SECTION 3.7 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.

$$11 = 9 + 2$$
$$9 = 4 \cdot 2 + 1$$

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:

$$78 = 2 \cdot 35 + 8$$
$$35 = 4 \cdot 8 + 3$$
$$8 = 2 \cdot 3 + 2$$
$$3 = 2 + 1$$

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.

$$55 = 2 \cdot 21 + 13$$
$$21 = 13 + 8$$
$$13 = 8 + 5$$
$$8 = 5 + 3$$
$$5 = 3 + 2$$
$$3 = 2 + 1$$

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. We need to show that $13\cdot 937 \equiv 1 \pmod{2436}$, or in other words, that $13\cdot 937 - 1 = 12180$ is divisible by 2436. A calculator shows that it is, since $12180 = 2436\cdot 5$.

6. We need to find a number x such that $2x \bmod 17 = 1$. This can be done by inspection, since we immediately notice that $2 \cdot 9 = 18$, and $18 \bmod 17 = 1$. If we did not notice this so quickly, then we could have used the technique shown below for Exercise 8.

8. We need to find s and t such that $144s + 233t = 1$. Then clearly s will be the desired inverse, since $144s \equiv 1 \pmod{233}$ (i.e., $144s - 1 = -233t$ is divisible by 233). To do so, we proceed as in Exercise 2. First we go through the Euclidean algorithm computation that $\gcd(144, 233) = 1$:

$$\begin{aligned}
233 &= 144 + 89 \\
144 &= 89 + 55 \\
89 &= 55 + 34 \\
55 &= 34 + 21 \\
34 &= 21 + 13 \\
21 &= 13 + 8 \\
13 &= 8 + 5 \\
8 &= 5 + 3 \\
5 &= 3 + 2 \\
3 &= 2 + 1
\end{aligned}$$

Then we reverse our steps and write 1 as the desired linear combination:

$$\begin{aligned}
1 &= 3 - 2 \\
&= 3 - (5 - 3) = 2 \cdot 3 - 5 \\
&= 2 \cdot (8 - 5) - 5 = 2 \cdot 8 - 3 \cdot 5 \\
&= 2 \cdot 8 - 3 \cdot (13 - 8) = 5 \cdot 8 - 3 \cdot 13 \\
&= 5 \cdot (21 - 13) - 3 \cdot 13 = 5 \cdot 21 - 8 \cdot 13 \\
&= 5 \cdot 21 - 8 \cdot (34 - 21) = 13 \cdot 21 - 8 \cdot 34 \\
&= 13 \cdot (55 - 34) - 8 \cdot 34 = 13 \cdot 55 - 21 \cdot 34 \\
&= 13 \cdot 55 - 21 \cdot (89 - 55) = 34 \cdot 55 - 21 \cdot 89 \\
&= 34 \cdot (144 - 89) - 21 \cdot 89 = 34 \cdot 144 - 55 \cdot 89 \\
&= 34 \cdot 144 - 55 \cdot (233 - 144) = 89 \cdot 144 - 55 \cdot 233
\end{aligned}$$

Thus $s = 89$, so an inverse of 144 modulo 233 is 89, since $144 \cdot 89 = 12816 \equiv 1 \pmod{233}$.

10. 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.

12. We know from Exercise 6 that 9 is an inverse of 2 modulo 17. Therefore if we multiply both sides of this equation by 9 we will get $x \equiv 9 \cdot 7 \pmod{17}$. Since $63 \bmod 17 = 12$, the solutions are all integers congruent to 12 modulo 17, such as 12, 29, and -5. We can check, for example, that $2 \cdot 12 = 24 \equiv 7 \pmod{17}$.

14. **a)** We can search for inverses using the technique shown in Exercise 8. With a little work (or trial and error, which is actually faster in this case), we find that $2 \cdot 6 \equiv 1 \pmod{11}$, $3 \cdot 4 \equiv 1 \pmod{11}$, $5 \cdot 9 \equiv 1 \pmod{11}$, and $7 \cdot 8 \equiv 1 \pmod{11}$. Actually, the problem does not ask us to show these pairs explicitly, only to show that they exist. The general argument given in Exercise 16 shows this.

b) In this specific case we can compute $10! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10 = 1 \cdot (2 \cdot 6) \cdot (3 \cdot 4) \cdot (5 \cdot 9) \cdot (7 \cdot 8) \cdot 10 \equiv 1 \cdot 1 \cdot 1 \cdot 1 \cdot 10 = 10 \equiv -1 \pmod{11}$. Alternatively, we can use the proof in Exercise 16.

