

## Congruences, continued

**Definition:** A set of  $m$  integers  $r_1, \dots, r_m$  is a *complete set of residues (CSR) modulo  $m$*  if every integer is congruent  $\pmod{m}$  to exactly one of the  $r_i$ 's.

**Examples:**  $\{0, \dots, m-1\}$  and all integers between  $-m/2$  and  $m/2$  (including one of them if  $m$  is even) are two CSR's modulo  $m$ .

$\{-10, 91, -3, 13, 109\}$  is a CSR modulo 5.

**Fact:** The integers modulo  $m$  form a commutative ring with unity.

**Theorem:** Let  $a, b, c, d, x, y, m$  and  $n$  be integers with  $m$  and  $n$  greater than 1. Then

(a) If  $a \equiv b \pmod{m}$  and  $c \equiv d \pmod{m}$ , then  $ax \pm cy \equiv bx \pm dy \pmod{m}$ .

(b) If  $a \equiv b \pmod{m}$  and  $c \equiv d \pmod{m}$ , then  $ac \equiv bd \pmod{m}$ .

(c) If  $f(x)$  is a polynomial with integer coefficients and  $a \equiv b \pmod{m}$ , then  $f(a) \equiv f(b) \pmod{m}$ .

(d) If  $a \equiv b \pmod{m}$  and  $n|m$ , then  $a \equiv b \pmod{n}$ .

Clock arithmetic is arithmetic modulo 12 or 24.

Addition, subtraction and multiplication of numbers modulo  $m$  work just like these operation on integers.

However, division does not always work as for integers:

$$2 \cdot 3 = 6 \equiv 18 = 2 \cdot 9 \pmod{12},$$

but  $3 \not\equiv 9 \pmod{12}$ .

In general  $ac \equiv bc \pmod{m}$  does not always imply  $a \equiv b \pmod{m}$ .

**Definition:** The *greatest common divisor* (or GCD) of two positive integers is the largest integer which divides both of them.

**Definition:** Two positive integers are *relatively prime* if their GCD is 1.

**Lemma.** If  $\gcd(a, m) = 1$  and  $0 \leq i < j < m$ , then  $ai \not\equiv aj \pmod{m}$ .

**Proof.** If not, then  $m \mid a(i-j)$ . Since  $\gcd(a, m) = 1$ , we have  $m \mid (i-j)$ , which contradicts the bounds on  $i$  and  $j$ .

**Theorem.** If  $\gcd(a, m) = 1$ , then there is an  $x$  in  $0 < x < m$  such that  $ax \equiv 1 \pmod{m}$ .

**Proof.** By the Lemma, the set

$$\{ai \pmod{m}; i = 1, \dots, m-1\}$$

is a permutation of  $\{1, \dots, m-1\}$ . Therefore 1 is in this set (the first one).

**Note:** The  $x$  in this Theorem is like " $a^{-1}$ "

Now we can say when we can divide in congruences:

**Theorem.** If  $m > 1$ ,  $a, b, c$  are integers, ( $c \neq 0$ ),  $\gcd(c, m) = 1$ , then  $ac \equiv bc \pmod{m}$  implies  $a \equiv b \pmod{m}$ .

**Proof.** By the previous Theorem, there is an  $x$  such that  $cx \equiv 1 \pmod{m}$ . Then  $ac \equiv bc$  implies  $acx \equiv bcx$  implies  $a1 \equiv b1$  implies  $a \equiv b \pmod{m}$ .

How to compute  $\text{gcd}(x, y)$ :

Euclidean Algorithm:

```
gcd(x,y)
int x, y;
return (y?gcd(y,x%y):abs(x));
```

(Non-recursive) Euclidean Algorithm:

```
gcd(x,y)
int x, y;
u = x; v = y;
while (v  $\neq$  0)
    t = u%v;
    u = v;
    v = t;
return (u);
```

**Theorem.** If  $a$  and  $b > 0$  are integers, then there exist integers  $x$  and  $y$  such that

$$xa + yb = \gcd(a, b).$$

Extended Euclidean Algorithm:

```
u1 = 1; u2 = 0; u3 = a;
v1 = 0; v2 = 1; v3 = b;
while (v3 ≠ 0)
    q = [u3/v3];
    t1 = u1 - q*v1;
    t2 = u2 - q*v2;
    t3 = u3 - q*v3;
    u1 = v1; u2 = v2; u3 = v3;
    v1 = t1; v2 = t2; v3 = t3;
```

At the end of the while loop we have  
 $a*u1 + b*u2 = u3 = \gcd(a, b)$ .

How to solve the congruence  $ax \equiv b \pmod{m}$ :

**Theorem.** Let  $m > 1$ ,  $a$  and  $b$  be integers. Let  $g = \gcd(a, m)$ . If  $g \nmid b$ , then  $ax \equiv b \pmod{m}$  has no solution. If  $g \mid b$ , then it has  $g$  solutions

$$x \equiv \frac{b}{g}x_0 + t\frac{m}{g} \pmod{m}, \quad t = 0, 1, \dots, g-1,$$

where  $x_0$  is any solution of  $\frac{a}{g}x_0 \equiv 1 \pmod{\frac{m}{g}}$ . That is,

$$x = \frac{b}{g}x_0 + t\frac{m}{g} \pmod{m}, \quad t = 0, 1, \dots,$$

are all integer solutions  $x$ .

**Examples.** (a) Solve  $7x \equiv 3 \pmod{12}$ .

$g = \gcd(7, 12) = 1$ ,  $g|b$  since  $1|3$ , so there is one solution.  $7 \cdot 7 \equiv 1 \pmod{12}$ , so  $x_0 = 7$  and the solution to  $7x \equiv 3 \pmod{12}$  is  $x = 3 \cdot 7 + t \cdot 12 = 21 + 12t \equiv 9 \pmod{12}$ .

(b) Solve  $657x \equiv 36 \pmod{963}$ .

$g = \gcd(657, 963) = 9$ . (See next slide.)  $g = 9|36 = b$ , so there are 9 solutions. To find them, we must solve

$$\frac{657}{9}x_0 \equiv 1 \pmod{\frac{963}{9}}.$$

That is,  $73x_0 \equiv 1 \pmod{107}$ . We find  $x_0 \equiv 22$ . (See next slide.) Then,

$$x_0 = \frac{36}{9} \cdot 22 + t \frac{963}{9} = 88 + 107t,$$

That is,  $x \equiv 88 \pmod{107}$ . The nine solutions of the original congruence are:

$$x \equiv 88, 88+107, 88+2 \cdot 107, \dots, 88+8 \cdot 107 \pmod{963}.$$