Lecture 23 Some Diophantine geometry

Classical Diophantine consisted in finding the points of

$$V_I(\mathbb{Q}) := \{ P \in \mathbb{Q}^n \mid \forall f \in I : f(P) = 0 \},$$

where $I \leq \mathbb{Q}[X_1, \dots, X_n]$ is an ideal. It is useful to embed $V_I \hookrightarrow \mathbb{P}^n$ since the points of the closure V_I^{proj} of V_I in $\mathbb{P}^n$ may be taken with integral coordinates thus giving canonically

$$V_I^{proj}(\mathbb{Q}) \longrightarrow V_{\tilde{I}}^{proj}(\mathbb{F}_p)$$

$$(x_0 : x_1 : \dots : x_n) \mapsto (\tilde{x}_0 : \tilde{x}_1 : \dots : \tilde{x}_n)$$

Indeed,

$$V_I^{proj}(\mathbb{Q}) := \{ P = (x_0 : x_1 : \ldots : x_n) \in \mathbb{P}^n(\mathbb{Q}) \mid \forall f \in I^{hom} : f(P) = 0 \},$$

where $I^{hom} = \{ f^{hom} \in \mathbb{Q}[X_0, \ldots, X_n] \mid f \in I \}$,

$\underline{d = \deg(f)}$ $\quad f^{hom} := X_0^{\deg(f)} f\left(\frac{X_1}{X_0}, \ldots, \frac{X_n}{X_0} \right)$

is the homogeneous polynomial in $n+1$ variables att'd to f. Here

$$\mathbb{P}^n(\mathbb{Q}) := \left(\mathbb{Q}^{n+1} - \{0\}\right) / \mathbb{Q}^\times,$$

i.e. $(x_0 : x_1 : \ldots : x_n) = (x_0' : x_1' : \ldots : x_n') \Leftrightarrow (x_0, x_1, \ldots, x_n) = \alpha (x_0', x_1', \ldots, x_n')$, for some $\alpha \in \mathbb{Q}^\times$. Thus WLOG, P may be taken s.t. $x_1, \ldots, x_n \in \mathbb{Z}$.

Remark The existence of $P \in V_I^{proj}(\mathbb{Q})$ implies that

$$\forall \text{ prime number } p: \quad V_I^{proj}(\mathbb{F}_p) \neq \emptyset.$$

So a method to prove that $V_I^{proj}(\mathbb{Q}) = \emptyset$ may be furnished by attempting to find a prime p s.t. $V_I^{proj}(\mathbb{F}_p) = \emptyset$.

Thm (Ostrowski) If K_v is a completion of $\mathbb{Q}$ WRT an absolute value v, then either $K_v \cong \mathbb{R}$ or $K_v \cong \mathbb{Q}_p$, for some prime number p.

The finite fields $\mathbb{F}_p$ and $\mathbb{Q}_p$ are related as follows. Let

$$\mathbb{Z}_p := \{ x \in \mathbb{Q}_p \mid |x|_p \leq 1 \}$$

$$\mathfrak{m}_p := \{ x \in \mathbb{Q}_p \mid |x|_p < 1 \}.$$

Then $\mathbb{Z}_p$ is a local ring with maximal ideal $\mathfrak{m}_p$ and

$$\mathbb{Z}_p / \mathfrak{m}_p \cong \mathbb{F}_p$$

We thus have a natural map

$$V^{\text{proj}}(\mathbb{Q}_p) \longrightarrow V^{\text{proj}}(\mathbb{F}_p)$$

<u>Thm</u> (Hasse–Minkowski) Let C be a conic defined by an eq'n with coefficients in $\mathbb{Q}$. The following are equivalent

(i) $C(\mathbb{Q}) \neq \emptyset$

(ii) $\forall$ completion K_ν of $\mathbb{Q}$: $C(K_\nu) \neq \emptyset$.

<u>Remark</u> The above thm does not extend to cubics. Indeed, the Selmer cubic C, which is defined by

$$3x^3 + 4y^3 + 5z^3 = 0$$

is s.t. (ii) but it does not satisfy (i).