Hasse-Minkowski theorem, lec 2: p-adic integers

2.0) Introduction

Recall two equations from Section 0:

(2) $x_1^2 - 2x_2^2 + 3x_3^2 - 6x_4^2 = 0$

(3) $x_1^2 + x_2^3 + x_3^2 - 7x_4^2 = 0$

We claim that neither has nonzero solutions in $\mathbb{Q}^4$. Indeed, we can rescale & assume that $x_1, \dots, x_4$ are coprime integers. Then we claim that (2) has no coprime solutions modulo 9, while (3) has no coprime solutions mod 8. Let's elaborate on the latter. Any complete square is congruent to 1, 4, or 0 modulo 8. The equation becomes $\sum_{i=1}^{4} x_i^2 \equiv 0 \mod 8$, & since $x_i^2 \equiv 0, 1, 4 \mod 8$, all x_i have to be even contradicting the coprime assumption.

So we can ask the following vague question:

Question: What can solving polynomial equations modulo prime powers tell us about integer solutions?

Answer: this can give solutions that are "p-adic integers."

2.1) Reminder on residues mod p^k

Fix a prime number p. For $k \in \mathbb{Z}_{>0}$, let $\mathbb{Z}/p^k\mathbb{Z}$ denote the set of residues mod p^k. We'll think about them as elements of $\{0, 1, \dots p^k - 1\}$, i.e. possible remainders under division by p^k.

Given two residues $a, b \in \mathbb{Z}/p^k\mathbb{Z}$ we can add, subtract & multiply them in $\mathbb{Z}/p^k\mathbb{Z}$ e.g. $a \cdot b \in \mathbb{Z}/p^k\mathbb{Z}$ is defined as the unique element of $\{0, 1, \dots, p^k - 1\}$ congruent to the usual product of a, b as integers mod p^k. These operations have the usual properties of addition, subtraction & multiplication of integers: we have commutativity, associativity & distributivity rules, multiplying $a \in \mathbb{Z}/p^k\mathbb{Z}$ by the residue 1 gives a, etc.

Thanks to these operations it makes sense to plug elements of $\mathbb{Z}/p^k\mathbb{Z}$ into any polynomial from $\mathbb{Z}[x_1, \dots x_n]$. The result is a residue from $\mathbb{Z}/p^k\mathbb{Z}$

Division is more subtle: we can divide by all nonzero residues only for $k = 1$: for every $b, c \in \mathbb{Z}/p\mathbb{Z}$, $b \neq 0$ there's unique $a \in \mathbb{Z}/p\mathbb{Z}$ with $ab = c$ so we write $a = b^{-1}c$.

2.2) p-adic integers.

Definition: We say that a collection of residues $a(k) \in \mathbb{Z}/p^k\mathbb{Z}$ for $k \geq 1$ is compatible if $a(k+1) - a(k)$ is divisible by p^k $\forall$ $k \geq 1$. By a p-adic integer we mean any compatible collection of residues $(a(k))_{k \geq 1}$. The set of p-adic integers will be denoted by $\mathbb{Z}_p$.

Example: Every integer $a \in \mathbb{Z}$ gives a p-adic integer via $(a \bmod p^k)_{k \geq 1}$.

Sending $a \in \mathbb{Z}$ to $(a \bmod p^k)_{k \geq 1} \in \mathbb{Z}_p$ defines a map $\mathbb{Z} \to \mathbb{Z}_p$. It's injective: $a, b \in \mathbb{Z}$ have the same image $\Leftrightarrow$ $a - b \equiv 0 \bmod p^k$ $\forall$ $k \geq 1 \Leftrightarrow a = b$. We'll view $\mathbb{Z}$ as a subset of $\mathbb{Z}_p$ via this map.

The next important feature of $\mathbb{Z}_p$ is that it comes w. addition, subtraction & multiplication extending those on its subset $\mathbb{Z}$. For this notice that for two compatible sequences $a(k) \in \mathbb{Z}/p^k\mathbb{Z}$ & $b(k) \in \mathbb{Z}/p^k\mathbb{Z}$ $(k \geq 1)$ each of the following sequences is compatible: $(a(k) + b(k))_{k \geq 1}$, $(a(k) - b(k))_{k \geq 1}$,

$(a(k)b(k))_{k\geq 1}$, where the operations are done in $\mathbb{Z}/p^k\mathbb{Z}$ (e.g. $a(k+1)\equiv a(k)$, $b(k+1)\equiv b(k) \bmod p^k \Rightarrow a(k+1)b(k+1)\equiv a(k)b(k) \bmod p^k$)

We define the operations on $\mathbb{Z}_p$ accordingly, e.g.:

$(a(k))_{k\geq 1} + (b(k))_{k\geq 1} := (a(k)+b(k))_{k\geq 1}$.

