# Number Theory: Chinese Remainder Theorem, Section 4.4 and

# Relations, Section 9.1


CS261 Mathematical Foundations of CS

Professor Leah Buechley

Spring 2024

University of New Mexico

# The Chinese Remainder Theorem 1

In the first century, the Chinese mathematician Sun-Tsu asked:

There are certain things whose number is unknown. When divided by 3, the remainder is 2; when divided by 5, the remainder is 3; when divided by 7, the remainder is 2. What will be the number of things?

This puzzle can be translated into the solution of the system of congruences:

$x \equiv 2 \pmod{3}$,

$x \equiv 3 \pmod{5}$,

$x \equiv 2 \pmod{7}$?

We'll see how the theorem that is known as the *Chinese Remainder Theorem* can be used to solve Sun-Tsu's problem.

# The Chinese Remainder Theorem 2

**Theorem 2**: (*The Chinese Remainder Theorem*) Let $m_1, m_2, \ldots, m_n$ be pairwise relatively prime positive integers greater than one and $a_1, a_2, \ldots, a_n$ arbitrary integers. Then the system

$$x \equiv a_1 \pmod{m_1}$$
$$x \equiv a_2 \pmod{m_2}$$
$$\cdot$$
$$\cdot$$
$$\cdot$$
$$x \equiv a_n \pmod{m_n}$$

has a unique solution modulo $m = m_1 m_2 \cdots m_n$.

(That is, there is a solution x with $0 \le x < m$ and all other solutions are congruent modulo $m$ to this solution.)

**Proof**: We'll show that a solution exists by describing a way to construct the solution. Showing that the solution is unique modulo $m$ is Exercise 30.

# The Chinese Remainder Theorem 3

To construct a solution first let $M_k = m/m_k$ for $k = 1,2,\ldots,n$ and $m = m_1 m_2 \cdots m_n$. Since $\gcd(m_k, M_k) = 1$, by Theorem 1, there is an integer $y_k$, an inverse of $M_k$ modulo $m_k$, such that

$$M_k y_k \equiv 1 \pmod{m_k}$$

Form the sum

$$x = a_1 M_1 y_1 + a_2 M_2 y_2 + \cdots + a_n M_n y_n.$$

Note that because $M_j \equiv 0 \pmod{m_k}$ whenever $j \neq k$, all terms except the $k$th term in this sum are congruent to 0 modulo $m_k$.

Because $M_k y_k \equiv 1 \pmod{m_k}$, we see that $x \equiv a_k M_k y_k \equiv a_k \pmod{m_k}$, for $k = 1,2,\ldots,n$.

Hence, $x$ is a simultaneous solution to the $n$ congruences.

$$x \equiv a_1 \pmod{m_1}$$
$$x \equiv a_2 \pmod{m_2}$$
$$\vdots$$
$$x \equiv a_n \pmod{m_n}$$

# The Chinese Remainder Theorem 4

Example: Consider the 3 congruences from Sun-Tsu's problem:

$x \equiv 2 \pmod 3$, $x \equiv 3 \pmod 5$, $x \equiv 2 \pmod 7$.

Let $m = 3 \cdot 5 \cdot 7 = 105$, $M1 = m/3 = 35$, $M3 = m/5 = 21$, $M3 = m/7 = 15$

We see that

- 2 is an inverse of $M1 = 35$ modulo 3 since $35 \cdot 2 \equiv 2 \cdot 2 \equiv 1 \pmod 3$.
- 1 is an inverse of $M2 = 21$ modulo 5 since $21 \equiv 1 \pmod 5$.
- 1 is an inverse of $M3 = 15$ modulo 7 since $15 \equiv 1 \pmod 7$.

Hence,

$x = a1M1y1 + a2M2y2 + a3M3y3$

$= 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 = 233 \equiv 23 \pmod{105}$

We have shown that 23 is the smallest positive integer that is a simultaneous solution. Check it!

# Back Substitution

We can also solve systems of linear congruences with pairwise relatively prime moduli by rewriting a congruences as an equality using Theorem 4 in Section 4.1, substituting the value for the variable into another congruence, and continuing the process until we have worked through all the congruences. This method is known as *back substitution*.

**Example**: Use the method of back substitution to find all integers $x$ such that $x \equiv 1 \pmod 5$, $x \equiv 2 \pmod 6$, and $x \equiv 3 \pmod 7$.

**Solution**: By Theorem 4 in Section 4.1, the first congruence can be rewritten as $x = 5t + 1$, where $t$ is an integer.

- Substituting into the second congruence yields $5t + 1 \equiv 2 \pmod 6$.
- Solving this tells us that $t \equiv 5 \pmod 6$.
- Using Theorem 4 again gives $t = 6u + 5$ where $u$ is an integer.
- Substituting this back into $x = 5t + 1$, gives $x = 5(6u + 5) + 1\ 30u + 26$.
- Inserting this into the third equation gives $30u + 26 \equiv 3 \pmod 7$.
- Solving this congruence tells us that $u \equiv 6 \pmod 7$.
- By Theorem 4, $u = 7v + 6$, where $v$ is an integer.
- Substituting this expression for $u$ into $x = 30u + 26$, tells us that $x = 30(7v + 6) + 26 = 210u + 206$.

Translating this back into a congruence we find the solution $x \equiv 206 \pmod{210}$.

# Relations and Their Properties

Section 9.1

# Section Summary 1

Relations and Functions.

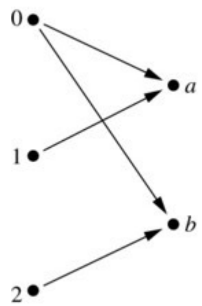
 

# Binary Relations

**Definition:** A *binary relation R* from a set *A* to a set *B* is a subset $R \subseteq A \times B$.

**Example**:

- Let $A = \{0,1,2\}$ and $B = \{a,b\}$.
- $\{(0,a),(0,b),(1,a),(2,b)\}$ is a relation from *A* to *B*.
- We can represent relations from a set *A* to a set *B* graphically or using a table:




| $R$ | $a$ | $b$ |
|---|---|---|
| 0 | × | × |
| 1 | × | |
| 2 | | × |

Relations are more general than functions. A function is a relation where exactly one element of *B* is related to each element of *A*.

Access the text alternative for slide images.

# Binary Relations on a Set[1]

**Definition:** A binary relation $R$ *on a set* $A$ is a subset of $A \times A$ or a relation from $A$ to $A$.

**Example**:

- Suppose that $A = \{a, b, c\}$. Then $R = \{(a,a),(a,b),(a,c)\}$ is a relation on $A$.
- Let $A = \{1, 2, 3, 4\}$. The ordered pairs in the relation $R = \{(a,b) \mid a \text{ divides } b\}$ are $(1, 1), (1, 2), (1, 3), (1, 4), (2, 2), (2, 4), (3, 3)$, and $(4, 4)$.

# Binary Relations on a Set 2

**Question**: How many relations are there on a set $A$?

**Solution**: Because a relation on $A$ is the same thing as a subset of $A \times A$, we count the subsets of $A \times A$. Since $A \times A$ has $n^2$ elements when $A$ has $n$ elements, and a set with $m$ elements has $2^m$ subsets, there are subsets of $A \times A$. Therefore, there are relations on a set $A$.