

**NOTES ON DIOPHANTINE GEOMETRY**  
**FEBRUARY 5, 2008**

CHIA-LIANG SUN, NING KANG

Correction for last time:

Let  $F(t)$  be the field of rational functions over a field  $F$ . For any irreducible polynomial  $p$  in  $F[t]$ , define  $v_p : F(t) \rightarrow \mathbb{Z} \cup \{\infty\}$  by setting  $v_p(0) = \infty$ , and  $v_p(f) = m$ , where  $f = p^m a/b$ , and  $a$  and  $b$  are in  $F[t]$  and both coprime to  $p$ .

Also, define  $v_\infty : F(t) \rightarrow \mathbb{Z} \cup \{\infty\}$  by setting  $v_\infty(0) = \infty$ , and  $v_\infty(\frac{a}{b}) = \deg b - \deg a$ , where  $a$  and  $b$  are in  $F[t]$ .

Let  $S$  be the set of all monic irreducible polynomials in  $F[t]$ . The correct sum formula is that for any  $f \in F(t) \setminus \{0\}$ ,

$$v_\infty(f) + \sum_{p \in S} v_p(f) \deg p = 0.$$

Note that this sum involves only finitely many non-zero terms.

**Theorem 1.** *Let  $f \in \mathbb{Z}[x_1, \dots, x_n]$  be absolutely irreducible. Then for all but finitely many primes  $p$ , there is a solution to the equation  $f = 0$  in  $\mathbb{Z}_p^n$ .*

*Remark.* The proof given below works for any global field.

*Outline of Proof.* Step 1: If  $f \in \mathbb{Z}[x_1, \dots, x_n]$  is absolutely irreducible, then  $f \in (\mathbb{Z}/p\mathbb{Z})[x_1, \dots, x_n]$  is absolutely irreducible for all but finitely many primes  $p$ .

Step 2: If  $f$  is absolutely irreducible in  $(\mathbb{Z}/p\mathbb{Z})[x_1, \dots, x_n]$  and  $p$  is large with respect to  $\deg f$  and  $n$ , then the variety defined by  $f = 0$  has a smooth point in  $(\mathbb{Z}/p\mathbb{Z})^n$ .

Step 3: If the variety defined by  $f = 0$  has a smooth point in  $(\mathbb{Z}/p\mathbb{Z})^n$ , then it has a point in  $\mathbb{Z}_p^n$ .

*Proof.* Step 1: If  $f \in \mathbb{Z}[x_1, \dots, x_n]$  is absolutely irreducible, then  $f \in (\mathbb{Z}/p\mathbb{Z})[x_1, \dots, x_n]$  is absolutely irreducible for all but finitely many primes  $p \in \mathbb{N}$ .

Let  $d = \deg f$ . Fix  $d \geq 2$  and  $n \geq 1$ . Let us think a polynomial of degree  $d$  in  $n$  variables as a vector of its coefficients; in this way, we can identify the set of polynomials of degree  $d$  in  $n$  variables with the vector space  $V_{n,d}$  of dimension  $N = \binom{n+d}{n}$ . Under this identification, we define the map  $\phi_k : V_{n,k} \times V_{n,d-k} \rightarrow V_{n,d}$ , where  $1 \leq k \leq d-1$ , by  $(g, h) \mapsto gh$ , where  $g$  and  $h$  are polynomials in the same  $n$  variables with  $\deg g = k$ ,  $\deg h = n-k$ , and  $gh$  is the product of  $g$  and  $h$  as polynomials. By the formula of multiplication of polynomials in terms of their coefficients, the image of  $\phi_k$  is an algebraic set in the  $N$ -dimensional affine space  $V_{n,d}$ , so is the union  $U$  of the image of  $\phi_k$  over  $1 \leq k \leq d-1$ . Therefore  $U$  is the set of common zeros  $(c_1, \dots, c_N)$  of some  $F_1, \dots, F_r \in \mathbb{Z}[y_1, \dots, y_N]$ . This means that  $f$  factors nontrivially if and only if  $F_1 = \dots = F_r = 0$  at  $f \in V_{n,d}$ , that is, the coefficients of  $f$  satisfies the polynomial equations  $F_1 = \dots = F_r = 0$  in  $N$  variables. In fact, the polynomial equations can be written explicitly in some case as the following exercise shows.

**Exercise.** Let  $f(x, y) = a_1x^2 + a_2xy + a_3y^2 + a_4x + a_5y + a_6$  be a polynomial of degree 2 over a field whose characteristic is not 2. Then  $f$  factors nontrivially if and only if

$$\det \begin{pmatrix} a_1 & \frac{a_2}{2} & \frac{a_4}{2} \\ \frac{a_2}{2} & a_3 & \frac{a_5}{2} \\ \frac{a_4}{2} & \frac{a_5}{2} & a_6 \end{pmatrix} = 0$$

By the assumption that  $f \in \mathbb{Z}[x_1, \dots, x_n]$  is absolutely irreducible, there must be some  $F_i$  which does not vanish at  $f$ . Since the coefficients of  $F_i$  and  $f$  are all in  $\mathbb{Z}$ ,  $F_i(f)$  is a nonzero rational integer. Hence  $F_i(f) \neq 0$  in  $\mathbb{Z}/p\mathbb{Z}$  for all but finitely many primes  $p$ , which implies that  $f \in (\mathbb{Z}/p\mathbb{Z})[x_1, \dots, x_n]$  is absolutely irreducible for those prime since the construction of  $F_1, \dots, F_r$  passes naturally through quotients.

