SECTION 3.7 Applications of Number Theory

Many of these exercises are reasonably straightforward calculations, but the amount of arithmetic involved in some of them can be formidable. Look at the worked out examples in the text if you need help getting the hang of it. The theoretical exercises, such as #16 and #17 give you a good taste of the kinds of proofs in an elementary number theory course. Look at Exercise 45: it will give you a better understanding of some of the issues underlying this section, by forcing you to confront the difference between calculations that can be done without trial and error and those that seem to require it.

1. **a)** This first one is easy to do by inspection. Clearly 10 and 11 are relatively prime, so their greatest common divisor is 1, and $1 = 11 - 10 = (-1) \cdot 10 + 1 \cdot 11$.

b) In order to find the coefficients s and t such that $21s + 44t = \gcd(21, 44)$, we carry out the steps of the Euclidean algorithm.

$$44 = 2 \cdot 21 + 2$$
$$21 = 10 \cdot 2 + 1$$

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 44, 21, and 2. In particular, the last equation tells us that $1 = 21 - 10 \cdot 2$, so that we have expressed the gcd as a linear combination of 21 and 2. But now the first equation tells us that $2 = 44 - 2 \cdot 21$; we plug this into our previous equation and obtain

$$1 = 21 - 10 \cdot (44 - 2 \cdot 21) = 21 \cdot 21 - 10 \cdot 44 .$$

Thus we have expressed 1 as a linear combination (with integer coefficients) of 21 and 44, namely $\gcd(21, 44) = 21 \cdot 21 + (-10) \cdot 44$.

c) Again, we carry out the Euclidean algorithm. Since $48 = 1 \cdot 36 + 12$, and $12 \mid 36$, we know that $\gcd(36, 48) = 12$. From the equation shown here, we can immediately write $12 = (-1) \cdot 36 + 48$.

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

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

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

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

e) 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.

$$\begin{aligned} 213 &= 1 \cdot 117 + 96 \\ 117 &= 1 \cdot 96 + 21 \\ 96 &= 4 \cdot 21 + 12 \\ 21 &= 1 \cdot 12 + 9 \\ 12 &= 1 \cdot 9 + 3 \end{aligned}$$

Since $3 \mid 9$, we have $\gcd(117, 213) = 3$.

$$\begin{aligned} 3 &= 12 - 9 \\ &= 12 - (21 - 12) = 2 \cdot 12 - 21 \\ &= 2 \cdot (96 - 4 \cdot 21) - 21 = 2 \cdot 96 - 9 \cdot 21 \\ &= 2 \cdot 96 - 9 \cdot (117 - 96) = 11 \cdot 96 - 9 \cdot 117 \\ &= 11 \cdot (213 - 117) - 9 \cdot 117 = 11 \cdot 213 - 20 \cdot 117 \end{aligned}$$

f) Clearly $\gcd(0, 223) = 223$, so we can write $223 = s \cdot 0 + 1 \cdot 223$ for any integer s.

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.

$$\begin{aligned} 2347 &= 19 \cdot 123 + 10 \\ 123 &= 12 \cdot 10 + 3 \\ 10 &= 3 \cdot 3 + 1 \end{aligned}$$

Thus the greatest common divisor is 1.

$$\begin{aligned} 1 &= 10 - 3 \cdot 3 \\ &= 10 - 3 \cdot (123 - 12 \cdot 10) = 37 \cdot 10 - 3 \cdot 123 \\ &= 37 \cdot (2347 - 19 \cdot 123) - 3 \cdot 123 = 37 \cdot 2347 - 706 \cdot 123 \end{aligned}$$

h) 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.

$$\begin{aligned}
4666 &= 3454 + 1212 \\
3454 &= 2 \cdot 1212 + 1030 \\
1212 &= 1030 + 182 \\
1030 &= 5 \cdot 182 + 120 \\
182 &= 120 + 62 \\
120 &= 62 + 58 \\
62 &= 58 + 4 \\
58 &= 14 \cdot 4 + 2
\end{aligned}$$

Since $2 \mid 4$, the greatest common divisor is 2.

