

2. Under the hypotheses, we have $c = as$ and $d = bt$ for some s and t . Multiplying we obtain $cd = ab(st)$, which means that $ab \mid cd$, as desired.
4. A zero appears at the end of a number for every factor of 10 ($= 2 \cdot 5$) the number has. Now $100!$ certainly has more factors of 2 than it has factors of 5, so the number of factors of 10 it has is the same as the number of factors of 5. Each of the twenty numbers 5, 10, 15, ..., 100 contributes a factor of 5 to $100!$, and in addition the four numbers 25, 50, 75, and 100 contribute one more factor of 5. Therefore there are 24 factors of 5 in $100!$, so $100!$ ends in exactly 24 zeros.
6. Among the infinite set of correct answers are 4, 16, -8 , 1204, and -7016360 .
8. By Exercise 33, we know that the product of the greatest common divisor and the least common multiple of two numbers is the product of the two numbers. Therefore the answer is $(2^7 \cdot 3^8 \cdot 5^2 \cdot 7^{11}) / (2^3 \cdot 3^4 \cdot 5) = 2^4 \cdot 3^4 \cdot 5 \cdot 7^{11}$.
10. From $a \equiv b \pmod{m}$ we know that $b = a + sm$ for some integer s . Now if d is a common divisor of a and m , then it divides the right-hand side of this equation, so it also divides b . We can rewrite the equation as $a = b - sm$, and then by similar reasoning, we see that every common divisor of b and m is also a divisor of a . This shows that the set of common divisors of a and m is equal to the set of common divisors of b and m , so certainly $\gcd(a, m) = \gcd(b, m)$.

SECTION 2.5 Applications of Number Theory

2. a) In order to find the coefficients s and t such that $9s + 11t = \gcd(9, 11)$, we carry out the steps of the Euclidean algorithm.

$$\begin{aligned} 11 &= 9 + 2 \\ 9 &= 4 \cdot 2 + 1 \end{aligned}$$

Then we work up from the bottom, expressing the greatest common divisor (which we have just seen to be 1) in terms of the numbers involved in the algorithm, namely 11, 9, and 2. In particular, the last equation tells us that $1 = 9 - 4 \cdot 2$, so that we have expressed the gcd as a linear combination of 9 and 2. But now the first equation tells us that $2 = 11 - 9$; we plug this into our previous equation and obtain

$$1 = 9 - 4 \cdot (11 - 9) = 5 \cdot 9 - 4 \cdot 11.$$

Thus we have expressed 1 as a linear combination (with integer coefficients) of 9 and 11, namely $\gcd(9, 11) = 5 \cdot 9 - 4 \cdot 11$.

b) Again, we carry out the Euclidean algorithm. Since $44 = 33 + 11$, and $11 \mid 33$, we know that $\gcd(33, 44) = 11$. From the equation shown here, we can immediately write $11 = (-1) \cdot 33 + 44$.

c) The calculation of the greatest common divisor takes several steps:

$$\begin{aligned} 78 &= 2 \cdot 35 + 8 \\ 35 &= 4 \cdot 8 + 3 \\ 8 &= 2 \cdot 3 + 2 \\ 3 &= 2 + 1 \end{aligned}$$

Then we need to work our way back up, successively plugging in for the remainders determined in this calculation:

$$\begin{aligned} 1 &= 3 - 2 \\ &= 3 - (8 - 2 \cdot 3) = 3 \cdot 3 - 8 \\ &= 3 \cdot (35 - 4 \cdot 8) - 8 = 3 \cdot 35 - 13 \cdot 8 \\ &= 3 \cdot 35 - 13 \cdot (78 - 2 \cdot 35) = 29 \cdot 35 - 13 \cdot 78 \end{aligned}$$

d) Here are the two calculations—down to the gcd using the Euclidean algorithm, and then back up by substitution until we have expressed the gcd as the desired linear combination of the original numbers.

