# The Chinese Remainder Theorem

**Abstract**

In this session, we shall motivate and explore the *Chinese Remainder Theorem*. Consider a system of congruences of the form

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_k \pmod{m_k}. \end{aligned}$$

Can we determine *whether* this has a solution $x$? If it has a solution, can we explicitly *compute* all such solutions $x$? We explore this topic by starting with this basic question, then continuing to generalizations and applications of this.

*Background needed:* Prerequisites include concepts of *modular arithmetic* (and therefore of *divisbility*), as well as properties of integers that are *relatively prime* (or *coprime*). In particular, we will use the existence of *modular multiplicative inverse* in the context of *Bézout's Identity*. Past experience with these ideas will be helpful, but this worksheet will present a self-contained introduction to what will be used.

## 0 Warmup

*Exercises:*

0.1 Let $a, b, m$ be integers. What does it mean that $a$ is *congruent to $b$ modulo $m$* (denoted $a \equiv b \pmod{m}$)?

0.2 What is the remainder when dividing 94 by 3? By 5? By 7?

0.3 Consider the system of congruences

$$x \equiv 2 \pmod 3$$
$$x \equiv 1 \pmod 5.$$

Does this have a solution? If so, can you find at least one such solution?

0.4 Consider the system of congruences

$$x \equiv 2 \pmod 3$$
$$x \equiv 1 \pmod 6.$$

Does this have a solution? If so, can you find at least one such solution?

# 1 Preliminaries: Definitions and Notation

Let's begin with some very basic notation:

*Notation.* The sets below are denoted as follows:

1.1 The set of *natural numbers*, denoted $\mathbb{N}$, is the set $\{1,2,3,...\}$ of all positive integers.

1.2 The set of all *integers*, denoted $\mathbb{Z}$, is the set $\{\ldots,-3,-2,-1,0,1,2,3,\ldots\}$.

1.3 The set of all *rational numbers*, denoted $\mathbb{Q}$, is the set

$$\mathbb{Q} := \left\{ \frac{r}{s} : r, s \in \mathbb{Z}, s \neq 0 \right\}$$

consisting of all quotients of integers with nonzero denominator.

That is, the set of rational numbers is the set of all *fractions* of integers, so long as we do not divide by zero.

1.4 The set of all *real numbers* is denoted $\mathbb{R}$.

Next, we introduce the following fundamental definitions:

**Definition 1.1.** Let $a, b \in \mathbb{Z}$. We say *$a$ divides $b$*, denoted $a \mid b$, if and only if there exists some $n \in \mathbb{Z}$ such that $an = b$. (Equivalently: $a$ is a *divisor* of $b$, and $b$ is a *multiple* of $a$.)

**Example 1.2.** Some examples of divisibility:

(a) $2 \mid 6$ since $2 \cdot 3 = 6$ and $3 \in \mathbb{Z}$.

(b) $3 \nmid 5$, since there is no *integer* $n$ such that $3n = 5$.

(c) For every integer $a$, $a \mid 0$, since $a \cdot 0 = 0$.

**Definition 1.3.** Let $a, b, m \in \mathbb{Z}$. Then $a$ is *congruent to $b$ modulo $m$*, denoted $a \equiv b \pmod{m}$, if and only if $m \mid a - b$.

**Example 1.4.** Some examples of congruence:

(a) $17 \equiv 3 \pmod{7}$, since $7 \mid 17 - 3$.

(b) $9 \not\equiv 4 \pmod{6}$, since $6 \nmid 9 - 4$.

(c) For all $m \in \mathbb{Z}$, $m - 1 \equiv -1 \pmod{m}$. This is because for all $m$, $m \mid [(m-1) - (-1)]$.

*Remark.* Intuitively, $a \equiv b \pmod{m}$ if and only if $a$ and $b$ have the same remainder upon being divided by $m$. Congruence modulo $m$ is also an *equivalence relation*. Further, in practice we are typically interested only in the case where $m \geq 2$, even though this definition makes sense for all integers $m$.

**Definition 1.5.** Let $a, b$ be integers. If at least one of $a, b$ is nonzero, and if $d$ is the largest common divisor of $a$ and $b$, we say $d$ is the *greatest common divisor* of $a$ and $b$, denoted $\gcd(a, b)$. If $a = b = 0$, we define $\gcd(0, 0) := 0$.

