Number Theory – II

QF Math Circle
November 24 2025
Dr. Hasan Demirkoparan

1

Chinese Remainder Problem

Chinese Remainder Problem:

A general in ancient China wanted to count his troops. Suppose that when his soldiers were split into three equal groups there was one soldier left over, when split into five equal groups there were two left over, when split into seven equal groups there were four left over. What is the minimum number of soldiers that makes this possible?

2

2

Chinese Remainder Problem

Chinese Remainder Problem:

Let x be the minimum number of soldiers that makes this possible. Then,

x must have the remainder **one** divided by **three**,

must have the remainder **two** when divided by **five** and must have the remainder **four** when divided by **seven**.

Remark: we can use linear Diophantine Equation Theorem recursively to find x but will develop new terminology to solve the problem. This new terminology will be helpful to solve many other problems.

3

3

Congruence

Definition: Given a natural number n, the integers x and y are congruent modulo n if x − y is divisible by n.

We write this as $x \equiv y \pmod{n}$.

The number n is called the modulus.

Examples:

- $6 \equiv 20 \pmod{14}$
- $80 \equiv 230 \pmod{50}$
- $1024 \equiv 0 \pmod{16}$
- $10^n \equiv 1 \pmod{3}$ for all $n \in N$.

4

4

Congruence

Congruence modulo n partitions the set of integers into n "equivalence classes". These classes are often called remainder classes or congruence classes modulo n. The set of congruence classes is written as Z_n or Z / nZ.

Example:

1. Congruence modulo 2 partitions the set of integers into two sets:

the set of even integers and the set of odd integers.

All even integers are congruent to each other modulo 2.

All odd integers are congruent to each other modulo 2.

2. Congruence modulo 3 partitions the set of integers into three sets:

$S_0 = \{\ldots,-3, 0, 3, 6,\ldots\}$,

$S_1 = \{\ldots,-2, 1, 4, 7,\ldots\}$,

$S_2 = \{\ldots,-1, 2, 5, 8,\ldots\}$.

5

5

Congruence

Lemma: If $a \equiv r \pmod n$ and $b \equiv s \pmod n$, then

- $a + b \equiv r + s \pmod n$ and
- $ab \equiv rs \pmod n$.

Proof:

Write $a = q_1 n + r$ and $b = q_2 n + s$.

Then $a + b = n(q_1 + q_2) + (r + s)$.

Thus $a + b \equiv r + s \pmod n$.

Similarly $ab = (q_1 n + r)(q_2 n + s) = n(nq_1q_2 + rq_2 + sq_1) + rs$.

Thus $ab \equiv rs \pmod n$.

6

6

Congruence

Examples:

17 ≡ 5 (mod 6) and 44 ≡ 2 (mod 6).

17 + 44 = 61 = 6·10 + 1 ≡ 1 mod 6.

Alternatively: 17 + 44 ≡ 5 + 2 ≡ 7 ≡ 1 (mod 6).

17·44 = 748 = 6·124 + 4 ≡ 4 (mod 6).

Alternatively: 17·44 ≡ 5·2 ≡ 10 ≡ 4 (mod 6).

Exercises: Evaluate a + b and ab modulo n.

1. a = 52, b = 90, n = 11.
2. a = 40, b = 68, n = 16.
3. a = 1326, b = 1729, n = 10.
4. a = 42311, b = 9315, n = 3.

7

7

Congruence

We have proved that if a ≡ b (mod n) and c ≡ d (mod n), then a + c ≡ b + d (mod n) and ac ≡ bd (mod n).

Question: How about subtraction and division?

Question: If x + z ≡ y + z (mod n), is it true that x ≡ y (mod n)?
Answer: YES! (proof?)

Question: If xz ≡ yz (mod n), is it true that x ≡ y (mod n)?
Answer: Not always true.
Example: 15 . 2 ≡ 9 . 2 (mod 4) but 15 ≢ 9 (mod 4).

Question: What conditions can we place on z and/or n to make this true?

8

8

Chinese Remainder Problem

Chinese Remainder Problem:

Let x be the minimum number of soldiers that makes this possible. Then,

x must have the remainder **one** divided by **three**,

must have the remainder **two** when divided by **five** and must have the remainder **four** when divided by **seven**.

By using the congruence, we can compactly write the question as: Find smallest positive integer x such that

$$x \equiv 1 \ (mod\ 3)$$
$$x \equiv 2 \ (mod\ 5)$$
$$x \equiv 4 \ (mod\ 7)$$

9

9

Chinese Remainder Problem

Theorem (Chinese Remainder Theorem):
If $\{n_i\}$ is a set of r natural numbers that are pairwise relatively prime, and $\{a_i\}$ are any r integers, then the system of congruences $x \equiv a_i \pmod{n_i}$ has a unique solution modulo $N = n_1.n_2.n_3 \ldots n_r$.

