

**Lemma.** If  $b \equiv c \pmod{m}$  then  $(b, m) = (c, m)$ .

PROOF: If  $b \equiv c \pmod{m}$  then  $c = b + sm$  for some  $s$ . Now if  $d = (b, m)$  then  $d \mid b + sm$  so  $d \mid (b + sm, m)$ . Likewise if  $d' = (b + sm, m)$  then  $d' \mid (b + sm) - sm = b$  so  $d' \mid (b, m) = d$ . Thus  $d = d'$ .  $\square$

**Theorem.** A congruence  $ax \equiv b \pmod{m}$  has solutions if and only if  $(a, m) \mid b$ . In this case, it has exactly  $d$  incongruent solutions modulo  $m$ , where  $d = (a, m)$ .

PROOF: Let  $d = (a, m)$ . Write  $m = kd$  and  $a = \ell d$ . Then  $(k, \ell) = 1$  so for any integers  $x_1$  and  $x_2$ ,  $m = kd$  will divide  $a(x_1 - x_2) = \ell d(x_1 - x_2)$  if and only if  $k \mid x_1 - x_2$ , i.e.  $x_1 \equiv x_2 \pmod{k}$ . This shows that if  $x_1$  is a solution to  $ax \equiv b \pmod{m}$ , then this congruence has exactly  $d$  incongruent solutions, namely  $x_1, x_1 + k, x_1 + 2k, \dots, x_1 + (d - 1)k$ .

Now there are  $m$  different possible incongruent values for  $x$  and by the preceding paragraph a congruence  $ax \equiv b \pmod{m}$  has exactly  $d$  solutions whenever it has a solution at all. It follows that as  $x$  takes all possible values, there are  $m/d = k$  different incongruent values for  $ax$  that occur. I.e. there are  $k$  different incongruent values for  $b$  such that  $ax \equiv b \pmod{m}$  has a solution.

Now if there exists  $x$  with  $ax \equiv b \pmod{m}$  then by the lemma above,  $(ax, m) = (b, m)$ . But  $d \mid (ax, m)$ , so thus  $d \mid (b, m)$  and it follows that  $d \mid b$ , so that  $b = dy$  for some  $y$ . Now use the Division Algorithm to write  $y = kq + r$  with  $0 \leq r < k$ . Then  $b = dy = kqd + rd \equiv rd \pmod{m}$ . Thus if  $ax \equiv b \pmod{m}$  has a solution then  $b$  must be congruent modulo  $m$  to one of the  $k$  possible values  $0, d, 2d, \dots, (k - 1)d$ . But we saw above that there must be  $k$  different incongruent values  $b$  such that  $ax \equiv b \pmod{m}$  has a solution. Thus none of the congruence classes above represented by  $0, d, \dots, (k - 1)d$  can be omitted. Thus if  $b$  is any multiple of  $d$ , the congruence  $ax \equiv b \pmod{m}$  must in fact have a solution.  $\square$