

Introduction to p -adic Numbers

Exercise Sheet 1

No submission – to be discussed in the exercise class.

Throughout, p denotes a prime number. Let $x = \frac{a}{b} \in \mathbb{Q}$ with $a, b \in \mathbb{Z}$ coprime and $p \nmid b$. Since b is invertible modulo every power of p , it makes sense to write

$$x \equiv c \pmod{p^k} \iff a \equiv bc \pmod{p^k} \quad (c \in \mathbb{Z}, k \geq 1).$$

Exercise 1.1**The p -adic expansion of a fraction.**

- (a) Show that for every $k \geq 0$ there are unique digits $a_0, \dots, a_k \in \{0, \dots, p-1\}$ with

$$x \equiv a_0 + a_1p + \dots + a_kp^k \pmod{p^{k+1}},$$

and that the digits obtained for $k+1$ extend those obtained for k . The resulting sequence $(a_k)_{k \geq 0}$ is the p -adic expansion of x , written $(\dots a_2a_1a_0)_p$.

- (b) In the lecture we computed the digits by the following algorithm: choose $a_0 \in \{0, \dots, p-1\}$ with $a - a_0b \equiv 0 \pmod{p}$ and set $r_0 = \frac{a - a_0b}{p}$; for $k \geq 0$ choose $a_{k+1} \in \{0, \dots, p-1\}$ with $r_k - a_{k+1}b \equiv 0 \pmod{p}$ and set $r_{k+1} = \frac{r_k - a_{k+1}b}{p}$.

Show that in each step there is exactly one such digit, that all r_k are integers, and that

$$a - b(a_0 + a_1p + \dots + a_kp^k) = p^{k+1}r_k \quad \text{for all } k \geq 0.$$

Conclude that the algorithm yields exactly the p -adic expansion of x from (a).

- (c) Use the algorithm to compute the first six 5-adic digits of $\frac{1}{3}$. What do you observe? Check your result by verifying $3(a_0 + a_1 \cdot 5 + \dots + a_4 \cdot 5^4) \equiv 1 \pmod{5^5}$.

Exercise 1.2

Shifting digits. Let x be as above with p -adic expansion $(\dots a_2a_1a_0)_p$.

- (a) Show that px has the p -adic expansion $(\dots a_2a_1a_00)_p$, i.e. its digits are $0, a_0, a_1, a_2, \dots$.
- (b) In the lecture we found $\frac{24}{17} = (\dots 2110201010)_3$. Deduce the 3-adic expansion of $\frac{8}{17}$ and explain why the last digit 0 has to be removed.
- (c) For a fraction whose denominator is divisible by p we allow finitely many digits after the point: $(\dots a_1a_0.a_{-1} \dots a_{-m})_p$ stands for $\sum_{k \geq -m} a_kp^k$. Write down the 3-adic expansions of $\frac{8}{51}$ and $\frac{8}{153}$.

Exercise 1.3

A p -adic solution of a Fermat equation. Let $n \geq 1$ with $p \nmid n$ and set $c = 1 + p^n$.

- (a) Let $m \geq 1$ and $z \in \mathbb{Z}$ with $z \equiv 1 \pmod{p}$ and $z^n \equiv c \pmod{p^m}$. Show that there is a unique $t \in \{0, \dots, p-1\}$ with

$$(z + tp^m)^n \equiv c \pmod{p^{m+1}}.$$

Hint: Binomial theorem. Which terms vanish modulo p^{m+1} ? Where do you need $p \nmid n$?

- (b) Conclude that there are integers $z_m \in \{0, \dots, p^m - 1\}$, $m \geq 1$, with

$$z_m^n \equiv c \pmod{p^m} \quad \text{and} \quad z_{m+1} \equiv z_m \pmod{p^m} \quad \text{for all } m \geq 1.$$

As explained in Section 1.2 of the lecture, this defines a p -adic number z with $z^n = 1 + p^n$. In particular, $x^n + y^n = z^n$ has the p -adic solution $x = 1$, $y = p$, z with $xyz \neq 0$.

- (c) Let $p = 5$ and $n = 3$. Explain why $z_1 = z_2 = z_3 = 1$ and compute z_4 and z_5 .
- (d) Show that for $p = 2$ and $n = 2$ the congruence $z^2 \equiv 1 + 2^2 \pmod{8}$ has no solution $z \in \mathbb{Z}$. So the assumption $p \nmid n$ cannot simply be dropped.