Dinsdag 12/07/2011 Rouen

Yesterday: solving equations modulo p equivalently: (equations in the finite field $\mathbb{Z}/p$)

Then (Chevalley – Warning)

Let $F(x_1, \dots, x_s) \in \mathbb{Z}/p[x_1 \dots x_s]$

If $s > \deg F$, then $p \mid \#\{\underline{a} = (a_1 \dots a_s) \in (\mathbb{Z}/p)^s : F(\underline{a}) = 0\}$

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

Proof: Constant term is 0; means $F(\underline{0}) = 0$.

So $\# \{-\} \geq 1$, then $\Rightarrow \# \{\ \} \geq p$. □

Example: $p \geq 2$

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

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

(3) $a_1 x_1^k + \dots + a_s x_s^k$ $\quad s \geqslant k+1$

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

Move on to solving equations modulo powers of a prime $\pmod{p^k}$

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

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

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

If $F(x_1, \dots, x_s) \in \mathbb{Z}[x_1 \dots x_s]$ then any $\underline{a} = (a_1, \dots a_s) \in \mathbb{Z}^s$ such that $F(\underline{a}) = 0$ gives a solution

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

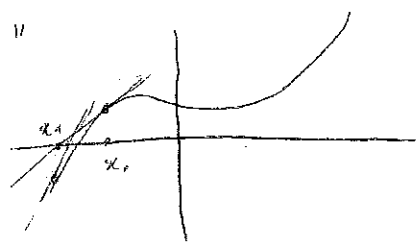
$(a_1 \bmod p^k, \dots, a_s \bmod p^k)$

Note $\underline{a}^{(k)} \equiv \underline{a}^{(k-1)} \bmod p^{k-1}$ since 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 $F(a_0) = 0 \quad (p^{k-1})$ then there exists $a \in \mathbb{Z}$ such that $F(a) = 0 \quad (p^k)$ and $a \equiv a_0 \quad (p^{k-1})$ if $F'(a_0) \not\equiv 0 \quad (p)$ (i.e. $F'(a_0) \in (\mathbb{Z}/p^{k-1})^\times$)

["Newton's method"



]

Moreover a is uniquely determined modulo p^k and $F'(a) = F'(a_0) \bmod p$

Proof is constructive : gives a formula for a.

Can go from a solution $\bmod p^{k-1}$
to a solution $\bmod p^k$
to a solution $\bmod p^{k+1}$
⋮ ⋮ ⋮

Proof : key observation :

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

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

This means

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

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

So $F(a_0 + p^{k-1}b) = F(a_0) + F'(a_0)p^{k-1}b \quad (p^k)$

So we want to solve

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

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

so we can take

$$b \equiv \left(-\frac{F(a_0)}{p^{k-1}}\right) F'(a_0)^{-1} \pmod{p}$$

inverse modulo p (i.e. in $\mathbb{Z}/p$)

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

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

Example: $F(x) = x^2 + 1 \qquad p = 5$

$a_0 = 2 \qquad 2^2 + 1 = 5 \equiv 0 \quad (5)$

Now let's find a such that $a^2 \equiv -1 \quad (5^2)$ and $a \equiv 2 \quad (5)$

$a = a_0 + 5b \qquad b \equiv -\left(\frac{5}{5^2}\right)\frac{1}{4} \equiv -4$

$F'(x) = 2x \qquad a \equiv 2 + 5(-4) \equiv -18 \equiv 7 \quad (5^2)$

$F'(a_0) \equiv 4 \qquad 7^2 = 49 \equiv -1 \quad (25)$

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

Ex: $x^2 + y^2 + 3 \equiv 0 \bmod 5^k$

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

Fix y such that $y \equiv 1 \pmod 5$ e.g. $y = 1$

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

Hensel's lemma produces a solution to $x^2 + 4 \equiv 0 \pmod{5^k}$ such that $x_0 \equiv 1 \pmod 5$

Then $(x_0, 1)$ will be a solution to $x^2 + y^2 + 3 \equiv 0 \pmod{5^k}$

point: can often specialise all but one of the variables to end up in a situation to which Hensel's lemma applies

Application: let $F(x_1, \dots, x_s) = a_1 x_1^n + \dots + a_s x_s^n$ such that $p \nmid a_1 \dots a_s$ as $s > n$, $p \nmid n$

Then there exists $\underline{c} = (c_1, \dots, c_s)$ such that $F(\underline{c}) \equiv 0 \bmod p^k$ + some c_i is not divisible by p.

Why? Chevalley-Warning Theorem gives a solution modulo p.

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

Renumbering variables if necessary, we can assume $c_1^{(0)} \not\equiv 0 \pmod p$

So choose $c_1 \dots c_s \in \mathbb{Z}$ such that $c_i \equiv c_i^{(0)} \pmod p$

Consider the polynomial $f(x) = F(x, c_2 \dots c_s)$ $i \geq 2$

To apply Hensel's lemma we need to know

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

$f'(x) = \underbrace{a_1 n}\, x^{n-1}$

↳ not divisible by p.