Algorithm Design
M. T. Goodrich and R. Tamassia
John Wiley & Sons
Solution of Exercise R-10.8

Consider the numbers $1, 2, \cdots, p-1$. We claim that multiplication by x yields distinct values (mod p) for each of the numbers between 1 and $p-1$. Why? Well, suppose not. Then there are some i and j, $p > i > j$ such that $ai \equiv aj \bmod p$. (If $i < j$, then we can just switch the two, and continue with the proof.) From our discussion above, this means that $ai - aj = kp$, or $a(i-j) = kp$. Now, a and p are relatively prime. Thus, a must divide k. This means that $i - j$ is a multiple of p, a contradiction, since $i - j < p$, so this can't be true. Therefore, Corollary **??** is proved. Since the set $\{ix \bmod p, i = 0, 1, \cdots, p-1\}$ is the same as Z_p, for $x > 0$, there must be an i such that $ix \equiv 1 \bmod p$, which proves Theorem **??**.