Homework 4

MATH 110 | Introduction to Number Theory | Summer 2023

Whenever you use a result or claim a statement, provide a **justification** or a **proof**, unless it has been covered in the class. In the later case, provide a **citation** (such as "by the *2-out-of-3 principle*" or "by Coro. 0.31 in the textbook").

You are encouraged to *discuss* the problems with your peers. However, you must write the homework **by yourself** using your words and **acknowledge your collaborators**.

Problem 1. A *Sophie Germain prime* is a prime number p such that $2p+1$ is also a prime. For example, $p = 2, 3, 5$ are Sophie Germain primes, but $p = 7$ is not (since $15 = 2 \cdot 7 + 1$ is not a prime).
Prove that if p is a Sophie Germain prime, then $2p + 1$ is a divisor either of $2^p - 1$ or of $2^p + 1$, but not of both.

Problem 2. **Find** the smallest positive integer a such that $2^a \equiv 11 \pmod{23}$.

Problem 3. Let p be a prime number.

(a) Let $f(T)$ be a polynomial modulo p of degree 2 or 3. **Prove that** $f(T)$ is irreducible if and only if $f(T)$ has no roots modulo p.

Hint. Prove the contrapositive, looking at the degrees of the divisors of $f(T)$.

(b) **Count** the number of monic polynomials modulo p of degree d.

(c) **Count** the number of monic irreducible polynomials modulo p of degree 2.

(d) **Count** the number of monic irreducible polynomials modulo p of degree 3.

Problem 4. For n a nonzero integer, recall that $v_p(n)$ is the exponent of p appearing in the prime factorization of n. Namely, $p^{v_p(n)} \mid n$, while $p^{v_p(n)+1} \nmid n$. Extend this definition to nonzero fractions as follows:

$$v_p(\frac{n}{m}) := v_p(n) - v_p(m).$$

(a) **Show that**, if the two fractions $\frac{n}{m}$ and $\frac{n'}{m'}$ represent the same rational number, then $v_p(\frac{n}{m}) = v_p(\frac{n'}{m'})$.

Hence, we obtain a function $v_p \colon \mathbb{Q}^\times \to \mathbb{Z}$. (Recall that $\mathbb{Q}^\times$ consists of nonzero rational numbers). The **p-adic norm** of a rational number x is defined to be

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

For example,

$$\left|\frac{24}{25}\right|_2 = \frac{1}{8}, \qquad \left|\frac{24}{25}\right|_3 = \frac{1}{3}, \qquad \left|\frac{24}{25}\right|_5 = 25.$$

(b) **Prove** the *ultrametric triangle inequality*: for all $x, y \in \mathbb{Q}$,

$$|x+y|_p \leq \max\Big\{|x|_p, |y|_p\Big\}.$$

(c) **Verify that**, the p-adic norm satisfies the three defining properties of a norm, namely:

1. $|x|_p = 0$ if and only if $x = 0$.
2. $|xy|_p = |x|_p |y|_p$ for all $x, y \in \mathbb{Q}$.
3. $|x+y|_p \leqslant |x|_p + |y|_p$ for all $x, y \in \mathbb{Q}$.

(d) **Show that**, for any two rational numbers x and y, we have $|x-y|_p \leqslant r$ if and only if $x \equiv y \pmod{p^e}$, where $e = \lceil -\log_p(r) \rceil$.

Say a sequence $(x_n)_{n\in\mathbb{N}}$ of rational numbers is a **Cauchy sequence with respect to the p-adic norm** (a **Cauchy sequence** for short) if for every positive real number $\varepsilon > 0$, there is a positive integer N such that for all natural numbers $m, n > N$,

$$|x_m - x_n|_p < \varepsilon.$$

Say a rational number $x \in \mathbb{Q}$ is the **limit** of a sequence $(x_n)_{n\in\mathbb{N}}$ of rational numbers **with respect to the p-adic norm** if for every positive real number $\varepsilon > 0$, there is a positive integer N such that for all natural numbers $n > N$,

$$|x_n - x|_p < \varepsilon.$$

Say two Cauchy sequences $(x_n)_{n\in\mathbb{N}}$ and $(y_n)_{n\in\mathbb{N}}$ are **equivalent** if the sequence $(x_n - y_n)_{n\in\mathbb{N}}$ has the limit 0.

(e) **Prove that**, if a sequence $(x_n)_{n\in\mathbb{N}}$ of rational numbers has a limit $x \in \mathbb{Q}$ with respect to the p-adic norm, then it is a Cauchy sequence.

(f) Let $f(T)$ be an integer polynomial. **Show that**, if a sequence $(x_n)_{n\in\mathbb{N}}$ of rational numbers has a limit $x \in \mathbb{Q}$ with respect to the p-adic norm, then the sequence $(f(x_n))_{n\in\mathbb{N}}$ has the limit $f(x)$.

(g) **Deduce** the following version of *Hensel's lifting* from the one in the lecture:

> Let $f(T)$ be an integer polynomial. If x_0 is an integer such that $|f(x_0)| < 1$ but $|f'(x_0)| = 1$, then it can be extended into a unique (up to equivalence) Cauchy sequence $(x_n)_{n\in\mathbb{N}}$ such that the sequence $(f(x_n))_{n\in\mathbb{N}}$ has the limit 0 with respect to the p-adic norm.

Hint. Using problem 4.(d) to translate the statement in the language of congruence.

(h) However, a Cauchy sequence needs not to have a limit in $\mathbb{Q}$ with respect to the p-adic norm. **Give such a counterexample**.

Remark. Lack of limits in $\mathbb{Q}$ is one motivation to introduce *p-adic numbers*.