9. $(3314430)_5$

11. $(4320023)_5$

13. $(16665)_{16}$

15. $(B705736)_{16}$

17. We represent the integer $(18235187)_{10}$ using three words—$((018)(235)(187))_{1000}$—and the integer $(22135674)_{10}$ using three words—$((022)(135)(674))_{1000}$—where each base 1000 digit is represented by three base 10 digits in parentheses. To find the sum, difference, and product of these integers from their base 1000 representations, we carry out the algorithms for such computations for base 1000.

19. To add numbers using the one's complement representation, first decide whether the answer will be negative or positive. To do this is easy if both numbers have the same lead (sign) bit; otherwise, conduct a bit-by-bit comparison of a positive summand's digits and the complement of the negative's. Now add the other digits (all but the initial (sign) bit) as an ordinary binary number. If the sum is greater than 2^n, we have an overflow error. If not, consider the three quantities of the two summands and the sum. If exactly zero or two of these are negative, we're done. Otherwise, we need to add $(1)_2$ to this answer. Also, add an appropriate sign bit to the front of the number.

21. Let $a = (a_m a_{m-1} \ldots a_2 a_1)_!$ and $b = (b_m b_{m-1} \ldots b_2 b_1)_!$. Then $a + b$ is obtained by adding the digits from right to left with the following rule for producing carries. If $a_j + b_j + c_{j-1}$, where c_{j-1} is the carry from adding a_{j-1} and b_{j-1}, is greater than j, then $c_j = 1$, and the resulting jth digit is $a_j + b_j + c_{j-1} - j - 1$. Otherwise, $c_j = 0$. To subtract b from a, assuming $a > b$, we let $d_i = a_i - b_i + c_{i-1}$ and set $c_i = 0$ if $a_i - b_i + c_{i-1}$ is between 0 and j. Otherwise, $d_i = a_i - b_i + c_{i-1} + j + 1$ and set $c_i = -1$. In this manner, $a - b = (d_m d_{m-1} \ldots d_2 d_1)_!$.

23. We have $(a_n \ldots a_1 5)_{10}^2 = (10(a_n \ldots a_1)_{10} + 5)^2 = 100(a_n \ldots a_1)_{10}^2 + 100(a_n \ldots a_1)_{10} + 25 = 100(a_n \ldots a_1)_{10}((a_n \ldots a_1)_{10} + 1) + 25$. The decimal digits of this number consist of the decimal digits of $(a_n \ldots a_1)_{10}((a_n \ldots a_1)_{10} + 1)$ followed by 25 because this first product is multiplied by 100, which shifts its decimal expansion two digits.

Section 2.3

1. **a.** yes **b.** no **c.** yes **d.** yes **e.** yes **f.** yes

3. First note that $(n^3 + 4n^2 \log n + 101n^2)$ is $O(n^3)$ and that $(14n \log n + 8n)$ is $O(n \log n)$ as in Example 2.12. Now applying Theorem 2.3 yields the result.

5. Use Exercise 4 and follow Example 2.12 noting that $(\log n)^3 \leq n^3$ whenever n is a positive integer.

7. Let k be an integer with $1 \leq k \leq n$. Consider the function $f(k) = (n + 1 - k)k$, whose graph is a concave-down parabola with k-intercepts at $k = 0$ and $k = n + 1$. Because $f(1) = f(n) = n$, it is clear that $f(k) \geq n$ for $k = 1, 2, 3, \ldots, n$. Now consider the product $(n!)^2 = \prod_{k=1}^{n} k(n + 1 - k) \geq \prod_{k=1}^{n} n$, by the inequality above. This last is equal to n^n. Thus, we have $n^n \leq (n!)^2$. Taking logarithms of both sides yields $n \log(n) \leq 2 \log(n!)$, which shows that $n \log(n)$ is $O(\log(n!))$.

9. Suppose that f is $O(g)$ where $f(n)$ and $g(n)$ are positive integers for every integer n. Then there is an integer C such that $f(n) < Cg(n)$ for all $x \in S$. Then $f^k(n) < C^k g^k(n)$ for all $x \in S$. Hence, f^k is $O(g^k)$.

11. The number of digits in the base b expansion of n is $1 + k$ where k is the largest integer such that $b^k \leq n < b^{k+1}$ because there is a digit for each of the powers of $b^0, b^1, \ldots, b^k$. Note that this inequality is equivalent to $k \leq \log_b n < k + 1$, so that $k = [\log_b n]$. Hence, there are $[\log_b n] + 1$ digits in the base b expansion of n.

13. To multiply an n-digit integer by an m-digit integer in the conventional manner, one must multiply every digit of the first number by every digit of the second number. There are nm such pairs.

15. **a.** $O(n \log_2^2 n \log_2 \log_2 n \log_2 \log_2 \log_2 n)$ **b.** $O((n \log n)^{1+\epsilon})$ for any $\epsilon > 0$

17. $(1100011)_2$

19. **a.** $ab = (10^{2n} + 10^n)A_1B_1 + 10^n(A_1 - A_0)(B_0 - B_1) + (10^n + 1)A_0B_0$ where A_i and B_i are defined as in identity (2.2). **b.** 6351 **c.** 11,522,328

21. That the given equation is an identity may be seen by direct calculation. The seven multiplications necessary to use this identity are $a_{11}b_{11}$, $a_{12}b_{21}$, $(a_{11} - a_{21} - a_{22})(b_{11} - b_{12} - b_{22})$, $(a_{21} + a_{22})(b_{12} - b_{11})$, $(a_{11} + a_{12} - a_{21} - a_{22})b_{22}$, $(a_{11} - a_{21})(b_{22} - b_{12})$, and $a_{22}(b_{11} - b_{21} - b_{12} + b_{22})$.

23. Let $k = [\log_2 n] + 1$. Then the number of multiplications for $2^k \times 2^k$ matrices is $O(7^k)$. But, $7^k = 2^{(\log_2 7)([\log_2 n]+1)} = O(2^{\log_2 n \log_2 7} 2^{\log_2 7}) = O(n^{\log_2 7})$. The other bit operations are absorbed into this term.

Section 3.1

1. **a.** yes **b.** yes **c.** yes **d.** no **e.** yes **f.** no

3. 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 127, 131, 137, 139, 149

5. none

7. Using the identity given in the hint with k such that $1 < k < n$ and $k \mid n$, then $a^k - 1 \mid a^n - 1$. Because $a^n - 1$ is prime by hypothesis, $a^k - 1 = 1$. From this, we see that $a = 2$ and $k = 1$, contradicting the fact that $k > 1$. Thus, we must have $a = 2$ and n is prime.

9. We need to assume $n \geq 3$ to assure that $S_n > 1$. Then by Lemma 3.1, S_n has a prime divisor p. If $p \leq n$, then $p|n!$, and so $p|n! - S_n = 1$, a contradiction. Therefore, we must have $p > n$. Because we can find arbitrarily large primes, there must be infinitely many.

11. 3, 7, 31, 211, 2311, 59

13. If n is prime, we are done. Otherwise $n/p < (\sqrt[3]{n})^2$. If n/p is prime, then we are done. Otherwise, by Theorem 3.2, n/p has a prime factor less than $\sqrt{n/p} < \sqrt[3]{n}$, a contradiction.

15. **a.** 7 **b.** 19 **c.** 71

17. A positive integer has a decimal expansion ending in 1 if and only if it is of the form $10k + 1$ for some integer k. This represents an arithmetic progression. Because $(10, 1) = 1$, we may apply Dirichlet's theorem to conclude that there are infinitely many primes of this form.

19. A positive integer has a decimal expansion ending in 123 if and only if it is of the form $1000k + 123$ for some integer k. This represents an arithmetic progression. Because $(1000, 123) = 1$, we may apply Dirichlet's theorem to conclude that there are infinitely many primes of this form.

21. Let n be fixed, and let a be the integer with decimal expansion a string of n 1s followed by a 3. Consider the arithmetic progression $10^{n+1}k + a$. Because a ends in 3, it can not be divisible by 2 or 5, so $(10^{n+1}, a) = 1$. Then by Dirichlet's theorem, there are infinitely many primes in this progression, and each has the desired form.

23. If n is prime the statement is true for n. Otherwise, n is composite, so n is the product of two integers a and b such that $1 < a \leq b < n$. Because $n = ab$ and because by the inductive hypothesis both a and b are the product of primes, we conclude that n is also the product of primes.

25. 53

27. For $n = 0, 1, 2, \ldots 10$, the values of the function are 11, 13, 19, 29, 43, 61, 83, 109, 139, 173, 211, each of which is prime. But $2 \cdot 11^2 + 11 = 11(2 \cdot 11 + 1) = 11 \cdot 23,$.

29. Assume not. Let x_0 be a positive integer. It follows that $f(x_0) = p$ where p is prime. Let k be an integer. We have $f(x_0 + kp) = a_n(x_0 + kp)^n + \cdots + a_1(x_0 + kp) + a_0$. Note that

by the binomial theorem, $(x_0 + kp)^j = \sum_{i=1}^{j} \binom{j}{i} x_0^{j-i}(kp)^i$. It follows that $f(x_0 + kp) = \sum_{j=0}^{n} a_j x_0^j + Np = f(x_0) + Np$, for some integer N. Because $p \mid f(x_0)$ it follows that $p \mid (f(x_0) + Np) = f(x_0 + kp)$. Because $f(x_0 + kp)$ is supposed to be prime, it follows that $f(x_0 + kp) = p$ for all integers k. This contradicts the fact that a polynomial of degree n takes on each value no more than n times. Hence $f(y)$ is composite for at least one integer y.

31. At each stage of the procedure for generating the lucky numbers the smallest number left, say k, is designated to be a lucky number and infinitely many numbers are left after the deletion of every kth integer left. It follows that there are infinitely many steps, and at each step a new lucky number is added to the sequence. Hence there are infinitely many lucky numbers.

Section 3.2

1. 24, 25, 26, 27, 28

3. Suppose that p, $p + 2$, and $p + 4$ were all prime. We consider three cases. First, suppose that p is of the form $3k$. Then p cannot be prime unless $k = 1$, and the prime triplet is 3, 5, and 7. Next, suppose that p is of the form $3k + 1$. Then $p + 2 = 3k + 3 = 3(k + 1)$ is not prime. We obtain no prime triplets in this case. Finally, suppose that p is of the form $3k + 2$. Then $p + 4 = 3k + 6 = 3(k + 2)$ is not prime. We obtain no prime triplet in this case either.

5. (7, 11, 13), (13, 17, 19), (37, 41, 43), (67, 71, 73)

7. **a.** 5 **b.** 7 **c.** 29 **d.** 53

9. 127, 149, 173, 197, 227, 257, 293, 331, 367, 401

11. If p is a prime of the form $105n + 97$, then $p + 2 = 105n + 99 = 3(35n + 33)$ which is not prime, so p can not be the first member of a prime triple. Also, $p - 2 = 105n + 95 = 5(21n + 19)$, which is not prime, so p can not be the second member of a prime triple. Finally, $p - 6 = 105n + 91 = 7(15n + 13)$ is not prime, so p can not be the third member of a prime triple. Because $(97, 105) = 1$, Dirichlet's theorem tells us that the arithmetic progression $105n + 97$ contains infinitely many such primes.

13. **a.** $7 = 3 + 2 + 2$ **b.** $17 = 11 + 3 + 3$ **c.** $27 = 23 + 2 + 2$ **d.** $97 = 89 + 5 + 3$
e. $101 = 97 + 2 + 2$ **f.** $199 = 191 + 5 + 3$

15. Suppose that $n > 5$ and that Goldbach's conjecture is true. Apply Goldbach's conjecture to $n - 2$ if n is even, or $n - 3$ if n is odd. Conversely, suppose that every integer greater than 5 is the sum of three primes. Let $n > 2$ be an even integer. Then $n + 2$ is also an even integer that is the sum of three primes, not all odd.

17. Let $p < n$ be prime. Using the division algorithm, we divide each of the first $p + 1$ integers in the sequence by p to get $a = q_0 p + r_0$, $a + k = q_1 p + r_1, \ldots, a + pk = q_p + r_p$, with $0 \le r_i < p$ for each i. By the pigeonhole principle, at least two of the remainders must be equal, say, $r_i = r_j$. We subtract the corresponding equations to get $a + ik - a - jk = q_i p + r_i - q_j p + r_j$, which reduces to $(i - j)k = (q_i - q_j)p$. Therefore $p|(i - j)k$, and because p is prime, it must divide one of the factors. But because $(i - j) < p$, we must have $p|k$.

19. The difference is 6, achieved with 5, 11, 17, 23.

21. The difference is 30, achieved with 7, 37, 67, 97, 127, 157.

23. If $p^\alpha - q^\beta = 1$, with p, q primes, then p or q is even, so p or q is 2. If $p = 2$, there are several cases: we have $2^\alpha - q^\beta = 1$. If α is even, say, $\alpha = 2k$, $(2^{2k} - 1) = (2^k - 1)(2^k + 1) = q^\beta$. So $q|(2^k - 1)$ and $q|(2^k + 1)$; hence, $q = 1$, a contradiction. If α is odd and β is odd, $2^\alpha = 1 + q^\beta = (1 + q)(q^{\beta-1} - q^{\beta-2} + \cdots + 1)$. So $1 + q = 2^n$ for some n. Then $2^\alpha = (2^n - 1)^\beta + 1 = 2^n$(odd number), because β is odd. So $2^{\alpha-n} =$ odd number, and so $\alpha = n$. Therefore, $2^\alpha = 1 + (2^\alpha - 1)^\beta$ and so $\beta = 1$, which is not allowed. If $\alpha = 2k + 1$ and $\beta = 2n$ we have $2^{2k+1} = 1 + q^{2n}$. Because

q is odd, q^2 is of the form $4m + 1$, and by the binomial theorem, so is q^{2n}. Thus, the right-hand side of the last equation is of the form $4m + 2$, but this forces $k = 0$, a contradiction. If $q = 2$, we have $p^\alpha - 2^\beta = 1$. Whence $2^\beta = (p - 1)(p^{\alpha-1} + p^{\alpha-2} + \cdots + p + 1)$, where the last factor is the sum of α odd terms but must be a power of 2; therefore, $\alpha = 2k$ for some k. Then $2^\beta = (p^k - 1)(p^k + 1)$. These last two factors are powers of 2 that differ by 2, which forces $k = 1$, $\alpha = 2$, $\beta = 3$, $p = 3$, and $q = 2$ as the only solution: $3^2 - 2^3 = 1$.

25. Because $3p > 2n$, p and $2p$ are the only multiples of p that appear as factors in $(2n)!$. So p divides $(2n)!$ exactly twice. Because $2p > n$, p is the only multiple of p that appears as a factor in $n!$. So $p \mid n!$ exactly once. Then, because $\binom{2n}{n} = 2n!/(n!n!)$, the two factors of p in the numerator are canceled by the two in the denominator.

27. By Bertrand's conjecture, there must be a prime in each interval of the form $(2^{k-1}, 2^k)$, for $k = 2, 3, 4, \ldots$. Thus, there are at least $k - 1$ primes less than 2^k. Because the prime 2 isn't counted here, we have at least k primes less than 2^k.

29. Because $1/1$ is an integer, we may assume $n > 1$. First suppose that $m < n$. Then $1/n + 1/(n + 1) + \cdots + 1/(n + m) \le 1/n + 1/(n + 1) + \cdots + 1/(2n - 1) < 1/n + 1/n + \cdots + 1/n \le n(1/n) = 1$, so the sum can not be an integer. Now suppose $m \ge n$. Then by Bertrand's postulate, there is a prime p such that $n < p < n + m$. Let p be the largest such prime. Then $n + m < 2p$; otherwise, there would be a prime q with $p < q < 2p \le n + m$, contradicting the choice of p. Suppose that $1/n + 1/(n + 1) + \cdots + 1/p + \cdots + 1/(n + m) = a$ where a is an integer. Note that p occurs as a factor in only one denominator, because $2p > n + m$. Let $Q = \prod_{j=n}^{n+m} j$, and let $Q_i = Q/i$, for $i = n, n + 1, \ldots, n + m$. If we multiply the equation by Q, we get $Q_n + Q_{n+1} + \cdots + Q_p + \cdots + Q_{n+m} = Qa$. Note that every term on both sides of the equation is divisible by p except for Q_p. If we solve the equation for Q_p and factor a p out of the other side, we have an equation of the form $Q_p = pN$ where N is some integer. But this implies that p divides Q_p, a contradiction.

31. Suppose n has the stated property and $n \ge p^2$ for some prime p. Because p^2 is not prime, there must a prime dividing both p^2 and n, and the only possibility for this is p itself, that is, $p|n$. Now if $n \ge 7^2$, then it is greater than 2^2, 3^2, and 5^2, and hence divisible by 2, 3, 5, and 7. This is the basis step for induction. Now assume n is divisible by $p_1, p_2, \ldots, p_k$. By Bonse's inequality, $p_{k+1}^2 < p_1 p_1 \cdots p_k < n$, so $p_{k+1}|n$ also. This induction implies that every prime divides n, which is absurd. Therefore, if n has the stated property, it must be less than $7^2 = 49$. To finish, check the remaining cases.

33. First suppose $n \ge 8$. Note that by Bertrand's postulate we have $p_{n-1} < p_n < 2p_{n-1}$ and $p_{n-2} < p_{n-1} < 2p_{n-2}$. Therefore, $p_n^2 < (2p_{n-1})(2p_{n-1}) < (2p_{n-1})(4p_{n-2}) = 8p_{n-1}p_{n-2} = p_{n-1}p_{n-2}p_5 \le p_{n-1}p_{n-2}p_{n-3}$, because $n \ge 8$. Now check the cases $n = 6$ and 7.

35. From Corollary 3.4.1, we expect $p_{1,000,000} \sim 10^6 \log 10^6 \approx 10^6 6(2.306) = 13{,}836{,}000$. The millionth prime is, in fact, 15, 485, 863.

Section 3.3

1. **a.** 5 **b.** 111 **c.** 6 **d.** 1 **e.** 11 **f.** 2

3. a

5. 1

7. Let a and b be even integers. Then $a = 2k$ and $b = 2l$ for some integers k and l. Let $d = (a, b)$. Then by Bezout's theorem, there exist integers m and n such that $d = ma + nb = m2k + n2l = 2(mk + nl)$. Therefore $2 \mid d$, and so d is even.

9. By Theorem 3.8, $(ca, cb) = cma + cnb = |c| \cdot |ma + nb|$, where $cma + cnb$ is as small as possible. Therefore, $|ma + nb|$ is as small a positive integer as possible, i.e., equal to (a, b).

11. 1 or 2

13. Let $a = 2k$. Because $(a, b) \mid b$, and b is odd, (a, b) is odd. But $(a, b) \mid a = 2k$. Thus, $(a, b) \mid k$. So $(a, b) = (k, b) = (a/2, b)$.

15. Let $d = (a, b)$. Then $(a/d, b/d) = 1$, so if $g|a/d$, then $(g, b/d) = 1$. In particular, if we let $e = (a/d, bc/d)$, then $e|a/d$, so $(e, b/d) = 1$, so we must have $e|c$. Because $e|a/d$, then $e|a$, so $e|(a, c)$. Conversely, if $f = (a, c)$, then $(f, b) = 1$, so $(d, f) = 1$, so $f|a/d$, and, trivially, $f|bc/d$. Therefore $f|e$, whence $e = f$. Then $(a, b)(a, c) = de = d(a/d, bc/d) = (a, bc)$.

17. 10, 26, 65

19. **a.** 2 **b.** 5 **c.** 99 **d.** 3 **e.** 7 **f.** 1001

21. Let $A = (a_1, a_2, \ldots, a_n)$ and $D = (ca_1, ca_2, \ldots, ca_n)$. Then for each i, we have $A \mid a_i$, so that $cA \mid ca_i$. Thus, $cA \mid D$. Next, note that for each i, $c \mid ca_i$, so $c \mid D$. Then $D = cd$ for some integer d. Then for each i, $D = cd \mid ca_i$, and hence $d \mid a_i$. Therefore $d \mid A$, and so $D = cd \mid cA$. Because $cA \mid D$ and $D \mid cA$, we have $cA = D$, which completes the proof.

23. Suppose that $(6k + a, 6k + b) = d$. Then $d \mid b - a$. We have $a, b \in \{-1, 1, 2, 3, 5\}$, so if $a < b$, it follows that $b - a \in \{1, 2, 3, 4, 6\}$. Hence, $d \in \{1, 2, 3, 4, 6\}$. To show that $d = 1$, it is sufficient to show that neither 2 nor 3 divides $(6k + a, 6k + b)$. If $p = 2$ or $p = 3$ and $p \mid (6k + a, 6k + b)$, then $p \mid a$ and $p \mid b$. However, there are no such pairs a, b in the set $\{-1, 1, 2, 3, 5\}$.

25. Applying Theorem 3.7, we have $(8a + 3, 5a + 2) = (8a + 3 - (5a + 2), 5a + 2) = (3a + 1, 5a + 2) = (3a + 1, 5a + 2 - (3a + 1)) = (3a + 1, 2a + 1) = (3a + 1 - (2a + 1), 2a + 1) = (a, 2a + 1) = (a, 2a + 1 - 2a) = (a, 1) = 1$, so $8a + 3$ and $5a + 2$ are relatively prime.

27. Applying Theorem 3.7 to the numerator and denominator, we have $(15k + 4, 10k + 3) = (15k + 4 - (10k + 3), 10k + 3) = (5k + 1, 10k + 3) = (5k + 1, 10k + 3 - 2(5k + 1)) = (5k + 1, 1) = 1$. Because the numerator and denominator are relatively prime, the fraction must be in lowest terms.

29. From Exercise 21, we know that $6k - 1$, $6k + 1$, $6k + 2$, $6k + 3$, and $6k + 5$ are pairwise relatively prime. To represent n as the sum of two relatively prime integers greater than 1, let $n = 12k + h$, $0 \le h < 12$. We now examine the twelve cases, one for each possible value of h:

h	n
0	$(6k - 1) + (6k + 1)$
1	$(6k - 1) + (6k + 2)$
2	$(6k - 1) + (6k + 3)$
3	$(6k + 1) + (6k + 2)$
4	$(6k + 1) + (6k + 3)$
5	$(6k + 2) + (6k + 3)$
6	$(6k + 1) + (6k + 5)$
7	$(6k + 2) + (6k + 5)$
8	$(6k + 3) + (6k + 5)$
9	$(12k + 7) + 2$
10	$(12k + 7) + 3$
11	$(12k + 9) + 2$

31. Applying Theorem 3.7, we have $(2n^2 + 6n - 4, 2n^2 + 4n - 3) = (2n^2 + 6n - 4 - (2n^2 + 4n - 3), 2n^2 + 4n - 3) = (2n - 1, 2n^2 + 4n - 3) = (2n - 1, 2n^2 + 4n - 3 - n(2n - 1)) = (2n - 1, 5n - 3) = (2n - 1, 5n - 3 - 2(2n - 1)) = (2n - 1, n - 1) = (2n - 1 - 2(n - 1), n - 1) = (1, n - 1) = 1$, so the numbers are relatively prime.

33. $\frac{0}{1}, \frac{1}{5}, \frac{1}{4}, \frac{1}{3}, \frac{2}{5}, \frac{1}{2}, \frac{3}{5}, \frac{2}{3}, \frac{3}{4}, \frac{4}{5}, \frac{1}{1}$

35. From Exercise 36, we have $cb - ad = de - cf = 1$. Then $c(b + f) = d(a + e)$, and so $c/d = (a + e)/(b + f)$.

37. Because $a/b < (a + c)/(b + d) < c/d$, we must have $b + d > n$, or a/b and c/d would not be consecutive, because otherwise, $(a + c)/(b + d)$ would have appeared in the Farey series of order n.

39. Because $(a/b) + (c/d) = (ad + bc)/bd$ is an integer, $bd \mid ad + bc$. Certainly, then, $bd \mid d(ad + bc) = ad^2 + cbd$. Now, because $bd \mid cbd$, it must be that $bd \mid ad^2$. From this, $bdn = ad^2$ for some integer n, and it follows that $bn = ad$, or $b \mid ad$. Because $(a, b) = 1$, we must have $b \mid d$. Similarly, we can find that $d \mid b$; hence, $b = d$.

41. Consider the lattice points inside or on the triangle with vertices $(0, 0)$, $(a, 0)$, and (a, b). Note that a lattice point lies on the diagonal from $(0, 0)$ to (a, b) if and only if $[bx/a]$ is an integer. Let $d = (a, b)$ and $a = cd$, so that $(c, b) = 1$. Then $[bx/a]$ will be an integer exactly when x is a multiple of c, because then $d|b$ and $c|x$ so then $a = cd|bx$. But there are exactly d multiples of c less than or equal to a because $cd = a$, so there are exactly $d + 1$ lattice points on the diagonal when we count $(0, 0)$ also. So one way to count the lattice points in the triangle is to consider the rectangle that has $(a + 1)(b + 1)$ points and divide by 2. But we need to add back in half the points on the diagonal, which gives us $(a + 1)(b + 1)/2 + ((a, b) + 1)/2$ total points in or on the triangle. Another way to count all the points is to count each column above the horizontal axis, starting with $i = 1, 2, \ldots, a - 1$. The equation of the diagonal is $y = (b/a)x$, so for a given i, the number of points on or below the diagonal is $[bi/a]$. So the total number of interior points in the triangle plus the points on the diagonal is $\sum_{i=1}^{a-1}[bi/a]$. Then the right-hand boundary has b points (not counting $(a, 0)$) and the lower boundary has $a + 1$ points (counting $(0, 0)$). So in all, we have $\sum_{i=1}^{a-1}[bi/a] + a + b + 1$ points in or on the triangle. If we equate our two expressions and multiply through by 2, we have $(a + 1)(b + 1) + (a, b) + 1 = 2\sum_{i=1}^{a-1}[bi/a] + 2a + 2b + 2$, which simplifies to our expression.

43. Assume there are exactly r primes and consider the $r + 1$ numbers $(r + 1)! + 1$. From Lemma 3.1, each of these numbers has a prime divisor, but from Exercise 34, these numbers are pairwise relatively prime, so these prime divisors must be unique, and so we must have at least $r + 1$ different prime divisors, a contradiction.

Section 3.4

1. **a.** 15 **b.** 6 **c.** 2 **d.** 5

3. **a.** $(-1)75 + (2)45$ **b.** $(6)222 + (-13)102$ **c.** $-138(666) + (65)1414$ **d.** $-1707(20{,}785) + 800(44{,}350)$

5. **a.** 1 **b.** 7 **c.** 5

7. **a.** $16 \cdot 6 - 8 \cdot 10 - 15$ **b.** $105 - 21 \cdot 70 + 14 \cdot 98$ **c.** $0 \cdot 280 + 0 \cdot 330 - 75 \cdot 405 + 62 \cdot 490$

9. 2

11. $2n - 2$

13. Suppose we have the balanced ternary expansions for integers $a \geq b$. If both expansions end in zero, then both are divisible by 3, and we can divide this factor of 3 out by deleting the trailing zeros (a shift), in which case $(a, b) = 3(a/3, b/3)$. If exactly one expansion ends in zero, then we can divide the factor of 3 out by shifting, and we have $(a, b) = (a/3, b)$, say. If both expansions end in 1 or in -1, then we can subtract the larger from the smaller to get $(a, b) = (a - b, b)$, say, and then the expansion for $a - b$ ends in zero. Finally, if one expansion ends in 1 and the other in -1, then we can add the two to get $(a + b, b)$, where the expansion of $a + b$ now ends in zero.

Because $a + b$ is no larger than $2a$ and because we can now divide $a + b$ by 3, the larger term is reduced by a factor of at least $2/3$ after two steps. Therefore, this algorithm will terminate in a finite number of steps, when we finally have $a = b = 1$.

15. Let $r_0 = a$ and $r_1 = b$ be positive integers with $a \geq b$. By successively applying the least-remainder division algorithm, we find that

$$r_0 = r_1 q_1 + e_2 r_2, \ \frac{-r_1}{2} < e_2 r_2 \leq \frac{r_1}{2}$$
$$\vdots$$
$$r_{n-2} = r_{n-1} q_{n-1} + e_n r_n, \ \frac{-r_{n-1}}{2} < e_n r_n \leq \frac{r_{n-1}}{2}$$
$$r_{n-1} = r_n q_n.$$

We eventually obtain a remainder of zero because the sequence of remainders $a = r_0 > r_1 > r_2 > \cdots \geq 0$ cannot contain more than a terms. By Lemma 3.3, we see that $(a, b) = (r_0, r_1) = (r_1, r_2) = \cdots = (r_{n-2}, r_{n-1}) = (r_{n-1}, r_n) = (r_n, 0) = r_n$. Hence $(a, b) = r_n$, the last nonzero remainder.

17. Let $v_2 = v_3 = 2$, and for $i \geq 4$, $v_i = 2v_{i-1} + v_{i-2}$.

19. Performing the Euclidean algorithm with $r_0 = m$ and $r_1 = n$, we find that $r_0 = r_1 q_1 + r_2$, $0 \leq r_2 < r_1$, $r_1 = r_2 q_2 + r_3$, $0 \leq r_3 < r_2$, $\ldots$, $r_{k-3} = r_{k-2} q_{k-2} + r_{k-1}$, $0 \leq r_{k-1} < r_{k-2}$, and $r_{k-2} = r_{k-1} q_{k-1}$. We have $(m, n) = r_{k-1}$. We will use these steps to find the greatest common divisor $a^m - 1$ and $a^n - 1$. First, we show that if u and v are positive integers, then the least positive residue of $a^u - 1$ modulo $a^v - 1$ is $a^r - 1$, where r is the least positive residue of u modulo v. To see this, note that $u = vq + r$, where r is the least positive residue of u modulo v. It follows that $a^u - 1 = a^{vq+r} - 1 = (a^v - 1)(a^{v(q-1)+r} + \cdots + a^{v+r} + a^r) + (a^r - 1)$. This shows that the remainder is $a^r - 1$ when $a^u - 1$ is divided by $a^v - 1$. Now let $R_0 = a^m - 1$ and $R_1 = a^n - 1$. When we perform the Euclidean algorithm starting with R_0 and R_1, we obtain $R_0 = R_1 Q_1 + R_2$, where $R_2 = a^{r_2} - 1$, $R_1 = R_2 Q_2 + R_3$ where $R_3 = a^{r_3} - 1$, $\ldots$, $R_{k-3} = R_{k-2} Q_{k-2} + R_{k-1}$ where $R_{k-1} = a^{r_{k-1}} - 1$. Hence, the last nonzero remainder, $R_{k-1} = a^{r_{k-1}} - 1 = a^{(m,n)} - 1$, is the greatest common divisor of $a^m - 1$ and $a^n - 1$.

21. Note that $(x, y) = (x - ty, y)$, as any divisor of x and y is also a divisor of $x - ty$. Therefore, every move in the game of Euclid preserves the g.c.d. of the two numbers. Because $(a, 0) = a$, if the game beginning with $\{a, b\}$ terminates, then it must do so at $\{(a, b), 0)\}$. Because the sum of the two numbers is always decreasing and positive, the game must terminate.

23. Choose the integer m so that d has no more than m bits and that q has $2m$ bits, appending extra zeros to the front of q if necessary. Then $m = O(\log_2 q) = O(\log_2 d)$. Then from Theorems 2.7 and 2.5, we know that there is an algorithm for dividing q by d in $O(m^2) = O(\log_2 q \log_2 d)$ bit operations. Now let n be the number of steps needed in the Euclidean algorithm to find the greatest common divisor of a and b. Then by Theorem 3.12, $n = O(\log_2 a)$. Let q_i and r_i be as in the proof of Theorem 3.12. Then the total number of bit operations for divisions in the Euclidean algorithm is $\sum_{i=1}^{n} O(\log_2 q_i \log_2 r_i) = \sum_{i=1}^{n} O(\log_2 q_i \log_2 b) = O\left(\log_2 b \sum_{i=1}^{n} \log_2 q_i\right) = O\left(\log_2 b \log_2 \prod_{i=1}^{n} q_i\right)$. By dropping the remainder in each step of the Euclidean algorithm, we have the system of inequalities $r_i \geq r_{i+1} q_{i+1}$, for $i = 0, 1, \ldots, n - 1$. Multiplying these inequalities together yields $\prod_{i=0}^{n-1} r_i \geq \prod_{i=1}^{n} r_i q_i$. Cancelling common factors reduces this to $a = r_0 \geq r_n \prod_{i=1}^{n} q_i$. Therefore, from above, we have that the total number of bit operations is $O\left(\log_2 b \log_2 \prod_{i=1}^{n} q_i\right) = O(\log_2 b \log_2 a) = O((\log_2 a)^2)$.

25. We apply the Q_i's one at a time. When we multiply $q_n 11 0 r_n 0 = q_n r_n r_n = r_{n-1} r_n$, the top component is the last equation in the series of equations in the proof of Lemma 3.3. When we multiply this result on the left by the next matrix we get $q_{n-1} 110 r_{n-1} r_n = q_{n-1} r_{n-1} + r_n r_{n-1} =$

$r_{n-2}r_{n-1}$, which is the matrix version of the last two equations in the proof of Lemma 3.3. In general, at the ith step we have $q_{n-i}110r_{n-i-1}r_{n-i} = q_{n-i}r_{n-i-1} + r_{n-i}r_{n-i-1} = r_{n-i-2}r_{n-i-1}$, so that we inductively work our way up the equations in the proof of Lemma 3.3, until finally we have $r_0r_1 = ab$.

