$\left(\frac{2}{n_2}\right)^s (-1)^{(t-1)/2\cdot(n_2-1)/2}\left(\frac{n_2}{|t|}\right)$. Because $n_1 \equiv n_2 \pmod{|\, t\,|}$, we have $\left(\frac{n_1}{|t|}\right) = \left(\frac{n_2}{|t|}\right)$, and because $4 \mid a$, $n_1 \equiv n_2 \pmod 4$, and so $(-1)^{(t-1)/2\cdot(n_1-1)/2} = (-1)^{(t-1)/2\cdot(n_2-1)/2}$. Now $a \equiv 0 \pmod 4$, so $s \geq 2$. If s is 2, then certainly $\left(\frac{2}{n_1}\right)^2 = \left(\frac{2}{n_2}\right)^2$. If $s > 2$, then $8 \mid a$ and $n_1 \equiv n_2 \pmod 8$, so $\left(\frac{2}{n_1}\right) = (-1)^{(n_1^2-1)/8} = (-1)^{(n_2^2-1)/8} = \left(\frac{2}{n_2}\right)$. Therefore, $\left(\frac{a}{n_1}\right) = \left(\frac{a}{n_2}\right)$.

19. If $a \equiv 1 \pmod 4$, then $|a| \equiv 1 \pmod 4$ if $a > 0$ and $|a| \equiv -1 \pmod 4$ if $a < 0$, so by Exercise 16 we have $\left(\frac{a}{|a|-1}\right) = \left(\frac{|a|-1}{|a|}\right) = \left(\frac{-1}{|a|}\right) = (-1)^{(|a|-1)/2} = 1$ if $a > 0$ and $= -1$ if $a < 0$. If $a \equiv 0 \pmod 4$, $a = 2^s t$ with t odd and $|t| \geq 3$, then by Exercise 16 $\left(\frac{a}{|a|-1}\right) = \left(\frac{2}{|a|-1}\right)^s (-1)^{(t-1)/2}\left(\frac{|a|-1}{|t|}\right)$. Because $s \geq 2$, check that $\left(\frac{2}{|a|-1}\right)^s = 1$, $(|\, a\,| - 1 \equiv 7 \pmod 8$ if $s > 2)$. Also, $(-1)^{(t-1)/2}\left(\frac{|a|-1}{|t|}\right) = (-1)^{(t-1)/2}\left(\frac{-1}{|t|}\right) = (-1)^{(t-1)/2+(|t|-1)/2} = 1$ if $t > 0$ and $= -1$ if $t < 0$.

Section 11.4

1. We have $2^{(561-1)/2} = 2^{280} = \left(2^{10}\right)^{28} \equiv (-98)^{28} \equiv \left(-98^2\right)^{14} \equiv 67^{14} \equiv \left(67^2\right)^7 \equiv 1^7 = 1 \pmod{561}$. Furthermore, we see that $\left(\frac{2}{561}\right) = 1$ because $561 \equiv 1 \pmod 8$. But $561 = 3 \cdot 11 \cdot 17$ is not prime.

3. Suppose that n is an Euler pseudoprime to both the bases a and b. Then $a^{(n-1)/2} \equiv \left(\frac{a}{n}\right)$ and $b^{(n-1)/2} \equiv \left(\frac{b}{n}\right) \pmod n$. It follows that $(ab)^{(n-1)/2} \equiv \left(\frac{a}{n}\right)\left(\frac{b}{n}\right) = \left(\frac{ab}{n}\right) \pmod n$. Hence, n is an Euler pseudoprime to the base ab.

5. Suppose that $n \equiv 5 \pmod 8$ and n is an Euler pseudoprime to the base 2. Because $n \equiv 5 \pmod 8$, we have $\left(\frac{2}{n}\right) = -1$. Because n is an Euler pseudoprime to the base 2, we have $2^{(n-1)/2} \equiv \left(\frac{2}{n}\right) = -1 \pmod n$. Write $n - 1 = 2^2 t$ where t is odd. Because $2^{(n-1)/2} \equiv 2^{2t} \equiv -1 \pmod n$, n is a strong pseudoprime to the base 2.

7. $n \equiv 5 \pmod{40}$

9. 80

Section 11.5

1. 1229

3. Because $p, q \equiv 3 \pmod 4$, -1 is not a quadratic residue modulo p or q. If the four square roots are found using the method in Example 9.19, then only one of each possibility for choosing $+$ or $-$ can yield a quadratic residue in each congruence, so there is only one system that results in a square.

5. If Paula chooses $c = 13$, then $v = 713$, which is a quadratic residue of 1411, and which has square root $u = 837 \pmod{1411}$. Her random number is 822, so she computes $x \equiv 822^2 \equiv 1226 \pmod{1411}$ and $y \equiv v\overline{x} \equiv 713 \cdot 961 \equiv 858 \pmod{1411}$. She sends $x = 1226$, $y = 858$ to Vince. Vince checks that $xy \equiv 1226 \cdot 858 \equiv 713 \pmod{1411}$ and then sends the bit $b = 1$ to Paula, so she computes $\overline{r} \equiv \overline{822} \equiv 1193 \pmod{1411}$ and $u\overline{r} \equiv 837 \cdot 1193 \equiv 964 \pmod{1411}$, which she sends to Vince. Because Vince sent $b = 1$, he computes $964^2 \equiv 858 \pmod{1411}$ and notes that it is indeed equal to y.

7. The prover sends $x = 1403^2 = 1{,}968{,}409 \equiv 519 \pmod{2491}$. The verifier sends $\{1, 5\}$. The prover sends $y = 1425$. The verifier computes $y^2 z = 1425^2 \cdot 197 \cdot 494 \equiv 519 \equiv x \pmod{2491}$

9. **a.** 959, 1730, 2895, 441, 2900, 2684 **b.** 1074 **c.** $1074^2 \cdot 959 \cdot 1730 \cdot 441 \cdot 2684 \equiv 336 \equiv 403^2 \pmod{3953}$

11. If Paula sends back a to Vince, then $a^2 \equiv w^2 \pmod{n}$, with $a \not\equiv w \pmod{n}$. Then $a^2 - w^2 = (a-w)(a+w) \equiv 0 \pmod{n}$. By computing $(a-w, n)$ and $(a+w, n)$, Vince will likely produce a nontrivial factor of n.

Section 12.1

1. **a.** $.4$ **b.** $.41\overline{6}$ **c.** $.\overline{923076}$ **d.** $.5\overline{3}$ **e.** $.\overline{009}$ **f.** $.\overline{000999}$

3. **a.** 3/25 **b.** 11/90 **c.** 4/33

5. $b = 2^r 3^s 5^t 7^u$, with r, s, t, and u nonnegative integers

7. **a.** pre-period 1, period 0 **b.** pre-period 2, period 0 **c.** pre-period 1, period 4 **d.** pre-period 2, period 0 **e.** pre-period 1, period 1 **f.** pre-period 2, period 4

9. **a.** 3 **b.** 11 **c.** 37 **d.** 101 **e.** 41 and 271 **f.** 7 and 13

11. Using the construction from Theorem 12.2 and Example 12.1, we use induction to show that $c_k = k - 1$ and $\gamma_k = (kb - k + 1)/(b-1)^2$. Clearly, $c_1 = c$ and $\gamma_1 = b/(b-1)^2$. The induction step is as follows: $c_{k+1} = \left[b\gamma_k\right] = \left[(kb^2 - bk + b)/(b-1)^2\right] = \left[(k(b-1)^2 + b(k+1) - k)/(b-1)^2\right] = \left[k + (b(k+1) - k)/(b-1)^2\right] = k$, and $\gamma_{k+1} = ((k+1)b - k)/(b-1)^2$, if $k \neq b - 2$. If $k = b - 2$, we have $c_{b-2} = b - 1$, so we have determined $b - 1$ consecutive digits of the expansion. From the binomial theorem, $(x+1)^a \equiv ax + 1 \pmod{x^2}$, so $\text{ord}_{(b-1)^2} b = b - 1$, which is the period length. Therefore, we have determined the entire expansion.

13. The base b expansion is $(.100100001\ldots)_b$, which is non-repeating and therefore by Theorem 12.4 represents an irrational number.

15. Let γ be a real number. Set $c_0 = [\gamma]$ and and $\gamma_1 = \gamma - c_0$. Then $0 \le \gamma_1 < 1$ and $\gamma = c_0 + \gamma_1$. From the condition that $c_k < k$ for $k = 1, 2, 3, \ldots$, we must have $c_1 = 0$. Let $c_2 = [2\gamma_1]$ and $\gamma_2 = 2\gamma_1 - c_2$. Then $\gamma_1 = (c_2 + \gamma_2)/2$, so $\gamma = c_0 + c_1/1! + c_2/2! + \gamma_2/2!$ Now let $c_3 = [3\gamma_2]$ and $\gamma_3 = 3\gamma_2 - c_3$. Then $\gamma_2 = (c_3 + \gamma_3)/3$ and so $\gamma = c_0 + c_1/1! + c_2/2! + c_3/3! + \gamma_3/3!$. Continuing in this fashion, for each $k = 2, 3, \ldots$, define $c_k = [k\gamma_{k-1}]$ and $\gamma_k = k\gamma_{k-1} - c_k$. Then $\gamma = c_0 + c_1/1! + c_2/2! + c_3/3! + \cdots + c_k/k! + \gamma_k/k!$. Because each $\gamma_k < 1$, we know that $\lim_{k\to\infty} \gamma_k/k! = 0$, so we conclude that $\gamma = c_0 + c_1/1! + c_2/2! + c_3/3! + \cdots + c_k/k! + \cdots$.

17. In the proof of Theorem 12.2, the numbers $p\gamma_n$ are the remainders of b^n upon division by p. The process recurs as soon as some γ_i repeats a value. Because $1/p = (.\overline{c_1 c_2 \ldots c_{p-1}})$ has period length $p - 1$, we have by Theorem 12.4 that $\text{ord}_p b = p - 1$, so there is an integer k such that $b^k \equiv m \pmod{p}$. So the remainders of mb^n upon division by p are the same as the remainders of $b^k b^n$ upon division by p. Hence, the nth digit of the expansion of m/p is determined by the remainder of b^{k+n} upon division by p. Therefore, it will be the same as the $(k+n)$th digit of $1/p$.

19. n must be prime with 2 a primitive root.

21. Let $\gamma b^{j-1} = a + \epsilon$, where a is an integer and $0 \le \epsilon < 1$. Then $[\gamma b^j] - b[\gamma b^{j-1}] = [(a+\epsilon)b] - b[a+\epsilon] = ab + [\epsilon b] - ab = [\epsilon b]$. Because $0 \le \epsilon < 0$, this last expression is an integer between 0 and $b - 1$. Therefore, $0 \le [\gamma b^j] - b[\gamma b^{j-1}] \le b - 1$. Now consider the sum $\sum_{j=1}^{N}([\gamma b^j] - b[\gamma b^{j-1}])/b^j$. Factor out $1/b^N$ to clear fractions and this becomes $(1/b^N)\sum_{j=1}^{N}(b^{N-j}[\gamma b^j] - b^{N-(j-1)}[\gamma b^{j-1}])$. This sum telescopes to $(-b^N[\gamma] + [\gamma b^N])/b^N = [\gamma b^N]/b^N$ because $[\gamma] = 0$. But $[\gamma b^N]/b^N = (\gamma b^N - \gamma b^N + [\gamma b^N])/b^N = \gamma - (\gamma b^N - [\gamma b^N])/b^N$. But $0 \le \gamma b^N - [\gamma b^N] < 1$, so taking limits as $N \to \infty$ of both sides of this equation yields $\gamma = \sum_{j=1}^{\infty}([\gamma b^j] - b[\gamma b^{j-1}])/b^j$. By the uniqueness of the base b expansion given in Theorem 12.1, we must have $c_j = [\gamma b^j] - b[\gamma b^{j-1}]$ for each j.

23. Let $\alpha = \sum_{i=1}^{\infty} \frac{(-1)^{a_i}}{10^{i!}}$, and $\frac{p_k}{q_k} = \sum_{i=1}^{k} \frac{(-1)^{a_i}}{10^{i!}}$. Then $\left|\alpha - \frac{p_k}{q_k}\right| = \left|\sum_{i=k+1}^{\infty} \frac{(-1)^{a_i}}{10^{i!}}\right| \le \sum_{i=k+1}^{\infty} \frac{1}{10^{i!}}$. As in the proof of Corollary 12.5.1, it follows that $\left|\alpha - \frac{p_k}{q_k}\right| < \frac{2}{10^{(k+1)!}}$, which shows that there can be no real number C as in Theorem 12.5. Hence, α must be transcendental.

25. Suppose $e = h/k$. Then $k!(e - 1 - 1/1! - 1/2! - \cdots 1/k!)$ is an integer. But this is equal to $k!(1/(k+1)! + 1/(k+2)! + \cdots) = 1/(k+1) + 1/(k+1)(k+2) + \cdots < 1/(k+1) + 1/(k+1)^2 + \cdots = 1/k < 1$. But $k!(1/(k+1)! + 1/(k+2)! + \cdots)$ is positive, and therefore cannot be an integer, a contradiction.

Section 12.2

1. **a.** 15/7 **b.** 10/7 **c.** 6/31 **d.** 355/113 **e.** 2 **f.** 3/2 **g.** 5/3 **h.** 8/5

3. **a.** $[1; 2, 1, 1, 2]$ **b.** $[1; 1, 7, 2]$ **c.** $[2; 9]$ **d.** $[3; 7, 1, 1, 1, 1, 2]$ **e.** $[-1; 13, 1, 1, 2, 1, 1, 2, 2]$ **f.** $[0; 9, 1, 3, 6, 2, 4, 1, 2]$

5. **a.** 1, 3/2, 4/3, 7/5, 18/13 **b.** 1, 2, 15/8, 32/17 **c.** 2, 19/9 **d.** 3, 22/7, 25/8, 47/15, 72/23, 119/38, 310/99. **e.** −1, −12/13, −13/14, −25/27, −63/68,−88/95, −151/163, −390/421, −931/1005 **f.** 0, 1/9, 1/10, 4/39, 25/244, 54/527, 241/2352, 295/2879, 831/8110

7. **a.** $3/2 > 7/5$ and $1 < 4/3 < 18/13$ **b.** $2 > 32/17$ and $1 < 15/8$ **c.** vacuous **d.** $22/7 > 47/15 > 119/38$ and $3 < 25/8 < 72/23 < 310/99$ **e.** $-12/13 > -25/27 > -88/95 > -390/421$ and $-1 < -13/14 < -63/68 < -151/163 < -931/1005$ **f.** $1/9 > 4/39 > 54/527 > 295/2879$ and $0 < 1/10 < 25/244 < 241/2352 < 831/8110$

9. Let $\alpha = r/s$. The Euclidean algorithm for $1/\alpha = s/r < 1$ gives $s = 0(r) + s$; $r = a_0(s) + a_1$, and continues just like for r/s.

11. Proceed by induction. The basis case is trivial. Assume $q_j \ge f_j$ for $j < k$. Then $q_k = a_k q_{k-1} + q_{k-2} \ge a_k f_{k-1} + f_{k-2} \ge f_{k-1} + f_{k-2} = f_k$, as desired.

13. By Exercise 10, we have $p_n/p_{n-1} = [a_n; a_{n-1}, \ldots, a_0] = [a_0; a_1, \ldots, a_n] = p_n/q_n = r/s$ if the continued fraction is symmetric. Then $q_n = p_{n-1} = s$ and $p_n = r$, so by Theorem 12.10 we have $p_n q_{n-1} - q_n p_{n-1} = r q_{n-1} - s^2 = (-1)^{n-1}$. Then $r q_{n-1} = s^2 + (-1)^{n-1}$ and so $r \mid s^2 - (-1)^n$. Conversely, if $r \mid s^2 + (-1)^{n-1}$, then $(-1)^{n-1} = p_n q_{n-1} - q_n p_{n-1} = r q_{n-1} - p_{n-1} s$. So $r \mid p_{n-1} s + (-1)^{n-1}$ and hence $r \mid (s^2 + (-1)^{n-1}) - (p_{n-1} s + (-1)^{n-1}) = s(s - p_{n-1})$. Because s, $p_{n-1} < r$ and $(r, s) = 1$, we have $s = p_{n-1}$. Then $[a_n; a_{n-1}, \ldots, a_0] = p_n/p_{n-1} = r/s = [a_0; a_1, \ldots, a_n]$.

15. Note that the notation $[a_0; a_1, \ldots, a_n]$ makes sense, even when the a_j's are not integers. Use induction. Assume the statement is true for k odd and prove it for $k + 2$. Define $a_k' = [a_k; a_{k+1}, a_{k+2}]$ and check that $a_k' < [a_k; a_{k+1}, a_{k+2} + x] = a_k' + x'$. Then $[a_0; a_1, \ldots, a_{k+2}] = [a_0; a_1, \ldots, a_k'] > [a_0; a_1, \ldots, a_k' + x'] = [a_0; a_1, \ldots, a_{k+2} + x]$. Proceed similarly for k even.

Section 12.3

1. **a.** $[1; 2, 2, 2, \ldots]$ **b.** $[1; 1, 2, 1, 2, \ldots]$ **c.** $[2; 4, 4, \ldots]$ **d.** $[1; 1, 1, 1, \ldots]$

3. 312689/99532

5. If $a_1 > 1$, let $A = [a_2; a_3, \ldots]$. Then $[a_0; a_1, \ldots] + [-a_0 - 1; 1, a_1 - 1, a_2, a_3, \ldots] = a_0 + \frac{1}{a_1 + (1/A)} + \left(-a_0 - 1 + \frac{1}{1 + \frac{1}{a_1 - 1 + (1/A)}}\right) = 0$. Similarly if $a_1 = 1$.

7. If $\alpha = [a_0; a_1, a_2, \ldots]$, then $1/\alpha = 1/[a_0; a_1, a_2, \ldots] = 0 + \frac{1}{a_0 + \frac{1}{a_1 + \cdots}} = [0; a_0, a_1, a_2, \ldots]$. Then the kth convergent of $1/\alpha$ is $[0; a_0, a_1, a_2, \ldots, a_{k-1}] = 1/[a_0; a_1, a_2, \ldots, a_{k-1}]$, which is the reciprocal of the $(k-1)$st convergent of α.

9. By Theorem 12.19, such a p/q is a convergent of α. Now $(\sqrt{5}+1)/2 = [1; 1, 1, \ldots]$, so $q_n = f_n$ (Fibonacci) and $p_n = q_{n+1}$. Then $\lim_{n\to\infty} q_{n-1}/q_n = \lim_{n\to\infty} q_{n-1}/p_{n-1} = 2/(\sqrt{5}+1) = (\sqrt{5}-1)/2$. So $\lim_{n\to\infty} \left((\sqrt{5}+1)/2 + (q_{n-1}/q_n)\right) = (\sqrt{5}+1)/2 + (\sqrt{5}-1)/2 = \sqrt{5}$. So $(\sqrt{5}+1)/2 + (q_{n-1}/q_n) > c$ only finitely often. Whence, $1/\left((\sqrt{5}+1)/2 + (q_{n-1}/q_n)\right) q_n^2 < 1/(cq_n^2)$ only finitely often. The following identity finishes the proof. Note that $\alpha_n = \alpha$ for all n. Then $\left|\alpha - (p_n/q_n)\right| = \left|(\alpha_{n+1}p_n + p_{n-1})/(\alpha_{n+1}q_n + q_{n-1}) - (p_n/q_n)\right| = \left|(-(p_nq_{n-1} - p_{n-1}q_n))/(q_n(\alpha q_n + q_{n-1}))\right| = 1/(q_n^2(\alpha + (q_{n-1}/q_n))$.

11. If β is equivalent to α, then $\beta = (a\alpha + b)/(c\alpha + d)$. Solving for α gives $\alpha = (-d\beta + b)/(c\beta - a)$, so α is equivalent to β.

13. By symmetry and transitivity (Exercises 11 and 12), it suffices to show that every rational number $\alpha = m/n$ (which we can assume is in lowest terms) is equivalent to 1. By the Euclidean algorithm, we can find a and b such that $ma + nb = 1$. Let $d = m + b$ and $c = a - n$. Then $(a\alpha + b)/(c\alpha + d) = 1$.

15. Note that $p_{k,t}q_{k-1} - q_{k,t}p_{k-1} = t(p_{k-1}q_{k-1} - q_{k-1}p_{k-1}) + (p_{k-2}q_{k-1} - p_{k-1}q_{k-2}) = \pm 1$. Thus, $p_{k,t}$ and $q_{k,t}$ are relatively prime.

17. See, for example, the classic work by O. Perron, *Die Lehre von den Kettenbrüchen*, Leipzig, Teubner (1929).

19. 179/57

21. Note first that if $b < d$, then $|a/b - c/d| < 1/2d^2$ implies that $|ad - bc| < b/2d < 1/2$, but because $b \neq d$, $|ad - bc|$ is a positive integer, and so is greater than 1/2. Thus, $b \geq d$. Now assume that c/d is not a convergent of the continued fraction for a/b. Because the denominators of the convergents increase to b, there must be two successive convergents p_n/q_n and p_{n+1}/q_{n+1} such that $q_n < d < q_{n+1}$. Next, by the triangle inequality we have $1/2d^2 > \left|\frac{a}{b} - \frac{c}{d}\right| = \left|\frac{c}{d} - \frac{p_n}{q_n}\right| - \left|\frac{a}{b} - \frac{p_n}{q_n}\right| \geq \left|\frac{c}{d} - \frac{p_n}{q_n}\right| - \left|\frac{p_{n+1}}{q_{n+1}} - \frac{p_n}{q_n}\right|$, because the $n+1$st convergent is on the other side of a/b from the nth convergent. Because the numerator of the first difference on the right side is a nonzero integer, and applying Corollary 12.3 to the second difference, we have the last expression greater than or equal to $1/dq_n - 1/q_{n+1}q_n$. If we multiply through by d^2, we get $\frac{1}{2} > \frac{d}{q_n}\left(1 - \frac{d}{q_{n+1}}\right) > 1 - \frac{d}{q_{n+1}}$ because $d/q_n > 1$. From which we deduce that $1/2 < d/q_{n+1}$.

The convergents p_n/q_n and p_{n+1}/q_{n+1} divide the line into three regions. As c/d could be in any of these, there are three cases. Case 1: If c/d is between the convergents, then $\frac{1}{dq_n} \leq \left|\frac{c}{d} - \frac{p_n}{q_n}\right|$ because the numerator of the fraction is a positive integer and the denominators on both sides of the inequality are the same. This last is less than or equal to $\left|\frac{p_{n+1}}{q_{n+1}} - \frac{p_n}{q_n}\right| = \frac{1}{q_{n+1}q_n}$ because the $n+1$st convergent is farther from the nth convergent than c/d and where we have applied Corollary 12.3. But this implies that $d \geq q_{n+1}$, a contradiction. Case 2: If c/d is closer to p_n/q_n, then again $\frac{1}{dq_n} \leq \left|\frac{c}{d} - \frac{p_n}{q_n}\right| \leq \left|\frac{a}{b} - \frac{c}{d}\right|$ because a/b is on the other side of the nth convergent from c/d. But this last is less than $1/2d^2$, and if we multiply through by d, we have $1/q_n < 1/2d$, which implies that $q_n > d$, a contradiction. Case 3: If c/d is closer to p_{n+1}/q_{n+1}, then with the same reasoning as in Case 2, we have $\frac{1}{dq_{n+1}} \le \left|\frac{c}{d} - \frac{p_{n+1}}{q_{n+1}}\right| < \left|\frac{a}{b} - \frac{c}{d}\right| < 1/2d^2$. But this implies that $d/q_{n+1} < 1/2$, contradicting the inequality established above. Having exhausted all the cases, we must conclude that c/d must be a convergent of the continued fraction for a/b.

Section 12.4

1. **a.** $[2; \overline{1, 1, 1, 4}]$ **b.** $[3; \overline{3, 6}]$ **c.** $[4; \overline{1, 3, 1, 8}]$ **d.** $[6; \overline{1, 5, 1, 12}]$ **e.** $[7; \overline{1, 2, 7, 2, 1, 14}]$ **f.** $[9; \overline{1, 2, 3, 1, 1, 5, 1, 8, 1, 5, 1, 1, 3, 2, 1, 18}]$

3. **a.** $[2; \overline{2}]$ **b.** $[1; \overline{2, 2, 2, 1, 12, 1}]$ **c.** $[0; 1, 1, \overline{2, 3, 10, 3}]$

5. **a.** $(23 + \sqrt{29})/10$ **b.** $(-1 + 3\sqrt{5})/2$ **c.** $(8 + \sqrt{82})/6$

7. **a.** $\sqrt{10}$ **b.** $\sqrt{17}$ **c.** $\sqrt{26}$ **d.** $\sqrt{37}$

9. **a.** We have $\alpha_0 = \sqrt{d^2 - 1}$, $a_0 = d - 1$, $P_0 = 0$, $Q_0 = 1$, $P_1 = (d - 1)(1) - 0 = d - 1$, $Q_1 = ((d^2 - 1) - (d - 1)^2)/1 = 2d - 2$, $\alpha_1 = (d - 1 + \sqrt{d^2 - 1})/(2(d - 1)) = 1/2 + 1/2\sqrt{(d + 1)/(d - 1)}$, $a_1 = 1$, $P_2 = 1(2d - 2) - (d - 1) = d - 1$, $Q_2 = (d^2 - 1 - (d - 1)^2)/(2d - 2) = 1$, $\alpha_2 = (d - 1 + \sqrt{d^2 - 1})/1$, $a_2 = 2d - 2$, $P_3 = 2(d - 1)(1) - (d - 1) = d - 1 = P_1$, $Q_3 = ((d^2 - 1) - (d - 1)^2)/1 = 2d - 2 = Q_1$, so $\alpha = [d - 1; \overline{1, 2(d - 1)}]$. **b.** We have $\alpha_0 = \sqrt{d^2 - d}$, $a_0 = [\sqrt{d^2 - d}] = d - 1$, because $(d - 1)^2 < d^2 - d < d^2$. Then $P_0 = 0$, $Q_0 = 1$, $P_1 = d - 1$, $Q_1 = d - 1$, $\alpha_1 = ((d - 1) + \sqrt{d^2 - d})/(d - 1) = 1 + \sqrt{d/(d - 1)}$, $a_1 = 2$, $P_2 = d - 1$, $Q_2 = 1$, $\alpha_2 = ((d - 1) + \sqrt{d^2 - d})/1$, $a_2 = 2(d - 1)$, $P_3 = P_1$, $Q_3 = Q_1$. Therefore, $\sqrt{d^2 - d} = [d - 1; \overline{2, 2(d - 1)}]$. **c.** $[9; \overline{1, 18}]$, $[10; \overline{2, 20}]$, $[16; \overline{2, 32}]$, $[24; \overline{2, 48}]$

11. **a.** Note that $d < \sqrt{d^2 + 4} < d + 1$. Then $\alpha_0 = \sqrt{d^2 + 4}$, $a_0 = d$, $P_0 = 0$, $Q_0 = 1$, $P_1 = d$, $Q_1 = 4$, $\alpha_1 = (d + \sqrt{d^2 + 4})/4$, $a_1 = [2d/4] = (d - 1)/2$, because d is odd. Also, $P_2 = d - 2$, $Q_2 = d$, $\alpha_2 = (d - 2 + \sqrt{d^2 + 4})/d$, $((d - 2) + d)/d < \alpha_2 < (d - 2 + d + 1)/d$, so $a_2 = 1$, $P_3 = 2$, $Q_3 = d$, $\alpha_3 = (2 + \sqrt{d^2 + 4})/d$, $a_3 = 1$, $P_4 = d - 2$, $Q_4 = 4$, $\alpha_4 = (d - 2 + \sqrt{d^2 + 4})/4$, $(d - 2 + d)/4 = (d - 1)/2 < \alpha_4 < (d - 2 + d + 1)/4$, so $a_4 = (d - 1)/2$, $P_5 = d$, $Q_5 = 1$, $\alpha_5 = (d + \sqrt{d^2 + 4})/1$, $a_5 = 2d$, $P_6 = d = P_1$, $Q_6 = 4 = Q_1$. Thus, $\alpha = [d; \overline{(d - 1)/2, 1, 1, (d - 1)/2, 2d}]$. **b.** Note that $d - 1 < \sqrt{d^2 - 4} < d$. Then $\alpha_0 = \sqrt{d^2 - 4}$, $a_0 = d - 1$, $P_0 = 0$, $Q_0 = 1$, $P_1 = d - 1$, $Q_1 = 2d - 5$, $\alpha_1 = (d - 1 + \sqrt{d^2 - 4})/(2d - 5)$, $(d - 1 + d - 1)/(2d - 5) < \alpha_0 < (d - 1 + d)/(2d - 5)$ and $d > 3$ so $a_1 = 1$, $P_2 = d - 4$, $Q_2 = 4$, $a_2 = (d - 4 + \sqrt{d^2 - 4})/4$, $a_2 = (d - 3)/2$, $P_3 = d - 2$, $Q_3 = d - 2$, $\alpha_3 = (d - 2 + \sqrt{d^2 - 4})/(d - 2)$, $a_3 = 2$, $P_4 = d - 2$, $Q_4 = 4$, $\alpha_4 = (d - 2 + \sqrt{d^2 - 4})/4$, $a_4 = (d - 3)/2$, $P_5 = d - 4$, $Q_5 = 2d - 5$, $\alpha_5 = (d - 4 + \sqrt{d^2 - 4})/(2d - 5)$, $a_5 = 1$, $P_6 = d - 1$, $Q_6 = 1$, $\alpha_6 = (d - 1 + \sqrt{d^2 - 4})/1$, $a_6 = 2d - 2$, $P_7 = d - 1 = P_1$, $Q_7 = 2d - 5 = Q_1$. Thus, $\alpha = [d - 1; \overline{1, (d - 3)/2, 2, (d - 3)/2, 1, 2d - 2}]$.

13. Suppose $\sqrt{d}$ has period length 2. Then $\sqrt{d} = [a; \overline{c, 2a}]$ from the discussion preceding Example 12.16. Then $\sqrt{d} = [a; y]$ with $y = [\overline{c; 2a}] = [c; 2a, y] = c + 1/(2a + (1/y)) = (2acy + c + y)/(2ay + 1)$. Then $2ay^2 - 2acy - c = 0$, and because y is positive, we have $y = (2ac + \sqrt{(2ac)^2 + 4(2a)c})/(4a) = (ac + \sqrt{(ac)^2 + 2ac})/(2a)$. Then $\sqrt{d} = [a; y] = a + (1/y) = a + 2a/(ac + \sqrt{(ac)^2 + 2ac}) = \sqrt{a^2 + 2a/c}$, so $d = a^2 + 2a/c$, and $b = 2a/c$ is an integral divisor of $2a$. Conversely, let $\alpha = \sqrt{a^2 + b}$ and $b | 2a$, say, $kb = 2a$. Then $a_0 = [\sqrt{a^2 + b}] = a$, because $a^2 < a^2 + b < (a + 1)^2$. Then $P_0 = 0$, $Q_0 = 1$, $P_1 = a$, $Q_1 = b$, $\alpha_1 = (a + \sqrt{a^2 + b})/b$, $a_1 = 4k$, $P_2 = a$, $Q_2 = 1$, $\alpha_2 = (a + \sqrt{a^2 + b})/1$, $a_2 = 2a$, $P_3 = a = P_1$, $Q_3 = b = Q_1$, so $\alpha = [a; \overline{4k, 2a}]$, which has period length 2.

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

17. Let $\alpha = (a + \sqrt{b})/c$. Then $-1/\alpha' = -(c)/(a - \sqrt{b}) = (ca + \sqrt{bc^2})/(b - a^2) = (A + \sqrt{B})/C$, say. By Exercise 16, $0 < a < \sqrt{b}$ and $\sqrt{b} - a < c < \sqrt{b} + a < 2\sqrt{b}$. Multiplying by c gives $0 < ca < \sqrt{bc^2}$ and $\sqrt{bc^2} - ca < c^2 < \sqrt{bc^2} + ca < 2\sqrt{bc^2}$. That is, $0 < A < \sqrt{B}$ and $\sqrt{B} - A < c^2 < \sqrt{B} + A < 2\sqrt{B}$. Multiply $\sqrt{b} - a < c$ by $\sqrt{b} + a$ to get $C = b - a^2 < \sqrt{bc^2} + ca = A + \sqrt{B}$. Multiply $c < \sqrt{b} + a$ by $\sqrt{b} - a$ to get $\sqrt{B} - A = \sqrt{bc^2} - ac < b - a^2 = C$. So, $-1/\alpha'$ satisfies all the inequalities in Exercise 16, and therefore is reduced.

19. Start with $\alpha_0 = \sqrt{D_k} + 3^k + 1$ (this will have the same period because it differs from $\sqrt{D_k}$ by an integer) and use induction. Apply the continued fraction algorithm to show $\alpha_{3i} = \sqrt{D_k} + 3^k - 2 \cdot 3^{k-i} + 2/(2 \cdot 3^{k-i})$, $i = 1, 2, \ldots, k$, but $\alpha_{3k+3i} = \sqrt{D_k} + 3^k - 2/(2 \cdot 3^i)$, $i = 1, 2, \ldots, k - 1$, and $\alpha_{6k} = \sqrt{D_k} + 3^k + 1 = \alpha_0$. Because $\alpha_i \neq \alpha_0$ for $i < 6k$, we see that the period is $6k$.

Section 12.5

1. Note that $19^2 - 2^2 = (19 - 2)(19 + 2) \equiv 0 \pmod{119}$. Then $(19 - 2, 119) = (17, 119) = 17$ and $(19 + 2, 119) = (21, 119) = 7$ are factors of 119.

3. $3119 \cdot 4261$

5. We have $17^2 = 289 \equiv 3 \pmod{143}$ and $19^2 = 361 \equiv 3 \cdot 5^2 \pmod{143}$. Combining these, we have $(17 \cdot 19)^2 \equiv 3^2 5^2 \pmod{143}$. Hence, $323^2 \equiv 15^2 \pmod{143}$. It follows that $323^2 - 15^2 = (323 - 15)(323 + 15) \equiv 0 \pmod{143}$. This produces the two factors $(323 - 15, 143) = (308, 143) = 11$ and $(323 + 15, 143) = (338, 143) = 13$ of 143.

7. $3001 \cdot 4001$

Section 13.1

1. **a.** (3, 4, 5), (5, 12, 13), (15, 8, 17), (7, 24, 25), (21, 20, 29), (35, 12, 37) **b.** those in part (a) and (6, 8, 10), (9, 12, 15), (12, 16, 20), (15, 20, 25), (18, 24, 30), (21, 28, 35), (24, 32, 40), (10, 24, 26), (15, 36, 39), (30, 16, 34)

3. By Lemma 13.1, 5 divides at most one of x, y, and z. If $5 \nmid x$ or y, then $x^2 \equiv \pm 1 \pmod 5$ and $y^2 \equiv \pm 1 \pmod 5$. Then $z^2 \equiv 0, 2,$ or $-2 \pmod 5$. But ± 2 is not a quadratic residue modulo 5, so $z^2 \equiv 0 \pmod 5$, whence $5 \mid z$.

5. Let k be an integer ≥ 3. If $k = 2n + 1$, let $m = n + 1$. Then m and n have opposite parity, $m > n$ and $m^2 - n^2 = 2n + 1 = k$, so m and n define the desired triple. If k has an odd divisor $d > 1$, then use the construction above for d and multiply the result by k/d. If k has no odd divisors, then $k = 2^j$ for some integer $j > 1$. Let $m = 2^{j-1}$ and $n = 1$. Then $k = 2mn$, $m > n$, and m and n have opposite parity, so m and n define the desired triple.

7. Substituting $y = x + 1$ into the Pythagorean equation gives us $2x^2 + 2x + 1 = z^2$, which is equivalent to $m^2 - 2z^2 = -1$ where $m = 2x + 1$. Dividing by z^2 yields $m^2/z^2 - 2 = -1/z^2$. Note that $m/z \geq 1$, $1/z^2 = 2 - m^2/z^2 = (\sqrt{2} + m/z)(\sqrt{2} - m/z) < 2(\sqrt{2} - m/z)$. So by Theorem 12.18, m/z must be a convergent of the continued fraction expansion of $\sqrt{2}$. Further, by the proof of Theorem 12.13, it must be one of the even-subscripted convergents. Therefore, each solution is given by the recurrence $m_{n+1} = 3m_n + 2z_n$, $z_{n+1} = 2m_n + 3m_n$. (See, e.g., Theorem 13.11.) Substituting x back in yields the recurrences of Exercise 6.

