Lecture II

C. Skinner

The Diophantine Problem

Given a polynomial $F(X_1, \ldots X_n) \in \mathbb{Z}[X_1, \ldots X_n]$,

does there exist $\underline{a} = (a_1, \ldots a_n) \in \mathbb{Z}^n$ such that $F(\underline{a}) = 0$.

Ex: $x^2+y^2=z^2$, $x^3+y^3=z^3$, $\ldots$ $x^n+y^n=z^n$.

There is no algorithm answering this question.

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

If we have a solution $F(\underline{a})=0$ then $F(\underline{a}) \equiv 0 \bmod (N)$ for any integer N

so: a necessary condition for solving the problem is solubility modulo N, for any integer N.

Ex (1) $x^2-3y^2=2$

If it had a solution then $x^2 \equiv 2 \bmod (3)$, so no solution

(2) $x^2-3y^2=7$ mod 3. have solutions

mod 4 $x^2, y^2 \equiv 0, 1 \bmod (4)$ then $(x^2+y^2 \not\equiv 3 \bmod (4))$

& mod 7

(3) $X^3+y^3+z^3=0 \Rightarrow$ 3 divides xyz

(impossible modulo 9)

Chinese Remainder Theorem

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

$\mathbb{Z}/N$: residue class modulo N.

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

$$a \bmod (N) \longrightarrow (a \bmod (N_1), \ldots, a \bmod (N_r))$$

In particular, injective ... $\exists a$

$$a \equiv a_i \bmod (N_i) \quad i = 1, \ldots, r.$$

conclusion

Ex $N = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ prime factorization.

One need to find all solutions mod (p^{α_i}).

(by the Chinese remainder theorem).

Congruence modulo p (p prime)

$\mathbb{Z}/p$ is a field

$0 \neq x \in \mathbb{Z}/p$ under $\mathbb{Z}/p \longrightarrow \mathbb{Z}/p$ what x

$a \longmapsto ax$ $\quad ax = 1$

injective $\Leftrightarrow$ injective. no one needs to prove

$$ax = 0 \Rightarrow a = 0$$

$\bmod p$ p prime.

$p \mid ax \Rightarrow (p \mid a$ or $p \mid x)$

Useful fact. Let k be a field. A polynomial

$$f(x) = a_0 + a_1 x + \cdots + a_{d-1} x^{d-1} + x^d$$

has at most d zeros in k.

proof By induction on d.

If $f(\alpha) = 0$ then $f(x) = (x - \alpha) g(x)$

with $\deg g \leq d - 1$.

Ex $x^2 \equiv 1 \bmod (p)$ $\quad x^2 - 1 = 0$ in $\mathbb{Z}/p$

only two solutions $x = \pm 1$

$x^2 \equiv -1 \bmod (p)$ $\quad x^2 + 1 \equiv 0$ in $\mathbb{Z}/p$

$p = 2$ one solution

$p = 3$ not solution

$p = 5$ two solutions. $(2, 3)$

$(\mathbb{Z}/p)^\times$: units in $\mathbb{Z}/p$

group under multiplication of order $p - 1$.

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

Proof: As an abstract group $(\mathbb{Z}/p)^\times$ is a product of cyclic groups $(\mathbb{Z}/p)^\times \simeq \mathbb{Z}/q_1^{\alpha_1} \times \cdots \times \mathbb{Z}/q_r^{\alpha_r}$

with q_i prime (not necessarily distinct).

(If q_i intersect, by the C.R.T. we are done).

if $q_1 = q_2$ then there are at least q^2 elements of order q in $(\mathbb{Z}/q)^\times$

We used here q^2 solutions of

$$x^2 = 1 \pmod p$$ (contradiction)

$q_i \neq q_j \xrightarrow[(CRT)]{} (\mathbb{Z}/p)^\times$ cyclic. ∎

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

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

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

i.e.

Suppose a is a solution to

$$x^2 \equiv -1 \bmod p. \qquad p \neq 2$$

Then $a^2 \neq 1$ but in $(\mathbb{Z}/p)^\times$

but $a^4 = 1$ in $(\mathbb{Z}/p)^\times$

$\Rightarrow$ a has <u>order 4</u> in $(\mathbb{Z}/p)^\times$

happens if and only if $4 \mid p-1$.

<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 divides

$$\#\{\underline{a} = (a_1, a_2 \dots a_s) \in (\mathbb{Z}/p)^s : F(\underline{a}) = 0\}$$

(The number can be zero!)

In particular, if you have one solution there are more...

<u>Ex</u>: $ax^2 + by^2 + cz^2 = 0$

$\deg = 2 \qquad s = 3 > \deg$

$(0,0,0)$ one solution, so must have another by the theorem.

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

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

(Proof) Let g be a primitive root of $(\mathbb{Z}/p)^\times$

Then

$$\sum_{x \in \mathbb{Z}/p} x^r = \sum_{x \in (\mathbb{Z}/p)^\times} x^r = 0 + g^r + g^{2r} + \dots + g^{(p-2)r}$$

($x \neq 0$!)

$$= \sum_{i=0}^{p-2} g^{ri} = \frac{g^{r(p-1)} - 1}{g^r - 1} = 0$$

If $(p-1) \mid r \Rightarrow x^r \equiv 1 \bmod (p)$

$\Rightarrow \sum x^r = p-1.$ (Recall $g^{p-1} \equiv 1 \bmod (p)$)

(proof of theorem)

$$F(\underline{a})^{p-1} \equiv \begin{cases} 0 & \text{if } F(\underline{a}) = 0 \\ 1 & \text{if } F(\underline{a}) \neq 0 \end{cases}$$

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

$$\| \quad \text{where } G(x_1, \dots, x_s) = 1 - F(x_1, \dots, x_s)^{p-1}$$

$$\sum_{\underline{a} \in (\mathbb{Z}/p)^s} G(\underline{a}) \qquad \deg G = (p-1) \deg F$$

G is a sum of monomials of the

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

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

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

two cases: $I = \{1, 2, \dots, s\}$ key lemma.

$I \neq \{1, 2, \dots, s\}$ easy $\sum_{a \in \mathbb{Z}/p} 1 = p$

what's coming up?

II.4

- congruences modulo p^k, $k > 1$
- Introduce p-adic integers $\mathbb{Z}_p$ as a way of looking at congruences modulo powers of p at once.
- p-adic numbers $\mathbb{Q}_p$
- equation over $\mathbb{Z}_p$ & $\mathbb{Q}_p$.