Section 3.5

1. **a.** $2^2 \cdot 3^2$ **b.** $3 \cdot 13$ **c.** $10^2 = 2^2 \cdot 5^2$ **d.** 17^2 **e.** $2 \cdot 111 = 2 \cdot 3 \cdot 37$ **f.** 2^8 **g.** $5 \cdot 103$ **h.** $23 \cdot 43$ **i.** $10 \cdot 504 = 2 \cdot 5 \cdot 4 \cdot 126 = 2^4 \cdot 3^2 \cdot 5 \cdot 7$ **j.** $8 \cdot 10^3 = 2^6 \cdot 5^3$ **k.** $3 \cdot 5 \cdot 7^2 \cdot 13$ **l.** $9 \cdot 1111 = 3^2 \cdot 11 \cdot 101$

3. $3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19$

5. **a.** 2, 3 **b.** 2, 3, 5 **c.** 2, 3, 5, 7, 11, 13, 17, 19 **d.** 2, 3, 7, 13, 29, 31, 37, 41, 43, 47

7. integers of the form p^2 where p is prime; integers of the of the form pq or p^3 where p and q are distinct primes.

9. Let $n = p_1^{2a_1}p_2^{2a_2} \cdots p_k^{2a_k}q_1^{2b_1+3}q_2^{2b_2+3} \cdots q_l^{2b_l+3}$ be the factorization of a powerful number. Then $n = (p_1^{a_1}p_2^{a_2} \cdots p_k^{a_k}q_1^{b_1}q_2^{b_2} \cdots q_l^{b_l})^2(q_1q_2 \cdots q_l)^3$ is a product of a square and a cube.

11. **a.** Suppose that $p^a \,||\, m$ and $p^b \,||\, n$. Then $m = p^aQ$ and $n = p^bR$, where both Q and R are products of primes other than p. Hence, $mn = (p^aQ)(p^bR) = p^{a+b}QR$. It follows that $p^{a+b} \,||\, mn$ because p does not divide QR. **b.** If $p^a \,||\, m$ then $m = p^an$, where $p \nmid n$. Then $p \nmid n^k$ and we have $m^k = p^{ka}n^k$ and we see that $p^{ka} \,||\, m^k$. **c.** Suppose that $p^a \,||\, m$ and $p^b \,||\, n$ with $a \neq b$. Then $m = p^aQ$ and $n = p^bR$ where both Q and R are products of primes other than p. Suppose, without loss of generality, that $a = \min(a, b)$. Then $m + n = p^aQ + p^bR = p^{\min(a,b)}(Q + p^{b-a}R)$. Then $p \nmid (Q + p^{b-a}R)$ because $p \nmid Q$ but $p \mid p^{b-a}R$. It follows that $p^{\min(a,b)} \,||\, (m + n)$.

13. $2^{18} \cdot 3^8 \cdot 5^4 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19$

15. 300, 301, 302, 303, 304

17. We compute $\alpha\beta = (ac - 5bd) + (ad + bc)\sqrt{-5}$. Thus, $N(\alpha\beta) = (ac - 5bd)^2 + 5(ad + bc)^2 = a^2c^2 - 10acbd + 25b^2d^2 + 5a^2d^2 + 10adbc + 5b^2c^2 = a^2(c^2 + 5d^2) + 5b^2(5d^2 + c^2) = (a^2 + 5b^2)(c^2 + 5d^2) = N(\alpha)N(\beta)$.

19. Suppose $3 = \alpha\beta$. Then by Exercise 17, $9 = N(3) = N(\alpha)N(\beta)$. Then $N(\alpha) = 1$, 3, or 9. Let $\alpha = a + b\sqrt{-5}$. Then we must have $a^2 + 5b^2 = 1$, 3, or 9. So either $b = 0$ and $a = \pm 1$ or ± 3, or $b = \pm 1$ and $a = \pm 2$. Because $a = \pm 1$, $b = 0$ is excluded, and because $a = \pm 3$ forces $\beta = \pm 1$, we must have $b = \pm 1$. That is, $\alpha = \pm 2 \pm \sqrt{-5}$. But then $N(\alpha) = 9$, and hence $N(\beta) = 1$, which forces $\beta = \pm 1$.

21. Note that $21 = 3 \cdot 7 = (1 + 2\sqrt{-5})(1 - 2\sqrt{-5})$. We know 3 is prime from Exercise 19. Similarly, if we seek $\alpha = a + b\sqrt{-5}$ such that $N(\alpha) = a^2 + 5b^2 = 7$, we find there are no solutions. For $|b| = 0$ implies $a^2 = 7$, $|b| = 1$ implies $a^2 = 2$, and $|b| > 1$ implies $a^2 < 0$, and in each case there is no such a. Hence, if $\alpha\beta = 7$, then $N(\alpha\beta) = N(\alpha)N(\beta) = N(7) = 49$. So one of $N(\alpha)$ and $N(\beta)$ must be equal to 49 and the other equal to 1. Hence, 7 is also prime. We have shown that there are no numbers of the form $a + b\sqrt{-5}$ with norm 3 or 7. So in a similar fashion to the argument above, if $\alpha\beta = 1 \pm 2\sqrt{-5}$, then $N(\alpha\beta) = N(\alpha)N(\beta) = N(1 \pm 2\sqrt{-5}) = 21$. And there are no numbers with norm 3 or 7, so one of α and β has norm 21 and the other has norm 1. Hence, $1 \pm 2\sqrt{-5}$ is also prime.

23. The product of $4k + 1$ and $4l + 1$ is $(4k + 1)(4l + 1) = 16kl + 4k + 4l + 1 = 4(4kl + k + l) + 1 = 4m + 1$, where $m = 4kl + k + l$. Hence, the product of two integers of the form $4k + 1$ is also of this form.

25. We proceed by strong mathematical induction on the elements of H. The first Hilbert number greater than 1—5—is a Hilbert prime because it is an integer prime. This completes the basis step.

For the inductive step, we assume that all numbers in H less than or equal to n can be factored into Hilbert primes. The next greatest number in H is $n+4$. If $n+4$ is a Hilbert prime, then we are done. Otherwise, $n+4=hk$, where h and k are less than $n+4$ and in H, and so both are less than or equal to n. By the inductive hypothesis, h and k can be factored into Hilbert primes. Thus, $n+4$ can be written as the product of Hilbert primes.

27. 1, 2, 3, 4, 6, 8, 12, 24

29. **a.** 77 **b.** 36 **c.** 150 **d.** 33,633 **e.** 605,605 **f.** 277,200

31. **a.** $2^2 3^3 5^3 7^2$, $2^7 3^5 5^5 7^7$ **b.** $1, 2\cdot 3\cdot 5\cdot 7\cdot 11\cdot 13\cdot 17\cdot 19\cdot 23\cdot 29$
c. $2\cdot 5\cdot 11$, $2^3\cdot 3\cdot 5^7\cdot 7\cdot 11^{13}\cdot 13$ **d.** 101^{1000}, $41^{11}47^{11}79^{111}83^{111}101^{1001}$

33. the year 2121

35. Let $a=p_1^{r_1}p_2^{r_2}\cdots p_k^{r_k}$ and $b=p_1^{s_1}p_2^{s_2}\cdots p_k^{s_k}$, where p_i is a prime and r_i and s_i are nonnegative. $(a,b)=p_1^{\min(r_1,s_1)}\cdots p_k^{\min(r_k,s_k)}$ and $[a,b]=p_1^{\max(r_1,s_1)}\cdots p_k^{\max(r_k,s_k)}$. So $[a,b]=(a,b)p_1^{\max(r_1,s_1)-\min(r_1,s_1)}\cdots p_k^{\max(r_k,s_k)-\min(r_k,s_k)}$. Because $\max(r_i,s_i)-\min(r_i,s_i)$ is clearly nonnegative, we now see that $(a,b)\mid[a,b]$, and we have equality when $\max(r_i,s_i)-\min(r_i,s_i)=0$ for each i, that is, if $r_i=s_i$ for each i, that is if $a=b$.

37. **a.** If $[a,b]\mid c$, then because $a\mid[a,b]$, $a\mid c$. Similarly, $b\mid c$. Conversely, suppose that $a=p_1^{a_1}p_2^{a_2}\cdots p_n^{a_n}$ and $b=p_1^{b_1}p_2^{b_2}\cdots p_n^{b_n}$ and $c=p_1^{c_1}p_2^{c_2}\cdots p_n^{c_n}$. If $a|c$ and $b|c$, then $\max(a_i,b_i)\le c_i$ for $i=1,2,\ldots,n$. Hence, $[a,b]\mid c$. **b.** We proceed by induction on n. The basis step is given by part (a). Suppose the result holds for sets of $n-1$ integers. Then $[a_1,\ldots,a_n]\mid d$ if and only if $[[a_1,\ldots,a_{n-1}],a_n]\mid d$. (See Exercise 49.) This is true if and only if $[a_1,\ldots,a_{n-1}]\mid d$ and $a_n\mid d$ by part (a). By the induction hypothesis, this is true if and only if $a_i\mid d$ for $i=1,2,\ldots,n$. This completes the induction step.

39. Assume that $p\mid a^n=\pm\mid a\mid\cdot\mid a\mid\cdots\mid a\mid$. Then by Lemma 3.5, $p\mid\mid a\mid$ and so $p\mid a$.

41. **a.** Suppose that $(a,b)=1$ and $p\mid(a^n,b^n)$ where p is a prime. It follows that $p\mid a^n$ and $p\mid b^n$. By Exercise 41, $p\mid a$ and $p\mid b$. But then $p\mid(a,b)=1$, which is a contradiction. **b.** Suppose that a does not divide b, but $a^n\mid b^n$. Then there is some prime power, say, p^r, that divides a but does not divide b (or else $a\mid b$ by the fundamental theorem of arithmetic). Thus, $a=p^rQ$, where Q is an integer. Now $a^n=(p^rQ)^n=p^{rn}Q^n$, so $p^{rn}\mid a^n\mid b^n$. Then $b^n=mp^{rn}$, from which it follows that each of the n b's must by symmetry contain r p's. But this is a contradiction.

43. Suppose that $x=\sqrt{2}+\sqrt{3}$. Then $x^2=2+2\sqrt{2}\sqrt{3}+3=5+2\sqrt{6}$. Hence, $x^2-5=2\sqrt{6}$. It follows that $x^4-10x^2+25=24$. Consequently, $x^4-10x^2+1=0$. By Theorem 3.17, it follows that $\sqrt{2}+\sqrt{3}$ is irrational, because it is not an integer (we can see this because $3<\sqrt{2}+\sqrt{3}<4$).

45. Suppose that $m/n=\log_p b$. This implies that $p^{\frac{m}{n}}=b$, from which it follows that $p^m=b^n$. Because b is not a power of p, there must be another prime, say, q, such that $q\mid b$. But then $q\mid b\mid b^n=p^m=p\cdot p\cdots p$. By Lemma 2.4, $q\mid p$, which is impossible because p is a prime number.

47. Let $a=p_1^{r_1}p_2^{r_2}\cdots p_k^{r_k}$, $b=p_1^{s_1}p_2^{s_2}\cdots p_k^{s_k}$, and $c=p_1^{t_1}p_2^{t_2}\cdots p_k^{t_k}$, with p_i prime and r_i, s_i, and t_i nonnegative. Observe that $\min(x,\max(y,z))=\max(\min(x,y),\min(x,z))$. We also know that $[a,b]=p_1^{\max(r_1,s_1)}p_2^{\max(r_2,s_2)}\cdots p_k^{\max(r_k,s_k)}$, and so $([a,b],c)=p_1^{\min(t_1,\max(r_1,s_1))}p_2^{\min(t_2,\max(r_2,s_2))}\cdots p_k^{\min(t_k,\max(r_k,s_k))}$. We also know that $(a,c)=p_1^{\min(r_1,t_1)}p_2^{\min(r_2,t_2)}\cdots p_k^{\min(r_k,t_k)}$ and $(b,c)=p_1^{\min(s_1,t_1)}p_2^{\min(s_2,t_2)}\cdots p_k^{\min(s_k,t_k)}$. Then $[(a,c),(b,c)]=p_1^{\max(\min(r_1,t_1),\min(s_1,t_1))}p_2^{\max(\min(r_2,t_2),\min(s_2,t_2))}\cdots p_k^{\max(\min(r_k,t_k),\min(s_k,t_k))}$. Therefore, $([a,b],c)=[(a,c),(b,c)]$. In a similar manner, noting that $\min(\max(x,z),\max(y,z))=\max(\min(x,y),z)$, we find that $[(a,b),c]=([a,c],[b,c])$.

49. Let $c = [a_1, \ldots, a_n]$, $d = [[a_1, \ldots, a_{n-1}], a_n]$, and $e = [a_1, \ldots, a_{n-1}]$. If $c \mid m$, then all a_i's divide m, and hence $e \mid m$ and $a_n \mid m$, so $d \mid m$. Conversely, if $d \mid m$, then $e \mid m$ and $a_n \mid m$, and so all a_i's divide m; thus $c \mid m$. Because c and d divide all the same numbers, they must be equal.

51. **a.** There are six cases, all handled the same way. So without loss of generality, suppose that $a \le b \le c$. Then $\max(a, b, c) = c$, $\min(a, b) = a$, $\min(a, c) = a$, $\min(b, c) = b$, and $\min(a, b, c) = a$. Hence, $c = \max(a, b, c) = a + b + c - \min(a, b) - \min(a, c) - \min(b, c) + \min(a, b, c) = a + b + c - a - a - b + a$. **b.** The power of a prime p that occurs in the prime factorization of $[a, b, c]$ is $\max(a, b, c)$ where a, b, and c are the powers of this prime in the factorizations of a, b, and c, respectively. Also, $a + b + c$ is the power of p in abc, $\min(a, b)$ is the power of p in (a, b), $\min(a, c)$ is the power of p in (a, c), $\min(b, c)$ is the power of p in (b, c), and $\min(a, b, c)$ is the power of p in (a, b, c). It follows that $a + b + c - \min(a, b) - \min(a, c) - \min(b, c)$ is the power of p in $abc(a, b, c)/((a, b)(a, c)(b, c))$. Hence, $[a, b, c] = abc(a, b, c)/((a, b)(a, c)(b, c))$.

53. Let $a = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$, $b = p_1^{s_1} p_2^{s_2} \cdots p_k^{s_k}$, and $c = p_1^{t_1} p_2^{t_2} \cdots p_k^{t_k}$, with p_i prime and r_i, s_i, and t_i nonnegative. Then $p_i^{r_i+s_i+t_i} \parallel abc$, but $p_i^{\min(r_i,s_i,t_i)} \parallel (a, b, c)$ and $p_i^{r_i+s_i+t_i-\min(r_i,s_i,t_i)} \parallel [ab, ac, ab]$, and $p_i^{\min(r_i,s_i,t_i)} \cdot p_i^{r_i+s_i+t_i-\min(r_i,s_i,t_i)} = p_i^{r_i+s_i+t_i}$.

55. Let $a = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$, $b = p_1^{s_1} p_2^{s_2} \cdots p_k^{s_k}$, and $c = p_1^{t_1} p_2^{t_2} \cdots p_k^{t_k}$, with p_i prime and r_i, s_i, and t_i nonnegative. Then, using that $(a, b, c) = p_1^{\min(r_1,s_1,t_1)} p_2^{\min(r_2,s_2,t_2)} \cdots p_k^{\min(r_k,s_k,t_k)}$, and $[a, b, c] = p_1^{\max(r_1,s_1,t_1)} p_2^{\max(r_2,s_2,t_2)} \cdots p_k^{\max(r_k,s_k,t_k)}$, we can write the prime factorization of $([a, b], [a, c], [b, c])$ and $[(a, b), (a, c), (b, c)]$. For instance, consider the case where $k = 1$. Then $([a, b], [a, c], [b, c]) = (p_1^{\max(r_1,s_1)}, p_1^{\max(r_1,t_1)}, p_1^{\max(s_1,t_1)}) = p_1^{\min(\max(r_1,s_1),\max(r_1,t_1),\max(s_1,t_1)}$. Similarly, $[(a, b), (a, c), (b, c)] = p_1^{\max(\min(r_1,s_1),\min(r_1,t_1),\min(s_1,t_1)}$. Clearly, these two are equal (examine the six orderings $r_1 \ge s_1 \ge t_1, \ldots$).

57. First note that there are arbitrarily long sequences of composites in the integers. For example, $(n + 2)! + 2$, $(n + 2)! + 3$, $\ldots$, $(n + 2)! + (n + 2)$ is a sequence of n consecutive composites. To find a sequence of n composites in the sequence a, $a + b$, $a + 2b$, $\ldots$, look at the integers in a, $a + b$, $a + 2b$, $\ldots$ with absolute values between $(nb + 2)! + 2$ and $(nb + 2)! + (nb + 2)$. There are clearly n or $n + 1$ such integers, and all are composite.

59. 103

61. 701

63. Let $a = \prod_{i=1}^{s} p_i^{\alpha_i}$ and $b = \prod_{i=1}^{t} p_i^{\beta_i}$. The condition $(a, b) = 1$ is equivalent to $\min(\alpha_i, \beta_i) = 0$ for all i, and the condition $ab = c^n$ is equivalent to $n \mid (\alpha_i + \beta_i)$ for all i. Hence, $n \mid \alpha_i$ and $\beta_i = 0$ or $n \mid \beta_i$ and $\alpha_i = 0$. Let d be the product of $p_i^{\alpha_i/n}$ over all i of the first kind, and let e be the product of $p_i^{\beta_i/n}$ over all i of the second kind. Then $d^n = a$ and $e^n = b$.

65. Suppose the contrary and that $a \le n$ is in the set. Then $2a$ cannot be in the set. Thus, if there are k elements in the set not exceeding n, then there are k integers between $n + 1$ and $2n$ that cannot be in the set. So there are at most $k + (n - k) = n$ elements in the set.

67. $m = n$ or $\{m, n\} = \{2, 4\}$

69. For $j \ne i$, $p_i | Q_j$, because it is one of the factors. So p_i must divide $S - \sum_{j \ne i} Q_j = Q_i = p_1 \cdots p_{i-1} p_{i+1} \cdots p_r$, but by the fundamental theorem of arithmetic, p_i must be equal to one of these last factors, a contradiction.

71. Let p be the largest prime less than or equal to n. If $2p$ were less than or equal to n, then Bertrand's postulate would guarantee another prime q such that $p < q < 2p \le n$, contradicting the choice of p. Therefore, we know that $n < 2p$. Therefore, in the product $n! = 1 \cdot 2 \cdot 3 \cdots n$, there appears

only one multiple of p, namely, p itself, and so in the prime factorization of n, p appears with exponent 1.

73. **a.** Uniqueness follows from the Fundamental Theorem. If a prime p_i doesn't appear in the prime factorization, then we include it in the product with an exponent of 0. Because $e_i \geq 0$, we have $p_1^{e_1} = p_1^{e_1} p_2^0 \cdots p_r^0 \leq p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r} = m$. **b.** Because $p_1^{e_i} < p_i^{e_i} \leq m \leq Q = p_r^n$, we take logs of both sides to get $e_i \log p_1 \leq n \log p_r$. Solving for e_i gives the first inequality. If $1 \leq m \leq Q$, then m has a prime-power factorization of the form given in part (a), so the r-tuples of exponents count the number of integers in the range $1 \leq m \leq Q$. **c.** To bound the number of r-tuples, by part (b) there are at most $Cn + 1$ choices for each e_i, and therefore there are at most $(Cn + 1)^r$ r-tuples, which by part (b) gives us $p_r^n \leq (Cn + 1)^r = (n(C + 1/n))^r \leq n^r (C + 1)^r$. **d.** Taking logs of both sides of the inequality in part (c) and solving for n yields $n \leq (r \log n + \log(C + 1))/ \log p_r$, but because n grows much faster than $\log n$, the left side must be larger than the right for large values of n. This contradiction shows there must be infinitely many primes.

75. $S(40) = 5$, $S(41) = 41$, $S(43) = 43$

77. $a(n) = 1, 2, 3, 4, 5, 9, 7, 32, 27, 25, 11, \ldots$

79. From Exercise 78, we have $S(p) = p$ whenever p is prime. If $m < p$ and $m | S(p)! = p!$, then $m | (p - 1)!$, so $S(p)$ must be the first time that $S(n)$ takes on the value p. Therefore, of all the inverses of p, p is the least.

81. Let n be a positive integer and suppose n is square-free. Then no prime can appear to a power greater than 1 in the prime-power factorization of n. So $n = p_1 p_2 \cdots p_r$ for some distinct primes p_i. Then $rad(n) = p_1 p_2 \cdots p_r = n$. Conversely, if n is not square-free, then some prime factor p_1 appears to a power greater than 1 in the prime-power factorization of n. So $n = p_1^a p_2^{b_2} \cdots p_r^{b_r}$ with $a \geq 2$. Then $rad(n) = p_1 p_2 \cdots p_r < n$.

83. Because every prime occurring in the prime-power factorization of mn occurs in either the factorization of m or n, every factor in $\text{rad}(mn)$ occurs at least once in the product $\text{rad}(m)\text{rad}(n)$, which gives us the inequality. If $m = p_1^{a_1} \cdots p_r^{a_r}$ and $n = q_1^{b_1} \cdots q_s^{b_s}$ are relatively prime, then we have $\text{rad}(mn) = p_1 \cdots p_r q_1 \cdots q_s = \text{rad}(m)\text{rad}(n)$.

85. First note that if $p \mid \binom{2n}{n}$, then $p \leq 2n$. This is true because every factor of the numerator of $\binom{2n}{n} = \frac{(2n)!}{(n!)^2}$ is less than or equal to $2n$. Let $\binom{2n}{n} = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$ be the factorization of $\binom{2n}{n}$ into distinct primes. By the definition of π, $k \leq \pi(2n)$. By Exercise 84, $p_i^{r_i} \leq 2n$. It now follows that $\binom{2n}{n} = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k} \leq (2n)(2n) \cdots (2n) \leq (2n)^{\pi(2n)}$.

87. Note that $\binom{2n}{n} \leq \sum_{a=0}^{2n} \binom{2n}{a} = (1 + 1)^{2n} = 2^{2n}$. Then from Exercise 86, $n^{\pi(2n) - \pi(n)} < \binom{2n}{n} \leq 2^{2n}$. Taking logarithms gives $(\pi(2n) - \pi(n)) \log n < \log(2^{2n}) = n \log 4$. Now divide by $\log n$.

89. Note that $2^n = \prod_{a=1}^{n} 2 \leq \prod_{a=1}^{n} (n + a)/a = \binom{2n}{n}$. Then by Exercise 85, $2^n \leq (2n)^{\pi(2n)}$. Taking logs gives $\pi(2n) \geq n \log 2/ \log 2n$. Hence, for a real number x, we have $\pi(x) \geq \left[x/2\right] \log 2/ \log [x] > c_1 x/ \log x$. For the other half, Exercise 65 gives $\pi(x) - \pi(x/2) < ax/ \log x$, where a is a constant. Then $\log x/2^m \pi(x/2^m) - \log x/2^{m+1} \pi(x/2^{m+1}) < ax/2^m$ for any positive integer m. Then $\log x \pi(x) = \sum_{m=0}^{v} \left(\log x/2^m \pi(x/2^m) - \log x/2^{m+1} \pi(x/2^{m+1})\right) < ax \sum_{m=0}^{v} 1/2^m < c_2 x$, where v is the largest integer such that $2^{v+1} \leq x$. Then $\pi(x) < c_2 x/\log x$.

Section 3.6

1. **a.** $3 \cdot 5^2 \cdot 7^3 \cdot 13 \cdot 101$ **b.** $11^3 \cdot 13 \cdot 19 \cdot 641$ **c.** $13 \cdot 17 \cdot 19 \cdot 47 \cdot 71 \cdot 97$

3. **a.** $143 = 12^2 - 1 = (12 + 1)(12 - 1) = 13 \cdot 11$ **b.** $2279 = 48^2 - 5^2 = (48 + 5)(48 - 5) = 53 \cdot 43$
c. 43 is prime. **d.** $11413 = 107^2 - 6^2 = (107 + 6)(107 - 6) = 113 \cdot 101$

5. Note that $(50+n)^2 = 2500 + 100n + n^2$ and $(50-n)^2 = 2500 - 100n + n^2$. The first equation shows that the possible final two digits of squares can be found by examining the squares of the integers 0, 1, . . . , 49, and the second equation shows that these final two digits can be found by examining the squares of the integers 0, 1, . . . , 25. We find that $0^2 = 0$, $1^2 = 1$, $2^2 = 4$, $3^2 = 9$, $4^2 = 16$, $5^2 = 25$, $6^2 = 36$, $7^2 = 49$, $8^2 = 64$, $9^2 = 81$, $10^2 = 100$, $11^2 = 121$, $12^2 = 144$, $13^2 = 169$, $14^2 = 196$, $15^2 = 225$, $16^2 = 256$, $17^2 = 289$, $18^2 = 324$, $19^2 = 361$, $20^2 = 400$, $21^2 = 441$, $22^2 = 484$, $23^2 = 529$, $24^2 = 576$, and $25^2 = 625$. It follows that the last two digits of a square are 00, $e1$, $e4$, 25, $o6$, and $e9$, where e represents an even digit and o represents an odd digit.

7. Suppose that $x^2 - n$ is a perfect square with $x > (n+p^2)/2p$, say, a^2. Now, $a^2 = x^2 - n > ((n+p^2)/2p)^2 - n = ((n-p^2)/2p)^2$. It follows that $a > (n-p^2)/2p$. From these inequalities for x and a, we see that $x + a > n/p$, or $n < p(x+a)$. Also, $a^2 = x^2 - n$ tells us that $(x-a)(x+a) = n$. Now, $(x-a)(x+a) = n < p(x+a)$. Canceling, we find that $x - a < p$. But because $x - a$ is a divisor of n less than p, the smallest prime divisor of n, it follows that $x - a = 1$. In this case, $x = (n+1)/2$.

9. From the identity in Exercise 8, it is clear that if $n = n_1$ is a multiple of $2k+1$, then so is n_k, because it is the sum of two multiples of $2k+1$. If $(2k+1) \mid n_k$, then $(2k+1) \mid r_k$ and it follows from $r_k < 2k+1$ that $r_k = 0$. Thus, $n_k = (2k+1)q_k$. Continuing, we see that $n = n + 2n_k - 2(2k+1)q_k = (2k+1)n + 2(n_k - kn) - 2(2k+1)q_k$. It follows from Exercise 8 that $n = (2k+1)n - 2(2k+1)\sum_{i=1}^{k-1} q_i - 2(2k+1)q_k = (2k+1)n - 2(2k+1)\sum_{i=1}^{k} q_i$. Using Exercise 8 again, we conclude that $n = (2k+1)(n - 2\sum_{i=1}^{k} q_i) = (2k+1)m_{k+1}$.

11. To see that u is even, note that $a - c$ is the difference of odd numbers and that $b - d$ is the difference of even numbers. Thus, $a - c$ and $b - d$ are even, and u must be as well. That $(r, s) = 1$ follows trivially from Theorem 2.1 (i). To continue, $a^2 + b^2 = c^2 + d^2$ implies that $(a+c)(a-c) = (d-b)(d+b)$. Dividing both sides of this equation by u, we find that $r(a+c) = s(d+b)$. From this, it is clear that $s \mid r(a+c)$. But because $(r, s) = 1$, $s \mid a + c$.

13. To factor n, observe that $[(\frac{u}{2})^2 + (\frac{v}{2})^2](r^2 + s^2) = (1/4)(r^2u^2 + r^2v^2 + s^2u^2 + s^2v^2)$. Substituting $a - c$, $d - b$, $a + c$, and $d + b$ for ru, su, sv, and rv, respectively, will allow everything to be simplified down to n. As u and v are both even, both of the factors are integers.

15. We have $2^{4n+2} + 1 = 4(2^n)^4 + 1 = (2 \cdot 2^{2n} + 2 \cdot 2^n + 1)(2 \cdot 2^{2n} - 2 \cdot 2^n + 1)$. Using this identity, we have the factorization $2^{18} + 1 = 4(2^4)^4 + 1 = (2 \cdot 2^8 + 2 \cdot 2^4 + 1)(2 \cdot 2^8 - 2 \cdot 2^4 + 1) = (2^9 + 2^5 + 1)(2^9 - 2^5 + 1) = 545 \cdot 481$.

17. We can prove that the last digit in the decimal expansion of F_n is 7 for $n \geq 2$ by proving that the last digit in the decimal expansion of 2^{2^n} is 6 for $n \geq 2$. This can be done using mathematical induction. We have $2^{2^2} = 16$, so the result is true for $n = 2$. Now assume that the last decimal digit of 2^{2^n} is 6, that is, $2^{2^n} \equiv 6 \pmod{10}$. It follows that $2^{2^{n+1}} = (2^{2^n})^{2^{n+1}-2^n} \equiv 6^{2^{n+1}-2^n} \equiv 6 \pmod{10}$. This completes the proof.

19. Because every prime factor of $F_5 = 2^{2^5} + 1 = 4{,}294{,}967{,}297$ is of the form $2^7k + 1 = 128k + 1$, attempt to factor F_5 by trial division by primes of this form. We find that $128 \cdot 1 + 1 = 129$ is not prime, $128 \cdot 2 + 1 = 257$ is prime but does not divide 4,294,967,297, $128 \cdot 3 + 1 = 385$ is not prime, $128 \cdot 4 + 1 = 513$ is not prime, and $128 \cdot 5 + 1 = 641$ is prime and does divide 4,294,967,297 with $4{,}294{,}967{,}297 = 641 \cdot 6{,}700{,}417$. Any factor of 6,700,417 is also a factor of 4,294,967,297. We attempt to factor 6,700,417 by trial division by primes of the form $128k + 1$ beginning with 641. We first note that 641 does not divide 6,700,417. Among the other integers of the form $128k + 1$ less than $\sqrt{6{,}700{,}417}$, namely the integers 769, 897, 1025, 1153, 1281, 1409, 1537, 1665, 1793, 1921, 2049, 2177, 2305, 2433, and 2561, only 769, 1153, and 1409 are prime, and none of them divide 6,700,417. Hence, 6,700,417 is prime and the prime factorization of F_5 is $641 \cdot 6{,}700{,}417$.

21. $2^n / \log_2 10 + 1$

23. See Exercise 23 in Section 3.2.

Section 3.7

1. **a.** $x = 33 - 5t,\ y = -11 + 2t$ **b.** $x = -300 + 13t,\ y = 400 - 17t$ **c.** $x = 21 - 2t,\ y = -21 + 3t$ **d.** no solutions **e.** $x = 889 - 1969t,\ y = -633 + 1402t$

3. 63 US$, 41 Can$

5. 53 Euros, 35 Pounds

7. 17 apples, 23 oranges

9. **a.** (1, 16), (4, 14), (7, 12), . . . , (22, 2), (25, 0) **b.** no solutions
c. 18 solutions: (0, 37), (3, 35), . . . , (54, 1)

11. **a.** $x = -5 + 3s - 2t,\ y = 5 - 2s,\ z = t$ **b.** no solutions **c.** $x = -1 + 102s + t,\ y = 1 - 101s - 2t,\ z = t$

13. Let x, y, and z be the number of pennies, dimes, and quarters, respectively. When $z = 0$, we have $x = 9,\ y = 9; x = 19,\ y = 8; x = 29,\ y = 7; x = 39,\ y = 6; x = 49,\ y = 5; x = 59,\ y = 4; x = 69,\ y = 3; x = 79,\ y = 2; x = 89,\ y = 1; x = 99,\ y = 0$. When $z = 1$, we have $x = 4,\ y = 7; x = 14,\ y = 6; x = 24,\ y = 5; x = 34,\ y = 4; x = 44,\ y = 3; x = 54,\ y = 2; x = 64,\ y = 1; x = 74,\ y = 0$. When $z = 2$, we have $x = 9,\ y = 4; x = 19,\ y = 3; x = 29,\ y = 2; x = 39,\ y = 1; x = 49,\ y = 0$. When $z = 3$, we have $x = 4,\ y = 2; x = 14,\ y = 1; x = 24,\ y = 0$.

15. **a.** $x = 92 + 6t,\ y = 8 - 7t,\ z = t$ **b.** no solution **c.** $x = 50 - t,\ y = -100 + 3t,\ z = 150 - 3t,\ w = t$

17. 9, 19, 41

19. The quadrilateral with vertices $(b, 0)$, $(0, a)$, $(b - 1, -1)$, and $(-1, a - 1)$ has area $a + b$. Pick's Theorem, from elementary geometry, states that the area of a simple polygon whose vertices are lattice points (points with integer coordinates) is given by $\frac{1}{2}x + y - 1$, where x is the number of lattice points on the boundary and y is the number of lattice points inside the polygon. Because $(a, b) = 1$, $x = 4$, and therefore, by Pick's Theorem, the quadrilateral contains $a + b - 1$ lattice points. Every point corresponds to a different value of n in the range $ab - a - b < n < ab$. Therefore, every n in the range must get hit, so the equation is solvable.

21. See the solution to Exercise 19. The line $ax + by = ab - a - b$ bisects the rectangle with vertices $(-1, a - 1)$, $(-1, -1)$, $(b - 1, a - 1)$, and $(b - 1, -1)$ but contains no lattice points. Hence, half the interior points are below the line and half are above. The half below correspond to $n < ab - a - b$ and there are $(a - 1)(b - 1)/2$ of them.

