01204211 Discrete Mathematics
Lecture 19: Modular arithmetic 1

Jittat Fakcharoenphol

October 10, 2015

The jug puzzle

Possibilities

Integer linear combinations

The minimum integer linear combinations

Review

In previous lectures, we studied various properties of integers and primes, and discussed primality testing algorithms. In this lecture, we will dive deeper into **modular arithmetic**, where we work with integers that "wrap around" when reaching a particular value, called the "modulus".

An example

Alice was born on July. Betty was born in the next 7 months. Before Betty was born for 3 months, Cathy was born. Dave was born 10 months before Cathy. What is Dave's birth month?

We shall encode 12 months as numbers from 0 (for January) to 11 (for December). Let a be Alice's birth month. If we denote by b, c, and d birth months of Betty, Cathy, and Dave, we can write down the conditions as follows:

$$\begin{aligned} a \bmod 12 &= 6 \bmod 12 \\ (a+7) \bmod 12 &= b \bmod 12 \\ (b-3) \bmod 12 &= c \bmod 12 \\ (c-10) \bmod 12 &= d \bmod 12 \end{aligned}$$

This is a familiar system of linear equations, but with a little twist: a "modulus" at the end.

Congruence

To deal with these equations, Carl Friedrich Gauss introduced a notation for them, called congruence. Instead of writing

$$(a + 7) \bmod 12 = b \bmod 12,$$

we write

$$a + 7 \equiv b \pmod{12}.$$

Formally, if

$$x \bmod m = y \bmod m,$$

we can write

$$x \equiv y \pmod{m}.$$

The system with the congruence notation

Let's rewrite our previous set of equations using this notation:

$$\begin{aligned} a &\equiv 6 \pmod{12} \\ a+7 &\equiv b \pmod{12} \\ b-3 &\equiv c \pmod{12} \\ c-10 &\equiv d \pmod{12} \end{aligned}$$

Now everything looks fairly much like normal equations. But do they behave the same?

Addition, subtraction, and multiplication

Suppose that, for a positive integer q, we know that

$$a \equiv b \pmod{q},$$

and

$$c \equiv d \pmod{q}.$$

It is not hard to show that

$$a + c \equiv b + d \pmod{q},$$

$$a - c \equiv b - d \pmod{q},$$

and

$$ac \equiv bd \pmod{q}.$$

Thus, we can treat a system of congruences in the same way we deal with a system of linear equations, except the division.