9. See Exercise 15 with $p = 3$.

11. (9, 12, 15), (35, 12, 37), (5, 12, 13), (12, 16, 20)

13. $x = 2m$, $y = m^2 - 1$, $z = m^2 + 1$, $m > 1$

15. primitive solutions given by $x = (m^2 - pn^2)/2$, $y = mn$, $z = (m^2 + pn^2)/2$ where $m > \sqrt{p}n$

17. Substituting $f_n = f_{n+2} - f_{n+1}$ and $f_{n+3} = f_{n+2} + f_{n+1}$ into $(f_n f_{n+3})^2 + (2f_{n+1}f_{n+2})^2$ yields $(f_{n+2} - f_{n+1})^2(f_{n+2} + f_{n+1})^2 + 4f_{n+1}^2 f_{n+2}^2 = (f_{n+2}^2 - f_{n+1}^2)^2 + 4f_{n+1}^2 f_{n+2}^2 = f_{n+2}^4 - 2f_{n+1}^2 f_{n+2}^2 + f_{n+1}^4 + 4f_{n+1}^2 f_{n+2}^2 = f_{n+2}^4 + 2f_{n+1}^2 f_{n+2}^2 + f_{n+1}^4 = (f_{n+2}^2 + f_{n+1}^2)^2$, proving the result.

19. the point $(1, 0)$ and all points (r, s) with $r = (t^2 - 1)/(t^2 + 1)$ and $s = -2t/(t^2 + 1)$, with t rational

21. the point $(1, -1)$ and all points (r, s) with $r = (t^2 - t - 1)/(t^2 + 1)$ and $s = (1 - 2t)/(t^2 + 1)$ with t rational

23. the point $(-1, 1)$ and all points (r, s) with $r = (1 - t^2)/(1 + t + t^2)$ and $s = (t^2 + 2t)/(t^2 + t + 1)$ with t rational

25. Suppose x and y are rational numbers such that $x^2 + y^2 = 3$. Then there exists integers p, q, and r such that $x = p/r$ and $y = q/r$, where we assume without loss of generality that x and y have equal denominators. Then we have $p^2 + q^2 = 3r^2$. Further, without loss of generality, we may assume p, q and r are not all even, because we could divide the equation by 4 and have another solution. First suppose r is odd. Then $r^2 \equiv 1 \pmod 4$ so $p^2 + q^2 \equiv 3 \pmod 4$. Because a square modulo 4 must be congruent to either 0 or 1, there are no solutions to this last congruence. Now suppose r is even. Then $r^2 \equiv 0 \pmod 4$, so that $p^2 + q^2 \equiv 0 \pmod 4$. The only solutions to this congruence requires that p and q are both even, which contradicts our assumption that p, q and r are not all even. Therefore, there are no rational points on the circle $x^2 + y^2 = 3$.

27. the point $(0, 0, 1)$ and all points (r, s, t) where $r = -2u/(u^2 + v^2 - 1)$, $s = -2v/(u^2 + v^2 - 1)$ and $t = (u^2 + v^2 + 1)/(u^2 + v^2 - 1)$ with u and v rational

Section 13.2

1. Assume without loss of generality that $x < y$. Then $x^n + y^n = x^2x^{n-2} + y^2y^{n-2} < (x^2 + y^2)y^{n-2} = z^2y^{n-2} < z^2z^{n-2} = z^n$.

3. **a.** If $p \mid x$, y, or z, then certainly $p \mid xyz$. If not, then by Fermat's Little Theorem, $x^{p-1} \equiv y^{p-1} \equiv z^{p-1} \equiv 1 \pmod p$. Hence, $1 + 1 \equiv 1 \pmod p$, which is impossible. **b.** We know $a^p \equiv a \pmod p$ for every integer a. Then $x^p + y^p \equiv z^p \pmod p$ implies $x + y \equiv z \pmod p$, so $p \mid x + y - z$.

5. Let x and y be the lengths of the legs and let z be the hypotenuse. Then $x^2 + y^2 = z^2$. If the area is a perfect square, we have $A = \frac{1}{2}xy = r^2$. Then, if $x = m^2 - n^2$, and $y = 2mn$, we have $r^2 = mn(m^2 - n^2)$. All of these factors are relatively prime, so $m = a^2$, $n = b^2$, and $m^2 - n^2 = c^2$, say. Then, $a^4 - b^4 = c^2$, which contradicts Exercise 4.

7. We use the method of infinite descent. Assume there is a nonzero solution where $|x|$ is minimal. Then $(x, y) = 1$. Also x and z cannot both be even, because then y would be odd and then $z^2 \equiv 8 \pmod{18}$, but 8 is not a quadratic residue modulo 16. Therefore, x and z are both odd, because $8y^4$ is even. From here it is easy to check that $(x, z) = 1$. We may also assume (by negating if necessary) that $x \equiv 1 \pmod 4$ and $z \equiv 3 \pmod 4$. Clearly, $x^2 > |z|$. We have $8y^4 = x^4 - z^2 = (x^2 - z)(x^2 + z)$. Because $z \equiv 3 \pmod 4$, we have $x^2 - z \equiv 2 \pmod 4$, so $m = (x^2 - z)/2$ is odd, and $n = (x^2 + z)/4$ is an integer. Because no odd prime can divide both m and n, we have $(m, n) = 1$, $m, n > 0$ and $mn = y^4$, whence $m = r^4$ and $n = s^4$, with $(r, s) = 1$. So now $r^4 + 2s^4 = m + 2n = x^2$. This implies $(x, r) = 1$, because no odd prime divides r and x but not s, and r and x are both odd. Also, $|x| > r^2 > 0$. Now consider $2s^4 = (x^2 - r^4) = (x - r^2)(x + r^2)$. Then s must be even because a difference of squares is not congruent to $2 \pmod 4$, so $s = 2t$ and $32t^4 = (x - r^2)(x + r^2)$. Recalling $x \equiv 1 \pmod 4$ and r is odd, we have $U = (x + r^2)/2$ is odd and $V = (x - r^2)/16$ is an integer. Again $(U, V) = 1$ and $UV = t^4$, but we don't know the sign of x. So $U = \pm u^4$ and $V = \pm v^4$, depending on the sign of x. Now $r^2 = \pm(u^4 - 8v^4)$. But because u is odd, we can rule out the case with the minus sign (or else $r^2 \equiv 7 \pmod 8$). Therefore, we must have the plus sign (hence, x is positive), and we have $u^4 - 8v^4 = r^2$. Finally, $|v| > 0$ because $|x + r^2| > 0$. So we haven't reduced to a trivial case. Then $u^4 = U < |x + r^2|/2 < x$, so $|u| < x$, and so $|x|$ was not minimal. This contradiction shows that there are no nontrivial solutions.

9. Suppose that $x = a/b$, where a and b are relatively prime and $b \neq 0$. Then $y^2 = (a^4 + b^4)/b^4$, from which we deduce that $y = z/b^2$ from some integer z. Then $z^2 = a^4 + b^4$, which has no nonzero solutions by Theorem 13.3. Because $b \neq 0$, it follows that $z \neq 0$. Therefore, $a = 0$, and hence $x = 0$, and consequently $y = \pm 1$. These are the only solutions.

11. If x were even, the $y^2 = x^3 + 23 \equiv 3 \pmod 4$, which is impossible, so x must be odd, making y even, say, $y = 2v$. If $x \equiv 3 \pmod 4$, then $y^2 \equiv 3^3 + 23 \equiv 2 \pmod 4$, which is also impossible, so $x \equiv 1 \pmod 4$. Add 4 to both sides of the equation to get $y^2 + 4 = 4v^2 + 4 = x^3 + 27 = (x + 3)(x^2 - 3x + 9)$. Then $z = x^2 - 3x + 9 \equiv 1 - 3 + 9 \equiv 3 \pmod 4$, so a prime $p \equiv 3 \pmod 4$ must divide z. Then $4v^2 + 4 \equiv 0 \pmod p$ or $v^2 \equiv -1 \pmod p$. But this shows that a prime congruent to 3 modulo 4 has -1 as a quadratic residue, which contradicts Theorem 11.5. Therefore, the equation has no solutions.

13. This follows from Exercise 4 and Theorem 13.2.

15. Assume that $n \nmid xyz$, and $(x, y, z) = 1$. Now $(-x)^n = y^n + z^n = (y + z)(y^{n-1} - y^{n-2}z + \cdots + z^{n-1})$, and these factors are relatively prime, so they are nth powers, say, $y + z = a^n$, and $y^{n-1} - y^{n-2}z + \cdots + z^{n-1} = \alpha^n$, whence $x = a\alpha$. Similarly, $z + x = b^n$, and $(z^{n-1} - z^{n-2}x + \cdots + x^{n-1}) = \beta^n$, $-y = b\beta$, $x + y = c^n$, and $(x^{n-1} - x^{n-2}y + \cdots + y^{n-1}) = \gamma^n$, and $-z = c\gamma$. Because $x^n + y^n + z^n \equiv 0 \pmod p$, we have $p \mid xyz$, say, $p \mid x$. Then $\gamma^n = (x^{n-1} - x^{n-2}y + \cdots + y^{n-1}) \equiv y^{n-1} \pmod p$. Also, $2x \equiv b^n + c^n + (-a)^n \equiv 0 \pmod p$, so by the condition on p, we have $p \mid abc$. If $p \mid b$, then $y = -b\beta \equiv 0 \pmod p$, but then $p \mid x$ and y, a contradiction. Similarly, p cannot divide c. Therefore, $p \mid a$, so $y \equiv -z \pmod p$, and so $\alpha^n \equiv (y^{n-1} - y^{n-2}z + \cdots + z^{n-1}) \equiv ny^{n-1} \equiv n\gamma^n \pmod p$. Let g be the inverse of $\gamma \pmod p$; then $(ag)^n \equiv n \pmod p$, which contradicts the condition that there is no solution to $w^n \equiv n \pmod p$.

17. 3, 4, 5, 6

19. If $m \geq 3$, then modulo 8 we have $3^n \equiv -1 \pmod 8$, which is impossible, so $m = 1$ or 2. If $m = 1$, then $3^n = 2 - 1 = 1$, which implies that $n = 0$, which is not a positive integer, so we have no solutions in this case. If $m = 2$, then $3^n = 2^2 - 1 = 3$, which implies that $n = 1$, and this is the only solution.

21. **a.** Substituting the expressions into the left-hand side of the equation yields $a^2 + b^2 + (3ab - c)^2 = a^2 + b^2 + 9a^2b^2 - 6abc + c^2 = (a^2 + b^2 + c^2) + 9a^2b^2 - 6abc$. Because (a, b, c) is a solution to Markoff's equation, we substitute $a^2 + b^2 + c^2 = 3abc$ to get the last expression equal to $3abc + 9a^2b^2 - 6abc = 9a^2b^2 - 3abc = 3ab(3ab - c)$, which is the right-hand side of Markoff's equation evaluated at these expressions. **b.** Case 1: If $x = y = z$, then Markoff's equation becomes $3x^2 = 3xyz$, so that $1 = yz$. Then $y = z = 1$ and then $x = 1$, so the only solution in this case is (1, 1, 1).

Case 2: If $x = y \neq z$, then $2x^2 + z^2 = 3x^2z$, which implies that $x^2|z^2$ or $x|z$, say $dx = z$. Then $2x^2 + d^2x^2 = 3dx^3$ or $2 + d^2 = 3dx$ or $2 = d(3x - d)$. So $d|2$, but because $x \neq z$, we must have $d = 2$. Then $3x - d = 1$, so that $x = 1 = y$ and $z = 2$, so the only solution in this case is (1, 1, 2).

Case 3: Assume $x < y < z$. From $z^2 - 3xyz + x^2 + y^2 + z^2$, we apply the quadratic formula to get $2z = 3xy \pm \sqrt{9x^2y^2 - 4(x^2 + y^2)}$. Note that $8x^2y^2 - 4x^2 - 4y^2 = 4x^2(y^2 - 1) + 4y^2(x^2 - 1) > 0$, so in the "minus" case of the quadratic formula, we have $2z < 3xy - \sqrt{9x^2y^2 - 8x^2y^2} = 3xy - xy = 2xy$, or $z < xy$. But $3xyz = x^2 + y^2 + z^2 < 3z^2$, so that $xy < z$, a contradiction; therefore, we must have the "plus" case in the quadratic formula and $2z = 3xy + \sqrt{9x^2y^2 - 4(x^2 + y^2)} > 3xy$, so that $z > 3xy - z$. This last expression is the formula for the generation of z in part (a). Therefore, by successive use of the formula in part (a), we will reduce the value of $x + y + z$ until it is one of the solutions in case 1 or case 2.

23. Let $\epsilon > 0$ be given then the *abc* conjecture gives us $\max(|a|, |b|, |c|) \leq K(\epsilon)\text{rad}(abc)^{1+\epsilon}$ for integers $(a, b) = 1$ and $a + b = c$. Set $M = \log K(\epsilon)/\log 2 + (3 + 3\epsilon)$. Suppose x, y, z, a, b, c are positive integers with $(x, y) = 1$ and $x^a + y^b = c^z$, so that we have a solution to Beal's equation. Assume $\min(a, b, c) > M$. From the *abc* conjecture, and because $\text{rad}(x^a y^b y^c) = \text{rad}(xyz)$, we have $\max(x^a, y^b, y^c) \leq K(\epsilon)\text{rad}(xyz)^{1+\epsilon} \leq (xyz)^{1+\epsilon}$. If $\max(x, y, z) = x$, then we would have $x^a \leq K(\epsilon)x^{3(1+\epsilon)}$. Taking log's of both sides yields $a \leq \log K(\epsilon)/\log x + (3 + 3\epsilon) < \log K(\epsilon)/\log 2 + (3 + 3\epsilon) = M$, a contradiction. Similarly if the maximum is y or z. Therefore, if the *abc* conjecture is true, there are no solutions to the Beal conjecture for sufficiently large exponents.

Section 13.3

1. **a.** $19^2 + 4^2$ **b.** $23^2 + 11^2$ **c.** $37^2 + 9^2$ **d.** $137^2 + 9^2$

3. **a.** $5^2 + 3^2$ **b.** $9^2 + 3^2$ **c.** $10^2 + 0^2$ **d.** $21^2 + 7^2$ **e.** $133^2 + 63^2$ **f.** $448^2 + 352^2$

5. **a.** $1^2 + 1^2 + 1^2$ **b.** $8^2 + 5^2 + 1^2$ **c.** $3^2 + 1^2 + 1^2$ **d.** $3^2 + 3^2 + 0^2$ **e.** not possible **f.** not possible

7. Let $n = x^2 + y^2 + z^2 = 4^m(8k + 7)$. If $m = 0$, then see Exercise 6. If $m \geq 1$, then n is even, so none or two of x, y, z are odd. If two are odd, $x^2 + y^2 + z^2 \equiv 2$ or $6 \pmod 8$, but then $4 \nmid n$, a contradiction, so all of x, y, z are even. Then $4^{m-1}(8k + 7) = (\frac{x}{2})^2 + (\frac{y}{2})^2 + (\frac{z}{2})^2$ is the sum of three squares. Repeat until $m = 0$ and use Exercise 6 to get a contradiction.

9. **a.** $10^2 + 1^2 + 0^2 + 2^2$ **b.** $22^2 + 4^2 + 1^2 + 3^2$ **c.** $14^2 + 4^2 + 1^2 + 5^2$ **d.** $56^2 + 12^2 + 17^2 + 1^2$

11. Let $m = n - 169$. Then m is the sum of four squares: $m = x^2 + y^2 + z^2 + w^2$. If, say, x, y, z are 0, then $n = w^2 + 169 = w^2 + 10^2 + 8^2 + 2^2 + 1^2$. If, say, x, y are 0, then $n = z^2 + w^2 + 169 = z^2 + w^2 + 12^2 + 4^2 + 3^2$. If, say, x is 0, then $n = y^2 + z^2 + w^2 + 169 = y^2 + z^2 + w^2 + 12^2 + 5^2$. If none are 0, then $n = x^2 + y^2 + z^2 + w^2 + 13^2$.

13. If k is odd, then 2^k is not the sum of four positive squares. Suppose $k \geq 3$, and $2^k = x^2 + y^2 + z^2 + w^2$. Then either none, two, or four of the squares are odd. Modulo 8, we have $0 \equiv x^2 + y^2 + z^2 + w^2$, and because an odd square is congruent to 1 modulo 8, the only possibility is to have x, y, z, w all even. But then we can divide by 4 to get $2^{k-2} = (\frac{x}{2})^2 + (\frac{y}{2})^2 + (\frac{z}{2})^2 + (\frac{w}{2})^2$. Either $k - 2 \geq 3$ and we can repeat the argument, or $k - 2 = 1$, in which case we have two equal to the sum of four positive squares, a contradiction.

15. If $p = 2$ the theorem is obvious. Else, $p = 4k + 1$, whence -1 is a quadratic residue modulo p, say, $a^2 \equiv -1 \pmod p$. Let x and y be as in Thue's lemma. Then $x^2 < p$ and $y^2 < p$ and $-x^2 \equiv (ax)^2 \equiv y^2 \pmod p$. Thus, $p \mid x^2 + y^2 < 2p$; therefore, $p = x^2 + y^2$ as desired.

17. The left sum runs over every pair of integers $i < j$, for $1 \leq i < j \leq 4$, so there are six terms. Each integer subscript 1, 2, 3, and 4 appears in exactly three pairs, so

$$\sum_{1 \leq i < j \leq 4} [(x_i + x_j)^4 + (x_i - x_j)^4] = \sum_{1 \leq i < j \leq 4} (2x_i^4 + 12x_i^2 x_j^2 + 2x_j^4)$$

$$= \sum_{k=1}^{4} 6x_k^4 + \sum_{1 \leq i < j \leq 4} 12x_i^2 x_j^2 = 6\left(\sum_{k=1}^{4} x_k^2\right)^2.$$

19. If m is positive, then $m = \sum_{k=1}^4 x_k^2$, for some x_k's. Then $6m = 6\sum_{k=1}^4 x_k^2 = \sum_{k=1}^4 6x_k^2$. Each term of the last sum is the sum of 12 fourth powers by Exercise 18. Therefore, $6m$ is the sum of 48 fourth powers.