23. (0, 25, 75); (4, 18, 78); (8, 11, 81); (12, 4, 84)

Section 4.1

1. **a.** $2 \mid (13 - 1) = 12$ **b.** $5 \mid (22 - 7) = 15$ **c.** $13 \mid (91 - 0) = 91$ **d.** $7 \mid (69 - 62) = 7$ **e.** $3 \mid (-2 - 1) = -3$ **f.** $11 \mid (-3 - 30) = -33$ **g.** $40 \mid (111 - (-9)) = 120$ **h.** $37 \mid (666 - 0) = 666$

3. **a.** 1, 2, 11, 22 **b.** 1, 3, 9, 27, 37, 111, 333, 999 **c.** 1, 11, 121, 1331

5. Suppose that a is odd. Then $a = 2k + 1$ for some integer k. Then $a^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 4k(k + 1) + 1$. If k is even, then $k = 2l$ where l is an integer. Then $a^2 = 8l(2l + 1) + 1$. Hence, $a^2 \equiv 1 \pmod 8$. If k is odd, then $k = 2l + 1$ when l is an integer. Then $a^2 = 4(2l + 1)(2l + 2) + 1 = 8(2l + 1)(l + 1) + 1$. Hence, $a^2 \equiv 1 \pmod 8$. It follows that $a^2 \equiv 1 \pmod 8$ whenever a is odd.

7. **a.** 15 **b.** 8 **c.** 25 **d.** 27 **e.** 8 **f.** 27

9. **a.** 1 **b.** 5 **c.** 9 **d.** 13

11. By the Division Algorithm, there exist integers q_1, q_2, r_1, r_2 such that $a = q_1m + r_1$ and $b = q_2m + r_2$, with $0 \le r_1, r_2 < m$. Then $a \bmod m = r_1$ and $b \bmod m = r_2$. Suppose that $r_1 = r_2$; then $a - b = m(q_1 - q_2) + (r_1 - r_2) = m(q_1 - q_1)$. Then $m|a - b$, and so $a \equiv b \pmod m$.

13. Because $a \equiv b \pmod m$, there exists an integer k such that $a = b + km$. Thus, $ac = (b + km)c = bc + k(mc)$. By Theorem 4.1, $ac \equiv bc \pmod{mc}$.

15. **a.** We proceed by induction on n. It is clearly true for $n = 1$. For the inductive step, we assume that $\sum_{j=1}^{n} a_j \equiv \sum_{j=1}^{n} b_j \pmod m$ and that $a_{n+1} \equiv b_{n+1} \pmod m$. Now $\sum_{j=1}^{n+1} a_j = (\sum_{j=1}^{n} a_j) + a_{n+1} \equiv (\sum_{j=1}^{n} b_j) + b_{n+1} = \sum_{j=1}^{n+1} b_j \pmod m$ by Theorem 4.6(i). This completes the proof. **b.** We use induction on n. For $n = 1$, the identity clearly holds. This completes the basis step. For the inductive step, we assume that $\prod_{j=1}^{n} a_j \equiv \prod_{j=1}^{n} b_j \pmod m$ and $a_{n+1} \equiv b_{n+1} \pmod m$. Then $\prod_{j=1}^{n+1} a_j = a_{n+1}(\prod_{j=1}^{n} a_j) \equiv b_{n+1}(\prod_{j=1}^{n} b_j) = \prod_{j=1}^{n+1} b_j \pmod m$ by Theorem 4.6(iii). This completes the proof.

17. Let $m = 6$, $a = 4$, and $b = 5$. Then $4 \bmod 6 = 4$ and $5 \bmod 6 = 5$, but $4 \cdot 5 \bmod 6 = 2 \ne 4 \cdot 5$.

19. By the Division Algorithm, there exist integers q_1, q_2, r_1, r_2 such that $a = q_1m + r_1$ and $b = q_2m + r_2$, with $0 \le r_1, r_2 < m$. Then $ab \equiv r_1r_2 \pmod m$ by Theorem 4.6(iii). By definition, $a \bmod m = r_1$ and $b \bmod m = r_2$, so $((a \bmod m)(b \bmod m) \bmod m = (r_1r_2) \bmod m = ab \bmod m$, by Exercise 10.

21.

$-$	0	1	2	3	4	5
0	0	5	4	3	2	1
1	1	0	5	4	3	2
2	2	1	0	5	4	3
3	3	2	1	0	5	4
4	4	3	2	1	0	5
5	5	4	3	2	1	0

23. **a.** 4 o'clock **b.** 6 o'clock **c.** 4 o'clock

25. $a \equiv \pm b \pmod p$

27. Note that $1 + 2 + 3 + \cdots + (n + 1) = (n - 1)n/2$. If n is odd, then $(n - 1)$ is even, so $(n - 1)n/2$ is an integer. Hence, $n \mid (1 + 2 + 3 + \cdots + (n - 1))$ if n is odd, and $1 + 2 + 3 + \cdots + (n - 1) \equiv 0 \pmod n$. If n is even, then $n = 2k$ where k is an integer. Then $(n - 1)n/2 = (n - 1)k$. We can easily see that n does not divide $(n - 1)k$, because $(n, n - 1) = 1$ and $k < n$. It follows that $1 + 2 + \cdots + (n - 1)$ is not congruent to 0 modulo n if n is even.

29. those n relatively prime to 6

31. If $n = 1$, then $5 = 5^1 = 1 + 4(1) \pmod{16}$, so the basis step holds. For the inductive step, we assume that $5^n = 1 + 4n \pmod{16}$. Now $5^{n+1} \equiv 5^n 5 \equiv (1 + 4n)5 \pmod{16}$ by Theorem 4.4(iii). Further, $(1 + 4n)5 \equiv 5 + 20n \equiv 5 + 4n \pmod{16}$. Finally, $5 + 4n = 1 + 4(n + 1)$. So $5^{n+1} \equiv 1 + 4(n + 1) \pmod{16}$.

33. Note that if $x \equiv 0 \pmod 4$ then $x^2 \equiv 0 \pmod 4$, if $x \equiv 1 \pmod 4$ then $x^2 \equiv 1 \pmod 4$, if $x \equiv 2 \pmod 4$ then $x^2 \equiv 4 \equiv 0 \pmod 4$, and if $x \equiv 3 \pmod 4$ then $x^2 \equiv 9 \equiv 1 \pmod 4$. Hence, $x^2 \equiv 0$ or $1 \pmod 4$ whenever x is an integer. It follows that $x^2 + y^2 \equiv 0$, 1 or $2 \pmod 4$ whenever x and y are integers. We see that n is not the sum of two squares when $n \equiv 3 \pmod 4$.

35. By Theorem 4.1, for some integer a, $ap^k = x^2 - x = x(x - 1)$. By the fundamental theorem of arithmetic, p^k is a factor of $x(x - 1)$. Because p cannot divide both x and $x - 1$, we know that $p^k \mid x$ or $p^k \mid x - 1$. Thus, $x \equiv 0$ or $x \equiv 1 \pmod{p^k}$.

37. First note that there are m_1 possibilities for a_1, m_2 possibilities for a_2, and in general m_i possibilities for a_i. Thus, there are $m_1 m_2 \cdots m_k$ expressions of the form $M_1 a_1 + M_2 a_2 + \cdots M_k a_k$ where $a_1, a_2, \ldots, a_k$ run through complete systems of residues modulo $m_1, m_2, \ldots, m_k$, respectively. Because this is exactly the size of a complete system of residues modulo M, the result will follow if we can show distinctness of each of these expressions modulo M. Suppose that $M_1 a_1 + M_2 a_2 + \cdots + M_k a_k \equiv M_1 a_1' + M_2 a_2' + \cdots + M_k a_k' \pmod{M}$. Then $M_1 a_1 \equiv M_1 a_1' \pmod{m_1}$, because m_1 divides each of $M_2, M_3, \ldots, M_k$, and, further, $a_1 \equiv a_1' \pmod{m_1}$, because $(M_1, m_1) = 1$. Similarly, $a_i \equiv a_i' \pmod{m_i}$. Thus, a_i' is in the same congruence class modulo m_i as a_i for all i. The result now follows.

39. **a.** Let $\sqrt{n} = a + r$, where a is an integer and $0 \le r < 1$. We now consider two cases, when $0 \le r < \frac{1}{2}$ and when $\frac{1}{2} \le r < 1$. For the first case, $T = [\sqrt{n} + \frac{1}{2}] = a$, and so $t = T^2 - n = -(2ar + r^2)$. Thus, $|t| = 2ar + r^2 < 2a(\frac{1}{2}) + (\frac{1}{2})^2 = a + \frac{1}{4}$. Because both T and n are integers, t is also an integer. It follows that $|t| \le [a + \frac{1}{4}] = a = T$. For the second case, when $\frac{1}{2} \le r < 1$, we find that $T = [\sqrt{n} + \frac{1}{2}] = a + 1$ and $t = 2a(1 - r) + (1 - r^2)$. Because $\frac{1}{2} \le r < 1$, $0 < (1 - r) \le \frac{1}{2}$ and $0 < 1 - r^2 < 1$. It follows that $t \le 2a(\frac{1}{2}) + (1 - r^2)$. Because t is an integer, we can say that $|t| \le [a + (1 - r^2)] = a < T$. **b.** By the division algorithm, we see that if we divide x by T, we get $x = aT + b$, where $0 \le b < T$. If a were negative, then $x = aT + b \le (-1)T + b < 0$; but we assumed x to be nonnegative. This shows that $0 \le a$. Suppose now that $a > T$. Then $x = aT + b \ge (T + 1)T = T^2 + T \ge (\sqrt{n} - \frac{1}{2})^2 + (\sqrt{n} - \frac{1}{2}) = n - \frac{1}{4}$ and, as x and n are integers, $x \ge n$. This is a contradiction, which shows that $a \le T$. Similarly, $0 \le c \le T$ and $0 \le d < T$. **c.** $xy = (aT + b)(cT + d) = acT^2 + (ad + bc)T + bd \equiv ac(t + n) + zT + bd \equiv act + zT + bd \pmod{n}$. **d.** Use part (c), substituting $eT + f$ for ac. **e.** The first half is identical to part (b); the second half follows by substituting $gT + h$ for $z + et$ in part (c) and noting that $T^2 \equiv t \pmod{n}$. **f.** Certainly, ft and gt can be computed because all three numbers are less than T, which is less than $\sqrt{n} + 1$. So $(f + g)t$ is less than $2n < w$. Similarly, we can compute $j + bd$ without exceeding the word size. And, finally, using the same arguments, we can compute $hT + k$ without exceeding the word size.

41. **a.** 1 **b.** 1 **c.** 1 **d.** 1 **e.** Fermat's little theorem (Section 6.1)

43. Because $f_{n-2} + f_{n-1} \equiv f_n \pmod{m}$, if two consecutive numbers recur in the same order, then the sequence must be repeating both as n increases and as it decreases. But there are only m residues, and so m^2 ordered sequence of two residues. As the sequence is infinite, some two elements of the sequence must recur by the pigeonhole principle. Thus, the sequence of least positive residues of the Fibonacci numbers repeats. It follows that if m divides some Fibonacci number, that is, if $f_n \equiv 0 \pmod{m}$, then m divides infinitely many Fibonacci numbers. To see that m does divide some Fibonacci number, note that the sequence must contain a 0, namely, $f_0 \equiv 0 \pmod{m}$.

45. Let a and b be positive integers less than m. Then they have $O(\log m)$ digits (bits). Therefore by Theorem 2.4, we can multiply them using $O(\log^2 m)$ operations. Division by m takes $O(\log^2 m)$ operations by Theorem 2.7. Therefore, in all we have $O(\log^2 m)$ operations.

47. Let N_i be the number of coconuts the ith man leaves for the next man and let $N_0 = N$. At each stage, the ith man finds N_{i-1} coconuts, gives k coconuts to the monkeys, takes $(1/n)(N_{i-1} - k)$ coconuts for himself, and leaves the rest for the next man. This yields the recursive formula $N_i = (N_{i-1} - k)(n - 1)/n$. For convenience, let $w = (n - 1)/n$. If we iterate this formula a few times, we get $N_1 = (N_0 - k)w$, $N_2 = (N_1 - k)w = ((N_0 - k)w - k)w = N_0 w^2 - kw^2 - kw$, $N_3 = N_0 w^3 - kw^3 - kw^2 - kw$, ... The general pattern $N_i = N_0 w^i - kw^i - kw^{i-1} - \cdots - kw = N_0 w^i - kw(w^i - 1)/(w - 1)$ may be proved by induction. When the men rise in the morning, they find $N_n = N_0 w^n - kw(w^n - 1)/(w - 1)$ coconuts, and we must have $N_n \equiv k \pmod{n}$, that is, $N_n = N_0 w^n - kw(w^n - 1)/(w - 1) = k + tn$ for some integer t. Substituting $w = (n - 1)/n$ back in for w, solving for N_0, and simplifying

yields $N = N_0 = n^{n+1}(t+k)/(n-1)^n - kn + k$. For N to be an integer, because $(n, n-1) = 1$, we must have $(t+k)/(n-1)^n$ an integer. Because we seek the smallest positive value for N, we take $t + k = (n-1)^n$, so $t = (n-1)^n - k$. Substituting this value back into the formula for N yields $N = n^{n+1} - kn + k$.

49. **a.** Let $f_1(x) = \sum_{i=0}^{m} a_i x^i$, $f_2(x) = \sum_{i=1}^{m} b_i x^i$, $g_1(x) = \sum_{i=1}^{m} c_i x^i$, and $g_2(x) = \sum_{i=1}^{m} d_i x^i$, where the leading coefficients may be zero to keep the limits of summation the same for all polynomials. Then $a_i \equiv c_i \pmod{n}$ and $b_i \equiv d_i \pmod{n}$, for $i = 0, 1, \ldots, m$. Therefore by Theorem 4.6 part (i), $a_i + b_i \equiv c_i + d_i \pmod{n}$ for $i = 0, 1, \ldots, m$. Because $(f_1 + f_2)(x) = \sum_{i=1}^{m}(a_i + b_i)x^i$ and $(g_1 + g_2)(x) = \sum_{i=1}^{m}(c_i + d_i)x^i$, this shows the sums of the polynomials are congruent modulo n. **b.** With the same set up as in part (a), the coefficient on x^k in $(f_1 f_2)(x)$ is given by $a_0 b_k + a_1 b_{k-1} + \cdots + a_k b_0$, and the corresponding coefficient in $(g_1 g_2)(x)$ is given by $c_0 d_k + c_1 d_{k-1} + \cdots + c_k d_0$. Because each $a_i \equiv c_i \pmod{n}$ and $b_i \equiv d_i \pmod{n}$, by Theorem 4.6 the two expressions are congruent modulo n, and so, therefore, are the polynomials.

51. The basis step for induction on k is Exercise 42. Assume that $f(x) \equiv h(x) \pmod{p}$ and $f(x) = (x - a_1) \cdots (x - a_{k-1})h(x)$, where $h(x)$ is a polynomial with integer coefficients. Substituting a_k for x in this congruence gives us $0 \equiv (a_k - a_1) \cdots (a_k - a_1)h(a_k) \pmod{p}$. None of the factors $a_k - a_i$ can be congruent to zero modulo p, so we must have $h(a_k) \equiv 0 \pmod{p}$. Applying Exercise 50 to $h(x)$ and a_k gives us $h(x) \equiv (x - a_k)g(x) \pmod{p}$, and substituting this in the congruence for $f(x)$ yields $f(x) \equiv (x - a_1) \cdots (x - a_k)g(x) \pmod{p}$, which completes the induction step.

Section 4.2

1. **a.** $x \equiv 6 \pmod{7}$ **b.** $x \equiv 2, 5$ or $8 \pmod{9}$ **c.** $x \equiv 10 \pmod{40}$ **d.** $x \equiv 20 \pmod{25}$ **e.** $x \equiv 111 \pmod{999}$ **f.** $x \equiv 75 + 80k \pmod{1600}$ where k is an integer

3. $x \equiv 1074 + 3157k \pmod{28927591}$

5. 19 hours

7. 77 solutions when c is a multiple of 77

9. **a.** 13 **b.** 7 **c.** 5 **d.** 16

11. **a.** 1, 7, 11, 13, 17, 19, 23, 29 **b.** Note that 1, 11, 19 and 29 are their own inverses; 7 and 13 are inverses of each other, as are 23 and 17.

13. If $ax + by \equiv c \pmod{m}$, then there exists an integer k such that $ax + by - mk = c$. Because $d \mid ax + by - mk$, $d \mid c$. Thus, there are no solutions when $d \nmid c$. Now assume that $d \mid c$ and let $a = da'$, $b = db'$, $c = dc'$, and $m = dm'$, so that $(a', b', m') = 1$. Then we can divide the original congruence by d to get (*) $a'x + b'y \equiv c' \pmod{m'}$, or $a'x \equiv c' - b'y \pmod{m'}$, which has solutions if and only if $g = (a', m') \mid c - b'y$, which is equivalent to $b'y \equiv c' \pmod{g}$ having solutions. Because $(a', b', m') = 1$, and $(a', m') = g$, we must have $(b', g) = 1$, and so the last congruence has only one incongruent solution y_0 modulo g. But the m'/g solutions $y_0, y_0 + g, y_0 + 2g, \ldots, y_0 + (m'/g - 1)g$ are incongruent modulo m'. Each of these yields g incongruent values of x in the congruence (*). Therefore, there are $g(m'/g) = m'$ incongruent solutions to (*).

Now let (x_1, y_1) be one solution of the original congruence. Then the d values $x_1, x_1 + m', x_1 + 2m', \ldots, x_1 + (d-1)m'$ are congruent modulo m' but incongruent modulo m. Likewise, the d values $y_1, y_1 + m', y_1 + 2m', \ldots, y_1 + (d-1)m'$ are congruent modulo m' but incongruent modulo m. So for each solution of (*), we can generate d^2 solutions of the original congruence. Because there are m' solutions to (*), we have $d^2 m' = dm$ solutions to the original congruence.

15. Suppose that $x^2 \equiv 1 \pmod{p^k}$, where p is an odd prime and k is a positive integer. Then $x^2 - 1 \equiv (x+1)(x-1) \equiv 0 \pmod{p^k}$. Hence, $p^k \mid (x+1)(x-1)$. Because $(x+1) - (x-1) = 2$

and p is an odd prime, we know that p divides at most one of $(x-1)$ and $(x+1)$. It follows that either $p^k \mid (x+1)$ or $p^k \mid (x-1)$, so that $p \equiv \pm 1 \pmod{p^k}$.

17. To find the inverse of a modulo m, we must solve the Diophantine equation $ax + my = 1$, which can be done using the Euclidean algorithm. Using Corollary 2.5.1, we can find the greatest common divisor in $O(\log^3 m)$ bit operations. The back substitution to find x and y will take no more than $O(\log m)$ multiplications, each taking $O(\log^2 m)$ operations. Therefore, the total number of operations is $O(\log^3 m) + O(\log m)O(\log^2 m) = O(\log^3 m)$.

Section 4.3

1. $x \equiv 1 \pmod 6$

3. $32 + 60m$

5. $x \equiv 1523 \pmod{2310}$

7. 204

9. 1023

11. $x \equiv 2101 \pmod{2310}$

13. We can construct a sequence of k consecutive integers each divisible by a square as follows. Consider the system of congruences $x \equiv 0 \pmod{p_1^2}$, $x \equiv -1 \pmod{p_2^2}$, $x \equiv -2 \pmod{p_3^2}$, $\ldots$, $x \equiv -k+1 \pmod{p_k^2}$, where p_k is the kth prime. By the Chinese remainder theorem, there is a solution to this simultaneous system of congruence because the moduli are relatively prime. It follows that there is a positive integer N that satisfies each of these congruences. Each of the k integers $N, N+1, \ldots, N+k-1$ is divisible by a square because p_j^2 divides $N + j - 1$ for $j = 1, 2, \ldots, k$.

15. Suppose that x is a solution to the system of congruences. Then $x \equiv a_1 \pmod{m_1}$, so that $x = a_1 + km_1$ for some integer k. We substitute this into the second congruence to get $a_1 + km_1 \equiv a_2 \pmod{m_2}$ or $km_1 \equiv (a_2 - a_1) \pmod{m_2}$, which has a solution in k if and only if $(m_1, m_2) \mid (a_2 - a_1)$. Now assume such a solution k_0 exists. Then all incongruent solutions are given by $k = k_0 + m_2 t/(m_1, m_2)$, where t is an integer. Then $x = a_1 + km_1 = a_1 + \left(k_0 + \dfrac{m_2 t}{(m_1, m_2)}\right) m_1 = a_1 + k_0 m_1 + \dfrac{m_1 m_2}{(m_1, m_2)} t$. Note that $m_1 m_2/(m_1, m_2) = [m_1, m_2]$, so that if we set $x_1 = a_1 + k_0 m_1$, we have $x = x_1 + [m_1, m_2]t \equiv x_1 \pmod{[m_1, m_2]}$, and so the solution is unique modulo $[m_1, m_2]$.

17. **a.** $x = 430 + 2100j$ **b.** $x = 9102 + 10010j$

19. First, suppose the system has a solution. Then for any distinct i and j, there is a solution to the two-congruence system $x \equiv a_i \pmod{m_i}$, $x \equiv a_j \pmod{m_j}$. By Exercise 15, we must have $(m_i, m_j) \mid (a_i - a_j)$. For the converse, we proceed by mathematical induction on the number of congruences r. For $r = 2$, Exercise 15 shows that the system has a solution. This is the basis step. Now suppose the proposition is true for systems of r congruences and consider a system of $r+1$ congruences. Let $M = [m_1, m_2, \ldots, m_r]$. By the induction hypothesis, the system of the the first r congruences has a unique solution $A \pmod M$. Consider the system of two congruences $x \equiv A \pmod M$, $x \equiv a_{r+1} \pmod{m_{r+1}}$. A solution to this system will be a solution to the system of $r+1$ congruences. Note that for $i = 1 \ldots r$, we have $(m_i, m_{r+1}) \mid m_{r+1} \mid a_i - a_{r+1}$, and likewise $(m_i, m_{r+1}) \mid m_i \mid (a_i - A)$, because we must have $A \equiv a_i \pmod{m_i}$. Therefore, $A \equiv a_{r+1} \pmod{(m_i, m_{r+1})}$, which is equivalent to $A \equiv a_{r+1} \pmod{[(m_1, m_{r+1}), (m_2, m_{r+1}), \ldots, (m_r, m_{r+1})]}$. Check that this last modulus is equal to (M, m_{r+1}). Then we have $(M, m_{r+1}) \mid (A - a_{r+1})$. Therefore, by the induction

hypothesis, the system $x \equiv A \pmod{M}$, $x \equiv a_{r+1} \pmod{m_{r+1}}$ has a unique solution modulo $[M, m_{r+1}] = [m_1, m_2, \ldots, m_{r+1}]$, and this is a solution to the system of $r + 1$ congruences.

21. 2101

23. 73,800 pounds

25. 0000, 0001, 0625, 9376

27. We need to solve the system $x \equiv 23 + 2 \pmod{4 \cdot 23}$, $x \equiv 28 + 1 \pmod{4 \cdot 28}$, $x \equiv 33 \pmod{4 \cdot 33}$, where we have added 2 and 1 to make the system solvable under the conditions of Exercise 19. The solution to this system is $x \equiv 4257 \pmod{85008}$.

29. every 85,008 quarter-days, starting at 0

31. We examine each congruence class modulo 24. If x is congruent to an odd number modulo 24, then $x \equiv 1 \pmod{2}$, so all the odd congruence classes are covered. Note that the congruence classes of 2, 6, 10, 14, 18, 22 are all congruent to 2 (mod 4). This leaves only 0, 4, 8, 12, 16, 20. $0 \equiv 0 \pmod{24}$, $4 \equiv 12 \equiv 20 \equiv 4 \pmod{8}$, $8 \equiv 8 \pmod{12}$, and $16 \equiv 1 \pmod{3}$, so all congruence classes modulo 24 are covered.

33. If the set of distinct congruences covers the integers modulo the least common multiple of the moduli, then that set will cover all integers. Examine the integers modulo 210, the l.c.m. of the moduli in this set of congruences. The first four congruences take care of all numbers containing a prime divisor of 2, 3, 5, or 7. The remaining numbers can be examined one at a time, and each can be seen to satisfy one (or more) of the congruences.

35. most likely 318 inches

37. $x = 225a_1 + 1000a_2 + 576a_3 + 1800k$, where k is an integer and a_1 is 3 or 7, a_2 is 2 or 7, and a_3 is 14 or 18

Section 4.4

1. **a.** 1 or 2 (mod 7) **b.** 8 or 37 (mod 39) **c.** 106 or 233 (mod 343)

3. 785 or 1615 (mod 2401)

5. 184, 373, 562, 751, 940, 1129, and 1318 (mod ()1323)

7. 3404 or 279 (mod 4375)

9. two

11. Because $(a, p) = 1$, we know that a has an inverse b modulo p. Let $f(x) = ax - 1$. Then $x \equiv b \pmod{p}$ is the unique solution to $f(x) \equiv 0 \pmod{p}$. Because $f'(x) = a \not\equiv 0 \pmod{p}$, we know that $r \equiv b$ lifts uniquely to solutions modulo p^k for all natural numbers k. By Corollary 4.14.1, we have that $r_k = r_{k-1} - f(r_{k-1})\overline{f'(b)} = r_{k-1} - (ar_{k-1} - 1)\overline{a} = r_{k-1} - (ar_{k-1} - 1)b = r_{k-1}(1 - ab) + b$. This gives a recursive formula for lifting b to a solution modulo p^k for any k.

13. There are 1, 3, 3, 9, and 18 solutions for $n = 1$, 2, 3, 4, and 5, respectively.

Section 4.5

1. **a.** $x \equiv 2 \pmod{5}$ and $y \equiv 2 \pmod{5}$ **b.** no solutions **c.** $x \equiv 3 \pmod{5}$, $y \equiv 0 \pmod{5}$; $x \equiv 4 \pmod{5}$, $y \equiv 1 \pmod{5}$; $x \equiv 0 \pmod{5}$, $y \equiv 2 \pmod{5}$; $x \equiv 1 \pmod{5}$, $y \equiv 3 \pmod{5}$; and $x \equiv 2 \pmod{5}$, $y \equiv 4 \pmod{5}$.

3. 0, 1, p, or p^2

5. The basis step, where $k = 1$, is clear by assumption. For the inductive hypothesis, assume that $\mathbf{A} \equiv \mathbf{B} \pmod{m}$ and $\mathbf{A}^k \equiv \mathbf{B}^k \pmod{m}$. Then, $\mathbf{A} \cdot \mathbf{A}^k \equiv \mathbf{A} \cdot \mathbf{B}^k \pmod{m}$ by Theorem 4.16. Further, $\mathbf{A}^{k+1} = \mathbf{A} \cdot \mathbf{A}^k \equiv \mathbf{A} \cdot \mathbf{B}^k \equiv \mathbf{B} \cdot \mathbf{B}^k = \mathbf{B}^{k+1} \pmod{m}$.

7. false; take $m = 8$ and $\mathbf{A} = \begin{pmatrix} 3 & 0 \\ 0 & 1 \end{pmatrix}$

9. **a.** $\begin{pmatrix} 4 & 4 & 3 \\ 4 & 3 & 4 \\ 3 & 4 & 4 \end{pmatrix}$ **b.** $\begin{pmatrix} 2 & 0 & 6 \\ 2 & 1 & 4 \\ 3 & 4 & 0 \end{pmatrix}$ **c.** $\begin{pmatrix} 5 & 5 & 5 & 4 \\ 5 & 5 & 4 & 5 \\ 5 & 4 & 5 & 5 \\ 4 & 5 & 5 & 5 \end{pmatrix}$

11. **a.** 5 **b.** 5 **c.** 5 **d.** 1

13. In Gaussian elimination, the chief operation is to subtract a multiple of one equation or row from another, in order to put a 0 in a desirable place. Given that an entry a must be changed to 0 by subtracting a multiple of b, we proceed as follows: Let $\overline{b}$ be the inverse for $b \pmod{k}$. Then $a - (a\overline{b})b = 0$, and elimination proceeds as for real numbers. If $\overline{b}$ doesn't exist, and one cannot swap rows to get an invertible b, then the system is underdetermined.

15. Consider summing the ith row. Let $k = xn + y$, where $0 \le y < n$. Then x and y must satisfy the Diophantine equation $i \equiv a + cy + ex \pmod{n}$, if k is in the ith row. Then $x - ct$ and $y + et$ is also a solution for any integer t. By Exercise 14, there must be n positive solutions that yield n numbers k between 0 and n^2. Let $s, s+1, \ldots, s+n-1$ be the values for t that give these solutions. Then the sum of the ith row is $\sum_{r=0}^{n-1}(n(x - c(s+r)) + y + e(s+r)) = n(n+1)$, which is independent of i.

Section 4.6

1. **a.** $7 \cdot 19$ **b.** $29 \cdot 41$ **c.** $41 \cdot 47$ **d.** $47 \cdot 173$ **e.** $131 \cdot 277$ **f.** $29 \cdot 1663$

3. Numbers generated by linear functions where $a > 1$ will not be random in the sense that $x_{2s} - x_s = ax_{2s-1} + b - (ax_{s-1} + b) = a(x_{2s-1} - x_{s-1})$ is a multiple of a for all s. If $a = 1$, then $x_{2s} - x_s = x_0 + sb$. In this case, if $x_0 \neq 0$, then we will not notice if a factor of b that is not a factor of x_0 is a divisor of n.

Section 5.1

1. **a.** $256 = 2^8$ **b.** $16 = 2^4$ **c.** $1024 = 2^{10}$ **d.** $2 = 2^1$

3. **a.** by 3 but not by 9 **b.** by both 3 and 9 **c.** by both 3 and 9 **d.** by neither 3 nor 9

5. **a.** $2^1 = 2$ **b.** $2^0 = 1$ **c.** $2^6 = 64$ **d.** $2^0 = 1$

7. **a.** no **b.** no **c.** yes **d.** yes

9. **a.** by neither 3 nor 5 **b.** by both 3 and 5 **c.** by neither 3 nor 5 **d.** by 5 but not by 3

11. if and only if the number of digits is a multiple of 3 (respectively, 9)

13. if and only if the number of digits is a multiple of 6 in each case

15. if and only if the number of digits is a multiple of d, where $d \mid b - 1$

17. A palindromic integer with $2k$ digits has the form $(a_k a_{k-1} \ldots a_1 a_1 a_2 \ldots a_k)_{10}$. Using the test for divisibility by 11 developed in this section, we find that $a_k - a_{k-1} + \cdots \pm a_1 \mp a_1 \pm a_2 \mp \cdots - a_k = 0$, and so $(a_k a_{k-1} \ldots a_1 a_1 a_2 \ldots a_k)_{10}$ is divisible by 11.

19. An integer $a_k a_{k-1} \ldots a_1 a_0$ is divisible by 37 if and only if $a_0 a_1 a_2 + a_3 a_4 a_5 + a_6 a_7 a_8 + \cdots$ is; $37 \not| \; 443692$; $37 \mid 11092785$

21. **a.** no **b.** by 5 but not by 2 **c.** by neither 5 nor 13 **d.** yes

23. 6

25. **a.** no solutions **b.** 0, 3, 6, or 9 **c.** any digit is a solution **d.** 9 **e.** 9 **f.** no solutions

27. no

29. First note that $n = a_k 10^k + a_{k-1}10^{k-1} + \cdots + a_1 10 + a_0$, so that $(n - a_0)/10 = (a_k 10^k + a_{k-1}10^{k-1} + \cdots + a_1 10)/10 = a_k 10^{k-1} + \cdots + a_1$. Now suppose $d \mid n$. Then $n = a_k 10^k + a_{k-1}10^{k-1} + \cdots + a_1 10 + a_0 \equiv 10(a_k 10^{k-1} + \cdots + a_1) + a_0 \equiv 0 \pmod{d}$. Multiplying both sides by e, which is an inverse for 10 modulo d, gives us $(a_k 10^{k-1} + \cdots + a_1) + ea_0 \equiv 0 \pmod{d}$. Which is $n' = (n - a_0)/10 + ea_0 \equiv 0 \pmod{d}$. These steps are reversible, so we have that $d \mid n$ if and only if $d \mid n'$.

To show the technique will work, we need to show that n, n', $(n')'$, ... is a decreasing sequence until we get a term that is not much bigger than d. Suppose that $n > 10d$. Then, because $a_0 \leq 9$, we have $9n > 10a_0 d$. Because e is a least positive residue modulo d, we have $e < d$, so, in particular, $10e - 1 < 10d$. Using this in the above inequality gives us $9n > a_0(10e - 1)$. Adding n to both sides gives us $10n > n - a_0 + 10ea_0$, or $n > (n - a_0)/10 + ea_0 = n'$. This shows that the sequence generated will be decreasing at least until some term is less than $10d$, which we may examine by hand.

31. **a.** Multiply the last digit by 4 and add this result to the number formed by deleting the last digit of the integer and repeat. **b.** Multiply the last digit by 2 and add this result to the number formed by deleting the last digit of the integer and repeat. **c.** Multiply the last digit by 2 and subtract this result from the number formed by deleting the last digit of the integer and repeat. **d.** Multiply the last digit by 8 and subtract this result from the number formed by deleting the last digit of the integer and repeat.