16. a) Every positive integer less than p has an inverse modulo p, and by Exercise 9 this inverse is unique among positive integers less than p. This follows from Theorem 3, since every number less than p must be relatively prime to p (because p is prime it has no smaller divisors). We can group each positive integer less than p with its inverse. The only issue is whether some numbers are their own inverses, in which case this grouping does not produce pairs. By Exercise 15 only 1 and -1 (which is the same as $p-1$ modulo p) are their own inverses. Therefore all the other positive integers less than p can be grouped into pairs consisting of inverses of each other, and there are clearly $(p-1-2)/2 = (p-3)/2$ such pairs.

b) When we compute $(p-1)!$, we can write the product by grouping the pairs of inverses modulo p. Each such pair produces the product 1 modulo p, so modulo p the entire product is the same as the product of the only unpaired elements, namely $1 \cdot (p-1) = p-1$. Since this equals -1 modulo p, our proof is complete.

c) By the contrapositive of what we have just proved, we can conclude that if $(n-1)! \not\equiv -1 \pmod{n}$ then n is not prime.

18. Since 3, 4, and 5 are pairwise relatively prime, we can use the Chinese Remainder Theorem. The answer will be unique modulo $3 \cdot 4 \cdot 5 = 60$. Using the notation in the text, we have $a_1 = 2$, $m_1 = 3$, $a_2 = 1$, $m_2 = 4$, $a_3 = 3$, $m_3 = 5$, $m = 60$, $M_1 = 60/3 = 20$, $M_2 = 60/4 = 15$, $M_3 = 60/5 = 12$. Then we need to find inverses y_i of M_i modulo m_i for $i = 1, 2, 3$. This can be done by inspection (trial and error), since the moduli here are so small, or systematically using the Euclidean algorithm (as in Example 3); we find that $y_1 = 2$, $y_2 = 3$, and $y_3 = 3$. Thus our solution is $x = 2 \cdot 20 \cdot 2 + 1 \cdot 15 \cdot 3 + 3 \cdot 12 \cdot 3 = 233 \equiv 53 \pmod{60}$. So the solutions are all integers of the form $53 + 60k$, where k is an integer.

20. We cannot apply the Chinese Remainder Theorem directly, since the moduli are not pairwise relatively prime. However, we can, using the Chinese Remainder Theorem, translate these congruences into a set of congruences that together are equivalent to the given congruence. Since we want $x \equiv 5 \pmod{6}$, we must have $x \equiv 5 \equiv 1 \pmod{2}$ and $x \equiv 5 \equiv 2 \pmod{3}$. Similarly, from the second congruence we must have $x \equiv 1 \pmod{2}$ and $x \equiv 3 \pmod{5}$; and from the third congruence we must have $x \equiv 2 \pmod{3}$ and $x \equiv 3 \pmod{5}$. Since these six statements are consistent, we see that our system is equivalent to the system $x \equiv 1 \pmod{2}$, $x \equiv 2 \pmod{3}$, $x \equiv 3 \pmod{5}$. These can be solved using the Chinese Remainder Theorem (see Exercise 19 or Example 6) to yield $x \equiv 23 \pmod{30}$. Therefore the solutions are all integers of the form $23 + 30k$, where k is an integer.

22. This is just a restatement of the Chinese Remainder Theorem. Given any such a we can certainly compute $a \bmod m_1$, $a \bmod m_2$, ..., $a \bmod m_n$ to represent it. The Chinese Remainder Theorem says that there is only one nonnegative integer less than m yielding each n-tuple, so the representation is unique.

24. We follow the hint and suppose that there are two solutions to the set of congruences. Thus suppose that $x \equiv a_i \pmod{m_i}$ and $y \equiv a_i \pmod{m_i}$ for each i. We want to show that these solutions are the same modulo m; this will guarantee that there is only one nonnegative solution less than m. The assumption certainly implies that $x \equiv y \pmod{m_i}$ for each i. But then Exercise 23 tells us that $x \equiv y \pmod{m}$, as desired.

26. 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 39).

28. a) By Fermat's Little Theorem we know that $3^4 \equiv 1 \pmod{5}$; therefore $3^{300} = (3^4)^{75} \equiv 1^{75} \equiv 1 \pmod{5}$, and so $3^{302} = 3^2 \cdot 3^{300} \equiv 9 \cdot 1 = 9 \pmod{5}$, so $3^{302} \bmod 5 = 4$. Similarly, $3^6 \equiv 1 \pmod{7}$; therefore

$3^{300} = (3^6)^{50} \equiv 1 \pmod 5$, and so $3^{302} = 3^2 \cdot 3^{300} \equiv 9 \pmod 7$, so $3^{302} \bmod 7 = 2$. Finally, $3^{10} \equiv 1 \pmod{11}$; therefore $3^{300} = (3^{10})^{30} \equiv 1 \pmod{11}$, and so $3^{302} = 3^2 \cdot 3^{300} \equiv 9 \pmod{11}$, so $3^{302} \bmod 11 = 9$.

b) Since 3^{302} is congruent to 9 modulo 5, 7, and 11, it is also congruent to 9 modulo 385. (This was a particularly trivial application of the Chinese Remainder Theorem.)