$$\begin{aligned}
2 &= 58 - 14 \cdot 4 \\
&= 58 - 14 \cdot (62 - 58) = 15 \cdot 58 - 14 \cdot 62 \\
&= 15 \cdot (120 - 62) - 14 \cdot 62 = 15 \cdot 120 - 29 \cdot 62 \\
&= 15 \cdot 120 - 29 \cdot (182 - 120) = 44 \cdot 120 - 29 \cdot 182 \\
&= 44 \cdot (1030 - 5 \cdot 182) - 29 \cdot 182 = 44 \cdot 1030 - 249 \cdot 182 \\
&= 44 \cdot 1030 - 249 \cdot (1212 - 1030) = 293 \cdot 1030 - 249 \cdot 1212 \\
&= 293 \cdot (3454 - 2 \cdot 1212) - 249 \cdot 1212 = 293 \cdot 3454 - 835 \cdot 1212 \\
&= 293 \cdot 3454 - 835 \cdot (4666 - 3454) = 1128 \cdot 3454 - 835 \cdot 4666
\end{aligned}$$

i) 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.

$$\begin{aligned}
11111 &= 9999 + 1112 \\
9999 &= 8 \cdot 1112 + 1103 \\
1112 &= 1103 + 9 \\
1103 &= 122 \cdot 9 + 5 \\
9 &= 5 + 4 \\
5 &= 4 + 1
\end{aligned}$$

Thus 1 is the greatest common divisor.

$$\begin{aligned}
1 &= 5 - 4 \\
&= 5 - (9 - 5) = 2 \cdot 5 - 9 \\
&= 2 \cdot (1103 - 122 \cdot 9) - 9 = 2 \cdot 1103 - 245 \cdot 9 \\
&= 2 \cdot 1103 - 245 \cdot (1112 - 1103) = 247 \cdot 1103 - 245 \cdot 1112 \\
&= 247 \cdot (9999 - 8 \cdot 1112) - 245 \cdot 1112 = 247 \cdot 9999 - 2221 \cdot 1112 \\
&= 247 \cdot 9999 - 2221 \cdot (11111 - 9999) = 2468 \cdot 9999 - 2221 \cdot 11111
\end{aligned}$$

3. We simply need to show that $15 \cdot 7 \equiv 1 \pmod{26}$, or in other words, that $15 \cdot 7 - 1$ is divisible by 26. But this quantity is 104, which is $26 \cdot 4$.

5. We could look for the inverse by trial and error, since there are only nine possibilities. Alternately, we could write 1 (the greatest common divisor of 4 and 9) as a linear combination of 4 and 9. Indeed, using the techniques shown in Exercise 1, we have $1 = 7 \cdot 4 - 3 \cdot 9$. This tells us that $7 \cdot 4 - 1$ is divisible by 9, which means that $7 \cdot 4 \equiv 1 \pmod{9}$. In other words, 7 is the desired inverse of 4 modulo 9.

7. Using the techniques of Exercise 1, we can determine that $1 = 52 \cdot 19 - 7 \cdot 141$. This immediately tells us that $52 \cdot 19 \equiv 1 \pmod{141}$, so 52 is the desired inverse.

9. We follow the hint. Suppose that we had two inverses of a modulo m, say b and c. In symbols, we would have $ba \equiv 1 \pmod{m}$ and $ca \equiv 1 \pmod{m}$. The first congruence says that m divides $ba - 1$, and the second says that m divides $ca - 1$. Therefore m divides the difference $(ba - 1) - (ca - 1) = ba - ca$. (The difference of two multiples of m is a multiple of m.) Thus $ba \equiv ca \pmod{m}$. It follows immediately from Theorem 2 (the roles of a, b, and c need to be permuted) that $b \equiv c \pmod{m}$, which is what we wanted to prove.

11. By Exercise 5, we know that 7 is an inverse of 4 modulo 9. Therefore we can multiply both sides of the given congruence by 7 and obtain $x \equiv 7 \cdot 5 = 35 \equiv 8 \pmod{9}$. Therefore the solution set consists of all numbers congruent to 8 modulo 9, namely $\ldots, -10, -1, 8, 17, \ldots$. We can check, for example, that $4 \cdot 8 = 32 \equiv 5 \pmod{9}$.

