Introduction to Number Theory

Math 110 | Winter 2023

Xu Gao

March 3, 2023

What we have seen last time:

- Chinese Remainder Theorem

Today's topics

- Reduction and lifting

Chinese Remainder Theorem

Chinese Remainder Theorem

Let m_i ($i \in I$) be moduli which are coprime to each other and let M be the product of them. The ***Chinese Remainder Theorem*** (***CRT***) essentially says that the natural reduction map

$$\mathbb{Z}/M \longrightarrow \prod_{i \in I} \mathbb{Z}/m_i \colon [A]_M \mapsto ([A]_{m_i})_{i \in I}$$

is an isomorphism.

This allows us to translate between problems modulo M and systems of similar problems modulo each m_i.

Corollary 20.1

Let $f(T)$ be an integer polynomial (i.e. $f(T) \in \mathbb{Z}[T]$). The natural reduction map induces a bijection

$$\{[A]_M \in \mathbb{Z}/M \mid f(A) \equiv 0 \pmod{M}\} \xrightarrow{\sim} \left\{([a_i]_{m_i})_{i \in I} \in \prod_{i \in I} \mathbb{Z}/m_i \,\middle|\, f(a_i) \equiv 0 \pmod{m_i}, \forall i \in I\right\}.$$

Proof. Let's say $f(T) = c_n T^n + \cdots + c_1 T + c_0$. Then for any congruence class $[A]_M \in \mathbb{Z}/M$, we have

$$\begin{aligned} f([A]_M) &= [c_n]_M [A]_M^n + \cdots + [c_1]_M [A]_M + [c_0]_M \\ &= [c_n A^n + \cdots + c_1 A + c_0]_M = [f(A)]_M. \end{aligned}$$

The natural reduction map then maps it to

$$\begin{aligned} ([f(A)]_{m_i})_{i \in I} &= ([c_n A^n + \cdots + c_1 A + c_0]_{m_i})_{i \in I} \\ &= ([c_n]_{m_i} [A]_{m_i}^n + \cdots + [c_1]_{m_i} [A]_{m_i} + [c_0]_{m_i})_{i \in I} = (f([A]_{m_i}))_{i \in I}. \end{aligned}$$

Therefore, we have that $f([A]_M) = [0]_M$ if and only if $f([A]_{m_i}) = [0]_{m_i}$ for all $i \in I$. $\square$

$T^2 - 29$ mod 35

Example 20.2

Solve the congruence equation $x^2 \equiv 29 \pmod{35}$.

We first note that $35 = 5 \times 7$.

Then the congruence equation $x^2 \equiv 29 \pmod{35}$ is equivalent to the following two:

$$x^2 \equiv 29 \pmod{5} \qquad \text{and} \qquad x^2 \equiv 29 \pmod{7}.$$

The first one is further equivalent to $x^2 \equiv 4 \pmod{5}$ and thus whose solution is $x \equiv \pm 2 \pmod{5}$. The second one is further equivalent to $x^2 \equiv 1 \pmod{7}$ and thus whose solution is $x \equiv \pm 1 \pmod{7}$. (Note that 5 and 7 are primes. That's why there are at most two roots.)

roots $\leq$ degree

Chinese Remainder Theorem

Now, we need to combine the solutions on each piece $\mathbb{Z}/5$ and $\mathbb{Z}/7$. Namely, we need to apply CRT to reduce the system of congruences

$$\begin{cases} x \equiv a \pmod{5} \\ x \equiv b \pmod{7} \end{cases} \Rightarrow x \equiv ? \pmod{35},$$

where the pair (a, b) are $(2, 1)$, $(2, -1)$, $(-2, 1)$, or $(-2, -1)$.

For this, we start with a Bézout's identity

$$7 \cdot (-2) + 5 \cdot 3 = 1.$$

Then we have

$$x \equiv a \cdot 7 \cdot (-2) + b \cdot 5 \cdot 3 \pmod{35}.$$

Plug in each cases of (a, b), we get

a ($\cancel{a_1}$) \ b ($\cancel{a_2}$)	1	-1
2	$2 \cdot 7 \cdot (-2) + 1 \cdot 5 \cdot 3 \equiv 22 \pmod{35}$	$2 \cdot 7 \cdot (-2) + (-1) \cdot 5 \cdot 3 \equiv 27 \pmod{35}$
-2	$(-2) \cdot 7 \cdot (-2) + 1 \cdot 5 \cdot 3 \equiv 8 \pmod{35}$	$(-2) \cdot 7 \cdot (-2) + (-1) \cdot 5 \cdot 3 \equiv 13 \pmod{35}$

Chinese Remainder Theorem

Summarize: to find roots of a polynomial $f(T)$ in $\mathbb{Z}/M$, we can first decompose M into prime powers $p^{v_p(M)}$ and solve this problem in each $\mathbb{Z}/p^{v_p(M)}$, then combine the pieces from each modular world to get answers.

$$\{\text{roots of } f(T) \text{ in } \mathbb{Z}/M\} \xrightarrow{\sim} \prod_{\substack{p \text{ is a prime} \\ p|m}} \left\{\text{roots of } f(T) \text{ in } \mathbb{Z}/p^{v_p(M)}\right\}.$$

Q: We have knowledge on polynomials over $\mathbb{F}_p$, what about polynomials over $\mathbb{Z}/p^{v_p(M)}$?