21. For $n = 1, 2, \ldots, 50$, $n = \sum_1^n 1^4$. For $n = 51, 52, \ldots, 81$, $n - 48 = n - 3(2^4) = \sum_1^{n-48} 1^4$, so $n = 2^4 + 2^4 + 2^4 + \sum_1^{n-48} 1^4$ is the sum of $(n - 45)$ fourth powers, and $n = 45 \leq 36 \leq 50$. This result, coupled with the result from Exercise 20, shows that all positive integers can be written as the sum of 50 or fewer fourth powers. That is, $g(4) \leq 50$.

23. The only quartic residues modulo 16 are 0 and 1. Therefore, the sum of fewer than 15 fourth powers must have a least nonnegative residue between 0 and 14 $\pmod{16}$, which excludes any integer congruent to 15 $\pmod{16}$.

Section 13.4

1. **a.** $(\pm 2, 0)$, $(\pm 1, \pm 1)$ **b.** none **c.** $(\pm 1, \pm 2)$

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

5. (73, 12), (10657, 1752), (1555849, 255780)

7. (6239765965720528801, 798920165762330040)

9. Reduce modulo p to get $x^2 \equiv -1 \pmod{p}$. Because -1 is a quadratic nonresidue modulo p if $p = 4k + 3$, there is no solution.

11. Let $p_1 = 0$, $p_1 = 3$, $p_k = 2p_{k-1} + 2_{k-2}$, $q_0 = 1$, $q_1 = 1$, and $q_k = 2q_{k-1} + q_{k-2}$. Then the legs are $x = p_k^2 + 2p_kq + k$ and $y = 2p_kq_k + 2q_k^2$.

13. Suppose there is a solution (x, y). Then x must be odd. Note that $(x^2 + 1)^2 = x^4 + 2x^2 + 1 = 2y^2 + 2x^2$ and $(x^2 - 1)^2 = x^4 - 2x^2 + 1 = 2y^2 - 2x^2$. Multiplying these two equations together yields $(x^4 - 1)^2 = 4(y^4 - x^4)$, or because $x^4 \equiv 1 \pmod{4}$, $((x^4 - 1)/2)^2 = y^4 - x^4$. This contradicts Exercise 4 in Section 13.2.

Section 13.5

1. Let (x, y, z) be a primitive Pythagorean triple. Then there exist relatively prime integers m and n of opposite parity such that $x = m^2 - n^2$, $y = 2mn$ and $z = m^2 + n^2$. Then the area of the triangle is $xy/2 = (m^2 - n^2)2nm/2 = mn(m^2 - n^2)$ which is even because one of m and n must be even.

3. 14, 330, 390, 210

5. **a.** 15 **b.** 21 **c.** 210 **d.** 5

7. Let n be any positive integer and consider the Pythagorean triangle with sides $3n$, $4n$, and $5n$. The area of this triangle is $(3n)(4n)/2 = 6n^2$. Therefore, $6n^2$ is a congruent number for every positive integer n.

9. Consider the right triangle with legs of length $\sqrt{2}$. The length of the hypotenuse is $\sqrt{\sqrt{2}^2 + \sqrt{2}^2} = 2$, so if we assume that $\sqrt{2}$ is rational, this is a rational triangle. We compute its area to be $(1/2)\sqrt{2}\sqrt{2} = 1$. This implies that 1 is a congruent number, which is false. Therefore, $\sqrt{2}$ must be irrational.

11. Let n be a congruent number and suppose $n = 2k^2$ where k is an integer. Assume n is a congruent number. Then Theorem 13.16 tells us that n must be the common difference of a progression of three squares. Specifically, there are integers r, s, and t such that $t^2 - s^2 = n$ and $s^2 - r^2 = n$. Then $t^2 = s^2 + n$ and $r^2 = s^2 - n$. Multiplying these last two equations yields $(rt)^2 = s^4 - n^2 = s^4 - 4k^4$. Let $z = rt$, $x = s$, and $y = k$. Then the equation becomes $x^4 - 4y^4 = z^2$. Suppose that the equation has solutions in the positive integers. By the well-ordering property, there is a solution (x, y, z) having the smallest value for x. Rewriting the equation as $z^2 + (2y^2)^2 = (x^2)^2$ shows that $(z, 2y^2, x^2)$ is a Pythagorean triple. Check that this triple must be primitive. Then there exist relatively prime integers u and v of opposite parity such that $z = u^2 - v^2$, $2y^2 = 2uv$, and $x^2 = u^2 + v^2$. Then $y^2 = uv$ and $(u, v) = 1$, so $u = a^2$ and

$v = b^2$ for some integers a and b. Then $x^2 = a^4 + b^4$, which has no nonzero solutions according to Theorem 13.3. Therefore, n can not be congruent.

13. **a.** Because 1 is not a congruent number, Theorem 13.16 says that it cannot be the common difference of an arithmetic progression of three squares. **b.** Because $8 = 2^2 2$ and 2 is not a congruent number, we know that 8 is not a congruent number. By Theorem 13.16, 8 cannot be the common difference of an arithmetic progression of three squares. **c.** By Theorem 13.15, $25 = 5^2$ cannot be the area of a rational right triangle and therefore cannot be a congruent number. Then by Theorem 13.16, 25 cannot be the common difference of an arithmetic progression of three squares. **d.** If $48 = 4^2 3$ were the common difference of an arithmetic progression of three squares, then it would be a congruent number by Theorem 13.16. By definition, it would be the area of a rational right triangle. But then we could divide the lengths of the sides of the triangle by 4 and we would have a rational right triangle of area 3, which implies that 3 would be a congruent number, contrary to Exercise 12.

15. $r = 337/120$

17. $(12, 7/2, 25/2)$

19. **a.** Let r be the common difference of the arithmetic progression. Then $a^2 = b^2 - r$ and $c^2 = b^2 + r$. Then $(a/b)^2 + (c/b)^2 = (a^2 + c^2)/b^2 = ((b^2 - r) + (b^2 + r))/b^2 = 2b^2/b^2 = 2$. Therefore, $(a/b, c/b)$ is a rational point on $x^2 + y^2 = 2$. **b.** Because $x^2 + y^2 = 2 = 1 + 1$, we have $y^2 - 1 = 1 - x^2$. Multiply through by t^2 to get $(ty)^2 - t^2 = t^2 - (tx)^2$, which shows that $(tx)^2, t^2, (ty)^2$ is an arithmetic progression.

21. $(x, y) = (112/9, 980/27)$

23. If there is a rational point on the elliptic curve $y^2 = x^3 - 2^2x$, then by Theorem 13.18, 2 would be a congruent number, a contradiction.

25. $(11894/1443, 26760/3367, 115658/10101)$

27. $P_3 = (16689/2704, -1074861/140608)$ and the triangle is $(76130/10101, 32112/3367, 112768/10101)$

29. $(1151/140)^2, (1201/140)^2, (1249/140)^2$ and $(4319999/2639802)^2, (7776485/2639802)^2, (10113607/2639802)^2$

31. **a.** The solutions to $1 = 2x^2 + y^2 + 32z^2$ are $x = z = 0$, $y = \pm 1$, so $A_1 = 2$. The solutions to $1 = 2x^2 + y^2 + 8z^2$ are $x = z = 0$, $y = \pm 1$, so $B_1 = 2$. Because $A_1 \neq B_1/2$, we conclude that 1 is not a congruent number by Tunnell's theorem. **b.** The solutions to $10 = 8x^2 + 2y^2 + 64z^2$ are $(\pm 1, \pm 1, 0)$, so $C_{10} = 4$. The solutions to $10 = 8x^2 + 2y^2 + 16z^2$ are $(\pm 1, \pm 1, 0)$, so $D_{10} = 4$. Because $C_{10} \neq D_{10}/2$, we conclude that 10 is not a congruent number by Tunnell's theorem. **c.** The solutions to $17 = 2x^2 + y^2 + 32z^2$ are $(\pm 2, \pm 3, 0)$, so $A_{17} = 4$. The solutions to $17 = 2x^2 + y^2 + 8z^2$ are $(\pm 2, \pm 3, 0)$, $(\pm 2, \pm 1, \pm 1)$, and $(0, \pm 3, \pm 1)$, so $B_{17} = 16$. Because $A_{17} \neq B_{17}/2$, we conclude that 17 is not a congruent number by Tunnell's theorem.

33. The solutions to $41 = 2x^2 + y^2 + 32z^2$ are $(\pm 4, \pm 3, 0)$, $(\pm 2, \pm 1, \pm 1)$, and $(0, \pm 3, \pm 1)$, so $A_{41} = 16$. The solutions to $41 = 2x^2 + y^2 + 8z^2$ are $(\pm 4, \pm 3, 0)$, $(\pm 4, \pm 1, \pm 1)$, $(\pm 2, \pm 5, \pm 1)$, $(\pm 2, \pm 1, \pm 2)$, and $(0, \pm 3, \pm 2)$ so $B_{41} = 32$. Because $A_{41} = B_{41}/2$ we conclude that 41 is a congruent number by Tunnell's theorem.

35. For the case $n \equiv 5$ or $7 \pmod 8$, we note that n is odd and reduce the left sides of the first two equations in Tunnell's theorem modulo 8. Both expressions become $2x^2 + y^2 \pmod 8$. Because a square must be congruent to 0, 1, or 4 (mod 8), the right side of the congruence must be congruent to 0, 1, 2, 3, 4, or 6, and none of these are 5 or 7 (mod 8). Therefore $A_n = 0 = B_n/2$. By Tunnell's theorem, n must be a congruent number. For the case $n \equiv 6 \pmod 8$, we note that n is even and reduce the last two equations in Tunnell's theorem modulo 8. Both equations reduce to $6 \equiv n \equiv 2y^2 \pmod 8$. Because n is even, we may divide by 2 to get $3 \equiv n/2 \equiv y^2 \pmod 4$. Because 3 is not a quadratic residue modulo 4, there are no solutions to either equation. Therefore, $C_n = 0 = D_n/2$. By Tunnell's theorem, n must be a congruent number.

37. First suppose $n \geq 2$. Let $r = 2n/(n-2)$ and $s = (n-2)/4$. Check that $(2, r - 1/r, r + 1/r)$ and $(2, s - 1/s, s + 1/s)$ satisfy the Pythagorean theorem, so these triples represent right triangles. Because n is an integer, we see that the sides of both triangles are have rational lengths. If we glue these triangles together along the side of length 2, then we have a triangle with sides $(r + 1/2, s + 1/s, r - 1/r + s - 1/s)$. Note that the common side of length 2 is now an altitude of the new triangle. Therefore, the area of the triangle is $(1/2)2(r - 1/r + s - 1/s) = 2n/(n-2) - (n-2)/2n + (n-2)/4 - 4/(n-2) = (2n-4)/(n-2) + (n^2 - 4n + 4)/4n = 2 + (n^2 - 4n + 4)/4n = (n^2 + 4n + 4)/4n = (n+2)^2/4n$, which is rational, making this a Heron triangle. If we multiply all the sides by the rational number $2n/(n+2)$, then the area will by multiplied by its square, yielding $((n+2)^2/4n)(4n^2/(n+2)^2) = n$ for the final area. If $n = 1$ or 2, then we perform the above construction to get a Heron triangle of area 4 or 8, respectively, and then divide all sides by 2, which will divide the area by 4, yielding a Heron triangle of area 1 or 2, respectively.

39. **a.** Suppose n is a t-congruent number. Then there exist rational numbers a, b, and c satisfying $2n = ab(2t)/(t^2+1)$ and $c^2 = a^2 + b^2 - 2ab(t^2-1)/(t^2+1)$. Note that the first equation implies $n/t = ab/(t^2+1)$. We seek to show that the point $(c^2/4, (ca^2 - cb^2)/8)$ is a point on the curve. First note that $x - n/t = c^2/4 - n/t = (a^2 + b^2 - 2ab(t^2-1)/(t^2+1))/4 - ab/(t^2+1) = (a^2 + b^2 - 2ab)/4 = (a-b)^2/4$. Then note that $x + nt = c^2/4 + nt = (a^2 + b^2 - 2ab(t^2-1)/(t^2+1))/4 + 2abt^2/(t^2+1) = (a^2 + b^2 + 2ab)/4 = (a+b)^2/4$. Then $x(x - n/t)(x + nt) = (c^2/4)((a-b)^2/4)((a+b)^2)/4 = ((ca^2 - cb^2)/8)^2 = y^2$, so this is a rational point on the curve. Note that $y \neq 0$ unless $a = b$. If $a = b$, then the defining equations become $2a^2 - 2a^2(t^2-1)/(t^2+1) = c^2$, and $n/t = a^2/(t^2+1)$. Solve the first equation to get $t^2 + 1 = (2a/c)^2$ and use this in the second equation to get $n/t = (c/a)^2$, so both t^2+1 and n/t are rational squares. Conversely, suppose (x, y) is a rational point on the curve with $y \neq 0$. Substitute the values $a = n|x(1+t^2)/(yt)|$, $b = |(x - n/t)(x + nt)/y|$, and $c = |(x^2 + n^2)/y|$ into the defining equations to see that n is a t-congruent number. If n/t and $t^2 + 1$ are nonzero rational squares, then substitute $c = 2\sqrt{n/t}$ and $a = c = \sqrt{n(t^2+1)/t}$ into the defining equations to see that n is a t-congruent number. **b.** For the given values, $x(x - n/t)(x + nt) = -6(-6 - 12/(4/3))(-6 + 12(4/3)) = -6(-6-9)(-6+16) = 6(15)(10) = 900 = 30^2 = y^2$. **c.** Part (b) shows that, for $n = 12$ and $t = 4/3$, the curve $y^2 = x(x - n/t)(x + nt)$ has a rational point, $(-6, 30)$ with $y \neq 0$. Therefore, 12 is a 4/3-congruent number. Then using the formulas from part (a), we have $a = |((-6)^2 + 12^2)/30| = 6$, $b = |(-6 - 12/(4/3))(-6 + 12(4/3))/30| = 5$, and $c = 12| - 6((4/3 + 1/(4/3))/30| = 5$. Check that the triangle with sides 6, 5, and 5 has area equal to 12. **d.** Given a positive integer n, Exercise 37 tells us there exists a Heron triangle (x, y, z) of area n. Then from Exercise 38, if the angle between x and y is θ, then $\sin\theta = 2t/(t^2+1)$ and $cos\theta = (t^2-1)/(t^2+1)$ for some rational t. The law of cosines tells us that $z^2 = x^2 + y^2 - 2xy\cos\theta = x^2 + y^2 - 2xy(t^2-1)/(t^2+1)$. Because the area is $n = xy\sin(\theta)/2 = xy(2t/(t^2+1)$, we see that n is a t-congruent number.

Section 14.1

1. **a.** $5 + 15i$ **b.** $46 - 9i$ **c.** $-26 - 18i$

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

5. $(4a - 3b) + (4b + 3a)i$ where a and b are rational integers (see the *Student Solutions Manual* for the display of such integers).

7. Because $\alpha|\beta$ and $\beta|\gamma$, there exist Gaussian integers μ and ν such that $\mu\alpha = \beta$ and $\nu\beta = \gamma$. Because the product of Gaussian integers is a Gaussian integer, $\nu\mu$ is also a Gaussian integer. It follows that $\alpha|\gamma$.

9. Note that $x^5 = x$ if and only if $x^5 - x = x(x-1)(x+1)(x-i)(x+i) = 0$. The solutions of this equation are 0, 1, -1, i, and $-i$. These are the four Gaussian integers that are units, together with 0.

11. Because $\alpha|\beta$ and $\beta|\alpha$, there exist Gaussian integers μ and ν such that $\alpha\mu = \beta$ and $\beta\nu = \alpha$. Then $\alpha = \alpha\mu\nu$. Taking norms of both sides yields $N(\alpha) = N(\alpha\mu\nu) = N(\alpha)N(\mu\nu)$ by Theorem 14.1. So that $N(\mu)N(\nu) = 1$. Because μ and ν are Gaussian integers, their norms must be nonnegative rational integers. Therefore, $N(\mu) = N(\nu) = 1$, and so μ and ν are units, and hence, α and β are associates.

13. The pair $\alpha = 1 + 2i$, $\beta = 2 + i$ is a counterexample.

15. We show that such an associate exists. If $a > 0$ and $b \geq 0$, then the desired inequalities are met. If $a \leq 0$ and $b > 0$, then we multiply by $-i$ to get $-i\alpha = b - ai = c + di$ which has $c > 0$ and $d \geq 0$. If $a < 0$ and $b \leq 0$, then we multiply by -1 to get $-\alpha = -a - bi = c + di$, which has $c > 0$ and $d \geq 0$. If $a \geq 0$ and $b < 0$ then we multiply by i to get $i\alpha = -b + ai = c + di$, which has $c > 0$ and $d \geq 0$. (We have covered the quadrants in the plane in counterclockwise order.) Having found the associate $c + di$ in the first quadrant, we observe that it is unique, because if we multiply by any unit other than one, we get, respectively, $-c - di$, which has $-c < 0$, $-d + ci$, which has $-d \leq 0$, or $d - ci$, which has $-c < 0$.

17. **a.** $\gamma = 3 - 5i, \rho = -3i, N(\rho) = 3^2 + 0^2 = 9 < N(\beta) = 3^2 + 3^2 = 18$ **b.** $\gamma = 5 - i, \rho = -1 - 2i$, $N(\rho) = 5 < N(\beta) = 25$ **c.** $\gamma = -1 + 8i,\ \rho = -5 - 3i,\ N(\rho) = 5^2 + 3^2 = 34 < N(\beta) = 11^2 + 2^2 = 125$

19. **a.** $\gamma = 2 - 5i, \rho = 3$ **b.** $\gamma = 4 - i, \rho = 2 + 2i$ **c.** $\gamma = -1 + 7i., \rho = -3 + 8i$

21. 1, 2, and 4

23. If a and b are both even, then the Gaussian integer is divisible by 2. Because $(1+i)(1-i) = 2$, then $1 + i$ is a divisor of 2, which is in turn a divisor of $a + bi$. If a and b are both odd, we may write $a + bi = (1+i) + (a-1) + (b-1)i$, and $a - 1$ and $b - 1$ are both even. Because both of theses Gaussian integers are multiples of $1 + i$, so is their sum. If a is odd and b is even, then $a - 1 + bi$ is a multiple of $1 + i$ and hence $(a + bi) - (a - 1 + bi) = 1$ is a multiple of $1 + i$ if $a + bi$ is, a contradiction. A similar argument shows that if a is even and b is odd, then $1 + i$ does not divide $a + bi$.

