Hence, $1 = 5 - 2 \cdot 2 = 5 - (7 - 5 \cdot 1) \cdot 2 = 5 \cdot 3 - 2 \cdot 7 = (12 - 7 \cdot 1) \cdot 3 - 2 \cdot 7 = 12 \cdot 3 - 5 \cdot 7$. Therefore, a particular solution to the linear diophantine equation is $x_0 = -20$ and $y_0 = 12$. Hence, all solutions of the linear congruences are given by $x \equiv -20 \equiv 4 \pmod{12}$. ◀

Later we will want to know which integers are their own inverses modulo $p$, where $p$ is prime. The following theorem tells us which integers have this property.

**Theorem 4.11.** Let $p$ be prime. The positive integer $a$ is its own inverse modulo $p$ if and only if $a \equiv 1 \pmod{p}$ or $a \equiv -1 \pmod{p}$.

*Proof.* If $a \equiv 1 \pmod{p}$ or $a \equiv -1 \pmod{p}$, then $a^2 \equiv 1 \pmod{p}$, so that $a$ is its own inverse modulo $p$.

Conversely, if $a$ is its own inverse modulo $p$, then $a^2 = a \cdot a \equiv 1 \pmod{p}$. Hence, $p \mid (a^2 - 1)$. Since $a^2 - 1 = (a-1)(a+1)$, either $p \mid (a-1)$ or $p \mid (a+1)$. Therefore, either $a \equiv 1 \pmod{p}$ or $a \equiv -1 \pmod{p}$. ■

## 4.2 Exercises

1. Find all solutions of each of the following linear congruences.

   a) $2x \equiv 5 \pmod{7}$
   b) $3x \equiv 6 \pmod{9}$
   c) $19x \equiv 30 \pmod{40}$
   d) $9x \equiv 5 \pmod{25}$
   e) $103x \equiv 444 \pmod{999}$
   f) $980x \equiv 1500 \pmod{1600}$

2. Find all solutions of each of the following linear congruences.

   a) $3x \equiv 2 \pmod{7}$
   b) $6x \equiv 3 \pmod{9}$
   c) $17x \equiv 14 \pmod{21}$
   d) $15x \equiv 9 \pmod{25}$
   e) $128x \equiv 833 \pmod{1001}$
   f) $987x \equiv 610 \pmod{1597}$

3. Find all solutions to the congruence $6{,}789{,}783x \equiv 2{,}474{,}010 \pmod{28{,}927{,}591}$.

4. Suppose that $p$ is prime and that $a$ and $b$ are positive integers with $(p, a) = 1$. The following method can be used to solve the linear congruence $ax \equiv b \pmod{p}$.

   a) Show that if the integer $x$ is a solution of $ax \equiv b \pmod{p}$, then $x$ is also a solution of the linear congruence

   $$a_1 x \equiv -b[m/a] \pmod{p},$$

   where $a_1$ is the least positive residue of $p$ modulo $a$. Note that this congruence is of the same type as the original congruence, with a positive integer smaller than $a$ as the coefficient of $x$.

   b) When the procedure of part (a) is iterated, one obtains a sequence of linear congruences with coefficients of $x$ equal to $a_0 = a > a_1 > a_2 > \cdots$. Show that there is a positive integer $n$ with $a_n = 1$, so that at the $n$th stage, one obtains a linear congruence $x \equiv B \pmod{p}$.

   c) Use the method described in part (b) to solve the linear congruence $6x \equiv 7 \pmod{23}$.

5. An astronomer knows that a satellite orbits the Earth in a period that is an exact multiple of 1 hour that is less than 1 day. If the astronomer notes that the satellite completes 11 orbits in an interval that starts when a 24-hour clock reads 0 hours and ends when the clock reads 17 hours, how long is the orbital period of the satellite?

6. For which integers $c$, $0 \leq c < 30$, does the congruence $12x \equiv c \pmod{30}$ have solutions? When there are solutions, how many incongruent solutions are there?

7. For which integers $c$, $0 \leq c < 1001$, does the congruence $154x \equiv c \pmod{1001}$ have solutions? When there are solutions, how many incongruent solutions are there?

8. Find an inverse modulo 13 of each of the following integers.

a) 2 c) 5
b) 3 d) 11

9. Find an inverse modulo 17 of each of the following integers.

a) 4 c) 7
b) 5 d) 16

10. a) Determine which integers $a$, where $1 \leq a \leq 14$, have an inverse modulo 14.
b) Find the inverse of each of the integers from part (a) that have an inverse modulo 14.

11. a) Determine which integers $a$, where $1 \leq a \leq 30$, have an inverse modulo 30.
b) Find the inverse of each of the integers from part (a) that have an inverse modulo 30.

12. Show that if $\bar{a}$ is an inverse of $a$ modulo $m$ and $\bar{b}$ is an inverse of $b$ modulo $m$, then $\bar{a}\,\bar{b}$ is an inverse of $ab$ modulo $m$.

13. Show that the linear congruence in two variables $ax + by \equiv c \pmod{m}$, where $a$, $b$, $c$, and $m$ are integers, $m > 0$, with $d = (a, b, m)$, has exactly $dm$ incongruent solutions if $d \mid c$, and no solutions otherwise.

14. Find all solutions of each of the following linear congruences in two variables.

a) $2x + 3y \equiv 1 \pmod{7}$ c) $6x + 3y \equiv 0 \pmod{9}$
b) $2x + 4y \equiv 6 \pmod{8}$ d) $10x + 5y \equiv 9 \pmod{15}$

15. Let $p$ be an odd prime and $k$ a positive integer. Show that the congruence $x^2 \equiv 1 \pmod{p^k}$ has exactly two incongruent solutions, namely $x \equiv \pm 1 \pmod{p^k}$.

16. Show that the congruence $x^2 \equiv 1 \pmod{2^k}$ has exactly four incongruent solutions, namely $x \equiv \pm 1$ or $\pm(1 + 2^{k-1}) \pmod{2^k}$, when $k > 2$. Show that when $k = 1$ there is one solution and that when $k = 2$ there are two incongruent solutions.

17. Show that if $a$ and $m$ are relatively prime positive integers such that $a < m$, then an inverse of $a$ modulo $m$ can be found using $O(\log^3 m)$ bit operations.

18. Show that if $p$ is an odd prime and $a$ is a positive integer not divisible by $p$, then the congruence $x^2 \equiv a \pmod{p}$ has either no solution or exactly two incongruent solutions.