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

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

is an isomorphism.

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

Corollary 6.3.1

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

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

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

$$f([A]_M) = [c_n]_M [A]_M^n + \cdots + [c_1]_M [A]_M + [c_0]_M$$
$$= [c_n A^n + \cdots + c_1 A + c_0]_M = [f(A)]_M.$$

The natural reduction map then maps it to

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

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

Example 6.3.2

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

Example 6.3.2

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:

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

Example 6.3.2

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.)

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 $(-2, -1)$.

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

$a \backslash b$	1	-1
2	$2 \cdot 7 \cdot (-2) + 1 \cdot 5 \cdot 3$	
-2		

Chinese Remainder Theorem: applications

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

$a \backslash b$	1	-1
2	$2 \cdot 7 \cdot (-2) + 1 \cdot 5 \cdot 3 \equiv 22 \pmod{35}$	
-2		

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

$a \backslash b$	1	-1
2	$2 \cdot 7 \cdot (-2) + 1 \cdot 5 \cdot 3 \equiv 22 \pmod{35}$	$2 \cdot 7 \cdot (-2) + (-1) \cdot 5 \cdot 3$
-2		

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

$a \backslash b$	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		

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

$a \backslash b$	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	$(-2) \cdot 7 \cdot (-2) + 1 \cdot 5 \cdot 3$	

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

$a \backslash b$	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	$(-2) \cdot 7 \cdot (-2) + 1 \cdot 5 \cdot 3 \equiv 8 \pmod{35}$	

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

$a \backslash b$	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	$(-2) \cdot 7 \cdot (-2) + 1 \cdot 5 \cdot 3 \equiv 8 \pmod{35}$	$(-2) \cdot 7 \cdot (-2) + (-1) \cdot 5 \cdot 3$

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

$a \backslash b$	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	$(-2) \cdot 7 \cdot (-2) + 1 \cdot 5 \cdot 3 \equiv 8 \pmod{35}$	$(-2) \cdot 7 \cdot (-2) + (-1) \cdot 5 \cdot 3 \equiv 13 \pmod{35}$

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.

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

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.

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

Question

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