

**book problems**

§4.4 #11 Let  $d = \gcd(m, n)$ . Then,  $d|n$  and  $d|m$ . If  $x \equiv a \pmod{n}$  and  $x \equiv b \pmod{m}$ , then  $d|x - a$  and  $d|x - b$ . Therefore,  $d|(x - b) - (x - a)$ , implying that  $d|a - b$ . Conversely, if  $d|a - b$  then there is a solution to the linear diophantine equation  $k_1m + k_2n = a - b$ . Set  $x = a - k_2n = b + k_1m$ . Then we see that  $x \equiv a \pmod{n}$  and  $x \equiv b \pmod{m}$ .

§5.2 #12 By definition

$$\binom{p-1}{k} = \frac{(p-1)!}{k!(p-1-k)!}$$

This simplifies to

$$\binom{p-1}{k} = \frac{(p-1)(p-2)\cdots(p-k)}{k!}$$

Therefore,

$$\binom{p-1}{k} \equiv \frac{(-1)(-2)\cdots(-k)}{k!} \equiv \frac{(-1)^k k!}{k!} \equiv (-1)^k \pmod{p}$$

**Non-book problems:**

**Extra credit problem:**