

A planar rotation is a mapping of the type

$$F:\mathbb{R}^2\to\mathbb{R}^2 \qquad \begin{pmatrix}x\\y\end{pmatrix}\mapsto\begin{pmatrix}\cos(2\pi\nu) & -\sin(2\pi\nu)\\ \sin(2\pi\nu) & \cos(2\pi\nu)\end{pmatrix}\begin{pmatrix}x\\y\end{pmatrix} \qquad \nu\in[0,1) \tag{34}$$

describing an anticlockwise rotation by an angle $2\pi\nu$. The quantity ν is called the **rotation number**. The rotation is said to be rational (irrational), if ν is rational (irrational).

In the irrational case —the one we are interested in— all orbits of F, apart from the origin, are non-periodic and dense on circles centred at the origin.

Let us consider the matrix

$$A=\begin{pmatrix}\lambda & -1\\ 1 & 0\end{pmatrix} \qquad \lambda=2\cos(2\pi\nu). \tag{35}$$

Denoting by J the matrix appearing in (34), and letting

$$C=\begin{pmatrix}1 & -\cos(2\pi\nu)\\ 0 & \sin(2\pi\nu)\end{pmatrix}$$

one verifies that $CA=JC$. This means that C induces a semi-conjugacy between J and A. Because $\det(C)=\sin(2\pi\nu)$, we have

$$A=C^{-1}JC \qquad \nu\neq 0,\frac{1}{2}.$$

This equation shows that, apart from two trivial cases, the dynamics induced by J and by A are **conjugate**, that is, they have the same orbit structure. The invariant sets of A are the ellipses

$$x^2-\lambda xy+y^2=const.$$

We shall use the following result

Lemma 24 *Let $\lambda=2\cos(2\pi\nu)$, where ν is a real number. If λ is rational, but not an integer, then ν is irrational.*

The proof requires some knowledge of the arithmetic of roots of unity, and it will be omitted (see, e.g., [10, chapter 3]).

We shall now perturb the linear mapping defined by the matrix (35), by discretising the space. Our aim is to model the effects of space discretisation that is present in a computer representation of a dynamical system. Because the linear motion is regular, it will be possible to isolate the irregular fluctuations that appear when the space is discrete. We remark that these phenomena, still far from understood, have attracted the interest of dynamicists for a long time [12].

We consider the following lattice map

$$\Psi=\mathbb{Z}^2\to\mathbb{Z}^2 \qquad (x,y)\mapsto(\lfloor\lambda x\rfloor-y,x) \qquad \lambda=2\cos(2\pi\nu) \tag{36}$$

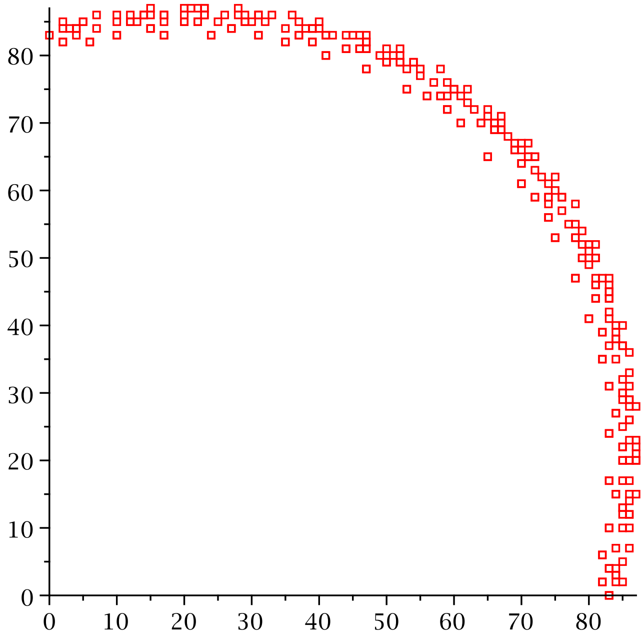

Figure 2: A portion of a periodic orbit of the map Ψ, for $\lambda = 1/2$. The period is 696.

where $\lfloor \cdot \rfloor$ denotes the floor function. Without the floor function, this mapping reduces to the action of the matrix A.

Letting $\Psi(x,y) = (x',y')$, we find

$$(x,y) = (y', \lfloor \lambda y' \rfloor - x')$$

that is, the mapping Ψ is invertible. It follows that the orbits of Ψ are either periodic, or they escape to infinity in both time directions. In this model the discretisation length —the spacing beween lattice points— is fixed, and the limit of vanishing discretisation corresponds to motions at infinity.

We consider the following family of parameter values

$$\lambda = \frac{q}{p^n} \qquad \gcd(q,p) = 1, \quad |q| \leqslant 2p^n, \quad n \geqslant 1.$$

From (36) and lemma 24, we conclude that the corresponding values of the rotation number μ are irrational. An orbit of the map Ψ for the parameter $\lambda = 1/2$ is shown in figure 2. This orbit is periodic, and consists of an irregular set of points arranged along an ellipse.