13. The hypothesis tells us that m divides $ac - bc$, which is the product $(a - b)c$. Let m' be $m/\gcd(c, m)$. Then m' is a factor of m, so certainly $m' \mid (a - b)c$. Now since all the common factors of m and c were divided out of m to get m', we know that m' is relatively prime to c. It follows from Lemma 1 that $m' \mid a - b$. But this means that $a \equiv b \pmod{m'}$, exactly what we were trying to prove.

15. We want to find numbers x such that $x^2 \equiv 1 \pmod{p}$, in other words, such that p divides $x^2 - 1$. Factoring this expression, we see that we are seeking numbers x such that $p \mid (x + 1)(x - 1)$. By Lemma 2, this can only happen if $p \mid x + 1$ or $p \mid x - 1$. But these two congruences are equivalent to the statements $x \equiv -1 \pmod{p}$ and $x \equiv 1 \pmod{p}$.

17. **a)** If two of these integers were congruent modulo p, say ia and ja, where $1 \leq i < j < p$, then we would have $p \mid ja - ia$, or $p \mid (j - i)a$. By Lemma 1, since a is not divisible by p, p must divide $j - i$. But this is impossible, since $j - i$ is a positive integer less than p. Therefore no two of these integers are congruent modulo p.

b) By part **(a)**, since no two of a, $2a$, $\ldots$, $(p - 1)a$ are congruent modulo p, each must be congruent to a different number from 1 to $p - 1$. Therefore if we multiply them all together, we will obtain the same product, modulo p, as if we had multiplied all the numbers from 1 to $p - 1$. In symbols,

$$a \cdot 2a \cdot 3a \cdots (p - 1)a \equiv 1 \cdot 2 \cdot 3 \cdots (p - 1) \pmod{p}.$$

The left-hand side of this congruence is clearly $(p - 1)! \cdot a^{p-1}$, and the right-hand side is just $(p - 1)!$, as desired.

c) Wilson's Theorem says that $(p - 1)!$ is congruent to -1 modulo p. Therefore the congruence in part **(b)** says that $(-1) \cdot a^{p-1} \equiv -1 \pmod{p}$. Multiplying both sides by -1, we see that $a^{p-1} \equiv 1 \pmod{p}$, as desired. Note that we already assumed the hypothesis that $p \nmid a$ in part **(a)**.

d) If $p \mid a$, then both sides of $a^p \equiv a \pmod{p}$ are 0 modulo p, so the congruence holds. If not, then we just multiply the result obtained in part **(c)** by a.

19. Since 2, 3, 5, and 11 are pairwise relatively prime, we can use the Chinese Remainder Theorem. The answer will be unique modulo $2 \cdot 3 \cdot 5 \cdot 11 = 330$. Using the notation in the text, we have $a_1 = 1$, $m_1 = 2$, $a_2 = 2$, $m_2 = 3$, $a_3 = 3$, $m_3 = 5$, $a_4 = 4$, $m_4 = 11$, $m = 330$, $M_1 = 330/2 = 165$, $M_2 = 330/3 = 110$, $M_3 = 330/5 = 66$, $M_4 = 330/11 = 30$. Then we need to find inverses y_i of M_i modulo m_i for $i = 1, 2, 3, 4$. 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 $y_1 = 1$, $y_2 = 2$, $y_3 = 1$, and $y_4 = 7$ (for this last one, $30 \equiv 8 \pmod{11}$, so we want to solve $8y_4 = 1 \pmod{11}$, and we observe that $8 \cdot 7 = 56 \equiv 1 \pmod{11}$). Thus our solution is $x = 1 \cdot 165 \cdot 1 + 2 \cdot 110 \cdot 2 + 3 \cdot 66 \cdot 1 + 4 \cdot 30 \cdot 7 = 1643 \equiv 323 \pmod{330}$. So the solutions are all integers of the form $323 + 330k$, where k is an integer.

