11/July/2011

notes by Jorge Miranda

The Diophantine Problem:

- Given a polynomial $F(x_1, \dots, x_n) \in \mathbb{Z}[x_1, \dots, x_n]$, does there exist $\underline{a} = (a_1, \dots, a_n) \in \mathbb{Z}^n$ such that $F(\underline{a}) = 0$?

Ex: $x^2+y^2=z^2$
$x^3+y^3=z^3$
$x^n+y^n=z^n$

Can replace $\mathbb{Z}$ with:
- $\mathbb{Q}$
- $\mathbb{C}$ (easier)
- $\mathbb{F}_p$

If $F(\underline{a})=0$, then

(*) $F(\underline{a}) \equiv 0 \pmod{N}$

for any integer N

so solving (*) modulo every N is a necessary condition for having an integer solution.

Ex (1): $x^2-3y^2=2$
If it had a solution then $x^2 \equiv 2 \pmod 3$, so no solutions.

(2): $x^2-3y^2=7$
- mod 3 – have solutions
- mod 4 : $x^2 \equiv 0,1 \pmod 4$
(or mod 7) y^2

(3) $x^3+y^3+z^3=0$ considering modulo 9
$\Rightarrow 3 \mid xyz$

Chinese Remainder Theorem:

$$N = N_1 \cdots N_r \ , \ \gcd(N_i, N_j) = 1 \ , \ i \neq j$$

$\mathbb{Z}/N$ = residue classes modulo N, (ring)

$\mathbb{Z}/N = \mathbb{Z}/N\mathbb{Z}$

$$\mathbb{Z}/N \xrightarrow{\sim} \mathbb{Z}/N_1 \times \cdots \times \mathbb{Z}/N_r$$

$$a \bmod N \mapsto (a \bmod N_1, \ldots, a \bmod N_r) = (a_1, \ldots, a_r)$$

<u>ex</u>: $N = \pm p_1^{e_1} \cdots p_r^{e_r}$ (prime factorization)

$\Rightarrow$ By Chinese Remainder Theorem, to have a solution to (*) modulo every N, it is enough to have a solution modulo <u>all prime powers</u> p^k, p prime, $k \geq 1$.

Congruences modulo p (p a prime)

- $\mathbb{Z}/p$ is a field (the finite field with p elements)

$0 \neq x \in \mathbb{Z}/p$, consider $\mathbb{Z}/p \xrightarrow{\phi} \mathbb{Z}/p$

$$a \mapsto ax$$

<u>want to know</u>: there exists a s.t. $ax \equiv 1$

This will be true if ϕ injective since <u>$\mathbb{Z}/p$ is finite</u>

If $ax \equiv 0$ (i.e. $p \mid ax$), then either $a \equiv 0$ or $x \equiv 0$.
But $x \not\equiv 0$ by hyp., so $a \equiv 0$, and ϕ is injective.

<u>Useful fact</u>: Let K be a field

A polynomial $f(x) = a_0 + a_1 x + \dots + a_{d-1} x^{d-1} + x^d$, $a_i \in K$
has <u>at most</u> d zeros in K.

<u>Proof</u>: By induction on d.

If $f(\alpha)=0$, $f(x) = (x-\alpha) g(x)$ with $\boxed{\deg g = d-1}$.

<u>ex</u>: $x^2 \equiv 1 \pmod p \rightarrow x^2 - 1 = 0$ in $\mathbb{Z}/p$
only zeros $x = \pm 1$

$x^2 \equiv -1 \pmod p \rightarrow x^2 + 1 = 0$ in $\mathbb{Z}/p$

- $p=2$: 1 solution
- $p=3$: no solutions
- $p=5$: 2 solutions

$(\mathbb{Z}/p)^\times$ = units in $\mathbb{Z}/p$ (everything $\neq 0$ for prime p)

- group under multiplication
- order $p-1$

Claim: Cyclic group of order $p-1$

<u>Proof</u>: As an <u>abstract group</u>

$$(\mathbb{Z}/p)^\times \simeq \mathbb{Z}/q_1^{a_1} \times \dots \times \mathbb{Z}/q_r^{a_r} \overset{\text{If } q_i \text{ distinct (CRT)}}{\simeq} \mathbb{Z}/\textstyle\prod q_i^{a_i}$$

q_i primes, $a_i \geq 1$ (not a priori distinct).

