

## 5 Congruences

**Definition 5.1.** Two integers  $a, b$  are said to be *congruent modulo  $n$*  if  $n$  divides  $b - a$ .

$$a \equiv b \pmod{n} \Leftrightarrow n \mid (b - a).$$

The number  $n$  is called the *modulus* and is always a positive integer (usually at least 2).

Congruence modulo  $n$  is an *equivalence relation*, i.e.,

1. (reflexive)  $x \equiv x$  for all  $x$
2. (symmetric)  $x \equiv y \Rightarrow y \equiv x$
3. (transitive)  $x \equiv y \equiv z \Rightarrow x \equiv z$ .

The equivalence classes are called *congruence classes* and written:

$$\bar{a} = [a] = a + n\mathbb{Z} = \{a + nx \mid x \in \mathbb{Z}\}.$$

There are exactly  $n$  equivalence classes modulo  $n$  and they are:

$$n\mathbb{Z}, n\mathbb{Z} + 1, n\mathbb{Z} + 2, \dots, n\mathbb{Z} + n - 1.$$

The set of equivalence classes modulo  $n$  is written  $\mathbb{Z}/n\mathbb{Z}$ .

$$\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}.$$

**Theorem 5.2.** (*existence*) If  $n, a$  are relatively prime then there is a unique solution mod  $n$  to the equation

$$ax \equiv y \pmod{n} \tag{1}$$

for any integer  $y$ .

*Proof.* Whenever you hear the term “relatively prime” you should immediately write down the following equation:

$$1 = as + nt$$

Modulo  $n$  this equation says:

$$as \equiv 1 \pmod{n}.$$

Multiplying both sides by  $y$  gives:

$$asy \equiv y \pmod{n}.$$

So  $x = sy$  is a solution of the equation (1). This proves that the solution always exists.

(uniqueness) [Uniqueness proofs are always the same.] To prove uniqueness suppose that  $x'$  is another solution to (1). Then we will show that  $x \equiv x' \pmod n$ .

We are given that  $ax \equiv y \pmod n$  and  $ax' \equiv y \pmod n$ . Thus

$$ax \equiv ax' \pmod n.$$

Multiply both sides by  $s$ . Since  $sa \equiv 1 \pmod n$  we get

$$x = 1x \equiv (sa)x = s(ax) \equiv s(ax') = (sa)x' \equiv 1x' = x' \pmod n.$$

□

In terms of functions, this theorem can be stated as follows.

**Theorem 5.3.** *If  $\gcd(a, n) = 1$  then multiplication by  $\bar{a}$  gives a bijection*

$$\bar{a} \cdot : \mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}.$$

**Theorem 5.4 (Chinese remainder theorem).** *Suppose that  $m, m'$  are relatively prime. Then the equations*

$$\begin{aligned} x &\equiv b \pmod m \\ x &\equiv b' \pmod{m'} \end{aligned}$$

*have a simultaneous solution  $x$  which is unique modulo  $mm'$ .*

*Proof.* Without hesitation we write:

$$1 = sm + tm'.$$

After staring at this equation we try something else. Try  $x = b$ . This will certainly solve the first equation but maybe not the second. In fact it is  $b' - b$  too small. Look again at the equation  $1 = sm + tm'$  and we realize that the number  $sm$  when added to  $x$  will increase its remainder mod  $m'$  by 1 but not change its remainder mod  $m$ . So we do it  $b' - b$  times to get

$$x = b + (b' - b)sm.$$

This number, by construction, is a solution of the two equations. [The expression “by construction” means “by the procedure with which the number (or other quantity) was obtained.” You shouldn’t check the answer unless the checking process is shorter or more convincing than the construction process.] □

The Chinese remainder theorem can also be expressed as a bijective correspondence

$$\mathbb{Z}/mm'\mathbb{Z} \cong \mathbb{Z}/m \times \mathbb{Z}/m'.$$

Homework: