

## p-adic Numbers

### Lecture 14

Robert F. Coleman

## 1 Hasse-Minkowski

**Lemma 1.1** *If  $n \in \mathbf{N}$ ,*

$$\sum_{x=1}^{p-1} x^n \equiv \begin{cases} 0 & \text{if } p-1 \nmid n \\ -1 & \text{if } p-1 \mid n \end{cases} \pmod{p}.$$

Why is it enough to assume  $a, b$  and  $c$  are coprime integers when solving the equation

$$ax^2 + by^2 + cz^2 = 0$$

over  $\mathbf{Q}$ ?

**Proposition 1.2** *Suppose  $p \neq 2$ , and  $a, b$  and  $c$  are coprime integers not divisible by  $p$ . Then the equation*

$$ax^2 + by^2 + cz^2 = 0$$

*has a non-trivial solution mod  $p$ .*

Proof. We use a “dastardly trick”. Let  $N$  be the number of solutions in  $\mathbf{F}_p^3$ . Then

$$N \equiv \sum_{(x,y,z) \in \mathbf{F}_p^3} (ax^2 + by^2 + cz^2)^{p-1} \pmod{p}.$$

If

$$(aX^2 + bY^2 + cZ^2)^{p-1} = \sum_{\substack{0 \leq i,j,k \leq p-1 \\ i+j+k=p-1}} A_{i,j,k} X^{2i} Y^{2j} Z^{2k},$$

for some  $A_{i,j,k} \in \mathbf{Z}$ ,

$$\sum_{(x,y,z) \in \mathbf{F}_p^3} (ax^2 + by^2 + cz^2)^{p-1} = \sum_{\substack{0 \leq i,j,k \leq p-1 \\ i+j+k=p-1}} A_{i,j,k} \sum_{(x,y,z) \in \mathbf{F}_p^3} x^{2i} y^{2j} z^{2k},$$

where we take  $x^0 = 1$  etc.

**Corollary 1.3** *If  $p$  is odd and  $p \nmid abc$*

$$ax^2 + by^2 + cz^2 = 0$$

*has a solution in  $\mathbf{Q}_p$ .*

Proof.

## 2 Homework

Do problems 126, 128 and 129.