

MATH 8: HANDOUT 28 [MAY 5, 2024]
NUMBER THEORY 6: CHINESE REMAINDER THEOREM

SUMMARY OF PREVIOUS RESULTS

Modular inverse

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

Theorem. 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

$$ax \equiv b \pmod m$$

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

$$hax \equiv x \equiv hb \pmod m.$$

Least common multiple

Theorem. 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 $ta \equiv 0 \pmod b$. Since a, b are relatively prime, a is invertible mod b . Multiplying both sides of congruence by inverse of $a \bmod b$, we get $t \equiv 0 \pmod b$, so t is divisible by b , i.e. $t = sb$ for some t . Thus, $m = ta = sab$ is a multiple of ab . \square

CHINESE REMAINDER THEOREM

From the previous result, we can 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 :

$$\begin{cases} x \equiv 0 \pmod a \\ x \equiv 0 \pmod b \end{cases} \iff x \equiv 0 \pmod{(ab)}$$

Proof. Indeed, if x is divisible by a , then $x = ta$ for some t . Also, since $\gcd(a, b) = 1$, then there is inverse h : $ha \equiv 1 \pmod b$ and $t \equiv hx \equiv 0 \pmod b$. Therefore $t = sb$ for some s and $x = sab$ and $x \equiv 0 \pmod{(ab)}$. \square

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

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

$$\begin{aligned} x &\equiv k \pmod a \\ x &\equiv l \pmod b \end{aligned}$$

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 $0 \leq x < ab$.

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 $k + ta \equiv l \pmod b$, which gives $ta \equiv l - k \pmod b$. Notice now that because a, b are relatively prime, a has an inverse $h \pmod b$ such that $ah \equiv 1 \pmod b$. Therefore $t \equiv h(l - k) \pmod b$, 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 $0 \leq x, x' < ab$. Then we have

$$\begin{aligned} x - x' &\equiv k - k \equiv 0 \pmod a \\ x - x' &\equiv l - l \equiv 0 \pmod b \end{aligned}$$

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 . \square

HOMEWORK

1. (a) Find inverse of 7 mod 11.
(b) Find all solutions of the equation

$$7x \equiv 5 \pmod{11}$$

2. Solve the following systems of congruences

(a)

$$\begin{cases} x \equiv 1 \pmod{3} \\ x \equiv 1 \pmod{5} \end{cases}$$

(b)

$$\begin{cases} z \equiv 1 \pmod{5} \\ z \equiv 6 \pmod{7} \end{cases}$$

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). 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? I.e., in how many years will we return to the same animal and element?
6. (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 $\gcd(a, b) \cdot \text{lcm}(a, b) = ab$.