Theorem (Chinese Remainder Theorem) Abstract Version.

Let m_i $(i \in I)$ be some moduli and assume they are coprime.

Then there is an "isomorphism"

(bijection + preserving operations)

$$M = \prod_{i \in I} m_i$$

$$\mathbb{Z}/M \xrightarrow{\text{P.}} \prod_{i \in I} \mathbb{Z}/m_i = \left\{ (a_i)_{i \in I} \;\middle|\; a_i \in \mathbb{Z}/m_i \right\}$$

$$[a]_M \longmapsto ([a]_{m_i})_{i \in I}$$

operations are defined componentwise

$$[a_i)_{i \in I} + (\beta_i)_{i \in I} := (a_i + \beta_i)_{i \in I}$$

$$(a_i)_{i \in I} \cdot (\beta_i)_{i \in I} := (a_i \beta_i)_{i \in I}$$

$$\mathbf{0} := (0)_{i \in I} \quad \text{netrd}$$

$$\mathbf{1} := (1)_{i \in I} \quad \text{identity}$$

Translate Questions in $\mathbb{Z}/M$ to systems of questions in each $\mathbb{Z}/m_i$

$\varphi(p^e) = p^{e-1}(p-1)$

Coro. φ is multiplicative

Proof: The isomorphism $\mathbb{Z}/_{mn} \xrightarrow{\text{P.}} \mathbb{Z}/_{m} \times \mathbb{Z}/_{n}$ (where m, n are coprime)

induces an isomorphism $\Phi(mn) \longrightarrow \Phi(m) \times \Phi(n)$.

Why? Only need to verify:

For any $a \in \Phi(mn)$, the natural rep of a modulo m (resp. modulo n) is multiplicatively invertible, i.e. $\in \Phi(m)$ (resp. $\Phi(n)$)

Proof. take $b \in \Phi(mn)$ s.t. $ab \equiv 1 \bmod mn$.

Then $ab \equiv 1 \bmod m$ (and mod n)

Hence a, as well as its nat. rep. is invertible mod m (and mod n)

"Invertibility modulo M" $\Leftrightarrow$ "Invertibility modulo m_i for all $i \in I$"

Solving equations: $f(T) \in \mathbb{Z}[T]$ "integer coefficents"

Say $[a] \in \mathbb{Z}/m$ is a root of $f(T)$ if $f(a) \equiv 0 \bmod m$.

Note that, this property doesn't depent on the choice of rep. of $[a]$.

For m_i $(i \in I)$ moduli coprime to each other, and $M = \prod_{i \in I} m_i$,

the isomorphism in CRT induces the following bijection:

$$\left\{\text{roots of } f(T) \text{ in } \mathbb{Z}/M\right\} \xrightarrow{P_\bullet}_{\sim} \prod_{i \in I} \left\{\text{roots of } f(T) \text{ in } \mathbb{Z}/m_i\right\}.$$

proof: Suppose $f(T) = a_n T^n + \cdots + a_1 T + a_0$, then for any $x \in \mathbb{Z}/M$,

$x \in \mathbb{Z}/M \rightsquigarrow P_i(x) \in \mathbb{Z}/m_i$

$$P_\bullet([a_n]_M x^n + \cdots + [a_1]_M x + [a_0]_M) = ([a_n]_{m_i} P_i(x)^n + \cdots + [a_1]_{m_i} P_i(x) + [a_0]_{m_i})_{i \in I}$$

Since $P_\bullet$ is bijective, $[f(x)]_M$ is zero $\iff$ $P_i(x)^n$ is zero for all $i \in I$

$\iff$ x is a root in $\mathbb{Z}/M$ $\iff$ $P_i(x)$ is a root in $\mathbb{Z}/m_i$ for all $i \in I$

e.g. Solve $T^2 \equiv 29 \mod 35$ $\quad T^2 - 29$

Step 1: $35 = 5 \times 7$

Step 2: "$T^2 \equiv 29 \mod 35$" can be interpreted (via CRT) as

"$T^2 \equiv 29 \mod 5$" $\wedge$ "$T^2 \equiv 29 \mod 7$"

Step 3a: "$T^2 \equiv 29 \mod 5$" $\Leftrightarrow$ "$T^2 \equiv 4 \mod 5$" ($\deg 2 \Rightarrow$ # roots ≤ 2; 5 prime.)