10

10

Chinese Remainder Problem

Consider $x \equiv 1 \pmod 3$

$x \equiv 2 \pmod 5$

$x \equiv 4 \pmod 7$.

Note that $n_1 = 3$, $n_2 = 5$, $n_3 = 7$.

As gcd (3, 5) = gcd (5, 7) = gcd (3, 7) =1, moduli are pairwise relatively prime. We can use the previous algorithm.

N = 3 5 7 = 105. $N_1 = 35$, $N_2 = 21$, $N_3 = 15$.

Also note that $a_1 = 1$, $a_2 = 2$, $a_3 = 4$.

$N_1 y_1 \equiv 1 \pmod{n_1}$, $N_2\ y_2 \equiv 1 \pmod{n_2}$, $N_3 y_3 \equiv 1 \pmod{n_3}$.

$35y_1 \equiv 1 \pmod 3$, $21\ y_2 \equiv 1 \pmod 5$, $15y_3 \equiv 1 \pmod 7$.

11

11

Chinese Remainder Problem

Consider $x \equiv 1 \pmod 3$

$x \equiv 2 \pmod 5$

$x \equiv 4 \pmod 7$.

$N_1 y_1 \equiv 1 \pmod{n_1}$, $N_2\ y_2 \equiv 1 \pmod{n_2}$, $N_3 y_3 \equiv 1 \pmod{n_3}$.

$35y_1 \equiv 1 \pmod 3$, $21\ y_2 \equiv 1 \pmod 5$, $15y_3 \equiv 1 \pmod 7$.

$2y_1 \equiv 1 \pmod 3$, $y_2 \equiv 1 \pmod 5$, $y_3 \equiv 1 \pmod 7$.

Hence $y_1 = 2$, $y_2 = 1$, $y_3 = 1$.

$x \equiv N_1\ y_1\ a_1 + N_2\ y_2\ a_2 + N_3\ y_3\ a_3 \pmod N$

$x \equiv 35\ \ 2\ \ 1 + 21\ \ 1\ \ 2 + 15\ \ 1\ \ 4 \pmod{105}$

$x \equiv 70 + 42 + 60 \pmod{105}$

$x \equiv 172 \pmod{105}$. Hence x= 172 – 105 = 67 soldiers.

12

12

Chinese Remainder Problem

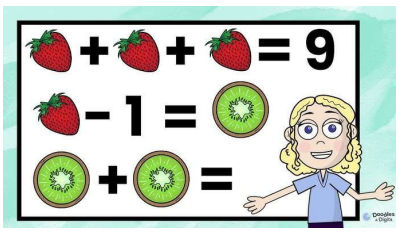
Question 1: A troop of 17 Monkeys store their bananas in 11 piles of equal size each containing more than one banana with a 12th pile of 6 left over. When they divide bananas into 17 equal groups, none remain. What is the smallest number of bananas that they can have?

13

13

Chinese Remainder Problem

Question 2: There is to be a campus-wide activity in which students compete in teams to solve puzzles. Everyone at CMUQ is expected to participate. Unfortunately, when we make groups of 3, there is one person left over. If we make groups of 5, then four people are left over. If we make groups of 7, five people are left over. How many students are there at CMUQ? (We know the answer is somewhere between 400 and 450.)



14

14

ISBN

International Standard Book Numbers (ISBN):

Since 1968, most published books have been assigned a ten-digit number called the International Standard Book Number-abbreviated ISBN- which identifies

the country of publication, the publisher, and the book itself. In fact, all relevant information is stored in the first nine digits; the tenth digit is a check digit whose sole purpose is to give us confidence that the first nine digits are correct.

If the digits of an ISBN are denoted $a_1, a_2, \ldots, a_{10}$, with the first nine in the range 0-9, then a_{10} is chosen in the range 0-10 so that $a_1 + 2\,a_2 + 3\,a_3 + \ldots + 9\,a_9 + 10\,a_{10} \equiv 0 \pmod{11}$. If a_{10} happens to be 10, it is recorded as an X.

15

15

ISBN

Example:

The ISBN of a textbook is 0-13-092000-2.

Note that this can be verified easily.

$1(0) + 2(1) + 3(3) + 4(0) + 5(9) + 6(2) + 7(0) + 8(0) + 9(0) + 10(2) \equiv 88 \equiv 0 \pmod{11}$.

Question: The ISBN of a textbook is 0-13-468955-0.

Verify that it is a valid ISBN number.

16

16