Let us consider the polynomial $f(x) = x^2 - qx + p^{2n}$. We find

$$f(x) \equiv x(x-q) \,(\mathrm{mod}\ p^{2n}) \qquad f'(x) = 2x - q.$$

Thus

$$f(0) = f(q) \equiv 0 \,(\mathrm{mod}\ p^{2n}), \qquad f'(0) \equiv -q \,(\mathrm{mod}\ p^{2n}), \qquad f'(q) \equiv q \,(\mathrm{mod}\ p^{2n}).$$

Since p and q are co-prime, the polynomial f has two distinct rots modulo p, with non-zero derivative. From Hensel's lemma, it follows that f has two distinct roots $\theta, \bar{\theta}$ in $\mathbb{Z}_p$, where

$$\theta \equiv 0 \,(\mathrm{mod}\; p^{2n}) \qquad \bar{\theta} \equiv q \,(\mathrm{mod}\; p^{2n}). \tag{37}$$

We have (see exercises)

$$|\theta|_p = \frac{1}{p^{2n}} \qquad |\bar{\theta}|_p = 1.$$

Using Newton's method with initial condition $\theta = 0$ (see equation (37)), we find (see exercises)

$$\theta = \frac{p^{2n}}{q} + \frac{p^{4n}}{q^3} + 2\frac{p^{6n}}{q^5} + \cdots$$

and hence

$$\frac{\theta}{p^n} = \frac{p^n}{q} + O(p^{2n}). \tag{38}$$

We shall embed the round-off map (36) in the ring $\mathbb{Z}_p$ of p-adic integers. Considering that $\theta/p^n \in p^n\mathbb{Z}_p$, from (38), we define the map

$$\mathscr{L} : \mathbb{Z}^2 \to \mathbb{Z}_p \qquad (x,y) \mapsto x - y\frac{\theta}{p^n}. \tag{39}$$

Because $\theta \notin \mathbb{Q}$, being the root of the quadratic irreducible polynomial f, the map $\mathscr{L}$ is *injective*. The image under $\mathscr{L}$ of the lattice $\mathbb{Z}^2$, namely the set

$$\mathscr{Z} = \mathscr{L}(\mathbb{Z}^2) \subset \mathbb{Z}_p$$

is an additive subgroup of the p-adic integers.

We now define the map

$$\Psi^* : \mathscr{Z} \to \mathscr{Z} \qquad \Psi^* = \mathscr{L} \circ \Psi \circ \mathscr{L} \tag{40}$$

which is conjugate to Ψ on $\mathscr{Z}$. For the purpose of characterising the map Ψ^*, we first define the **shift mapping σ** on $\mathbb{Z}_p$. Given a p-adic integer z

$$z = b_0 + b_1 p + b_2 p^2 + \cdots \qquad b_k \in \{0, 1, \ldots, p-1\}$$

we let

$$\sigma(z) = b_1 + b_2 p + b_3 p^3 \cdots. \tag{41}$$

This is a smooth expansive map, with a dense set of periodic points. It preserves the standard probability measure on $\mathbb{Z}_p$ (the additive Haar measure), obtained by assigning to the residue class $z\,(\mathrm{mod}\; p^k)$ the measure p^{-k}.

Furthermore, given $x \in \mathbb{Z}$, we define the integer $c(x)$ via the equation

$$\frac{qx - c(x)}{p^n} = \left\lfloor \frac{qx}{p^n} \right\rfloor. \tag{42}$$

We shall prove the following.

Theorem 25 *The mapping Ψ^* can be extended continuously to the whole of $\mathbb{Z}_p$, giving*

$$\Psi^* : \mathbb{Z}_p \to \mathbb{Z}_p \qquad z \mapsto \sigma^n(\bar{\theta} z)$$

where $\bar{\theta}$ is the p-adic unit given in (37), and σ is the shift mapping (41).

PROOF. Because θ and $\bar{\theta}$ are roots of f, we have

$$\theta + \bar{\theta} = q \qquad \theta\bar{\theta} = p^{2n}.$$

Let $z = \mathscr{L}(x,y) = x - y\frac{\theta}{p^n}$. We compute

$$\begin{aligned} \Phi^*(z) &= \mathscr{L}\left(\left\lfloor \frac{qx}{p^n} \right\rfloor - y, x\right) = \left\lfloor \frac{qx}{p^n} \right\rfloor - y - \frac{\theta}{p^n} \\ &= \frac{1}{p^n}\left(x(q-\theta) - p^n y - c(x)\right) = \frac{1}{p^n}\left(x\bar{\theta} - \frac{\theta\bar{\theta}}{p^n} y - c(x)\right) \\ &= \frac{1}{p^n}(\bar{\theta} z - c(x)). \end{aligned}$$

From equation (38), we find that $y\theta/p^n = O(p^n)$. Thus

$$qx \equiv qz \equiv \bar{\theta} z \,(\text{mod } p^n)$$

which shows that

$$\Psi^*(z) = \sigma^n(\bar{\theta} z).$$

Now, if $z^{(k)} \to z$ is a Cauchy sequence in $\mathscr{X}$, then so is $\sigma^n(\bar{\theta} z^{(k)})$, and since $\mathscr{X}$ is dense in $\mathbb{Z}_p$, we can extend Ψ^* to the whole of $\mathbb{Z}_p$. □

The theorem above shows that the round-off mapping Ψ is conjugate to a restriction to a dense set of an expanding map Ψ^* over the p-adic integers.

