MATH 8B: HANDOUT 25 [MAY 4, 2025]
NUMBER THEORY 6: CHINESE REMAINDER THEOREM

Summary of previous results

Modular inverse. Recall that we say that t is inverse of a mod n if $at \equiv 1 \mod n$.

Theorem 1. *A number a has an inverse mod n if and only if a is relatively prime with n, i.e.* $\gcd(a, n) = 1$.

This theorem is easily proven using Euclid's algorithm (recall how!). With it, we can easily solve equations of the form

$$ax \equiv b \mod m$$

if a has an inverse h modulo m, i.e., $ha \equiv 1 \mod m$: just multiply both sides by h and observe that

$$hax \equiv x \equiv hb \mod m\,.$$

Least common multiple. For any two natural numbers a, b, there is a smallest number which is a multiple of both. It is called the *least common multiple* of a and b, denoted lcm(a, b). (Consider the set of common multiples of a and b; it is non-empty since ab is in it. By the well-ordering principle, it has a smallest element.)

Theorem 2. *Let a, b be relatively prime. Then any common multiple of a, b is a multiple of ab; in particular, the least common multiple of a, b is ab.*

Proof. Assume that m is a common multiple of a, b. Then $m = ta$ for some t. Since m is also a multiple of b, we get $ta \equiv 0 \mod b$. Since a, b are relatively prime, a is invertible mod b. Multiplying both sides of congruence by inverse of a mod b, we get $t \equiv 0 \mod b$, so t is divisible by b, i.e. $t = sb$ for some t. Thus, $m = ta = sab$ is a multiple of ab. □

Chinese Remainder Theorem

From the previous result, we can immediately deduce that if a, b are relatively prime, then x is divisible by ab if and only if it is divisible by a and b:

$$\begin{cases} x \equiv 0 \mod a \\ x \equiv 0 \mod b \end{cases} \iff x \equiv 0 \mod ab$$

This is also a special case of the following famous result below.

Theorem 3 (Chinese Remainder Theorem)**.** *Let a, b be relatively prime. Then, for any choice of k, l, the following system of congruences:*

$$x \equiv k \mod a$$

$$x \equiv l \mod b$$

has a unique solution mod ab, i.e. it has solutions and any two solutions differ by a multiple of ab. In particular, there exists exactly one solution x such that $0 \le x < ab$.

Proof. Let $x = k + ta$ for some integer t. Then x satisfies the first congruence, and our goal will be to find t such that x satisfies the second congruence.

To do this, write $k + ta \equiv l \mod b$, which gives $ta \equiv l - k \mod b$. Notice now that because a, b are relatively prime, a has an inverse $h \mod b$ such that $ah \equiv 1 \mod b$. Therefore $t \equiv h(l-k) \mod b$, and $x = k + ah(l-k)$ is a solution to both the congruences.

To see uniqueness, suppose x and x' are both solutions to both congruences such that $0 \le x, x' < ab$. Then we have

$$x - x' \equiv k - k \equiv 0 \mod a$$
$$x - x' \equiv l - l \equiv 0 \mod b$$

Thus $x - x'$ is a multiple of both a and b; because a, b are relatively prime, this implies that $x - x'$ is a multiple of ab. Thus, any two solutions differ by a multiple of ab. □

Classwork

Suppose we are given a and b which are relatively prime. Let a' be the inverse of a mod b, and b' the inverse of b mod a. Now suppose we have a system of congruences as above: $x \equiv k \mod a$, and $x \equiv l \mod b$. Consider the number $m = kbb' + laa'$. What properties does it satisfy modulo a and b?

Homework

1. (a) Find the inverse of 7 mod 11.
(b) Find all solutions of the equation $7x \equiv 5 \mod 11$.

2. Solve the following systems of congruences

(a)
$$\begin{cases} x \equiv 1 \mod 3 \\ x \equiv 1 \mod 5 \end{cases}$$

(b)
$$\begin{cases} z \equiv 1 \mod 5 \\ z \equiv 6 \mod 7 \end{cases}$$

3. (a) Find the remainder upon division of 23^{2021} by 7.
(b) Find the remainder upon division of 23^{2021} by 70. [Hint: use $70 = 7 \cdot 10$ and Chinese Remainder Theorem.]

4. (a) Find the remainder upon division of 24^{46} by 100.
(b) Determine all integers k such that $10^k - 1$ is divisible by 99.

5. In the calendar used in many Asian countries, every year is associated with one of 12 animals (e.g. 2021 is the Year of the Ox), repeating cyclically. Also, every year is associated with one of 5 elements: wood, fire, earth, metal, water (2021 is the year of metal). Can you find the period of this calendar? That is, in how many years will we return to the same animal and element?

6. Daniil has number of toys. If he tries to divide them equally among 4 kids, one toy is left over. The same happens if he tries to divide them equally among 5 or 6 kids; however, the toys can be divided equally among 7 kids. What is the smallest number of toys Daniil can have? [Hint: if number of toys is n, what can you say about the number $n-1$?]

7. (a) Assume that $\gcd(a, b) = d$. Let $a' = a/d, b' = b/d$. Show that then numbers a', b' are relatively prime, and deduce from that that any common multiple of a, b is a multiple of $da'b'$.
(b) Use the previous problem to show that for any positive integers a, b we have $\gcd(a, b) \cdot \text{lcm}(a, b) = ab$.