21. 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 $x \equiv 4 \pmod{12}$, we must have $x \equiv 4 \equiv 1 \pmod 3$ and $x \equiv 4 \equiv 0 \pmod 4$. Similarly, from the third congruence we must have $x \equiv 1 \pmod 3$ and $x \equiv 2 \pmod 7$. Since the first congruence is consistent with the requirement that $x \equiv 1 \pmod 3$, we see that our system is equivalent to the system $x \equiv 7 \pmod 9$, $x \equiv 0 \pmod 4$, $x \equiv 2 \pmod 7$. These can be solved using the Chinese Remainder Theorem (see Exercise 19 or Example 6) to yield $x \equiv 16 \pmod{252}$. Therefore the solutions are all integers of the form $16 + 252k$, where k is an integer.

23. We will argue for the truth of this statement using the Fundamental Theorem of Arithmetic. What we must show is that $m_1 m_2 \cdots m_n \mid a - b$. Look at the prime factorization of both sides of this proposition. Suppose that p is a prime appearing in the prime factorization of the left-hand side. Then $p \mid m_j$ for some j. Since the m_i's are relatively prime, p does not appear as a factor in any of the other m_i's. Now we know from the hypothesis that $m_j \mid a - b$. Therefore $a - b$ contains the factor p in its prime factorization, and p must appear to a power at least as large as the power to which it appears in m_j. But what we have just shown is that each prime power p^r in the prime factorization of the left-hand side also appears in the prime factorization of the right-hand side. Therefore the left-hand side does, indeed, divide the right-hand side.

25. We are asked to solve the simultaneous congruences $x \equiv 1 \pmod 2$ and $x \equiv 1 \pmod 3$. The solution will be unique modulo $2 \cdot 3 = 6$. By inspection we see that the answer is simply that $x \equiv 1 \pmod 6$. The solution set is $\{\ldots, -11, -5, 1, 7, 13, \ldots\}$.

27. **a)** We calculate $2^{340} = (2^{10})^{34} \equiv 1^{34} = 1 \pmod{11}$, since Fermat's Little Theorem says that $2^{10} \equiv 1 \pmod{11}$.
b) We calculate $2^{340} = (2^5)^{68} = 32^{68} \equiv 1^{68} = 1 \pmod{31}$, since $32 \equiv 1 \pmod{31}$.
c) Since 11 and 31 are relatively prime, and $11 \cdot 31 = 341$, it follows from the first two parts and Exercise 23 that $2^{340} \equiv 1 \pmod{341}$.

29. **a)** By Fermat's Little Theorem we know that $5^6 \equiv 1 \pmod 7$; therefore $5^{1998} = (5^6)^{333} \equiv 1^{333} \equiv 1 \pmod 7$, and so $5^{2003} = 5^5 \cdot 5^{1998} \equiv 3125 \cdot 1 \equiv 3 \pmod 7$. So 5^{2003} **mod** $7 = 3$. Similarly, $5^{10} \equiv 1 \pmod{11}$; therefore $5^{2000} = (5^{10})^{200} \equiv 1^{200} \equiv 1 \pmod{11}$, and so $5^{2003} = 5^3 \cdot 5^{2000} \equiv 125 \cdot 1 \equiv 4 \pmod{11}$. So 5^{2003} **mod** $11 = 4$. Finally, $5^{12} \equiv 1 \pmod{13}$; therefore $5^{1992} = (5^{12})^{166} \equiv 1^{166} \equiv 1 \pmod{13}$, and so $5^{2003} = 5^{11} \cdot 5^{1992} \equiv 48{,}828{,}125 \cdot 1 \equiv 8 \pmod{13}$. So 5^{2003} **mod** $13 = 8$.
b) We now apply the Chinese Remainder Theorem to the results of part **(a)**, as in Example 6. Let $m = 7 \cdot 11 \cdot 13 = 1001$, $M_1 = m/7 = 143$, $M_2 = m/11 = 91$, and $M_3 = m/13 = 77$. We see that 5 is an inverse of 143 modulo 7, since $143 \equiv 3 \pmod 7$, and $3 \cdot 5 = 15 \equiv 1 \pmod 7$. Similarly, 4 is an inverse of 91 modulo 11, and 12 is an inverse of 77 modulo 13. (An algorithm to compute inverses—if we don't want to find them by inspection as we've done here—is given in Theorem 3. See Example 3.) Therefore the answer is $(3 \cdot 143 \cdot 5 + 4 \cdot 91 \cdot 4 + 8 \cdot 77 \cdot 12)$ **mod** $1001 = 10993$ **mod** $1001 = 983$.