33. **a.** $13 \nmid 798$; $19 \mid 798$; $21 \mid 798$; $27 \nmid 798$ **b.** $13 \mid 2340$; $19 \nmid 2340$; $21 \nmid 2340$; $27 \nmid 2340$ **c.** $13 \nmid 34257$; $19 \mid 34257$; $21 \nmid 34257$; $27 \nmid 34257$. **d.** $13 \nmid 348327$; $19 \mid 348327$; $21 \mid 348327$; $27 \mid 348327$.

Section 5.2

1. Happy Birthday!

3. twice

5. $W \equiv k + [2.6m - 0.2] - 2C + Y + [Y/4] + [C/4] - [C/40] \pmod{7}$.

7. answer is person dependent

9. 2500

11. If the 13th falls on the same day of the week on two consecutive months, then the number of days in the first month must be congruent to 0 modulo 7, and the only such month is February during non-leap year. If February 13th is a Friday, then January 1st is a Thursday.

13. In the perpetual calendar formula, we let $W = 5$ and $k = 13$ to get $5 \equiv 13 + [2.6m - 0.2] - 2C + Y + [Y/4] + [C/4] \pmod{7}$. Then $[2.6m - 0.2] \equiv 6 + 2C - Y - [Y/4] - [C/4] \pmod{7}$. We note that as the month varies from March to December, the expression $[2.6m - 0.2]$ takes on every residue class modulo 7. So regardless of the year, there is always an m which makes the left side of the last congruence congruent to the right side.

15. The months with 31 days are March, May, July, August, October, December, and January, which is considered in the previous year. The corresponding numbers for these months are 1, 3, 5, 6, 8, 10, and 12. Given Y and C, we let $k = 31$ in the perpetual calendar formula and get $W \equiv 31 + [2.6m - 0.2] - 2C + Y + [Y/4] + [C/4] \equiv 3 + [2.6m - 0.2] - 2C + Y + [Y/4] + [C/4] \pmod{7}$. To see which days of the week the 31st will fall on, we let m take on the values 1, 3, 5, 6, 8, 10 and reduce. Finally, we decrease the year by 1 (which may require decreasing the century by 1) and let m take on the value 12 and reduce modulo 7. The collection of values of W tells us the days of the week on which the 31st will fall.

Section 5.3

1. **a.** Teams i and j are paired in round k if and only if $i + j \equiv k \pmod 7$ with team i drawing a bye if $2i \equiv k \pmod 7$. Round 1: 1–7, 2–6, 3–5, 4–bye; round 2: 2–7, 3–6, 4–5, 1–bye; round 3: 1–2, 3–7, 4–6, 5–bye; round 4: 1–3, 4–7, 5–6, 2–bye; round 5: 1–4, 2–3, 5–7, 6–bye; round 6: 1–5, 2–4, 6–7, 3–bye; round 7: 1–6, 2–5, 3–4, 7–bye. **b.** Teams i and j are paired in round k if and only if $i + j \equiv k \pmod 7$, $i, j \neq 8$; team i plays team 8 if $2i \equiv k \pmod 7$. **c.** Teams i and j are paired in round k if and only if $i + j \equiv k \pmod 9$, with team i drawing a bye if $2i \equiv k \pmod 9$. **d.** Teams i and j are paired in round k if and only if $i + j \equiv k \pmod 9$, $i, j \neq 10$; team i plays team 10 if $2i \equiv k \pmod 9$.

3. **a.** home teams in round 1: 4 and 5; round 2: 2 and 3; round 3: 1 and 5; round 4: 3 and 4; round 5: 1 and 2 **b.** home teams in round 1: 5, 6, and 7; round 2: 2, 3, and 4; round 3: 1, 6, and 7; round 4: 3, 4, and 5; round 5: 1, 2, and 7; round 6: 4, 5, and 6; round 7: 1, 2, and 3 **c.** home teams in round 1: 6, 7, 8, and 9; round 2: 2, 3, 4, and 5; round 3: 1, 7, 8, and 9; round 4: 3, 4, 5, and 6; round 5: 1, 2, 8, and 9; round 6: 4, 5, 6, and 7; round 7: 1, 2, 3, and 9; round 8: 5, 6, 7, and 8; round 9: 1, 2, 3, and 4

Section 5.4

1. Let k be the six-digit number on the license plate of a car. We can assign this car the space numbered $h(k) \equiv k \pmod{101}$, where the spaces are numbered $0, 1, 2, \ldots, 100$. When a car is assigned the same space as another car we can assign it to the space $h(k) + g(k)$ where $g(k) \equiv k + 1 \pmod{99}$ and $0 < g(k) \leq 98$. When this space is occupied, we next try $h(k) + 2g(k)$, then $h(k) + 3g(k)$, and so on. All spaces are examined because $(g(k), 101) = 1$.

3. **a.** It is clear that m memory locations will be probed as $j = 0, 1, 2, \ldots, m - 1$. To see that they are all distinct, and hence every memory location is probed, assume that $h_i(K) \equiv h_j(K) \pmod m$. Then $h(K) + iq \equiv h(K) + jq \pmod m$. From this it follows that $iq \equiv jq \pmod m$, and as $(q, m) = 1$, $i \equiv j \pmod m$ by Corollary 4.5.1. And so $i = j$ because i and j are both less than m. **b.** It is clear that m memory locations will be probed as $j = 0, 1, 2, \ldots, m - 1$. To see that they are all distinct, and hence every memory location is probed, assume that $h_i(K) \equiv h_j(K) \pmod m$. Then $h(K) + iq \equiv h(K) + jq \pmod m$. From this it follows that $iq \equiv jq \pmod m$, and as $(q, m) = 1$, $i \equiv j \pmod m$ by Corollary 4.5.1. And so $i = j$ because i and j are both less than m.

5. 558, 1002, 2174, 4035

Section 5.5

1. **a.** 0 **b.** 0 **c.** 1 **d.** 1 **e.** 0 **f.** 1

3. **a.** 0 **b.** 1 **c.** 0

5. **a.** 7 **b.** 1 **c.** 4

7. Transposition means that adjacent digits are in the wrong order. Suppose, first, that the first two digits, x_1 and x_2, or equivalently, the fourth and fifth digits, are exchanged, and the error is not detected. Then $x_7 \equiv 7x_1 + 3x_2 + x_3 + 7x_4 + 3x_5 + x_6 \equiv 7x_2 + 3x_1 + x_3 + 7x_4 + 3x_5 + x_6 \pmod{10}$. It follows that $7x_1 + 3x_2 \equiv 7x_2 + 3x_1 \pmod{10}$ or $4x_1 \equiv 4x_2 \pmod{10}$. By Corollary 4.5.1, we see that $x_1 \equiv x_2 \pmod 5$. This is equivalent to $| x_1 - x_2 | = 5$, as x_1 and x_2 are single digits. Similarly, if the second and third (or fifth and sixth) digits are transposed, we find that $2x_2 \equiv 2x_3 \pmod{10}$, which again reduces to $x_2 \equiv x_3 \pmod 5$ by Corollary 4.5.1. Also, if the third and fourth digits are transposed, we find that $6x_3 \equiv 6x_4 \pmod{10}$ and $x_3 \equiv x_4 \pmod 5$, similarly as before. The reverse argument will complete the proof.

9. **a.** 0 **b.** 3 **c.** 4 **d.** X

11. **a.** valid **b.** not valid **c.** valid **d.** valid **e.** not valid

13. 0-07-289905-0

15. **a.** no **b.** yes **c.** yes **d.** no

17. It can.

19. **a.** valid **b.** not valid **c.** valid **d.** not valid **e.** valid

21. Let $c_i = 1$ if i is odd and $c_i = 3$ if i is even, for $i = 1, 2, \ldots 13$. Then $\sum_{i=1}^{13} c_i a_i \equiv 0 \pmod{10}$. Suppose that one digit, say, a_k, of an ISBN-13 code is misread as $b \neq a_i$. To get a contradiction, suppose that when the above congruence is changed by replacing a_k by b the sum is still congruent to 0 modulo 10. If we subtract these two congruences, we get $c_k(a_k - b) \equiv 0 \pmod{10}$. Because both 1 and 3 are relatively prime to 10, we can multiply both sides by c_k^{-1}, which gives us $a_k - b \equiv 0 \pmod{10}$. But because a_k and b are both integers between 0 and 9, we must have $a_k = b$, contradicting the assumption that $b \neq a_k$. Therefore, any single error is detected by the code.

23. **a.** yes **b.** no

25. **a.** 94 **b.** If x_i is misentered as y_i, then if the congruence defining x_{10} holds, we see that $ax_i \equiv ay_i \pmod{11}$ by setting the two definitions of x_{10} congruent. From this, it follows by Corollary 4.5.1 that $x_i \equiv y_i \pmod{11}$ and so $x_i = y_i$. If the last digit, x_{11}, is misentered as y_{11}, then the congruence defining x_{11} will hold if and only if $x_{11} = y_{11}$. **c.** Suppose that x_i is misentered as y_i and x_j is misentered as y_j, with $i < j < 10$. Suppose both of the congruences defining x_{10} and x_{11} hold. Then by setting the two versions of each congruence congruent to each other, we obtain $ax_i + bx_j \equiv ay_i + by_j \pmod{11}$ and $cx_i + dx_j \equiv cy_i + dy_j \pmod{11}$ where $a \neq b$. If it is the case that $ad - bc \not\equiv 0 \pmod{11}$, then the coefficient matrix is invertible and we can multiply both sides of this system of congruences by the inverse to obtain $x_i = y_i$ and $x_j = y_j$. Indeed, after (tediously) checking each possible choice of a, b, c, and d, we find that all the matrices are invertible modulo 11.

27. **a.** 1 **b.** 1 **c.** 6

29. Errors involving a difference of 7 cannot be detected: 0 for 7, 1 for 8, 2 for 9, or vice versa. All others can be detected.

31. **a.** 1 **b.** X **c.** 2 **d.** 8

33. Yes. Assume not and compare the expressions modulo 11 to get a congruence of the form $ad_i + bd_j \equiv ad_j + bd_i \pmod{11}$, which reduces to $(a - b)d_i \equiv (a - b)d_j \pmod{11}$. Because $0 < a - b < 11$ and 11 is prime, it follows that $d_i \equiv d_j \pmod{11}$. Because these digits are between 0 and X, they must be equal.

Section 6.1

1. Note that $10! + 1 = 1(2 \cdot 6)(3 \cdot 4)(5 \cdot 9)(7 \cdot 8)10 + 1 = 1 \cdot 12 \cdot 12 \cdot 45 \cdot 56 \cdot 10 + 1 \equiv 1 \cdot 1 \cdot 1 \cdot 1 \cdot 1 \cdot (-1) + 1 \equiv 0 \pmod{11}$. Therefore, 11 divides $10! + 1$.

3. 9

5. 6

7. 436

9. 2

11. 6

13. $(3^5)^2 \equiv 243^2 \equiv 1^2 \equiv 1 \pmod{11^2}$.

15. **a.** $x \equiv 9 \pmod{17}$ **b.** $x \equiv 17 \pmod{19}$

17. Suppose that p is an odd prime. Then Wilson's theorem tells us that $(p-1)! \equiv -1 \pmod{p}$. Because $(p-1)! = (p-3)!(p-1)(p-2) \equiv (p-3)!(-1)(-2) \equiv 2 \cdot (p-3)! \pmod{p}$, this implies that $2 \cdot (p-3)! \equiv -1 \pmod{p}$.

19. Because $(a, 35) = 1$, we have $(a, 7) = (a, 5) = 1$, so we may apply Fermat's little theorem to get $a^{12} - 1 \equiv (a^6)^2 - 1 \equiv 1^2 - 1 \equiv 0 \pmod{7}$ and $a^{12} - 1 \equiv (a^4)^3 - 1 \equiv 1^3 - 1 \equiv 0 \pmod{5}$. Because both 5 and 7 divide $a^{12} - 1$, then 35 must also divide it.

21. When n is even, so is n^7, and when n is odd, so is n^7. It follows that $n^7 \equiv n \pmod{2}$. Furthermore, because $n^3 \equiv n \pmod{3}$, it follows that $n^7 = (n^3)^2 \cdot n \equiv n^2 \cdot n \equiv n^3 \equiv n \pmod{3}$. We also know by Fermat's little theorem that $n^7 \equiv n \pmod{7}$. Because $42 = 2 \cdot 3 \cdot 7$, it follows that $n^7 \equiv n \pmod{42}$.

23. By Fermat's little theorem, $\sum_{k=1}^{p-1} k^{p-1} \equiv \sum_{k=1}^{p-1} 1 \equiv p - 1 \pmod{p}$.

25. By Fermat's little theorem, we have $a \equiv a^p \equiv b^p \equiv b \pmod{p}$; hence, $b = a + kp$ for some integer k. Then by the binomial theorem, $b^p = (a + kp)^p = a^p + \binom{p}{1} a^{p-1} kp + p^2 N$, where N is some integer. Then $b^p \equiv a^p + p^2 a^{p-1} k + p^2 N \equiv a^p \pmod{p^2}$, as desired.

27. 641

29. Suppose that p is prime. Then by Fermat's little theorem, for every integer a, $a^p \equiv a \pmod{p}$, and by Wilson's theorem, $(p-1)! \equiv -1 \pmod{p}$, so that $a(p-1)! \equiv -a \pmod{p}$. It follows that $a^p + (p-1)!a \equiv a + (-a) \equiv 0 \pmod{p}$. Consequently, $p \mid [a^p + (p-1)!a]$.

31. Because $p - 1 \equiv -1$, $p - 2 \equiv -2, \ldots, (p-1)/2 \equiv -(p-1)/2 \pmod{p}$, we have $((p-1)/2)!^2 \equiv -(p-1)! \equiv 1 \pmod{p}$. (Because $p \equiv 3 \pmod{4}$ the minus signs work out.) If $x^2 \equiv 1 \pmod{p}$, then $p \mid x^2 - 1 = (x-1)(x+1)$, so $x \equiv \pm 1 \pmod{p}$.

33. Suppose that $p \equiv 1 \pmod{4}$. Let $y = \pm[(p-1)/2]!$. Then $y^2 \equiv [(p-1)/2]!^2 \equiv [(p-1)/2]!^2 (-1)^{(p-1)/2} \equiv (1 \cdot 2 \cdot 3 \cdots (p-1)/2)(-1 \cdot (-2) \cdot (-3) \cdots (-(p-1)/2)) \equiv 1 \cdot 2 \cdot 3 \cdots (p-1)/2 \cdot (p+1)/2 \cdots (p-3)(p-2)(p-1) = (p-1)! \equiv -1 \pmod{p}$, where we have used Wilson's theorem. Now suppose that $x^2 \equiv -1 \pmod{p}$. Then $x^2 \equiv y^2 \pmod{p}$ where $y = [(p-1)/2]!$. Hence, $(x^2 - y^2) = (x-y)(x+y) \pmod{p}$. It follows that $p \mid (x-y)$ or $p \mid (x+y)$ so that $x \equiv \pm y \pmod{p}$.

35. If n is composite and $n \neq 4$, then Exercise 16 shows that $(n-1)!/n$ is an integer, so $[((n-1)!+1)/n - [(n-1)!/n]] = [(n-1)!/n + 1/n - (n-1)!/n] = [1/n] = 0$, and if $n = 4$, then the same expression is also equal to 0. But if n is prime, then by Wilson's Theorem $(n-1)! = Kn - 1$ for some integer K. So $[((n-1)!+1)/n - [(n-1)!/n]] = [(Kn - 1 + 1)/n - [(Kn-1)/n]] = [K - (K-1)] = 1$. Therefore, the sum increases by 1 exactly when n is prime, so it must be equal to $\pi(n)$.

37. Let $n = 4k + r$ with $0 \leq r < 4$. Then by Fermat's little theorem, we have $b^n \equiv b^{4k+r} \equiv (b^4)^k b^r \equiv 1^k b^r \equiv b^r \pmod{5}$ for any integer b. Then $1^n + 2^n + 3^n + 4^n \equiv 1^r + 2^r + 3^r + 4^r \pmod{5}$. We consider each of the 4 possibilities for r. If $r = 0$, then $1^r + 2^r + 3^r + 4^r \equiv 1 + 1 + 1 + 1 \equiv 4 \pmod{5}$. If $r = 1$, then $1^r + 2^r + 3^r + 4^r \equiv 1 + 2 + 3 + 4 \equiv 0 \pmod{5}$. If $r = 2$, then $1^r + 2^r + 3^r + 4^r \equiv 1 + 4 + 9 + 16 \equiv 30 \equiv 0 \pmod{5}$. If $r = 3$, then $1^r + 2^r + 3^r + 4^r \equiv 1 + 8 + 27 + 64 \equiv 1 + 3 + 2 + 4 \equiv 0 \pmod{5}$. So 5 divides $1^n + 2^n + 3^n + 4^n$ if and only if $r = 0$, that is, if and only if $4 \mid n$.

39. Suppose that n and $n + 2$ are twin primes. By Wilson's theorem, n is prime if and only if $(n-1)! = -1 \pmod{n}$. Hence, $4[(n-1)!+1] + n \equiv 4 \cdot 0 + n \equiv 0 \pmod{n}$. Also, because $n + 2$ is prime, by Wilson's theorem it follows that $(n+1)! \equiv -1 \pmod{n+2}$, so that $(n+1)n \cdot (n-1)! \equiv (-1)(-2)(n-1)! \equiv 2(n-1)! \equiv -1 \pmod{n+2}$. Hence, $4[(n-1)!+1] + n \equiv 2(2 \cdot (n-1)!) + 4 + n \equiv 2 \cdot (-1) + 4 + n = n + 2 \equiv 0 \pmod{n+2}$. Because $(n, n+2) = 1$,

it follows that $4[(n-1)!+1]+n \equiv 0 \pmod{n(n+2)}$. The converse follows for n odd, by reversing these calculations. For n even, it's easy to check that one of the congruences in the system fails to hold.

41. We have $1 \cdot 2 \cdots (p-1) \equiv (p+1)(p+2)\cdots(2p-1) \pmod{p}$. Each factor is prime to p, so $1 \equiv ((p+1)(p+2)\cdots(2p-1))/(1 \cdot 2 \cdots (p-1)) \pmod{p}$. Thus, $2 \equiv ((p+1)(p+2)\cdots(2p-1)2p)/(1 \cdot 2 \cdots (p-1)p) \equiv \binom{2p}{p} \pmod{p}$.

43. We first note that $1^p \equiv 1 \pmod{p}$. Now suppose that $a^p \equiv a \pmod{p}$. Then by Exercise 42, we see that $(a+1)^p \equiv a^p + 1 \pmod{p}$. But by the inductive hypothesis $a^p \equiv a \pmod{p}$, we see that $a^p + 1 \equiv a + 1 \pmod{p}$. Hence, $(a+1)^p \equiv a + 1 \pmod{p}$.

45. **a.** If $c < 26$, then c cards are put into the deck above the card, so it ends up in the $2c$th position and $2c < 52$, so $b = 2c$. If $c \geq 26$, then the card is in the $c - 26$th place in the bottom half of the deck. In the shuffle, $c - 26 - 1$ cards are put into the deck above the card, so it ends up in the $b = (c - 26 + c - 26 - 1)$th place. Then $b = 2c - 53 \equiv 2c \pmod{53}$. **b.** 52

47. Assume without loss of generality that $a_p \equiv b_p \equiv 0 \pmod{p}$. Then by Wilson's theorem, $a_1 a_2 \cdots a_{p-1} \equiv b_1 b_2 \cdots b_{p-1} \equiv -1 \pmod{p}$. Then $a_1 b_1 \cdots a_{p-1} b_{p-1} \equiv (-1)^2 \equiv 1 \pmod{p}$. If the set were a complete system, the last product would be $\equiv -1 \pmod{p}$.

49. The basis step is omitted. Assume $(p-1)^{p^{k-1}} \equiv -1 \pmod{p^k}$. Then $(p-1)^{p^k} \equiv ((p-1)^{p^{k-1}})^p \equiv (-1 + mp^k)^p \equiv -1 + \binom{p}{1} mp^k + \cdots + (mp^k)^p \equiv -1 \pmod{p^{k+1}}$, where we have used the fact that $p \mid \binom{p}{j}$ for $j \neq 0$ or p.

51. First suppose n is prime. Then from Exercise 72 in Section 3.5, we have $\binom{n}{k}$ is divisible by n for $k = 1, 2, 3, \ldots, n-1$. Then by the binomial theorem, $(x-a)^n = x^n - \binom{n}{1}x^{n-1}a + \binom{n}{2}x^{n-2}a^2 + \cdots + (-a)^n \equiv x^n + (-a)^n \pmod{n}$, because all the binomial coefficients, except the first and last, are divisible by n. Then by Fermat's little theorem, because $(n, -a) = 1$, we have $x^n + (-a)^n \equiv x^n - a \pmod{n}$, so these two polynomials are congruent modulo n as polynomials. Conversely, suppose n is not prime and let p be the smallest prime dividing n, and let $q = p^\alpha \,||\, n$. Looking at the expression above, it suffices to show that one of the binomial coefficients is not divisible by q, and hence not divisible by n. Let $n = mq$. Then $\binom{n}{q} = \dfrac{n(n-1)\cdots(n-(q-1))}{q!} = \dfrac{m(n-1)\cdots(n-(q-1))}{(q-1)!}$. Because q is the highest power of p dividing n, we have $(q, m) = 1$. Further, if $q \mid (n-b)$, for $b = 1, 2, \ldots, q-1$, then $q \mid b$, but $1 \leq b \leq q-1$, a contradiction. Therefore, q doesn't divide the numerator of the fraction, and so neither does n. Therefore, $\binom{n}{q} \not\equiv 0 \pmod{n}$. Because the coefficient of x^q is 0 in $x^n - a$, these two polynomials cannot be congruent modulo n as polynomials.

Section 6.2

1. $3^{90} \equiv 1 \pmod{91}$, but $91 = 7 \cdot 13$

3. $2^{161038} \equiv 2 \pmod{161038}$

5. $(n-a)^n \equiv (-a)^n \equiv -(a^n) \equiv -a \equiv (n-a) \pmod{n}$

7. Raise the congruence $2^{2^m} \equiv -1 \pmod{F_m}$ to the $2^{2^m - m}$th power, to obtain $2^{2^{2^m}} \equiv 1 \pmod{2^{2^m}+1}$, which says that $2^{F_m - 1} \equiv 1 \pmod{F_m}$.

9. Suppose that n is a pseudoprime to the bases a and b. Then $b^n \equiv b \pmod{n}$ and $a_n \equiv a \pmod{n}$. It follows that $(ab)^n \equiv a^n b^n \equiv ab \pmod{n}$. Hence, n is a pseudoprime to the base ab.

11. If $(ab)^{n-1} \equiv 1 \pmod{n}$, then, $1 \equiv a^{n-1}b^{n-1} \equiv 1 \cdot b^{n-1} \pmod{n}$, which implies that n is a pseudoprime to the base b, a contradiction.

13. A computation shows $2^{1387} \equiv 2 \pmod{1387}$, so 1387 is a pseudoprime. But $1387 - 1 = 2 \cdot 693$ and $2^{693} \equiv 512 \pmod{1387}$, which is all that must be checked, because $s = 1$. Thus, 1387 fails Miller's test and hence is not a strong pseudoprime.

15. Note that $25326001 - 1 = 2^4 1582875 = 2^s t$ and with this value of t, $2^t \equiv -1 \pmod{25326001}$, $3^t \equiv -1 \pmod{25326001}$, and $5^t \equiv 1 \pmod{25326001}$.

17. Suppose $c = 7 \cdot 23 \cdot q$, with q an odd prime, is a Carmichael number. Then by Theorem 6.7, we must have $(7 - 1)|(c - 1)$, so $c = 7 \cdot 23 \cdot q \equiv 1 \pmod{6}$. Solving this yields $q \equiv 5 \pmod{6}$. Also, we must have $(23 - 1)|(c - 1)$, so $c = 7 \cdot 23 \cdot q \equiv 1 \pmod{22}$. Solving this yields $q \equiv 19 \pmod{22}$ If we apply the Chinese remainder theorem to these two congruences, we obtain $q \equiv 41 \pmod{66}$, that is, $q = 41 + 66k$. Then we must have $(q - 1)|(c - 1)$, which is $(40 + 66k)|(7 \cdot 23 \cdot (41 + 66k) - 1$. So there is an integer m such that $m(40 + 66k) = 6600 + 10626k = 160 + 6440 + 10626k = 160 + 161(40 + 66k)$. Therefore, 160 must be a multiple of $40 + 66k$, which happens only when $k = 0$. Therefore, $q = 41$ is the only such prime.

19. We have $321,197,185 - 1 = 321,197,184 = 4 \cdot 80,299,296 = 18 \cdot 17,844,288 = 22 \cdot 14,599,872 = 28 \cdot 11,471,328 = 36 \cdot 8,922,144 = 136 \cdot 2,361,744$, so $p - 1|321,197,185 - 1$ for every prime p which divides 321,197,185. Therefore, by Theorem 6.7, 321,197,185 is a Carmichael number.

21. We can assume that $b < n$. Then b has fewer than $\log_2 n$ bits. Also, $t < n$ so it has fewer than $\log_2 n$ bits. It takes at most $\log_2 n$ multiplications to calculate b^{2^s}, so it takes $O(\log_2 n)$ multiplications to calculate $b^{2^{\log_2 t}} = b^t$. Each multiplication is of two $\log_2 n$ bit numbers, and so takes $O((\log_2 n)^2)$ operations. So all together we have $O((\log_2 n)^3)$ operations.

Section 6.3

1. **a.** 1, 5 **b.** 1, 2, 4, 5, 7, 8 **c.** 1, 3, 7, 9 **d.** 1, 3, 5, 9, 11, 13 **e.** 1, 3, 5, 7, 9, 11, 13, 15 **f.** 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16

3. If $(a, m) = 1$, then $(-a, m) = 1$, so $-c_i$ must appear among the c_j. Also $c_i \not\equiv -c_i \pmod{m}$, or else $2c_i \equiv 0 \pmod{m}$ and so $(c_i, m) \neq 1$. Hence, the elements of in the sum can be paired so that each pair sums to 0 (mod m), and thus the entire sum is 0 (mod m).

5. 1

7. 11

9. Because $a^2 \equiv 1 \pmod{8}$ whenever a is odd, it follows that $a^{12} \equiv 1 \pmod{8}$ whenever $(a, 32760) = 1$. Euler's theorem tells us that $a^{\phi(9)} = a^6 \equiv 1 \pmod{9}$ whenever $(a, 9) = 1$, so that $a^{12} = (a^6)^2 \equiv 1 \pmod{9}$ whenever $(a, 32760) = 1$. Furthermore, Fermat's little theorem tells us that $a^4 \equiv 1 \pmod{5}$ whenever $(a, 5) = 1$, $a^6 \equiv 1 \pmod{7}$ whenever $(a, 7) = 1$, and $a^{12} \equiv 1 \pmod{13}$ whenever $(a, 13) = 1$. It follows that $a^{12} \equiv (a^4)^3 \equiv 1 \pmod{5}$, $a^{12} \equiv (a^6)^2 \equiv 1 \pmod{7}$, and $a^{12} \equiv 1 \pmod{13}$ whenever $(a, 32760) = 1$. Because $32760 = 2^3 3^2 \cdot 5 \cdot 7 \cdot 13$ and the moduli 8, 9, 5, 7, and 13 are pairwise relatively prime, we see that $a^{12} \equiv 1 \pmod{32760}$.

11. **a.** $x \equiv 9 \pmod{14}$ **b.** $x \equiv 13 \pmod{15}$ **c.** $x \equiv 7 \pmod{16}$

13. For a particular $i = 1, 2, \ldots k$, note that $\phi(n) = \phi(p_1)\phi(p_2) \cdots \phi(p_k) = \phi(p_i)N$ for some integer N. Then, by Euler's theorem, $a^{\phi(n)+1} \equiv a^{\phi(p_i)N+1} \equiv a^{\phi(p_i)N} a \equiv 1^N a \equiv a \pmod{p_i}$. This gives us a set of k linear congruences with moduli mutually relatively prime. So by the Chinese remainder theorem, the unique solution to the system modulo n is a. So $a^{\phi(n)+1} \equiv a \pmod{n}$.

15. **a.** $x \equiv 37 \pmod{187}$ **b.** $x \equiv 23 \pmod{30}$ **c.** $x \equiv 6 \pmod{210}$ **d.** $x \equiv 150,999 \pmod{554,268}$.

17. 1

19. $\phi(13) = 12$, $\phi(14) = 6$, $\phi(15) = 8$, $\phi(16) = 8$, $\phi(17) = 16$, $\phi(18) = 6$, $\phi(19) = 18$, $\phi(20) = 8$

21. If $(a, b) = 1$ and $(a, b-1) = 1$, then $a \mid (b^{k\phi(a)} - 1)/(b-1)$, which is a base b repunit. If $(a, b-1) = d > 1$, then d divides any repunit of length $k(b-1)$, and $(a/d) \mid (b^{k\phi(a/d)} - 1)/(b-1)$ and these sets intersect infinitely often.

23. Let $a_1, a_2, \ldots, a_r$ be the bases to which n is a pseudoprime and for which $(a_i, n) = 1$ for each i. Then by part (a), we know that, for each i, n is not a pseudoprime to the base ba_i. Thus, we have $2r$ different elements relatively prime to n. Then by the definition of $\phi(n)$, we have $r \leq \phi(n)/2$.

Section 7.1

1. **a.** Because for all positive integers m and n, $f(mn) = 0 = 0 \cdot 0 = f(m) \cdot f(n)$, f is completely multiplicative. **b.** Because $f(6) = 2$, but $f(2) \cdot f(3) = 2 \cdot 2 = 4$, f is not completely multiplicative. **c.** Because $f(6) = 3$, but $f(2) \cdot f(3) = \frac{2}{2} \cdot \frac{3}{2} = \frac{3}{2}$, f is not completely multiplicative. **d.** Because $f(4) = \log(4) > 1$, but $f(2) \cdot f(2) = \log(2) \cdot \log(2) < 1$, f is not completely multiplicative. **e.** Because for any positive integers m and n, $f(mn) = (mn)^2 = m^2n^2 = f(m) \cdot f(n)$, f is completely multiplicative. **f.** Because $f(4) = 4! = 24$, but $f(2) \cdot f(2) = 2!2! = 4$, f is not completely multiplicative. **g.** Because $f(6) = 7$, but $f(2) \cdot f(3) = 4 \cdot 3 = 12$, f is not completely multiplicative **h.** Because $f(4) = 4^4 = 256$, but $f(2) \cdot f(2) = 2^2 2^2 = 16$, f is not completely multiplicative. **i.** Because for any positive integers m and n, $f(mn) = \sqrt{mn} = \sqrt{m}\sqrt{n} = f(m) \cdot f(n)$, f is completely multiplicative.

3. We have the following prime factorizations of 5186, 5187, and 5188: $5186 = 2 \cdot 2593$, $5187 = 3 \cdot 7 \cdot 13 \cdot 19$, and $5188 = 2^2 1297$. Hence, $\phi(5186) = \phi(2)\phi(2593) = 1 \cdot 2592 = 2592$, $\phi(5187) = \phi(3)\phi(7)\phi(13)\phi(19) = 2 \cdot 6 \cdot 12 \cdot 18 = 2592$, and $\phi(5188) = \phi(2^2)\phi(1297) = 2 \cdot 1296 = 2592$. It follows that $\phi(5186) = \phi(5187) = \phi(5188)$.

5. 7, 9, 14, 18

7. 35, 39, 45, 52, 56, 70, 72, 78, 84, 90

9. $\phi(2n)$

11. multiples of 3

13. powers of 2 greater than 1

15. If n is odd, then $(2, n) = 1$ and $\phi(2n) = \phi(2)\phi(n) = 1 \cdot \phi(n) = \phi(n)$. If n is even, say $n = 2^s t$ with t odd. Then $\phi(2n) = \phi(2^{s+1}t) = \phi(2^{s+1})\phi(t) = 2^s\phi(t) = 2(2^{s-1}\phi(t)) = 2(\phi(2^s)\phi(t)) = 2(\phi(2^s t)) = 2\phi(n)$.

17. $n = 2^k p_1 p_2 \cdots p_r$ where each p_i is a distinct Fermat prime.

19. Let $n = p_1^{a_1} \cdots p_r^{a_r}$ be the factorization for n. If $n = 2\phi(n)$ then, $p_1^{a_1} \cdots p_r^{a_r} = 2\prod_{j=1}^{r} p_j^{a_j - 1}(p_j - 1)$. Cancelling the powers of all p_j's yields $p_1 \cdots p_r = 2\prod_{j=1}^{r}(p_j - 1)$. If any p_j is an odd prime, then the factor $(p_j - 1)$ is even and must divide the product on the left-hand side. But there can be at most one factor of 2 on the left-hand side and it is accounted for by the factor of 2 in front of the product on the right-hand side. Therefore, no odd primes appear in the product. That is, $n = 2^j$ for some j.

21. Because $(m, n) = p$, p divides one of the terms, say, n, exactly once, so $n = kp$ with $(m, k) = 1 = (n, k)$. Then $\phi(n) = \phi(kp) = \phi(k)\phi(p) = \phi(k)(p-1)$, and $\phi(mp) = p\phi(m)$ by the formula in Example 7.7. Then $\phi(mn) = \phi(mkp) = \phi(mp)\phi(k) = (p\phi(m))(\phi(n)/(p-1))$.