4 perfect square $= 2^2 = (-2)^2$

The latter can be solved by trying:

$0^2 \equiv 0,\ 1^2 \equiv 1,\ 2^2 \equiv 4,\ 3^2 \equiv 4,\ 4^2 \equiv 1 \mod 5$ $\quad T \equiv 2, 3 \mod 5$

Step 3a: "$T^2 \equiv 29 \mod 7$" $\Leftrightarrow$ "$T^2 \equiv 1 \mod 7$" ($\deg 2 \Rightarrow$ # roots ≤ 2; 7 prime)

$1 = 1^2 = (-1)^2$

The latter can be solved by trying:

$0^2 \equiv 0,\ 1^2 \equiv 1,\ 2^2 \equiv 4,\ 3^2 \equiv 2,\ 4^2 \equiv 2,\ 5^2 \equiv 4,\ 6^2 \equiv 1 \mod 7$

$T \equiv 1, 6 \mod 7$

Step 4: Combine "$T \equiv 2 \text{ or } 3 \bmod 5$" and "$T \equiv 1 \text{ or } 6 \bmod 7$" using the algorithm in CRT.

$$3 \cdot 5 - 2 \cdot 7 = 1.$$

$m_1 = 5,\ M_1 = 7,\ N_1 = -2,\ a_1 = 2 \text{ or } 3$

$m_2 = 7,\ M_2 = 5,\ N_2 = 3,\ a_2 = 1 \text{ or } 6$

$M = 35$

$$T \equiv a_1 M_1 N_1 + a_2 M_2 N_2 \bmod M$$

(a_1, a_2)	$T \bmod 35$
2, 1	$2 \cdot 7 \cdot (-2) + 1 \cdot 5 \cdot 3 = -13 \equiv 22$
2, 6	$2 \cdot 7 \cdot (-2) + 6 \cdot 5 \cdot 3 = 62 \equiv 27$
3, 1	$3 \cdot 7 \cdot (-2) + 1 \cdot 5 \cdot 3 = -27 \equiv 8$
3, 6	$3 \cdot 7 \cdot (-2) + 6 \cdot 5 \cdot 3 = 48 \equiv 13$

Summarizing:

We can reduce polynomials mod M to polynomial mod m_i $(i \in I)$

By Prime factorization of positive integers, ($n > 0$ integer)
we have a bijection:

$$\left\{\text{Roots of } f(T) \text{ in } \mathbb{Z}/n\right\} \xleftrightarrow[\sim]{CRT} \prod_{\substack{p \text{ is a} \\ \text{prime divisor} \\ \text{of } n}} \left\{\text{Roots of } f(T) \text{ in } \mathbb{Z}/p^{v_p(n)}\right\}$$

We have studied polynomials mod p, how about mod p^e?

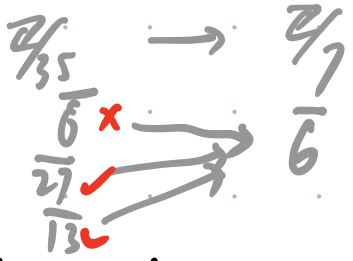
"Henselian lifting".

e.g. $28 = 2^2 \cdot 7$

"roots of f in $\mathbb{Z}/28$"

$\hookrightarrow$ "roots of f in $\mathbb{Z}/4$" $\times$ "roots of f in $\mathbb{Z}/7$".

Reduction & Lifting



$T^2 - 29$

$n \mid m$ $\quad \mathbb{Z}/m \longrightarrow \mathbb{Z}/n$ $\quad$ We say the class α **decents** to β

$\alpha \longmapsto \beta$ $\quad$ or α is a **lifting** of β.

Q: $f(T) \in \mathbb{Z}[T]$. Suppose $a \bmod n$ is a root of $f(T)$ in $\mathbb{Z}/n$.

How to lift $a \bmod n$ to a root of $f(T)$ in $\mathbb{Z}/m$.

⚠: Although $f([a]_m) = [0]_m \Rightarrow f([a]_n) = [0]_n$, $(n \mid m)$

the inverse is NOT TRUE!

e.g. $m = 6$, $n = 2$ $\quad f(T) = T + 2$ $\quad a = 0$

Then

$f(0) = 2 \equiv 0 \bmod 2$ but $f(0) = 2 \equiv \underset{*0}{2} \bmod 6$

Theorem. (lifting multiplicative inverse)

Let p be a prime and $e > 0$ be an integer.

Suppose x is a multiplicative inverse of a mod p^e.