If $\underbrace{q_1 = q_2}_{q}$, then there are at least q^2 elements of order $| q$ in $(\mathbb{Z}/_p)^\times$, i.e., there would be q^2 solutions to $x^q \equi 1$ (contradiction) $\boxed{?}$

$(\mathbb{Z}/_p)^\times$ is a cyclic group of order $p-1$

Any generator g is called a <u>primitive root</u> modulo p

$(\mathbb{Z}/_p)^\times = \{g, g^2, \dots, g^{p-1} = 1\}$

<u>Ex</u>:
Suppose a is a solution of

$x^2 \equiv -1 \pmod p$

Then $a^2 \not\equiv 1$ in $(\mathbb{Z}/_p)^\times$, but $a^4 = 1$ in $(\mathbb{Z}/_p)^\times$ $(p \neq 2)$

This means that a has order 4 in $(\mathbb{Z}/_p)^\times$, and this happens <u>if and only if</u> $4 | p-1$ (if $a = g^{\frac{p-1}{4}}$, g a primitive root)

<u>Theorem</u> (Chevalley-Warning)

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

If $s > \deg F$, then

$p \,|\, \#\{\underline{a} = (a_1, \dots, a_s) \in (\mathbb{Z}/_p)^s : F(\underline{a}) = 0\} =$ number of solutions to $F=0$

Ex: $ax^2 + by^2 + cz^2 \equiv 0$

- $\deg = 2$ $\quad (x,y,z) = (0,0,0)$ one solution
- $s = 3 > \deg$ $\implies$ must have another root by theorem

<u>Key Lemma:</u> Let $r \geq 0$ be an integer, Then

$$\sum_{x \in \mathbb{Z}/p} x^r = \begin{cases} p-1 & \text{if } p-1 \mid r \\ 0 & \text{otherwise} \end{cases}$$

<u>Proof:</u> Let g be primitive root in $(\mathbb{Z}/p)^\times$

Then

$$\sum_{x \in \mathbb{Z}/p} x^r = \sum_{x \in (\mathbb{Z}/p)^\times} x^r = \sum_{i=0}^{p-2} g^{ir} = \begin{cases} \dfrac{g^{r(p-1)} - 1}{g^r - 1} \overset{g^{p-1} - 1 \equiv 0}{\equiv} 0 & \text{if } p-1 \nmid r \\ \sum_{i=0}^{p-2} 1 = p-1 & \text{if } p-1 \mid r \end{cases}$$

<u>Proof of Theorem:</u>

$$F(\underline{a})^{p-1} \equiv \begin{cases} 0 & \text{if } F(\underline{a}) \equiv 0 \\ 1 & \text{if } F(\underline{a}) \not\equiv 0 \end{cases}$$

$$\sum_{\underline{a} \in (\mathbb{Z}/p)^s} 1 - (F(\underline{a}))^{p-1} \equiv \# \{ \underline{a} \in (\mathbb{Z}/p)^s : F(\underline{a}) \equiv 0 \}$$

$$\parallel$$

$$\sum_{\underline{a} \in (\mathbb{Z}/p)^s} G(\underline{a}) \quad \text{where } G(x_1, \dots, x_s) = 1 - F(x_1, \dots, x_s)^{p-1}$$

$$\deg G \leq (p-1) \deg F$$

G is a sum of monomials of the form

$I \subseteq \{1, \dots, s\}$,

$\prod_{i \in I} x_i^{d_i}$. $\sum_{i \in I} d_i \leq \deg G \leq (p-1)\deg F$
$< (p-1)\Delta$

$\sum_{\underline{a}} \prod_{i \in I} a_i^{d_i}$

<u>Two cases</u>: • $I = \{1, \dots, s\}$: some $d_i < p-1$ (<u>use Key Lemma</u>)

• $I \neq \{1, \dots, s\}$, $\sum_{a \in \mathbb{Z}/p} 1 = p$

---

what's coming up?

- Congruences modulo p^k, $k > 1$
- Introduce p-adic integers $\mathbb{Z}_p$ as a way of looking at congruences modulo all powers of p <u>at once</u>.
- p-adic numbers $\mathbb{Q}_p$
- equations / $\mathbb{Z}_p$ + $\mathbb{Q}_p$