Thus, in a sense, the round-off errors in the model (36) are a manifestation of p-adic chaos!

6.1 Exercises

Let $f(x) = x^2 - qx + p^{2n}$, where p is a prime number, q is co-prime to p, and n is a positive integer. Let $\theta, \bar{\theta}$ be the roots of f in $\mathbb{Q}_p$, with $\theta \equiv 0 \,(\text{mod } p)$, and $\bar{\theta} \equiv q \,(\text{mod } p)$.

Problem 1. Prove that

$$|\theta|_p = \frac{1}{p^n} \qquad\qquad |\bar{\theta}|_p = 1.$$

Problem 2. Using Newton's method, show that

$$\theta = \frac{p^{2n}}{q} + \frac{p^{4n}}{q^3} + 2\frac{p^{6n}}{q^5} + 5\frac{p^{8n}}{q^7} + \cdots.$$

Obtain a similar expansion for $\bar{\theta}$.

Problem 3. Let $q = 1, p = 2, n = 1$. By iterating Newton's method, show that

$$\theta \equiv 56724 \pmod{2^{16}}$$

and hence obtain the 2-adic expansion

$$\theta = .0010100110111011\ldots.$$

Problem 4.

(This exercise requires knowledge of algebraic number theory.)

Let λ be a root of f. Show that in the ring $\mathbb{Z}[\lambda]$, the ideal (p) splits into the product of two distinct prime ideals: $(p) = P\overline{P}$. Hence show that, for all positive integers k, the ideal P^k has the $\mathbb{Z}$-basis

$$P^k = [p^k, s_k - \lambda] \qquad \text{with} \qquad s_k \equiv \theta \pmod{p^k}$$

where P and λ are paired via the congruence $\lambda \equiv 0 \pmod{P}$.

7 Solutions to exercises

7.1 Section 1

Solution 1:

If all orbits are periodic, then each point has a single pre-image, thence f is invertible. Conversely, let x be non-periodic. Then there exist positive integers $t_1 < t_2$, such that $f^{t_1}(x) = f^{t_2}(x)$. Assume that t_2 (hence also t_1) is minimal. The points

$$f^{t_1-1}(x) \qquad f^{t_2-1}(x)$$

map to the same point. By the minimality of t_2, they are distinct (think about it), hence f is non-invertible.

Solution 2:

The sufficiency of both statements follows from the fact that the rationals with denominator q in the unit interval I are a finite set, which is left invariant by f_ω. Furthermore, if ω is co-prime to q, then the restriction of f_ω to this set is invertible, giving periodicity.

Conversely, let $x \in I$ be eventually periodic. Then the digits d_k in base ω are eventually repeating. Without loss of generality, we may assume that the fractional part of x is purely periodic:

$$x = 0.\overline{d_1 \cdots d_n}. \tag{43}$$

(Any real number may be reduced to this form by first multiplying by a power of ω and then subtracting an integer, and neither operation affects the property of having repeated digits.) We define the integer

$$D = \sum_{k=1}^{n} d_k \omega^{n-k}.$$

From equation (43), we find

$$\begin{aligned} x &= \frac{D}{\omega^n} + \frac{D}{\omega^{2n}} + \frac{D}{\omega^{3n}} + \cdots = D \sum_{k=1}^{\infty} \left(\frac{1}{\omega^n} \right)^k \\ &= \frac{D}{\omega^n - 1}. \end{aligned}$$

We see that x is rational. $\square$

Solution 3:

(a)

$$0011, 0001, 0111.$$

There are 2^6 binary strings of length 6. Of those, 2^3 have minimal period 3 or 1, which must be subtracted. Furthermore 2^2 strings have minimal period 2 or 1, which must also be subtracted, except that in doing so we subtract the 1-strings twice. Thus the total number of strings of minimal period 6 is

$$2^6 - 2^3 - 2^2 + 2^1 = 64 - 8 - 4 + 2 = 54.$$

The total number of *orbits* is then given by $54/6 = 9$.

(b) Let $x_0 = 1/51$. The numerators of the points in the orbits are

$$1, 2, 4, 8, 16, 32, 13, 26, 1, \ldots$$

So the orbit has period 8. We partition the unit interval into four sub-intervals

$$I_k = \big[(k-1)/4, k/4\big) \quad k = 1, \ldots, 4 \qquad\qquad \bigcap_{k=1}^{4} I_k = [0, 1).$$

We have (referring to numerators only)

$$\{1, 2, 4, 8\} \in I_1 \qquad \{13, 16\} \in I_2 \qquad \{26, 32\} \in I_3.$$

So for $x \in I_k$, the density $\rho(x)$ is equal to the relative number of points in I_k divided by the measure of I_k (which is $1/4$)

$$\rho(x) = \begin{cases} 2 & x \in I_1 \\ 1 & x \in I_2 \\ 1 & x \in I_3 \\ 0 & x \in I_4 \end{cases} \qquad\qquad \int_0^1 \rho(x)\, dx = 1.$$

Likewise, if $x_0 = 1/13$ we find

$$1, 2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7$$

so the period is 12. This time the density is uniform

$$\rho(x) = 1.$$

(c)

$$x_0 = 0.\overline{0000111100101101} = 259/4369.$$

The string above contains all 4-substrings. (There is more than one orbit with this feature.)

