

**NOTES ON DIOPHANTINE GEOMETRY**  
**FEBRUARY 7, 2008**

CHIA-LIANG SUN, NING KANG

We continue the proof of the following theorem.

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

Under the given assumption, we have established the following consequences:

1.  $f \in (\mathbb{Z}/p\mathbb{Z})[x_1, \dots, x_n]$  is absolutely irreducible for all sufficiently large primes  $p$ .
2. For all sufficiently large primes  $p$ , the variety defined by  $f = 0$  has a smooth point in  $(\mathbb{Z}/p\mathbb{Z})^n$ .

The final step is to turn the smooth point in  $(\mathbb{Z}/p\mathbb{Z})^n$  of the variety defined by  $f = 0$  to a  $p$ -adic point.

Essentially we want to prove Hensel's Lemma:

**Lemma 1.** *(Hensel) Suppose  $f \in \mathbb{Z}[x]$  and  $a \in \mathbb{Z}$  is such that  $f(a) \equiv 0 \pmod{p}$  and  $f'(a) \not\equiv 0 \pmod{p}$ . Then there exists an  $\alpha \in \mathbb{Z}_p$  such that  $\alpha \equiv a \pmod{p}$  and  $f(\alpha) = 0$ .*

*Remark.* Note that the assumption  $f(a) \equiv 0 \pmod{p}$  is equivalent to  $|f(a)|_p < 1$ ; the assumption  $f'(a) \not\equiv 0 \pmod{p}$  is equivalent to  $|f'(a)|_p = 1$ ; the conclusion asserts that there exists an  $\alpha \in \mathbb{Z}_p$  such that  $|\alpha - a|_p < 1$  and  $f(\alpha) = 0$ . Therefore Hensel's Lemma is an analogue to the Newton's method of finding zeros of differentiable functions on the real line.

*Proof.* First we prove by induction on  $n$  that there exist  $a_n \in \mathbb{Z}$  such that  $a_n \equiv a_{n-1} \pmod{p^{n-1}}$  for  $n \geq 2$ , and  $f(a_n) \equiv 0 \pmod{p^n}$  and  $f'(a_n) \not\equiv 0 \pmod{p}$  for  $n \geq 1$ . Letting  $a_1 = a$ , we have the base case for free. As for inductive steps, we want to find  $z \in \mathbb{Z}$  such that  $f(a_{n-1} + zp^{n-1}) \equiv 0$  and  $f'(a_{n-1} + zp^{n-1}) \not\equiv 0 \pmod{p}$ , therefore we can put  $a_n = a_{n-1} + zp^{n-1}$ .

Write  $f(x) = \sum_{i=0}^d c_i x^i$ . Observe the equality

$$f(a_{n-1} + zp^{n-1}) = f(a_{n-1}) + f'(a_{n-1})zp^{n-1} + \frac{f''(a_{n-1})}{2!}(zp^{n-1})^2 + \dots + \frac{f^{(d)}(a_{n-1})}{d!}(zp^{n-1})^d.$$

We claim  $f(a_{n-1} + zp^{n-1}) \equiv f(a_{n-1}) + zp^{n-1}f'(a_{n-1}) \pmod{p^n}$  by showing  $\frac{f^{(k)}(c)}{k!} \in \mathbb{Z}$  for any  $c \in \mathbb{Z}$  and  $1 \leq k \leq d$ . Note that  $\frac{f^{(k)}(c)}{k!} = \sum_{i=k}^d \frac{i(i-1)\dots(i-k+1)}{k!} c_i c^{i-k}$ , and that  $\frac{i(i-1)\dots(i-k+1)}{k!} = \binom{i}{k} \in \mathbb{Z}$ , which proves the claim.

Now I want to find  $z \in \mathbb{Z}$  such that  $f(a_{n-1}) + zp^{n-1}f'(a_{n-1}) \equiv 0 \pmod{p^n}$ . By inductive hypothesis  $f(a_{n-1}) \equiv 0 \pmod{p^{n-1}}$ , we write  $f(a_{n-1}) = up^{n-1}$  for some