If $n \geq 3$ and $a_1, a_2, \ldots, a_n$ are all integers, we define $\gcd(a_1, a_2, \ldots, a_n)$ recursively by $\gcd(a_1, a_2, \ldots, a_n) := \gcd\big(\gcd(a_1, a_2, \ldots, a_{n-1}), a_n\big)$.

*Remark.* The ordering of the $a_i$ does not matter when considering the greatest common divisor of three or more integers. Can you explain why?

**Definition 1.6.** Let $a, b$ be integers. We say that $a$ and $b$ are *relatively prime* or *coprime* if and only if $\gcd(a, b) = 1$.

If $a_1, a_2, \ldots, a_n$ are integers, we say that the integers $a_1, a_2, \ldots, a_n$ are relatively prime if and only if $\gcd(a_1, a_2, \ldots, a_n) = 1$. Further, we say that $a_1, a_2, \ldots, a_n$ are *pairwise relatively prime* or *pairwise coprime* if and only if $\gcd(a_i, a_j) = 1$ whenever $i \neq j$.

**Example 1.7.** When $n \geq 3$, pairwise coprimality is a stronger condition than mere coprimality; that is, a pairwise relatively prime set is always relatively prime, but there are relatively prime sets that are not pairwise relatively prime.

For example, $\gcd(6,10,15) = 1$, so $\{6,10,15\}$ forms a relatively prime set. However, $\gcd(6,10) = 2 > 1$, $\gcd(6,15) = 3 > 1$, and $\gcd(10,15) = 5 > 1$, so this set is *not* pairwise relatively prime. You might consider how, for each positive integer $n \geq 3$, to form a set of $n$ positive integers such that $a_1, a_2, \ldots, a_n$ is relatively prime, but this set is not pairwise relatively prime.

**Definition 1.8.** Let $a, m$ be integers. We say that the integer $b$ is a *modular multiplicative inverse* of $a$ modulo $m$ (or, if context is clear, simply *inverse*) if and only if $ab \equiv 1 \pmod{m}$.

We assert the following theorem without proof, since it will be enormously helpful in what follows:

**Theorem 1.9.** *Let $a, m$ be integers. Then $a$ has a multplicative inverse modulo $m$ if and only if* $\gcd(a,m) = 1$.

**Example 1.10.** (a) 3 has a multiplicative inverse mod 17. In the context of Theorem 1.9, this is because $\gcd(3,17) = 1$. Explicitly, note that $3 \cdot 6 = 18 \equiv 1 \pmod{17}$, so

(b) 9 does *not* have a multiplicative inverse modulo 15. This is because $\gcd(9,15) = 3 > 1$. Can you see why the congruence $9b \equiv 1 \pmod{15}$ has no solution where $b$ is an integer?

## 2 Systems of Congruences

Consider the following system of congruences:

$$x \equiv 2 \pmod{3} \tag{2.1}$$
$$x \equiv 1 \pmod{5}. \tag{2.2}$$

How might we interpret this geometrically?

In Figure 2.1, we consider three copies of the set of integers. The black points represent all integers, at least that we can see in this finite region. The red points are those satisfying (2.1), and the blue points are those satisfying (2.2). Visually, then, the system (2.2)–(2.2) above has a solution $x$ if and only if there is some black point that is simultaneously red and blue. As we see, $x = 11$ is such a "purple point". For (2.1)–(2.2), we can see in Figure 2.1 that there is at least one solution: $x = 11$. Further, the section shown in the figure repeats every $3 \cdot 5 = 15$ units, and it follows that every $x$ such that $x \equiv 11 \pmod{15}$ is also a solution.

Next, let's modify (2.1)–(2.2): Consider the following system of congruences:

$$x \equiv 2 \pmod{3} \tag{2.3}$$
$$x \equiv 1 \pmod{6}. \tag{2.4}$$

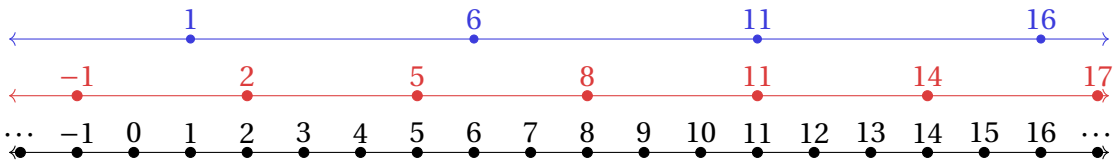


Figure 2.1: Visualizing the system of congruences $x \equiv 2 \pmod 3$ and $x \equiv 1 \pmod 5$.