*Remark.* The classical algebraic geometry works only on algebraically closed fields, hence in the priori the coefficients of  $F_1, \dots, F_r$  are in  $\bar{\mathbb{Q}}$ . However the elimination theory ensure that we can get  $F_1, \dots, F_r$  in  $\mathbb{Q}[y_1, \dots, y_N]$ , hence in  $\mathbb{Z}[y_1, \dots, y_N]$  by clearing denominators.

*Remark.* There is a similar statement for smoothness: If the variety  $X$  is smooth, then  $X \bmod p$  is smooth for all but finitely many primes  $p$ .

Let  $X$  be defined by the polynomial equation  $f(x_1, \dots, x_n) = 0$ . We say  $X$  is not smooth if there is  $c = (c_1, \dots, c_n)$  such that

$$f(c) = \frac{\partial f}{\partial x_i}(c) = 0, \quad i = 1, \dots, n.$$

For this to be true, there must be a relation among the coefficients of  $f$ . For cubics to be singular, it needs at least one condition for the coefficients; for them to be reducible, it needs at least two conditions for the coefficients.

If  $X$  is smooth, primes  $p$  with  $X \bmod p$  smooth is called the primes of good reduction (associated with  $X$ ).

Now let us get some geometric intuition about good or bad reductions. As mentioned in the beginning of semester, in order to see the geometry, we have to work on algebraically closed fields. Thus let  $F$  be an algebraically closed field and  $R = F[t]$ ,  $K = F(t)$ . Since  $F$  is algebraically closed, the prime ideals in  $R$  are of the form  $(t - c)R$  with  $c \in F$ . Thus the set of prime ideals in  $R$  can be identified with  $F$ . In this case,  $F[t]$  plays the role of  $\mathbb{Z}$ , and  $F$  plays the role of the set of primes  $p \in \mathbb{N}$ . Now consider a polynomial  $f \in R[x_1, \dots, x_n]$ , i.e. the coefficients of  $f$  are in  $F[t]$ . We write  $f$  as  $f_t$  to indicate the dependence. For any  $c \in F$ , the element  $f \in (R/(t - c)R)[x_1, \dots, x_n]$  is simply  $f_c$ ; this corresponds the algebraic set  $V_c$  defined by  $f_c = 0$  in the  $n$ -dimensional affine space. The primes of good reduction corresponds the points  $c \in F$  such that  $V_c$  is smooth. In this context, one can show the set of all  $c \in F$  such that  $V_c$  is not smooth is closed in the Zariski topology of  $F$ , hence is finite. Step 1 is the corresponding statement when  $F[t]$  is replaced by  $\mathbb{Z}$ .

In general, if we do not assume that  $F$  is algebraically closed, the primes of  $F[t]$  corresponds the monic irreducible polynomials, which can be identified with the Galois orbits of elements in the algebraic closure of  $F$ .

Step 2: If  $f$  is absolutely irreducible in  $(\mathbb{Z}/p\mathbb{Z})[x_1, \dots, x_n]$  and  $p$  is large with respect to  $\deg f$  and  $n$ , then the variety defined by  $f = 0$  has a smooth point in

$(\mathbb{Z}/p\mathbb{Z})^n$ .

To show this, we use the Lang-Weil estimate (which we do not prove):

**Theorem 2.** *Given  $n \geq 1$ ,  $d \geq 1$ , there are constants  $C(n, d)$ ,  $C_1(n, d)$  such that for any primes  $q$  and any absolute irreducible  $f \in \mathbb{F}_q[x_1, \dots, x_n]$  with degree  $d$ ,*

$$|\#\{p \in \mathbb{F}_q^n \mid f(p) = 0\} - q^{n-1}| \leq C(n, d)q^{n-\frac{3}{2}} + C_1(n, d)$$

Hyperplane sections reduce to  $n = 2$  which is due to Hasse-Weil. (Function field analogues of the Riemann Hypothesis)

Fact:  $C(2, d) = (d-1)(d-2)$

To do Step 2, we want a solution  $c \in (\mathbb{Z}/p\mathbb{Z})^n$  to  $f = 0 \pmod{p}$  with  $\frac{\partial f}{\partial x_i}(c) \not\equiv 0 \pmod{p}$  for some  $i$ .

Lang-Weil gives that the number of solution to  $f = 0 \pmod{p}$  is about  $p^{n-1}$ . Solutions to  $f = 0 \pmod{p}$ ,  $\frac{\partial f}{\partial x_1} = 0 \pmod{p}$  must satisfy  $\text{Res}_{x_n}(f, \frac{\partial f}{\partial x_1}) = 0$ , a equation in  $x_1, \dots, x_{n-1}$ . The latter one has about  $p^{n-2}$  solutions by Lang-Weil; and given one of its solution  $x_1, \dots, x_{n-1}$ , there are at most  $d$  values for  $x_n$  with  $f(x_1, \dots, x_n) = 0$ . Hence we conclude the number of solutions to  $f = \frac{\partial f}{\partial x_1} = 0 \pmod{p}$  is at most  $d(p^{n-2} + C(n-1, d)p^{n-\frac{5}{2}} + C_1(n-1, d))$ . For  $p$  large enough, this is less than  $p^{n-1} - C(n, d)q^{n-\frac{3}{2}} - C_1(n, d)$ , which is a lower bound of the number of solution to  $f = 0 \pmod{p}$ . Therefore, for  $p$  large enough, there exists a solution to  $f = 0 \pmod{p}$  which is not a solutions to  $\frac{\partial f}{\partial x_1} = 0 \pmod{p}$ . Step 2 is done.