25. $\pm 1 \pm 2i$

27. Suppose $7 = (a + bi)(c + di)$ where $a + bi$ and $c + di$ are nonunit Gaussian integers. Taking norms of both sides yields $49 = (a^2 + b^2)(c^2 + d^2)$. Because $a + bi$ and $c + di$ are not units, we have that the factors on the right are not equal to 1, so we must have $a^2 + b^2 = 7$, a contradiction, because 7 is not the sum of two squares.

29. Because α in neither a unit nor a prime, it has factors $\alpha = \beta\gamma$ with β and γ nonunits, so that $1 < N(\beta)$ and $1 < N(\gamma)$. Then $N(\alpha) = N(\beta)N(\gamma)$. If $N(\beta) > \sqrt{N(\alpha)}$, then $N(\gamma) = N(\alpha)/N(\beta) < N(\alpha)/\sqrt{N(\alpha)} = \sqrt{N(\alpha)}$. Consequently, either β or γ divides α and has norm not exceeding $\sqrt{N(\alpha)}$.

31. The Gaussian primes with norm less than 100 are 3, 7, $1 + i$, $2 + i$, $4 + i$, $6 + i$, $3 + 2i$, $5 + 2i$, $7 + 2i$, $8 + 3i$, $5 + 4i$, $9 + 4i$, $6 + 5i$, and $8 + 5i$, together with their conjugates and associates.

33. **a.** Note that $\alpha - \alpha = 0 = 0 \cdot \mu$, so $\mu|\alpha - \alpha$. Thus, $\alpha \equiv \alpha \pmod{\mu}$. **b.** Because $\alpha \equiv \beta \pmod{\mu}$, we have $\mu|\alpha - \beta$, so there exists a Gaussian integer γ such that $\mu\gamma = \alpha - \beta$. But then $\mu(-\gamma) = \beta - \alpha$, so $\mu|\beta - \alpha$. Therefore, $\beta \equiv \alpha \pmod{\mu}$. **c.** Because $\alpha \equiv \beta \pmod{\mu}$ and $\beta \equiv \gamma \pmod{\mu}$, there exist Gaussian integers δ and ϵ such that $\mu\delta = \alpha - \beta$ and $\mu\epsilon = \beta - \gamma$. Then $\alpha - \gamma = \alpha - \beta + \beta - \gamma = \mu\delta + \mu\epsilon = \mu(\delta + \epsilon)$. Therefore $\alpha \equiv \gamma \pmod{\mu}$.

35. Let $\alpha = a_1 + ib_1$, $\beta = a_2 + ib_2$, and $p = (a_1 + b_1)(a_2 + b_2)$. Then the real part of $\alpha\beta$ is given by the two multiplications $R = a_1a_2 - b_1b_2$, and the imaginary part is given by $p - R$, which requires only one more multiplication. The second way in the hint goes as follows. Let $m_1 = b_2(a_1 + b_1)$, $m_2 = a_2(a_1 - b_1)$, and $m_3 = b_1(a_2 - b_2)$. These are the three multiplications. Then the real part of $\alpha\beta$ is given by $m_2 + m_3$, and the imaginary part by $m_1 + m_3$.

37. **a.** i, $1 + i$, $1 + 2i$, $2 + 3i$, $3 + 5i$, $5 + 8i$ **b.** Using the definition of G_k and the properties of the Fibonacci sequence, we have $G_k = f_k + if_{k+1} = (f_{k-1} + f_{k-2}) + (f_k + f_{k-1})i = (f_{k-1} + f_k i) + (f_{k-2} + f_{k-1}i) = G_{k-1} + G_{k-2}$.

39. We proceed by induction. For the basis step, note that $G_2G_1 - G_3G_0 = (1 + 2i)(1 + i) - (2 + 3i)(i) = 2 + i$, so the basis step holds. Now assume the identity holds for values less than n. We compute, using the identity in Exercise 37, $G_{n+2}G_{n+1} - G_{n+3}G_n = (G_{n+1} + G_n)G_{n+1} - (G_{n+2} + G_{n+1})G_n = G_{n+1}^2 - G_{n+2}G_n = G_{n+1}^2 - (G_{n+1} + G_n)G_n = G_{n+1}^2 - G_n^2 - G_{n+1}G_n = (G_{n+1} + G_n)(G_{n+1} - G_n) - G_{n+1}G_n = G_{n+2}G_{n-1} - G_{n+1}G_n = -(-1)^{n-1}(2 + i) = (-1)^n(2 + i)$, which completes the induction step.

41. Because the coefficients of the polynomial are real, the other root is $r - si$, and over the complex numbers the polynomial must factor as $(z - (r + si))(z - (r - si)) = z^2 - 2rz + r^2 + s^2$. The z-coefficients, $a = 2r$ and $b = r^2 + s^2$, are integers. Then $r = a/2$ and $s^2 = (4b - a^2)/4$, which shows that $s = c/2$ for some integer c. Multiplying by 4, we have $a^2 + c^2 \equiv 0 \pmod 4$, which can be true only if both a and c are even; hence, r and s are integers and $r + si$ is a Gaussian integer.

43. Let $\beta = 1 + 2i$ so that $N(\beta) = 5$. From the proof of the Division algorithm, we have for a Gaussian integer α that there exist Gaussian integers γ and ρ such that $\alpha = \gamma\beta + \rho$ with $N(\rho) \le N(\beta)/2 = 5/2$. Therefore, the only possible remainders upon division by $1 + 2i$ are 0, 1, i, $1 + i$ and their associates. Furthermore, we can always replace a remainder of $1 + i$ with a remainder of -1 because $\alpha = \beta\gamma + (1 + i) = \beta(\gamma + 1) + (1 + i) - (1 + 2i) = \beta(\gamma + 1) - i$. So we may take the entire set of remainders to be 0, 1, -1, i and $-i$. Consider dividing each of the Gaussian primes $\pi_1, \ldots, \pi_4$ by β. If any two left the same remainder ρ, then β divides the difference between the two primes. But all these differences are either 2 or $\pm 1 \pm i$, which are not divisible by β. Further, since these are all prime, none of the remainders are 0. Therefore, the remainders are exactly the set 1, -1, i, and $-i$. Now divide $a + bi$ by β and let the remainder be ρ. If ρ is not zero, then it is one of 1, -1, i, or $-i$. But then one of $\pi_1, \ldots, \pi_4$ leaves the same remainder upon division by β, say π_k. Then β divides $\pi_k - (a + bi)$ which is a unit, a contradiction. Therefore, $\rho = 0$. Therefore, $1 + 2i$ divides $a + bi$. A similar argument shows that $1 - 2i$ also divides $a + bi$. Therefore, the product of these primes $(1 - 2i)(1 + 2i) = 5$ also divides $a + bi$, and hence each of the components. Now suppose that $b = 0$. Then $a \pm 1$ are prime and by Exercise 23, $a \pm 1$ are odd. Therefore, one of them, say $a + 1$, is a prime congruent to 1 modulo 4. By Theorem 13.5, there exist integers x, and y such that $a + 1 = x^2 + y^2 = (x + yi)(x - yi)$. Because $a + 1$ is prime, one of $x \pm yi$ is a unit, which implies that one of x or y is zero, which in turn implies that $a + 1$ is a square. So in any case, one of $a \pm 1$ is not a Gaussian prime. Therefore, $b \ne 0$. Similarly, if we apply Exercise 26, we see that $a \ne 0$.

45. Taking norms of the equation $\alpha\beta\gamma = 1$ shows that all three numbers must be units in the Gaussian integers, which restricts our choices to 1, -1, i, and $-i$. Choosing three of these in the equation $\alpha + \beta + \gamma = 1$, we have the possible solutions, up to permutation, $(1, 1, -1)$, $(1, i, -i)$, but only the second solution works in the first equation, leaving $(1, i, -i)$ as the only solution.

Section 14.2

1. Certainly $1 | \pi_1$ and $1 | \pi_2$. Suppose $\delta | \pi_1$ and $\delta | \pi_2$. Because π_1 and π_2 are Gaussian primes, δ must be either a unit or an associate of the primes. But because π_1 and π_2 are not associates, then they can not have an associate in common, so δ is a unit and so $\delta | 1$. Therefore, 1 satisfies the definition of a greatest common divisor for π_1 and π_2.

3. Because γ is a greatest common divisor of α and β, we have $\gamma|\alpha$ and $\gamma|\beta$, so there exist Gaussian integers μ and ν such that $\mu\gamma = \alpha$ and $\nu\gamma = \beta$. So that $\overline{\mu\gamma} = \overline{\mu} \cdot \overline{\gamma} = \overline{\alpha}$ and $\overline{\nu\gamma} = \overline{\nu} \cdot \overline{\gamma} = \overline{\beta}$; so that $\overline{\gamma}$ is a common divisor of $\overline{\alpha}$ and $\overline{\beta}$. Further, if $\delta|\overline{\alpha}$ and $\delta|\overline{\beta}$, then $\overline{\delta}|\alpha$ and $\overline{\delta}|\beta$, and so $\overline{\delta}|\gamma$ by the definition of greatest common divisor. But then $\overline{\overline{\delta}}|\overline{\gamma}$ and $\overline{\overline{\delta}} = \delta$, which shows that $\overline{\gamma}$ is a greatest common divisor for $\overline{\alpha}$ and $\overline{\beta}$.

5. Let $\epsilon\gamma$, where ϵ is a unit, be an associate of γ. Because $\gamma|\alpha$, there is a Gaussian integer μ such that $\mu\gamma = \alpha$. Because ϵ is a unit, $1/\epsilon$ is also a Gaussian integer. Then $(1/\epsilon)\mu(\epsilon\gamma) = \alpha$, so $\epsilon\gamma|\alpha$. Similarly, $\epsilon\gamma|\beta$. If $\delta|\alpha$ and $\delta|\beta$, then $\delta|\gamma$ by definition of greatest common divisor, so there exists a Gaussian integer ν such that $\nu\delta = \gamma$. Then $\epsilon\nu\delta = \epsilon\gamma$, and because $\epsilon\nu$ is a Gaussian integer, we have $\delta|\epsilon\gamma$, so $\epsilon\gamma$ satisfies the definition of a greatest common divisor.

7. Take $(3 - 2i)$ and $(3 + 2i)$, for example.

9. Because a and b are relatively prime rational integers, there exist rational integers m and n such that $am + bn = 1$. Let δ be a greatest common divisor of the Gaussian integers a and b. Then δ divides $am + bn = 1$. Therefore, δ is a unit in the Gaussian integers and hence a and b are relatively prime Gaussian integers.

11. **a.** We have $44 + 18i = (12 - 16i)(1 + 2i) + 10i$; $12 - 16i = (10i)(-2 - i) + (2 + 4i)$; $10i = (2 + 4i)(2 + i) + 0$. The last nonzero remainder, $2 + 4i$, is a greatest common divisor. **b.** By part (a), $2 + 4i = (12 - 16i) - (10i)(-2 - i) = (12 - 16i) - ((44 + 18i) - (12 - 16i)(1 + 2i))(-2 - i) = (2 + i)(44 + 18i) + (1 + (1 + 2i)(-2 - i))(12 - 16i) = (2 + i)(44 + 18i) + (1 - 5i)(12 - 16i)$. Take $\mu = 2 + i$ and $\nu = 1 - 5i$.

13. We proceed by induction. We have $G_0 = i$ and $G_1 = 1 + i$. Because G_0 is a unit, these are relatively prime and this completes the basis step. Assume we know that G_k and G_{k-1} are relatively prime. Suppose $\delta|G_k$ and $\delta|G_{k+1}$. Then $\delta|(G_{k+1} - G_k) = (G_k + G_{k-1} - G_k) = G_{k-1}$, so δ is a common divisor of G_k and G_{k-1}, which are relatively prime. Hence, 1 is a greatest common divisor of G_{k+1} and G_k.

15. Let k be the smallest rational integer such that $N(\alpha) < 2^k$. Dividing $\beta = \rho_0$ by $\alpha = \rho_1$ in the first step of the Euclidean algorithm gives us $\beta = \gamma_2\alpha + \rho_2$ with $N(\rho_2) < N(\alpha) < 2^{k-1}$. The next step of the Euclidean algorithm gives us $\alpha = \gamma_3\rho_2 + \rho_3$ with $N(\rho_3) < N(\rho_2) < 2^{k-2}$. Continuing with the algorithm shows us that $N(\rho_k) < 2^{k-(k-1)} = 2$, so that the Euclidean algorithm must terminate in no more than $k = [\log_2 N(\alpha)] + 1$ steps. And thus we have $k = O(\log_2(N(\alpha))$.

17. **a.** $(-1)(1 - 2i)(1 - 4i)$ **b.** $3 - 13i = (-1)(1 + i)(5 + 8i)$ **c.** $(-1)(1 + i)^4(7)$
d. $i(1 + i)^8(1 + 2i)^2(1 - 2i)^2$

19. **a.** 48 **b.** 120 **c.** 1792 **d.** 2592

21. Assume n and $a + bi$ are relatively prime. Then there exist Gaussian integers μ and ν such that $\mu n + \nu(a + bi) = 1$. If we take conjugates of both sides and recall that the conjugate of a rational integer is itself, we have $\overline{\mu}n + \overline{\nu}(a - bi) = 1$, so n is also relatively prime to $a - bi$. Because $a - bi$ is an associate of $b + ai$ (multiply by i), we have the result. The converse is true by symmetry.

23. Suppose that $\pi_1, \pi_2, \ldots, \pi_k$ are all of the Gaussian primes and form the Gaussian integer $Q = \pi_1\pi_2 \cdots \pi_k + 1$. From Theorem 14.10, we know that Q has a unique factorization into Gaussian primes, and hence is divisible by some Gaussian prime ρ. Then $\rho|Q$ and $\rho|\pi_1\pi_2 \cdots \pi_k$, so ρ divides their difference, which is 1, a contradiction, unless ρ is a prime different from $\pi_1, \pi_2, \ldots, \pi_k$, proving that we did not have all the Gaussian primes.

25. $-2i$

27. Because α and μ are relatively prime, there exist Gaussian integers σ and τ such that $\sigma\alpha + \tau\mu = 1$. If we multiply through by β, we get $\beta\sigma\alpha + \beta\tau\mu = \beta$, so that we know $\alpha(\beta\sigma) \equiv \beta \pmod{\mu}$ and thus $x \equiv \beta\sigma \pmod{\mu}$ is the solution.

29. **a.** $x \equiv 5 - 4i \pmod{13}$ **b.** $x \equiv 1 - 2i \pmod{4 + i}$ **c.** $x \equiv 3i \pmod{2 + 3i}$

31. *Chinese Remainder Theorem for Gaussian Integers.* Let $\mu_1, \mu_2, \ldots, \mu_r$ be pairwise relatively prime Gaussian integers, and let $\alpha_1, \alpha_2, \ldots, \alpha_r$ be Gaussian integers. Then the system of congruences $x \equiv \alpha_i \pmod{\mu_i}$, $i = 1, \ldots, r$ has a unique solution modulo $M = \mu_1\mu_2 \cdots \mu_r$. *Proof:* To construct a solution, for each $k = 1, \ldots, r$, let $M_k = M/\mu_k$. Then M_k and μ_k are relatively prime, because μ_k is relatively prime to all of the factors of M_k. Then from Exercise 24, we know M_k has an inverse λ_k modulo μ_k, so that $M_k\lambda_k \equiv 1 \pmod{\mu_k}$. Now let $x = \alpha_1 M_1 \lambda_1 + \cdots + \alpha_r M_r \lambda_r$. We will show x is the solution to the system.

Because $\mu_k | M_j$ whenever $j \neq k$, we have $\alpha_j M_j \lambda_k \equiv 0 \pmod{\mu_k}$ whenever $j \neq k$. Therefore, $x \equiv \alpha_k M_k \lambda_k \pmod{\mu_k}$ Also, because λ_k is an inverse for M_k modulo μ_k, we have $x \equiv \alpha_k \pmod{\mu_k}$ for every k, as desired.

Now suppose there is another solution y to the system. Then $x \equiv \alpha_k \equiv y \pmod{\mu_k}$, and so $\mu_k | (x - y)$ for every k. Because the μ_k are pairwise relatively prime, no Gaussian prime appears in more than one of their prime factorizations. Therefore, if a Gaussian prime power $\pi^e | (x - y)$, then it divides exactly one of the μ_k's. Therefore, the product M of the μ_k's also divides $x - y$, and so $x \equiv y \pmod{M}$, showing that x is unique modulo M.

33. $x \equiv 9 + 23i \pmod{26 + 7i}$

35. **a.** $\{0, 1\}$ **b.** $\{0, 1, i, 1 + i\}$ **c.** $\{0, 1, 2, 2i, -1 - i, -i, 1 - i, -1 + i, i, 1 + i, -2i, -2, -1\}$

37. Let $\alpha = a + bi$ and $d = \gcd(a, b)$. We assert that the set $S = \{p + qi | 0 \leq p < N(\alpha)/d, 0 \leq q < d\}$ is a complete residue system. Note that this represents a rectangle of lattice points in the plane. We create two multiples of α. First, $N(\alpha)/d = \alpha(\overline{\alpha}/d)$ is a real number and a multiple of α. Second, there exist rational integers r and s such that $ra + sb = d$. So we have the multiple of α given by $v = (s + ir)\alpha = (s + ir)(a + bi) = (as - br) + di$. Now it is clear that any Gaussian integer is congruent modulo α to an integer in the rectangle S, because first we can add or subtract multiples of v until the imaginary part is between 0 and $d - 1$ and then add and subtract multiples of $N(\alpha)/d$ until the real part is between 0 and $N(\alpha)/d - 1$. It remains to show the elements of S are incongruent to each other modulo α. Suppose β and γ are in S and congruent to each other modulo α. Then the imaginary part of $\beta - \gamma$ must be divisible by d, but because these must lie in the interval from 0 to $d - 1$, they must be equal. Therefore, the difference between β and γ is real and divisibly by α, hence by $\overline{\alpha}$ and hence by $\alpha\overline{\alpha}/d = N(\alpha)/d$, which proves they are equal. Because S has $N(\alpha)$ elements, we are done.

