Lecture 7.7: The Chinese remainder theorem

Matthew Macauley

Department of Mathematical Sciences
Clemson University
http://www.math.clemson.edu/~macaule/

Math 4120, Modern Algebra

Motivating example

Exercise 1

Find all solutions to the system $\begin{cases} 2x \equiv 5 \pmod{7} \\ 3x \equiv 4 \pmod{9} \end{cases}$

Motivating example

Exercise 2

Find all solutions to the system $\begin{cases} x \equiv 3 \pmod 4 \\ x \equiv 0 \pmod 6 \end{cases}$

Number theory version

Chinese remainder theorem

Let $n_1, \dots, n_k \in \mathbb{Z}^+$ be pairwise co-prime (that is, $\gcd(n_i, n_j) = 1$ for $i \neq j$). For any $a_1, \dots, a_k \in \mathbb{Z}$, the system

$$\begin{cases} x \equiv a_1 \pmod{n_1} \\ \quad\vdots \\ x \equiv a_1 \pmod{n_1} \end{cases}$$

has a solution $x \in \mathbb{Z}$. Moreover, all solutions are congruent modulo $N = n_1 n_2 \cdots n_k$.

This can be generalized. To see how, first recall the following operations on ideals:

1. *Intersection*: $I \cap J = \{r \in R \mid r \in I \text{ and } r \in J\}$.
2. *Product*: $IJ = \langle ab \mid a \in I,\ b \in J\rangle = \{a_1 b_1 + \cdots + a_k b_k \mid a_i \in I,\ b_j \in J\} \subseteq I \cap J$.
3. *Sum*: $I + J = \{a + b \mid a \in I,\ b \in J\}$.

Example: $R = \mathbb{Z}$, $I = \langle 9\rangle = 9\mathbb{Z}$, $J = \langle 6\rangle = 6\mathbb{Z}$.

1. *Intersection*: $\langle 9\rangle \cap \langle 6\rangle = \langle 18\rangle \quad (\text{lcm})$
2. *Product*: $\langle 9\rangle\langle 6\rangle = \langle 54\rangle \quad (\text{product})$
3. *Sum*: $\langle 9\rangle + \langle 6\rangle = \langle 3\rangle \quad (\text{gcd})$.

Ring theory version

Note that $\gcd(m,n)=1$ iff $am+bn=1$ for some $a,b\in\mathbb{Z}$.

Or equivalently, $\langle m\rangle+\langle n\rangle=\mathbb{Z}$.

Definition

Two ideals I,J of R are co-prime if $I+J=R$.

Chinese remainder theorem (2 ideals)

Let R have 1 and $I+J=R$. Then for any $r_1,r_2\in R$, the system

$$\begin{cases} x\equiv r_1 \pmod{I} \\ x\equiv r_2 \pmod{J} \end{cases}$$

has a solution $r\in R$. Moreover, any two solutions are congruent modulo $I\cap J$.

Recall that such a solution $r\in R$ satisfies $r-r_1\in I$ and $r-r_2\in J$.

Ring theory version

Chinese remainder theorem (2 ideals)

Let R have 1 and $I + J = R$. Then for any $r_1, r_2 \in R$, the system

$$\begin{cases} x \equiv r_1 \pmod{I} \\ x \equiv r_2 \pmod{J} \end{cases}$$

has a solution $r \in R$. Moreover, any two solutions are congruent modulo $I \cap J$.

Proof

Write $1 = a + b$, with $a \in I$ and $b \in J$, and set $r = r_2 a + r_1 b$.

$\square$

Ring theory version

Chinese remainder theorem

Let R have 1 and $I_1, \dots, J_n$ be pairwise co-prime ideals. Then for any $r_1, \dots, r_n \in R$, the system

$$\begin{cases} x \equiv r_1 \pmod{I_1} \\ \quad\vdots \\ x \equiv r_2 \pmod{I_n} \end{cases}$$

has a solution $r \in R$. Moreover, any two solutions are congruent modulo $I_1 \cap \cdots \cap I_n$.

