Lecture 28: Solving equations over $\mathbb{Z}_p$

Recall Motivation: Diophantine Equations

Thm: $f \in \mathbb{Z}[x_1, \dots, x_n]$. Then $f(x_1, \dots, x_n) = 0$ has a sol'n mod p^k for all k $\iff$ it has a sol'n with $x_i \in \mathbb{Z}_p$.

Pf: ($\Leftarrow$) Follows from the ring hom $\mathbb{Z}_p \longrightarrow \mathbb{Z}/p^n\mathbb{Z}$,

$$(a_k) \longmapsto a_n$$

($\Rightarrow$) For notational simplicity, suppose there's only one variable, i.e. $f(x) \in \mathbb{Z}[x]$.

Set $S_k = \{a \in \mathbb{Z}/p^k\mathbb{Z} \mid f(a) = 0\}$, which is nonempty.

Idea: If $a = (a_1, a_2, a_3, \dots) \in \mathbb{Z}_p$ with $a_k \in S_k$, then $f(a) = 0$.

[Can't just pick a_k at random from S_k as need $a_{k+1} \equiv a_k \bmod p^k$. Will use an inductive construction ("compactness")]

For $S = \bigcup_{k=1}^{\infty} S_k$, we have $\pi_1 : S \to S_1$.

$$a \longmapsto a \bmod p$$

Choose $a_1 \in S_1$ so that $\pi_1^{-1}(a_1)$ is infinite.

i.e. $\exists$ ∞-many pairs $(k, a_k \in S_K)$ s.t. $a_k \equiv a_1 \bmod p$.

Can do since $S = \bigcup_{b_1 \in S_1} \pi^{-1}(b_1)$.

infinite $\quad$ finite

Similarly, choose $a_2 \in S_2$ so that

① $a_2 \equiv a_1 \bmod p$ $\quad$ ② $\exists$ infinitely many $a_K \in S$ so that $a_k \equiv a_2 \bmod p^2$

Repeating gives $a = (a_1, a_2, \dots) \in \mathbb{Z}_p$ with $f(a) = 0$. ▨

<u>Ex</u>: -1 is a square in $\mathbb{Z}_5$, i.e. x^2+1 has a sol'n

$$a = (a_k) = \sum_{k=0}^{\infty} b_k 5^k$$

<u>Step 1</u>: $a_1^2 + 1 \equiv 0 \bmod 5 \Rightarrow a_1 = b_0 = \boxed{2}$ or 3 $\quad$ pick

<u>Step 2</u>: $a_2 = a_1 + b_1 5 = 2 + b_1 5$

$$a_2^2 + 1 \equiv 5 + 20 b_1 \equiv 0 \bmod 5^2 \Rightarrow b_1 = 1 \Rightarrow a_2 = 7.$$

<u>Step 3</u>: $a_3^2 + 1 \equiv (a_2 + b_2 5^2)^2 + 1 \equiv 49 + 2 \cdot 5^2 \cdot 7 b_2 + 1 \bmod 5^3$

$$\equiv 50 + 50 \cdot 7 b_2 \equiv 0 \bmod 5^3$$

$$\Rightarrow 1 + 7 b_2 \equiv 0 \bmod 5 \Rightarrow b_2 = 2$$

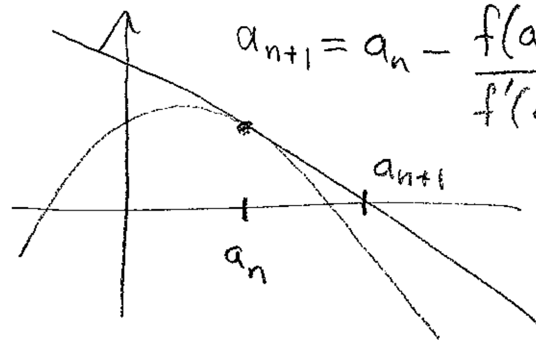
Note that because $\mathbb{Z}/5^k\mathbb{Z}$ is not a field,

the fact the eqn is linear does not immediately lead to the existence of a solution.

<u>Lemma</u>: $f \in \mathbb{Z}[x]$. If a_1 is a simple root of f mod p, then $\exists\, a \in \mathbb{Z}_p$ with $f(a) = 0$ and $a \equiv a_1$ mod p.

Pf: Newton's Method!

$$a_{n+1} = a_n - \frac{f(a_n)}{f'(a_n)}$$



Suppose we have found a_n with $f(a_n) = 0$ mod p^n and $a_n \equiv a_1$ mod p.

(i.e. $\exists\, a_n \in \mathbb{Z}$, with $|f(a_n)|_p \leq p^{-n}$)

Set $a_{n+1} = a_n + \delta$ in $\mathbb{Z}/p^{n+1}$ where $\delta = -\dfrac{f(a_n)}{f'(a_n)}$
which makes sense as $f'(a_n)$ is invertable mod p^k as $f'(a_n) \equiv f'(a_1) \not\equiv 0$ mod p, as a_1 is a simple root mod p.

We have

$$f(a_n + t) \overset{\text{exand in } t}{=} f(a_n) + f'(a_n)\,t + \frac{f''(a_n)}{2}\,t^2 + \cdots$$

Now $\delta \equiv 0$ mod p^n since $f(a_n) \equiv 0$ mod p^n.
Thus $\delta^k \equiv 0$ mod p^{n+1} for all $k \geqslant 2$.

Hence

$f(a_{n+1}) \equiv$

$$f(a_n+\delta) \equiv f(a_n) + f'(a_n)\left(-\frac{f(a_n)}{f'(a_n)}\right) \equiv 0 \mod p^{n+1}$$

As $a_{n+1} \equiv a_n \equiv a_1 \mod p$, inductively we construct $a \in \mathbb{Z}_p$ with $f(a) = 0$ and $f(a) \equiv a_1 \mod p$. $\blacksquare$