23. Let $p_1, \cdots, p_r$ be those primes dividing a but not b. Let $q_1, \cdots, q_s$ be those primes dividing b but not a. Let $r_1, \cdots r_t$ be those primes dividing a and b. Let $P = \prod(1 - \frac{1}{p_i})$, $Q = \prod(1 - \frac{1}{q_i})$ and $R = \prod(1 - \frac{1}{r_i})$. Then we have $\phi(ab) = abPQR = \frac{aPRbQR}{R} = \frac{\phi(a)\phi(b)}{R}$. But $\phi((a, b)) = (a, b)R$, so $R = \frac{\phi((a,b))}{(a,b)}$ and we have $\phi(ab) = \frac{\phi(a)\phi(b)}{R} = \frac{(a,b)\phi(a)\phi(b)}{\phi((a,b))}$, as desired. The final conclusion now follows from the fact that $\phi((a, b)) < (a, b)$ when $(a, b) > 1$.

25. Assume there are only finitely many primes, $2, 3, \ldots, p$. Let $N = 2 \cdot 3 \cdot 5 \cdots p$. Then $\phi(N) = 1$ because there is exactly one positive integer less than N that is relatively prime to N, namely, 1, because every prime is a factor of N. However, $\phi(N) = \phi(2)\phi(3)\phi(5) \cdots \phi(p) = 1 \cdot 2 \cdot 4 \cdots (p-1) > 1$. This contradiction shows that there are infinitely many primes.

27. From the formula for the ϕ function, we see that if $p|n$, then $p - 1|k$. Because k has only finitely many divisors, there are only finitely many possibilities for prime divisors of n. Further, if p is prime and $p^a|n$, then $p^{a-1}|k$. Hence, $a \leq \log_p(k) + 1$. Therefore, each of the finitely many primes which might divide n may appear to only finitely many exponents. Therefore, there are only finitely many possibilities for n.

29. As suggested, we take $k = 2 \cdot 3^{6j+1}$ with $j \geq 1$, and suppose that $\phi(n) = k$. From the formula for $\phi(n)$, we see that $\phi(n)$ has a factor of $(p-1)$, which is even, for every odd prime that divides n. Because there is only one factor of 2 in k, there is at most one odd prime divisor of n. Because k is not a power of 2, we know that an odd prime p must divide n. Further, because $2 \parallel k$, we know that $4 \nmid n$. So n is of the form p^a or $2p^a$. Recall that $\phi(p^a) = \phi(2p^a)$. It remains to discover the value of p. If $a = 1$, then $\phi(p^a) = p - 1 = 2 \cdot 3^{6j+1}$. But then $p = 2 \cdot 3^{6j+1} + 1 \equiv 6 \cdot (3^6)^j + 1 \equiv (-1)(1)^j + 1 \equiv 0 \pmod 7$. Hence, $p = 7$. But $\phi(7) = 6 = 2 \cdot 3^{6j+1}$ implies that $j = 0$, contrary to hypothesis, so this is not a solution. Therefore, $a > 1$ and we have $\phi(p^a) = (p-1)p^{a-1} = 2 \cdot 3^{6j+1}$, from which we conclude that $p = 3$ and $a = 6j + 2$. Therefore, the only solutions are $n = p^{6j+2}$ and $n = 2p^{6j+2}$.

31. If $n = p^r m$, then $\phi(p^r m) = (p^r - p^{r-1})\phi(m) \mid (p^r m - 1)$, and hence $p \mid 1$ or $r = 1$. So n is square-free. If $n = pq$, then $\phi(pq) = (p-1)(q-1) \mid (pq - 1)$. Then $(p-1) \mid (pq-1) - (p-1)q = q - 1$. Similarly, $(q-1) \mid (p-1)$, a contradiction.

33. Let $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$. Let P_i be the property that an integer is divisible by p_i. Let S be the set $\{1, 2, \ldots, n-1\}$. To compute $\phi(n)$, we need to count the elements of S with more of the properties $P_1, P_2, \cdots, P_k$. Let $n(P_{i_1}, P_{i_2}, \cdots, P_{i_m})$ be the number of elements of S with all of properties $P_{i_1}, P_{i_2}, \cdots, P_{i_m}$. Then $n(P_{i_1}, \cdots P_{i_m}) = \frac{n}{p_{i_1} p_{i_2} \cdots p_{i_m}}$. By Exercise 24 of Section 3.1, we have $\phi(n) = n - (\frac{n}{p_1} + \frac{n}{p_2} + \cdots + \frac{n}{p_k}) + (\frac{n}{p_1 p_2} + \cdots + \frac{n}{p_{k-1} p_k}) + \cdots + (-1)^k (\frac{n}{p_1 \cdots p_k}) = n(1 - \sum_{p_i|n} \frac{1}{p_i} + \sum_{p_{i_1} p_{i_2} | n} \frac{1}{p_{i_1} p_{i_2}} - \sum_{p_{i_1} p_{i_2} p_{i_3}} \frac{1}{p_{i_1} p_{i_2} p_{i_3}} + \cdots + (-1)^k \frac{n}{p_1 \cdots p_k})$. On the other hand, notice that each term in the expansion of $(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \cdots (1 - \frac{1}{p_k})$ is obtained by choosing either 1 or $-\frac{1}{p_i}$ from each factor and multiplying the choices together. This gives each term the form $\frac{(-1)^m}{p_{i_1} p_{i_2} \cdots p_{i_m}}$. Note that each term can occur in only one way. Thus, $n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \cdots (1 - \frac{1}{p_k}) = n(1 - \sum_{p_i|n} \frac{1}{p_i} + \sum_{p_{i_1} p_{i_2}} \frac{1}{p_{i_1} p_{i_2}} - \cdots (-1)^k \frac{n}{p_1 \cdots p_k}) = \phi(n)$.

35. Note that $1 \leq \phi(m) \leq m - 1$ for $m > 1$. Hence if $n \geq 2$, $n > n_1 > n_2 > \cdots \geq 1$ where $n_i = \phi(n)$ and $n_i = \phi(n_{i-1})$ for $i > 1$. Because n_i, $i = 1, 2, 3, \ldots$ is a decreasing sequence of positive integers, there must be a positive integer r such that $n_r = 1$.

37. Note that the definition of $f * g$ can also be expressed as $(f * g)(n) = \sum_{a \cdot b = n} f(a)g(b)$. Then the fact that $f * g = g * f$ is evident.

39. **a.** If either $m > 1$ or $n > 1$, then $mn > 1$ and one of $\iota(m)$ or $\iota(n)$ is equal to zero. Then $\iota(mn) = 0 = \iota(m)\iota(n)$. Otherwise, $m = n = 1$ and we have $\iota(mn) = 1 = 1 \cdot 1 = \iota(m)\iota(n)$. Therefore, $\iota(n)$ is multiplicative. **b.** $(\iota * f)(n) = \sum_{d|n} \iota(d) f(\frac{n}{d}) = \iota(1) f(\frac{n}{1}) = f(n)$ because $\iota(d) = 0$ except when $d = 1$.$(f * \iota)(n) = (\iota * f)(n) = f(n)$ by Exercise 37.

41. Let $h = f * g$ and let $(m, n) = 1$. Then $h(mn) = \sum_{d|mn} f(d)g(\frac{mn}{d})$. Because $(m, n) = 1$, each divisor d of mn can be expressed in exactly one way as $d = ab$ where $a \mid m$ and $b \mid n$. Then $(a, b) = 1$ and $(\frac{m}{a}, \frac{n}{b}) = 1$. Then there is a one-to-one correspondence between the divisors d of mn and the pairs of products ab where $a \mid m$ and $b \mid n$. Then

$$h(mn) = \sum_{\substack{a|m \\ b|n}} f(ab)g(\frac{mn}{ab}) = \sum_{\substack{a|m \\ b|n}} f(a)f(b)g(\frac{m}{a})g(\frac{n}{b})$$

$$= \sum_{a|m} f(a)g(\frac{m}{a}) \sum_{b|n} f(b)g(\frac{n}{b}) = h(m)h(n),$$

as desired.

43. **a.** -1 **b.** -1 **c.** 1 **d.** 1 **e.** -1 **f.** -1 **g.** 1

45. Let $f(n) = \sum_{d|n} \lambda(d)$. Suppose $p^t \parallel n$. Then $f(p^t) = \lambda(1) + \lambda(p) + \lambda(p^2) + \cdots + \lambda(p^t) = 1 - 1 + 1 - \cdots + (-1)^t = 0$ if t is odd and equal to 1 if t is even. Note that $f(n) = f(p^t b) = \sum_{d|n} \lambda(d) = \sum_{e|b} \lambda(e)(\lambda(1) + \lambda(p) + \cdots \lambda(p^t)) = f(b)f(p^t)$. By induction, this shows that f is multiplicative. Then $f(n) = f(p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}) = \prod f(p_i^{a_i}) = 0$ if any a_i is odd (n is not a square) and equal to 1 if all a_i are even (n is a square).

47. If f and g are completely multiplicative and m and n are positive integers, then we have $(fg)(mn) = f(mn)g(mn) = f(m)f(n)g(m)g(n) = f(m)g(m)f(n)g(n) = (fg)(m)(fg)(n)$, so fg is also completely multiplicative.

49. $f(mn) = \log mn = \log m + \log n = f(m) + f(n)$

51. **a.** 2 **b.** 3 **c.** 1 **d.** 4 **e.** 8 **f.** 15

53. Let $(m, n) = 1$. Then by the additivity of f, we have $f(mn) = f(m) + f(n)$. Then $g(mn) = 2^{f(mn)} = 2^{f(m)+f(n)} = 2^{f(m)}2^{f(n)} = g(m)g(n)$.

Section 7.2

1. **a.** 48 **b.** 399 **c.** 2340 **d.** $2^{101} - 1$ **e.** 6912 **f.** 813, 404, 592 **g.** 15, 334, 088 **h.** 13, 891, 399, 238, 731, 734, 720

3. perfect squares

5. **a.** 6, 11 **b.** 10, 17 **c.** 14, 15, 23 **d.** 33, 35, 47 **e.** none **f.** 44, 65, 83

7. Note that $\tau(p^{k-1}) = k$ whenever p is prime and k is a positive integer $k > 1$. Hence, the equation $\tau(n) = k$ has infinitely many solutions.

9. squares of primes

11. $n^{\tau(n)/2}$

13. **a.** The nth term is $\sigma(2n)$. **b.** The nth term is $\sigma(n) - \tau(n)$. **c.** The nth term is the least positive integer m with $\tau(m) = n$. **d.** The nth term is the number of solutions k to the equation $\sigma(k) = n$.

15. 2, 4, 6, 12, 24, 36

17. Let a be the largest highly composite integer less than or equal to n. Note that $2a$ is less than or equal to $2n$ and has more divisors than a, and hence $\tau(2a) > \tau(a)$. By Exercise 16, there must be a highly composite integer b with $a < b \leq 2a$. If $b \leq n$, this contradicts the choice of a. Therefore, $n < b \leq 2n$. It follows that there must be a highly composite integer k with $2^m < k \leq 2^{m+1}$ for every nonnegative integer m. Therefore, there are at least m highly composite integers less than or equal to 2^m. Thus, the mth highly composite integer is less than or equal to 2^m.

19. 1, 2, 4, 6, 12, 24, 36, 48

21. $1 + p^k$

23. Suppose that a and b are positive integers with $(a, b) = 1$. Then $\sum_{d|ab} d^k = \sum_{d_1|a, d_2|b} (d_1 d_2)^k = \sum_{d_2|a} d_1^k \sum_{d_2|a} d_2^k = \sigma_k(a)\sigma_k(b)$.

25. prime numbers

27. Let $n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$ and let x and y be integers such that $[x, y] = n$. Then $x \mid n$ and $y \mid n$, so we have $x = p_1^{b_1} p_2^{b_2} \cdots p_r^{b_r}$ and $y = p_1^{c_1} p_2^{c_2} \cdots p_r^{c_r}$, where b_i and $c_i = 0, 1, 2, \ldots, a_i$. Because $[x, y] = n$, we must have $\max\{b_i, c_i\} = a_i$ for each i. Then one of b_i and c_i must be equal to a_i and the other can range over $0, 1, \ldots, a_i$. Therefore, we have $2a_i + 1$ ways to choose the pair (b_i, c_i) for each i. Then in total, we can choose the exponents $b_1, b_2, \ldots b_r, c_1, \ldots, c_r$ in $(2a_1 + 1)(2a_2 + 1) \cdots (2a_r + 1) = \tau(n^2)$ ways.

29. Suppose that n is composite. Then $n = ab$ where a and b are integers with $1 < a \le b < n$. It follows that either $a \ge \sqrt{n}$ or $b \ge \sqrt{n}$. Consequently, $\sigma(n) \ge 1 + a + b + n > 1 + \sqrt{n} + n > n + \sqrt{n}$. Conversely, suppose that n is prime. Then $\sigma(n) = n + 1$ so that $\sigma(n) \le n + \sqrt{n}$. Hence, $\sigma(n) > n + \sqrt{n}$ implies that n is composite.

31. For $n = 1$, the statement is true. Suppose that $\sum_{j=1}^{n-1} \tau(j) = 2 \sum_{j=1}^{[\sqrt{n-1}]} \left[\frac{n-1}{j}\right] - [\sqrt{n-1}]^2$. For the induction step, it suffices to show that $\tau(n) = 2 \sum_{j=1}^{[\sqrt{n-1}]} \left(\left[\frac{n}{j}\right] - \left[\frac{n-1}{j}\right]\right) = 2 \sum_{\substack{j \le [\sqrt{n-1}] \\ j \mid n}} 1$, which is true by the definition of $\tau(n)$, because there is one factor less than $\sqrt{n}$ for every factor greater than $\sqrt{n}$. Note that if n is a perfect square, we must add the term $2\sqrt{n} - (2\sqrt{n} - 1) = 1$ to the last two sums. For $n = 100$, we have $\sum_{j=1}^{100} \tau(j) = 2 \sum_{j=1}^{10} \left[\frac{n}{j}\right] - 100 = 482$.

33. Let $a = \sum p_i^{a_i}$ and $b = \sum p_i^{b_i}$ and let $c_i = \min(a_i, b_i)$ for each i. We first prove that the product $\prod_{p_i} \sum_{j=0}^{c_i} p_i^j \sigma(p_i^{a_i + b_i - 2j}) = \sum_{d \mid (a,b)} d\sigma(ab/d^2)$. To see this, let d be any divisor of (a, b), say, $d = \prod_{p_i} d_i$. Then $d_i \le c_i$ for each i, so each of the terms $p_i^{d_i} \sigma(p_i^{a_i + b_i - 2d_i})$ appears in exactly one of the sums in the product. Therefore, if we expand the product, we will find, exactly once, the term $\prod_{p_i} p_i^{d_i} \sigma(p_i^{a_i + b_i - 2d_i}) = d\sigma\left(\prod_{p_i} p_i^{a_i + b_i - 2d_i}\right) = d\sigma\left(\prod_{p_i} (p_i^{a_i}/p_i^{d_i})(p_i^{b_i}/p_i^{d_i})\right) = d\sigma((a/d)(b/d))$. This proves the first identity. Next, consider the sum $\sum_{j=0}^{c} (p^{a+b-j} + p^{a+b-j-1} + \cdots + p^j)$, where $c = \min(a, b)$. The term p^k appears in this sum once each time that $k = a + b - j$, which happens exactly when $a + b - c \le k \le a + b$, that is, $c + 1$ times. On the other hand, in the expansion of the product $(p^a + p^{a-1} + \cdots + 1)(p^b + p^{b-1} + \cdots + 1) = \sigma(p^a)\sigma(p^b)$, the same term p^k appears whenever $k = (a - m) + (b - n)$, where $0 \le m \le a$ and $0 \le n \le b$. Each of m and n determines the other, so p^k appears exactly $\min(a + 1, b + 1) = c + 1$ times. Given this identity, we have $\sigma(a)\sigma(b) = \prod_{p_i} (p_i^{a_i} + p_i^{a_i - 1} + \cdots + 1)(p_i^{b_i} + p_i^{b_i - 1} + \cdots + 1) = \prod_{p_i} \sum_{j=0}^{c_i} (p_i^{a_i + b_i - j} + p_i^{a_i + b_i - j - 1} + \cdots + p_i^j)$, which is the right side of the identity, as we proved above.

35. From Exercises 52 and 53 in Section 7.1, we know that the arithmetic function $f(n) = 2^{\omega(n)}$ is multiplicative. Further, because the Dirichlet product $h(n) = \sum_{d \mid n} 2^{\omega(d)} = f * g(n)$, where $g(n) = 1$ is also multiplicative, we know that $h(n)$ is also multiplicative. See Exercise 41 in Section 7.1. Because $\tau(n)$ and n^2 are multiplicative, so is $\tau(n^2)$. Therefore, it sufficient to prove the identity for n equal to a prime power, p^a. We have $\tau(p^{2a}) = (2a + 1)$. On the other hand, we have $\sum_{d \mid p^a} 2^{\omega(d)} = \sum_{i=0}^{a} 2^{\omega(p^i)} = 1 + \sum_{i=1}^{a} 2^1 = 2a + 1$.

37. $\phi(1)\phi(2) \cdots \phi(n)$

39. If p and $p + 2$ are prime, then $\sigma(p) = p + 1 = \phi(p + 2)$. If $2^p - 1$ is prime, then $\phi(2^{p+1}) = 2^p = \sigma(2^p - 1)$.

Section 7.3

1. 6; 28; 496; 8128; 33,550,336; 8,589,869,056

3. **a.** 31 **b.** 127 **c.** 127

5. 12, 18, 20, 24, 30, 36

7. Suppose that $n = p^k$ where p is prime and k is a positive integer. Then $\sigma(p^k) = \frac{p^{k+1}-1}{p-1}$. Note that $2p^k - 1 < p^{k+1}$ because $p \geq 2$. It follows that $p^{k+1} - 1 < 2(p^{k+1} - p^k) = 2p^k(p-1)$, so that $\frac{(p^{k+1}-1)}{p-1} < 2p^k = 2n$. It follows that $n = p^k$ is deficient.

9. Suppose that n is abundant or perfect. Then $\sigma(n) \geq 2n$. Suppose that $n \mid m$. Then $m = nk$ for some integer k. The divisors of m include the integers kd and $d \mid n$. Hence, $\sigma(m) \geq \sum_{d|n}(k+1)d = (k+1)\sum_{d|n} d = (k+1)\sigma(n) \geq (k+1)2n > 2kn = 2m$. Hence, m is abundant.

11. If p is any prime, then $\sigma(p) = p + 1 < 2p$, so p is deficient. Because there are infinitely many primes, we must have infinitely many deficient numbers.

13. See Exercises 6 and 9 for an alternate solution. For a positive integer a, let $n = 3^a 5 \cdot 7$ and compute $\sigma(n) = \sigma(3^a 5 \cdot 7) = (3^{a+1} - 1)/(3-1)(5+1)(7+1) = (3^{a+1} - 1)24 = 3^{a+1}24 - 24 = 2 \cdot 3^a(36) - 24 = 2 \cdot 3^a(35) + 2 \cdot 3^a - 24 = 2n + 2 \cdot 3^a - 24$, which will be greater than $2n$ whenever $a \geq 3$. This demonstrates infinitely many odd abundant integers.

15. **a.** The prime factorizations of 220 and 284 are $220 = 2^2 \cdot 5 \cdot 11$ and $284 = 2^2 \cdot 71$. Hence, $\sigma(220) = \sigma(2^2)\sigma(5)\sigma(11) = 7 \cdot 6 \cdot 12 = 504$ and $\sigma(284) = \sigma(2^2)\sigma(71) = 7 \cdot 72 = 504$. Because $\sigma(220) = \sigma(284) = 220 + 284 = 504$, it follows that 220 and 284 form an amicable pair. **b.** The prime factorizations of 1184 and 1210 are $1184 = 2^5 \cdot 37$ and $1210 = 2 \cdot 5 \cdot 11^2$. Hence, $\sigma(1184) = \sigma(2^5)\sigma(37) = 63 \cdot 38 = 2394$ and $\sigma(1210) = \sigma(2)\sigma(5)\sigma(11^2) = 3 \cdot 6 \cdot 133 = 2394$. Because $\sigma(1184) = \sigma(1210) = 1184 + 1210 = 2394$, 1184 and 1210 form an amicable pair. **c.** The prime factorizations of 79,750 and 88,730 are $79{,}750 = 2 \cdot 5^3 \cdot 11 \cdot 29$ and $88{,}730 = 2 \cdot 5 \cdot 19 \cdot 467$. Hence, $\sigma(79{,}750) + \sigma(2)\sigma(5^3)\sigma(11)\sigma(29) = 3 \cdot 156 \cdot 12 \cdot 30 = 168{,}480$ and similarly $\sigma(88{,}730) = \sigma(2)\sigma(5)\sigma(19)\sigma(467) = 3 \cdot \cdot 6 \cdot 20 \cdot 468 = 168{,}480$. Because $\sigma(79{,}750) = \sigma(88{,}730) = 79{,}750 + 88{,}730 = 168{,}480$, it follows that 79,750 and 88,730 form an amicable pair.

17. $\sigma(120) = \sigma(2^3 \cdot 3 \cdot 5) = \sigma(2^3)\sigma(3)\sigma(5) = 15 \cdot 4 \cdot 6 = 360 = 3 \cdot 120$

19. $\sigma(2^7 3^4 5 \cdot 7 \cdot 11^2 \cdot 17 \cdot 19) = \frac{2^8-1}{2-1} \cdot \frac{3^5-1}{3-1}(5+1)(7+1)\frac{11^3-1}{11-1}(17+1)(19+1) = 255 \cdot 121 \cdot 6 \cdot 8 \cdot 133 \cdot 18 \cdot 20 = 5 \cdot 14{,}182{,}439{,}040$.

21. Suppose that n is 3-perfect and 3 does not divide n. Then $\sigma(3n) = \sigma(3)\sigma(n) = 4 \cdot 3n$. Hence, $3n$ is 4-perfect.

23. 908,107,200

25. $\sigma(\sigma(16)) = \sigma(31) = 32 = 2 \cdot 16$

27. Certainly if r and s are integers, then $\sigma(rs) \geq rs + r + s + 1$. Suppose $n = 2^q t$ is superperfect with t odd and $t > 1$. Then $2n = 2^{q+1}t = \sigma\ (\sigma(2^q t)) = \sigma\left(\left(2^{q+1} - 1\right)\sigma(t)\right) \geq (2^{q+1} - 1)\sigma(t) + (2^{q+1} - 1) + \sigma(t) + 1 > 2^{q+1}\sigma(t) \geq 2^{q+t}(t+1)$. Then $t > t + 1$, a contradiction. Therefore, we must have $n = 2^q$, in which case we have $2n = 2^{q+1} = \sigma\ (\sigma(2^q)) = \sigma\left(2^{q+1} - 1\right) = \sigma(2n - 1)$. Therefore, $2n - 1 = 2^{q+1} - 1$ is prime.

29. **a.** yes **b.** no **c.** yes **d.** no

31. $M_n(M_n + 2) = (2^n - 1)(2^n + 1) = 2^{2n} - 1$. If $2n + 1$ is prime, then $\phi(2n+1) = 2n$ and $2^{2n} \equiv 1 \pmod{2n+1}$. Then $(2n+1) \mid 2^{2n} - 1 = M_n(M_n + 2)$. Therefore, $(2n+1) \mid M_n$ or $(2n+1) \mid (M_n + 2)$.

33. Because m is odd, $m^2 \equiv 1 \pmod 8$, so $n = p^a m^2 \equiv p^a \pmod 8$. By Exercise 32 (a), $a \equiv 1 \pmod 4$, so $p^a \equiv p^{4k} p \equiv p \pmod 8$, because p^{4k} is an odd square. Therefore, $n = p \pmod 8$.

35. First suppose that $n = p^a$ where p is prime and a is a positive integer. Then $\sigma(n) = \frac{p^{a+1}-1}{p-1} < \frac{p^{a+1}}{p-1} = \frac{np}{p-1} = \frac{n}{1-\frac{1}{p}} \leq \frac{n}{\frac{2}{3}} = \frac{3n}{2}$ so that $\sigma(n) \neq 2n$ and n is not perfect. Next suppose that $n = p^a q^b$ where a and b are primes and a and b are positive integers. Then $\sigma(n) = \frac{p^{a+1}-1}{p-1} \cdot \frac{q^{b+1}-1}{q-1} <$

$\frac{p^{a+1}q^{b+1}}{(p-1)(q-1)} = \frac{npq}{(p-1)(q-1)} = \frac{n}{(1-\frac{1}{p})(1-\frac{1}{q})} \leq \frac{n}{(\frac{2}{3})(\frac{4}{5})} = \frac{15n}{8} < 2n$. Hence, $\sigma(n) \neq 2n$ and n is not perfect.

37. integers of the form p^5 and p^2q where p and q are primes.

39. Suppose $M_n = 2^n - 1 = a^k$, with n and k integers greater than 1. Then a must be odd. If $k = 2j$, then $2^n - 1 = (a^j)^2$. Because $n > 1$ and the square of an odd integer is congruent to 1 modulo 4, reduction of the last equation modulo 4 yields the contradiction $-1 \equiv 1 \pmod 4$; therefore, k must be odd. Then $2^n = a^k + 1 = (a+1)(a^{k-1} - a^{k-2} + \cdots + 1)$. So $a + 1 = 2^m$ for some integer m. Then $2^n - 1 = (2^m - 1)^k$. Now $n > mk$ so reduction modulo 2^{2m} gives $-1 \equiv k2^m - 1 \pmod{2^{2m}}$ or, because k is odd, $2^m \equiv 0 \pmod{2^{2m}}$, a contradiction.

Section 7.4

1. **a.** 0 **b.** 1 **c.** -1 **d.** 0 **e.** -1 **f.** 1 **g.** 0

3. 0, -1, -1, -1, 0, -1, 1, -1, 0, -1, -1, respectively

5. 1, 6, 10, 14, 15, 21, 22, 26, 33, 34, 35, 38, 39, 46, 51, 55, 57, 58, 62, 65, 69, 74, 77, 82, 85, 86, 87, 91, 93, 94, 95

7. 1, 0, -1, -1, -2, -1, -2, -2, -2, -1, respectively

9. Because $\mu(n)$ is 0 for nonsquarefree n, 1 for n a product of an even number of distinct primes and -1 for n a product of a odd number of distinct primes, the sum $M(n) = \sum_{i=1}^{n} \mu(i)$ is unaffected by the nonsquarefree numbers, but counts 1 for every even product and -1 for every odd product. Thus, $M(n)$ counts how many more even products than odd products there are.

11. For any nonnegative integer k, the numbers $n = 36k + 8$ and $n + 1 = 36k + 9$ are consecutive and divisible by $4 = 2^2$ and $9 = 3^2$, respectively. Therefore, $\mu(36k + 8) + \mu(36k + 9) = 0 + 0 = 0$.

13. 3

15. Let $h(n) = n$ be the identity function. Then from Theorem 7.7, we have $h(n) = n = \sum_{d|n} \phi(n)$. Then by the Möbius inversion formula, we have $\phi(n) = \sum_{d|n} \mu(d)h(n/d) = \sum_{d|n} \mu(d)(n/d) = n \sum_{d|n} \mu(d)/d$.

17. Because μ and f are multiplicative, then so is their product, μf, by Exercise 46 of Section 7.1. Further, the summatory function $\sum_{d|n} \mu(d)f(d)$ is also multiplicative by Theorem 7.17. Therefore, it suffices to prove the proposition for n a prime power. We compute $\sum_{d|p^a} \mu(d)f(d) = \mu(p^a)f(p^a) + \mu(p^{a-1})f(p^{a-1}) + \cdots + \mu(p)f(p) + \mu(1)f(d)$. But for exponents greater than 1, $\mu(p^j) = 0$, so the above sum equals $\mu(p)f(p) + \mu(1)f(1) = -f(p) + 1$.

19. $\phi(n)/n$

21. $(-1)^k \prod_{i=1}^{k} p_i$

23. Because both sides of the equation are known to be multiplicative (see Exercise 35 in Section 7.2), it suffices to prove the identity for $n = p^a$, a prime power. On one hand, we have $\sum_{d|p^a} \mu^2(d) = \mu^2(p) + \mu^2(1) = 1 + 1 = 2$. On the other hand, we have $\omega(p^a) = 1$, so the right side is $2^1 = 2$.

25. Let λ play the role of f in the identity of Exercise 17. Then the left side equals $\prod_{j=1}^{k}(1 - \lambda(p_j)) = \prod_{j=1}^{k}(1 - (-1)) = 2^k = 2^{\omega(n)}$.

27. We compute $\mu * \nu(n) = \sum_{d|n} \mu(d)\nu(n/d) = \sum_{d|n} \mu(d) = \iota(n)$, by Theorem 7.15.

29. Because $\nu(n)$ is identically 1, we have $F(n) = \sum_{d|n} f(d) = \sum_{d|n} f(d)\nu(n/d) = f * \nu(n)$. If we Dirichlet multiply both sides by μ, we have $F * \mu = f * \nu * \mu = f * \iota = f$.

31. From the Möbius inversion formula, we have $\Lambda(n) = \sum_{d|n} \mu(d) \log(n/d) = \sum_{d|n} \mu(d)(\log n - \log d) = \sum_{d|n} \mu(d) \log(n) - \sum_{d|n} \mu(d) \log(d) = \log n \sum_{d|n} \mu(d) - \sum_{d|n} \mu(d) \log(d) = \log n \nu(n) - \sum_{d|n} \mu(d) \log(d) = -\sum_{d|n} \mu(d) \log(d)$, because $\nu(n) = 0$ if n is not 1, and $\log n = 0$ if $n = 1$.

33. **a.** Let k be an integer in the range $0 \le k \le n-1$, and let $d = (k, n)$, so that $n = dj$ for some integer j. If ζ is a primitive nth root of unity, we have $\zeta^n = (\zeta^d)^j = 1$, so ζ^d is a jth root of unity. If ζ^d were not a primitive jth root of unity, then $1 = (\zeta^d)^b = \zeta^{db}$ with $db < dj = n$, contradicting the assumption that ζ is a primitive nth root of unity. So $\Pi_{(k,n)=d}(x - (\zeta^d)^k) = \Phi_j(x)$ as the product runs through a complete set of reduced residues modulo j. It remains to note that $x^n - 1 = \Pi_{k=0}^{n-1}(x - \zeta^k)$ because both polynomials have the same degree and the same roots. The last product equals $\Pi_{d|n}\Pi_{(k,n)=d}(x - (\zeta^d)^k) = \Pi_{d|n}\Phi_j(x)$. **b.** From part (a), we have $x^p - 1 = \prod_{d|p} \Phi_d(x) = \Phi_1(x)\Phi_p(x) = (1-x)\Phi_p(x)$. Then $\Phi_p(x) = (x^p - 1)/(x - 1) = x^{p-1} + x^{p-2} + \cdots + x + 1$. **c.** From part (b), we have $x^{2p} = \prod_{d|2p} \Phi_d(x) = \Phi_1(x)\Phi_2(x)\Phi_p(x)\Phi_{2p}(x)$. Because $\Phi_1(x) = x - 1$, $\Phi_2(x) = x + 1$, and $\Phi_p(x) = (x^p - 1)/(x - 1)$, from part (b), we compute $\Phi_{2p}(x) =$

$$\frac{x^{2p} - 1}{(x-1)(x+1)(x^p - 1)/(x-1)} = \frac{(x^p - 1)(x^p + 1)}{(x+1)(x^p - 1)} = \frac{x^p + 1}{x + 1} = x^{p-1} - x^{p-2} + \cdots - x + 1.$$

35. We need a little lemma: Let $f(x)$ and $g(x)$ be monic polynomials with rational coefficients. If $f(x)g(x)$ has integer coefficients, then so do $f(x)$ and $g(x)$. Proof: Let $f(x) = x^m + a_{m-1}x^{m-1} + \cdots + a_0$ and $g(x) = x^n + b_{n-1}x^{n-1} + \cdots + b_0$, and let M and N be the smallest positive integers such that $Mf(x)$ and $Ng(x)$ have integer coefficients. Then all coefficients of $MNf(x)g(x)$ are divisible by MN, because $f(x)g(x)$ is an integer polynomial. Let p be a prime divisor of MN. If $p \nmid M$, then p doesn't divide the leading coefficient of $Mf(x)$. If $p \mid M$, then some coefficient Ma_i is not divisible by p, otherwise this would contradict the minimality of M. Let I be the largest index such that Ma_I is not divisible by p. Similarly, let J be the largest index such that Nb_J is not divisible by p. (In both cases, we take $a_m = b_n = 1$.) Then the coefficient of x^{I+J} in $MNf(x)g(x)$ is $Ma_INb_J + R$ where R is a sum of products involving Ma_i and Nb_j with either $i > I$ or $j > J$, and hence $p \mid R$ and therefore $p \nmid Ma_INb_J + R$. But this contradicts that p divides the coefficients of $MNf(x)g(x)$. This proves the lemma. Now, from Exercise 34, we have $\Phi_n(x) = \prod_{d|n}(x^d - 1)^{\mu(n/d)}$. Let $P(x)$ be the product of those factors for which $\mu(n/d) = -1$, and let $Q(x)$ be the product of those factors for which $\mu(n/d) = 1$. Then we have $P(x)\Phi_n(x) = Q(x)$. Because $Q(x)$ has integer coefficients, so does $\Phi_n(x)$, by the lemma.