Then

$$\tilde{x} := -ax^2 + 2x$$

is a multiplicative inverse of a mod p^{2e}

Proof: $ax = 1 + p^e \cdot r$

$$a\tilde{x} = -a^2x^2 + 2ax = -(1+p^e r)^2 + 2(1+p^e r)$$

$$= 1 - p^{2e} \cdot r^2 \equiv 1 \bmod p^{2e}.$$

Rmk: $\tilde{x} = x - \underbrace{x p^e \cdot r}_{\text{modification}}$

Lift solution of $aX + b \equiv 0 \mod p^e$ to mod p^{2e}

1) If $b = 0$, there is nothing to do

2) Suppose $b \neq 0$. Let x be a solution of

$$aX + b \equiv 0 \mod p^e.$$

we use a_1, a_2 not a^{-1} to distinguish multiplicative inverse mod p^e & p^{2e}

Let a_1 be the multiplicative inverse of a mod p^e

Then $x = -a_1 b$.

Lift a_1 to a_2, the multiplicative inverse of a mod p^{2e}

Then $\tilde{x} := -a_2 b = x - \underbrace{x p^e \cdot r}_{\text{modification.}}$,

where $a a_1 = 1 + p^e \cdot r$

Theorem (Hensel's lemma)

Let $f(T) \in \mathbb{Z}[T]$, p be a prime and $e > 0$ be an integer.

Suppose x is a root of $f(T) \bmod p^e$ and $f'(x) \not\equiv 0 \bmod p$

(as congruence class; f': derivative.)

Then there is a unique lifting $\tilde{x}$ of x (Namely $\tilde{x} \equiv x \bmod p^e$)

such that $\tilde{x}$ is a root of $f(T) \bmod p^{2e}$.

Rmk: We may replace p^{2e} by p^{e+f} as long as $f \leq e$

$\tilde{x} \bmod p^{2e}$

$\uparrow$

$x \bmod p^e$

Reduction: $\mathbb{Z}/p^{2e} \longrightarrow \mathbb{Z}/p^{e+f}$

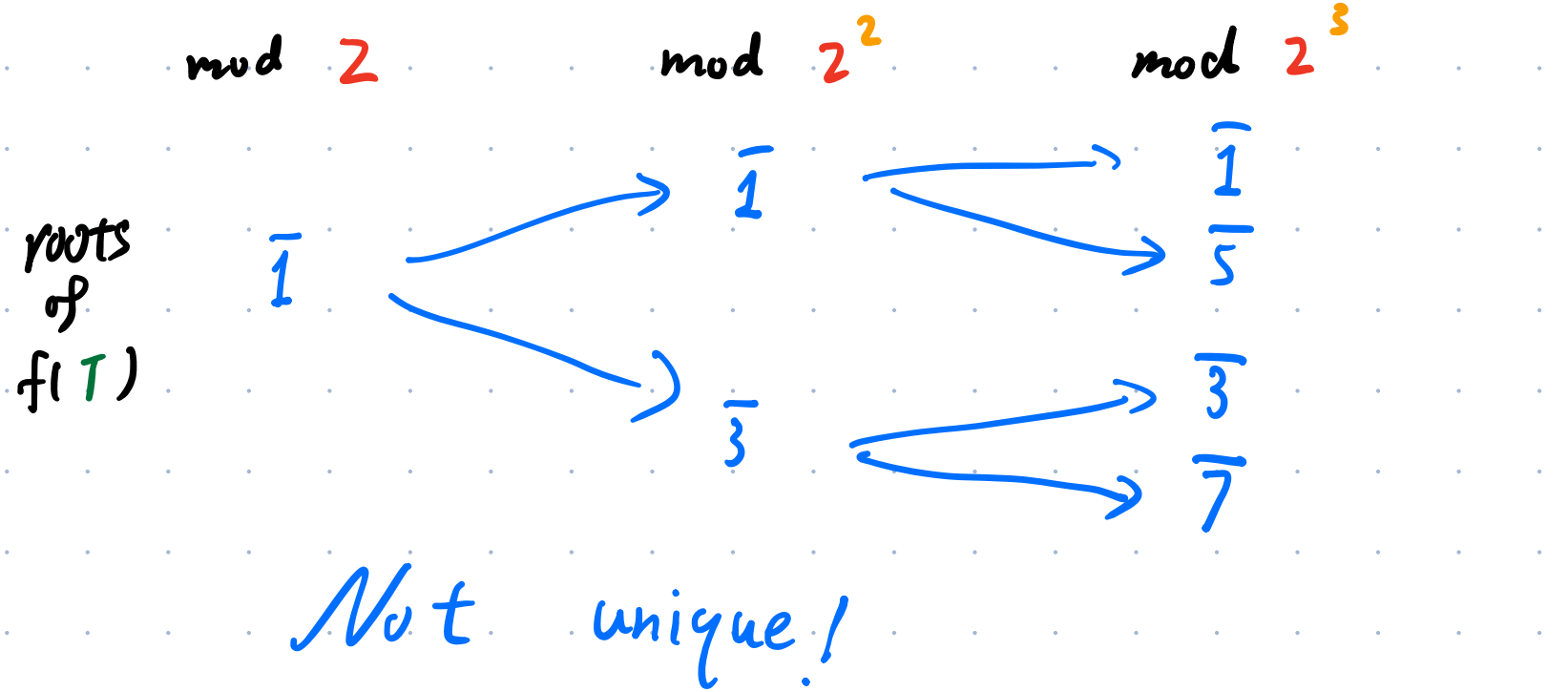
Rmk: $\tilde{x}$ is of the form $\tilde{x} = x + C \cdot p^e$ (or $C < p^f$)