These operations have the usual properties: commutativity, associativity, distributivity, etc. They also extend the usual operations on $\mathbb{Z}$ (exercise).

Here's a useful way to present p-adic numbers. Since $a(k+1)-a(k) : p^k$, $a(k)\in\{0,1,..,p^k-1\}$, $a(k+1)\in\{0,1,..,p^{k+1}-1\} \Rightarrow$ there's unique $a_k\in\{0,1,..p-1\}$ s.t. $a(k+1)=a(k)+a_k p^k$. So we get a sequence $a_i\in\{0,..p-1\}$ w. $i\geq 0$ s.t. $a(k)=\sum_{i=0}^{k-1} a_i p^i$. We will write the p-adic integer $(a(k))_{k\geq 1}$ as the infinite sum $\sum_{i=0}^{\infty} a_i p^i$. With this presentation non-negative integers go to their expansion base p, while for negative integers this is more subtle:

Examples: 1) We claim that $-1\in\mathbb{Z}\subset\mathbb{Z}_p$ is given by $\sum_{i=0}^{\infty}(p-1)p^i$. This boils down to checking that $-1\equiv\sum_{i=0}^{k-1}(p-1)p^i \bmod p^k$ $\forall\, k>0$, which follows b/c $\sum_{i=0}^{k-1}(p-1)p^i=\sum_{i=1}^{k-1}p^{i+1}-p^i=p^k-1$.

2) Let $p=3$ & consider the 3-adic integer $a=\sum_{i=0}^{\infty} 3^i$. Then $2a=\sum_{i=0}^{\infty} 2\cdot 3^i=[1)]=-1$. This a gives an example of a 3-adic integer, which does not lie in $\mathbb{Z}\subset\mathbb{Z}_3$: the equation $2a+1=0$ doesn't have integer solutions.

2.3) Invertible p-adic integers

An advantage of p-adic integers over the usual ones is that finding p-adic solutions to polynomial equations is easier: it's a recursive procedure.

Namely suppose we have a polynomial $f(x)$ w. coefficients in $\mathbb{Z}_p$ & we want to solve $f(x)=0$ in p-adic integers: find $x=\sum_{i=0}^{\infty} a_i p^i$ w. $f(\sum_{i=0}^{\infty} a_i p^i)=0$. For this we first solve $f(a_0)=0$ in $\mathbb{Z}/p\mathbb{Z}$. And once we found a solution $\sum_{i=0}^{k-1} a_i p^i$ to $f(x)=0$ in $\mathbb{Z}/p^k\mathbb{Z}$ we try to find $a_k\in\{0,\dots p-1\}$ so that $\sum_{i=0}^{k} a_i p^i$ solves $f(x)=0$ in $\mathbb{Z}/p^{k+1}\mathbb{Z}$, this boils down to an equation on a_k in $\mathbb{Z}/p\mathbb{Z}$.

We apply this reasoning to finding invertible p-adic integers: $b\in\mathbb{Z}_p$ s.t. $bx=1$ has solution in $\mathbb{Z}_p$ (auto-

matically unique: if x, y are solutions, then $y = y(bx) = (yb)x = x$.

Lemma: $b = \sum_{i=0}^{\infty} b_i p^i$ is invertible $\Leftrightarrow b_0 \neq 0$.

Proof: We need to find $a = \sum_{i=0}^{\infty} a_i p^i$ s.t. $ba = 1$, equivalently $\left(\sum_{i=0}^{k-1} b_i p^i\right)\left(\sum_{i=0}^{k-1} a_i p^i\right) \equiv 1 \bmod p^k \ \forall\, k \geq 1$. By what we recalled in Sec 2.1, there's unique $a_0 \in \{0, 1, \dots, p-1\}$ with $a_0 b_0 \equiv 1 \bmod p$. Now suppose we found $a_0, \dots, a_{k-1}$ s.t.

$$\left(\sum_{i=0}^{k-1} b_i p^i\right)\left(\sum_{i=0}^{k-1} a_i p^i\right) = 1 + p^k c \text{ for } c \in \mathbb{Z}$$

and want to find a_k from

$$1 \equiv \left(\sum_{i=0}^{k} b_i p^i\right)\left(\sum_{i=0}^{k} a_i p^i\right) \equiv 1 + p^k c + b_k a_0 p^k + b_0 a_k p^k \bmod p^{k+1}$$

$$\Leftrightarrow b_0 a_k \equiv -c - b_k a_0 \bmod p$$

The right hand side only contains numbers we already know and, since $b_0 \neq 0$ in $\mathbb{Z}/p\mathbb{Z}$, the last equation has a solution $a_k \in \{0, 1, \dots, p-1\}$, finishing the proof. □

Exercise: Explicitly (as $\sum_{i=0}^{\infty} a_i 3^i$) find $\frac{1}{2} \in \mathbb{Z}_3$.