Proof

$\underline{n=1}$. For $j = 2, \dots, n$, write $1 = a_j + b_j$, where $a_j \in I_1$, $b_j \in I_j$. Then

$$\begin{aligned} 1 &= (a_2 + b_2)(a_3 + b_3) \cdots (a_n + b_n) \\ &= a_2\big[(a_3 + b_3) \cdots (a_n + b_n)\big] + b_2\big[(a_3 + b_3) \cdots (a_n + b_n)\big] \in I_1 + \prod_{j=2}^{n} I_j = R. \end{aligned}$$

Now apply the CRT for 2 ideals to the system $\begin{cases} x \equiv 1 \pmod{I_1} \\ x \equiv 0 \pmod{\prod_{j \neq 1} I_j} \end{cases}$

Let $s_1 \in R$ be a solution.

Ring theory version

Chinese remainder theorem

Let R have 1 and $I_1, \dots, J_n$ be pairwise co-prime ideals. Then for any $r_1, \dots, r_n \in R$, the system

$$\begin{cases} x \equiv r_1 \pmod{I_1} \\ \quad\vdots \\ x \equiv r_2 \pmod{I_n} \end{cases}$$

has a solution $r \in R$. Moreover, any two solutions are congruent modulo $I_1 \cap \cdots \cap I_n$.

Proof (cont.)

$\underline{n = k}$. For $j = 1, \dots \cancel{k}, \dots, n$, write $1 = a_j + b_j$, where $a_j \in I_k$, $b_j \in I_j$. Then

$$1 = (a_2 + b_2) \cdots \cancel{(a_k + b_k)} \cdots (a_n + b_n) \in I_k + \prod_{j \neq k} I_j = R.$$

Now apply the CRT for 2 ideals to the system $\begin{cases} x \equiv 1 \pmod{I_k} \\ x \equiv 0 \pmod{\prod_{j \neq 1} I_j} \end{cases}$

Let $s_k \in R$ be a solution.

Ring theory version

Chinese remainder theorem

Let R have 1 and $I_1, \dots, J_n$ be pairwise co-prime ideals. Then for any $r_1, \dots, r_n \in R$, the system

$$\begin{cases} x \equiv r_1 \pmod{I_1} \\ \quad\vdots \\ x \equiv r_2 \pmod{I_n} \end{cases}$$

has a solution $r \in R$. Moreover, any two solutions are congruent modulo $I_1 \cap \dots \cap I_n$.

Proof (cont.)

By construction, $s_k \in \pmod{\prod_{j \neq k} I_j}$, and so $s_k \in I_j$ for all $j \neq k$.

We have $s_k \equiv 1 \pmod{I_k}$ and $s_k \equiv 1 \pmod{I}_j$ for $j \neq k$.

Set $r = r_1 s_1 + \dots + r_n s_n$. It is easy to see that this works.

If $s \in R$ is another solution, then $s \equiv r_j \equiv r \pmod{I_j}$, for $j = 1, \dots, n$, and so

$$s \equiv r \mod \bigcap_{j=1}^{n} I_j.$$

Applications

When is $\mathbb{Z}_n$ isomorphic to a product?

Let $R = \mathbb{Z}$ and $I_j = \langle m_j \rangle$, for $j = 1, \dots, n$ with $\gcd(m_i, m_j) = 1$ for $i \neq j$. Then

$$I_1 \cap \cdots \cap I_n = \langle m_1 m_2 \cdots m_n \rangle, \qquad \text{and} \qquad \mathbb{Z}_{m_1 m_2 \cdots m_n} \cong \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_n}.$$

Corollary

Factor $n = p_1^{d_1} \cdots p_n^{d_n}$ into a product of distinct primes. Then

$$\mathbb{Z}_n \cong \mathbb{Z}_{{p_1}^{d_1}} \times \cdots \times \mathbb{Z}_{{p_n}^{d_n}}.$$

Remark

If R is a Euclidean domain, then the proof of the CRT is *constructive*.

Specifically, we can use the Euclidean algorithm to write

$$c_k m_k + d_k \prod_{j \neq k} m_j = \gcd\Big(m_k, \prod_{j \neq k} m_j\Big) = 1, \quad \text{where} \quad I_j = \langle m_j \rangle.$$

Then, set $s_k = d_k \prod_{j \neq k} m_j$, and $r = r_1 s_1 + \cdots + r_n s_n$ is the solution.