April 27, 2025 Math 8

Handout 26. Number theory 5: Congruences and modular arithmetic (continued).

Recap: Corollaries of Euclid's algorithm

As a corollary of Euclid's algorithm, we have proven the following result:

Theorem 8. An integer n can be written in the form

$$m = xa + yb$$

for some $x, y \in \mathbb{Z}$ if and only if m is a multiple of $d = gcd(a, b)$.

Euclid's algorithm provides an explicit way to find x and y (it provides an algorithm for solving a Diophantine equation $d = x'a + y'b$). Thus, it also gives us a way of solving congruences

$$ax \equiv m \bmod b$$

As a corollary, we get the following theorem.

Theorem 13. $\forall a, b \in \mathbb{Z}$, an equation

$$ax \equiv 1 \bmod b$$

has an integer solution $x \in \mathbb{Z}$ if and only if $gcd(a, b) = 1$, i. e. if a, b are relatively prime. Such an x is called inverse of a modulo b.

As another corollary, we see that in some (but not all) situations we can divide both sides of a congruence by a number.

Theorem 14. Let a, b be relatively prime. Then,

$$an \equiv 0 \bmod b$$

if and only if $n \equiv 0 \bmod b$.

Indeed, let h be inverse of a mod b. Then, multiplying both sides of congruence by h, we get $han \equiv 0 \bmod b$. Since $ha \equiv 1 \bmod b$, we get $n \equiv 0 \bmod b$.

Example 1. 3 is invertible mod 10 because $3 \cdot 7 \equiv 1 \bmod 10$, but is not invertible mod 9, because $3 \cdot 6 \equiv 0 \bmod 9$.

Example 2. 7 is invertible mod 15, because $7 \cdot 13 \equiv 1 \bmod 15$, but is not invertible in mod 14 because $7 \cdot 2 \equiv 0 \bmod 14$.

Homework problems

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

1. Prove that $30^{2025} + 61^{2024}$ is divisible by 31.
2. Find the last two digits of 2024^{2025}.
3. Prove that for any integer n, $n^9 - n$ is a multiple of 5. [Hint: can you prove it if $n \equiv 1 \bmod 5$? if $n \equiv 2 \bmod 5$? If … ?]
4.
    a. Find the inverses of the following numbers modulo 14 (if they exist): 3; 9; 19; 21.
    b. Of all the numbers 1,2,…,14, how many are invertible modulo 14?
5.
    a. Find inverse of 3 modulo 28
    b. Solve $3x \equiv 7 \bmod 28$ [Hint: multiply both sides by the inverse of 3...]
6. Prove that if a, b are relatively prime, and m divisible by a and also divisible by b, then m is divisible by ab. [Hint: $m = ax = by$, so $ax \equiv 0 \bmod b$]. Deduce from this that the least common multiple of a, b is ab. Is it true without the assumption that a, b are relatively prime? Can you prove this without using prime factorization?
7. Find all solutions of the following equations
    a. $5x \equiv 4 \bmod 7$
    b. $7x \equiv 12 \bmod 30$
    c. In a calendar of some ancient people, all months were exactly 30 days long; however, they used the same weeks as we do. If in that calendar, first day of a certain month is Friday, how many weeks will pass before Friday will fall on the 13th day of a month? [Hint: this can be rewritten as some congruence of the form $7x \equiv \cdots \bmod \ldots$, where x is the number of weeks.]
8. *
    a. Let p be a prime other than 2. Consider the remainders of numbers $2, 4, 6, \ldots, 2(p-1)$ modulo p. Prove that they are all different and that every possible remainder from 1 to $p-1$ appears in this list exactly once. [Hint: $2x \equiv 2y$, then $2(x-y) \equiv 0$]. Check it by writing this collection of remainders for $p = 7$.
    b. Use the previous part to show that

$$1 \cdot 2 \cdot 3 \cdot \ldots \cdot 2(p-1) \equiv 2 \cdot 4 \cdot 6 \ldots \cdot 2(p-1) \bmod p$$

Deduce from it that

$$2^{p-1} \equiv 1 \bmod p$$

    c. Show that for any a which is not a multiple of p, we have

$$a^{p-1} \equiv 1 \bmod p$$