39. **a.** $\{i, -i, 1, -1\}$ **b.** $\{i, -i, 1, 1 + 2i, 2 + i, 2 - i, -1, -1 + 2i\}$ **c.** $\{i, 2 - i, -2 + i, -i, 1, 1 + 2i, -1 - 2i, -1\}$

41. By the properties of the norm function and Exercise 37, we know that there are $N(\pi^e) = N(\pi)^e$ residue classes modulo π^e. Let $\pi = r + si$, and $d = \gcd(r, s)$. Also, by Exercise 37, a complete residue system modulo π^e is given by the rectangle $S = \{p + qi | 0 \leq p < N(\pi^e)/d, 0 \leq q < d\}$, while a complete residue system modulo π is given by the rectangle $T = \{p + qi | 0 \leq p < N(\pi)/d, 0 \leq q < d\}$. Note that in T there is exactly one element not relatively prime to π, and that there are $N(\pi)^{e-1}$ copies of T, congruent modulo π, inside of S. Therefore, there are exactly $N(\pi)^{e-1}$ elements in S not relatively prime to π. Thus, there are $N(\pi)^e - N(\pi)^{e-1}$ elements in a reduced residue system modulo π^e.

43. **a.** First note that because $r + s\sqrt{-5}$ is a root of a monic polynomial with integer coefficient, the other root must be $r - s\sqrt{-5}$ and the polynomial is $(x - (r + s\sqrt{-5}))(x - (r - s\sqrt{-5})) = x^2 - 2rx + (r^2 + 5s^2) = x^2 - ax + b$, where a and b are rational integers. Then $r = a/2$ and $5s^2 = (4b - a^2)/4$, so that $s = c/2$ for some integer c. (Note that 5 cannot appear in the denominator of s, or else when we square it, the single factor of 5 in the expression leaves a remaining factor in the denominator, which does not appear on the right side of the equation.) Substituting these expressions for r and s, we have $(a/2)^2 + 5(c/2)^2 = b^2$, or upon multiplication by 4, $a^2 + 5c^2 = 4b^2 \equiv 0 \pmod 4$, which has solutions only when a and c are even. Therefore, r and s are rational integers. **b.** Let $\alpha = a + b\sqrt{-5}$ and $\beta = c + d\sqrt{-5}$. Then $\alpha + \beta = (a + c) + (b + d)\sqrt{-5}$ and $\alpha - \beta = (a - c) + (b - d)\sqrt{-5}$, and $\alpha\beta = (ac - 5bd) + (ad + bc)\sqrt{-5}$. Because the rational integers are closed under addition, subtraction, and multiplication, all of the results are again of the form $p + q\sqrt{-5}$ with p and q rational integers. **c.** yes, no **d.** Let $\alpha = a + b\sqrt{-5}$ and $\beta = c + d\sqrt{-5}$. Then $N(\alpha)N(\beta) = (a^2 + 5b^2)(c^2 + 5d^2) = a^2c^2 + 5a^2d^2 + 5b^2c^2 + 25b^2d^2$. On the other hand, $\alpha\beta = (ac - 5bd) + (ad + bc)\sqrt{-5}$ and $N((ac - 5bd) + (ad + bc)\sqrt{-5}) = (ac - 5bd)^2 + 5(ad + bc)^2 = a^2c^2 - 10acbd + 25b^2d^2 + 5(a^2d^2 + 2adbc + b^2c^2) = a^2c^2 + 5a^2d^2 + 5b^2c^2 + 25b^2d^2$, which is equal to the expression above, proving the assertion. **e.** If ϵ is a unit in $\mathbf{Z}[\sqrt{-5}]$, then there exists an η such that $\epsilon\eta = 1$. From part (d), we have $N(\epsilon\eta) = N(\epsilon)N(\eta) = N(1) = 1$, so $N(\epsilon) = 1$. Suppose $\epsilon = a + b\sqrt{-5}$, then $N(\epsilon) = a^2 + 5b^2 = 1$, which shows that $b = 0$, and hence $a^2 = 1$, so that we know $a = \pm 1$. Therefore, the only units are 1 and -1. **f.** If an integer α in $\mathbf{Z}[\sqrt{-5}]$ is not a unit and not prime, then it must have two non-unit divisors β and γ such that $N(\beta)N(\gamma) = N(\alpha)$. To see that 2 is prime, note that a divisor $\beta = a + b\sqrt{-5}$ has norm $a^2 + 5b^2$, while $N(2) = 4$, which forces $b = 0$. If β is not a unit, then $a = \pm 2$, but then this forces γ to be a unit; hence 2 is prime. To see that 3 is prime, we seek divisors of $N(3) = 9$ among $a^2 + 5b^2$. We see that b can be only 0 or ± 1, or else the norm is too large. And if $b = \pm 1$, then the only possible divisor is 9 itself, forcing the other divisor to be a unit. If $b = 0$, then $a = \pm 3$, and hence 3 is prime. To see that $1 \pm \sqrt{-5}$ is prime, note that its norm is 6. A divisor $a + bi$ can have b take on the values 0 and ± 1, else the norm is too large. If $b = 0$, then $a^2 \mid 6$ a contradiction, so $b = \pm 1$. But then $(a^2 + 5) \mid 6$, forcing $a = \pm 1$. But $N(\pm 1 \pm \sqrt{-5}) = 6$, so the other divisor is a unit, and so $1 \pm \sqrt{5}$ is also prime. Note then that $2 \cdot 3 = 6$ and $(1 - \sqrt{-5})(1 + \sqrt{-5}) = 6$, so that we do not have unique factorization into primes in $\mathbf{Z}[\sqrt{-5}]$. **g.** Suppose γ and ρ exist. Note first that $(7 - 2\sqrt{-5})/(1 + \sqrt{-5}) = -1/2 - 3/2\sqrt{-5}$, so $\rho \neq 0$. Let $\gamma = a + b\sqrt{-5}$ and $\rho = c + d\sqrt{-5}$. Then from $7 - 2\sqrt{-5} = (1 + \sqrt{-5})(a + b\sqrt{-5}) + (c + d\sqrt{-5}) = (a - 5b + c) + (a + b + d)\sqrt{-5}$, we get $7 = a - 5b + c$ and $-2 = a + b + d$. If we subtract the second equation from the first, we have $9 = -6b + c - d$ or $c - d = 6b + 9$. Therefore, $3 \mid c - d$, and because $\rho \neq 0$, $c - d \neq 0$, so $|c - d| \geq 3$. We consider $N(\rho) = c^2 + 5d^2$. If $d = 0$, then $N(\rho) \geq c^2 \geq 3^2 > 6$. If $d = \pm 1$, then $|c| \geq 2$ and $N(\rho) = c^2 + 5d^2 \geq 4 + 5 > 6$. If $|d| \geq 2$, then $N(\rho) \geq 5d^2 \geq 5 \cdot 2^2 = 20 > 6$, so in every case the norm of ρ is greater than 6. So no such γ and ρ exist, and there is no analog for the division algorithm in $\mathbf{Z}[\sqrt{-5}]$. **h.** Suppose $\mu = a + b\sqrt{-5}$ and $\nu = c + d\sqrt{-5}$ is a solution to the equation. Then $3(a + b\sqrt{-5}) + (1 + \sqrt{-5})(c + d\sqrt{-5}) = (3a + c - 5d) + (3b + c + d)\sqrt{-5} = 1$. So we must have $3a + c - 5d = 1$ and $3b + c + d = 0$. If we subtract the second equation from the first, we get $3a - 3b - 6d = 1$, which implies that $3 \mid 1$, an absurdity. Therefore, no such solution exists.

Section 14.3

1. **a.** 8 **b.** 8 **c.** 0 **d.** 16

3. We first check that a greatest common divisor δ of α and β divides γ, otherwise no solution exists. If a solution exists, we use the Euclidean algorithm and back substitution to express δ as a linear combination of α and β: $\alpha\mu + \beta\nu = \delta$. Because δ divides γ, there is a Gaussian integer η such that $\delta\eta = \gamma$. If we multiply the last equation by η, we have $\alpha\mu\eta + \beta\nu\eta = \delta\eta = \gamma$, so we may take $x_0 = \mu\eta$ and $y_0 = \nu\eta$ as a solution. The set of all solutions is given by $x = x_0 + \beta\tau/\delta$, $y = y_0 - \alpha\tau/\delta$, where τ ranges over the Gaussian integers.

5. **a.** no solutions **b.** no solutions

7. Let $\alpha = a + bi$. Then $N(\alpha) = a^2 + b^2 = p$, and by Theorem 14.5, we know that α and $\overline{\alpha}$ are Gaussian primes. Similarly, if $\gamma = c + di$, then γ and $\overline{\gamma}$ are Gaussian primes. By Theorem 14.10, α must be an associate of γ or $\overline{\gamma}$. So α must equal one of the following: $\pm c \pm di$, $\pm d \pm ci$, and in any of these cases we must have $a = \pm c$ and $b = \pm d$ or $a = \pm d$ and $b = \pm c$. Squaring these equations gives the result.

9. Suppose x, y, z is a primitive Pythagorean triple with y even, so that x and z are necessarily odd. Then $z^2 = x^2 + y^2 = (x + iy)(x - iy)$ in the Gaussian integers. If a rational prime p divides $x + iy$, then it must divide both x and y, which contradicts the fact that the triple is primitive. Therefore, the only Gaussian primes that divide $x + iy$ are of the form $m + in$ with $n \neq 0$. Also, if $1 + i | x + iy$, then we have the conjugate relationship $1 - i | x - iy$, which implies that $2 = (1 - i)(1 + i)$ divides z^2, which is odd, a contradiction. Therefore, we conclude that $1 + i$ does not divide $x + iy$, and hence neither does 2. Suppose δ is a common divisor of $x + iy$ and $x - iy$. Then δ divides the sum $2x$ and the difference $2iy$. Because we know that 2 is not a common factor, δ must divide both x and y, which we know are relatively prime. Hence, δ is a unit and $x + iy$ and $x - iy$ are also relatively prime. Then we know that every prime that divides $x + iy$ is of the form $\pi = u + iv$, and so $\overline{\pi} = u - iv$ divides $x - iy$. Because their product equals a square, each factor is a square. Thus, $x + iy = (m + in)^2$ and $x - iy = (m - in)^2$ for some Gaussian integer $m + in$ and its conjugate. But then $x + iy = m^2 - n^2 + 2mni$, so $x = m^2 - n^2$ and $y = 2mn$. And $z^2 = (m + ni)^2(m - ni)^2 = (m^2 + n^2)^2$, so $z = m^2 + n^2$. Further, if m and n were both odd or both even, we would have z even, a contradiction, so we may conclude that m and n have opposite parity. Finally, having found m and n that work, if $m < n$, then we can multiply by i and reverse their roles to get $m > n$. The converse is exactly as in Section 13.1.

11. By Lemma 14.3, there is a unique rational prime p such that $\pi | p$. Let $\alpha = a + bi$ and consider 3 cases.

Case 1: If $p = 2$, then π is an associate of $1 + i$ and $N(\pi) - 1 = 1$. Since there are only two congruence classes modulo $1 + i$ and since α and $1 + i$ are relatively prime, we have $\alpha^{N(\pi)-1} = \alpha \equiv 1 \pmod{1 + i}$.

Case 2: If $p \equiv 3 \pmod 4$, then π and p are associates and $N(\pi) - 1 = p^2 - 1$. Also $(-i)^p = -i$. By the binomial theorem, we have $\alpha^p = (a + bi)^p \equiv a^p + (bi)^p \equiv -ib^p \equiv a - bi \equiv \alpha \pmod p$, using Fermat's little theorem. Similarly, $\overline{\alpha}^p \equiv \alpha \pmod p$, so that $\alpha^{p^2} \equiv \overline{\alpha}^p \equiv \alpha \pmod p$, and since $p = \pi$ and α and π are relatively prime, we have $\alpha^{N(\pi)-1} \equiv 1 \pmod p$.

Case 3: If $p \equiv 1 \pmod 4$, then $\pi\overline{\pi} = p$, $i^p = i$, and $N(\pi) - 1 = p - 1$. By the Binomial theorem, we have $\alpha^p = (a + bi)^p \equiv a^p + (bi)^p \equiv a + bi \equiv \alpha \pmod p$, using Fermat's little theorem. Cancelling an α gives us $\alpha^{p-1} \equiv 1 \pmod p$, and because $\pi | p$, we have $\alpha^{N(\pi)-1} \equiv 1 \pmod \pi$, which concludes the proof.

13. Let π be a Gaussian prime. If $\alpha^2 \equiv 1 \pmod \pi$, then $\pi | \alpha^2 - 1 = (\alpha - 1)(\alpha + 1)$, so that either $\alpha \equiv 1$ or $\alpha \equiv -1 \pmod \pi$. Therefore, only 1 and -1 can be their own inverses modulo π. Now let $\alpha_1 = 1, \alpha_2, \ldots, \alpha_{r-1}, \alpha_r = -1$ be a reduced residue system modulo π. For each α_k, $k = 2, 3, \ldots, r - 1$, there is a multiplicative inverse modulo π α'_k such that $\alpha_k\alpha'_k \equiv 1 \pmod \pi$. If we group all such pairs in the reduced residue system together, then the product is easy to evaluate: $\alpha_1\alpha_2 \cdots \alpha_r = 1(\alpha_2\alpha'_2)(\alpha_3\alpha'_3) \cdots (\alpha_{r-1})(\alpha'_{r-1})(-1) \equiv -1 \pmod \pi$, which proves the theorem.

Appendix A

1. **a.** $a(b + c) = (b + c)a = ba + ca = ab + ac$ **b.** $(a + b)^2 = (a + b)(a + b) = a(a + b) + b(a + b) = a^2 + ab + ba + b^2 = a^2 + 2ab + b^2$ **c.** $a + (b + c) = a + (c + b) = (a + c) + b = (c + a) + b$ **d.** $(b - a) + (c - b) + (a - c) = (-a + b) + (-b + c) + (-c + a) = -a + (b - b) + (c - c) + a$

3. By the definition of the inverse of an element, $0 + (-0) = 0$. But because 0 is an identity element, we have $0 + (-0) = -0$. It follows that $-0 = 0$.

5. Let x be a positive integer. Because $x = x - 0$ is positive, $x > 0$. Now let $x > 0$. Then $x - 0 = x$ is positive.

7. We have $a - c = a + (-b + b) - c = (a - b) + (b - c)$, which is positive from our hypothesis and the closure of the positive integers.

9. Suppose that there are positive integers less than 1. By the well-ordering property, there is a least such integer, say, a. Because $a < 1$ and $a > 0$, Example A.2 shows that $a^2 = aa < 1a = a$. Because $a^2 > 0$, it follows that a^2 is a positive integer less than a, which is a contradiction.

Appendix B

1. **a.** We have $\binom{100}{0} = 100!/(0!100!) = 1$. **b.** We have $\binom{50}{1} = 50!/(1!49!) = 50$. **c.** We have $\binom{20}{3} = 20!/(3!17!) = 1140$. **d.** We have $\binom{11}{5} = 11!/(5!6!) = 462$. **e.** We have $\binom{10}{7} = 10!/(7!3!) = 120$. **f.** We have $\binom{70}{70} = 70!/(70!0!) = 1$.

3. **a.** $a^5 + 5a^4b + 10a^3b^2 + 10a^2b^3 + 5ab^4 + b^5$ **b.** $x^{10} + 10x^9y + 45x^8y^2 + 120x^7y^3 + 210x^6y^4 + 252x^5y^5 + 210x^4y^6 + 120x^3y^7 + 45x^2y^8 + 10xy^9 + y^{10}$ **c.** $m^7 - 7m^6n + 21m^5n^2 - 35m^4n^3 + 35m^3n^4 - 21m^2n^5 + 7mn^6 - n^7$ **d.** $16a^4 + 96a^3b + 216a^2b^2 + 216ab^3 + 81b^4$ **e.** $243x^5 - 1620x^4y + 4320x^3y^2 - 5760x^2y^3 + 3840xy^4 - 1024y^5$ **f.** $390625x^8 + 4375000x^7 + 21437500x^6 + 60025000x^5 + 105043750x^4 + 117649000x^3 + 82354300x^2 + 32941720x + 5764801$

5. On the one hand, $(1 + (-1))^n = 0^n = 0$. On the other hand, by the binomial theorem, $\sum_{k=0}^{n}(-1)^k\binom{n}{k} = (1 + (-1))^n$.

7. $\binom{n}{r}\binom{r}{k} = n!/(r!(n-r)!) \cdot r!/(k!(r-k)!) = n!(n-k)!/(k!(n-k)!(n-r)!(n-k-n+r)!) = \binom{n}{k}\binom{n-k}{n-r}$

9. We fix r and proceed by induction on n. It is easy to check the cases when $n = r$ and $n = r + 1$. Suppose the identity holds for all values from r to $n - 1$. Then consider the sum $\binom{r}{r} + \binom{r+1}{r} + \cdots + \binom{n}{r} = \binom{r-1}{r-1} + \left(\binom{r}{r} + \binom{r}{r-1}\right) + \left(\binom{r+1}{r} + \binom{r+1}{r-1}\right) + \cdots + \left(\binom{n-1}{r} + \binom{n-1}{r-1}\right)$, where we have used $\binom{r}{r} = \binom{r-1}{r-1}$ and Pascal's identity. Regrouping this sum gives us $\left(\binom{r-1}{r-1} + \binom{r}{r-1} + \cdots + \binom{n-1}{r-1}\right) + \left(\binom{r}{r} + \binom{r+1}{r} + \cdots + \binom{n-1}{r}\right)$. By our induction hypothesis, these two sums are equal to $\binom{n}{r+1} + \binom{n+1}{r+1} = \binom{n+1}{r+1}$, which concludes the induction step.

11. Using Exercise 10, $\binom{x}{n} + \binom{x}{n+1} = x!/(n!(x-n)!) + x!/((n+1)!(x-n-1)!) = (x!(n+1))/((n+1)!(x-n)!) + (x!(x-n))/((n+1)!(x-n)!) = (x!(x-n+n+1))/((n+1)!(x-n)!) = (x+1)!/((n+1)!(x-n)!) = \binom{x+1}{n+1}$.

13. Let S be a set of n copies of $x + y$. Consider the coefficient of x^ky^{n-k} in the expansion of $(x + y)^n$. Choosing the x from each element of a k-element subset of S, we notice that the coefficient of x^ky^{n-k} is the number of k-element subsets of S, $\binom{n}{k}$.

15. By counting elements with exactly 0, 1, 2, and 3 properties, we see that only elements with 0 properties are counted in $n - [n(P_1) + n(P_2) + n(P_3)] + [n(P_1, P_2) + n(P_1, P_3) + n(P_2, P_3)] - [n(P_1, P_2, P_3)]$, and those only once.

17. A term of the sum is of the form $ax_1^{k_1}x_2^{k_2}\cdots x_m^{k_m}$ where $k_1 + k_2 + \cdots + k_m = n$ and $a = \frac{n!}{k_1!k_2!\cdots k_m!}$.