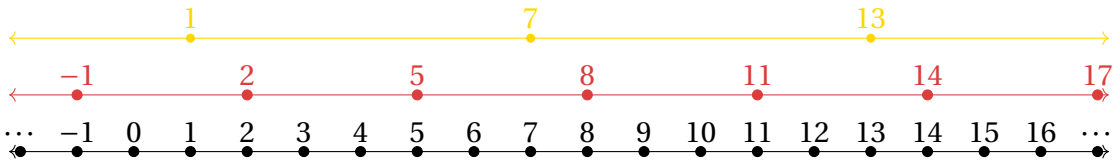


Figure 2.2: Visualizing the system of congruences $x \equiv 2 \pmod 3$ and $x \equiv 1 \pmod 6$.

How might we interpret this geometrically? In Figure 2.2, we now seek a point that is simultaneously red, satisfying (2.3), and yellow, satisfying (2.4). However, we see that there is nowhere the red and yellow points align to produce a "orange point".

In general, let $a, b, m, n$ be integers. Our goal is to determine whether the system of congruences

$$x \equiv a \pmod m \tag{2.5}$$
$$x \equiv b \pmod n. \tag{2.6}$$

Can we determine when (2.5)–(2.6) has a solution? If so, can we compute all solutions?

More generally, if we have $k$ congruences of the form

$$x \equiv a_1 \pmod{m_1} \tag{2.7}$$
$$x \equiv a_2 \pmod{m_2} \tag{2.8}$$
$$\vdots$$
$$x \equiv a_k \pmod{m_k}, \tag{2.9}$$

then when does (2.7)–(2.9) have a common solution $x$? If so, can we compute all such $x$ satisfying this system of congruences?

*Exercises:*

2.1 Does the system

$$x \equiv 3 \pmod 4$$
$$x \equiv 4 \pmod 7$$

have a solution? If so, what is it?

2.2 Does the system

$$x \equiv 3 \pmod 4$$
$$x \equiv 4 \pmod{10}$$

have a solution? If so, what is it?

2.3 Does the system

$$x \equiv 2 \pmod 4$$
$$x \equiv 4 \pmod 6$$

have a solution? If so, what is it?

# 3 The Chinese Remainder Theorem: Simplest Case

With Section 2 as background, we begin with our first answer to the question posed there and in the abstract.

**Theorem 3.1** (The Chinese Remainder Theorem: Simplest Case)**.** *Let $a, b, m, n$ be integers. Then if* $\gcd(m,n) = 1$*, the system of congruences*

$$x \equiv a \pmod m \tag{3.1}$$
$$x \equiv b \pmod n. \tag{3.2}$$

*always has a solution.*

*Furthermore, all such solutions are congruent modulo $mn$, in the following sense: if $x, y$ both satisfy* (3.1)–(3.2)*, then $x \equiv y \pmod{mn}$.*

*Remark.* Theorem 3.1 is *not* an if-and-only-if statement. It guarantees that if the moduli are relatively prime, then there is a solution to the system of congruence. There may be solutions, though, even when $\gcd(a,b) \neq 1$; see, for example, Exercise #2.3 above.

*Exercises:* The goal of the exercises in this section will be to explain why this is true, and to produce an explicit formula for solutions to (3.1)–(3.2) in terms of $a, b, m, n$ when $\gcd(m, n) = 1$.

3.1 Let $a, b, m, n$ be as in Theorem 3.1, so that $\gcd(m, n) = 1$.

(a) Prove that there exist integer $m', n'$ such that $mm' \equiv 1 \pmod{n}$ and $nn' \equiv 1 \pmod{n}$.

(b) To produce a solution to our system, the simplest possible formula to hope for would be a linear function of $a$ and $b$ of the form

$$x = Pa + Qb,$$

where $P$ and $Q$ are integers depending on $a, b, m, n$. If we reduce this mod $m$, we should recover $a$, and if we reduce mod $n$, we should recover $b$. In particular, this suggests that we would hope that $P$ reduces to $0 \pmod{n}$, and that $Q$ reduces to $0 \pmod{m}$.

Prove that if we set

$$P := nn',$$
$$Q := mm',$$

then $x = Pa + Qb = nn'a + mm'b$ satisfies our system of congruences.

*Remark.* For computational exercises, one in general will have to compute the modular multiplicative inverses $m'$ of $m$ modulo $n$ and $n'$ of $n$ modulo $m$.