$$\begin{aligned}
 55 &= 2 \cdot 21 + 13 \\
 21 &= 13 + 8 \\
 13 &= 8 + 5 \\
 8 &= 5 + 3 \\
 5 &= 3 + 2 \\
 3 &= 2 + 1
 \end{aligned}$$

Thus the greatest common divisor is 1.

$$\begin{aligned}
 1 &= 3 - 2 \\
 &= 3 - (5 - 3) = 2 \cdot 3 - 5 \\
 &= 2 \cdot (8 - 5) - 5 = 2 \cdot 8 - 3 \cdot 5 \\
 &= 2 \cdot 8 - 3 \cdot (13 - 8) = 5 \cdot 8 - 3 \cdot 13 \\
 &= 5 \cdot (21 - 13) - 3 \cdot 13 = 5 \cdot 21 - 8 \cdot 13 \\
 &= 5 \cdot 21 - 8 \cdot (55 - 2 \cdot 21) = 21 \cdot 21 - 8 \cdot 55
 \end{aligned}$$

e) We compute the greatest common divisor in one step: $203 = 2 \cdot 101 + 1$. Therefore we have $1 = (-2) \cdot 101 + 203$.

f) We compute the greatest common divisor using the Euclidean algorithm:

$$\begin{aligned}
 323 &= 2 \cdot 124 + 75 \\
 124 &= 75 + 49 \\
 75 &= 49 + 26 \\
 49 &= 26 + 23 \\
 26 &= 23 + 3 \\
 23 &= 7 \cdot 3 + 2 \\
 3 &= 2 + 1
 \end{aligned}$$

Thus the greatest common divisor is 1.

$$\begin{aligned}
 1 &= 3 - 2 \\
 &= 3 - (23 - 7 \cdot 3) = 8 \cdot 3 - 23 \\
 &= 8 \cdot (26 - 23) - 23 = 8 \cdot 26 - 9 \cdot 23 \\
 &= 8 \cdot 26 - 9 \cdot (49 - 26) = 17 \cdot 26 - 9 \cdot 49 \\
 &= 17 \cdot (75 - 49) - 9 \cdot 49 = 17 \cdot 75 - 26 \cdot 49 \\
 &= 17 \cdot 75 - 26 \cdot (124 - 75) = 43 \cdot 75 - 26 \cdot 124 \\
 &= 43 \cdot (323 - 2 \cdot 124) - 26 \cdot 124 = 43 \cdot 323 - 112 \cdot 124
 \end{aligned}$$

g) Here are the two calculations—down to the gcd using the Euclidean algorithm, and then back up by

substitution until we have expressed the gcd as the desired linear combination of the original numbers.

$$\begin{aligned}
 2339 &= 2002 + 337 \\
 2002 &= 5 \cdot 337 + 317 \\
 337 &= 317 + 20 \\
 317 &= 15 \cdot 20 + 17 \\
 20 &= 17 + 3 \\
 17 &= 5 \cdot 3 + 2 \\
 3 &= 2 + 1
 \end{aligned}$$

Thus the greatest common divisor is 1.

$$\begin{aligned}
 1 &= 3 - 2 \\
 &= 3 - (17 - 5 \cdot 3) = 6 \cdot 3 - 17 \\
 &= 6 \cdot (20 - 17) - 17 = 6 \cdot 20 - 7 \cdot 17 \\
 &= 6 \cdot 20 - 7 \cdot (317 - 15 \cdot 20) = 111 \cdot 20 - 7 \cdot 317 \\
 &= 111 \cdot (337 - 317) - 7 \cdot 317 = 111 \cdot 337 - 118 \cdot 317 \\
 &= 111 \cdot 337 - 118 \cdot (2002 - 5 \cdot 337) = 701 \cdot 337 - 118 \cdot 2002 \\
 &= 701 \cdot (2339 - 2002) - 118 \cdot 2002 = 701 \cdot 2339 - 819 \cdot 2002
 \end{aligned}$$

h) The procedure is the same:

$$\begin{aligned}
 4669 &= 3457 + 1212 \\
 3457 &= 2 \cdot 1212 + 1033 \\
 1212 &= 1033 + 179 \\
 1033 &= 5 \cdot 179 + 138 \\
 179 &= 138 + 41 \\
 138 &= 3 \cdot 41 + 15 \\
 41 &= 2 \cdot 15 + 11 \\
 15 &= 11 + 4 \\
 11 &= 2 \cdot 4 + 3 \\
 4 &= 3 + 1
 \end{aligned}$$

