

# Notes on Diophantine Geometry

Herivelto Borges

January 31, 2008

## Lecture 3

Last time we proved Legendre's Theorem. We can restate it in a form suitable for generalization.

**Theorem 1.** *A conic defined over  $\mathbb{Q}$  has a  $\mathbb{Q}$ -rational point if and only if it has a  $\mathbb{Q}_p$ -rational point for all  $p$ ,  $p$  prime or  $p = \infty$ .*

We will see that checking  $p$ -adic solubility is easy. Here are some (chronological) remarks.

Minkowski: A quadric (hypersurface of degree 2) has a point over  $\mathbb{Q}$  if and only if it has point over  $\mathbb{Q}_p$  for all  $p$ .

Meyer: A quadric of  $\dim \geq 4$  always has points over  $\mathbb{Q}_p$ , if  $p \neq \infty$  (clearly we can always find a quadric with no real points).

Hasse: Generalized Legendre and Minkowski to number fields and function fields (global fields). He formulated what is now called the Hasse Principle: Solutions over  $\mathbb{Q}_p$  for all  $p$  implies solution over  $\mathbb{Q}$ . It is not universally true but it is true for certain families of equations.

**Definition.** An absolute value on a field  $K$  is a map

$$|\cdot| : K \rightarrow \mathbb{R}$$

such that

1.  $\forall x \in K, |x| \geq 0$  and  $|x| = 0 \Leftrightarrow x = 0$ .
2.  $|xy| = |x||y| \quad \forall x, y \in K$ .

$$3. |x + y| \leq |x| + |y| \quad \forall x, y \in K.$$

**Example 1.** The “usual” absolute value on  $\mathbb{Q}$  is

$$|x|_\infty = \begin{cases} x, & \text{if } x \geq 0 \\ -x, & \text{if } x < 0 \end{cases}$$

$|\cdot|_p$  is the  $p$ -adic absolute value defined last lecture.

There is also the trivial absolute value :

$$|\cdot|_0 = \begin{cases} 1, & \text{if } x \neq 0 \\ 0, & \text{if } x = 0 \end{cases}$$

**Definition.** Two absolute values on  $K$  are equivalent if they induce the same topology.

**Theorem 2.** (Ostrowski) Every absolute value in  $\mathbb{Q}$  is equivalent to  $|\cdot|_p$  for some  $p$ ,  $p$  prime,  $p = \infty$  or  $p = 0$ .

If  $K/\mathbb{Q}$  is finite extension (i.e.  $K$  is a number field), then for each absolute value  $|\cdot|$  on  $\mathbb{Q}$  there is only a finite number of equivalence classes of absolute values on  $K$  that gives  $|\cdot|$  when restricted to  $\mathbb{Q}$ . We denote by  $M_K$  the set of equivalence classes of absolute values on  $K$ . If  $v \in M_K$ , then, there exists  $p = \text{prime}, 0$  or  $\infty$  such that  $|x|_v = |x|_p \forall x \in \mathbb{Q}$ . We say that  $v|p$  ( $v$  divides  $p$ ).

Product Formula: if  $x \in \mathbb{Q}$  and  $x \neq 0$ , then

$$\prod |x|_p = 1$$

To see this, we write  $x = \pm p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ ,  $\alpha_i \in \mathbb{Z}$ ,  $p_i$  prime, and notice that

$$|x|_p = \begin{cases} 1 & \text{if } p \neq p_i, \infty \\ p^{-\alpha_i} & \text{if } p = p_i \\ p_1^{\alpha_1} \cdots p_r^{\alpha_r} & \text{if } p = \infty \end{cases}$$

The product formula can be generalized to a number field  $K$ .

There is a choice of  $n_v \in \mathbb{Z}$ , for  $v \in M_K$ , such that  $\forall x \in K, x \neq 0$

$$\prod_v |x|_v^{n_v} = 1$$

In  $\mathbb{F}_q(t)$  there are absolute values corresponding to each irreducible polynomial in  $\mathbb{F}_q[t]$ . If  $x = p(t)^r \frac{a(t)}{b(t)}$ , where  $a(t), b(t), p(t) \in \mathbb{F}_q[t]$ ,  $p(t)$  is irreducible and  $p(t) \nmid a(t)b(t)$ , then we define  $v_{p(t)}(x) = r$  and

$$|x|_{p(t)} = q^{-r \deg p(t)}$$

For  $x = \frac{a}{b}$ ,  $a, b \in \mathbb{F}_q[t]$  and  $(a, b) = 1$ , we have

$$|x|_\infty = q^{\deg(a) - \deg(b)}$$

For instance,  $|\frac{1}{t}|_\infty = \frac{1}{q}$ .

Using valuation to define an absolute value, we have a way of writing the product formula eliminating the constant:

For  $x = p^r \frac{a}{b} \in \mathbb{F}(t)$ ,  $p$  irreducible and  $p \nmid ab$ , we set

$v_p(x) = r$  and  $|x|_p = c^{-v_p(x) \deg p}$  ( $c > 1$ ), and then

$$\prod |x|_p = 1 \Leftrightarrow \prod c^{-v_p(x) \deg p} = 1 \Leftrightarrow \sum v_p(x) \deg p = 0$$

Notice that the last part is just expressing the fact that for any rational function we have # zeros=#poles.

The previous discussion was intended to introduce the following result.

**Theorem 3.** (*Hasse-Minkowski*) *If  $K$  is a global field then a quadric defined over  $K$  has  $K$ -rational points if and only if it has  $K_v$ -rational points for all  $v \in M_K$ .*

The next theorem will be proved later on.

**Theorem 4.** *Let  $X$  be an absolutely irreducible algebraic variety over a global field  $K$ . Then  $X(K_v) \neq \emptyset$  for all but finitely many  $v \in M_K$ . Moreover, the exceptional  $v$  can be effectively listed.*

**Theorem 5.**  *$f(x_1, \dots, x_n) \in \mathbb{Z}[x_1, \dots, x_n]$  non-constant and absolutely irreducible. Then for all but finitely many primes  $p$ , and for all  $r \geq 0$ , there exist solutions to*

$$f(x_1, \dots, x_n) \equiv 0 \pmod{p^r}$$

**Definition.** If  $\mathcal{X}$  is a collection of varieties defined over a global field  $K$ , then we say that  $\mathcal{X}$  satisfy the Hasse principle if  $\forall X \in \mathcal{X}$

$$X(K) \neq \emptyset \iff X(K_v) \neq \emptyset \quad \forall v \in M_K$$

Big question: Which families satisfies the Hasse principle?

We know the following:

- Hasse-Minkowski: Quadrics satisfy the Hasse principle .
- Hooley, Heath Brown: Cubics in  $\geq 8$  variables satisfy the Hasse principle (over  $\mathbb{Q}$ ).

Question: Which varieties in  $\geq 3$  variables do not satisfy the Hasse principle?

It is known that  $3x^3 + 4y^3 + 5 = 0$  has points in  $\mathbb{Q}_p$  for all  $p$  but does not have a rational point and there is an example with three variables as well. The case of cubics with 4, 5, 6 and 7 variables is open.