

**Math 104A, Number Theory, Fall 2002.**  
**Summary of Lecture 11.**

**Propositions 3.1.7 and 3.1.10.**(a). If  $a \equiv b \pmod{m}$  and  $d|m$  then  $a \equiv b \pmod{d}$ .

(b).  $ac = bc \pmod{m}$  implies that  $a = b \pmod{m/(m,c)}$ .

(c). If  $(m,n) = 1$  then  $a \equiv b \pmod{m}$  and  $a \equiv b \pmod{n}$  if and only if  $a \equiv b \pmod{mn}$ .

**Definition 3.2.1.** The number  $b$  is the **inverse of  $a$  modulo  $m$**  if  $ab \equiv 1 \pmod{m}$ . We say  $a$  is invertible modulo  $m$  if it has an inverse.

**Example.** The multiplication tables modulo 5 and 6 are given below. One can see which elements have inverses.

$$\left( \begin{array}{c|cccccc} \times & \mathbf{0} & \mathbf{1} & \mathbf{2} & \mathbf{3} & \mathbf{4} \\ \hline \mathbf{0} & 0 & 0 & 0 & 0 & 0 \\ \mathbf{1} & 0 & 1 & 2 & 3 & 4 \\ \mathbf{2} & 0 & 2 & 4 & 1 & 3 \\ \mathbf{3} & 0 & 3 & 1 & 4 & 2 \\ \mathbf{4} & 0 & 4 & 3 & 2 & 1 \end{array} \right) \qquad \left( \begin{array}{c|cccccc} \times & \mathbf{0} & \mathbf{1} & \mathbf{2} & \mathbf{3} & \mathbf{4} & \mathbf{5} \\ \hline \mathbf{0} & 0 & 0 & 0 & 0 & 0 & 0 \\ \mathbf{1} & 0 & 1 & 2 & 3 & 4 & 5 \\ \mathbf{2} & 0 & 2 & 4 & 0 & 2 & 4 \\ \mathbf{3} & 0 & 3 & 0 & 3 & 0 & 3 \\ \mathbf{4} & 0 & 4 & 2 & 0 & 4 & 2 \\ \mathbf{5} & 0 & 5 & 4 & 3 & 2 & 1 \end{array} \right)$$

**Proposition 3.2.3.** An integer  $a$  is invertible modulo  $m$  if and only if  $(a, m) = 1$ . If  $a$  has an inverse then it is unique modulo  $m$ .

*Proof.* There exists  $x$  such that  $ax \equiv 1 \pmod{m}$  if and only if there exists  $x$  such that  $m|ax - 1$  which holds if and only if there exists  $x$  and  $y$  with  $ax + my = 1$ . We already know this can be solved if and only if  $(a, m) = 1$ .

If  $ax_0 \equiv 1 \pmod{m}$  and  $ax \equiv 1 \pmod{m}$  then  $x_0 \equiv x_0(ax) \equiv (x_0a)x \equiv x \pmod{m}$ . Hence inverses modulo  $m$  are unique.

**Proposition 3.2.7.** The linear congruence  $ax \equiv b \pmod{m}$  has exactly  $d = (a, m)$  solutions if  $d|b$  and no solutions if  $d \nmid b$ .

If  $d|b$  and  $x_0$  is a solution then the  $d$  distinct solutions modulo  $m$  are  $x_0 + mk/d \pmod{m}$  for  $k = 0, 1, \dots, (a, m) - 1$ . ■

*Proof.* There exists  $x$  such that  $ax \equiv b \pmod{m}$  if and only if there exists  $x$  such that  $m|ax - b$  which holds if and only if there exists  $x$  and  $y$  with

$$ax + my = b.$$

We already know this can be solved if and only if  $d|b$ .

We easily check that if  $x_0$  is a solution to  $ax \equiv b \pmod{m}$  then so is  $x = x_0 + km/d$ . Indeed,

$$a \left( x_0 + \frac{km}{d} \right) = b + m \frac{ka}{d} \equiv b \pmod{m}.$$

(Another way to see this is that if  $(x_0, y_0)$  is a solution to  $ax + my = b$ , then so are  $(x_0 + mk/d, y_0 - ak/d)$  for  $k$  an integer, so  $x_0 + mk/d$  are solutions to  $ax \equiv b \pmod{m}$ .) These give distinct solutions for  $k = 0, 1, \dots, d - 1$ .

Finally we must see that these are the only solutions. If  $ax_0 \equiv b \pmod{m}$  and  $ax \equiv b \pmod{m}$ , then  $ax_0 \equiv ax \pmod{m}$  and so by Prop. 3.1.7,  $x \equiv x_0 \pmod{m/d}$ . Hence  $x = x_0 + km/d$  for some integer  $k$ .