Section 7.5

1. **a.** (2), (1, 1); $p(2) = 2$ **b.** (4), (3, 1), (2, 2), (2, 1, 1), (1, 1, 1, 1); $p(4) = 5$ **c.** (6), (5, 1), (4, 2), (4, 1, 1), (3, 3), (3, 2, 1), (3, 1, 1, 1), (2, 2, 2), (2, 2, 1, 1), (2, 1, 1, 1, 1), (1, 1, 1, 1, 1, 1); $p(6) = 11$ **d.** (9), (8, 1), (7, 2), (7, 1, 1), (6, 3), (6, 2, 1), (6, 1, 1, 1), (5, 4), (5, 3, 1), (5, 2, 2), (5, 2, 1, 1), (5, 1, 1, 1, 1), (4, 4, 1), (4, 3, 2), (4, 3, 1, 1), (4, 2, 2, 1), (4, 2, 1, 1, 1), (4, 1, 1, 1, 1, 1), (3, 3, 3), (3, 3, 2, 1), (3, 3, 1, 1, 1), (3, 2, 2, 2), (3, 2, 2, 1, 1), (3, 2, 1, 1, 1, 1), (3, 1, 1, 1, 1, 1, 1), (2, 2, 2, 2, 1), (2, 2, 2, 1, 1, 1), (2, 2, 1, 1, 1, 1, 1), (2, 1, 1, 1, 1, 1, 1, 1), (1, 1, 1, 1, 1, 1, 1, 1, 1); $p(9) = 30$

3. $p_O(6) = 4$, $p^D(6) = 4$, $p_2(6) = 4$

5. **a.** 8 **b.** 0 **c.** 4 **d.** 7 **e.** 8 **f.** 2 **g.** 4 **h.** 2

7. Let n be a positive integer and let A be the set of all partitions of n. Then there are $p(n)$ elements in A. Create subsets of A, named $A_1, A_2, \ldots, A_n$, as follows. For each partition in A, count the number of parts. If the number of parts is k, put the partition in A_k. Then the number of elements in A_k will be $p(n, k)$. Because every partition of n has between 1 and n parts, all partitions go into

exactly one subset. Further, any two distinct subsets must be disjoint, so A is the disjoint union of the A_k. Thus, $p(n) = |A| = |A_1| + |A_2| + \cdots + |A_n| = \sum_{k=1}^{n} p(n, k)$.

9. $p(5, 1) = 1$, $p(5, 2) = 2$, $p(5, 3) = 2$, $p(5, 4) = 1$, $p(5, 5) = 1$. Then $1 + 2 + 2 + 1 + 1 = 7 = p(5)$.

11. $[n/2]$ (greatest integer function)

13. **a.** (5, 4, 2, 2, 1, 1), not self-conjugate **b.** (2, 2, 2, 2, 2, 2, 2, 1), not self-conjugate
c. (7, 4, 3, 1), not self-conjugate **d.** (10, 5), not self-conjugate

15. (8, 1, 1, 1, 1, 1, 1, 1), (6, 3, 3, 1, 1, 1), (5, 4, 3, 2, 1), (4, 4, 4, 3)

17. Let m and n be integers with $1 \leq m \leq n$. If P is a partition of n into at most m parts, then the Ferrers diagram with have at most m rows. Let Q be the conjugate of P. Then the Ferrers diagram for Q will have at most m columns, and hence represents a partition of n into parts not greater than m. Therefore, $p(n \mid \text{at most } m \text{ parts}) \leq p(n \mid \text{parts no greater than } m)$. Conversely, suppose Q is a partition of n into parts no greater than m. Then the Ferrers diagram of Q has at most m columns. If P is the conjugate of Q, then the Ferrers diagram for P has at most m rows, and hence represents a partition of n into parts no greater than m. Therefore, $p(n \mid \text{parts no greater than } m) \leq p(n \mid \text{at most } m \text{ parts})$. The two inequalities together prove the assertion.

19. $\prod_{k=1}^{\infty}(1 + x^{2^k}) = \sum_{n=1}^{\infty} x^n = 1/(1 - x)$

21. $\prod_{k=1}^{\infty}(1 + x^{2k})/(1 - x^{2k-1})$; 1, 2, 3, 4, 6, 12, 16, 22, 29

23. $\prod_{k=1}^{\infty}(1 - x^{dk})/(1 - x^k)$; 1, 2, 3, 4, 6, 12, 16, 22, 29

25. $\prod_{k=1}^{\infty}(1 - x^{k^2})/(1 - x^k)$: 0, 1, 1, 1, 2, 3, 3, 5, 5, 8

27. From the formula for the sum of a finite geometric series, we have $(1 - x^{(d+1)k})/(1 - x^k) = 1 + x^k + x^{2k} + \cdots + x^{dk}$. From Exercise 23, the generating function for $p_{\{k \mid d \nmid k+1\}}(n)$ is $\prod_{k=1}^{\infty}(1 - x^{d(k+1)})/(1 - x^k) = \prod_{k=1}^{\infty}(1 + x^k + x^{2k} + \cdots + x^{dk})$. But this last expression is the generating function for $p(n|\text{no part appears more than } d \text{ times})$ as found in Exercise 22.

29. **a.** The generating function for $p(n|\text{no part equals 1})$ is, by Theorem 7.21, $\prod_{k=2}^{\infty} 1/(1 - x^k) = (1 - x)\prod_{k=1}^{\infty} 1/(1 - x^k) = \prod_{k=1}^{\infty} 1/(1 - x^k) - x\prod_{k=1}^{\infty} 1/(1 - x^k)$. The coefficient of x^n in the first product is $p(n)$. The coefficient of x^n in the second product is $p(n - 1)$, because of the extra factor of x in front of the product. Therefore, the coefficient of x^n in the combined expression is $p(n) - p(n - 1)$. **b.** If we have a partition of $n - 1$, then we can add 1 as an additional part to get a partition of n that contains a 1. Conversely, if we have a partition of n having 1 as a part, then we can remove the 1 and obtain a partition of $n - 1$. So there is a one-to-one correspondence between the set of partitions of n having 1 as a part and the set of partitions of $n - 1$. Therefore, the number of partitions of n not having one as a part equals $p(n) - p(n|1 \text{ is not a part}) = p(n) - p(n - 1)$.

31. Consider a partition of n into distinct powers of 2. Define a process that changes the partition into a partition all of whose parts is 1, by taking any part 2^k and writing it as $2^{k-1} + 2^{k-1}$. By iterating this process, all parts will be reduced to $2^0 = 1$ and we will arrive at a partition of n into parts of size 1. Also define a reverse process in which, if any two like powers of 2 are present, say, 2^k and 2^k, they are merged into one part of size 2^k. If we iterate this process on a partition into parts of size $1 = 2^0$, then we must eventually have all distinct powers of 2. Thus, we have a bijection between the set of partitions of n into parts of size 1 and the set of partitions of n into distinct powers of two. Therefore, $p_{\{1\}}(n) = p(n|\text{distinct powers of 2})$. Because there is only one partition of n into parts of size 1, there must be only one partition of n into distinct powers of 2. Because such a partition is the binary expansion of n, this shows that the binary expansion is unique.

33. From Exercise 30, we know that $p_O^D(n)$ equals the number of self-conjugate partitions of n. Call this number N, and consider the set of partitions of n. The subset of non-self-conjugate partitions of n has an even number of elements, because each partition can be paired with its conjugate.

Then $p(n)$ equals the number of non-self-conjugate partitions plus the number of self-conjugate partitions, which is an even number plus N, which in turn is odd if and only if N is odd.

35. First, note that $p(n-2) = p(n|\text{at least one part equals 2})$ because adding and removing of a part of size 2 gives us a bijection between the two sets of partitions. Second, note that we can change an partition of n with no part of size 1 into at least one partition with a part of size 2 by taking the smallest part (which must be at least 2) and splitting off as many parts of size 1 as necessary. Therefore, $p(n|\text{at least one part of size 2}) \geq p(n|\text{no part equals 1})$. Now from Exercise 34, we have $p(n) = p(n-1) + p(n|\text{no part equals 1}) \leq p(n-1) + p(n|\text{at least one part equals 2}) = p(n-1) + p(n-2)$.

Next, note that $p(1) = 1 = f_2$ and $p(2) = 2 = f_3$. This is our basis step. Suppose $p(n) \leq f_{n+1}$ for all integers up to n. Then $p(n+1) \leq p(n) + p(n-1) \leq f_{n+1} + f_n = f_{n+2}$, which proves the induction step. So by mathematical induction, we have $p(n) \leq f_{n+1}$ for every n.

37. $p(1) = 1$; $p(2) = 2$; $p(3) = 3$; $p(4) = 5$; $p(5) = 7$; $p(6) = 11$; $p(7) = 15$; $p(8) = 22$; $p(9) = 30$; $p(10) = 42$; $p(11) = 56$; $p(12) = 77$

39. For the first part of the theorem, note that the product can be rewritten as $\prod_{j\in S} 1/(1-x^j) = \prod_{j\in S}(1 + x^j + x^{2j} + \cdots)$. Then the coefficient of x^n, when we expand this product, is the number of ways we can write $n = a_1k_1 + a_2k_2 + \cdots$ where the a_i are positive integers and the k_i are elements from S, but this is exactly the number of partitions of n into parts from S. For the second part of the theorem, note that when we expand the product $\prod_{j\in S}(1 + x^j)$, the coefficient of x^n is the number of ways to write $n = k_1 + k_2 + \cdots$ where the k_i are elements of S. But this is just the number of partitions into distinct parts from S.

41. The partitions of 11 into parts differing by at least 2 are (11), (10, 1), (9, 2), (8, 3), (7, 4), (7, 3, 1), and (6, 4, 1), for a total of 7. The positive integers less than or equal to 11 that are congruent to 1 or 4 modulo 5 are 1, 4, 6, 9, and 11, so the partitions of 11 into parts congruent to 1 or 5 modulo 5 are (11), (9, 1, 1), (6, 4, 1), (6, 1, 1, 1, 1, 1), (4, 4, 1, 1, 1), (4, 1, 1, 1, 1, 1, 1), and (1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1), for a total of 7 also. This verifies the first Rogers-Ramanujan identity for $n = 11$. The partitions of 11 into parts differing by at least 2 and that are at least two are (11), (9, 2), (8, 3), *and*(7, 4), for a total of 4. The partitions of 11 into parts congruent to 2 or 3 modulo 5 are (8, 3), (7, 2, 2), (3, 3, 3, 2), and (3, 2, 2, 2, 2), for a total of 4 also. This verifies the second Rogers-Ramanujan identity for $n = 11$.

Section 8.1

1. DWWDF NDWGD ZQ

3. IEXXK FZKXC UUKZC STKJW

5. READ MY LIPS

7. 12

9. AN IDEA IS LIKE A CHILD NONE IS BETTER THAN YOUR OWN FROM CHINESE FORTUNE COOKIE

11. 9, 12

13. THIS MESSAGE WAS ENCIPHERED USING AN AFFINE TRANSFORMATION

15. $C \equiv 7P + 16 \pmod{26}$

Section 8.2

1. VSPFXH HIPKLB KIPMIE GTG

3. TJEVT EESPZ TJIAN IARAB GSHWQ HASBU BJGAO XYACF XPHML AWVMO XANLB GABMS HNEIA TIEZV VWNQF TLEZF HJWPB WKEAG AENOF UACIH LATPR RDADR GKTJR XJDWA XXENB KA

5. Let n be the key length, and suppose $k_1, k_2, \ldots, k_n$ are the numerical equivalents of the letters of the keyword. If $p_i = p_j$ are two plaintext characters separated by a multiple of the key length, when we separate the plaintext into blocks of length n, p_i and p_j will be in the same position in their respective blocks, say, the mth position. So when we encrypt them, we get $c_i \equiv p_i + k_m \equiv p_j + k_m \equiv c_j \pmod{26}$.

7. The key is YES, and the plaintext is MISTA KESAR EAPAR TOFBE INGHU MANAP PRECI ATEYO URMIS TAKES FORWH ATTHE YAREP RECIO USLIF ELESS ONSTH ATCAN ONLYB ELEAR NEDTH EHARD WAYUN LESSI TISAF ATALM ISTAK EWHIC HATLE ASTOT HERSC ANLEA RNFRO M.

9. The key is BIRD, and the plaintext is IONCE HADAS PARRO WALIG HTUPO NMYSH OULDE RFORA MOMEN TWHIL EIWAS HOEIN GINAV ILLAG EGARD ENAND IFELT THATI WASMO REDIS TINGU ISHED BYTHA TCIRC UMSTA NCETH ATISH OULDH AVEBE ENBYA NYEPA ULETI COULD HAVEW ORN.

11. The key is SAGAN, and the plaintext is BUTTH EFACT THATS OMEGE NIUSE SWERE LAUGH EDATD OESNO TIMPL YTHAT ALLWH OAREL AUGHE DATAR EGENI USEST HEYLA UGHED ATCOL UMBUS THEYL AUGHE DATFU LTONT HEYLA UGHED ATTHE WRIGH TBROT HERSB UTTHE YALSO LAUGH EDATB OZOTH ECLOW N.

13. RL OQ NZ OF XM CQ KG QI VD AZ

15. TO SLEEP PERCHANCE TO DREAMX

17. 3, 24, 24, 25

19. We have $\mathbf{C} \equiv \mathbf{AP} \pmod{26}$. Multiplying both sides on the left by $\mathbf{A}$ gives $\mathbf{AC} \equiv \mathbf{A^2P} \equiv \mathbf{IP} \equiv \mathbf{P} \pmod{26}$. The congruence $\mathbf{A^2} \equiv \mathbf{I} \pmod{26}$ follows because $\mathbf{A}$ is involutory. It follows that $\mathbf{A}$ is also a deciphering matrix.

21. $\mathbf{C} = \begin{pmatrix} 11 & 6 \\ 2 & 13 \end{pmatrix} \pmod{26}$

23. If the plaintext is grouped into blocks of size m, we may take $\frac{[m,n]}{m}$ of these blocks to form a superblock of size $[m, n]$. If $\mathbf{A}$ is the $m \times m$ enciphering matrix, form the $[m, n] \times [m, n]$ matrix $\mathbf{B}$ with $\frac{[m,n]}{m}$ copies of $\mathbf{A}$ on the diagonal and zeros elsewhere: $\mathbf{B} = \begin{pmatrix} \mathbf{A} & 0 & \cdots & 0 \\ 0 & \mathbf{A} & \cdots & 0 \\ \vdots & & \ddots & \vdots \\ 0 & \cdots & & \mathbf{A} \end{pmatrix}$. Then $\mathbf{B}$ will encipher $\frac{[m,n]}{m}$ blocks of size m at once. Similarly, if $\mathbf{C}$ is the $n \times n$ enciphering matrix, form the corresponding $[m, n] \times [m, n]$ matrix $\mathbf{D}$. Then $\mathbf{BD}$ is an $[m, n] \times [m, n]$ enciphering matrix that does everything at once.

25. Multiplication of $(0 \cdots 010 \cdots 0) \begin{pmatrix} p_1 \\ p_2 \\ \vdots \\ p_n \end{pmatrix}$ with the 1 in the ith place yields the 1×1 matrix (P_i). So if the jth row of a matrix $\mathbf{A}$ is $(0 \cdots 010 \cdots 0)$, then $\mathbf{A} \begin{pmatrix} p_1 \\ \vdots \\ p_n \end{pmatrix} = \begin{pmatrix} C_1 \\ \vdots \\ C_n \end{pmatrix}$ gives $C_j = P_i$. So if every row of $\mathbf{A}$ has its 1 in a different column, then each C_j is equal to a different P_i. Hence, $\mathbf{A}$ is a "permutation" matrix.

27. $\mathbf{P} \equiv \begin{pmatrix} 17 & 4 \\ 1 & 7 \end{pmatrix} \mathbf{C} + \begin{pmatrix} 22 \\ 15 \end{pmatrix} \pmod{26}$

29. TOXIC WASTE

31. Make a frequency count of the trigraphs and use a published English language count of frequencies of trigraphs. Then proceed as in problem 18. There are 12 variables to determine, so 4 guesses are needed.

33. yes

35. 01 1101 1010

37. RENDE ZVOUS

39. Let $p_1p_2 \cdots p_m$ and $q_1q_2 \cdots q_m$ be two different plaintext bit streams. Let $k_1, k_2, \ldots, k_m$ be the keystream by which the plaintexts are encrypted. Then note that for any $i = 1, 2, \ldots, m$, $E_{k_i}(p_i) + E_{k_i}(q_i) = k_i + p_i + k_i + q_i = 2k_i + p_i + q_i \equiv p_i + q_i \pmod 2$. Therefore, by adding corresponding bits of the ciphertext streams, we get the sums of the corresponding bits of the plaintext streams. This partial information can lead to successful cryptanalysis of encrypted messages.

Section 8.3

1. 14 17 17 27 11 17 65 76 07 76 14

3. BEAM ME UP

5. We encipher messages using the transformation $c \equiv P^{11} \pmod{31}$. The deciphering exponent is the inverse of 11 modulo 30 because $\phi(31) = 30$. But 11 is its own inverse modulo 30 because $11 \cdot 11 \equiv 121 \equiv 1 \pmod{30}$. It follows that 11 is both the enciphering and deciphering exponent.

Section 8.4

1. 151, 97

3. Because a block of ciphertext p is less than n, we must have $(p, n) = p$ or q. Therefore, the cryptanalyst has a factor of n.

5. 1215 1224 1471 0023 0116

7. GREETINGSX

9. 0872 2263 1537 2392

11. No. It is as if the encryption key were (e_1e_2, n), and it is no more difficult (or easy) to discover the inverse of $e = e_1e_2$ than it would be to discover the inverse of either of the factors modulo $\phi(n)$.

13. Suppose P is a plaintext message and the two encrypting exponents are e_1 and e_2. Let $a = (e_1, e_2)$. Then there exist integers x and y such that $e_1x + e_2y = a$. Let $C_1 \equiv P^{e_1} \pmod n$ and $C_2 \equiv P^{e_2} \pmod n$ be the two cipher texts. Because C_1, C_2, e_1, and e_2 are known to the decipherer, and because x and y are relatively easy to compute, then it is also easy to compute $C_1^x C_2^y \equiv P^{e_1x} P^{e_2y} \equiv P^{e_1x+e_2y} \equiv P^a \pmod n$. If $a = 1$, then P has been recovered. If a is fairly small, then it may not be too difficult to compute ath roots of P^a and thereby recover P.

15. Encryption works the same as for the two prime case. For decryption, we must compute an inverse d for e modulo $\phi(n) = (p - 1)(q - 1)(r - 1)$ where $n = pqr$ the product of three primes. Then we proceed as in the two prime case.

17. Let the encryption key be (e, n). Then $C_1 \equiv P_1^e \pmod n$ and $C_2 \equiv P_2^e \pmod n$, where C_1 and C_2 are reduced residues modulo n. When we encrypt the product, we get $C \equiv (P_1P_2)^e \equiv P_1^e P_2^e \equiv C_1C_2 \pmod n$, as desired.

Section 8.5

1. **a.** yes **b.** no **c.** yes **d.** no

3. Proceed by induction. Certainly $a_1 < 2a_1 < a_2$. Suppose $\sum_{j=1}^{n-1} a_j < a_n$. Then $\sum_{j=1}^{n} a_j = \sum_{j=1}^{n-1} a_j + a_n < a_n + a_n = 2a_n < a_{n+1}$.

5. (17, 51, 85, 7, 14, 45, 73)

7. NUTS

9. If the multipliers and moduli are (w_1, m_1), [0](w_2, m_2), . . . , [0](w_r, m_r),[0] the inverse $\overline{w_1}, \overline{w_2}, \ldots, \overline{w_r}$ can be computed with respect to their corresponding moduli. Then we multiply and reduce succesively by $(\overline{w_r}, m_r)$, $(\overline{w_{r-1}}, m_{r-1})$, . . . , $(\overline{w_1}, m_1)$. The result will be the plaintext sequence of easy knapsack problems.

11. $8 \cdot 21 \cdot 95$

13. For $i = 1, 2, \ldots, n$, we have $b^{\alpha_i} \equiv a_i \pmod{m}$. Then $b^S \equiv P \equiv (b^{\alpha_1})^{x_1}(b^{\alpha_2})^{x_2} \cdots (b^{\alpha_n})^{x_n} \equiv b^{\alpha_1 x_1 + \cdots + \alpha_n x_n} \pmod{m}$. Then $S \equiv \alpha_1 x_1 + \cdots + \alpha_n x_n \pmod{\phi(m)}$. Because $S + k\phi(m)$ is also a logarithm of P to the base b, we may take the congruence to be an equation. Because the $x_i = 0$ or 1, this becomes an additive knapsack problem on the sequence $(\alpha_1, \alpha_2, \ldots, \alpha_n)$.

Section 8.6

1. 90

3. 476

5. Let $k_1, k_2, \ldots, k_n$ be the private keys for parties 1 through n, respectively. There are n steps in this protocol. The first step is for each of the parties 1 through n to compute the least positive residue of $r^{k_i} \pmod{p}$ and send this value y_i to the $i+1$st party. (The nth party sends his value to the 1st party.) Now the ith party has the value y_{i-1} (where we take y_0 to be y_n). The second step is for each party to compute the least positive residue of $y_{i-1}^{k_i} \pmod{p}$ and send this value to the $i+1$st party. Now the ith party has the least positive residue of $r^{k_{i-1}+k_{i-2}} \pmod{p}$. This process is continued for a total of n steps. However, at the nth step, the computed value is not sent on to the next party. Then the ith party will have the least positive residue of $r^{k_{i-1}+k_{i-2}+\cdots+k_1+k_n+k_{n-1}+\cdots k_{i+1}+k_i} \pmod{p}$, which is exactly the value of K desired.

7. **a.** 0371 0354 0858 0858 0087 1369 0354 0000 0087 1543 1797 0535 **b.** 0833 0457 0074 0323 0621 0105 0621 0865 0421 0000 0746 0803 0105 0621 0421

9. **a.** If $n_i < n_j$, then the block sizes are chosen small enough so that each block is unique modulo n_i. Because $n_i < n_j$, each block will be unique modulo n_j after applying the transformation D_{k_j}. Therefore we can apply E_{k_j} to $D_{k_i}(P)$ and retain uniqueness of blocks. If $n_i > n_j$, the argument is similar. **b.** If $n_i < n_j$, individual j receives $E_{k_j}(D_{k_i}(P))$ and knows an inverse for e_j modulo $\phi(n_i)$. So he can apply $D_{k_j}(E_{k_j}(D_{k_i}(P))) = D_{k_i}(P)$. Because he also knows e_i, he can apply $E_{k_i}(D_{k_i}(P)) = P$ and discover the plaintext P. If $n_i > n_j$, then individual j receives $D_{k_i}(E_{k_j}(P))$. Because he knows e_i, he can apply $E_{k_i}(D_{k_i}(E_{k_j}(P))) = E_{k_j}(P)$. Because he also knows $\overline{e_j}$, he can apply $D_{k_j}(E_{k_j}(P)) = P$ and discover the plaintext P. **c.** Because only individual i knows $\overline{e_i}$, only he can apply the transformation D_{k_i} and thereby make $E_{k_i}(D_{k_i}(P))$ intelligible. **d.** $n_i = 2867 > n_j = 2537$, so we compute $D_{k_i}(E_{k_j}(P))$. Both n_i and $n_j > 2525$, so we use blocks of four. REGARDS FRED becomes 1704 0600 1703 1805 1704 0323 (adding an X to fill out the last block). $e_i = 11$ and $\phi(n_i) = 2760$, so $\overline{e_i} = 251$. We apply $E_{k_j} \equiv P^{e_j} \equiv P^{13} \pmod{2537}$ to each block and get 1943 0279 0847 0171 1943 0088. Then we apply $D_{k_i}(E) = E^{251} \pmod{2867}$ and get 0479 2564 0518 1571 0479 1064. Now because $n_j < n_i$, individual j must

send $E_{k_i}(D_{k_j}(P))$, $e_j = 13$, $\phi(2537) = 2436$, and $\overline{e_j} = 937$. Then $D_{k_j}(P) \equiv P^{937} \pmod{2537}$ and $E_{k_i}(D) = D^{11} \pmod{2867}$. The cipher text is 1609 1802 0790 2508 1949 0267.

11. $k_1 \equiv 4 \pmod 8$, $k_2 \equiv 5 \pmod 9$, $k_3 \equiv 2 \pmod{11}$

13. The three shadows from Exercise 11 are $k_1 = 4$, $k_2 = 5$, and $k_3 = 2$. If k_1 and k_2 are known, we solve the system of congruences $x \equiv 4 \pmod 8$, $x \equiv 5 \pmod 9$ to get $x = 68$. If k_1 and k_3 are known, we solve the system of congruences $x \equiv 4 \pmod 8$, $x \equiv 2 \pmod{11}$ to get $x = 68$. If k_2 and k_3 are known, we solve the system of congruences $x \equiv 5 \pmod 9$, $x \equiv 2 \pmod{11}$ to get $x = 68$. In all three cases, we recover K_0. Then $K = K_0 - tp = 68 - 13 \cdot 5 = 3$.

Section 9.1

1. **a.** 4 **b.** 4 **c.** 6 **d.** 4

3. $2^1 \equiv 2 \pmod 3$ and $2^2 \equiv 1 \pmod 3$, so $\text{ord}_3\, 2 = 2$. $2^1 \equiv 2 \pmod 5$, $2^2 \equiv 4 \pmod 5$ and $2^4 = 16 \equiv 1 \pmod 5$, so $\text{ord}_5\, 2 = 4$. $2^1 \equiv 2 \pmod 7$, $2^2 \equiv 4 \pmod 7$ and $2^3 \equiv 1 \pmod 7$, so $\text{ord}_7\, 2 = 3$.

5. **a.** $\phi(6) = 2$, and $5^2 \equiv 1 \pmod 6$. **b.** $\phi(11) = 10$, $2^2 \equiv 4$, $2^5 \equiv -1$, $2^{10} \equiv 1 \pmod{11}$.

7. Only 1, 5, 7, and 11 are prime to 12. Each one squared is congruent to 1, but $\phi(12) = 4$.

9. There are two: 3 and 5.

11. That $\text{ord}_n a = \text{ord}_n \overline{a}$ follows from the fact that $a^t \equiv 1 \pmod n$ if and only if $\overline{a}^t \equiv 1 \pmod n$. To see this, suppose that $a^t \equiv 1 \pmod n$. Then $\overline{a}^t \equiv (\overline{a}^t a^t)(a^t) \equiv (a\overline{a})^t a^t \equiv 1^t \cdot 1 \equiv 1 \pmod n$. The converse is shown in a similar manner.

13. We have $[r, s]/(r, s) \le \text{ord}_n ab \le [r, s]$

15. Let $r = \text{ord}_m a^t$. Then $a^{tr} \equiv 1 \pmod m$, and hence $tr \ge ts$ and $r \ge s$. Because $1 \equiv a^{st} \equiv (a^t)^s \pmod n$, we have $s \ge r$.

17. Suppose that r is a primitive root modulo the odd prime p. Then $r^{(p-1)/q} \not\equiv 1 \pmod p$ for all prime divisors q of $p - 1$ because no smaller power than the $(p - 1)$st of r is congruent to 1 modulo p. Conversely, suppose that r is not a primitive root of p. Then there is an integer t such that $r^t \equiv 1 \pmod p$ with $t < p - 1$. Because t must divide $p - 1$, we have $p - 1 = st$ for some positive integer s greater than 1. Then $(p - 1)/s = t$. Let q be a prime divisor of s. Then $(p - 1)/q = t(s/q)$, so that $r^{(p-1)/q} = r^{t(s/q)} = (r^t)^{s/q} \equiv 1 \pmod p$.

19. Because $2^{2^n} + 1 \equiv 0 \pmod{F_n}$, then $2^{2^n} \equiv -1 \pmod{F_n}$. Squaring gives $(2^{2^n})^2 \equiv 1 \pmod{F_n}$. Thus, $\text{ord}_{F_n} 2 \le 2^n 2 = 2^{n+1}$.

21. Note that $a^t < m = a^n - 1$ whenever $1 \le t < n$. Hence, a^t cannot be congruent to 1 modulo m when t is a positive integer less than n. However, $a^n \equiv 1 \pmod m$ because $m = (a^n - 1) \mid (a^n - 1)$. It follows that $\text{ord}_m a = n$. Because $\text{ord}_m a \mid \phi(m)$, we see that $n \mid \phi(m)$.

23. First suppose that pq is a pseudoprime to the base 2. By Fermat's little theorem, $2^p \equiv 2 \pmod p$, so there exists an integer k such that $2^p - 2 = kp$. Then $2^{M_p - 1} - 1 = 2^{2^p - 2} - 1 = 2^{kp} - 1$. This last expression is divisible by $2^p - 1 = M_p$ by Lemma 6.1. Hence, $2^{M_p - 1} \equiv 1 \pmod{M_p}$, or $2^{M_p} \equiv 2 \pmod{M_p}$. Because pq is a pseudoprime to the base 2, we have $2^{pq} \equiv 2 \pmod{pq}$, so $2^{pq} \equiv 2 \pmod p$. But $2^{pq} \equiv (2^p)^q \equiv 2^q \pmod p$. Therefore, $2^q \equiv 2 \pmod p$. Then there exists an integer l such that $M_q - 1 = 2^q - 2 = lp$. Then $2^{M_q - 1} - 1 = 2^{2^q - 2} = 2^{lp} - 1$, so $2^p - 1 = M_p$ divides $2^{M_q - 1} - 1$. Therefore, $2^{M_q} \equiv 2 \pmod{M_p}$. Then we have $2^{M_p M_q} \equiv (2^{M_p})^{M_q} \equiv 2^{M_q} \equiv 2 \pmod{M_p}$. Similarly, $2^{M_p M_q} \equiv 2 \pmod{M_q}$. By the Chinese remainder theorem, noting that M_p and M_q are relatively prime, we have $2^{M_p M_q} \equiv 2 \pmod{M_p M_q}$. Therefore, $M_p M_q$ is a pseudoprime to the base 2. Conversely, suppose $M_p M_q$ is a pseudoprime to the base 2. From the reasoning in the proof of Theorem 6.6, we have that $2^{M_p} \equiv 2 \pmod p$. Therefore, $2^{M_p M_q} \equiv 2^{(M_p - 1)M_q + M_q} \equiv 2^{M_q} \equiv 2 \pmod p$. But because $M_p = 2^p - 1 \equiv 0 \pmod{M_p}$, we have

that the order of 2 modulo M_p is p. Therefore, $p|M_q - 1$. In other words, $2^q \equiv 2 \pmod{p}$. Then $2^{pq} \equiv 2^q \equiv 2 \pmod{p}$. Similarly, $2^{pq} \equiv 2 \pmod{q}$. Therefore, by the Chinese remainder theorem, $2^{pq} \equiv 2 \pmod{pq}$. Therefore, because pq is composite, it is a pseudoprime to the base 2.

25. **a.** Let k be an integer that satisfies all of the congruences. If $n \equiv 1 \pmod 2$, then because $\text{ord}_3 2 = 2$, we have $2^n + k \equiv 2^{2m+1} - 2^1 \equiv (2^2)^m 2 - 2 \equiv 1^m 2 - 2 \equiv 0 \pmod 3$, so $3 \mid 2^n + k$. If $n \equiv 2 \pmod 4$, then because $\text{ord}_5 2 = 4$, we have $2^n + k \equiv 2^{4m+2} - 2^2 \equiv 2^2 - 2^2 \equiv 0 \pmod 5$, so $5 \mid 2^n + k$. If $n \equiv 1 \pmod 3$, then because $\text{ord}_7 2 = 3$, we have $2^n + k \equiv 2^{3m+1} - 2^1 \equiv 2 - 2 \equiv 0 \pmod 7$, so $7 \mid 2^n + k$. If $n \equiv 8 \pmod{12}$, then because $\text{ord}_{13} 2 = 12$, we have $2^n + k \equiv 2^{12m+8} - 2^8 \equiv 2^8 - 2^8 \equiv 0 \pmod{13}$, so $13 \mid 2^n + k$. If $n \equiv 4 \pmod 8$, then because $\text{ord}_{17} 2 = 8$, we have $2^n + k \equiv 2^{8m+4} - 2^4 \equiv 2^4 - 2^4 \equiv 0 \pmod{17}$, so $17 \mid 2^n + k$. If $n \equiv 0 \pmod{24}$, then because $\text{ord}_{241} 2 = 24$, we have $2^n + k \equiv 2^{24m} - 2^0 \equiv 1 - 1 \equiv 0 \pmod{241}$, so $241 \mid 2^n + k$. So if n satisfies any of the above congruences, we see that $2^n + k$ cannot be prime. Let r the least nonnegative residue of n modulo 24. If r is odd, then $n \equiv 1 \pmod 2$. If $r = 2$, 6, 10, 14, 18, or 22, then $n \equiv 2 \pmod 4$. If $r = 4$ or 16, then $n \equiv 1 \pmod 3$. If $r = 8$ or 20, then $n \equiv 8 \pmod{12}$. If $r = 12$, then $n \equiv 4 \pmod 8$. If $r = 0$, then $n \equiv 0 \pmod{24}$. This shows that every positive integer n must satisfy one of the congruences $n \equiv 1 \pmod 2$, $n \equiv 3 \pmod 4$, $n \equiv 1 \pmod 3$, $n \equiv 8 \pmod{12}$, $n \equiv 4 \pmod 8$, and $n \equiv 0 \pmod{24}$. So if k simultaneously satisfies all the congruences stated in the exercise, then $2^n + k$ must be composite for all positive integers n. **b.** Simplifying the congruences in part (a) gives us $k \equiv 1 \pmod 3$, $k \equiv 1 \pmod 5$, $k \equiv 5 \pmod 7$, $k \equiv 4 \pmod{13}$, $k \equiv 1 \pmod{17}$, and $k \equiv -1 \pmod{241}$. Using computational software, we use the Chinese remainder theorem to simultaneously solve this system of congruences to get $k \equiv 1{,}518{,}781 \pmod{5{,}592{,}405}$. Note that the modulus is equal to $3 \cdot 5 \cdot 7 \cdot 13 \cdot 17 \cdot 241$. Then $2^n + 1{,}518{,}781$ is composite for all positive integers n.