(c) Let $x, y$ be solutions to (3.1)–(3.2). Prove that $x \equiv y \pmod{mn}$.

# 4 The Chinese Remainder Theorem: More General Case

We introduce generalizations of Theorem 3.1 in the exercises here.
*Exercises:* Throughout, consider the system of congruences in (2.7)–(2.9).

4.1 Assume that $\{m_1, m_2, \ldots, m_k\}$ is pairwise relatively prime.

For each $i$, prove that there is an integer $m_i'$ such that

$$m_i'(m_1 m_2 \cdots m_{i-1} m_{i+1} \cdots m_k) \equiv 1 \pmod{m_i};$$

that is, $m_i'$ is the modular multiplicative inverse mod $m_i$ for the product over all all the moduli *except* $m_i$.

4.2 Let $k \geq 3$, and assume the $m_i$ are pairwise relatively prime. Using Exercise #4.1, provide a formula for a general solution to the system of congruences.

4.3 Prove that if the $m_i$ are pairwise relatively prime, then any solution is unique modulo $m_1 m_2 \cdots m_k$.

4.4 *Open Question:* Can you provide a test to determine precisely when our system of congruences has a solution, even when the $m_i$ are *not* pairwise relatively prime?

4.5 Let $a_1, \ldots, a_k$ be integers, and let $m_1, \ldots, m_k$ be pairwise relatively prime integers. If $f(x)$ is a polynomial with integer coefficients, discuss whether

$$f(x) \equiv a_i \pmod{m_i} \text{ for all } i$$

has a solution $x$ in the integers.

# 5 Additional Exercises

The following exercises are more challenging. Many are taken from mathematics competitions, including William Lowell Putnam Mathematical Competition (or simply "The Putnam"), a notoriously difficult exam for undergraduate students.

5.1 There are four consecutive positive integers (natural numbers) less than 2005 such that the first (smallest) number is a multiple of 5, the second number is a multiple of 7, the third number is a multiple of 9 and the last number is a multiple of 11. What is the first of these four numbers?

*Note:* This appears as Question 9 from the Individual Contest of the 2005 *Primary Mathematics World Contest* (PMWC) form Hong Kong.

5.2 The following is Problem B4 from the 1955 Putnam, provided here:

"Can we find n such that $\mu(n) = \mu(n+1) = \cdots = \mu(n+1000000) = 0$? [The Möbius function $\mu(r) = 0$ if and only if $r$ has a square factor $> 1$.]"

*Note:* The full definition of the *Möbius function*, denoted $\mu$,[1] is not relevant for our purposes. It is enough to understand the question in the following context: can we produce an arbitrarily long finite sequence of integers, all of which are *squarefree* (in the sense of not being divisible by the square of any prime number)?

[1] Note that $\mu$ is the Greek letter "mu", pronounced "myoo".

5.3 The following is the first example provided in [2]:

"Everyone knows $5^2$ ends in 5 and $6^2$ ends in 6. Your task: find multi-digit numbers whose squares end in themselves (e.g., $25^2$ ends in 25, $76^2$ ends in 76, ...)."

*Note:* The advanced group of Chapel Hill Math Circle explored a highly related question in the session "An Introduction to $p$-adic Numbers, Part 1 of 2". In Exercises #1.7 from that session, we explored how to construct a nontrivial 10-adic integer $y$ such that $y^2 = y$. As a corollary, in Exercise #1.8, we showed that in $\mathbb{Z}_{10}$, the set of all 10-adic integers, there are *nonzero* elements $x, y$ such that $xy = 0$ in $\mathbb{Z}_{10}$.

5.4 Let $p, q$ be distinct positive prime integers, and let $f(x)$ be a polynomial with integer coefficients. (That is, $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, where each $a_j$ is an integer.) Assume that for every integer $a$, either $f(a)$ is a multiple of $p$ or $f(a)$ is a multiple of $q$. Prove that For one of these two primes, call it $p'$, $f(a)$ is a multiple of $p'$.

For example, say $f(x)$ is a polynomial with integer coefficients. For every integer $a$, either $f(a)$ is a multiple of 2, or $f(a)$ is a multiple of 3. Then one of these primes works *everywhere*: either every $f(a)$ is a multiple of 2, or every $f(a)$ is a multiple of 3.

*Note:* This is a simplified version of Theorem 4.4 of [1]. The example with $p := 2$, $q := 3$ is enumerated as an example in [2].