30. Let $x_k = b^{(n-1)/2^k} = b^{2^{s-k}t}$, for $k = 0, 1, 2, \ldots, s$. Because n is prime and $n \not| b$, Fermat's Little Theorem tells us that $x_0 = b^{n-1} \equiv 1 \pmod n$. By Exercise 15, because $x_1^2 = (b^{(n-1)/2})^2 = x_0 \equiv 1 \pmod n$, either $x_1 \equiv -1 \pmod n$ or $x_1 \equiv 1 \pmod n$. If $x_1 \equiv 1 \pmod n$, because $x_2^2 = x_1 \equiv 1 \pmod n$, either $x_2 \equiv -1 \pmod n$ or $x_2 \equiv 1 \pmod n$. In general, if we have found that $x_0 \equiv x_1 \equiv x_2 \equiv \cdots \equiv x_k \equiv 1 \pmod n$, with $k < s$, then, because $x_{k+1}^2 = x_k \equiv 1 \pmod n$, we know that either $x_{k+1} \equiv -1 \pmod n$ or $x_{k+1} \equiv 1 \pmod n$. Continuing this procedure for $k = 1, 2, \ldots, s$, we find that either $x_s = b^t \equiv 1 \pmod n$, or $x_k \equiv -1 \pmod n$ for some integer k with $0 \leq k \leq s$. Hence, n passes Miller's test for the base b.

32. This follows from Exercise 35, taking $m = 1$. Alternatively, we can argue directly as follows. Factor $1729 = 7 \cdot 13 \cdot 19$. We must show that this number meets the definition of Carmichael number, namely that $b^{1728} \equiv 1 \pmod{1729}$ for all b relatively prime to 1729. Note that if $\gcd(b, 1729) = 1$, then $\gcd(b, 7) = \gcd(b, 13) = \gcd(b, 19) = 1$. Using Fermat's Little Theorem we find that $b^6 \equiv 1 \pmod 7$, $b^{12} \equiv 1 \pmod{13}$, and $b^{18} \equiv 1 \pmod{19}$. It follows that $b^{1728} = (b^6)^{288} \equiv 1 \pmod 7$, $b^{1728} = (b^{12})^{144} \equiv 1 \pmod{13}$, and $b^{1728} = (b^{18})^{96} \equiv 1 \pmod{19}$. By Exercise 23 (or the Chinese Remainder Theorem) it follows that $b^{1728} \equiv 1 \pmod{1729}$, as desired.

34. Let b be a positive integer with $\gcd(b, n) = 1$. The $\gcd(b, p_j) = 1$ for $j = 1, 2, \ldots, k$, and hence, by Fermat's Little Theorem, $b^{p_j - 1} \equiv 1 \pmod{p_j}$ for $j = 1, 2, \ldots, k$. Because $p_j - 1 \,|\, n - 1$, there are integers t_j with $t_j(p_j - 1) = n - 1$. Hence for each j we know that $b^{n-1} = b^{(p_j-1)t_j} = (b^{(p_j-1)})^{t_j} \equiv 1 \pmod{p_j}$. Therefore $b^{n-1} \equiv 1 \pmod n$, as desired.

36. We could use the technique shown in the proof of Theorem 4 to solve each part, or use the approach in our solution to Exercise 26, but since there are so many to do here, it is simpler just to write out all the representations of 0 through 27 and find those given in each part. This task is easily done, since the pattern is clear:

$0 = (0,0)$	$7 = (3,0)$	$14 = (2,0)$	$21 = (1,0)$
$1 = (1,1)$	$8 = (0,1)$	$15 = (3,1)$	$22 = (2,1)$
$2 = (2,2)$	$9 = (1,2)$	$16 = (0,2)$	$23 = (3,2)$
$3 = (3,3)$	$10 = (2,3)$	$17 = (1,3)$	$24 = (0,3)$
$4 = (0,4)$	$11 = (3,4)$	$18 = (2,4)$	$25 = (1,4)$
$5 = (1,5)$	$12 = (0,5)$	$19 = (3,5)$	$26 = (2,5)$
$6 = (2,6)$	$13 = (1,6)$	$20 = (0,6)$	$27 = (3,6)$