Solution 4:

(a) We have

$$x_0 = 0.\overline{001} = \frac{1}{2^3} + \frac{1}{2^6} + \frac{1}{2^9} + \cdots = \sum_{k=1}^{\infty} \frac{1}{8} = \frac{1}{7}.$$

Then

$$x_1 \equiv 2x_0 \,(\mathrm{mod}\ 1) = \frac{2}{7} \qquad\qquad x_2 \equiv 2x_1 \,(\mathrm{mod}\ 1) = \frac{4}{7}.$$

(b) We have

$$\begin{aligned} x_0 &= 0.\overline{001101} = 0.\overline{000001} + 0.\overline{000100} + 0.\overline{001000} \\ &= 0.\overline{000001}\,(1+4+8) \\ &= 13\sum_{k=1}^{\infty}\left(\frac{1}{2^6}\right)^k = \frac{13}{63}. \end{aligned}$$

Iterating the map, we find

$$x_0 = \frac{13}{63}, \qquad x_1 = \frac{26}{63}, \qquad x_2 = \frac{52}{63}, \qquad x_3 = \frac{41}{63}, \qquad x_4 = \frac{19}{63}, \qquad x_5 = \frac{38}{63}.$$

7.2 Section 2

Solution 1:

(a) $512 = 2^9$
$\phi(2^9) = 2^8(2-1) = 2^8 = 256$

(b) $1155 = 3 \cdot 5 \cdot 7 \cdot 11$
$\phi(1155) = (3-1) \cdot (5-1) \cdot (7-1) \cdot (11-1) = 2 \cdot 6 \cdot 10 = 480$

(c) $10! = 2^8 \cdot 3^4 \cdot 5^2 \cdot 7$
$\phi(10!) = 2^7 \cdot (2-1) \cdot 3^3 \cdot (3-1) \cdot 5 \cdot (5-1) \cdot (7-1) = 829440$

Solution 2:

The map f has just two orbits precisely when m is prime, and ω is a primitive root modulo m.

(a) $m = 13$: $\phi(m) = 12$, so possible orders are $1, 2, 3, 4, 6, 12$. We have, modulo 13

$$2^2 \equiv 4; \qquad 2^3 \equiv 8; \qquad 2^4 \equiv 3; \qquad 2^6 \equiv 4 \cdot 3 \equiv -1.$$

So 2 has order 12, i.e., it is a primitive root. We have $\phi(12) = 4$, and a reduced residue system modulo 12 is $\{1, 5, 7, 11\}$. So the primitive roots are

$$2^1 \equiv 2; \qquad 2^5 \equiv 6; \qquad 2^7 \equiv -2 \equiv 11; \qquad 2^{11} \equiv 2^{-1} \equiv 7.$$

The desired values of ω are the integers congruent to the above ones.

(b) $m = 23$: $\phi(m) = 22$, so possible orders are $1, 2, 11, 22$. We have, modulo 23

$$2^2 \equiv 4; \qquad 2^3 \equiv 8; \qquad 2^4 \equiv 17 \equiv -7; \qquad 2^8 \equiv 49 \equiv 3; \qquad 2^{11} \equiv 3 \cdot 8 \equiv 1$$

So $\text{ord}_{23}(2) = 11$. Moreover, because $3 \equiv 2^8 \pmod{23}$, and $4 \equiv 2^2 \pmod{23}$, the order of both 3 and 4 is a divisor of that of 2, so 3 and 4 cannot be primitive roots. Try 5:

$$5^2 \equiv 2; \qquad 5^3 \equiv 10; \qquad 5^4 \equiv 4; \qquad 5^8 \equiv 4^4 \equiv -7; \qquad 5^{11} \equiv -70 \equiv -1$$

So 5 has order 22, and is a primitive root. We have $\phi(22) = 10$, and a reduced residue system modulo 22 is $\{1, 3, 5, 7, 9, 13, 15, 17, 19, 21\}$. So the primitive roots are

$$5^1 \equiv 5; \qquad 5^3 \equiv 10; \qquad 5^5 \equiv 20; \qquad 5^7 \equiv 17; \qquad 5^9 \equiv 11;$$

$$5^{13} \equiv 21; \qquad 5^{15} \equiv 19; \qquad 5^{17} \equiv 15; \qquad 5^{19} \equiv 7; \qquad 5^{21} \equiv 14.$$

The desired values of ω are the integers congruent to the above ones.