27. Let $j = \text{ord}_{\phi(n)} e$. Then $e^j \equiv 1 \pmod{\phi(n)}$. Because $\text{ord}_n P \mid \phi(n)$, we have $e^j \equiv 1 \pmod{\text{ord}_n P}$. Then by Theorem 9.2, $P^{e^j} \equiv P \pmod n$, so $C^{e^{j-1}} \equiv (P^e)^{e^{j-1}} \equiv P^{e^j} \equiv P \pmod n$ and $C^{e^j} \equiv P^e \equiv C \pmod n$.

Section 9.2

1. **a.** 2 **b.** 2 **c.** 3 **d.** 0

3. **a.** 2 **b.** 4 **c.** 8 **d.** 6 **e.** 12 **f.** 22

5. 2, 6, 7, 11

7. 2, 3, 10, 13, 14, 15

9. By Lagrange's theorem, there are at most two solutions to $x^2 \equiv 1 \pmod p$, and we know $x \equiv \pm 1$ are the two solutions. Because $p \equiv 1 \pmod 4$, $4 \mid (p-1) = \phi(p)$, so there is an element x of order 4 modulo p. Then $x^4 = (x^2)^2 \equiv 1 \pmod p$, so $x^2 \equiv \pm 1 \pmod p$. If $x^2 \equiv 1 \pmod p$, then x does not have order 4. Therefore, $x^2 \equiv -1 \pmod p$.

11. **a.** Let $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots a_0$, and let k be the largest integer such p does not divide a_k. Let $g(x) = a_k x^k + a_{k-1} x^{k-1} + \cdots a_0$. Then $f(x) \equiv g(x) \pmod p$ for every value of x. In particular, $g(x)$ has the same set of roots as $f(x)$. Because the number of roots is greater than $n > k$, this contradicts Lagrange's theorem. Therefore, no such k exists and p must divide every coefficient of $f(x)$. **b.** Note that the degree of $f(x)$ is $p-2$. By Fermat's little theorem, we have that $x^{p-1} - 1 \equiv 0 \pmod p$, for $x = 1, 2, \ldots, p-1$. Further, each x in the same range is a zero for $(x-1)(x-2)\cdots(x-p+1)$. Therefore, each $x = 1, 2, \ldots, p-1$ is a root of $f(x)$. Because $f(x)$ has degree $p-2$ and $p-1$ roots, part (a) tells us that all the coefficients of $f(x)$ are divisible by p. **c.** From part (b), we know that the constant term of $f(x)$ is divisible by p. The constant term is given by $f(0) = (-1)(-2)\cdots(-p+1) + 1 \equiv (-1)^{p-1}(p-1)! + 1 \equiv (p-1)! + 1 \equiv 0 \pmod p$, which is Wilson's theorem.

13. **a.** Because $q_i^{t_i} \mid \phi(p) = p - 1$, by Theorem 9.8 there exists $\phi(q_i^{t_i})$ elements of order $q_i^{t_i}$ for each $i = 1, 2, \ldots, r$. Let a_i be a fixed element of this order. **b.** Using induction and Exercise 10 of Section 9.1, we have $\text{ord}_p(a) = \text{ord}_p(a_1 a_2 \cdots a_r) = \text{ord}_p(a_1 \cdots a_{r-1})\ \text{ord}_p(a_r) = \cdots = \text{ord}_p(a_1) \cdots \text{ord}_p(a_r)$ because $\{\text{ord}_p(a_1), \text{ord}_p(a_2), \ldots, \text{ord}_p(a_r)\} = \{q_1^{t_1}, \ldots, q_r^{t_r}\}$ are pairwise relatively prime. **c.** 18

15. If n is odd, composite, and not a power of 3, then the product in Exercise 14 is $\prod_{j=1}^{r}(n-1, p_j - 1) \geq (n-1, 3-1)(n-1, 5-1) \geq 2 \cdot 2 = 4$. So there must be two bases other than -1 and $+1$.

17. **a.** Suppose that $f(x)$ is a polynomial with integer coefficients of degree $n-1$. Suppose that $x_1, x_2, \cdots, x_n$ are incongruent modulo p where p is prime. Consider the polynomial $g(x) = f(x) - \sum_{j=1}^{n}\left(f(x_j)\prod_{i\neq j}(x - x_i)\overline{(x_j - x_i)}\right)$. Note that x_j, $j = 1, 2, \cdots, n$ is a root of this polynomial modulo p because its value at x_j is $f(x_j) - [0 + 0 + \cdots + f(x_j)\prod_{i\neq j}(x_j - x_i)\overline{(x_j - x_i)} + \cdots + 0] \equiv f(x_j) - f(x_j) \cdot 1 \equiv 0 \pmod{p}$. Because $g(x)$ has n incongruent roots modulo p, and because it is of degree $n-1$ or less, we can easily use Lagrange's theorem (Theorem 9.6) to see that $g(x) \equiv 0 \pmod{p}$ for every integer x. **b.** 10

19. By Exercise 27 of Section 9.1, $j \mid \text{ord}_{\phi(n)}e$. Here, $\phi(n) = \phi(pq) = 4p'q'$, so $j \mid \phi(4p'q') = 2(p'-1)(q'-1)$. Choose e to be a primitive root modulo p'. Then $p' - 1 = \phi(p') | \phi(\phi(n))$, so $p' - 1 | \text{ord}_{\phi(n)}e$. The decrypter needs $e^j \equiv 1 \pmod{n}$, but this choice of e forces $j = p' - 1$, which will take quite some time to find.

Section 9.3

1. 4, 10, 22

3. **a.** 2 **b.** 2 **c.** 5 **d.** 2

5. **a.** 2 **b.** 2 **c.** 2 **d.** 3

7. **a.** 7 **b.** 3 **c.** 21 **d.** 27

9. 7, 13, 17, 19

11. 3, 13, 15, 21, 29, 33

13. Suppose that r is a primitive root of m, and suppose further that $x^2 \equiv 1 \pmod{m}$. Let $x \equiv r^t \pmod{m}$ where $0 \leq t \leq p - 1$. Then $r^{2t} \equiv 1 \pmod{m}$. Because r is a primitive root, it follows that $\phi(m) \mid 2t$ so that $2t = k\phi(m)$ and $t = k\phi(m)/2$ for some integer k. We have $x \equiv r^t = r^{k\phi(m)/2} = r^{(\phi(m)/2)k} \equiv (-1)^k \equiv \pm 1 \pmod{m}$, because $r^{\phi(m)/2} \equiv -1 \pmod{m}$. Conversely, suppose that m has no primitive root. Then m is not of one of the forms 2, 4, p^a, or $2p^a$ with p an odd prime. So either 2 distinct odd primes divide m or $m = 2^b M$ with $M > 1$ an odd integer and $b > 1$ or $m = 2^b$ with $b > 3$ or $m = 8$. If $m = 8$, note that $3^2 \equiv 1 \pmod{8}$. In each of the other cases, we have $\phi(m) = 2^c N$ with N odd and $c \geq 3$. From Theorem 9.12, we know there are at least three solutions y_1, y_2, y_3 to $y^2 \equiv 1 \pmod{2^c}$, and certainly $z \equiv 1 \pmod{N}$ is a solution of $x^2 \equiv 1 \pmod{N}$. By the Chinese remainder theorem, there is a unique solution modulo $2^c N$ of the system $x \equiv y_i \pmod{2^c}$, $z \equiv 1 \pmod{N}$ for $i = 1, 2, 3$. Because these solutions are distinct modulo m, at least one of them is not $\pm 1 \pmod{m}$.

15. By Theorem 9.12, we know that $\text{ord}_{2^k}5 = \phi(2^k)/2$. Hence, the 2^{k-2} integers 5^j, $j = 0, 1, \cdots, 2^{k-2} - 1$, are incongruent modulo $2k$. Similarly, the 2^{k-2} integers -5^j, $j = 0, 1, \cdots, 2^{k-2} - 1$, are incongurent modulo 2^k. Note that 5^j cannot be congruent to -5^i modulo 2^k where i and j are integers, because $5^j \equiv 1 \pmod{4}$ but $-5^i \equiv 3 \pmod{4}$. It follows that the integers $1, 5, \cdots, 5^{2^{k-2}-1}, -1, -5, \cdots, -5^{2^{k-2}-1}$ are 2^{k-1} incongruent integers modulo 2^k. Because $\phi(2^k) = 2^{k-1}$ and every integer of the form $(-1)^\alpha 5^\beta$ is relatively prime to 2^k, it follows that every odd integer is congruent to an integer of this form with $\alpha = 0$ or 1 and $0 \leq \beta = 2^{k-2} - 1$.

Section 9.4

1. The values of $\text{ind}_5 i$, $i = 1, 2, \ldots, 22$ are 22, 2, 16, 4, 1, 18, 19, 6, 10, 3, 9, 20, 14, 21, 17, 8, 7, 12, 15, 5, 13, 11, respectively.

3. **a.** 7, 18 **b.** none

5. 8, 9, 20, 21, 29 (mod 29)

7. all positive integers $x \equiv$ 1, 12, 23, 24, 45, 46, 47, 67, 69, 70, 78, 89, 91, 92, 93, 100, 111, 115, 116, 133, 137, 138, 139, 144, 155, 161, 162, 177, 183, 184, 185, 188, 199, 207, 208, 210, 221, 229, 230, 231, 232, 243, 253, 254, 265, 275, 276, 277, 287, 299, 300, 309, 321, 322, 323, 331, 345, 346, 353, 367, 368, 369, 375, 386, 391, 392, 397, 413, 414, 415, 419, 430, 437, 438, 441, 459, 460, 461, 463, 483, 484, 485, 496, 505 (mod 506)

9. Suppose that $x^4 \equiv -1 \pmod{p}$ and let $y = \text{ind}_r x$. Then $-x$ is also a solution and by Exercise 8, $\text{ind}_r(-x) \equiv \text{ind}_r(-1) + \text{ind}_r(x) \equiv (p-1)/2 + y \pmod{p-1}$. So, without loss of generality, we may take $0 < y < (p-1)/2$, or $0 < 4y < 2(p-1)$. Taking indices of both sides of the congruence yields $4y \equiv \text{ind}_r(-1) \equiv (p-1)/2 \pmod{p-1}$, again using Exercise 8. So $4y = (p-1)/2 + m(p-1)$ for some m. But $4y < 2(p-1)$, so either $4y = (p-1)/2$ and so $p = 8y + 1$ or $4y = 3(p-1)/2$. In this last case, 3 must divide y, so we have $p = 8(y/3) + 1$. So in either case, p is of the desired form. Conversely, suppose $p = 8k + 1$ and let r be a primitive root of p. Take $x = r^k$. Then $x^4 \equiv r^{4k} \equiv r^{(p-1)/2} \equiv -1 \pmod{p}$ by Exercise 8. So this x is a solution.

11. (1, 2), (0, 2)

13. $x \equiv 29 \pmod{32}$; $x \equiv 4 \pmod{8}$

15. (0, 0, 1, 1), (0, 0, 1, 4)

17. $x \equiv 17 \pmod{60}$

19. We seek a solution to $x^k \equiv a \pmod{2^e}$. We take indices as described before Exercise 11. Suppose $a \equiv (-1)^\alpha 5^\beta$ and $x \equiv (-1)^\gamma 5^\delta$ Then we have $\text{ind}\, x^k = (k\gamma, k\delta)$ and $\text{ind}\, a = (\alpha, \beta)$, so $k\gamma \equiv \alpha \pmod{2}$ and $k\delta \equiv \beta \pmod{2^{e-2}}$. Because k is odd, both congruences are solvable for γ and δ, which determine x.

21. First we show that $\text{ord}_{2^e} 5 = 2^{e-2}$. Indeed, $\phi(2^e) = 2^{e-1}$, so it suffices to show that the highest power of 2 dividing $5^{2^{e-2}} - 1$ is 2^e. We proceed by induction. The basis step is the case $e = 2$, which is true. Note that $5^{2^{e-2}} - 1 = (5^{2^{e-3}} - 1)(5^{2^{e-3}} + 1)$. The first factor is exactly divisible by 2^{e-1} by the induction hypothesis. The second factor differs from the first by 2, so it is exactly divisible by 2, and therefore $5^{2^{e-2}} - 1$ is exactly divisible by 2^e, as desired. Hence, if k is odd, the numbers $\pm 5^k, \pm 5^{2k}, \ldots, \pm 5^{2^{e-2}k}$ are 2^{e-1} incongruent kth power residues, which is the number given by the formula. If 2^m exactly divides k, then $5^k \equiv -5^k \pmod{2^e}$, so the formula must be divided by 2, hence the factor $(k, 2)$ in the denominator. Further, 5^{2^m} has order $2^{e-2}/2^m$ if $m \leq e - 2$ and order 1 if $m > e - 2$, so the list must repeat modulo 2^e every $\text{ord}_{2^e} 5^{2^m}$ terms, whence the other factor in the denominator.

23. **a.** From the first inequality in case (i) of the proof of Theorem 6.10, if n is not square-free, the probability is strictly less than $2n/9$, which is substantially smaller than $(n-1)/4$ for large n. If n is square-free, the argument following inequality (9.6) shows that if n has four or more factors, then the probability is less than $n/8$. The next inequality shows that the worst case for $n = p_1 p_2$ is when $s_1 = s_2$ and s_1 is as small as possible, which is the case stated in this exercise.
b. 0.24999 . . .

Section 9.5

1. We have $2^2 \equiv 4 \pmod{101}$, $2^5 \equiv 32 \pmod{101}$, $2^{10} \equiv (2^5)^2 \equiv 32^2 \equiv 14 \pmod{101}$, $2^{20} \equiv (2^{10})^2 \equiv 14^2 \equiv 95 \pmod{101}$, $2^{25} \equiv (2^5)^5 \equiv 32^5 \equiv (32^2)^2 32 \equiv 1024^2 32 \equiv 14^2 32 \equiv 196 \cdot 32 \equiv -6 \cdot 32 \equiv -192 \equiv 10 \pmod{101}$, $2^{50} \equiv (2^{25})^2 \equiv 10^2 = 100 \equiv -1 \pmod{101}$, $2^{100} \equiv (2^{50})^2 \equiv (-1)^2 \equiv 1 \pmod{101}$. Because $2^{\frac{(101-1)}{q}} \not\equiv 1 \pmod{101}$ for every proper divisor q of 100, and because $2^{(101-1)} \equiv 1 \pmod{101}$, it follows that 101 is prime.

3. $233 - 1 = 2^3 29$, $3^{116} \equiv -1 \pmod{233}$, $3^8 \equiv 37 \not\equiv 1 \pmod{233}$

5. The first condition implies $x^{F_n - 1} \equiv 1 \pmod{F_n}$. The only prime dividing $F_n - 1 = 2^{2^n}$ is 2, and $(F_n - 1)/2 = 2^{2^n - 1}$, so the second condition implies $2^{(F_n-1)/2} \not\equiv 1 \pmod{F_n}$. Then by Theorem 9.18, F_n is prime.

7. See [Le80]

9. Because $n - 1 = 9928 = 2^3 17 \cdot 73$, we take $F = 2^3 17 = 136$ and $R = 73$, noting that $F > R$. We apply Pocklington's test with $a = 3$. We check (using a calculator or computational software) that $3^{9928} \equiv 1 \pmod{9929}$ and $(3^{9928/2} - 1, 9929) = 1$ and $(3^{9928/17} - 1, 9929) = 1$, because 2 and 17 are the only primes dividing F. Therefore, n passes Pocklington's test and so is prime.

11. Note that $3329 = 2^8 13 + 1$ and $13 < 2^8$, so it is of the form that can be tested by Proth's test. We try $2^{(3329-1)/2} \equiv 2^{1664} \equiv 1 \pmod{3329}$ (using a calculator or computational software). So Proth's test fails for $a = 2$. Next we try $a = 3$ and compute $3^{1664} \equiv -1 \pmod{3329}$, which shows that 3329 is prime.

13. We apply Pocklington's test to this situation. Note that $n - 1 = hq^k$, so we let $F = q^k$ and $R = h$ and observe that by hypothesis $F > R$. Because q is the only prime dividing F, we need only check that there is an integer a such that $a^{n-1} \equiv 1 \pmod{n}$ and $(a^{(n-1)/q} - 1, n) = 1$. But both of these conditions are hypotheses.

Section 9.6

1. **a.** 20 **b.** 12 **c.** 36 **d.** 48 **e.** 180 **f.** 388,080 **g.** 8640 **h.** 125,411,328,000

3. 65,520

5. Suppose that $m = 2^{t_0} p_1^{t_1} \cdots p_s^{t_s}$. Then $\lambda(m) = [\lambda(2^{t_0}), \phi(p_1^{t_1}), \ldots, \phi(p_s^{t_s})]$. Furthermore, $\phi(m) = \phi(2^{t_0})\phi(p_1^{t_1}) \cdots \phi(p_s^{t_s})$. Because $\lambda(2^{t_0}) = 1, 2,$ or 2^{t_0-2} when $t_0 = 1, 2,$ or $t_0 \geq 3$, respectively, it follows that $\lambda(2^{t_0}) \mid \phi(2^{t_0}) = 2^{t_0-1}$. Because the least common multiple of a set of numbers divides the product of these numbers, or their multiples, we see that $\lambda(m) \mid \phi(m)$.

7. For any integer x with $(x, n) = (x, m) = 1$, we have $x^a \equiv 1 \pmod{n}$ and $x^a \equiv 1 \pmod{m}$. Then the Chinese remainder theorem gives us $x^a \equiv 1 \pmod{[n, m]}$. But because n is the largest integer with this property, we must have $[n, m] = n$, so $m|n$.

9. Suppose that $ax \equiv b \pmod{m}$. Multiplying both sides of this congruence by $a^{\lambda(m)-1}$ gives $a^{\lambda(m)}x \equiv a^{\lambda(m)-1}b \pmod{m}$. Because $a^{\lambda(m)} \equiv 1 \pmod{m}$, it follows that $x \equiv a^{\lambda(m)-1}b \pmod{m}$. Conversely, let $x_0 \equiv a^{\lambda(m)-1}b \pmod{m}$. Then $ax_0 \equiv aa^{\lambda(m)-1}b \equiv a^{\lambda(m)}b \equiv b \pmod{m}$, so x_0 is a solution.

11. **a.** First suppose that $m = p^a$. Then we have $x(x^{c-1} - 1) \equiv 0 \pmod{p^a}$. Let s be a primitive root for p^a; then the solutions to $x^{c-1} \equiv 1$ are exactly the powers s^k with $(c-1)k \equiv 1 \pmod{\phi(p^a)}$, and there are $(c - 1, \phi(p^a))$ of these. Also, 0 is a solution, so we have $1 + (c - 1, \phi(p^a))$ solutions all together. Now if $m = p_1^{a_1} \cdots p_r^{a_r}$, we can count the number of solutions modulo $p_i^{a_i}$ for each i. There is a one-to-one correspondence between solutions modulo m and the set of r-tuples of solutions to the system of congruences modulo each of the prime powers. **b.** Suppose $(c - 1, \phi(m)) = 2$, then $c - 1$ is even. Because $\phi(p^a)$ is even for all prime powers, except 2, we

have $(c-1, \phi(p_i^{a_i})) = 2$ for each i. Then by part (a), we have the number of solutions $= 3^r$. If 2^1 is a prime factor, then $\phi(m) = \phi(m/2)$, and because x^c and x have the same parity, x is a solution modulo m if and only if it is a solution modulo $m/2$, so the result still holds.

13. Let $n = 3pq$, with $p < q$ odd primes, be a Carmichael number. Then by Theorem 9.27, $p-1|3pq-1 = 3(p-1)q + 3q - 1$, so $p-1|3q-1$, say, $(p-1)a = 3q-1$. Because $q > p$, we must have $a \geq 4$. Similarly, there is an integer b such that $(q-1)b = 3p-1$. Solving these two equations for p and q yields $q = (2a+ab-3)/(ab-9)$ and $p = (2b+ab-3)/(ab-9) = 1 + (2b+6)/(ab-9)$. Then because p is an odd prime greater than 3, we must have $4(ab-9) \leq 2b+6$, which reduces to $b(2a-1) \leq 21$. Because $a \geq 4$, this implies that $b \leq 3$. Then $4(ab-9) \leq 2b+6 \leq 12$, so $ab \leq 21/4$, so $a \leq 5$. Therefore, $a = 4$ or 5. If $b = 3$, then the denominator in the expression for q is a multiple of 3, so the numerator must be a multiple of 3, but that is impossible because there is no choice for a that is divisible by 3. Thus, $b = 1$ or 2. The denominator of q must be positive, so $ab > 9$, which eliminates all remaining possibilities except $a = 5$, $b = 2$, in which case $p = 11$ and $q = 17$. So the only Carmichael number of this form is $561 = 3 \cdot 11 \cdot 17$.

15. Assume $q < r$. By Theorem 9.23, $q-1|pqr-1 = (q-1)pr + pr - 1$. Therefore, $q-1|pr-1$, say, $a(q-1) = pr-1$. Similarly, $b(r-1) = pq-1$. Because $q < r$, we must have $a > b$. Solving these two equations for q and r yields $r = (p(a-1)+a(b-1))/(ab-p^2)$ and $q = (p(b-1)+b(a-1))/(ab-p^2) = 1 + (p^2+pb-p-b)/(ab-p^2)$. Because this last fraction must be an integer, we have $ab - p^2 \leq p^2 + pb - p - b$, which reduces to $a(b-1) \leq 2p^2 + p(b-1)$ or $a - 1 \leq 2p^2/b + p(b-1)/b \leq 2p^2 + p$. So there are only finitely many values for a. Likewise, the same inequality gives us $b(a-1) \leq 2p^2 + pb - p$ or $b(a-1-p) \leq 2p^2 - p$. Because $a > b$ and the denominator of the expression for q must be positive, we have that $a \geq p+1$. If $a = p+1$, we have $(p+1)(q-1) = pq - p + q - 1 = pr - 1$, which implies that $p|q$, a contradiction. Therefore, $a > p+1$, and so $a-1-p$ is a positive integer. The last inequality gives us $b \leq b(a-1-p) \leq 2p^2 - p$. Therefore, there are only finitely many values for b. Because a and b determine q and r, we see that there can be only finitely many Carmichael numbers of this form.

17. We have $q_n(ab) \equiv ((ab)^{\lambda(n)} - 1)/n = (a^{\lambda(n)}b^{\lambda(n)} - a^{\lambda(n)} - b^{\lambda(n)} + 1 + a^{\lambda(n)} + b^{\lambda(n)} - 2)/n = (a^{\lambda(n)} - 1)(b^{\lambda(n)} - 1)/n + ((a^{\lambda(n)} - 1) + (b^{\lambda(n)} - 1))/n \equiv q_n(a) + q_n(b) \pmod{n}$. At the last step, we use the fact that n^2 must divide $(a^{\lambda(n)} - 1)(b^{\lambda(n)} - 1)$, because $\lambda(n)$ is the universal exponent.

Section 10.1

1. 69, 76, 77, 92, 46, 11, 12, 14, 19, 36, 29, 84, 05, 02, 00, 00, 00, . . .

3. 10

5. **a.** $a \equiv 1 \pmod{20}$ **b.** $a \equiv 1 \pmod{30030}$ **c.** $a \equiv 1 \pmod{111111}$ **d.** $a \equiv 1 \pmod{2^{25}-1}$.

7. **a.** 31 **b.** 715,827,882 **c.** 31 **d.** 195,225,786 **e.** 1,073,741,823 **f.** 1,073,741,823

9. 8, 64, 15, 71, 36, 64, 15, 71, 36, . . .

11. First we find that $\text{ord}_{77}8$ is 10. Because $\text{ord}_5 2 = 4$, the period length is 4.

13. Using the notation of Theorem 10.4, we have $\phi(77) = 60$, so $\text{ord}_{77}x_0$ is a divisor of $60 = 2^2 3 \cdot 5$. Then the only possible values for s are the odd divisors of 60, which are 3, 5, and 15. Then we note that $2^2 \equiv 1 \pmod{3}$, $2^4 \equiv 1 \pmod{5}$, and $2^4 \equiv 16 \equiv 1 \pmod{15}$. In each case we have shown that $\text{ord}_s 2 \leq 4$. Hence by Theorem 10.4, the maximum period length is 4.

15. 1, 24, 25, 18, 12, 30, 11, 10, 21

17. Check that 7 has maximal order 1800 modulo $2^{25} - 1$. To make a large enough multiplier, raise 7 to a power relatively prime to $\phi(2^{25} - 1) = 32{,}400{,}000$, for example, to the 11th power.

19. 665

21. **a.** 8, 2, 8, 2, 8, 2, . . . **b.** 9, 12, 6, 13, 8, 18, 2, 4, 16, 3, 9, 12, 6, . . .

Section 10.2

1. We select $k = 1234$ for our random integer. Converting the plaintext into numerical equivalents results in 0700 1515 2401 0817 1907 0300 2423, where we filled out the last block with an X. Using a calculator or computational software, we find $\gamma \equiv r^k \equiv 6^{1234} \equiv 517 \pmod{2551}$. Then for each block P, we compute $\delta \equiv P \cdot b^k \equiv P \cdot 33^{1234} \equiv P \cdot 651 \pmod{2551}$. The resulting blocks are $0700 \cdot 651 \equiv 1622 \pmod{2551}$, $1515 \cdot 651 \equiv 1579 \pmod{2551}$, $2401 \cdot 651 \equiv 1839 \pmod{2551}$, $0817 \cdot 651 \equiv 1259 \pmod{2551}$, $1907 \cdot 651 \equiv 1671 \pmod{2551}$, $0300 \cdot 651 \equiv 1424 \pmod{2551}$, and $2423 \cdot 651 \equiv 855 \pmod{2551}$. Therefore, the ciphertext is (517, 1622), (517, 1579), (517, 1839), (517, 1259), (517, 1671), (517, 1424), (517, 855). To decrypt this ciphertext, we compute $\gamma^{p-1-a} \equiv 517^{2551-1-13} \equiv 517^{2537} \equiv 337 \pmod{2551}$. Then for each block of the cipher text, we compute $P \equiv 337 \cdot \delta \pmod{2551}$. For the first block, we have $337 \cdot 1622 \equiv 0700 \pmod{2551}$, which was the first block of the plaintext. The other blocks are decrypted the same way.

3. RABBIT

5. $(\gamma, s) = (2022, 833)$; to verify this signature, we compute $V_1 \equiv 2022^{833}801^{2022} \equiv 1014 \equiv 3^{823} \equiv V_2 \pmod{2657}$ using computational software.

7. Let $\delta_1 = P_1 b^k$ and $\delta_2 = P_2 b^k$ as in the ElGamal cryptosystem. If P_1 is known, it is easy to compute an inverse for P_1 modulo p. Then $b^k \equiv \overline{P_1}\delta_1 \pmod{p}$. Then it is also easy to compute an inverse for $b^k \pmod{p}$. Then $P_2 \equiv \overline{b^k}\delta_2 \pmod{p}$. Hence, the plaintext P_2 is recovered.

Section 10.3

1. **a.** 8 **b.** 5 **c.** 2 **d.** 6 **e.** 30 **f.** 20

3. **a.** At each stage of the splicing, the kth wire of one section is connected to the $S(k)$th wire, where $S(k)$ is the least positive residue of $3k - 2 \pmod{50}$. **b.** At each stage of the splicing, the kth wire of one section is connected to the $S(k)$th wire, where $S(k)$ is the least positive residue of $21K + 56 \pmod{76}$. **c.** At each stage of the splicing, the kth wire of one section is connected to the $S(k)$th wire, where $S(k)$ is the least positive residue of $2k - 1 \pmod{125}$.

Section 11.1

1. **a.** 1 **b.** 1, 4 **c.** 1, 3, 4, 9, 10, 12 **d.** 1, 4, 5, 6, 7, 9, 11, 16, 17

3. 1, −1, −1, 1

5. **a.** $\left(\frac{7}{11}\right) \equiv 7^{(11-1/2} \equiv 7^5 \equiv 49^2 \cdot 7 \equiv 5^2 \cdot 7 \equiv 3 \cdot 7 \equiv -1 \pmod{11}$ **b.** $(7, 14, 21, 28, 35) \equiv (7, 3, 10, 6, 2) \pmod{11}$ and three of these are greater than 11/2, so $\left(\frac{7}{11}\right) = (-1)^3 = -1$

7. We have $\left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)$ by Theorem 11.4. Using Theorems 11.5 and 11.6, we have: If $p \equiv 1 \pmod{8}$ then, $\left(\frac{-2}{p}\right) = (1)(1) = 1$. If $p \equiv 3 \pmod{8}$, then $\left(\frac{-2}{p}\right) = (-1)(-1) = 1$. If $p \equiv -1 \pmod{8}$, then $\left(\frac{-2}{p}\right) = (-1)(1) = -1$. If $p \equiv -3 \pmod{8}$, then $\left(\frac{-2}{p}\right) = (1)(-1) = -1$.

9. Because $p - 1 \equiv -1$, $p - 2 \equiv -2$, . . . , $(p + 1)/2 \equiv -(p - 1)/2 \pmod{p}$, we have $((p - 1)/2)!^2 \equiv -(p - 1)! \equiv 1 \pmod{p}$ by Wilson's theorem. (Because $p \equiv 3 \pmod{4}$, we have that

$(p-1)/2$ is odd, so that $(-1)^{(p-1)/2} = -1$.) By Euler's criterion, $((p-1)/2)! \equiv \left(\frac{1}{p}\right)\left(\frac{2}{p}\right)\cdots\left(\frac{(p-1)/2}{p}\right) \equiv (-1)^t \pmod{p}$, by definition of the Legendre symbol. Because $((p-1)/2)! \equiv \pm 1 \pmod{p}$, and $(p-1)/2$ is odd, we have the result.

11. If $p \equiv 1 \pmod 4$, $\left(\frac{-a}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{a}{p}\right) = 1 \cdot 1 = 1$. If $p \equiv 3 \pmod 4$, $\left(\frac{-a}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{a}{p}\right) = (-1) \cdot 1 = -1$.

13. **a.** $x \equiv 2$ or $4 \pmod 7$ **b.** $x \equiv 1 \pmod 7$ **c.** no solutions

15. Suppose that p is a prime that is at least 7. At least one of the three incongruent integers 2, 3, and 6 is a quadratic residue of p, because if neither 2 nor 3 is a quadratic residue of p, then $2 \cdot 3 = 6$ is a quadratic residue of p. If 2 is a quadratic residue, then 2 and 4 are quadratic residues that differ by 2; if 3 is a quadratic residue, then 1 and 3 are quadratic residues that differ by 2; while if 6 is a quadratic residue, then 4 and 6 are quadratic residues that differ by 2.

17. **a.** Because $p = 4n+3$, $2n+2 = (p+1)/2$. Then $x^2 \equiv (\pm a^{n+1})^2 \equiv a^{2n+2} \equiv a^{(p+1)/2} \equiv a^{(p-1)/2}a \equiv 1 \cdot a \equiv a \pmod{p}$, using the fact that $a^{(p-1)/2} \equiv 1 \pmod{p}$, because a is a quadratic residue of p. By Lemma 11.1, there are only these two solutions. **b.** By Lemma 11.1, there are exactly two solutions to $y^2 \equiv 1 \pmod{p}$, namely, $y \equiv \pm 1 \pmod{p}$. Because $p \equiv 5 \pmod 8$, -1 is a quadratic residue of p and 2 is a quadratic nonresidue of p. Because $p = 8n+5$, we have $4n+2 = (p-1)/2$ and $2n+2 = (p+3)/4$. Then $(\pm a^{n+1})^2 \equiv a^{(p+3)/4} \pmod{p}$ and $(\pm 2^{2n+1}a^{n+1})^2 \equiv 2^{(p-1)/2}a^{(p+3)/4} \equiv -a^{(p+3)/4} \pmod{p}$ by Euler's criterion. We must show that one of $a^{(p+3)/4}$ or $-a^{(p+3)/4} \equiv a \pmod{p}$. Now, a is a quadratic residue of p, so $a^{(p-1)/2} \equiv 1 \pmod{p}$ and therefore $a^{(p-1)/4}$ solves $x^2 \equiv 1 \pmod{p}$. But then $a^{(p-1)/4} \equiv \pm 1 \pmod{p}$, that is, $a^{(p+3)/4} \equiv \pm a \pmod{p}$ or $\pm a^{(p+3)/4} \equiv a \pmod{p}$, as desired.