Now we can read off the answers.

a) 0 **b)** 21 **c)** 1 **d)** 22 **e)** 2 **f)** 24 **g)** 14 **h)** 19 **i)** 27

38. To add 4 and 7 we first find that 4 is represented by $(1, 4)$ and that 7 is represented by $(1, 2)$. Adding coordinate-wise, we see that the sum is represented by $(1+1, 4+2) = (2, 6) = (2, 1)$; we are working modulo 5 in the second coordinate. Then we find $(2, 1)$ in the table and see that it represents 11. Therefore we conclude that $4 + 7 = 11$. Note that we can only compute answers less than $3 \cdot 5 = 15$ using this method.

40. The statement we are asked to prove involves the result of dividing $2^a - 1$ by $2^b - 1$. Let us actually carry out that division algebraically—long division of these expressions. The leading term in the quotient is 2^{a-b} (as long as $a \geq b$), with a remainder at that point of $2^{a-b} - 1$. If now $a - b \geq b$ then the next step

in the long division produces the next summand in the quotient, 2^{a-2b}, with a remainder at this stage of $2^{a-2b}-1$. This process of long division continues until the remainder at some stage is less than the divisor, i.e., $2^{a-kb}-1<2^a-1$. But then the remainder is $2^{a-kb}-1$, and clearly $a-kb$ is exactly $a \bmod b$. This completes the proof.

42. By Exercise 41, 2^a-1 and 2^b-1 are relatively prime precisely when $2^{\gcd(a,b)}-1=1$, which happens if and only if $\gcd(a,b)=1$. Thus it is enough to check here that 35, 34, 33, 31, 29, and 23 are relatively prime. This is clear, since the prime factorizations are, respectively, 35, $2\cdot 17$, $3\cdot 11$, 31, 29, and 23.

44. To decide whether $2^{13}-1=8191$ is prime, we need only look for a prime factor not exceeding $\sqrt{8191}\approx 90.5$. By Exercise 43 every such prime divisor must be of the form $26k+1$. The only candidates are therefore 53 and 79. We easily check that neither is a divisor, and so we conclude that 8191 is prime.

We can take the same approach for $2^{23}-1=8{,}388{,}607$, but we might worry that there will be far too many potential divisors to test, since we must go as far as 2896. By Exercise 43 every prime divisor of $2^{23}-1$ must be of the form $46k+1$. The first candidate divisor is therefore 47. Luckily $47\,|\,8{,}388{,}607$, so we conclude that it is not prime.

46. Translating the letters into numbers we have 0019 1900 0210. Thus we need to compute $C=P^{13} \bmod 2537$ for $P=19$, $P=1900$, and $P=210$. The results of these calculations, done by fast modular multiplication or a computer algebra system are 2299, 1317, and 2117, respectively. Thus the encrypted message is 2299 1317 2117.

48. We take $a=356$ and $b=252$ to avoid a needless first step. When we apply the Euclidean algorithm we obtain the following quotients and remainders: $q_1=1$, $r_2=104$, $q_2=2$, $r_3=44$, $q_3=2$, $r_4=16$, $q_4=2$, $r_5=12$, $q_5=1$, $r_6=4$, $q_6=3$. Note that $n=6$. Thus we compute the successive s's and t's as follows, using the given recurrences:

$s_2=s_0-q_1s_1=1-1\cdot 0=1,$ $\qquad t_2=t_0-q_1t_1=0-1\cdot 1=-1$

$s_3=s_1-q_2s_2=0-2\cdot 1=-2,$ $\qquad t_3=t_1-q_2t_2=1-2\cdot(-1)=3$

$s_4=s_2-q_3s_3=1-2\cdot(-2)=5,$ $\qquad t_4=t_2-q_3t_3=-1-2\cdot 3=-7$

$s_5=s_3-q_4s_4=-2-2\cdot 5=-12,$ $\qquad t_5=t_3-q_4t_4=3-2\cdot(-7)=17$

$s_6=s_4-q_5s_5=5-1\cdot(-12)=17,$ $\qquad t_6=t_4-q_5t_5=-7-1\cdot 17=-24$

Thus we have $s_6a+t_6b=17\cdot 356+(-24)\cdot 252=4$, which is $\gcd(356,252)$.

