

**Math 104A, Number Theory, Fall 2002.**  
**Summary of Lecture 12.**

**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.**

$$\begin{pmatrix} \times & \mathbf{0} & \mathbf{1} & \mathbf{2} & \mathbf{3} & \mathbf{4} \\ \mathbf{0} & 0 & 0 & 0 & 0 & 0 \\ \mathbf{1} & 0 & 1 & 2 & 3 & 4 \\ \mathbf{2} & 0 & 2 & 4 & 1 & 3 \\ \mathbf{3} & 0 & 3 & 1 & 4 & 2 \\ \mathbf{4} & 0 & 4 & 3 & 2 & 1 \end{pmatrix} \qquad \begin{pmatrix} \times & \mathbf{0} & \mathbf{1} & \mathbf{2} & \mathbf{3} & \mathbf{4} & \mathbf{5} \\ \mathbf{0} & 0 & 0 & 0 & 0 & 0 & 0 \\ \mathbf{1} & 0 & 1 & 2 & 3 & 4 & 5 \\ \mathbf{2} & 0 & 2 & 4 & 0 & 2 & 4 \\ \mathbf{3} & 0 & 3 & 0 & 3 & 0 & 3 \\ \mathbf{4} & 0 & 4 & 2 & 0 & 4 & 2 \\ \mathbf{5} & 0 & 5 & 4 & 3 & 2 & 1 \end{pmatrix}$$

**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  $m$ .

**Example.** Find the inverse of 15 modulo 8.

**Solution.** To solve

$$15x \equiv 1 \pmod{8},$$

since  $15 \equiv 7 \pmod{8}$ , this equation for  $x$  is equivalent to

$$7x \equiv 1 \pmod{8},$$

Now  $(7, 8) = 1$  so there is a unique solution. Using the Euclidean algorithm we have

$$8 = 7 + 1,$$

but then

$$1 = 8 - 7$$

and reducing modulo 8, we have

$$1 \equiv (-1) \cdot 7 \equiv 7 \cdot 7 \pmod{8}.$$

The inverse of 7 (and of 15) modulo 8 is 7.

**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  $x_0 + (m/d)k \pmod{m}$  for  $k = 0, 1, \dots, d-1$ . ■

The **Proof** of this is given in the notes for Lecture 11. We remark in addition that

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

if and only if

$$\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{m}{d}}.$$

For example, we can see what happens for  $m = 6$  in the table above. Let's look at the row with  $a = 2$ . We have  $(2, 6) = 2$ . The equation

$$2x \equiv b \pmod{6}$$

has solutions if  $b \equiv 0, 2, 4 \pmod{6}$  since these are the numbers divisible by 2. The number of solutions in each case is 2, for example

$$2x \equiv 4 \pmod{6}$$

has solutions  $x \equiv 2$  and  $x = 5$ . Notice that these differ by  $3 = 6/2$ . Furthermore, they are also solutions to the equation

$$x \equiv 2 \pmod{3}.$$

We did examples, including the last one of 3.2.8.