31. First note that $2047 = 23 \cdot 89$, so 2047 is composite. To apply Miller's test, we write $2047 - 1 = 2046 = 2 \cdot 1023$, so $s = 1$ and $t = 1023$. We must show that either $2^{1023} \equiv 1 \pmod{2047}$ or $2^{1023} \equiv -1 \pmod{2047}$. To compute, we write $2^{1023} = (2^{11})^{93} = 2048^{93} \equiv 1^{93} = 1 \pmod{2047}$, as desired. (We could also compute this using the modular exponentiation algorithm given in Section 3.6—see Example 11 in that section.)

33. We factor $2821 = 7 \cdot 13 \cdot 31$. We must show that this number meets the definition of Carmichael number, namely that $b^{2820} \equiv 1 \pmod{2821}$ for all b relatively prime to 2821. Note that if $\gcd(b, 2821) = 1$, then $\gcd(b, 7) = \gcd(b, 13) = \gcd(b, 31) = 1$. Using Fermat's Little Theorem we find that $b^6 \equiv 1 \pmod 7$, $b^{12} \equiv 1 \pmod{13}$, and $b^{30} \equiv 1 \pmod{31}$. It follows that $b^{2820} = (b^6)^{470} \equiv 1 \pmod 7$, $b^{2820} = (b^{12})^{235} \equiv$

$1 \pmod{13}$, and $b^{2820} = (b^{30})^{94} \equiv 1 \pmod{31}$. By Exercise 23 (or the Chinese Remainder Theorem) it follows that $b^{2820} \equiv 1 \pmod{2821}$, as desired.

35. **a)** If we multiply out this expression, we get $n = 1296m^3 + 396m^2 + 36m + 1$. Clearly $6m \mid n - 1$, $12m \mid n - 1$, and $18m \mid n - 1$. Therefore, the conditions of Exercise 34 are met, and we conclude that n is a Carmichael number.

b) Letting $m = 51$ gives $n = 172{,}947{,}529$. We note that $6m + 1 = 307$, $12m + 1 = 613$, and $18m + 1 = 919$ are all prime.

37. It is straightforward to calculate the remainders when the integers from 0 to 14 are divided by 3 and by 5. For example, the remainders when 10 is divided by 3 and 5 are 1 and 0, respectively, so we represent 10 by the pair $(1, 0)$. The exercise is simply asking us to tabulate these remainders, as in Example 7.

$0 = (0, 0)$	$3 = (0, 3)$	$6 = (0, 1)$	$9 = (0, 4)$	$12 = (0, 2)$
$1 = (1, 1)$	$4 = (1, 4)$	$7 = (1, 2)$	$10 = (1, 0)$	$13 = (1, 3)$
$2 = (2, 2)$	$5 = (2, 0)$	$8 = (2, 3)$	$11 = (2, 1)$	$14 = (2, 4)$

39. The method of solving a system of congruences such as this is given in the proof of Theorem 4. Here we have $m_1 = 99$, $m_2 = 98$, $m_3 = 97$, and $m_4 = 95$, so that $m = 99 \cdot 98 \cdot 97 \cdot 95 = 89403930$. We compute the values $M_k = m/m_k$ and obtain $M_1 = 903070$, $M_2 = 912285$, $M_3 = 921690$, and $M_4 = 941094$. Next we need to find the inverses y_k of M_k modulo m_k. To do this we first replace each M_k by its remainder modulo m_k (to make the arithmetic easier), and then apply the technique shown in the solution to Exercise 7. For $k = 1$ we want to find the inverse of 903070 modulo 99, which is the same as the inverse of 903070 **mod** 99, namely 91. To do this we apply the Euclidean algorithm to express 1 as a linear combination of 91 and 99.