5.5 We have the following result for computing the remainder upon dividing a polynomial by certain linear polynomials:

**Theorem 5.1** (The Polynomial Remainder Theorem)**.** *Let $f(x)$ be a polynomial (with, say, real coefficients), and let $r$ be a real number. Then the remainder upon dividing $f(x)$ by the linear polynomial $x - r$ is the number $f(r)$.*

That is, to compute the polynomial remainder upon dividing $f(x)$ by $x - r$, evaluate $f(x)$ at the number $r$.

(a) Let $f(x) := x^2 + 2x - 1$. What is the remainder upon dividing $f(x)$ by $x+4$? Compute this using the Polynomial Remainder Theorem, then verify your answer by long division.

(b) Explain how Theorem 5.1 is equivalent to the following statement:

**Theorem 5.2.** *Let $f(x)$ be a polynomial with real coefficients. If $r$ is a real number, then*

$$f(x) \equiv f(r) \pmod{x-r}. \tag{5.1}$$

*Note:* What does notation like "$f(x) \equiv g(x) \pmod{m(x)}$" even mean in the first place?

(c) Let $r_1, r_2, \ldots r_n$ be $n$ distinct real numbers, and let $b_1, b_2, \ldots, b_n$ be any real numbers. (The $r_i$ may not include any repetitions, but the $b_i$ need not be distinct.) Prove that there is some polynomial $f(x)$ such that $f(r_1) = b_1$, $f(x_2) = b_2, \ldots,$ and $f(x_n) = b_n$.

That is, prove that if you have $n$ distinct points $r_1, r_2, \ldots r_n$ in the domain, then you can create a polynomial $f(x)$ whose values at the $r_i$ are whatever you want.

*Remark.* This appears as Theorem 4.19 in [1] and as The Lagrange Interpolation Theorem in [5].

5.6 For every positve integer $n$, define

$$f(n) = \frac{n}{1 \cdot 3 \cdot 5 \cdot \cdots \cdot (2n+1)}.$$

Suppose that the sum $f(1) + f(2) + \cdots + f(2020)$ can be expressed as $\frac{p}{q}$ for relatively prime integers $p$ and $q$. Find the remainder when $p$ is divided by 1000.

*Note:* This appears as Problem 7 from the 2020 *Christmas Invitational Mathematics Examination I* (CIME I)

5.7 The following military application of the Chinese Remainder Theorem appears as Exercise I.3.24 on page 27 of [3]:

"Let $N$ be an extremely large secret integer used to unlock a missile system, i.e., knowing $N$ would enable one to launch the missiles. Suppose you have a commanding general and $n$ different lieutenant generals. In the even that the commanding general (who knows $N$) is incapacitated, you want the lieutenant generals each to have enough partial information about $N$ so that any three of them (but never two of them) can agree to launch the missiles.

(a) "Let $p_1, \ldots, p_n$ be $n$ different primes, all of which are greater than $\sqrt[3]{N}$ but much smaller than $\sqrt{N}$. Using the $p_i$, describe the partial information about $N$ that should be given to the lieutenant generals.

(b) "Generalize this system to the situation where you want any set of $k$ ($k \geq 2$) of the lieutenant generals, working together, to be able to launch the missiles (but a set of $k-1$ of them can never unlock the system). Such a set-up is called a *$k$-threshold system for sharing a secret*."

*Followup:* Can you explain what real-world considerations might motivate trying to find such a threshold system?

# References

[1] Keith Conrad. The Chinese remainder theorem. https://kconrad.math.uconn.edu/blurbs/ugradnumthy/crt.pdf. online: retrieved August 28, 2024.

[2] Keith Conrad. reply to "Applications of the Chinese remainder theorem" (as user KConrad). https://mathoverflow.net/a/12007, May 23, 2024. online: retrieved December 9, 2016.

[3] Neal Koblitz. *A Course in Number Theory and Cryptography*. Springer-Verlag New York, Inc., second edition edition, 1994.

[4] Ivan Niven, Herbert S. Zuckerman, and Hugh L. Montgomery. *An Introduction to the Theory of Numbers*. John Wiley & Sons, Inc., New York, fifth edition, 1991.

[5] Qiaochu Yuan. The Chinese remainder theorem and Lagrange interpolation. https://artofproblemsolving.com/community/c1157h990758_the_chinese_remainder_theorem_and_lagrange_interpolation, November 5, 2008. online: retrieved August 28, 2024.