IV.1

Lecture IV

C. Skinner

Yesterday: solving equations modulo p (ie. field $\mathbb{Z}/p$) and theorem of Chevalley-Warning.

Corollary (of Chevalley-Warning's th)

If the constant term of F is zero, then there exists a solution $\underline{a} \neq 0$ to $F(\underline{a}) = 0$ $(s > \deg F)$.

(proof)

Constant term $= 0$ means $F(\underline{0}) = 0$ so $\#\{\text{solutions}\}$:

then $\#\{\text{solutions}\} \geq p$.

Examples: (1) $ax^2 + by^2 + cz^2$

$(p \geq 2)$ (2) $\sum_{1 \leq i, j \leq s} a_{ij} x_i x_j$ $s \geq 3$

(3) $a_1 x_1^k + \quad + a_s x_s^k$ $s \geq k+1$.

In each of these examples there exists a solution to $F(\underline{x}) = 0$ with not all $x_i = 0$.

— o —

Move on to solving equations modulo p^k

IV.2

$\mathbb{Z}/p^k$ is a ring (not a field if $k > 1$)

p is not invertible

~~the only thing not invertible~~.

$(\mathbb{Z}/p^k)^\times$ = residue class of integers not divisible by p

and $\# (\mathbb{Z}/p^k)^\times = \varphi(p^k) = (p-1)p^{k-1}$.

Important remark:

If $F(x_1, x_2 \ldots x_s) \in \mathbb{Z}[x_1, x_2 \ldots x_s]$ then any $\underline{a} = (a_1, a_2 \ldots a_s) \in \mathbb{Z}^s$ s.t.

$F(\underline{a}) = 0$ gives a solution

$$\underline{a}^{(k)} \in (\mathbb{Z}/p^k)^s \text{ to } F(\underline{x}) = 0 \pmod{p^k}$$

(where $\underline{a}^{(k)} = (a_1 \bmod p^k, \ldots, a_s \bmod p^k)$)

Note that, if the solution mod p^k come from the same $\mathbb{Z}$-solution they are "compatible":

$$\underline{a}^{(k)} \equiv \underline{a}^{(k-1)} \bmod p^{k-1}$$

(they are the reductions of the same solution $\underline{a} \in \mathbb{Z}^s$)

Lemma (Hensel's lemma I)

Let $F(x) \in \mathbb{Z}[x]$. Suppose $a_0 \in \mathbb{Z}$ such that

$F(a_0) \equiv 0 \bmod (p^{k-1})$ (new notation $F(a_0) \equiv 0\ (p^{k-1})$)

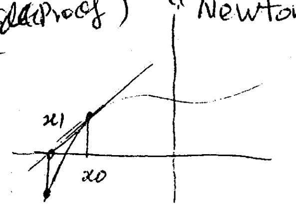
Then there exists $a \in \mathbb{Z}$ s.t.

$F(a) \equiv 0 (p^k)$ and $a \equiv a_0 (p^{k-1})$

if $F'(a_0) \not\equiv 0\ (p)$ (i.e. $F'(a_0) \in (\mathbb{Z}/p^{k-1})^\times$)

~~Moreover a is uniquely determined modulo p~~

(~~Idea~~ Proof) "Newton's method"



If x_0 is not a critical point the linear approximation has a zero x_1 and repeating the process one gets a sequence converging to a zero.

Moreover a is uniquely determined ~~by~~ modulo p^k

and $F'(a) \equiv F'(a_0) \bmod p$.

(The proof is constructive: gives a formula for a and can go from a solution mod p^{k-1} to a solution mod p^k, to a solution mod $p^{k+1}, \ldots$)

<u>Proof</u>

Key observation: $(a_0 + p^{k-1} b)^n$

$$= a_0^n + n a_0^{n-1} p^{k-1} b + \underbrace{\sum_{i \geq 2}^{n} \binom{n}{i} a_0^{n-i} (p^{k-1} b)^i}_{p^{2(k-1)} g_n(b)}$$