19. 56133000000

Bibliography

Printed resources in this bibliography include comprehensive books on number theory, as well as books and articles covering particular topics or applications. In particular, some of these references focus on factorization and primality testing, the history of number theory, or cryptography.

To learn more about number theory, you may want to consult other number theory textooks such as [AdGo76], [An94], [Ar70], [Ba69], [Be66], [Bo07], [BoSh66], [Bu10], [Da99], [Di05], [Du08], [ErSu03], [Fl89], [Gi70], [Go98], [Gr82], [Gu80], [HaWr08], [Hu82], [IrRo95], [Ki74], [La58], [Le90], [Le96], [Le02], [Lo95], [Ma–], [Na81], [NiZuMo91], [Or67], [Or88], [PeBy70], [Ra77], [Re96a], [Ro77], [Sh85], [Sh83], [Sh67], [Si87], [Si64], [Si70], [St78], [St64], [UsHe39], [Va01], [Vi54], and [Wr39].

Additional information on number theory, including the latest discoveries, can be found on Web sites. Appendix D lists some top number theory and cryptography Web sites. A comprehensive set of links to relevant Web sites can be found on the Web site for this book www.pearsonhighered.com/rosen.

[AdGo76] W.W. Adams and L.J. Goldstein, *Introduction to Number Theory,* Prentice Hall, Englewood Cliffs, New Jersey, 1976.

[Ad79] L.M. Adleman, "A subexponential algorithm for the discrete logarithm problem with applications to cryptography," *Proceedings of the 20th Annual Symposium on the Foundations of Computer Science*, 1979, 55–60.

[AdPoRu83] L.M. Adleman, C. Pomerance, and R.S. Rumely, "On distinguishing prime numbers from composite numbers," *Annals of Mathematics*, Volume 117 (1983).

[AgKaSa02] M.A. Agrawal, N. Kayal, N. Saxena, "PRIMES is in P," Department of Computer Science & Engineering, Indian Institute of Technology, Kanpur, India, August 6, 2002.

[AiZi10] M. Aigner and G.M. Ziegler, *Proofs from THE BOOK*, 4th ed., Springer-Verlag, Berlin, 2010.

[AlWi03] S. Alaca and K. Williams, *Introductory Algebraic Number Theory*, Cambridge University Press, 2003.

[AlGrPo94] W.R. Alford, A. Granville, and C. Pomerance, "There are infinitely many Carmichael Numbers," *Annals of Mathematics*, Volume 140 (1994), 703–722.

[An98] G.E. Andrews, *The Theory of Partitions*, Cambridge University Press, Cambridge, UK, 1976

[An94] G.E. Andrews, *Number Theory*, Dover, New York, 1994.

[AnEr04] G.E. Andrews and K. Ericksson, *Integer Partitions*, Cambridge University Press, Cambridge, U.K., 2004.

[Ap76] T.A. Apostol, *Introduction to Analytic Number Theory*, Springer-Verlag, New York, 1976.

[Ar70] R.G. Archibald, *An Introduction to the Theory of Numbers*, Merrill, Columbus, Ohio, 1970.

[BaSh96] E. Bach and J. Shallit, *Algorithmic Number Theory*, MIT Press, Cambridge, Massachusetts, 1996.

[Ba94] P. Bachmann, *Die Analytische Zahlentheorie*, Teubner, Leipzig, Germany, 1894.

[Ba03] E.J. Barbeau, *Pell's Equation*, Springer-Verlag, New York, 2003.

[Ba69] I.A. Barnett, *Elements of Number Theory*, Prindle, Weber, and Schmidt, Boston, 1969.

[Be66] A.H. Beiler, *Recreations in the Theory of Numbers*, 2nd ed., Dover, New York, 1966.

[BePi82] H. Beker and F. Piper, *Cipher Systems*, Wiley, New York, 1982.

[Be65] E.T. Bell, *Men of Mathematics*, Simon & Schuster, New York, 1965.

[Bl82] M. Blum, "Coin-flipping by telephone—a protocol for solving impossible problems," *IEEE Proceedings, Spring Compcon 82,* 133–137.

[Bo07] E.D. Bolker, *Elementary Number Theory*, Dover, New York, 2007.

[Bo99] D. Boneh, "Twenty years of attacks on the RSA cryptosystem," *American Mathematical Society Notices*, Volumn 46 (1999), 203–213.

[Bo82] B. Bosworth, *Codes, Ciphers, and Computers*, Hayden, Rochelle Park, New Jersey, 1982.

[Bo91] C.B. Boyer, *A History of Mathematics*, 2nd ed., Wiley, New York, 1991.

[BoSh66] Z.I. Borevich and I.R. Shafarevich, *Number Theory*, Academic Press, New York, 1966.

[Br91] R.P. Brent, "Improved techniques for lower bounds for odd perfect numbers," *Mathematics of Computation*, Volume 57 (1991), 857–868.

[Br00] R.P. Brent, "Recent progress and prospects for integer factorization algorithms," *Proc. COCOON* 2000, LNCS 1858, pages 3–22, Springer-Verlag, 2000.

[BrCote93] R.P. Brent, G.L. Cohen, and H.J.J. te Riele, "Improved techniques for lower bounds for odd perfect numbers," *Mathematics of Computation*, Volume 61 (1993), 857–868.

[Br89] D.M. Bressoud, *Factorization and Primality Testing*, Springer-Verlag, New York, 1989.

[BrWa00] D. Bressoud and S. Wagon, *A Course in Computational Number Theory*, Key College Publishing, Emeryville, California, 2000.

[Br81] J. Brillhart, "Fermat's factoring method and its variants," *Congressus Numerantium*, Volume 32 (1981), 29–48.

[Br88] J. Brillhart, D.H. Lehmer, J.L. Selfridge, B. Tuckerman, S.S. Wagstaff, Jr., *Factorizations of* $b^n \pm 1$, $b = 2, 3, 5, 6, 7, 10, 11, 12$ *up to high powers*, revised ed., American Mathematical Society, Providence, Rhode Island, 1988.

[Bu10] D.M. Burton, *Elementary Number Theory*, 7th ed., McGraw-Hill, New York, 2010.

[Bu02] D.M. Burton, *The History of Mathematics*, 5th ed., McGraw-Hill, New York, 2002.

[Ca59] R.D. Carmichael, *The Theory of Numbers and Diophantine Analysis*, Dover, New York, 1959 (reprint of the original 1914 and 1915 editions).

[Ch06] J. Chahal, "Congruent numbers and elliptic curve," *American Mathematical Monthly*, Volume 113 (2006), 308–317.

[Ch83] D. Chaum, ed., *Advances in Cryptology—Proceedings of Crypto 83*, Plenum, New York, 1984.

[ChRiSh83] D. Chaum, R.L. Rivest, A.T. Sherman, eds., *Advances in Cryptology—Proceedings of Crypto 82*, Plenum, New York, 1983.

[Ch98] V. Chandrashekar, "The congruent number problem," *Resonance*, Volume 8 (1998), 33–45.

[Ci88] B. Cipra, "PCs factor a 'most wanted' number," *Science*, Volume 242 (1988), 1634–1635.

[Ci90] B. Cipra, "Big number breakdown," *Science*, Volume 248 (1990), 1608.

[Co87] G.L. Cohen, "On the largest component of an odd perfect number," *Journal of the Australian Mathematical Society, (A)*, Volume 42 (1987), 280–286.

[CoWe91] W.N. Colquitt and L. Welsh, Jr., "A new Mersenne prime," *Mathematics of Computation*, Volume 56 (1991), 867–870.

[Co08] K. Conrad, "The congruent number problem," *Harvard College Mathematics Review*, Volume 2 (2008), No. 2, 58–74.

[CoGu96] R.H. Conway and R.K. Guy, *The Book of Numbers*, Copernicus Books, New York, 1996.

[Co97] D. Coppersmith, "Small solutions to polynomial equations, and low exponent RSA vulnerabilities," *Journals of Cryptology*, Volume 10 (1997), 233–260.

[CoLeRiSt10] T.H. Cormen, C.E. Leierson, R.L. Rivest, C. Stein, *Introduction to Algorithms*, 3rd ed., MIT Press, Cambridge, Massachusetts, 2010.

[CoSiSt97] G. Cornell, J.H. Silverman, and G. Stevens, *Modular Forms and Fermat's Last Theorem,* Springer-Verlag, New York, 1997.

[Cr94] R.E. Crandall, *Projects in Scientific Computation*, Springer-Verlag, New York, 1994.

[CrPo05] R. Crandall and C. Pomerance, *Prime Numbers, A Computational Perspective*, 2nd ed., Springer-Verlag, New York, 2005.

[Cs07] G.P. Csicery (director), *N Is a Number: Portrait of Paul Erdős* (DVD), Facets, Chicago, 2007.

[Da99] H. Davenport, *The Higher Arithmetic*, 7th ed., Cambridge University Press, Cambridge, England, 1999.

[De82] D.E.R. Denning, *Cryptography and Data Security*, Addison-Wesley, Reading, Massachusetts, 1982.

[De03] J. Derbyshire, *Prime Obsession*, Joseph Henry Press, Washington, D.C., 2003.

[Di57] L.E. Dickson, *Introduction to the Theory of Numbers*, Dover, New York, 1957 (reprint of the original 1929 edition).

[Di05] L.E. Dickson, *History of the Theory of Numbers*, three volumes, Dover, New York, 2005 (reprint of the 1919 original).

[Di70] *Dictionary of Scientific Biography*, Scribners, New York, 1970.

[DiHe76] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, Volume 22 (1976), 644–655.

[Di84] J.D. Dixon, “Factorization and primality tests,” *American Mathematical Monthly*, Volume 91 (1984), 333–353.

[Du08] U. Dudley, *Elementary Number Theory*, 2nd ed., Dover, New York, 2008.

[Ed96] H.M. Edwards, *Fermat’s Last Theorem*, 5th ed., Springer-Verlag, New York, 1996.

[Ed01] H.M. Edwards, *Riemann’s Zeta Function*, Dover, New York, 2001.

[ErSu03] P. Erdős and J. Surányi, *Topics in the History of Numbers*, Springer-Verlag, New York, 2003.

[Ev92] H. Eves, *An Introduction to the History of Mathematics*, 6th ed., Elsevier, New York, 1992.

[Ew83] J. Ewing, “$2^{86243} - 1$ is prime,” *The Mathematical Intelligencer*, Volume 5 (1983), 60.

[Fl89] D. Flath, *Introduction to Number Theory*, Wiley, New York, 1989.

[Fl83] D.R. Floyd, “Annotated bibliographical in conventional and public key cryptography,” *Cryptologia*, Volume 7 (1983), 12–24.

[Fr56] J.E. Freund, “Round robin mathematics,” *American Mathematical Monthly*, Volume 63 (1956), 112–114.

[Fr78] W.F. Friedman, *Elements of Cryptanalysis*, Aegean Park Press, Laguna Hills, California, 1978.

[Ga91] J. Gallian, “The mathematics of identification numbers,” *College Mathematics Journal*, Volume 22 (1991), 194–202.

[Ga92] J. Gallian, “Assigning drivers license numbers,” *Mathematics Magazine*, Volume 64 (1992), 13–22.

[Ga96] J. Gallian, “Error detection methods,” *ACM Computing Surveys*, Volume 28 (1996), 504–517.

[GaWi88] J. Gallian and S. Winters, “Modular arithmetic in the marketplace,” *American Mathematical Monthly*, Volume 95 (1988), 584–551.

[Ga86] C.F. Gauss, *Disquisitiones Arithmeticae*, revised English translation by W.C. Waterhouse, Springer-Verlag, New York, 1986.

[Ge63] M. Gerstenhaber, “The 152nd proof of the law of quadratic reciprocity,” *American Mathematical Monthly*, Volume 70 (1963), 397–398.

[Ge82] A. Gersho, ed., *Advances in Cryptography*, Department of Electrical and Computer Engineering, University of California, Santa Barbara, 1982.

[GeWaWi98] E. Gethner, S. Wagon, and B. Wick, “A stroll through the Gaussian primes,” *American Mathematical Monthly*, Volume 104 (1998), 216–225.

[Gi70] A.A. Gioia, *The Theory of Numbers*, Markham, Chicago, 1970.

[Go98] J.R. Goldman, *The Queen of Mathematics: An Historically Motivated Guide to Number Theory*, A.K. Peters, Wellesley, Massachusetts, 1998.

[Go80] J. Gordon, “Use of intractable problems in cryptography,” *Information Privacy*, Volume 2 (1980), 178–184.

[GoOh08] T. Goto and Y. Ohno, ”Odd perfect numbers have a prime factor exceeding 10^8,” *Mathematics of Computation*, Volume 77 (2008), 1859-1868.

[Gr04] A. Granville, “It is easy to determine whether a given integer is prime,” *Current Events in Mathematics*, American Mathematical Society, 2004.

[GrTu02] A. Granville and T.J. Tucker, “It’s as easy as abc,” *Notices of the American Mathematical Society*, Volume 49 (2002), 1224–1231.

[Gr82] E. Grosswald, *Topics from the Theory of Numbers*, 2nd ed., Birkhauser, Boston, 1982.

[GrKnPa94] R.L. Graham, D.E. Knuth, and O. Patashnik, *Concrete Mathematics*, 2nd ed., Addison-Wesley, Reading, Massachusetts, 1994.

[Gu80] H. Gupta, *Selected Topics in Number Theory*, Abacus Press, Kent, England, 1980.

[Gu75] R.K. Guy, "How to factor a number," *Proceedings of the Fifth Manitoba Conference on Numerical Mathematics*, Utilitas, Winnepeg, Manitoba, 1975, 49–89.

[Gu94] R.K. Guy, *Unsolved Problems in Number Theory*, 2nd ed., Springer-Verlag, New York, 1994.

[Ha83] P. Hagis, Jr., "Sketch of a proof that an odd perfect number relatively prime to 3 has at least eleven prime factors," *Mathematics of Computations*, Volume 46 (1983), 399–404.

[HaWr08] G.H. Hardy and E.M. Wright, *An Introduction to the Theory of Numbers*, 6th ed., Oxford University Press, Oxford, 2008.

[He80] A.K. Head, "Multiplication modulo n," *BIT*, Volume 20 (1980), 115–116.

[He79] M.E. Hellman, "The mathematics of public-key cryptography," *Scientific American*, Volume 241 (1979) 146–157.

[Hi31] L.S. Hill, "Concerning certain linear transformation apparatus of cryptography," *American Mathematical Monthly*, Volume 38 (1931), 135–154.

[Ho99] P. Hoffman, *The Man who Loved Only Numbers*, Hyperion, New York, 1999.

[Hu82] L. Hua, *Introduction to Number Theory*, Springer-Verlag, New York, 1982.

[Hw79] K. Hwang, *Computer Arithmetic: Principles, Architecture and Design*, Wiley, New York, 1979.

[IrRo95] K.F. Ireland and M.I. Rosen, *A Classical Introduction to Modern Number Theory*, 2nd ed., Springer-Verlag, New York, 1995.

[Ka96] D. Kahn, *The Codebreakers, the Story of Secret Writing*, 2nd ed., Scribners, New York, 1996.

[Ka98] V. Katz, *A History of Mathematics: An Introduction*, 2nd ed., Addison-Wesley, Boston, 1998.

[Ki04] S.V. Kim, "An elementary proof of the quadratic reciprocity law," *American Mathematical Monthly*, Volume 111, Number 1 (2004), 45–50.

[Ki74] A.M. Kirch, *Elementary Number Theory: A Computer Approach*, Intext, New York, 1974.

[Ki01] J. Kirtland, *Identification Numbers and Check Digit Schemes*, Mathematical Association of America, Washington, D.C., 2001.

[Kl72] M. Kline, *Mathematical Thought from Ancient to Modern Times*, Oxford University, New York, 1972.

[Kn97] D.E. Knuth, *Art of Computer Programming: Semi-Numerical Algorithms*, Volume 2, 3rd ed., Addison-Wesley, Reading, Massachusetts, 1997.

[Kn97a] D.E. Knuth, *Art of Computer Programming: Sorting and Searching*, Volume 3, 2nd ed., Addison-Wesley, Reading, Massachusetts, 1997.

[Ko96] N. Koblitz, *Introduction to Elliptic Curves and Modular Forms*, 2nd ed., Springer-Verlag, New York, 1996.

[Ko94] N. Koblitz, *A Course in Number Theory and Cryptography*, 2nd ed., Springer-Verlag, New York, 1994.

[Ko96a] P. Kocher, “Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems,” *Advances in Cryptology—CRYPTO ’96*, LNCS 1109, Springer-Verlag, New York, 1996, 104–113.

[Ko83] G. Kolata, “Factoring gets easier,” *Science*, Volume 222 (1983), 999–1001.

[Ko81] A.G. Konheim, *Cryptography: A Primer*, Wiley, New York, 1981.

[Kr86] E. Kranakis, *Primality and Cryptography*, Wiley-Teubner, Stuttgart, Germany, 1986.

[Kr79] L.Kronsjo, *Algorithms: Their Complexity and Efficiency*, Wiley, New York, 1979.

[Ku76] S. Kullback, *Statistical Methods in Cryptanalysis*, Aegean Park Press, Laguna Hills, California, 1976.

[La90] J.C. Lagarias, “Pseudo-random number generators in cryptography and number theory,” pages 115–143 in *Cryptology and Computational Number Theory*, Volume 42 of Proceedings of Symposia in Advanced Mathematics, American Mathematical Society, Providence, Rhode Island, 1990.

[LaOd82] J.C. Lagarias and A.M. Odlyzko, “New algorithms for computing $\pi(x)$,” Bell Laboratories Technical Memorandum TM-82-11218-57.

[La58] E. Landau, *Elementary Number Theory*, Chelsea, New York, 1958.

[La60] E. Landau, *Foundations of Analysis*, 2nd ed., Chelsea, New York, 1960.

[La35] H.P. Lawther, Jr., “An application of number theory to the splicing of telephone cables,” *American Mathematical Monthly*, Volume 42 (1935), 81–91.

[LePo31] D.H. Lehmer and R.E. Powers, “On factoring large numbers,” *Bulletin of the American Mathematical Society*, Volume 37 (1931), 770–776.

[Le00] F. Lemmermeyer, *Reciprocity Laws I,* Springer-Verlag, Berlin, 2000.

[Le79] A. Lempel, “Cryptology in transition,” *Computing Surveys*, Volume 11 (1979), 285–303.

