D-MATH
Prof. Richard Pink

Algebraic Number Theory

FS 2018

Solutions 9

p-adic Numbers, Absolute Values

1. Determine the p-adic expansions of ± 1 and $\frac{\pm 1}{1-p}$ for an arbitrary prime p.

   Solution: The answers are

$$\begin{aligned} 1 &= 1 + 0 \cdot p + 0 \cdot p^2 + \ldots, \\ -1 &= (p-1) + (p-1)p + (p-1)p^2 + \ldots, \\ \tfrac{1}{1-p} &= 1 + p + p^2 + p^3 + \ldots, \\ \tfrac{-1}{1-p} &= (p-1) + (p-2)p + (p-2)p^2 + (p-2)p^3 + \ldots. \end{aligned}$$

   The first case is obvious. In the second the partial sums of the right hand side are $-1 + p^n \equiv -1$ modulo $p^n\mathbb{Z}$ for all n. The remaining two cases are proved by multiplying by $1-p$ and computing modulo $p^n\mathbb{Z}$ again.

2. Represent the rational numbers $\frac{2}{3}$ and $-\frac{2}{3}$ as 5-adic numbers.

   Solution: The answers are

$$\begin{aligned} \tfrac{2}{3} &= 4 + 1 \cdot 5 + 3 \cdot 5^2 + 1 \cdot 5^3 + 3 \cdot 5^4 + \ldots = \ldots 31314, \\ -\tfrac{2}{3} &= 1 + 3 \cdot 5 + 1 \cdot 5^2 + 3 \cdot 5^3 + 1 \cdot 5^4 + \ldots = \ldots 13131, \end{aligned}$$

   where the digit sequences become periodic with period 2. Both equations are proved by multiplying with $1 - 5^2$ and expanding modulo $5^n\mathbb{Z}$ for all n.

3. (a) Show that a rational number x with $\mathrm{ord}_p(x) = 0$ has a purely periodic p-adic expansion if and only if $x \in [-1, 0)$.

   (b) Show that in $\mathbb{Q}_p$ the numbers with eventually periodic p-adic expansions are precisely the rational numbers.

   Solution: See Theorem 3.1 for (a) and Theorem 2.1 for (b) in this source:
   `http://www.math.uconn.edu/~kconrad/blurbs/gradnumthy/rationalsinQp.pdf`

4. Show that the equation $x^2 = 2$ has a solution in $\mathbb{Z}_7$ and compute its first few 7-adic digits.

   Solution: We have to find a sequence of integers $a_0, a_1, a_2, \dots \in \{0, \ldots, 6\}$ such that

$$(a_0 + a_1 7 + a_2 7^2 + \ldots)^2 \equiv 2 \bmod (7^n)$$

   for every $n \geqslant 1$. For $n = 1$, we obtain $a_0^2 \equiv 2 \bmod (7)$, which has the solutions $a_0 = 3$ and $a_0 = 4$. We choose $a_0 = 3$ (the other case is similar). Let $n > 1$

and suppose that we found $a_0, \dots, a_{n-1}$ that fit in the above equation $\bmod 7^n$ and let $b_{n-1} := \sum_{i=0}^{n-1} a_i 7^i$. Then $b_{n-1}^2 + 2b_{n-1}a_n 7^n \equiv (b_{n-1} + a_n 7^n)^2 \equiv 2 \bmod(7^{n+1})$ is equivalent to

$$\frac{b_{n-1}^2 - 2}{2 \cdot 7^n \cdot b_{n-1}} + a_n \equiv 0 \bmod(7),$$

as $7^n | (b_{n-1}^2 - 2)$. This equation possesses a unique solution for $a_n \in \{0, \dots, 6\}$. We calculate the first few values and obtain

$$x \;=\; 3+7+2\cdot 7^2+6\cdot 7^3+7^4+2\cdot 7^5+7^6+2\cdot 7^7+4\cdot 7^8+6\cdot 7^9+\dots \;=\; \dots 6421216213.$$

Aliter: The equation is equivalent to $(2x)^2 = 8 = 1 + 7$. Thus a solution is given by the binomial series

$$2x \;=\; \sum_{n \geqslant 0} \binom{\frac{1}{2}}{n} \cdot 7^k \;=\; 1 + \frac{1}{2} \cdot 7 - \frac{1}{8} \cdot 7^2 + \frac{1}{16} \cdot 7^3 - \frac{5}{128} 7^4 + \dots .$$

Dividing by two, we obtain the second solution to the equation

$$x = 4 + 5 \cdot 7 + 4 \cdot 7^2 + 5 \cdot 7^4 + 4 \cdot 7^5 + \dots \;=\; \dots 0245450454.$$

This is really minus the first solution, as can be seen by adding their p-adic expansions in the usual way.

*5. For any integer $n \geqslant 2$ consider the map

$$\pi \colon \prod_{i \geqslant 1} \{0, 1, \dots, n-1\} \;\longrightarrow\; [0,1], \quad (a_i)_i \mapsto \sum_{i \geqslant 1} a_i n^{-i}.$$

Show that π is surjective and determine its fibers. Prove that the natural topology on the interval $[0,1]$ is the quotient topology via π from the product topology on $\prod_{i \geqslant 1} \{0, 1, \dots, n-1\}$, where each factor is endowed with the discrete topology. Interpret this fact by comparing the topologies on the source and the target.

Solution: It is well-known that the map is well-defined and surjective, and that the only distinct sequences representing the same number are those of the form $(a_1, \dots, a_n, n-1, n-1, \dots)$ and $(a_1, \dots, a_{n-1}, a_n + 1, 0, 0, \dots)$ for arbitrary $n \geqslant 1$ and $a_1, \dots, a_n$ with $a_n < n - 1$.

