Number Theory: Linear Congruences

Adila A. Krisnadhi

Fakultas Ilmu Komputer, Universitas Indonesia

Version date: 2022-02-16 05:26:23+07:00
Reference: Rosen, Ed.8, Ch.4

Linear congruence

Modular congruence can be generalized into **linear congruence** of the form

$$ax \equiv b \pmod{m}$$

- Given integers a, b, m with m positive, we wish to find an integer x such that the linear congruence is satisfied.
- Not every linear congruence has a solution.
  - If $\gcd(a, m)$ does **not** divide b, then the linear congruence has no solution.
  - If $\gcd(a, m)$ divides b, the linear congruence has infinitely many solutions in one or more congruence classes.
  - Special case: if $\gcd(a, m) = 1$, all solutions are in a single, unique congruence class. The solution can be obtained via **modular inverse**.
- A system of (several) linear congruences can be solved using Chinese Remainder Theorem
- Read Section 4.4 for further details.

Modular inverse

Definition

Let a, m be integers with m positive. The integer $\bar{a}$ sastisfying $\bar{a}a \equiv 1 \pmod{m}$ is called **inverse** of a **modulo** m.

- Modular inverse of an integer does **not** always exist.
- Is 5 the inverse of 3 modulo 7?
- Does 2 have an modular inverse (modulo 4)?

When is a modular inverse guaranteed to exist?

Theorem

If a and m are relatively prime with $m > 1$, then a modular inverse of a (modulo m) always exists. Furthermore, it is unique modular m, i.e., every other inverse of a modulo m is congruent to it.

If $\gcd(a, m) = 1$, inverse of a modulo m can be calculated using Bezout's theorem.

Calculate inverse of 4 modulo 7 and of 101 modulo 4620.

Solving linear congruences with modular inverse

Let $ax \equiv b \pmod{m}$ such that $\gcd(a, m) = 1$. We solve x as follows:

- Since $\gcd(a, m) = 1$, a has an inverse modulo m, say $\bar{a}$ (can be computed using Bezout's theorem).
- Since $\bar{a}$ is the inverse of a modulo m, $\bar{a}a \equiv 1 \pmod{m}$.
- Thus, $\bar{a}ax \equiv \bar{a}b \pmod{m}$, which implies the solution $x \equiv \bar{a}b \pmod{m}$

Solve the linear congruence $3x \equiv 4 \pmod{11}$.

Solving linear congruences with *back substitution*

Find a solution for x if $x \equiv 1 \pmod 5$, $x \equiv 2 \pmod 6$, and $x \equiv 3 \pmod 7$

Fermat's little theorem

Theorem

If p is a prime and a is an integer not divisible by p, then $a^{p-1} \equiv 1 \pmod{p}$. Moreover, for every integer a we have $a^p \equiv a \pmod{p}$.

If the modulus in a modular congruence is a prime p, then we can use the above theorem to compute modular exponentiation.

What is $7^{222} \bmod 11$?