$u \in \mathbb{Z}$ . Therefore we aim to find  $z \in \mathbb{Z}$  so that  $(u + zf'(a_{n-1}))p^{n-1} = 0 \pmod{p^n}$ , i.e.  $u + zf'(a_{n-1}) = 0 \pmod{p}$ . By inductive hypothesis  $f'(a_{n-1}) \not\equiv 0 \pmod{p}$ , such  $z \in \mathbb{Z}$  can be therefore found. Since

$$f'(a_{n-1} + zp^{n-1}) = f'(a_{n-1}) + f''(a_{n-1})zp^{n-1} + \frac{f^{(3)}(a_{n-1})}{2!}(zp^{n-1})^2 + \dots + \frac{f^{(d)}(a_{n-1})}{(d-1)!}(zp^{n-1})^d$$

and we have shown that  $\frac{f^{(k)}(c)}{k!} \in \mathbb{Z}$  for any  $c \in \mathbb{Z}$  and  $1 \leq k \leq \deg f$ , we conclude that  $\frac{f^{(k)}(a_{n-1})}{(k-1)!} \in \mathbb{Z}$  for  $2 \leq k \leq \deg f$ , and  $f'(a_{n-1} + zp^{n-1}) = f'(a_{n-1}) \not\equiv 0 \pmod{p}$ . Therefore we put  $a_n = a_{n-1} + zp^{n-1}$  and complete the inductive step.

Now we have a sequence  $\{a_n\}_{n \geq 1}$  of integers with the stated properties. We claim  $\{a_n\}_{n \geq 1}$  forms a Cauchy sequence in the  $p$ -adic norm. To see this, we apply the strong triangular inequality: for any  $n > m$ ,

$$|a_n - a_m|_p = \left| \sum_{i=m}^{n-1} (a_{i+1} - a_i) \right|_p \leq \max\{|a_{i+1} - a_i|_p : m \leq i \leq n-1\} \leq p^{-m} \rightarrow 0$$

as  $m \rightarrow \infty$ . So there exists  $\alpha \in \mathbb{Z}_p$  such that  $a_n \rightarrow \alpha$  as  $n \rightarrow \infty$ , which implies  $f(a_n) \rightarrow f(\alpha)$  as  $n \rightarrow \infty$  since polynomials are continuous. We have also  $f(a_n) \equiv 0 \pmod{p^n}$ , which implies  $f(a_n) \rightarrow 0$  as  $n \rightarrow \infty$ , and therefore  $f(\alpha) = 0$ .

**Example.**  $f(x) = x^2 + 1$ ,  $p = 5$

$$a_1 = a = 2$$

$$f(2) = 5 = 0 \pmod{5}$$

$$f'(2) = 4 \not\equiv 0 \pmod{5}$$

$$a_2 = 2 + 5z_2$$

$$f(2 + 5z_2) = 5 + 2 \cdot 2 \cdot 5z_2 + 5^2z_2^2 = 5(1 + 4z_2) + 5^2z_2^2 = 0 \pmod{5^2} \Rightarrow z_2 = 1$$

$$a_3 = 7 + 5^2z_3$$

$$f(7 + 5^2z_3) = 50 + 2 \cdot 7 \cdot 5^2z_3 + 5^4z_3^2 = 5^2(2 + 14z_3) + 5^4z_3^2 = 0 \pmod{5^3} \Rightarrow z_3 = 2$$

Question: How to write negative rational integer as  $p$ -adic numbers?

Answer: For example, we have  $-1 \equiv p^n - 1 = (p-1)(1+p+p^2+\dots+p^{n-1}) \pmod{p^n}$ . Thus as a  $p$ -adic number,  $-1 = (p-1)(1+p+p^2+\dots)$ . Alternatively, using a bomb to kill an ant, we may apply Hensel's Lemma to the polynomial  $x + 1$  in order to write  $-1$  a  $p$ -adic number.

To turn a solution  $(a_1, \dots, a_n) \in (\mathbb{Z}/p\mathbb{Z})^n$  of  $f = 0$  and  $\frac{\partial f}{\partial x_i} \neq 0$  for some  $i$  into a  $p$ -adic one, simply apply Hensel's Lemma to  $f(a_1, \dots, a_{i-1}, x, a_{i+1}, \dots, a_n) \in \mathbb{Z}[x]$ . Then we have an  $\alpha \in \mathbb{Z}_p$  such that  $(a_1, \dots, a_{i-1}, \alpha, a_{i+1}, \dots, a_n)$  is a  $p$ -adic solution to  $f = 0$ . This completes the proof of Theorem 1.

Examining the proof of Theorem 1, we discuss how large the prime  $p$  needs to be in each step.