A standard computation from first year calculus shows that π is continuous. Thus for any closed subset $X \subset [0,1]$ the inverse image $\pi^{-1}(X)$ is closed. On the other hand, since the source is compact and the target is Hausdorff, the map is also closed. Thus for any subset $X \subset [0,1]$, if $\pi^{-1}(X)$ is closed, then so is $X = \pi(\pi^{-1}(X))$ by surjectivity. Therefore $[0,1]$ carries the quotient topology via π.

This may be somewhat surprising, because the space $\prod_{i \geqslant 1} \{0, 1, \dots, n-1\}$ is totally disconnected, whereas $[0,1]$ is connected. But π is only bijective outside a countable subset, and countably many pairs of distinct points are glued with each other. Roughly speaking π therefore pulls different pieces of the totally disconnected space $\prod_{i\geqslant 1}\{0,1,\ldots,n-1\}$ together to form the nice smooth connected interval $[0,1]$.

6. Consider the sequence of integers defined by $a_1 := 5$ and $a_{i+1} := a_i^2$ for all $i \geqslant 1$. Write the decimal expansions of these a_i below each other. Observe the pattern and formulate and prove a theorem about it. Explain the pattern by comparison with p-adic numbers. Does a similar pattern occur with other starting values and other bases besides 10 for the expansion?

   Solution: With a computer algebra system we can compute the first few numbers as

i	a_i
1	5
2	25
3	625
4	390625
5	152587890625
6	...386962890625
7	...855712890625
8	...793212890625
9	...668212890625
10	...418212890625
11	...918212890625
12	...918212890625

   We observe that for each $i \geqslant 1$ the last i digits of a_i coincide with those of a_{i+1}.

   To prove this note that for each i, we have $a_i = 5^{2^{i-1}} \equiv 0$ modulo 5^i. On the other hand we claim that $a_i \equiv 1$ modulo 2^i. Indeed, that is clear for $i = 1$; and if it holds for i, writing $a_i = 1 + 2^i b$ shows that $a_{i+1} = a_i^2 = 1 + 2^{i+1}b + 2^{2i}b^2 \equiv 1$ modulo 2^{i+1}; so the claim follows by induction. Together this shows that $a_i \equiv 0 \equiv a_{i+1}$ modulo 5^i and that $a_i \equiv 1 \equiv a_{i+1}$ modulo 2^i. Therefore $a_i \equiv a_{i+1}$ modulo 10^i, which precisely means that the last i decimal digits of a_i and a_{i+1} coincide.

   For a general explanation observe that giving the last i decimal digits of a non-negative integer is equivalent to giving the integer modulo 10^i. By the Chinese remainder theorem we have $\mathbb{Z}/10^i\mathbb{Z} \cong \mathbb{Z}/2^i\mathbb{Z}\times\mathbb{Z}/5^i\mathbb{Z}$; hence it is also equivalent to giving the integer modulo 5^i and modulo 2^i. For our sequence the above arguments show that $a_i \to 0$ in $\mathbb{Z}_5$ and $a_i \to 1$ in $\mathbb{Z}_2$, so the last digits stabilize.

   The same phenomenon occurs with any odd $a_1 = m$ and base $2m$, and surely one can find other cases.

7. Let $|\cdot|$ be an absolute value on a field K. Show that $|\cdot|^\alpha$ is also an absolute value for every $0 < \alpha \leqslant 1$.

Solution: Let $x, y \in K$. Since $|\cdot|$ is an absolute value, we have $|x|^\alpha \geqslant 0$ with equality if and only if $x = 0$. Furthermore $|xy|^\alpha = (|x||y|)^\alpha = |x|^\alpha |y|^\alpha$. Also there exists $z \in K$ with $|z| \notin \{0, 1\}$ and hence $|z|^\alpha \notin \{0, 1\}$. It remains to show the triangle inequality. For this note that $|\ |^\alpha = h \circ |\ |$ for the function $h\colon [0, \infty) \to [0, \infty)$, $a \mapsto a^\alpha$. Since the second derivative $h''(t) = \alpha(\alpha - 1)t^{\alpha-2}$ is negative on the interval $(0, \infty)$, this function is *concave*, i.e., for all $a, b \in [0, \infty)$ and $t \in [0, 1]$ we have

$$h(ta + (1 - t)b) \geqslant th(a) + (1 - t)h(b).$$

Since also $h(0) = 0$, using the following lemma from analysis we can conclude that $|x + y|^\alpha \leqslant (|x| + |y|)^\alpha \leqslant |x|^\alpha + |y|^\alpha$, as desired.

Lemma. *Any concave function $f\colon [0, \infty) \to \mathbb{R}$ with $f(0) \geqslant 0$ is* subadditive, *that is, it satisfies $f(a + b) \leqslant f(a) + f(b)$ for all $a, b \in [0, \infty)$.*

Proof. For all $x \in [0, \infty)$ and $t \in [0, 1]$ we have

$$f(tx) = f(tx + (1 - t)0) \geqslant tf(x) + (1 - t)f(0) \geqslant tf(x).$$

For all $a, b \in [0, \infty)$ it follows that

$$\begin{aligned} f(a) + f(b) &= f\left(\frac{a}{a+b}(a + b)\right) + f\left(\frac{b}{a+b}(a + b)\right) \\ &\geqslant \frac{a}{a+b} f(a + b) + \frac{b}{a+b} f(a + b) = f(a + b). \end{aligned}$$

□