Rmk (derivative, formally definition) $T^d \longmapsto d \cdot T^{d-1}$, $1 \longmapsto 0$.

E.g. $p=2$ $\quad f(T) = T^2 - 1$

Then $f'(T) = 2T$, which is zero polynomial mod 2

Hence, none roots of f mod 2^e has a unique lifting.



Not unique!

Proof (Sketch): x is a root of f mod p^e

Expand $f(x + p^e t)$ to its Taylor series

(t: variable)

$$f(x + p^e t) = f(x) + f'(x)p^e t + \frac{f''(x)}{2!}p^{2e}t^2 + \cdots$$

Note that: 1) this is a finite sum

2) $\frac{f^{(d)}(x)}{d!}$ is always an integer.

Hence, $f(x + p^e t) \equiv f(x) + f'(x)p^e t \mod p^{2e}$

We want $\tilde{x} = x + t \cdot p^e$ be a root of $f(T)$ mod p^{2e}.

This amounts to $f(x) + f'(x)p^e t \equiv 0 \mod p^{2e}$.

Solved by lifting multiplicative inverse.

Coro: Let $f(T) \in \mathbb{Z}[T]$ and p be a prime.

Suppose x is a root of $f(T) \bmod p$ and $f'(x) \not\equiv 0 \bmod p$

Then there is a sequence $\vec{x} = (x_n)_{n \in \mathbb{N}}$ s.t.

1) $x_1 = x$

2) $x_n \equiv x_m \bmod p^m$ whenever $m < n$

3) x_n is a root of $f(T) \bmod p^n$

Proof: Apply Hensel's lemma to $x_1 = x$, we get x_2, then x_4, x_8, ...

Reduce x_{2^e} to x_f with $f < 2^e$, we covers all x_n.

$$x_1 \bmod p \xrightarrow{\text{lift}} x_2 \bmod p^2 \xrightarrow{\text{lift}} x_4 \bmod p^4 \xrightarrow{\text{lift}} x_8 \bmod p^8 \cdots$$

$$x_3 \bmod p^3 \xrightarrow{\text{lift}} x_6 \bmod p^6 \cdots \quad (\text{reduction: } x_4 \to x_3)$$

Summarizing:

We can reduce polynomials mod M to polynomial mod m_i $(i \in I)$

By Prime factorization of positive integers,
we have a bijection:

$$\left\{\text{Roots of } f(T) \text{ in } \mathbb{Z}/n\right\} \xleftrightarrow[\sim]{\text{CRT}} \prod_{p \text{ is a prime divisor of } n} \left\{\text{Roots of } f(T) \text{ in } \mathbb{Z}/p^{v_p(n)}\right\}$$

$$\left\{\text{Roots of } f(T) \text{ in } \mathbb{Z}/p^{v_p(n)}\right\} \;\Big\updownarrow\; \left\{\text{Roots of } f(T) \text{ in } \mathbb{F}_p\right\}$$

(modular reduction $\downarrow$, Hensel lifting $\uparrow$)

Q: Solve polynomials in $\mathbb{F}_p$?

- Linear ✓
- Quadratic ? next time.