Reduction and lifting

Reduction and lifting

$$\begin{array}{ccc} m & \mathbb{Z}/m & \alpha \\ | & | & \text{descent} \downarrow \; \uparrow \text{lift} \\ n & \mathbb{Z}/n & \beta \end{array}$$

Recall that whenever $n \mid m$, we have a reduction map

$$\mathbb{Z}/m \longrightarrow \mathbb{Z}/n.$$

When the congruence class $\alpha \in \mathbb{Z}/m$ is mapped to $\beta \in \mathbb{Z}/n$, we say "α ***descends*** to β", "β is a ***reduction*** of α", and "α is a ***lifting*** of β".

Question

Let $f(T)$ be an integer polynomial. Given a root β of $f(T)$ in $\mathbb{Z}/n$, how to lift it to a root α in $\mathbb{Z}/m$?

Note that: although we can always reduce a root in $\mathbb{Z}/m$ to a root in $\mathbb{Z}/n$, but the converse is not ture. E.g. $[0]_2$ is a root of $T + 2$ in $\mathbb{Z}/2$ but its natural lifting $[0]_4$ in $\mathbb{Z}/4$ is not a root.

Theorem 20.3 (Lifting multiplicative inverse)

Let p be a prime and e be a positive integer. Then a multiplicative inverse x of a modulo p^e can always be lifted to a multiplicative inverse $\widetilde{x}$ of a modulo p^{2e}.

Proof. The requirement of $\widetilde{x}$ is

$$\widetilde{x} \equiv x \pmod{p^e} \qquad \text{and} \qquad a\widetilde{x} \equiv 1 \pmod{p^{2e}}.$$

The first tells us that $\widetilde{x}$ can be written as $x + up^e$. Plug it in the second, we get

$$ax + aup^e \equiv 1 \pmod{p^{2e}}.$$

Solve it !

$mn \mid m\ell \Rightarrow n \mid \ell$

We know $ax = 1 + vp^e$ for some v. Hence, we get

$$aup^e \equiv -vp^e \pmod{p^{2e}} \Rightarrow au \equiv -v \pmod{p^e}$$
$$\Rightarrow u \equiv -xv \pmod{p^e}.$$

$ax \equiv 1 \bmod p^e$

Therefore, we have

$$\begin{aligned}\widetilde{x} &= x + up^e \\ &\equiv x - xvp^e \pmod{p^{2e}} \\ &= x(1 - \underbrace{vp^e}_{=(ax-1)}) = x(2 - ax).\end{aligned}$$

□

Remark. One can replace $2e$ by any integer e' between e and $2e$: just reduce $\widetilde{x} \in \mathbb{Z}/p^{2e}$ to $\mathbb{Z}/p^{e'}$.

p^{2e} $p^{e'}$ p^e

Definition 20.4

Let $f(T) = c_n T^n + \cdots + c_1 T + c_0$ be an integer polynomial. Then its ***derivative*** is the integer polynomial

$$f'(T) = nc_n T^{n-1} + \cdots + c_1.$$

A root of $f(T)$ in R (either $\mathbb{Z}$ or $\mathbb{Z}/m$) is called a ***simple root*** if it is not a root of $f'(T)$ in R. $f(\alpha)=0$ $f'(\alpha) \neq 0$

N.B. The derivative is formal, not necessarily related to what you learned in Calculus.

Theorem 20.5 (Hensel's lifting)

Let $f(T)$ be an integer polynomial, p be a prime, and e be a positive integer. If x is a root of $f(T)$ modulo p^e which descends to a simple root in $\mathbb{F}_p$, then x can be uniquely lifted to a root $\widetilde{x}$ of $f(T)$ modulo p^{2e}.

Remark. One can replace $2e$ by any integer e' between e and $2e$: just reduce $\widetilde{x} \in \mathbb{Z}/p^{2e}$ to $\mathbb{Z}/p^{e'}$.

Example 20.6

The polynomial $T^2 - 1$ has no simple roots in $\mathbb{F}_2$ since its derivative $2T$ descends to the zero polynomial over $\mathbb{F}_2$.

Sketch of the proof

Let x be a representative of a root of $f(T)$ in $\mathbb{Z}/p^e$. Then a representative of a lifting of that root can be written as

$$\widetilde{x} = x + t, \qquad p^e \mid t$$

where t is some integer divided by p^e.