Solution 3:

From the previous problem we see that 13 is not a primitive root modulo 23, so its order is $1,2$ or 11. The order is not 1 and moreover $13^2 \equiv 8 \pmod{23}$. So the order of 13 is 11, whence $13^{-1} \equiv 13^{10} \pmod{23}$. We find, modulo 23

$$13^2 \equiv 8 \qquad 13^4 \equiv 64 \equiv -5 \qquad 13^5 \equiv -65 \equiv 4 \qquad 13^{10} \equiv 16 \equiv -7.$$

Solution 4:

The periodic point equation reads

$$(\omega^t - 1)x \equiv 0 \pmod{m}$$

where x is the initial condition. For every divisor d of m, consider the initial condition $x = dx'$, with x' co-prime to m. Simplification gives the congruence

$$\omega^t \equiv 1 \pmod{m/d}$$

and there are no other congruences. So the possible periods are the possible values of the order of ω modulo m/d (which exists, because ω and m are co-prime). If m is prime, then m has two divisors, and if $\omega \not\equiv 1 \pmod{m}$ then there are two periods, so the bound is sharp.

Solution 5:

Consider the quantities

$$s = \max_{k\in\mathbb{N}} \gcd(\omega^{k-1}, m) \qquad t = \phi(m/s)$$

and then let l be the smallest value of $k \in \mathbb{N}$ such that $\gcd(\omega^{k-1}, m) = s$. Consider the initial point $x = 1$. The first periodic point in the orbit of 1 is $x_0 = f^l(1)$, so this orbit has transient length l. Transients cannot be longer (think about it). The maximal period is t, which happens when ω is a primitive root modulo m/s.

Solution 6:

Let $t_1 = \mathrm{ord}_{m_1}(\omega)$, $t_2 = \mathrm{ord}_{m_2}(\omega)$, $s = \mathrm{lcm}(t_1, t_2)$. Then, for $i = 1,2$, s/t_i is an integer, and

$$\omega^s = \omega^{t_i} s/t_i \equiv (1)^{s/t_i} \pmod{m_i}.$$

Thus $\omega^s - 1$ is divisible by the integers m_1 and m_2, and hence by their product (because they are co-prime). It follows that s is a multiple of $\mathrm{ord}_{m_1 m_2}(\omega)$ (proposition 2.7 (i)). If $t < s$, then we cannot have $\omega^t - 1 \equiv 0 \pmod{m_1 m_2}$. Indeed if this were true, if we divide t by t_i $(i = 1,2)$, for at least one value of i we would get non-zero remainder $r_i < t_i$. The congruence $\omega^{r_i} \equiv 1 \pmod{m_i}$ would then contradict the definition of order (think about it).

Solution 7:

Let g be a primitive root modulo p. The squares modulo p correspond to the even powers of g. Thus

$$\prod_{t=1}^{(p-1)/2} g^{2t} = g^T$$

where

$$T = 2\sum_{t=1}^{(p-1)/2} t = \frac{p-1}{2}\frac{p+1}{2}.$$

Thus

$$\prod_{t=1}^{(p-1)/2} g^{2t} = \left(g^{(p-1)/2}\right)^{(p+1)/2} \equiv (-1)^{(p+1)/2} \pmod{p}.$$

Solution 8:

Let $q = 4p+1$, with p and q primes. We note that:

i) p is odd.

ii) There are $\phi(q) = q-1 = 4p$ reduced residue classes modulo q.

iii) The number of primitive roots is (from *i*) and *ii*)) $\phi(q-1) = \phi(4p) = \phi(4)\phi(p) = 2(p-1) = 2p-2$.

iv) Because $q \equiv 5 \pmod{8}$, 2 is a quadratic non-residue modulo q, from quadratic reciprocity.

Now, a primitive root is a non-residue, and from *ii*) the number of non-residues is $\phi(q)/2 = 2p$. From *iii*) it then follows that all but two non-residues are primitive roots.

Next we identify these two non-residues. Let g be a primitive root modulo q, and let a be an integer co-prime to q. Then $g^t = a$, for some t, and therefore

$$\left(\frac{a}{q}\right) = \left(\frac{g^t}{q}\right) = \left(\frac{g}{q}\right)^t = (-1)^t. \tag{1}$$

The possible orders modulo q are the divisors of $q-1 = 4p$, namely: $1, 2, 4, p, 2p, 4p$. We examine the elements of order 4. There are $\phi(4) = 2$ of them, and let a be one of them. The corresponding exponent t in (1) is a solution to the congruence

$$\gcd(4, 4p)t = 4t \equiv 0 \pmod{4p} \quad \Longrightarrow \quad t \equiv \pm p \pmod{4p}$$

Since p is odd, from (1) we have, either case, that $(a/q) = -1$, and therefore the elements of order 4 are non-residues.

It follows that the only non-residues which are not primitive roots are those of order 4 modulo q. To prove that 2 is a primitive root, it now suffices to show that 2 does not have order 4 modulo

q. The only prime which is of the form $4p+1$, and which is smaller that 2^4 is $q = 13 = 4\cdot 3+1$. But $2^4 \not\equiv 1 \,(\mathrm{mod}\, 13)$.