$$\begin{aligned}
99 &= 91 + 8 \\
91 &= 11 \cdot 8 + 3 \\
8 &= 2 \cdot 3 + 2 \\
3 &= 2 + 1 \\
\therefore\ 1 &= 3 - 2 \\
&= 3 - (8 - 2 \cdot 3) = 3 \cdot 3 - 8 \\
&= 3 \cdot (91 - 11 \cdot 8) - 8 = 3 \cdot 91 - 34 \cdot 8 \\
&= 3 \cdot 91 - 34 \cdot (99 - 91) = 37 \cdot 91 - 34 \cdot 99
\end{aligned}$$

We therefore conclude that the inverse of 91 modulo 99 is 37, so we have $y_1 = 37$. Similar calculations show that $y_2 = 33$, $y_3 = 24$, and $y_4 = 4$. Continuing with the procedure outlined in the proof of Theorem 4, we now form the sum of the products $a_k M_k y_k$, and this will be our solution. We have

$$65 \cdot 903070 \cdot 37 + 2 \cdot 912285 \cdot 33 + 51 \cdot 921690 \cdot 24 + 10 \cdot 941094 \cdot 4 = 3397886480\,.$$

We want our answer reduced modulo m, so we divide by 89403930 and take the remainder, obtaining 537140. (All of these calculations are not difficult using a scientific calculator.) Finally, let us check our answer: 537140 **mod** 99 = 65, 537140 **mod** 98 = 2, 537140 **mod** 97 = 51, 537140 **mod** 95 = 10.

41. One can compute $\gcd(2^a - 1, 2^b - 1)$ using the Euclidean algorithm. Let us look at what happens when we do so. If $b = 1$, then the answer is just $2^a - 1$, which is the same as $2^{\gcd(a,b)} - 1$ in this case. Otherwise, we reduce the problem to computing $\gcd(2^b - 1, (2^a - 1) \textbf{ mod } (2^b - 1))$. Now from Exercise 40 we know that this second argument equals $2^{a \textbf{ mod } b} - 1$. Therefore the exponents involved in the continuing calculation are b and a **mod** b—exactly the same quantities that are involved in computing $\gcd(a, b)$! It follows that when the process terminates, the answer must be $2^{\gcd(a,b)} - 1$, as desired.

43. Let q be a (necessarily odd) prime dividing $2^p - 1$. By Fermat's Little Theorem, we know that $q \mid 2^{q-1} - 1$. Then from Exercise 41 we know that $\gcd(2^p - 1, 2^{q-1} - 1) = 2^{\gcd(p,q-1)} - 1$. Since q is a common divisor of $2^p - 1$ and $2^{q-1} - 1$, we know that $\gcd(2^p - 1, 2^{q-1} - 1) > 1$. Hence $\gcd(p, q-1) = p$, since the only other possibility, namely $\gcd(p, q-1) = 1$, would give us $\gcd(2^p - 1, 2^{q-1} - 1) = 1$. Hence $p \mid q - 1$, and therefore there is a positive integer m such that $q - 1 = mp$. Since q is odd, m must be even, say $m = 2k$, and so every prime divisor of $2^p - 1$ is of the form $2kp + 1$. Furthermore, products of numbers of this form are also of this form, since $(2k_1p + 1)(2k_2p + 1) = 4k_1k_2p^2 + 2k_1p + 2k_2p + 1 = 2(2k_1k_2p + k_1 + k_2)p + 1$. Therefore all divisors of $2^p - 1$ are of this form.

