PAWS 2026: QUATERNION ALGEBRAS
PROBLEM SET 4

MATT BROE, DIVYASREE C-RAMACHANDRAN, XINYU FANG, ALEXANDER WANG

Here are some problems to help you get familiar with p-adic numbers and explore some new ideas along the way. As always, we'd love to hear your thoughts on the problems on Discord or during our virtual sessions. Happy problem-solving!

(1) This exercise is intended to give you more practice with the inverse limit representation and the p-adic expansion of a p-adic number.
   (a) In the lecture notes, we saw that 2 has a cube root in $\mathbb{Z}_5$ given as an element of $\varprojlim_{n\geq 1} \mathbb{Z}/5^n\mathbb{Z}$ by
   $$(3, 3, 53, 303, 2178, \dots).$$
   Verify that the first three numbers in this list are indeed correct.
   Hint: If you are having trouble getting started, return to the lecture notes to review what it means for a p-adic number to have this representation as an element of the inverse limit, especially Remark 4.4.
   (b) Compute the first five digits of the 5-adic expansion of the number in part (a).
   (c) Compute the first four digits of the 7-adic expansion of a square root of 2 in $\mathbb{Z}_7$. (We will see in a later exercise that 2 is indeed a square in $\mathbb{Z}_7$!)
   (d) Show that $\frac{2}{5}$ is in $\mathbb{Z}_3$ and compute the first three digits of its 3-adic expansion.
   Bonus: In fact, it is possible to write down the full 3-adic expansion without too much additional work. See [1].

(2) Recall the definition of the p-adic valuation on $\mathbb{Z}$. Prove that for $x, y \in \mathbb{Z}_+$, $x \equiv y \mod p^n$ if and only if $|x - y|_p \leq p^{-n}$.

(3) Prove the following theorem.

Theorem 1 (Properties of the p-adic valuation)**.** *The p-adic valuation v_p on $\mathbb{Q}$ satisfies the following properties.*
(a) $v_p(x) = \infty$ *if and only if* $x = 0$.
(b) $v_p(xy) = v_p(x) + v_p(y)$.
(c) $v_p(x + y) \geq \min\{v_p(x), v_p(y)\}$.

(4) For $N \geq 1$, let
$$s_N = 2 + 3 + 3^2 + \cdots + 3^N.$$
   (a) Show that
   $$2s_N - 1 = 3^{N+1}.$$
   (b) Deduce that
   $$v_3\left(s_N - \frac{1}{2}\right) = N + 1,$$
   and hence that s_N converges to $1/2$ in $\mathbb{Q}_3$.
   (c) Conclude that the 3-adic expansion of $1/2$ is
   $$\frac{1}{2} = 2 + 3 + 3^2 + 3^3 + \cdots.$$

(d) Explain why the series on the right does not converge in $\mathbb{R}$.

(5) Let p be a prime, and let (a_n) be a sequence in $\mathbb{Q}_p$.

(a) Show that for $x_1, \ldots, x_m \in \mathbb{Q}_p$,

$$v_p(x_1 + \cdots + x_m) \geq \min_{1 \leq r \leq m} v_p(x_r).$$

(b) Suppose that

$$v_p(a_n) \longrightarrow \infty.$$

Show that the partial sums of

$$\sum_{n=0}^{\infty} a_n$$

form a Cauchy sequence. Conclude that the series converges in $\mathbb{Q}_p$.

(c) Show conversely that if

$$\sum_{n=0}^{\infty} a_n$$

converges in $\mathbb{Q}_p$, then $a_n \to 0$.

(d) Show that each of the following series converges in $\mathbb{Q}_p$:

$$\sum_{n=0}^{\infty} p^{n^2}, \qquad \sum_{n=0}^{\infty} n!.$$

For the second series, you may use

$$v_p(n!) \geq \left\lfloor \frac{n}{p} \right\rfloor.$$

(6) Recall that $\mathbb{Z}_p^\times$ is the multiplicative group of invertible elements in $\mathbb{Z}_p$.

(a) Show that

$$\mathbb{Z}_p^\times = \{a \in \mathbb{Z}_p \mid v_p(a) = 0\}.$$

(b) Show that every nonzero $a \in \mathbb{Z}_p$ can be uniquely written in the form $p^n u$ with $n \geq 0$ and $u \in \mathbb{Z}_p^\times$.

(c) Write each of the following numbers in $\mathbb{Q}_p$ in the form $p^n u$:

(i) 7^{-9} in $\mathbb{Q}_2$;

(ii) $\frac{2}{21}$ in $\mathbb{Q}_7$;

(iii) $25!$ in $\mathbb{Q}_5$.

(7) In this problem, we explore how to determine whether a rational number is a square in a p-adic field. We will use the following fact: for an odd prime p, a unit $u \in \mathbb{Z}_p^\times$ is a square in $\mathbb{Z}_p$ if and only if its reduction modulo p is a nonzero square in $\mathbb{F}_p$.

(a) List the nonzero squares modulo 7. Use your list to determine whether 2, 3, and 5 are squares in $\mathbb{Q}_7$.

(b) Show that 29 is a square in $\mathbb{Q}_7$, even though 29 is not a square in $\mathbb{Q}$.

(c) Is 12 a square in $\mathbb{Q}_5$? Explain why or why not.

(8) Consider the equation $x^2 - 3y^2 = 5$, $x, y \in \mathbb{Q}$.

(a) Show that finding a rational solution to this equation is equivalent to finding a rational point on the conic

$$3X^2 + 5Y^2 = 1.$$

(b) Show that the quaternion algebra $(3,5)_{\mathbb{Q}_3}$ does not split over $\mathbb{Q}_3$ by considering its associated conic.
Hint: Suppose $X, Y \in \mathbb{Q}_3$ satisfy $3X^2 + 5Y^2 = 1$. First, use the 3-adic valuation to show that $X, Y \in \mathbb{Z}_3$. Then reduce the equation modulo 3 and recall which elements of $\mathbb{F}_3$ are squares.

(c) Does $(3,5)_{\mathbb{Q}}$ split over $\mathbb{Q}$? Why?

References

[1] Keith Conrad. *The p-adic expansion of rational numbers.* Expository notes. `https://kconrad.math.uconn.edu/blurbs/gradnumthy/rationalsinQp.pdf`.