In Step 1, we want  $f \in (\mathbb{Z}/p\mathbb{Z})[x_1, \dots, x_n]$  to be absolutely irreducible. This require that  $p$  is so large that does not divide an integer which depends only on coefficients of  $f$ .

In Step 2, we want a smooth point in  $(\mathbb{Z}/p\mathbb{Z})^n$  of the variety defined by  $f = 0$ . This require that  $p$  is so large in terms of the degree of  $f$  and the number of its variables that the Lang-Weil estimate gives a smooth solution of  $f = 0$ .

In Step 3, Hensel's Lemma can be applied for those primes  $p \in \mathbb{N}$  which a smooth solution in  $(\mathbb{Z}/p\mathbb{Z})^n$  is found in Step 2. This does not require the primes to be larger further.

Next, we investigate the question: How likely is it that an  $f \in \mathbb{Z}[x_1, \dots, x_n]$  has zeros in  $\mathbb{Z}_p^n$  for all primes  $p$ ?

**Theorem 2.** *For any  $n \geq 1$ ,  $d \geq 1$  and  $H \geq 1$ , let  $A_{n,d,H}$  be the set of polynomials in  $\mathbb{Z}[x_1, \dots, x_n]$  with total degree  $d$  whose coefficients are no bigger than  $H$  in their absolute values; let  $B_{n,d,H}$  be the set of polynomials in  $A_{n,d,H}$  such that for any prime  $p$  they have a zero in  $\mathbb{Z}_p^n$ . Then we have*

$$\lim_{H \rightarrow \infty} \frac{\#B_{n,d,H}}{\#A_{n,d,H}} > 0 \quad \text{if } n \geq 2, d \geq 2 \text{ and } (n, d) \neq (2, 2).$$

*Proof.* We count "bad" polynomials in each of three steps in the proof of Theorem 1.

In Step 3, no bad polynomial is there.

In Step 1, for  $n \geq 2, d \geq 2$  and  $(n, d) \neq (2, 2)$ , the subspace of reducible polynomials has codimension at least 2 in the space of polynomials of total degree  $d$  in  $n$  variables. So there are at least 2 numbers that need to be divisible by  $p$  in order for a polynomial in  $\mathbb{Z}[x_1, \dots, x_n]$  to be reducible in  $(\mathbb{Z}/p\mathbb{Z})[x_1, \dots, x_n]$ . Thus the probability of a polynomial in  $\mathbb{Z}[x_1, \dots, x_n]$  being bad modulo  $p$  is no bigger than  $\frac{1}{p^2}$ . Equivalently, the probability of a polynomial in  $\mathbb{Z}[x_1, \dots, x_n]$  being good modulo  $p$  is no less than  $1 - \frac{1}{p^2}$ . Hence the probability of a polynomial in  $\mathbb{Z}[x_1, \dots, x_n]$  being good, i.e., good modulo any primes  $p \in \mathbb{N}$ , is no bigger than  $\prod_p (1 - \frac{1}{p^2}) = \frac{6}{\pi^2} > 0$ . Of course this is a heuristic argument.

In Step 2, given fixed  $n$  and  $d$ , all but finitely many primes  $p \in \mathbb{N}$  are good for all polynomials in  $\mathbb{Z}[x_1, \dots, x_n]$  with total degree  $d$ . For each  $q$  of finitely many good primes, the probability of a polynomial in  $\mathbb{Z}[x_1, \dots, x_n]$  having a smooth zero is at least

$$\text{Prob} \left( f(0, \dots, 0) = 0 \pmod{q}, \frac{\partial f}{\partial x_1}(0, \dots, 0) \neq 0 \pmod{q} \right) = \frac{1}{q} \left(1 - \frac{1}{q}\right) > 0.$$

Again, this is a heuristic argument.

**Conjecture.** *Smooth hypersurfaces of degree  $d$  in  $n$  variables for  $d \leq n$  and  $n \geq 4$  satisfy the Hasse Principle.*

**Conjecture.** *Let  $A_{n,d,H}$  be as in Theorem 2, and  $B'_{n,d,H}$  be the set of polynomials in  $A_{n,d,H}$  which admits a zero in  $\mathbb{Q}^n$ . Then*

$$\lim_{H \rightarrow \infty} \frac{\#B'_{n,d,H}}{\#A_{n,d,H}} = \begin{cases} C_{n,d} > 0 & \text{if } d \leq n \\ ? & \text{if } d = n + 1 \\ 0 & \text{if } d \geq n + 2. \end{cases}$$