

## More Number Theory

**Wilson's Theorem.** If  $p$  is a prime, then

$$(p-1)! \equiv -1 \pmod{p}.$$

You are not responsible for the proof of Wilson's theorem.

**Theorem 4.13.** Let  $n \in \mathbb{N}$ , let  $a, b \in \mathbb{Z}$ , and let  $d = \gcd(a, n)$ .

(a) If  $d$  does not divide  $b$ , then

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

has no solutions.

(b) If  $d$  divides  $b$ , then

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

has a solution (in fact, exactly  $d$  incongruent solutions modulo  $n$ ).

*Proof.* (a) Read p. 133 in the book.

(b) We want to find an integer  $x$  such that  $ax - b$  is divisible by  $n$ , that is, show that there are integers  $x$  and  $y$  such that

$$ax - b = ny,$$

that is,

$$ax - ny = b.$$

By Theorem 3.16, this follows from the assumption that  $d = \gcd(a, n)$  divides  $b$ .

**Chinese Remainder Theorem.** How to solve the system of congruences:

$$x \equiv a_1 \pmod{n_1}$$

$$x \equiv a_2 \pmod{n_2}$$

$\vdots$

$$x \equiv a_k \pmod{n_k}$$

where any two of  $n_1, n_2, \dots, n_k$  are relatively prime.

Let

$$N_1 = n_2 n_3 \cdots n_k$$

$$N_2 = n_1 n_3 \cdots n_k$$

$$N_3 = n_1 n_2 n_4 \cdots n_k$$

$\vdots$

$$N_k = n_1 n_2 \cdots n_{k-1}.$$

Use the Euclidean algorithm (or even just guess if it is easy) to solve the following congruences separately:

$$\begin{aligned}y_1 N_1 &\equiv 1 \pmod{n_1} \\y_2 N_2 &\equiv 1 \pmod{n_2} \\&\vdots \\y_k N_k &\equiv 1 \pmod{n_k}.\end{aligned}$$

Then a solution to the original system of congruences is:

$$x = a_1 y_1 N_1 + a_2 y_2 N_2 + \cdots + a_k y_k N_k.$$

*Proof.* (1) Because since two of  $n_1, n_2, \dots, n_k$  are relatively prime, we have

$$\gcd(N_i, n_i) = 1.$$

Since  $\gcd(N_i, n_i)$  divides 1 (it's equal to 1), by Theorem 4.13, there is a solution  $y_i$  to

$$y_i N_i \equiv 1 \pmod{n_i}.$$

Then

$$a_i y_i N_i \equiv a_i \pmod{n_i}.$$

Key: If  $j \neq i$ , then

$$a_j y_j N_j \equiv 0 \pmod{n_i}.$$

Thus

$$a_1 y_1 N_1 + a_2 y_2 N_2 + \cdots + a_k y_k N_k \equiv a_i \pmod{n_i}$$

for all  $i = 1, 2, \dots, k$ .

Remark: in the last set of notes, an example of the Chinese Remainder Theorem was given.