

## Diophantine Geometry: February 12, 2008

We start by recalling the following conjecture from last time:

**Conjecture 0.1.** *Define:*

$$c_{d,n} = \lim_{H \rightarrow \infty} \frac{\#\{f \in \mathbb{Z}[x_1, \dots, x_n] : |\text{coeff}(f)| \leq H, \deg f = d, \exists a \in \mathbb{Q}^n f(a) = 0\}}{\#\{f \in \mathbb{Z}[x_1, \dots, x_n] : |\text{coeff}(f)| \leq H, \deg f = d\}}$$

*then the limit exists and we have:*

$$\begin{aligned} c_{d,n} &> 0 \text{ if } d \leq n \\ c_{d,n} &= 0 \text{ if } d \geq n + 2 \end{aligned}$$

No conjecture for  $d = n + 1$ . For  $d \geq n + 2$ , this conjecture is supported by the following heuristic argument:

**Lemma 0.2.** *If  $\Lambda$  is a lattice in  $\mathbb{R}^n$ , that is  $\Lambda = \{a_1\lambda_1 + \dots + a_n\lambda_n \mid a_i \in \mathbb{Z}\}$ , where the  $\lambda_i$  are linearly independent, then:*

$$\#\{\lambda \in \Lambda : \|\lambda\| \leq H\} = cH^n + O(H^{n-1})$$

*where:*

$$c = \frac{\text{Vol}(S^n)}{\text{Vol}(\mathbb{R}^n/\Lambda)} \times \text{Something that depends on the norm.}$$

Thus, letting  $N = \binom{n+d}{d} - 1$ , we have for  $a \in \mathbb{Q}^n$ , there exists some constant  $c(a) > 0$  such that

$$\#\{f : |\text{coeff}(f)| \leq H, f(a) = 0\} = c(a)H^N + O(H^{N-1})$$

Using this lemma we see that:

$$\sum_{a \in A} \#\{f : |\text{coeff}(f)| \leq H, f(a) = 0\} = \sum_{a \in A} c(a)H^N + O(H^{N-1})$$

for  $A$  finite. If the error terms didn't matter this would give us:

$$\#\{f : |\text{coeff}(f)| \leq H, \exists a \in A, f(a) = 0\} \leq \sum_{a \in A} c(a)H^N$$

Now, for  $d > n + 1$ ,

$$\sum_{a \in \mathbb{Q}^n} c(a) < \infty$$

and

$$\#\{f : |\text{coeff}(f)| \leq H\} \approx cH^{N+1}$$

so:

$$\frac{\#\text{f with solutions}}{\#\text{total}} \leq \frac{\sum_a c(a)H^N}{cH^{N+1}} = \frac{\sum_a c(a)}{cH}$$

which goes to 0 as  $H \rightarrow \infty$ .

Let  $K$  be a field. We will define  $n$ -dimensional projective space over  $K$ :

$$\mathbb{P}^n(K) = \{(a_0, \dots, a_n) \in K^{n+1} : \exists i, a_i \neq 0\} / \sim$$

where the equivalence relation  $\sim$  is defined by identifying  $\mathbf{a} = (a_0, \dots, a_n)$  and  $\mathbf{b} = (b_0, \dots, b_n)$ , denoted  $\mathbf{a} \sim \mathbf{b}$  if there exists  $\lambda \in K^*$  such that  $\mathbf{a} = \lambda \mathbf{b}$ . The class of  $(a_0, \dots, a_n)$  is denoted  $(a_0 : \dots : a_n)$ .

For example, when  $K = \mathbb{Q}$  by the equivalence we see that we can represent every element of projective space as a vector of coprime integers in exactly 2 ways.

Suppose  $f \in K[x_0, \dots, x_n]$  is homogeneous of degree  $d$ , that is to say:

$$f(\lambda x_0, \dots, \lambda x_n) = \lambda^d f(x_0, \dots, x_n)$$

now if  $\mathbf{a} \sim \mathbf{b}$  we have that  $f(a) = \lambda^d f(b)$  thus:

$$f(a) = 0 \Leftrightarrow f(b) = 0$$

Thus the set of points in  $\mathbb{P}^n(K)$  where  $f$  (homogeneous) vanishes is well defined. Thus we can make the following definition:

**Definition 0.3.** *A projective algebraic set is the set of common zeros of a collection of homogeneous polynomials.*

Let  $\phi : K^n \hookrightarrow \mathbb{P}^n(K)$  be defined by  $\phi(a_1, \dots, a_n) = (1 : a_1 : \dots : a_n)$ .

If  $f \in K[x_1, \dots, x_n]$  is any polynomial define:

$$\bar{f} = f\left(\frac{x_1}{x_0}, \dots, \frac{x_n}{x_0}\right) \in K[x_0, x_1, \dots, x_n]$$

which is homogeneous. If  $X = \{f_1 = \dots = f_m = 0\} \subset \mathbb{A}^n$  then we can define the algebraic set  $\bar{X} = \{\bar{f}_1 = \dots = \bar{f}_m = 0\} \subset \mathbb{P}^n$  called the projective closure of  $X$  such that:

$$\phi(X(K)) = \bar{X}(K) \cap \phi(K^n)$$

The points of  $\bar{X} - \phi(X)$  are called the points at infinity of  $\bar{X}$ .

Consider

$$f(x, y) = 0$$

so

$$\bar{f} = z^d f\left(\frac{x}{z}, \frac{y}{z}\right)$$

and  $\bar{f} = 0$  defines a curve in  $\mathbb{P}^2$ . The solutions to  $\bar{f}(x, y, 0) = 0$  are points at infinity.

**Example 0.4.** *Consider:*

$$y^2 = x^3 + ax + b$$

$$y^2 z = x^3 + axz^2 + bz^3$$

so the points at infinity correspond to  $z = 0$  which implies  $x^3 = 0$  or  $x = 0$ . So  $(0 : y : 0) \sim (0 : 1 : 0)$  is the point at infinity.

A line in  $\mathbb{P}^2(K)$  is the set of zeros of a linear homogeneous polynomial  $L$ .

**Theorem 0.5.** *Let  $P, Q \in \mathbb{P}^2(K)$   $P \neq Q$  then there exists a unique line  $L$  that contains  $P$  and  $Q$ . Given  $L_1$  and  $L_2$  lines in  $\mathbb{P}^2$  and  $L_1 \neq L_2$  then there exists a unique point  $P \in L_1 \cap L_2$ .*

*Proof.* let  $P = (a_0 : a_1 : a_2)$  and  $Q = (b_0 : b_1 : b_2)$

then:

$$\det \begin{pmatrix} x_0 & x_1 & x_2 \\ a_0 & a_1 & a_2 \\ b_0 & b_1 & b_2 \end{pmatrix} = 0$$

is a line containing  $P$  and  $Q$ .

For the second part notice that the solutions to  $\sum a_i x_i = 0$  and  $\sum b_i x_i = 0$  is a 1-dimensional vector space, so this defines a unique point in  $\mathbb{P}^2(K)$ .

□

If  $X \subseteq \mathbb{P}^2$  is a cubic then given  $P, Q \in X(K)$  there is a unique line  $\overline{PQ}$  through them. Usually  $\overline{PQ}$  meets  $X(K)$  at a third point. (Also, usually the tangent at  $P$  also meets  $X(K)$  in a new point). This allows us to usually produce new points from given points. The iteration of this process is known as the chord-tangent process.

**Theorem 0.6.** *(Mordell-Weil) Let  $X/K$  be a smooth cubic. If  $K$  is a global field then there exists a finite set  $G \subseteq X(K)$  such that  $X(K)$  can be obtained from  $G$  by the chord-tangent process.*