This completes the proof.

Consider now the map $f_{\omega,m}$, with $m = q$, q as above, and $\omega \equiv 2 \,(\mathrm{mod}\, m)$. We conclude that this map has exactly two two orbits, a fixed point at the origin, and one $(m-1)$-cycle.

Solution 9:

Figure 1 was generated by the following Maple code.

```
#-------- the first N primes
N:=10000:
Primes:=[seq(ithprime(k),k=2..N+1)]:
#-------- the sequence [[p,ord(2)]...]
Orders:=map(x->[x,numtheory[order](2,x)],Primes):
#-------- Artin’s constant
AC:=0.3739558:
#-------- Artin[k] is A(2,x) for x = the kth odd prime
Artin:=array(1..N):
total:=0:
for k to N do
   if Orders[k,1]-Orders[k,2]=1 then
      total:=total+1
   fi:
   Artin[k]:=total/k
od:
#-------- plot
plot([seq([Primes[k],Artin[k]],k=1..N)],
      [[0,AC],[Primes[-1],AC]],’x’=0..Primes[-1],’A’=0.35..0.42);
```

7.3 Section 3

Solution 1: See hints.

Solution 2:

$$|35|_7 = 1/7, \qquad |12/56|_7 = 7, \qquad |2400|_7 = 1, \qquad |2400/2401|_7 = 2401.$$

Solution 3:

By definition, we have $|0| = 0$. From lemma 4.3 $i)$, we have $|1| = 1$. From Euler's theorem, we have $x^{p-1} = 1$, whence $|x^{p-1}| = |x|^{p-1} = |1| = 1$, and $|x| = 1$ from lemma 4.3 $ii)$. So the absolute value is trivial.

Solution 4:

By theorem 4.2 $i)$, $|x-y|_p = 0$ iff $x-y = 0$, so $i)$ is established. By lemma 4.3 $ii)$ we have $|x-y|_p = |-(x-y)|_p = |y-x|_p$, and $ii)$ is proved. Finally, applying the non-archimedean property to the equation

$$(x-y) = (x-z) + (z-y)$$

we prove $iii)$.

Solution 5:

Let x be a positive integer, and let $x = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ be its prime factorization. We find

$$\begin{cases} |x|_q = 1 & \text{if } q \neq p_i \\ |x|_{p_i} p_i^{-\alpha_i} & \text{for } i = 1, \ldots, k \\ |x|_\infty = p_1^{\alpha_1} \cdots p_k^{\alpha_k} & \end{cases}$$

The result then follows. If x is a positive rational, then we deal with numerator and denominator separately, extending the result to this case. Finally, the sign makes no difference, due to lemma 4.3 $iii)$.

Solution 6:

1. We have

   $$|p^n|_p = |p|_p^n = (p^{-1})^n \to 0$$

   So the sequence converges to 0.

2. We find
$$v_p(n!) \geqslant \lfloor n/p \rfloor \to \infty$$
where $\lfloor \cdot \rfloor$ is the floor function. Hence $n!$ converges to zero.

3. The sequence n does not converge: indeed one can find consecutive terms of this sequence, that get arbitrarily close to 0 and to 1, respectively. Choose, for instance, $n = p^k$ and $n = p^k + 1$, for sufficiently large k.

4. The sequence $1/n$ does not converge, for the same reason.

5. From the binomial theorem
$$(1+p)^{p^n} = 1 + O(p^{n+1}) \to 1.$$

Solution 7:

Between 1 and n, there are $\lfloor n/p \rfloor$ integers divisible by p, $\lfloor n/p^2 \rfloor$ divisible by p^2, etc. Thus
$$v_p(n!) = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor .$$
Therefore
$$v_p(n!) \leqslant \sum_{k=1}^{\infty} \frac{n}{p^k} = \frac{n}{p-1}.$$
It follows that
$$|n!|_p = p^{-v_p(n!)} > p^{-n/(p-1)}$$
and therefore for the radius of convergence ρ we obtain the estimate
$$\rho \geqslant p^{-1/(p-1)}.$$

Solution 8:

Firstly, an integer a with the above properties does exist. Indeed, using a primitive root we see that for $p > 2$ half of the integers between 1 and $p-1$ are squares modulo p, whereas the number of integer squares in the same range is at most $\lfloor \sqrt{p-1} \rfloor$, where $\lfloor \cdot \rfloor$ is the floor function. So for $p > 5$ there are more modular squares than squares, and hence some modular square is not a square in $\mathbb{Z}$. For $p = 3, 5$, one may choose $a = 7, 6$, respectively.