Thus the greatest common divisor is 1.

$$\begin{aligned}
 1 &= 4 - 3 \\
 &= 4 - (11 - 2 \cdot 4) = 3 \cdot 4 - 11 \\
 &= 3 \cdot (15 - 11) - 11 = 3 \cdot 15 - 4 \cdot 11 \\
 &= 3 \cdot 15 - 4 \cdot (41 - 2 \cdot 15) = 11 \cdot 15 - 4 \cdot 41 \\
 &= 11 \cdot (138 - 3 \cdot 41) - 4 \cdot 41 = 11 \cdot 138 - 37 \cdot 41 \\
 &= 11 \cdot 138 - 37 \cdot (179 - 138) = 48 \cdot 138 - 37 \cdot 179 \\
 &= 48 \cdot (1033 - 5 \cdot 179) - 37 \cdot 179 = 48 \cdot 1033 - 277 \cdot 179 \\
 &= 48 \cdot 1033 - 277 \cdot (1212 - 1033) = 325 \cdot 1033 - 277 \cdot 1212 \\
 &= 325 \cdot (3457 - 2 \cdot 1212) - 277 \cdot 1212 = 325 \cdot 3457 - 927 \cdot 1212 \\
 &= 325 \cdot 3457 - 927 \cdot (4669 - 3457) = 1252 \cdot 3457 - 927 \cdot 4669
 \end{aligned}$$

i) The procedure is the same:

$$\begin{aligned}
 13422 &= 10001 + 3421 \\
 10001 &= 2 \cdot 3421 + 3159 \\
 3421 &= 3159 + 262 \\
 3159 &= 12 \cdot 262 + 15 \\
 262 &= 17 \cdot 15 + 7 \\
 15 &= 2 \cdot 7 + 1
 \end{aligned}$$

Thus the greatest common divisor is 1.

$$\begin{aligned}
 1 &= 15 - 2 \cdot 7 \\
 &= 15 - 2 \cdot (262 - 17 \cdot 15) = 35 \cdot 15 - 2 \cdot 262 \\
 &= 35 \cdot (3159 - 12 \cdot 262) - 2 \cdot 262 = 35 \cdot 3159 - 422 \cdot 262 \\
 &= 35 \cdot 3159 - 422 \cdot (3421 - 3159) = 457 \cdot 3159 - 422 \cdot 3421 \\
 &= 457 \cdot (10001 - 2 \cdot 3421) - 422 \cdot 3421 = 457 \cdot 10001 - 1336 \cdot 3421 \\
 &= 457 \cdot 10001 - 1336 \cdot (13422 - 10001) = 1793 \cdot 10001 - 1336 \cdot 13422
 \end{aligned}$$

4. If x is an inverse of a modulo m , then by definition $ax - 1 = tm$ for some integer t . If a and m in this equation both have a common divisor greater than 1, then 1 must also have this same common divisor, since $1 = ax - tm$. This is absurd, since the only positive divisor of 1 is 1. Therefore no such x exists.
6. We are asked to solve $x \equiv 0 \pmod{5}$ and $x \equiv 1 \pmod{3}$. We know from the Chinese Remainder Theorem that there is a unique answer modulo 15. It is probably quickest just to look for it by dividing each multiple of 5 by 3, and we see immediately that $x = 10$ satisfies the condition. Thus the solutions are all integers congruent to 10 modulo 15. If the numbers involved were larger, then we could use the technique implicit in the proof of Theorem 4 (see Exercise 29).