$g_n \in \mathbb{Z}[x]$

This means

$$F(a_0 + p^{k-1} b) = F(a_0) + F'(a_0) p^{k-1} b + p^{2(k-1)} G(b)$$

$G(x) \in \mathbb{Z}[x]$

and modulo p^k

one has $F(a_0 + p^{k-1} b) \equiv F(a_0) + F'(a_0) p^{k-1} b \ (p^k)$

~~so~~ we ~~want~~ ~~to solve~~

$$F(a_0) + F'(a_0) p^{k-1} b \equiv 0 \ p^k$$

for b

By hypothesis $p^{k-1} / F(a_0)$

so can take $b \equiv \left(-\frac{F(a_0)}{p^{k-1}}\right) F'(a_0)^{-1} \bmod (p)$

Then $a \equiv a_0 + p^{k-1} b$ satisfies

$F(a) \equiv 0 \pmod{p^k}$ and $a \equiv a_0 \pmod{p^{k-1}}$

<u>Note</u>
- b is determined up mod p (so it's determine a mod p^k)
- proof $F'(a) \equiv F'(a_0) \bmod p$ (exercise)

<u>Example</u>: $F(x) = x^2 + 1$

$p = 5$

$a_0 = 2$ $\quad$ a_0 solution modulo 5

Now let's find a s.t. $a^2 \equiv -1 \ (5^2)$
$a \equiv 2 \ (5)$

$a = a_0 + 5b$ $\quad$ $b = -\left(\frac{5}{5}\right) 4 = -4$

$F'(x) = 2x$

$F'(a_0) = 4$ $\quad$ ($F'(a_0)^{-1}$ mod 5 is 4)

$a = 2 + 5(-4) = -18 \equiv 7 \ (5^2)$

$7^2 = 49 \equiv -1 \ (25)$

(Note that, beginning with $a_0 = -2$ one gets another ~~four~~ solution a, different mod p^k to the one obtained from $a_0 = 2$ since they are distinct modulo p!!)

Can apply Hensel's lemma to equations with more than one variable

Example: $x^2+y^2 \cancel{+} 3 \equiv \bmod (5^k)$

First solve modulo 5 $(x,y)=(1,1)$

Fix y s.t. $y \equiv 1 \bmod (5)$ eg $Y=1$

Consider $x^2+1+3 \equiv 0 \pmod{5^k}$

Hensel's lemma gives a solution to

$\cancel{x^2} \quad x^2+4 \equiv 0 \bmod (5^k)$

st. $x_0 \equiv 1 \bmod (5)$

then $(x_0, 1)$ will be a solution

to $\underline{x^2+y^2+3 \equiv 0 \pmod{5^k}}$

$\stackrel{e}{=}$ In fact, with this procedure, we loose the UNICITY

Point: Can often specialize all but one of the variables to end up in a situation to which Hensel's lemma applies.

Application:

Let $F(x_1, x_2 \; x_s) = a_1 x_1^n + \cdots + a_s x_s^n$

s.t. $p \nmid a_1 \cdots a_s$, $s > n$ and $p \nmid n$

Then there exists ~~a non zero solution~~

$\underline{c} = (c_1 \, c_2 \; c_s)$

such that $F(\underline{c}) \equiv 0 \bmod p^k$

and some c_i is not divisible by p.

Why?

Chevalley - Warning theorem gives a solution modulo p, a non zero, solution modulo p

$0 \neq \underline{c}^{(0)} = (c_1^{(0)}, \ldots, c_s^{(0)})$

Assume $c_1^{(0)}$ is not divisible by p $(c_1^{(0)} \not\equiv 0 \bmod (p))$

to choose $c_2, \ldots, c_s \in \mathbb{Z}$ s.t.

$c_i \equiv c_i^{(0)} \pmod{p} \quad i \geq 2$

Consider the polynomial

$f(x) = a_1 x^n + a_2 c_2^n + \quad + a_s c_s^n$

then $c_1^{(0)}$ is a solution to $f(x) \equiv 0 \bmod (p)$

To apply Hensel's lemma we need to

know $f'(c_1^{(0)}) \not\equiv 0\ (p)$

But $f'(x) = a_1 n x^{n-1}$ not divisible by p.

so we are done ...

IV.5