45. Suppose that we know $n = pq$ and $(p-1)(q-1)$, and we wish to find p and q. Here is how we do so. Expanding $(p-1)(q-1)$ algebraically we obtain $pq - p - q + 1 = n - p - q + 1$. Thus we know the value of $n - p - q + 1$, and so we can easily calculate the value of $p + q$ (since we know n). But we also know the value of pq, namely n. This gives us two simultaneous equations in two unknowns, and we can solve them using the quadratic formula. Here is an example. Suppose that we want to factor $n = 341$, and we are told that $(p-1)(q-1) = 300$. We want to find p and q. Following the argument just outlined, we know that $p + q = 341 + 1 - 300 = 42$. Plugging $q = 42 - p$ into $pq = 341$ we obtain $p(42 - p) = 341$, or $p^2 - 42p + 341 = 0$. The quadratic formula then tells us that $p = (42 + \sqrt{42^2 - 4 \cdot 341})/2 = 31$, and so the factors are 31 and $42 - 31 = 11$. Note that absolutely no trial divisions were involved here—it was just straight calculation.

47. This problem requires a great amount of calculation. Ideally, one should do it using a computer algebra package, such as *Mathematica* or *Maple*. Let us follow the procedure outlined in Example 12. We need to compute 0667^{937} **mod** $2537 = 1808$, 1947^{937} **mod** $2537 = 1121$, and 0671^{937} **mod** $2537 = 0417$. (These calculations can in principle be done with a calculator, using the fast modular exponentiation algorithm, but it would probably take the better part of an hour and be prone to transcription errors.) Thus the original message is 1808 1121 0417, which is easily translated into letters as SILVER.

49. When we apply the Euclidean algorithm we obtain the following quotients and remainders: $q_1 = 1$, $r_2 = 55$, $q_2 = 1$, $r_3 = 34$, $q_3 = 1$, $r_4 = 21$, $q_4 = 1$, $r_5 = 13$, $q_5 = 1$, $r_6 = 8$, $q_6 = 1$, $r_7 = 5$, $q_7 = 1$, $r_8 = 3$, $q_8 = 1$, $r_9 = 2$, $q_9 = 1$, $r_{10} = 1$, $q_{10} = 2$. Note that $n = 10$. Thus we compute the successive s's and t's as follows, using the given recurrences:

$s_2 = s_0 - q_1 s_1 = 1 - 1 \cdot 0 = 1$, $t_2 = t_0 - q_1 t_1 = 0 - 1 \cdot 1 = -1$

$s_3 = s_1 - q_2 s_2 = 0 - 1 \cdot 1 = -1$, $t_3 = t_1 - q_2 t_2 = 1 - 1 \cdot (-1) = 2$

$s_4 = s_2 - q_3 s_3 = 1 - 1 \cdot (-1) = 2$, $t_4 = t_2 - q_3 t_3 = -1 - 1 \cdot 2 = -3$

$s_5 = s_3 - q_4 s_4 = -1 - 1 \cdot 2 = -3$, $t_5 = t_3 - q_4 t_4 = 2 - 1 \cdot (-3) = 5$

$s_6 = s_4 - q_5 s_5 = 2 - 1 \cdot (-3) = 5$, $t_6 = t_4 - q_5 t_5 = -3 - 1 \cdot 5 = -8$

$s_7 = s_5 - q_6 s_6 = -3 - 1 \cdot 5 = -8$, $t_7 = t_5 - q_6 t_6 = 5 - 1 \cdot (-8) = 13$

$s_8 = s_6 - q_7 s_7 = 5 - 1 \cdot (-8) = 13$, $t_8 = t_6 - q_7 t_7 = -8 - 1 \cdot 13 = -21$

$s_9 = s_7 - q_8 s_8 = -8 - 1 \cdot 13 = -21$, $t_9 = t_7 - q_8 t_8 = 13 - 1 \cdot (-21) = 34$

$s_{10} = s_8 - q_9 s_9 = 13 - 1 \cdot (-21) = 34$, $t_{10} = t_8 - q_9 t_9 = -21 - 1 \cdot 34 = -55$

Thus we have $s_{10}a + t_{10}b = 34 \cdot 144 + (-55) \cdot 89 = 1$, which is $\gcd(144, 89)$.