So our requirement can be interpreted as

$$f(x+t) \equiv 0 \pmod{p^{2e}}.$$

Sketch of the proof

Now, we need a formal* version of ***Taylor's expansion***:

deg(f)=n

$$f(x+t) = f(x) + \frac{f'(x)}{1!}t + \frac{f''(x)}{2!}t^2 + \cdots + \frac{f^{(n)}(x)}{n!}t^n,$$

where $f^{(k)}(T)$ is the k-th derivative of $f(T)$ and n is the degree of $f(T)$. What we need in particular is that each fraction $\frac{f^{(k)}(x)}{k!}$ is actually an integer. Hence, we have (notice that $p^e \mid t$)

$$f(x+t) \equiv f(x) + f'(x)t \pmod{p^{2e}}.$$

*There is NO continuity or calculus stuff involved.

Sketch of the proof

Since x descends to a simple root in $\mathbb{F}_p$, by theorem 20.3, $f'(x)$ is invertible modulo any power of p. Therefore, the linear congruence equation

$$f(x) + f'(x)t \equiv 0 \pmod{p^{2e}}$$

always has a unique solution (up to congruence $\pmod{p^{2e}}$). Substituting this solution back to $\widetilde{x} = x + t$, we get a desired lifting.

We may summarize above by the formula*:

$$[\widetilde{x}]_{p^{2e}} = [x]_{p^{2e}} + [-f(x)]_{p^{2e}}[f'(x)]_{p^{2e}}^{-1}. \qquad (\star)$$

*Note that those operations are in $\mathbb{Z}/p^{2e}$.

Example 20.7

Solve the congruence $x^2 \equiv 7 \pmod{27}$.

Let $f(T)$ be the polynomial $T^2 - 7$. Then its derivative is $f'(T) = 2T$.

Notice that $27 = 3^3$. We start with $\mathbb{F}_3$.

Since $T^2 - 7$ descends to $T^2 - \bar{1}$ over $\mathbb{F}_3$, we see that $[1]_3$ and $[2]_3$ are two roots of $f(T)$ in $\mathbb{F}_3$.

Since $f'(1) = 2 \not\equiv 0 \pmod{3}$ and $f'(2) = 4 \not\equiv 0 \pmod{3}$, both $[1]_3$ and $[2]_3$ are simple roots. Moreover, their multiplicative inverse modulo 3 are 2 and 1 respectively. $f'(1)$ and $f'(2)$

$f(T) = T^2 - 7$

Applying theorem 20.3, we can lift these multiplicative inverses from modulo 3 world to modulo 3^2 world:

$$[2]_3^{-1} = [2]_3 \implies [2]_{3^2}^{-1} = [2 \cdot (2 - 2 \cdot 2)]_{3^2} = [5]_{3^2},$$
$$[1]_3^{-1} = [1]_3 \implies [1]_{3^2}^{-1} = [1 \cdot (2 - 1 \cdot 1)]_{3^2} = [1]_{3^2}.$$

Applying the Hensel's lemma (theorem 20.5, but more precisely, the formula (⋆)), we get

$$[1]_3 \overset{\text{Hensel}}{\rightsquigarrow} [1]_{3^2} + \underline{[-f(1)]_{3^2}}\,\underline{[f'(1)]_{3^2}^{-1}} = [1 + 6 \cdot 5]_{3^2} = [4]_{3^2},$$
$$[2]_3 \overset{\text{Hensel}}{\rightsquigarrow} [2]_{3^2} + \underline{[-f(2)]_{3^2}}\,\underline{[f'(2)]_{3^2}^{-1}} = [2 + 3 \cdot 1]_{3^2} = [5]_{3^2}.$$

Reduction and lifting

$f(T) = T^2 - 7 \qquad f'(T) = 2 \cdot T$

Next, we use theorem 20.3 again to lift the multiplicative inverses of $f'(4) = 8$ and $f'(5) = 10$ from $\mathbb{Z}/3^2$ to $\mathbb{Z}/3^3$:

$$[8]_{3^2}^{-1} = [8]_{3^2} \implies [8]_{3^3}^{-1} = [8 \cdot (2 - 8 \cdot 8)]_{3^3} = [17]_{3^3},$$
$$[10]_{3^2}^{-1} = [1]_{3^2} \implies [10]_{3^3}^{-1} = [1 \cdot (2 - 10 \cdot 1)]_{3^3} = [19]_{3^3}.$$

Applying the Hensel's lemma again, we get

$$[4]_{3^2} \overset{\text{Hensel}}{\rightsquigarrow} [4]_{3^3} + [-f(4)]_{3^3}\,[f'(4)]_{3^3}^{-1} = [4 + (-9) \cdot 17]_{3^3} = [13]_{3^3},$$
$$[5]_{3^2} \overset{\text{Hensel}}{\rightsquigarrow} [5]_{3^3} + [-f(5)]_{3^3}\,[f'(5)]_{3^3}^{-1} = [5 + (-18) \cdot 19]_{3^3} = [14]_{3^3}$$