Because a is not a square in $\mathbb{Q}$, any solution of the equation $f(x) = x^2 - a = 0$ is not a rational number. We must show that there exists a Cauchy sequence of rational numbers that converges with respect to $|\cdot|_p$ to a root of f. Let x_0 be such that $a \equiv x_0^2 \,(\mathrm{mod}\ p)$. Then
$$f(x_0) \equiv 0 \,(\mathrm{mod}\ p) \qquad f'(x_0) \equiv 2b \not\equiv 0 \,(\mathrm{mod}\ p)$$

where the rightmost inequality holds because p is assumed to be odd. By Hensel's lemma, we can construct a sequence of integers

$$x_0, x_1, \ldots$$

such that, for all n, $f(x_n) \equiv 0 \pmod{p^n}$, and $x_{n+1} \equiv x_n \pmod{p^n}$. From lemma 5.4, this is a Cauchy sequence of rational numbers (integers, in fact), that converges with respect to $|\cdot|_p$ to a solution of the equation $f(x) = 0$. So $\mathbb{Q}$ is not complete.

Solution 9:

We consider cube roots instead of square roots. Thus let $f(x) = x^3 - 3$, and cube roots of 3 are not rational. We find

$$f(1) \equiv 0 \pmod{2} \qquad f'(1) \equiv 1 \pmod{2}.$$

Hensel's lemma applies, and we proceed as above.

7.4 Section 4

Solution 1: Let

$$L : \mathscr{C}_n \to \mathscr{C}_0 \qquad x \mapsto p^n x.$$

The map L, being linear and non-constant, is clearly bijective.

Solution 2:

For $\omega = 4, p = 5$, we find

$$\mathrm{ord}_5(4) = 2 \qquad |4^2 - 1|_5 = |15|_5 = 5^{-1}.$$

Using the notation of theorem 6.1, we have $r = 2, s = 1$, so the period modulo 5^k is

$$\begin{cases} 2 & \text{if } k = 1 \\ 2 \cdot 5^{k-1} & \text{if } k > 1. \end{cases}$$

For $\omega = 14, p = 29$, possible orders are 1,2,7,14,28. We compute, modulo 29,

$$14^2 = 196 = -5, \quad 14^4 = 25 = -4, \quad 14^7 = 20 \cdot 14 = 280 = -10, \quad 14^{14} = 100 = -1.$$

So 14 is a primitive root modulo 29 ($r = 28$). Using Maple, we find

$$|14^{28} - 1|^{29} = 29^{-2}$$

so $s = 2$. The required period modulo 29^k is

$$\begin{cases} 28 & \text{if } k = 1, 2 \\ 28 \cdot 29^{k-2} & \text{if } k > 2. \end{cases}$$

Solution 3:

We compute

$$f_\omega^t(x) - x = x(\omega^t - 1).$$

Now

$$|\omega^t - 1|_p = |t p^s + O(p^{2s})|_p \leqslant p^{-s}$$

and hence

$$|f_\omega^t(x) - x|_p \leqslant |x|_p p^{-s}.$$

We note that the left-hand side of this inequality represents the distance between the initial point x and an arbitrary point of its orbit.

7.5 Section 5

Solution 1:

The fixed points are roots of the polynomial

$$\Phi(x) = f(x) - x = x^2 - 2x + 2.$$

We find

$$\Phi(3) \equiv \Phi(4) \equiv 0 \pmod{5}; \qquad \Phi'(3) \equiv 4 \pmod{5}; \qquad \Phi'(4) \equiv 1 \pmod{5}.$$

From Hensel's lemma, the polynomial Φ has two distinct roots θ_1, θ_2 in $\mathbb{Z}_5$, with

$$\theta_1 \equiv 3 \pmod{5} \qquad \theta_2 \equiv 4 \pmod{5}.$$

We compute

$$\theta_1 = 3 + 1 \cdot 5 + 2 \cdot 5^2 + \cdots \qquad \theta_2 = 4 + 3 \cdot 5 + 2 \cdot 5^2 + \cdots$$

Thus

$$\theta_1 \equiv 58 \pmod{5^3} \qquad \theta_2 \equiv 69 \pmod{5^3}.$$

The corresponding multipliers $\omega_i = f'(\theta_i)$ are

$$\omega_1 = f'(\theta_1) \equiv 115 \pmod{5^3} \qquad \omega_2 = f'(\theta_2) \equiv 12 \pmod{5^3}.$$

Thus the fixed point θ_1 is an attractor, $|\omega_1|_p = 1/p$, while θ_2 is indifferent, $|\omega_2|_p = 1$.

In particular, iterating in the vicinity of θ_1, we converge to θ_1 (see problem 4). For example, the orbit through the point $x_0 = 3$, which is near to θ_1, is given by

$$(3, 8, 58, 3308, \ldots)$$

and we recover the approximation $\theta_1 \approx 58 \pmod{5^3}$ found above.