[Le80] H.W. Lenstra, Jr., “Primality testing,” *Studieweek Getaltheorie en Computers*, 1–5 September 1980, Stichting Mathematisch Centrum, Amsterdam, Holland.

[Le90] W.J. LeVeque, *Elementary Theory of Numbers*, Dover, New York, 1990.

[Le96] W.J. LeVeque, *Fundamentals of Number Theory*, Dover, New York, 1996.

[Le02] W.J. LeVeque, *Topics in Number Theory*, Dover, New York, 2002.

[Le74] W.J. LeVeque, editor, *Reviews in Number Theory* [1940–1972], and R.K. Guy, editor, *Reviews in Number Theory* [1973–1983], six volumes each, American Mathematical Society, Washington, D.C., 1974 and 1984, respectively.

[LiDu87] Y. Li and S. Du, *Chinese Mathematics: A Concise History*, translated by J. Crossley and A. Lun, Clarendon Press, Oxford, England, 1987.

[Li73] U. Libbrecht, *Chinese Mathematics in the Thirteenth Century, The Shu-shu chiu-chang of Ch’in Chiu-shao*, MIT Press, 1973.

[Li79] R.J. Lipton, “How to cheat at mental poker,” and “An improved power encryption method,” unpublished reports, Department of Computer Science, University of California, Berkeley, 1979.

[Lo95] C.T. Long, *Elementary Introduction to Number Theory*, 3rd ed., Waveland Press, Prospect Heights, Illinois, 1995.

[Lo90] J.H. Loxton, editor, *Number Theory and Cryptography*, Cambridge University Press, Cambridge, England, 1990.

[Ma79] D.G. Malm, *A Computer Laboratory Manual for Number Theory*, COMPress, Wentworth, New Hampshire, 1979.

[McRa79] J.H. McClellan and C.M. Rader, *Number Theory in Digital Signal Processing*, Prentice Hall, Englewood Cliffs, New Jersey, 1979.

[Ma–] G.B. Matthews, *Theory of Numbers*, Chelsea, New York (no publication date provided).

[Ma94] U. Maurer, "Towards the equivalence of breaking the Diffie-Hellman protocol and computing discrete logarithms," *Advances in Cryptology—CRYPTO '94*, LNCS 839, 1994, 271–281.

[Ma95] U. Maurer, "Fast generation of prime numbers and secure public-key cryptographic parameters," *Journal of Cryptology*, Volume 8 (1995), 123–155.

[Ma00] B. Mazur, "Questions about powers of numbers," *Notices of the American Mathematical Society,* Volume 47 (2000), 195–202.

[MevaVa97] A.J. Menezes, P.C. van Oorschot, S.A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, Boca Raton, Florida, 1997.

[Me82] R.C. Merkle, *Secrecy, Authentication, and Public Key Systems*, UMI Research Press, Ann Arbor, Michigan, 1982.

[MeHe78] R.C. Merkle and M.E. Hellman, "Hiding information and signatures in trapdoor knapsacks," *IEEE Transactions in Information Theory*, Volume 24 (1978), 525–530.

[MeMa82] C.H. Meyer and S.M. Matyas, *Cryptography: A New Dimension in Computer Data Security*, Wiley, New York, 1982.

[Mi76] G.L. Miller, "Riemann's hypothesis and tests for primality," *Journal of Computer and Systems Science*, Volume 13 (1976), 300–317.

[Mi47] W.H. Mills, "A prime-representing function," *Bulletin of the American Mathematical Society*, Volume 53 (1947), 604.

[Mo96] R.A. Mollin, *Quadratics*, CRC Press, Boca Raton, Florida, 1996.

[Mo99] R.A. Mollin, *Algebraic Number Theory*, CRC Press, Boca Raton, Florida, 1999.

[Mo96] M.B. Monagan, K.O. Geddes, K.M. Heal, G. Labahn, and S.M. Vorkoetter, *Maple V Programming Guide*, Springer-Verlag, New York, 1996.

[Mo80] L. Monier, "Evaluation and comparison of two efficient probabilistic primality testing algorithms," *Theoretical Computer Science*, Volume 11 (1980), 97–108.

[Mo69] L.J. Mordell, *Diophantine Equations*, Academic Press, New York, 1969.

[MoBr75] M.A. Morrison and J. Brillhart, "A method of factoring and the factorization of F7," *Mathematics of Computation*, Volume 29 (1985), 183–205.

[Na81] T. Nagell, *Introduction to Number Theory*, Chelsea, New York, 1981.

[Ne69] O.E. Neugebauer, *The Exact Sciences in Antiquity*, Dover, New York, 1969.

[NeSc99] J. Neukirch and N. Schappacher, *Algebraic Number Theory*, Springer-Verlag, New York, 1999.

[NiZuMo91] I. Niven, H.S. Zuckerman, and H.L. Montgomery, *An Introduction to the Theory of Numbers*, 5th ed., Wiley, New York, 1991.

[Odte85] A.M. Odlyzko and H.J.J. te Riele, "Disproof of the Mertens conjecture," *Journal für die reine und angewandte Mathematik*, Volume 357 (1985), 138–160.

[Od90] A.M. Odlyzko, "The rise and fall of knapsack cryptosystems," pages 75–88 in *Cryptology and Computational Number Theory*, Volume 42 of Proceedings of

Symposia in Applied Mathematics, American Mathematical Society, Providence, Rhode Island, 1990.

[Od95] A.M. Odlyzko, "The future of integer factorization," *RSA CrytoBytes*, Volume 2, Number 1, 1995, 5–12.

[Or67] O. Ore, *An Invitation to Number Theory*, Random House, New York, 1967.

[Or88] O. Ore, *Number Theory and its History*, Dover, New York, 1988.

[PaMi88] S.K. Park and K.W. Miller, "Random number generators: Good ones are hard to find," *Communications of the ACM*, Volume 31 (1988), 1192–1201.

[PeBy70] A.J. Pettofrezzo and D.R. Byrkit, *Elements of Number Theory*, Prentice Hall, Englewood Cliffs, New Jersey, 1970.

[Pf89] C.P. Pfleeger, *Security in Computing*, Prentice Hall, Englewood Cliffs, New Jersey, 1989.

[Po14] H.C. Pocklington, "The determination of the prime or composite nature of large numbers by Fermat's theorem," *Proceedings of the Cambridge Philosophical Society*, Volume 18 (1914/6), 29–30.

[PoHe78] S. Pohlig and M. Hellman, "An improved algorithm for computing logarithms over GF(p) and its cryptographic significance," *IEEE Transactions on Information Theory*, Volume 24 (1978), 106–110.

[Po99] H. Pollard and H. Diamond, *The Theory of Algebraic Numbers*, 3rd ed., Dover, New York, 1999.

[Po74] J.M. Pollard, "Theorems on factorization and primality testing," *Proceedings of the Cambridge Philosophical Society,* Volume 76 (1974), 521–528.

[Po75] J.M. Pollard, "A Monte Carlo method for factorization," *Nordisk Tidskrift for Informationsbehandling (BIT)*, Volume 15 (1975), 331–334.

[Po81] C. Pomerance, "Recent developments in primality testing," *The Mathematical Intelligencer*, Volume 3 (1981), 97–105.

[Po82] C. Pomerance, "The search for prime numbers," *Scientific American*, Volume 247 (1982), 136–147.

[Po84] C. Pomerance, *Lecture Notes on Primality Testing and Factoring*, Mathematical Association of America, Washington, D.C., 1984.

[Po90] C. Pomerance, ed., *Cryptology and Computational Number Theory*, American Mathematical Society, Providence, Rhode Island, 1990.

[Po93] C. Pomerance, "Carmichael numbers," *Nieuw Arch. v. Wiskunde*, Volume 4, number 11 (1993), 199–209.

[Ra79] M.O. Rabin, "Digitalized signatures and public-key functions as intractable as factorization," M.I.T. Laboratory for Computer Science Technical Report LCS/TR-212, Cambridge, Massachusetts, 1979.

[Ra80] M.O. Rabin, "Probabilistic algorithms for testing primality," *Journal of Number Theory*, Volume 12 (1980), 128–138.

[Ra77] H. Rademacher, *Lectures on Elementary Number Theory*, Krieger, 1977.

[Re96] D. Redfern, *The Maple Handbook*, Springer-Verlag, New York, 1996.

[Re96a] D. Redmond, *Number Theory: An Introduction*, Marcel Dekker, Inc., New York, 1996

[Ri79] P. Ribenboim, *13 Lectures on Fermat's Last Theorem*, Springer-Verlag, New York, 1979.

[Ri96] P. Ribenboim, *The New Book of Prime Number Record*, Springer-Verlag, New York, 1996.

[Ri01] P. Ribenboim, *Classical Theory of Algebraic Integers*, 2nd ed., Springer-Verlag, New York, 2001.

[Ri71] F. Richman, *Number Theory, An Introduction to Algebra*, Brooks/Cole, Belmont, California, 1971.

[Ri59] B. Riemann, "Uber die Anzahl der Primzahlen unter einer gegeben Grösse," *Monatsberichte der Berliner Akademie,* November, 1859.

[Ri85] H. Riesel, "Modern factorization methods," *BIT* (1985), 205–222.

[Ri94] H. Riesel, *Prime Numbers and Computer Methods for Factorization*, 2nd ed., Birkhauser, Boston, 1994.

[Ri78] R.L. Rivest, "Remarks on a proposed cryptanalytic attack on the M.I.T. public-key cryptosystem," *Cryptologia*, Volume 2 (1978), 62–65.

[RiShAd78] R.L. Rivest, A. Shamir, and L.M. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, Volume 21 (1978), 120–126.

[RiShAd83] R.L. Rivest, A. Shamir, and L.M. Adleman, "Cryptographic communications system and method," United States Patent #4,405,8239, issued September 20, 1983.

[Ro77] J. Roberts, *Elementary Number Theory*, MIT Press, Cambridge, Massachusetts, 1977.

[Ro97] K. Rosen et. al., *Exploring Discrete Mathematics with Maple,* McGraw-Hill, New York, 1997.

[Ro99a] K.H. Rosen, *Handbook of Discrete and Combinatorial Mathematics*, CRC Press, Boca Raton, Florida, 1999.

[Ro07] K.H. Rosen, *Discrete Mathematics and its Applications*, 6th ed., McGraw-Hill, New York, 2007.

[Ru64] W. Rudin, *Principles of Mathematical Analysis*, 2nd ed., McGraw-Hill, New York, 1964.

[Ru83] R. Rumely, "Recent advances in primality testing," *Notices of the American Mathematical Society*, Volume 30 (1983), 475–477.

[Sa03a] K. Sabbagh, *The Riemann Hypothesis*, Farrar, Strauss, and Giroux, New York, 2003.

[SaSa07] J. Sally and P.J. Sally, Jr., *Roots to Research*, AMS, Providence, Rhode Island, 2007.

[Sa90] A. Salomaa, *Public-Key Cryptography*, Springer-Verlag, New York, 1990.

[Sa03b] M. du Sautoy, *The Music of the Primes*, Harper Collins, New York, 2003.

[ScOp85] W. Scharlau and H. Opolka, *From Fermat to Minkowski, Lectures on the Theory of Numbers and its Historical Development*, Springer-Verlag, New York, 1985.

[Sc98] B. Schechter, *My Brain is Open*, Simon and Schuster, New York, 1998.

[Sc86] M.R. Schroeder, *Number Theory in Science and Communication*, 2nd ed., Springer-Verlag, Berlin, 1986.

[SePi89] J. Seberry and J. Pieprzyk, *Cryptography: An Introduction to Computer Security*, Prentice Hall, New York, 1989.

[Sh79] A. Shamir, "How to share a secret," *Communications of the ACM*, Volume 22 (1979), 612–613.

[Sh83] A. Shamir, "A polynomial time algorithm for breaking the basic Merkle-Hellman cryptosystem," in *Advances in Cryptology—Proceedings of Crypto 82*, 279–288.

[Sh84] A. Shamir, "A polynomial time algorithm for breaking the basic Merkle-Hellman cryptosystem," *IEEE Transactions on Information Theory*, Volume 30 (1984), 699–704. (This is an improved version of [Sh83].)

[ShRiAd81] A. Shamir, R.L. Rivest, and L.M. Adleman, "Mental poker," *The Mathematical Gardner*, ed. D.A. Klarner, Wadsworth International, Belmont, California, 1981, 37–43.

[Sh85] D. Shanks, *Solved and Unsolved Problems in Number Theory*, 3rd ed., Chelsea, New York, 1985.

[Sh83] H.S. Shapiro, *Introduction to the Theory of Numbers*, Wiley, New York, 1983.

[Sh67] J.E. Shockley, *Introduction to Number Theory*, Holt, Rinehart, and Winston, New York, 1967.

[Si64] W. Sierpinski, *A Selection of Problems in the Theory of Numbers*, Pergamon Press, New York, 1964.

[Si70] W. Sierpinski, *250 Problems in Elementary Number Theory*, Polish Scientific Publishers, Warsaw, 1970.

[Si87] W. Sierpinski, *Elementary Theory of Numbers*, 2nd ed., North-Holland, Amsterdam, 1987.

[Si82] G.J. Simmons, ed., *Secure Communications and Asymmetric Cryptosystems*, AAAS Selected Symposium Series Volume 69, Westview Press, Boulder, Colorado, 1982.

[Si97] S. Singh, *Fermat's Enigma: The Epic Quest to Solve the World's Greatest Mathematical Problem,* Walker and Company, New York, 1997.

[Si66] A. Sinkov, *Elementary Cryptanalysis*, Mathematical Association of America, Washington, D.C., 1966.

[SlPl95] N.J.A. Sloane and S. Plouffe, *The Encyclopedia of Integer Sequences*, Academic Press, New York, 1995.

[Sl78] D. Slowinski, "Searching for the 27th Mersenne prime," *Journal of Recreational Mathematics*, Volume 11 (1978/9), 258–261.

[SoSt77] R. Solovay and V. Strassen, "A fast Monte Carlo test for primality," *SIAM Journal for Computing*, Volume 6 (1977), 84–85 and erratum, Volume 7 (1978), 118.

[So86] M.A. Soderstrand et al., editors, *Residue Number System Arithmetic: Modern Applications in Digital Signal Processing*, IEEE Press, New York, 1986.

[Sp82] D.D. Spencer, *Computers in Number Theory*, Computer Science Press, Rockville, Maryland, 1982.

[St78] H.M. Stark, *An Introduction to Number Theory*, Markham, Chicago, 1970; reprint MIT Press, Cambridge, Massachusetts, 1978.

[St64] B.M. Stewart, *The Theory of Numbers*, 2nd ed., Macmillan, New York, 1964.

[St05] D.R. Stinson, *Cryptography, Theory and Practice*, 3rd ed., Chapman & Hall/CRC, Boca Raton, Florida, 2005.

[SzTa67] N.S. Szabo and R.J. Tanaka, *Residue Arithmetic and its Applications to Computer Technology*, McGraw-Hill, 1967.

[TrWa02] W. Trappe and L. Washington, *Introduction to Cryptography with Coding Theory*, Prentice Hall, Upper Saddle River, New Jersey, 2002.

[Tu83] J. Tunnell, "A classical diophantine problem and modular forms of weight 3/2," *Inventiones Mathematicae*, Volume 72 (1983), 323–334.

[UsHe39] J.V. Uspensky and M.A. Heaslet, *Elementary Number Theory*, McGraw-Hill, New York, 1939.

[Va89] S. Vajda, *Fibonacci and Lucas Numbers and the Golden Section: Theory and Applications*, Ellis Horwood, Chichester, England, 1989.

[Va96] A.J. van der Poorten, *Notes on Fermat's Last Theorem,* Wiley, New York, 1996.

[Va01] C. VandenEynden, *Elementary Number Theory*, McGraw-Hill, New York, 2001.

[Vi54] I.M. Vinogradov, *Elements of Number Theory*, Dover, New York, 1954.

[Wa86] S. Wagon, "Primality testing," *The Mathematical Intelligencer*, Volume 8, Number 3 (1986), 58–61.

[Wa99] S. Wagon, *Mathematica in Action,* 2nd ed. Telos, New York, 1999.

[Wa86] S.S. Wagstaff, "Using computers to teach number theory," *SIAM News*, Volume 19 (1986), 14 and 18.

[Wa90] S.S. Wagstaff, "Some uses of microcomputers in number theory research," *Computers and Mathematics with Applications*, Volume 19 (1990), 53–58.

[WaSm87] S.S. Wagstaff and J.W. Smith, "Methods of factoring large integers," in *Number Theory, New York, 1984–1985*, LNM, Volume 1240, Springer-Verlag, Berlin, 1987, 281–303.

[Wa08] L. Washington, *Elliptic Curves: Number Theory and Cryptography,* 2nd ed., Chapman and Hall/CRC, Boca Raton, Florida, 2008.

[We84] A. Weil, *Number Theory: An Approach Through History From Hummurapi to Legendre*, Birkhauser, Boston, 1984.

[Wi90] M.J. Wiener, "Cryptanalysis of short RSA secret exponents," *IEEE Transactions on Information Theory*, Volume 36 (1990), 553–558.

[Wi95] A. Wiles, "Modular elliptic-curves and Fermat's last theorem," *Annals of Mathematics,* Volume 141 (1995), 443–551.

[Wi86] H.C. Williams, ed., *Advances in Cryptology—CRYPTO '85*, Springer-Verlag, Berlin, 1986.

[Wi78] H.C. Williams, "Primality testing on a computer," *Ars Combinatorica*, Volume 5 (1978), 127–185.

[Wi82] H.C. Williams, "The influence of computers in the development of number theory," *Computers and Mathematics with Applications*, Volume 8 (1982), 75–93.

[Wi84] H.C. Williams, "An overview of factoring," in *Advances in Cryptology, Proceedings of Crypto 83*, Plenum, New York, 1984, 87–102.

[Wo03] S. Wolfram, *The Mathematica Book*, 5th ed., Cambridge University Press, New York, 2003.

[Wr39] H.N. Wright, *First Course in Theory of Numbers*, Wiley, New York, 1939.

[Wu85] M.C. Wunderlich, "Implementing the continued fraction algorithm on parallel machines," *Mathematics of Computation*, Volume 44 (1985), 251–260.

[WuKu90] M.C. Wunderlich and J.M. Kubina, "Extending Waring's conjecture to 471,600,000," *Mathematics of Computation*, Volume 55 (1990), 815–820.