D-MATH
Prof. Richard Pink

Number Theory I

FS 2024

Solutions 14

p-adic Numbers

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

Solution: The answers are

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

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

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

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:
`https://kconrad.math.uconn.edu/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 $a_0, a_1, a_2, \dots \in \{0, \dots, 6\}$ such that

$$(a_0 + a_1 7 + a_2 7^2 + \dots)^2 \equiv 2 \mod (7^n)$$

for every $n \geqslant 1$. For $n = 1$, we obtain $a_0^2 \equiv 2 \mod (7)$, 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 $a_0, \ldots, a_{n-1}$ that fit in the above equation $\mod 7^n$ and let $b_{n-1} := \sum_{i=0}^{n-1} a_i 7^i$. Then $b_{n-1}^2 + 2b_{n-1}a_n 7^n \equiv (b_{n-1} + a_n 7^n)^2 \equiv 2 \mod (7^{n+1})$ is equivalent to

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

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

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

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

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

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

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

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

5. For which primes p is -1, resp. 2, resp. 3 a square in $\mathbb{Q}_p$?

Solution: If p is odd, we have the group decomposition

$$\mathbb{Q}_p^\times = p^{\mathbb{Z}} \times \mu_{p-1} \times (1 + p\mathbb{Z}_p),$$

where the last factor is isomorphic to $\mathbb{Z}_p$. The assumption $p > 2$ also implies that 2 is invertible in $\mathbb{Z}_p$; hence every element of $1 + p\mathbb{Z}_p$ is a square. The subgroup of squares in $\mathbb{Q}_p^\times$ is therefore

$$p^{2\mathbb{Z}} \times \mu_{\frac{p-1}{2}} \times (1 + p\mathbb{Z}_p).$$

In the case $p = 2$ we similarly have

$$\mathbb{Q}_2^\times = 2^{\mathbb{Z}} \times \mu_2 \times (1 + 4\mathbb{Z}_2),$$

where the last factor is isomorphic to $\mathbb{Z}_2$. Here the subgroup of squares of $1 + 4\mathbb{Z}_2$ corresponds to the subgroup $2\mathbb{Z}_2 \subset \mathbb{Z}_2$ of index 2 and is therefore equal to $1 + 8\mathbb{Z}_2$. The subgroup of squares in $\mathbb{Q}_2^\times$ is therefore

$$2^{2\mathbb{Z}} \times (1 + 8\mathbb{Z}_2).$$

Now observe that the given integer a is never divisible by p^2. For it to be a square in $\mathbb{Q}_p$ it must therefore be prime to p. For $p = 2$ the above description of squares shows that none of the given integers is a square in $\mathbb{Q}_2$. For p odd the description of squares shows that a is a square if and only if its residue class modulo p is a square, that is, if $\left(\frac{a}{p}\right) = 1$.

In the case $a = -1$ the first supplement of the quadratic reciprocity law yields $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$. Thus -1 is a square in $\mathbb{Q}_p$ if and only if $p \equiv 1 \bmod (4)$.

In the case $a = 2$ the second supplement of the quadratic reciprocity law yields $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$. Thus 2 is a square in $\mathbb{Q}_p$ if and only if $p \equiv \pm 1 \bmod (8)$.

Finally, for $a = 3$ we computed in exercise 6 (b) of sheet 5 that

$$\left(\frac{3}{p}\right) = \begin{cases} 0 & \text{if } p = 3, \\ 1 & \text{if } p \equiv \pm 1 \bmod 12, \\ -1 & \text{if } p \equiv \pm 5 \bmod 12. \end{cases}$$

Thus 3 is a square in $\mathbb{Q}_p$ if and only if $p \equiv \pm 1 \bmod 12$.

*6. For any integer $b \geqslant 2$ consider the map

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

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 $\prod_{i \geqslant 1} \{0, 1, \ldots, b-1\}$, 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 $(a_1, \ldots, a_n, b-1, b-1, \ldots)$ and $(a_1, \ldots, a_{n-1}, a_n + 1, 0, 0, \ldots)$ for arbitrary $n \geqslant 1$ and $a_1, \ldots, a_n$ with $a_n < b-1$.

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 $\prod_{i \geqslant 1} \{0, 1, \ldots, b-1\}$ 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 $\prod_{i \geqslant 1} \{0, 1, \ldots, b-1\}$ together to form the nice smooth connected interval $[0,1]$.

7. Prove that for any prime p the ring of endomorphisms of the additive group $\mathbb{Z}[\frac{1}{p}]/\mathbb{Z}$ is canonically isomorphic to $\mathbb{Z}_p$.

Solution: The group $G := \mathbb{Z}[\frac{1}{p}]/\mathbb{Z}$ is the union of the groups $G_n := p^{-n}\mathbb{Z}/\mathbb{Z}$ for all $n \geqslant 0$, and G_n is the kernel of the homomorphism $G \to G$, $g \mapsto p^n g$. Thus any endomorphism of G maps G_n to itself. For the same reason, any endomorphism of G_{n+1} induces an endomorphism of G_n. Giving an endomorphism of G is therefore equivalent to giving a system of endomorphisms $\varphi_n \in \mathrm{End}(G_n)$ for all $n \geqslant 0$ that satisfy $\varphi_n = \varphi_{n+1}|G_n$.

For each $n \geqslant 0$, the group G_n is cyclic of order p^n; hence any endomorphism is determined by the image of a generator. This generator is mapped to a times itself for an integer a that is unique modulo (p^n). Since the endomorphism then maps every element of G_n to a times itself, the residue class $a + p^n\mathbb{Z} \in \mathbb{Z}/p^n\mathbb{Z}$ is in fact independent of the choice of generator. Together this yields a canonical bijection

$$\kappa_n \colon \mathbb{Z}/p^n\mathbb{Z} \xrightarrow{\sim} \mathrm{End}(G_n), \quad a + p^n\mathbb{Z} \mapsto (g \mapsto ag).$$

Direct computation shows that this is a ring isomorphism and that $\kappa_n(a+p^n\mathbb{Z}) = \kappa_{n+1}(a + p^{n+1}\mathbb{Z})|G_n$ for all $n \geqslant 0$. Altogether we therefore obtain a canonical ring isomorphism

$$\mathbb{Z}_p \;:=\; \varprojlim_n \mathbb{Z}/p^n\mathbb{Z} \;\xrightarrow{\sim} \mathrm{End}(G).$$