19. $x \equiv 1$, 4, 11, or 14 (mod 15)

21. 47, 96, 135, 278, 723, 866, 905, 954 (mod 1001)

23. If $x_0^2 \equiv a \pmod{p^{e+1}}$, then $x_0^2 \equiv a \pmod{p^e}$. Conversely, if $x_0^2 \equiv a \pmod{p^e}$, then $x_0^2 = a + bp^e$ for some integer b. We can solve the linear congruence $2x_0 y \equiv -b \pmod{p}$, say, $y = y_0$. Let $x_1 = x_0 + y_0 p^e$. Then $x_1^2 \equiv x_0^2 + 2x_0 y_0 p^e = a + p^e(b + 2x_0 y_0) \equiv a \pmod{p^{e+1}}$ because $p \mid 2x_0 y_0 + b$. This is the induction step in showing that $x^2 \equiv a \pmod{p^e}$ has solutions if and only if $(\frac{a}{p}) = 1$.

25. **a.** 4 **b.** 8 **c.** 0 **d.** 16

27. Suppose $p_1, p_2, \ldots, p_n$ are the only primes of the form $4k+1$. Let $N = 4(p_1 p_2 \cdots p_n)^2 + 1$. Let q be an odd prime factor of N. Then $q \neq p_i$, $i = 1, 2, \ldots, n$, but $N \equiv 0 \pmod q$, so $4(p_1 p_2 \cdots p_n)^2 \equiv -1 \pmod q$ and therefore $(\frac{-1}{q}) = 1$, so $q \equiv 1 \pmod 4$ by Theorem 11.5.

29. Let b_1, b_2, b_3, and b_4 be four incongruent modular square roots of a modulo pq. Then each b_i is a solution to exactly one of the four systems of congruences in the text. For convenience, let the subscripts correspond to the lowercase Roman numerals of the systems. Suppose two of the b_i's were quadratic residues modulo pq. Without loss of generality, say $b_1 \equiv y_1^2 \pmod{pq}$ and $b_2 \equiv y_2^2 \pmod{pq}$. Then from systems (i) and (ii), we have that $y_1^2 \equiv b_1 \equiv x_2 \pmod q$ and $y_2^2 \equiv b_2 \equiv -x_2 \pmod q$. Therefore, both x_2 and $-x_2$ are quadratic residues modulo q, but this is impossible because $q \equiv 3 \pmod 4$. The other cases are identical. Next we show that one of the modular square roots is a quadratic residue. Because a is a quadratic residue modulo p, there exists b such that $(\pm b)^2 \equiv a \pmod p$. Likewise, there exists c such that $(\pm c)^2 \equiv a \pmod q$. One of b or $-b$ is a quadratic residue modulo p, by Exercise 11. Without loss of generality, suppose $b \equiv d^2 \pmod p$. Likewise, suppose $c \equiv e^2 \pmod q$. Solve the system of congruences $x \equiv d \pmod p$, $x \equiv e \pmod q$. Then $x^2 \equiv b \pmod p$ and $x^2 \equiv c \pmod q$. Thus, x^2 satisfies one of the four congruences in the text and hence must be one of the b_i. Therefore, this b_i is a quadratic residue modulo pq.

31. Let r be a primitive root for p and let $a \equiv r^s \pmod{p}$ and $b \equiv r^t \pmod{p}$ with $1 \le s, t \le p-1$. If $a \equiv b \pmod{p}$, then $s = t$ and so s and t have the same parity. By Theorem 11.2, we have part (i). Further, we have $ab \equiv r^{s+t} \pmod{p}$. Then the right-hand side of (ii) is 1 exactly when s and t have the same parity, which is exactly when the left-hand side is 1. This proves part (ii). Finally, because $a^2 \equiv r^{2s} \pmod{p}$ and $2s$ is even, we must have that a^2 is a quadratic residue modulo p, proving part (iii).

33. If r is a primitive root of q, then the set of all primitive roots is given by $\{r^k : (k, \phi(q)) = (k, 2p) = 1\}$. So the $p-1$ numbers $\{r^k : k \text{ is odd and } k \neq p,\ 1 \le k < 2p\}$ are all the primitive roots of q. On the other hand, q has $(q-1)/2 = p$ quadratic residues, which are given by $\{r^2, r^4, \ldots, r^{2p}\}$. This set has no intersection with the first one.

35. First suppose $p = 2^{2^n} + 1$ is a Fermat prime and let r be a primitive root for p. Then $\phi(p) = 2^{2^n}$. Then an integer a is a nonresidue if and only if $a = r^k$ with k odd. But then $(k, \phi(p)) = 1$, so a is also a primitive root. Conversely, suppose that p is an odd prime and every quadratic nonresidue of p is also a primitive root of p. Let r be a particular primitive root of p. Then r^k is a quadratic nonresidue and hence a primitive root for p if and only if k is odd. But this implies that every odd number is relatively prime to $\phi(p)$, so $\phi(p)$ must be a power of 2. Thus, $p = 2^b + 1$ for some b. If b had a nontrivial odd divisor, then we could factor p as a difference of b powers, contradicting the primality of of p. Therefore, b is a power of 2 and so p is a Fermat prime.

37. **a.** We have $q = 2p + 1 = 2(4k+3) + 1 = 8k + 7$, so $(\frac{2}{q}) = 1$ by Theorem 11.6. Then by Euler's criterion, $2^{(q-1)/2} \equiv 2^p \equiv 1 \pmod{q}$. Therefore, $q \mid 2^p - 1$. **b.** $11 = 4(2) + 3$ and $23 = 2(11) + 1$, so $23 \mid 2^{11} - 1 = M_{11}$, by part (a); $23 = 4(5) + 3$ and $47 = 2(23) + 1$, so $47 \mid M_{23}$; $251 = 4(62) + 3$ and $503 = 2(251) + 1$, so $503 \mid M_{251}$.

39. Let $q = 2k + 1$. Because q does not divide $2^p + 1$, we must have, by Exercise 38, that $k \equiv 0$ or $3 \pmod{4}$. That is, $k \equiv 0, 3, 4$, or $7 \pmod{8}$. Then $q \equiv 2(0, 3, 4, \text{or } 7) + 1 \equiv \pm 1 \pmod{8}$.

41. Note that $\left(\frac{j(j+1)}{p}\right) = \left(\frac{j \cdot j(1+\overline{j})}{p}\right) = \left(\frac{j^2(1+\overline{j})}{p}\right) = \left(\frac{(1+\overline{j})}{p}\right)$ because j^2 is a perfect square. Then $\sum_{j=1}^{p-2} \left(\frac{j(j+1)}{p}\right) = \sum_{j=1}^{p-2} \left(\frac{\overline{j}+1}{p}\right) = \sum_{j=2}^{p-1} \left(\frac{j}{p}\right) = \sum_{j=1}^{p-1} \left(\frac{j}{p}\right) - 1 = -1$. Here we have used the method in the solution to Exercise 10 to evaluate the last sum, and the fact that as j runs through the values 1 through $p-2$, so does $\overline{j}$.

43. Let r be a primitive root of p. Then $x^2 \equiv a \pmod{p}$ has a solution if and only if $2 \operatorname{ind}_r x \equiv \operatorname{ind}_r a \pmod{p-1}$ has a solution in $\operatorname{ind}_r x$. Because $p-1$ is even, the last congruence is solvable if and only if $\operatorname{ind}_r a$ is even, which happens when $a = r^2, r^4, \ldots, r^{p-1}$, i.e., $(p-1)/2$ times.

45. $q = 2(4k+1) + 1 = 8k + 3$, so 2 is a quadratic nonresidue of q. By Exercise 33, 2 is a primitive root.

47. Check that $q \equiv 3 \pmod{4}$, so -1 is a quadratic nonresidue of q. Because $4 = 2^2$, we have $\left(\frac{-4}{q}\right) = \left(\frac{-1}{q}\right)\left(\frac{2^2}{q}\right) = (-1)(1) = -1$. Therefore, -4 is a nonresidue of q. By Exercise 33, -4 is a primitive root.

49. **a.** By adding $(\overline{2}b)^2$ to both sides, we complete the square. **b.** There are four solutions to $x^2 \equiv C + a \pmod{pq}$. From each, subtract $\overline{2}b$. **c.** DETOUR

51. **a.** By noting this, the second player can tell which cards dealt are quadratic residues, because the ciphertext will also be quadratic residues modulo p. **b.** All ciphers will be quadratic residues modulo p.

53. 1, 3, 4

Section 11.2

1. **a.** -1 **b.** 1 **c.** 1 **d.** 1 **e.** 1 **f.** 1

3. If $p \equiv 1 \pmod 6$, there are 2 cases: If $p \equiv 1 \pmod 4$, then $\left(\frac{-1}{p}\right) = 1$ and $\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right) = \left(\frac{1}{3}\right) = 1$. So $\left(\frac{-3}{p}\right) = 1$. If $p \equiv 3 \pmod 4$, then $\left(\frac{-1}{p}\right) = -1$ and $\left(\frac{3}{p}\right) = -\left(\frac{p}{3}\right)$, so $\left(\frac{-3}{p}\right) = (-1)(-1) = 1$. If $p \equiv -1 \pmod 6$ and $p \equiv 1 \pmod 4$, then $\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = 1 \cdot \left(\frac{p}{3}\right) = \left(\frac{-1}{3}\right) = -1$. If $p \equiv 3 \pmod 4$, then $\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = (-1)\left(-\left(\frac{p}{3}\right)\right) = \left(\frac{p}{3}\right) = \left(\frac{-1}{3}\right) = -1$.

5. $p \equiv 1, 3, 9, 19, 25,$ or $27 \pmod{28}$

7. **a.** $F_1 = 2^{2^1} + 1 = 5$. We find that $3^{(F_1-1)/2} = 3^{(5-1)/2} = 3^2 = 9 \equiv -1 \pmod{F_1}$. Hence by Pepin's test, we come (to the already obvious) conclusion that $F_1 = 5$ is prime. **b.** $F_3 = 2^{2^3} + 1 = 257$. We find that $3^{(F_3-1)/2} = 3^{(257-1)/2} = 3^{128} \equiv (3^8)^{16} \equiv 136^{16} \equiv (136^4)^4 \equiv 64^4 \equiv (64^2)^2 \equiv 241^2 \equiv 256 \equiv -1 \pmod{257}$. Hence by Pepin's test, $F_3 = 257$ is prime. **c.** $3^{32768} \equiv 3^{255 \cdot 128} 3^{128} \equiv 94^{128} 3^{128} \equiv -1 \pmod{F_4}$.

9. **a.** The lattice points in the rectangle are the points (i, j) where $0 < i < p/2$ and $0 < j < q/2$. There are the lattice points (i, j) with $i = 1, 2, \ldots, (p-1)/2$ and $j = 1, 2, \ldots, (q-1)/2$. Consequently, there are $(p-1)/2 \cdot (q-1)/2$ such lattice points. **b.** The points on the diagonal connecting **O** and **C** are the points (x, y) where $y = (q/p)x$. Suppose that x and y are integers with $y = (q/p)x$. Then $py = qx$. Because $(p, q) = 1$, it follows that $p \mid x$, which is impossible if $0 < x < p/2$. Hence, there are no lattice points on this diagonal. **c.** The number of lattice points in the triangle with vertices **O, A,** and **C** is the number of lattice points (i, j) with $i = 1, 2, \ldots, (p-1)/2$ and $1 \le j \le iq/p$. For a fixed value of i in the indicated range, there are $[iq/p]$ lattice points (i, j) in the triangle. Hence, the total number of lattice points in the triangle is $\sum_{i=1}^{(p-1)/2} [iq/p]$. **d.** The number of lattice points in the triangle with vertices **O, B,** and **C** is the number of lattice points (i, j) with $j = 1, 2, \ldots, (q-1)/2$ and $1 \le i < jp/q$. For a fixed value of j in the indicated range, there are $[jp/q]$ lattice points (i, j) in the triangle. Hence the total number of lattice points in the triangle is $\sum_{j=1}^{(q-1)/2} [jp/q]$. **e.** Because there are $(p-1)/2 \cdot (q-1)/2$ lattice points in the rectangle, and no points on the diagonal **OC,** the sum of the numbers of lattice points in the triangles **OBC** and **OAC** is $(p-1)/2 \cdot (q-1)/2$. By parts (b) and (c), it follows that $\sum_{j=1}^{(p-1)/2} [jq/p] + \sum_{j=1}^{(q-1)/2} [jp/q] = (p-1)/2 \cdot (q-1)/2$. By Lemma 11.3, it follows that $\left(\frac{p}{q}\right) = (-1)^{T(p,q)}$ and $\left(\frac{q}{p}\right) = (-1)^{T(q,p)}$ where $T(p, q) = \sum_{j=1}^{(p-1)/2} [jp/q]$ and $T(q, p) = \sum_{j=1}^{(q-1)/2} [jq/p]$. We conclude that $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)/2 \cdot (q-1)/2}$. This is the law of quadratic reciprocity.

11. First suppose $a = 2$. Then we have $p \equiv \pm q \pmod 8$ and so $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$ by Theorem 11.6. Now suppose a is an odd prime. If $p \equiv q \pmod{4a}$, then $p \equiv q \pmod a$ and so $\left(\frac{q}{a}\right) = \left(\frac{p}{a}\right)$. And because $p \equiv q \pmod 4$, $(p-1)/2 \equiv (q-1)/2 \pmod 2$. Then by Theorem 11.7, $\left(\frac{a}{p}\right) = \left(\frac{p}{a}\right)(-1)^{(p-1)/2 \cdot (a-1)/2} = \left(\frac{q}{a}\right)(-1)^{(q-1)/2 \cdot (a-1)/2} = \left(\frac{a}{q}\right)$. But if $p \equiv -q \pmod{4a}$, then $p \equiv -q \pmod a$ and so $\left(\frac{-q}{a}\right) = \left(\frac{p}{a}\right)$. And because $p \equiv -q \pmod 4$, $(p-1)/2 \equiv (q-1)/2 + 1 \pmod 2$. Then by Theorem 11.7, $\left(\frac{a}{p}\right) = \left(\frac{p}{a}\right)(-1)^{(p-1)/2 \cdot (a-1)/2} = \left(\frac{-q}{a}\right)(-1)^{((q-1)/2+1) \cdot (a-1)/2} = \left(\frac{-1}{a}\right)(-1)^{(a-1)/2}\left(\frac{a}{q}\right) = \left(\frac{a}{q}\right)$. The general case follows from the multiplicativity of the Legendre symbol.

13. **a.** Recall that $e^{xi} = 1$ if and only if x is a multiple of 2π. First, we compute $(e^{(2\pi i/n)k})^n = e^{(2\pi i/n)nk} = (e^{(2\pi i)})^k = 1^k = 1$, so $e^{(2\pi i/n)k}$ is an nth root of unity. Now, if $(k, n) = 1$, then

$((2\pi i/n)k)a$ is a multiple of $2\pi i$ if and only if $n|a$. Therefore, $a = n$ is the least positive integer for which $(e^{(2\pi i/n)k})^a = 1$. Therefore, $e^{(2\pi i/n)k}$ is a primitive nth root of unity. Conversely, suppose $(k, n) = d > 1$. Then $(e^{(2\pi i/n)k})^{(n/d)} = e^{(2\pi i)k/d} = 1$, because k/d is an integer, and so in this case $e^{(2\pi i/n)k}$ is not a primitive nth root of unity. **b.** Let $m = l + kn$ where k is an integer. Then $\zeta^m = \zeta^{l+kn} = \zeta^l\zeta^{kn} = \zeta^l$. Now suppose ζ is a primitive nth root of unity and that $\zeta^m = \zeta^l$, and without loss of generality, assume $m \geq l$. From the first part of this exercise, we may take $0 \leq l \leq m < n$. Then $0 = \zeta^m - \zeta^l = \zeta^l(\zeta^{m-l} - 1)$. Hence, $\zeta^{m-l} = 1$. Because n is the least positive integer such that $\zeta^n = 1$, we must have $m - l = 0$. **c.** First, $f(z+1) = e^{2\pi i(z+1)} - e^{-2\pi i(z+1)} = e^{2\pi iz}e^{2\pi i} - e^{-2\pi iz}e^{-2\pi i} = e^{2\pi iz}1 - e^{-2\pi iz}1 = f(z)$. Next, $f(-z) = e^{-2\pi iz} - e^{2\pi iz} = -(e^{2\pi iz} - e^{-2\pi iz}) = -f(z)$. Finally, suppose $f(z) = 0$. Then $0 = e^{2\pi iz} - e^{-2\pi iz} = e^{-2\pi iz}(e^{4\pi iz} - 1)$, so $e^{4\pi iz} = 1$. Therefore, $4\pi iz = 2\pi in$ for some integer n, and so $z = n/2$. **d.** Fix y and consider $g(x) = x^n - y^n$ and $h(x) = (x - y)(\zeta x - \zeta^{-1}y)\cdots(\zeta^{n-1}x - \zeta^{-(n-1)}y)$ as polynomials in x. Both polynomials have degree n. The leading coefficient in $h(x)$ is $\zeta^{1+2+\cdots+n-1} = \zeta^{n(n-1)/2} = (\zeta^n)^{(n-1)/2} = 1$, because $n - 1$ is even. So both polynomials are monic. Further, note that $g(\zeta^{-2k}y) = (\zeta^{-2k}y)^n - y^n = y^n - y^n = 0$ for $k = 0, 1, 2, \ldots, n-1$. Also, $h(\zeta^{-2k}y)$ has $(\zeta^k\zeta^{-2k}y - \zeta^{-k}y) = (\zeta^{-k}y - \zeta^{-k}y) = 0$ as one of its factors. So g and h are monic polynomials sharing these n distinct zeros (because $-2k$ runs through a complete set of residues modulo n, by Theorem 4.7) By the fundamental theorem of algebra, g and h are identical.

e. Let $x = e^{2\pi iz}$ and $y = e^{-2\pi iz}$ in the identity from part (d). Then the right-hand side becomes $\prod_{k=0}^{n-1}(\zeta^k e^{2\pi iz} - \zeta^{-k}e^{-2\pi iz}) = \prod_{k=0}^{n-1}(e^{2\pi i(z+k/n)} - e^{-2\pi i(z+k/n)}) = \prod_{k=0}^{n-1} f\left(z + \frac{k}{n}\right) = f(z)\prod_{k=1}^{(n-1)/2} f\left(z + \frac{k}{n}\right)\prod_{k=(n+1)/2}^{n-1} f\left(z + \frac{k}{n}\right)$. From the identities in part (c), this last product becomes $\prod_{k=(n+1)/2}^{n-1} f\left(z + \frac{k}{n}\right) = \prod_{k=1}^{(n-1)/2} f\left(z + \frac{n-k}{n}\right) = \prod_{k=1}^{(n-1)/2} f\left(z + 1 - \frac{k}{n}\right) = \prod_{k=1}^{(n-1)/2} f\left(z - \frac{k}{n}\right)$. So the product above is equal to $f(z)\prod_{k=1}^{(n-1)/2} f\left(z + \frac{k}{n}\right)\prod_{k=1}^{(n-1)/2} f\left(z - \frac{k}{n}\right) = f(z)\prod_{k=1}^{(n-1)/2} f\left(z + \frac{k}{n}\right) f\left(z - \frac{k}{n}\right)$. Then noting that the left side of the identity in part (d) is $(e^{2\pi iz})^n - (e^{-2\pi iz})^n = e^{2\pi inz} - e^{-2\pi inz} = f(nz)$ finishes the proof.

f. For $l = 1, 2, \ldots, (p-1)/2$, let k_l be the least positive residue of la modulo p. Then $\prod_{l=1}^{(p-1)/2} f\left(\frac{la}{p}\right) = \prod_{l=1}^{(p-1)/2} f\left(\frac{k_l}{p}\right)$ by the perodicity of f established in part (c). We break this product into two pieces $\prod_{k_l<p/2} f\left(\frac{k_l}{p}\right)\prod_{k_l>p/2} f\left(\frac{k_l}{p}\right) = \prod_{k_l<p/2} f\left(\frac{k_l}{p}\right)\prod_{k_l>p/2} -f\left(\frac{-k_l}{p}\right) = \prod_{k_l<p/2} f\left(\frac{k_l}{p}\right)\prod_{k_l>p/2} f\left(\frac{p-k_l}{p}\right) = \prod_{l=1}^{(p-1)/2} f\left(\frac{l}{p}\right)(-1)^N$, where N is the number of k_l exceeding $p/2$. But by Gauss' lemma, $(-1)^N = \left(\frac{a}{p}\right)$. This establishes the identity. **g.** Let $z = l/p$ and $n = q$ in the identities in parts (e) and (f). Then we have $\left(\frac{q}{p}\right) = \prod_{l=1}^{(p-1)/2} f\left(\frac{lq}{p}\right) \Big/ f\left(\frac{l}{p}\right) = \prod_{l=1}^{(p-1)/2}\prod_{k=1}^{(q-1)/2} f\left(\frac{l}{p} + \frac{k}{q}\right) f\left(\frac{l}{p} - \frac{k}{q}\right) = \prod_{l=1}^{(p-1)/2}\prod_{k=1}^{(q-1)/2} f\left(\frac{k}{q} + \frac{l}{p}\right) f\left(\frac{k}{q} - \frac{l}{p}\right)(-1)^{(p-1)/2\cdot(q-1)/2}$, where we have used the fact that $f(-z) = -f(z)$ and the fact that there are exactly $(p-1)/2 \cdot (q-1)/2$ factors in the double product. But, by symmetry, this is exactly the expression for $\left(\frac{p}{q}\right)(-1)^{(p-1)/2\cdot(q-1)/2}$, which completes the proof.

15. Because $p \equiv 1 \pmod 4$, we have $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)$. And because $p \equiv 1 \pmod q$ for all primes $q \leq 23$, then $\left(\frac{p}{q}\right) = \left(\frac{1}{q}\right) = 1$. Then if a is an integer with $1 < a < 29$ and prime factorization $a = p_1 p_2 \cdots p_k$, then each $p_i < 29$ and $\left(\frac{a}{p}\right) = \left(\frac{p_1}{p}\right) \cdots \left(\frac{p_k}{p}\right) = 1^k = 1$. So there are no quadratic nonresidues modulo p less than 29. Further, because a quadratic residue must be an even power of any primitive root r, then r^1 cannot be less than 29.

17. **a.** If $a \in T$, then $a = qk$ for some $k = 1, 2, \ldots (p-1)/2$. So $1 \leq a \leq q(p-1)/2 < (pq-1)/2$. Further, because $k \leq (p-1)/2$, and p is prime, we have $(p, k) = 1$. Because $(q, p) = 1$, then $(a, p) = (qk, p) = 1$, so $a \in S$, and hence $T \subset S$. Now suppose $a \in S - T$. Then $1 \leq a \leq (pq-1)/2$ and $(a, p) = 1$, and because $a \notin T$, then $a \neq qk$ for any k. Thus, $(a, q) = 1$, so $(a, pq) = 1$, and so $a \in R$. Thus, $S - T \subset R$. Conversely, if $a \in R$, then $1 \leq a \leq (pq-1)/2$ and $(a, pq) = 1$, so certainly $(a, q) = 1$, and so a is not a multiple of q, and hence $a \notin T$. Hence, $a \in S - T$. Thus, $R \subset S - T$. Therefore, $R = S - T$. **b.** Because by part (a), $R = S - T$ we have $\prod_{a \in S} a = \prod_{a \in R} a \prod_{a \in T} a = A(q \cdot 2q \cdots ((p-1)/2)a) = Aq^{(p-1)/2}((p-1)/2)! \equiv A\left(\frac{q}{p}\right)((p-1)/2)! \pmod p$ by Euler's criterion. Note that $(pq-1)/2 = p(q-1)/2 + (p-1)/2$, so that we can evaluate $\prod_{a \in S} a \equiv ((p-1)!)^{(q-1)/2}((p-1)/2)! \equiv (-1)^{(q-1)/2}((p-1)/2)! \pmod p$ by Wilson's theorem. When we set these two expressions congruent to each other modulo p and cancel, we get $A \equiv (-1)^{(q-1)/2}\left(\frac{q}{p}\right)$, as desired. **c.** Because the roles of p and q are identical in the hypotheses and in parts (a) and (b), the result follows by symmetry. **d.** Assume that $(-1)^{(q-1)/2}\left(\frac{q}{p}\right) = (-1)^{(p-1)/2}\left(\frac{p}{q}\right)$. By part (b), $A \equiv \pm 1 \pmod p$, and by part (c), $A \equiv \pm 1 \pmod q$. So by the Chinese remainder theorem, we have $A \equiv \pm 1 \pmod{pq}$. Conversely, suppose $A \equiv 1 \pmod{pq}$. Then $A \equiv 1 \pmod p$ and $A \equiv 1 \pmod q$. Then by parts (b) and (c), we have $(-1)^{(q-1)/2}\left(\frac{q}{p}\right) \equiv A \equiv 1 \pmod p$ and $(-1)^{(p-1)/2}\left(\frac{p}{q}\right) \equiv A \equiv 1 \pmod q$. We conclude that $(-1)^{(q-1)/2}\left(\frac{q}{p}\right) = (-1)^{(p-1)/2}\left(\frac{p}{q}\right)$, because each side is equal to 1. A similar argument works if $A \equiv -1 \pmod{pq}$. **e.** If a is an integer in R, it is in the range $1 \leq a \leq (pq-1)/2$ and therefore its additive inverse modulo pq is in the range $(pq+1)/2 \leq -a \leq pq - 1$ in the set of reduced residue classes. By the Chinese remainder theorem, the congruence $a^2 \equiv 1 \pmod{pq}$ has exactly four solutions, $1, -1, b$, and $-b \pmod{pq}$, and the congruence $a^2 \equiv -1 \pmod{pq}$ has solutions if and only $p \equiv q \equiv 1 \pmod 4$, and in this case it has exactly four solutions $i, -i, ib$, and $-ib \pmod{pq}$. Now for each element $a \in R$, $(a, pq) = 1$, so a has a multiplicative inverse v. By the remark above, exactly one of $v, -v$ is in R. We let U be the set of those elements that are their own inverse or their own negative inverse, that is, let $U = \{a \in R | a^2 \equiv \pm 1 \pmod{pq}\}$. Then when we compute A, all other elements will be paired with another element that is either its inverse or the negative of its inverse. Thus, we have $A = \prod_{a \in R} a \equiv \pm \prod_{a \in U} a \pmod{pq}$. So if $p \equiv q \equiv 1 \pmod{pq}$, then $A \equiv \pm \prod_{a \in U} a \equiv \pm(1 \cdot b \cdot i \cdot ib) \equiv b^2 i^2 \equiv \mp 1 \pmod{pq}$. Conversely, in the other case, $A \equiv \prod_{a \in U} a \equiv \pm(1 \cdot c) \not\equiv \pm 1 \pmod{pq}$, which completes the proof. **f.** By parts (d) and (e), we have that $(-1)^{(q-1)/2}\left(\frac{q}{p}\right) = (-1)^{(p-1)/2}\left(\frac{p}{q}\right)$ if and only if $p \equiv q \equiv 1 \pmod 4$. So if $p \equiv q \equiv 1 \pmod 4$, we have $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)$. But if $p \equiv 1 \pmod 4$ while $q \equiv 3 \pmod 4$, then we must have $-\left(\frac{q}{p}\right) \neq \left(\frac{p}{q}\right)$, which means we must change the sign and have $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)$.

The case where $p \equiv 3 \pmod 4$ but $q \equiv 1 \pmod 4$ is identical. If $p \equiv q \equiv 3 \pmod 4$, then we must have $-\left(\frac{q}{p}\right) \neq -\left(\frac{p}{q}\right)$ so that we must have $-\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)$, which concludes the proof.

Section 11.3

1. **a.** 1 **b.** -1 **c.** 1 **d.** 1 **e.** -1 **f.** 1

3. 1, 7, 13, 17, 19, 29, 37, 49, 61, 67, 71, 77, 83, 91, 101, 103, 107, 113, or 119 (mod 120)

5. The pseudo-squares modulo 21 are 5, 17, and 20.

7. The pseudo-squares modulo 143 are 1, 3, 4, 9, 12, 14, 16, 23, 25, 27, 36, 38, 42, 48, 49, 53, 56, 64, 69, 75, 81, 82, 92, 100, 103, 108, 113, 114, 126, and 133.

9. Because n is odd and square-free, n has prime factorization $n = p_1 p_2 \cdots p_r$. Let b be one of the $(p_1 - 1)/2$ quadratic nonresidues of p_1, so that $\left(\frac{b}{p_1}\right) = -1$. By the Chinese remainder theorem, let a be a solution to the system of linear congruences

$$\begin{aligned} x &\equiv b \pmod{p_1} \\ x &\equiv 1 \pmod{p_2} \\ &\vdots \\ x &\equiv 1 \pmod{p_r}. \end{aligned}$$

Then $\left(\frac{a}{p_1}\right) = \left(\frac{b}{p_1}\right) = -1$, $\left(\frac{a}{p_2}\right) = \left(\frac{1}{p_2}\right) = 1, \ldots, \left(\frac{a}{p_r}\right) = \left(\frac{1}{p_r}\right) = 1$.
Therefore, $\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\cdots\left(\frac{a}{p_r}\right) = (-1)\cdot 1 \cdots 1 = -1$.

11. **a.** Note that $(a, b) = (b, r_1) = (r_1, r_2) = \cdots = (r_{n-1}, r_n) = 1$ and because the q_i are even, the r_i are odd. Because $r_0 = b$ and $a \equiv \epsilon_1 r_1 \pmod b$, we have $\left(\frac{a}{b}\right) = \left(\frac{\epsilon_1 r_1}{r_0}\right) = \left(\frac{\epsilon_1}{r_0}\right)\left(\frac{r_1}{r_0}\right) = \left(\frac{\epsilon_1}{r_0}\right)\left(\frac{r_0}{r_1}\right)(-1)^{(r_0-1)/2\cdot(r_1-1)/2}$ by Theorem 11.11. If $\epsilon_1 = 1$, then $\left(\frac{a}{b}\right) = (-1)^{(r_0-1)/2\cdot(\epsilon_1 r_1-1)/2}\left(\frac{r_0}{r_1}\right)$
If $\epsilon_1 = -1$, then $\left(\frac{\epsilon_1}{r_0}\right) = (-1)^{(r_0-1)/2}$ and we have $\left(\frac{a}{b}\right) = (-1)^{(r_0-1)/2\cdot(r_1+1)/2}\left(\frac{r_0}{r_1}\right) = (-1)^{(r_0-1)/2\cdot(-r_1-1)/2}\left(\frac{r_0}{r_1}\right) = (-1)^{(r_0-1)/2\cdot(\epsilon_1 r_1-1)/2}\left(\frac{r_0}{r_1}\right)$, because $(r_1 + 1)/2$ and $(-r_1 - 1)/2$ have the same parity. Similarly, $\left(\frac{r_0}{r_1}\right) = (-1)^{(r_1-1)/2\cdot(\epsilon_2 r_2-1)/2}\left(\frac{r_1}{r_2}\right)$,
so $\left(\frac{a}{b}\right) = (-1)^{(r_0-1)/2\cdot(\epsilon_1 r_1-1)/2+(r_1-1)/2\cdot(\epsilon_2 r_2-1)/2}\left(\frac{r_1}{r_2}\right)$. Proceed inductively until the last step, when $\left(\frac{r_n}{r_{n-1}}\right) = \left(\frac{1}{r_{n-1}}\right) = 1$. **b.** If either $r_{i-1} \equiv 1 \pmod 4$ or $\epsilon_i r_i \equiv 1 \pmod 4$, then $(r_{i-1} - 1)/2 \cdot (\epsilon_1 r_i - 1)/2$ is even. Otherwise, that is, if $r_{i-1} \equiv \epsilon_i r_i \equiv 3 \pmod 4$, then $(r_{i-1} - 1)/2 \cdot (\epsilon_i r_i - 1)/2$ is odd. Then the exponent in part (a) is even or odd as T is even or odd.

13. **a.** -1 **b.** -1 **c.** -1

15. Let $n_1 = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$ and $n_2 = q_1^{b_1} q_2^{b_2} \cdots q_s^{b_s}$ be the prime factorizations of n_1 and n_2. Then by the definition of the Kronecker symbol, we have $\left(\frac{a}{n_1 n_2}\right) = \left(\frac{a}{p_1}\right)^{a_1} \cdots \left(\frac{a}{p_r}\right)^{a_r}\left(\frac{a}{q_1}\right)^{b_1} \cdots \left(\frac{a}{q_s}\right)^{b_s} = \left(\frac{a}{n_1}\right)\left(\frac{a}{n_2}\right)$.

17. If a is odd, then by Exercise 16, we have $\left(\frac{a}{n_1}\right) = \left(\frac{n_1}{|a|}\right)$. By Theorem 11.10($i$), we have $\left(\frac{n_1}{|a|}\right) = \left(\frac{n_2}{|a|}\right) = \left(\frac{a}{n_2}\right)$, using Exercise 16 again. If a is a multiple of 4, say, $a = 2^s t$ with $s \geq 2$ and t odd, Exercise 16 gives $\left(\frac{a}{n_1}\right) = \left(\frac{2}{n_1}\right)^s (-1)^{(t-1)/2\cdot(n_1-1)/2}\left(\frac{n_1}{|t|}\right)$ and $\left(\frac{a}{n_2}\right) =$