M3P14 MASTERY MATERIAL: p-ADIC INTEGERS AND HENSEL'S LEMMA

1. The p-adic integers

An observation we've used over and over again in this course is that if a diophantine equation has integer solutions, then it has solutions mod n for every n. One can thus rule out the existence of solutions to a diophantine equation if it has no solutions modulo n for some n, and the Chinese Remainder Theorem allows us to reduce to considering the cases where n is a prime power p^r. Conversely, if there is any hope at all of finding integer solutions to the equation, then it must have solutions mod p^r for every p and r.

It is therefore natural, given a diophantine equation and a prime p, to ask whether the equation has solutions modulo p^r for every r. We will see that in fact there is a single ring, called the ring $\mathbb{Z}_p$ of *p-adic integers*, such that a diophantine equation has a solution in $\mathbb{Z}_p$ if, and only if, it has solutions modulo p for every p.

Definition 1.1. Let p be a prime. A p-adic integer a is a sequence $a_1, a_2, \ldots$ such that:

- For each i, a_i is a congruence class in $\mathbb{Z}/p^i$, and
- For each i, $a_{i+1} \equiv a_i$ modulo p^i.

For example, if $p = 5$, the sequence:

$$2, 7, 57, 182, ...$$

defined by $a_1 = 2$, $a_i = a_{i-1} + 5^{i-1}$ if i is even, $a_i = a_{i-1} + 2 \cdot 5^{i-1}$ if i is odd is a 5-adic integer.

The p-adic integers form a ring, where if a represents the sequence $a_1, a_2, \ldots$, and b represents the sequence $b_1, b_2, \ldots$, then $a+b$ is the sequence $a_1+b_1, a_2+b_2, \ldots$, and ab is the sequence $a_1b_1, a_2b_2, \ldots$.

Exercise 1.2. Show that map $\mathbb{Z} \to \mathbb{Z}_p$ that takes an integer n to the sequence $n, n, n, \ldots$ is an injective ring homomorphism, so that we can regard $\mathbb{Z}$ as a subring of $\mathbb{Z}_p$. Show that the sequence $\alpha = 2, 7, 57, 182, \ldots$ defined above is equal to $\frac{-7}{24}$ in $\mathbb{Z}_5$ (that is, that $24\alpha + 7 = 0$ in $\mathbb{Z}_5$), so that this map is not surjective.

Henceforth we will regard $\mathbb{Z}$ as a subset of $\mathbb{Z}_p$ via the above inclusion.

Exercise 1.3. Show that the p-adic integers are uncountable. This gives another proof that they contain more than just the integers!

Exercise 1.4. Let $P(X)$ be a polynomial with integer coefficients. Show that if there exists $x \in \mathbb{Z}_p$ with $P(x) = 0$ then, for every $r > 0$, $P(X)$ has a root in $\mathbb{Z}/p^r$. (The converse is also true, but slightly tricky.)

Although the definition of p-adic integers as sequences of congruence classes is in some sense the most natural, there are a number of other useful ways to think about $\mathbb{Z}_p$. Let $a = a_1, a_2, \ldots$ be an element of $\mathbb{Z}_p$. We define the *p-adic absolute value* $|a|_p$ to be the real number p^{-r}, where r is the largest integer such that $a_r = 0$ in $\mathbb{Z}/p^r$. (Note than an element $a = a_1, a_2, \ldots$ of $\mathbb{Z}_p$ is divisible by p^r if, and only if $a_r = 0$ in $\mathbb{Z}/p^r$, so $|a|_p$ is the inverse of the largest power of p dividing a.) The p-adic distance between a, b in $\mathbb{Z}_p$ is given by the function $d(a, b) := |a - b|_p$.

Exercise 1.5. Show that the function $d(a, b)$ is a metric on $\mathbb{Z}_p$. It is called the p-adic metric on $\mathbb{Z}_p$. Show that $\mathbb{Z}$ is a dense subset of $\mathbb{Z}_p$ with respect to this metric.

Recall that a *Cauchy sequence* in a metric space X is a sequence $x_1, x_2, \ldots$ of elements of X such that, for all $\epsilon > 0$, there exists N_ϵ such that $|x_i - x_j| < \epsilon$ for all $i, j > N_\epsilon$. The space X is said to be *complete* if every Cauchy sequence in X converges (to a limit in X).

Exercise 1.6. For each i, let $a^{(i)}$ be the p-adic integer $a_1^{(i)}, a_2^{(i)}, \ldots$. Show that the sequence: $a^{(1)}, a^{(2)}, a^{(3)}, \ldots$ is Cauchy if, and only if, for all positive integers r, there exists N_r such that, for all $i \geq N_r$, we have $a_r^{(i)} = a_r^{(N_r)}$. Conclude that $\mathbb{Z}_p$ is complete.

We also recall that any metric space X has a *completion* $\hat{X}$. As a set, $\hat{X}$ is the set of equivalence classes of Cauchy sequences in X, where we say two sequences $x_1, x_2, \ldots$ and $y_1, y_2, \ldots$ are equivalent if $d(x_n, y_n)$ goes to zero as n goes to infinity. Then $\hat{X}$ inherits a metric from X that makes $\hat{X}$ into a complete metric space. Moreover, X embeds isometrically in $\hat{X}$ via the map that takes x to the equvalence class of the constant sequence $x, x, x, \ldots$. In some sense, $\hat{X}$ is the smallest complete metric space containing X.