51. We start with the pseudocode for the Euclidean algorithm (Algorithm 6 in Section 3.6) and add variables to keep track of the s and t values. We need three of them, since the new s depends on the previous two s's, and similarly for t. We also need to keep track of q.

```
procedure extended Euclidean(a, b : positive integers)
x := a
y := b
oldolds := 1
olds := 0
oldoldt := 0
oldt := 1
while y ≠ 0
begin
        q := x div y
        r := x mod y
        x := y
        y := r
        s := oldolds − q · olds
        t := oldoldt − q · oldt
        oldolds := olds
        oldoldt := oldt
        olds := s
        oldt := t
end { gcd(a, b) is x, and (oldolds)a + (oldoldt)b = x }
```

53. We need to prove that if the congruence $x^2 \equiv a \pmod{p}$ has any solutions at all, then it has exactly two solutions. So let us assume that s is a solution. Clearly $-s$ is a solution as well, since $(-s)^2 = s^2$. Furthermore, $-s \not\equiv s \pmod{p}$, since if it were, we would have $2s \equiv 0 \pmod{p}$, which means that $p \mid 2s$. Since p is an odd prime, that means that $p \mid s$, so that $s \equiv 0 \pmod{p}$. Therefore $a \equiv 0 \pmod{p}$, contradicting the conditions of the problem.

It remains to prove that there cannot be more than two incongruent solutions. Suppose that s is one solution and that t is a second solution. We have $s^2 \equiv t^2 \pmod{p}$. This means that $p \mid s^2 - t^2$, that is, $p \mid (s + t)(s - t)$. Since p is prime, Lemma 2 guarantees that $p \mid s - t$ or $p \mid s + t$. This means that $t \equiv s \pmod{p}$ or $t \equiv -s \pmod{p}$. Therefore any solution t must be either the first solution or its negative. In other words, there are at most two solutions.

55. There is really almost nothing to prove here. The value $\left(\frac{a}{p}\right)$ depends only on whether or not a is a quadratic residue modulo p, i.e., whether or not the equivalence $x^2 \equiv a \pmod{p}$ has a solution. Obviously, this depends only on the equivalence class of a modulo p.

57. By Exercise 56 we know that $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \equiv a^{(p-1)/2}b^{(p-1)/2} = (ab)^{(p-1)/2} \equiv \left(\frac{ab}{p}\right) \pmod{p}$. Since the only values either side of this equivalence can take on are ± 1, being congruent modulo p is the same as being equal.

59. We follow the hint. Working modulo 5, we want to solve $x^2 \equiv 4$. It is easy to see that there are exactly two solutions modulo 5, namely $x = 2$ and $x = 3$. Similarly there are only the solutions $x = 1$ and $x = 6$ modulo 7. Therefore we want to find values of x modulo $5 \cdot 7 = 35$ such that $x \equiv 2$ or $3 \pmod{5}$ and $x \equiv 1$ or $6 \pmod{7}$. We can do this by applying the Chinese Remainder Theorem (as in Example 6) four times, for the four combinations of these values. For example, to solve $x \equiv 2 \pmod{5}$ and $x \equiv 1 \pmod{7}$, we find that $m = 35$, $M_1 = 7$, $M_2 = 5$, $y_1 = 3$, $y_2 = 3$, so $x \equiv 2 \cdot 7 \cdot 3 + 1 \cdot 5 \cdot 3 = 57 \equiv 22 \pmod{35}$. Doing the similar calculation with the other three possibilities yields the other three solutions modulo 35: $x = 8$, $x = 13$, and $x = 27$.

61. Suppose that we use a prime for n. To find a private decryption key from the corresponding public encryption key e, one would need to find a number d that is an inverse for e modulo $n - 1$ so that the calculation shown before Example 12 can go through. But finding such a d is easy using the Euclidean algorithm, because the

person doing this would already know $n-1$. (In particular, to find d, one can work backward through the steps of the Euclidean algorithm to express 1 as a linear combination of e and $n-1$; then d is the coefficient of e in this linear combination.) The important point in the actual RSA system is that the person trying to find this inverse will not know $(p-1)(q-1)$ and therefore cannot simply use the Euclidean algorithm.