Solution 2:

We solve Schröder functional equation

$$L(f(x)) = \omega L(x)$$

for the power series

$$L(x) = \sum_{n \geqslant 0} b_n x^n.$$

As in the proof of Theorem 7.1, we find $b_0 = 0$, and b_1 arbitrary; hence we set $b_1 = 1$. The recursion relations for the coefficients b_n reads

$$b_m = -\frac{1}{\omega^m - 1} \sum_{n=\lceil m/2 \rceil}^{m-1} b_n \binom{n}{2n-m} \omega^{2n-m-1} a^{m-n} \qquad m > 1.$$

Since $m > 1$, the quantity $\omega^m - 1$ is a unit, from proposition 4.4. Let c_n be the coefficient of b_n in the above sum, namely

$$c_n = \binom{n}{2n-m} \omega^{2n-m-1} a^{m-n}$$

and let $c_n = 0$ for $0 < n < \lceil m/2 \rceil$. Considering that c_n is a p-adic integer, we find

$$|b|_m = \left| \sum_{n=1}^{m-1} b_n c_n \right| \leqslant \max_{0<n<m} (|b_n c_n|_p) \leqslant \max_{0<n<m} (|b_n|).$$

Hence all b_n are integers, and the series for L has a non-zero radius of convergence. We see the radius of convergence of L is not smaller than 1; in particular, the (semi)-conjugacy holds in the closed disc of radius $1/p$.

7.6 Section 6

Solution 1:

Since q is co-prime to p, then $\bar{\theta}$ is a unit. The congruence $\theta \equiv 0 \pmod{p^n}$ shows that $|\theta|_p \leqslant p^{-n}$. To prove equality, use, say, Newton's method (see next problem).

Solution 2:

The Newton map $\theta_s \mapsto \theta_{s+1}$ is given by

$$\theta_{s+1} = \theta_s - \frac{f(\theta_s)}{f'(\theta_s)} = \frac{\theta_s^2 - p^{2n}}{2\theta_s - q}.$$

Iterating this with initial condition $\theta_0 = 0$, we find

$$\theta_1 = \frac{p^{2n}}{q}, \qquad \theta_2 = \frac{q^2 p^{2n} - p^{4n}}{q(q^2 - 2p^{2n})},$$

etc. To get a power series, we note that

$$\frac{1}{q^2 - 2p^{2n}} = \frac{1}{q^2} \cdot \frac{1}{1 - 2p^{2n}/q^2}.$$

Since $|2p^{2n}/q^2|_p < 1$, we may expand the rightmost fraction in power series

$$\frac{1}{1 - 2p^{2n}/q^2} = 1 + \frac{2p^{2n}}{q^2} + \frac{4p^{4n}}{q^4} + \cdots,$$

etc. Iterating Newton's map once more, we obtain the expansion of θ modulo p^{8n}.

The expansion of $\bar{\theta}$ is dealt with similarly.

Solution 3:

The root θ is known with 2 digit accuracy. To obtain 16 digits accuracy, it suffices to iterate Newton's method three times, since the accuracy doubles at each iterations. We obtain

$$\theta \equiv -\frac{52}{119} \pmod{2^{16}} \equiv 56724 \pmod{2^{16}}$$

where the last congruence is obtained either with Euclid's algorithm, or —if you feel lazy— with Maple. Expanding 56724 in base 2 gives the desired digit string (with the digits written backwards!).

Solution 4:

This statement follows at once from the factorization of $f(X)$ modulo p into two distinct factors.

Because the norm of P^k is p^k, and the smallest positive integer contained in P^k is p^k (lest P and $\bar{P}$ would not be distinct), we conclude that the $\mathbb{Z}$-basis of P^k must be of the given form, for some s_k to be determined modulo p^k. The congruence class of of s_k is determined by noting that the local image of λ is θ, and that the local image of each basis element must be congruent to zero modulo p^k.

References

[1] V. Akiyama and H. Brunotte and A. Pethö and W. Steiner, Periodicity of certain piecewise affine integer sequences, *Tsukuba J. Math.* **32** (2008) 197–251.

[2] V. Anashin, and A. Khrennikov, *Applied algebraic dynamics*, Walter de Gruyter, Berlin (2009).

[3] D. Bosio and F. Vivaldi, Round-off errors and p-adic numbers, *Nonlinearity* **13** (2000) 309–322.

[4] G. Everest and T. Ward, *Heights of polynomials and entropy in algebraic dynamics*, Springer, London (1999).

[5] C F Gauss, *Disquisitiones Arithmeticae* (1801).

[6] F Q Gouvêa, *p-adic numbers* Springer, Berlin (2000).

[7] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, Oxford University Press Oxford (1979).

[8] J. Lubin, One-parameter formal Lie groups over p-adic integer rings, *Ann. Math.* **80** (1964) 464.

[9] J. Lubin and J. Tate, Formal complex multiplication in local fields, *Ann. Math.* **81** (1965) 380.

[10] D A Marcus, *Number fields* Springer, Berlin (1977).

[11] M. RamMurty, Artin's conjecture for primitive roots, *Math. Intelligencer* **10** (1988) 59–67.

[12] F.Rannou, Numerical study of discrete plane area-preserving mappings, *Astron. and Astrophys.* **31** (1974) 289–301.

[13] J. H. Silverman, *The arithmetic of dynamical systems*, Springer, New York (2007).

[14] B. L van der Waerden *Algebra* Springer-Verlag, New York (1991).

[15] F. Vivaldi and I. Vladimirov, Pseudo-randomness of round-off errors in discretized linear maps on the plane, *Int. J. of Bifurcations and Chaos*, **13** (2003) 3373–3393.

Index