Exercise 1.7. Show that $\mathbb{Z}_p$ is isomorphic to the p-adic completion of $\mathbb{Z}$; that is, the completion of $\mathbb{Z}$ when $\mathbb{Z}$ is considered a metric space via the p-adic metric. [Hint: given an element $a = a_1, a_2, \ldots$ of $\mathbb{Z}_p$, consider sequences $b_1, b_2, \ldots$ of integers such that $b_i \equiv a_i \pmod{p^i}$. Show that any such sequence is a Cauchy sequence in $\mathbb{Z}$, and that all such sequences (for a given a) are equivalent.]

This gives us another way to think about the p-adic integers, as a ring obtained by adding certain limits of sequences of integers to $\mathbb{Z}$. In particular we get a way to express p-adic integers as infinite sums:

Exercise 1.8. Show that every element of $\mathbb{Z}_p$ is expressible *uniquely* as an infinite sum:

$$\sum_{i=0}^{\infty} c_i p^i,$$

where, for each i, c_i is an integer such that $0 \leq c_i < p$.

In fact, convergence in the p-adics is rather nicer than convergence in the reals:

Exercise 1.9. Let $a_1, a_2, \ldots,$ be an infinite sequence of p-adic numbers, and suppose that $\lim_{i\to\infty} |a_i|_p = 0$. Show that the sum $\sum_{i=1}^{\infty} a_i$ converges in $\mathbb{Z}_p$.

Exercise 1.10. Define the power series $\exp_p(x)$ and $\log_p(1+x)$ by:

$$\exp_p(x) = \sum_{n=0}^{\infty} \frac{x^n}{n!}$$

$$\log_p(1+x) = \sum_{n=1}^{\infty} \frac{(-1)^{n+1} x^n}{n}.$$

Show that for $x \in \mathbb{Z}_p$, $\log_p(1+x)$ converges in $\mathbb{Z}_p$ when $|x|_p < 1$, and that $\exp_p(x)$ converges for $|x|_p < p^{-\frac{1}{p-1}}$. (For the latter, you will need to approximate the largest power of p dividing $n!$).

Exercise 1.11. (Optional, harder) Show that for $x \in \mathbb{Z}_p$, with $|x|_p$ sufficiently small, one has $\exp_p \log_p(1+x) = x$. Similarly, show that $\log_p \exp_p x = x$ for such x. (Note that the latter should be interpreted as the series obtained by substituting $\exp_p x - 1$ into the series for $\log_p x$.) Show further that $\exp_p(x+y) = (\exp_p x)(\exp_p y)$.

[HINT: show inductively that these relations hold mod p^n for every n.]

2. Hensel's Lemma

The fact that $\mathbb{Z}_p$ is complete is very useful for solving polynomial equations over $\mathbb{Z}_p$. In fact, one can often use a variant of Newton's method to turn mod p-solutions of a polynomial equation into p-adic solutions. This is the idea behind Hensel's Lemma.

Recall that if $P(X) = \sum_{i=0}^{d} c_i X^i$ is a polynomial with coefficients in a ring, then its derivative $P'(X)$ is the sum $\sum_{i=0}^{d-1} c_{i+1}(i+1)X^i$. We showed in class that $(PQ)' = P'Q + Q'P$, and that, if P has coefficients in $\mathbb{Z}/p$, and a is a root of P mod p, then $P'(a) = 0$ if, and only if, a is a double root of P.

Now let P be a polynomial with integer (or even p-adic) coefficients, and suppose a is a root of P mod p (i.e. $P(a) \equiv 0 \pmod{p}$.) Suppose further that $P'(a)$ is nonzero mod p.

Exercise 2.1. Show that, for a and c in $\mathbb{Z}$, and $i \geq 1$, we have $P(a+cp^i) \equiv P(a)+cP'(a)p^i \pmod{p^{i+1}}$. [Hint: first show this for monomials, then show that this implies the general case.]

Exercise 2.2. Inductively construct a sequence of integers a_i as follows: set $a_1 \equiv \alpha \pmod{p}$. Now show that for each i, there exists an a_{i+1} congruent to $a_i \bmod p^i$ such that $P(a_{i+1}) \equiv 0 \pmod{p^{i+1}}$. Show that the sequence $a_1, a_2, \ldots$ defines an element α of $\mathbb{Z}_p$ such that $P(\alpha) = 0$.

You have proven:

Theorem 2.3. *(Hensel's Lemma) Let P be a polynomial with coefficients in $\mathbb{Z}_p$, and a an integer such that $P(a)$ is zero mod p and $P'(a)$ is nonzero mod p. Then there exists α in $\mathbb{Z}_p$ such that $\alpha \equiv a$ (mod p) and $P(\alpha) = 0$.*

Exercise 2.4. Apply this technique to the polynomial x^2+1 and the root 2 of this polynomial mod 5 to obtain the first four terms of the series expansion for a square root of -1 in $\mathbb{Z}_5$.

Exercise 2.5. Use the technique of this section to show that there are 5 distinct fifth roots of -1 in $\mathbb{Z}_{11}$, and find the first three terms of the series expansion for the unique fifth root of -1 in $\mathbb{Z}_{11}$ that is congruent to 2 mod 11. (A calculator may be helpful.)