May 10, 2026 Math 8

Handout 27. Number theory 6: Modular arithmetic. Chinese remainder theorem.

Recap of previous results

Definition of the modular inverse. We say that x is inverse of a mod m if $ax \equiv 1 \bmod m$.

Theorem 13. A number a has an inverse mod m if and only if a is relatively prime with m, i. e., $\gcd(a, m) = 1$.

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

$$ax \equiv b \bmod m$$

if a has an inverse h modulo m, i.e., $ah \equiv 1 \bmod m$, we multiply both sides with h and observe that

$$hax \equiv x \equiv hb \bmod m$$

Least common multiple

Theorem 15a. Let a, b be relatively prime, $\gcd(a, b) = 1$. 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 $m = aq$ for some q. Since m is also a multiple of b, we get $aq \equiv 0 \bmod b$. Since a, b are relatively prime, a is invertible mod b. Multiplying both sides of congruence by inverse of a mod b, we get $q \equiv 0 \bmod b$, so q is divisible by b, i.e. $q = sb$ for some s. Thus, $m = qa = sab$ is a multiple of ab. □

Chinese remainder theorem

The previous result leads to the following theorem.

Theorem 15b. Let a, b be relatively prime, $\gcd(a, b) = 1$. Then x is divisible by ab if and only if it is divisible by both a and b:

$$\begin{cases} x \equiv 0 \bmod a \\ x \equiv 0 \bmod b \end{cases} \Leftrightarrow x \equiv 0 \bmod ab$$

Proof. Again, if x is divisible by a, then $x = qa$ for some q. Also, since $\gcd(a, b) = 1$, then there is inverse h: $ah \equiv 1 \bmod b$ and $q \equiv xh \equiv 0 \bmod b$. Therefore $q = sb$ for some s, so $x = sab$ and $x \equiv 0 \bmod (ab)$. □

This is a special case of the following famous result.

Theorem 16 (Chinese remainder theorem). Let a, b be relatively prime, $\gcd(a, b) = 1$. Then, for any choice of k, l, the following system of congruences:

$$\begin{cases} x \equiv k \bmod a \\ x \equiv l \bmod b \end{cases}$$

has a unique solution x 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 $x = k + qa$ for some integer q. Then x satisfies the first congruence, and our goal will be to find q such that x satisfies the second congruence. To do this, write $k + qa \equiv l \bmod b$, which gives $qa \equiv l - k \bmod b$. Notice now that because a, b are relatively prime, a has an inverse h mod b such that $ah \equiv 1 \bmod b$. Therefore $q \equiv h(l-k) \bmod b$, and $x = k + ah(l-k)$ is a solution to both congruences.

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

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

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. □

Homework problems

In this homework, you can use only integer numbers - no fractions or real numbers.

1.
   a. Find inverse $7 \bmod 11$
   b. Find all solutions of the equation $7x \equiv 5 \bmod 11$
2. Solve the following congruences
   a. $\begin{cases} x \equiv 1 \bmod 3 \\ x \equiv 1 \bmod 5 \end{cases}$
   b. $\begin{cases} x \equiv 1 \bmod 5 \\ x \equiv 6 \bmod 7 \end{cases}$
3.
   a. Find the remainder upon division of 23^{2025} by 7
   b. Find the remainder upon division of 23^{2025} 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. Find 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. 2025 is the Year of the Snake). Also, every year is associated with one of 5 elements: wood, fire, earth, metal, water (2025 is the year of wood). Can you find the period of this calendar? I.e., in how many years will we return to the same animal and element (e.g., the wood Snake)?
6.
   a. Assume that $gcd(a, b) = d$. Let $a' = a/d$ and $b' = b/d$. 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: $gcd(a, b) \cdot lcm(a, b) = ab$.