50. We take $a=100001$ and $b=1001$ to avoid a needless first step. When we apply the Euclidean algorithm we obtain the following quotients and remainders: $q_1=99$, $r_2=902$, $q_2=1$, $r_3=99$, $q_3=9$, $r_4=11$, $q_4=9$. Note that $n=4$. Thus we compute the successive s's and t's as follows, using the given recurrences:

$s_2=s_0-q_1s_1=1-99\cdot 0=1,$ $\qquad t_2=t_0-q_1t_1=0-99\cdot 1=-99$

$s_3=s_1-q_2s_2=0-1\cdot 1=-1,$ $\qquad t_3=t_1-q_2t_2=1-1\cdot(-99)=100$

$s_4=s_2-q_3s_3=1-9\cdot(-1)=10,$ $\qquad t_4=t_2-q_3t_3=-99-9\cdot 100=-999$

Thus we have $s_4a+t_4b=10\cdot 100001+(-999)\cdot 1001=11$, which is $\gcd(100001,1001)$.

52. We square the first five positive integers and reduce modulo 11, obtaining 1, 4, 9, 5, 3. The squares of the next five are necessarily the same set of numbers modulo 11, since $(-x)^2=x^2$, so we are done. Therefore the quadratic residues modulo 11 are all integers congruent to 1, 3, 4, 5, or 9 modulo 11.

54. Consider the list $x^2 \bmod p$ as x runs from 1 to $p-1$ inclusive. This gives us $p-1$ numbers between 1 and $p-1$ inclusive. By Exercise 53 every a that appears in this list appears exactly twice. Therefore exactly half of the $p-1$ numbers must appear in the list (i.e., be quadratic residues).

56. First assume that $\left(\frac{a}{p}\right) = 1$. Then the congruence $x^2 \equiv a \pmod{p}$ has a solution, say $x = s$. By Fermat's Little Theorem $a^{(p-1)/2} = (s^2)^{(p-1)/2} = s^{p-1} \equiv 1 \pmod{p}$, as desired. Next consider the case $\left(\frac{a}{p}\right) = -1$. Then the congruence $x^2 \equiv a \pmod{p}$ has no solution. Let i be an integer between 1 and $p-1$, inclusive. By Theorem 3, i has an inverse i' modulo p, and therefore there is an integer j, namely $i'a$, such that $ij \equiv a \pmod{p}$. Furthermore, since the congruence $x^2 \equiv a \pmod{p}$ has no solution, $j \neq i$. Thus we can group the integers from 1 to $p-1$ into $(p-1)/2$ pairs each with the product a. Multiplying these pairs together, we find that $(p-1)! \equiv a^{(p-1)/2} \pmod{p}$. But now Wilson's Theorem (see Exercise 16) tells us that this latter value is -1, again as desired.

58. If $p \equiv 1 \pmod{4}$, then $(p-1)/2$ is even, so the right-hand side of the equivalence in Exercise 56 with $a = -1$ is $+1$, that is, -1 is a quadratic residue. Conversely, if $p \equiv 3 \pmod{4}$, then $(p-1)/2$ is odd, so the right-hand side of the equivalence in Exercise 56 with $a = -1$ is -1, that is, -1 is not a quadratic residue.

60. We follow the hint. Working modulo 3, we want to solve $x^2 \equiv 16 \equiv 1$. It is easy to see that there are exactly two solutions modulo 3, namely $x = 1$ and $x = 2$. Similarly we find the solutions $x = 1$ and $x = 4$ to $x^2 \equiv 16 \equiv 1 \pmod{5}$; and the solutions $x = 3$ and $x = 4$ to $x^2 \equiv 16 \equiv 1 \pmod{7}$. Therefore we want to find values of x modulo $3 \cdot 5 \cdot 7 = 105$ such that $x \equiv 1$ or $2 \pmod{3}$, $x \equiv 1$ or $4 \pmod{5}$ and $x \equiv 3$ or $4 \pmod{7}$. We can do this by applying the Chinese Remainder Theorem (as in Example 6) eight times, for the eight combinations of these values. For example, to solve $x \equiv 1 \pmod{3}$, $x \equiv 1 \pmod{5}$, and $x \equiv 3 \pmod{7}$, we find that $m = 105$, $M_1 = 35$, $M_2 = 21$, $M_3 = 15$, $y_1 = 2$, $y_2 = 1$, $y_3 = 1$, so $x \equiv 1 \cdot 35 \cdot 2 + 1 \cdot 21 \cdot 1 + 3 \cdot 15 \cdot 1 = 136 \equiv 31 \pmod{105}$. Doing the similar calculation with the other seven possibilities yields the other solutions modulo 105: $x = 4$, $x = 11$, $x = 46$, $x = 59$, $x = 74$, $x = 94$ and $x = 101$.