Homework 7 (due Nov. 23)

MATH 110 | Introduction to Number Theory | Fall 2022

Problem 1. In what follows, we fix a prime number p. For n an 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) (2 pts) 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) (3 pts) Prove that $|-x|_p = |x|_p$, and $|xy|_p = |x|_p |y|_p$.

(c) (5 pts) Prove the *ultrametric triangle inequality*

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

Remark. Note that $\max\Big\{|x|_p, |y|_p\Big\} \leqslant |x|_p + |y|_p$. Hence, the ultrametric triangle inequality implies the usual triangle inequality. The previous two says that $|\cdot|_p$ can be viewed as analogy of the usual Euclidean norm of vectors, or the absolute value of real numbers.

For $z \in \mathbb{Q}$, the **p-adic ball** with center z and radius $r \in \mathbb{R}$ is defined to be

$$B_{|\,\cdot\,|_p}(z, r) := \Big\{x \in \mathbb{Q} \;\Big|\; |x - z|_p \leqslant r\Big\}.$$

(d) (5 pts) Prove that the p-adic ball $B_{|\,\cdot\,|_p}(0,1)$ is closed under addition and multiplication.

Since, clearly $0, 1 \in B_{|\,\cdot\,|_p}(0,1)$, we have actually proven that $B_{|\,\cdot\,|_p}(0,1)$ is a ring. This ring is called the **non-complete ring of p-adic integers** and is usually denoted by $\mathbb{Z}_{(p)}$.

(e) (2 pts) We can explicitly describe $\mathbb{Z}_{(p)}$. Prove that

$$\mathbb{Z}_{(p)} = \Big\{\frac{a}{b} \in \mathbb{Q} \;\Big|\; a, b \in \mathbb{Z},\ p \nmid b,\ \mathrm{GCD}(a,b) = 1\Big\}.$$

(f) (3 pts) Let a be an integer and e be a positive integer. Describe the p-adic ball $B_{|\cdot|_p}(a, p^{-e})$ using the language of congruence.

Problem 2. Let R be a ring. A **polynomial with coefficients in** R is an expression

$$f(T) = a_n T^n + \cdots + a_1 T + a_0, \tag{2.1}$$

where $a_0, \cdots, a_n \in R$. The set of all polynomials with coefficients in R is denoted $R[T]$.

Let $f(T)$ be a polynomial as in (2.1). Its **derivative** is the polynomial

$$f'(T) := n a_n T^{n-1} + \cdots + a_1.$$

Note that this definition is formal, not involving any limit. The **second derivative** $f''(T)$ of $f(T)$ is the derivative of $f'(T)$. In general, the k-th derivative $f^{(k)}(T)$ of $f(T)$ is the derivative of $f^{(k-1)}(T)$.

(a) (5 pts) Let $a \in R$. Prove the *Taylor expansion*:

$$f(a+T) = f(a) + f'(a)T + \frac{f''(a)}{2!}T^2 + \cdots + \frac{f^{(n)}(a)}{n!}T^n,$$

where n is the degree of $f(T)$.

(b) (5 pts) Let $f(T)$ be a polynomial with coefficients in $\mathbb{Z}$ and k a positive integer. Prove that $\frac{1}{k!}f^{(k)}(T)$ has coefficients in $\mathbb{Z}$. That is to say, every coefficient of $f^{(k)}(T)$ is a multiple of $k!$.

Problem 3. Let $\phi\colon R \to S$ be a map between rings preserving the operations (sum to sum, product to product, zero to zero, and one to one). Then we have a map

$$\phi_*\colon R[T] \longrightarrow S[T]$$

mapping a polynomial

$$f(T) = a_n T^n + \cdots + a_1 T + a_0 \in R[T],$$

to a polynomial

$$\phi_* f(T) = \phi(a_n)T^n + \cdots + \phi(a_1)T + \phi(a_0) \in S[T].$$

If this is the case, we say $f(T)$ **descends** to $\phi_* f(T)$, or $f(T)$ is a **lifting** of $\phi_* f(T)$.

Let $f(T)$ be a polynomial with coefficients in R. Say $r \in R$ is a **root** of $f(T)$ in R if $f(r) = 0$ in R. Say $s \in S$ is a **root** of $f(T)$ in S (through ϕ) if $\phi_* f(s) = 0$ in S.

(a) (2 pts) Show that, if $r \in R$ is a root of $f(T)$ in R, then $\phi(r)$ is a root of $f(T)$ in S.

If this is the case, we say r is a **lifting** of the root $\phi(r)$ of $f(T)$ to R.

(b) (3 pts) Give an example to show that even if $\phi\colon R \to S$ is subjective, NOT all roots in S can have a lifting in R.

Hint. Consider $R = \mathbb{Z}$, $S = \mathbb{Z}/m$ (for your favorite m), and ϕ the natural quotient map $\mathbb{Z} \to \mathbb{Z}/m$. Then consider a polynomial which have no roots in $\mathbb{Z}$.

Problem 4. In what follows, Let $f(T)$ be a polynomial with coefficients in $\mathbb{Z}$. Then for any positive integer m, we can talk about roots of $f(T)$ in $\mathbb{Z}/m$ (through the natural quotient map $\mathbb{Z} \to \mathbb{Z}/m$). In particular, we consider $m = p^e$, where p is a prime number and e is a positive integer.

(a) (4 pts) Show that, for any $a \in \mathbb{Z}$, we have

$$f(a + p^e T) \equiv f(a) + f'(a)p^e T \pmod{p^{2e}}.$$

(The congruence relation reads as saying both sides (as polynomials of T) descend to the same polynomial with coefficients in $\mathbb{Z}/p^{2e}$.) Note that this is a statement about polynomials not about integers.

Remark. This implies that $f(a + p^e t) \equiv f(a) + f'(a)p^e t \pmod{p^{2e}}$ for all $t \in \mathbb{Z}$.

(b) (5 pts) Finish proving the *Hensel's lemma*: if α is a root of $f(T)$ in $\mathbb{Z}/p^e$ and is NOT a root of $f'(T)$ in $\mathbb{Z}/p$, then there is a unique congruence class $\tilde{\alpha} \in \mathbb{Z}/p^{e+e'}$ (where $e' \leqslant e$) such that $\tilde{\alpha}$ is a lifting of the root $\alpha \in \mathbb{Z}/p^e$ of $f(T)$ to $\tilde{\alpha} \in \mathbb{Z}/p^{e+e'}$.

Hint. Read the lecture note. You can use the theorem on lifting multiplicative inverse.

In what follows, we fix a prime number p. 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.

(c) (3 pts) 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.

(d) (5 pts) Finish proving the following version of *Hensel's lemma*: if x_0 is an integer such that $p \mid f(x_0)$ but $p \nmid f'(x_0)$, 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 1.(f) to translate the statement in the language of congruence.

(e) (3 pts) Give an example to show that NOT every Cauchy sequence has a limit in $\mathbb{Q}$ with respect to the p-adic norm.

Hint. You may want to use problem 3.(b). Consider a sequence obtained from the Hensel's limit.