whichever is in shorter supply) so that the number of men and the number of women become the same, and put these fictitious people at the bottom of everyone's preference lists. **c)** This follows immediately from Exercise 63 in Section 3.1. **37.** 5; 15 **39.** The first situation in Exercise 37 **41.** **a)** For each subset S of $\{1, 2, \dots, n\}$, compute $\sum_{j \in S} w_j$. Keep track of the subset giving the largest such sum that is less than or equal to W, and return that subset as the output of the algorithm. **b)** The food pack and the portable stove **43.** **a)** The makespan is always at least as large as the load on the processor assigned to do the lengthiest job, which must be at least $\max_{j=1,2,\dots,n} t_j$. Therefore the minimum makespan satisfies this inequality. **b)** The total amount of time the processors need to spend working on the jobs (the total load) is $\sum_{j=1}^{n} t_j$. Therefore the average load per processor is $\frac{1}{p} \sum_{j=1}^{n} t_j$. The maximum load cannot be any smaller than the average, so the minimum makespan is always at least this large. **45.** Processor 1: jobs 1, 4; processor 2: job 2; processor 3: jobs 3, 5

CHAPTER 4

Section 4.1

1. **a)** Yes **b)** No **c)** Yes **d)** No **3.** Suppose that $a \mid b$. Then there exists an integer k such that $ka = b$. Because $a(ck) = bc$ it follows that $a \mid bc$. **5.** If $a \mid b$ and $b \mid a$, there are integers c and d such that $b = ac$ and $a = bd$. Hence, $a = acd$. Because $a \neq 0$ it follows that $cd = 1$. Thus either $c = d = 1$ or $c = d = -1$. Hence, either $a = b$ or $a = -b$. **7.** Because $ac \mid bc$ there is an integer k such that $ack = bc$. Hence, $ak = b$, so $a \mid b$. **9.** **a)** 2, 5 **b)** −11, 10 **c)** 34, 7 **d)** 77, 0 **e)** 0, 0 **f)** 0, 3 **g)** −1, 2 **h)** 4, 0 **11.** **a)** 7:00 **b)** 8:00 **c)** 10:00 **13.** **a)** 10 **b)** 8 **c)** 0 **d)** 9 **e)** 6 **f)** 11 **15.** If a **mod** $m = b$ **mod** m, then a and b have the same remainder when divided by m. Hence, $a = q_1 m + r$ and $b = q_2 m + r$, where $0 \leq r < m$. It follows that $a - b = (q_1 - q_2)m$, so $m \mid (a - b)$. It follows that $a \equiv b \pmod{m}$. **17.** There is some b with $(b-1)k < n \leq bk$. Hence, $(b-1)k \leq n-1 < bk$. Divide by k to obtain $b - 1 < n/k \leq b$ and $b - 1 \leq (n-1)/k < b$. Hence, $\lceil n/k \rceil = b$ and $\lfloor (n-1)/k \rfloor = b - 1$. **19.** x **mod** m if x **mod** $m \leq \lceil m/2 \rceil$ and $(x$ **mod** $m) - m$ if x **mod** $m > \lceil m/2 \rceil$ **21.** **a)** 1 **b)** 2 **c)** 3 **d)** 9 **23.** **a)** 1, 109 **b)** 40, 89 **c)** −31, 222 **d)** −21, 38259 **25.** **a)** −15 **b)** −7 **c)** 140 **27.** −1, −26, −51, −76, 24, 49, 74, 99 **29.** **a)** No **b)** No **c)** Yes **d)** No **31.** **a)** 13 **a)** 6 **33.** **a)** 9 **b)** 4 **c)** 25 **d)** 0 **35.** Let $m = tn$. Because $a \equiv b \pmod{m}$ there exists an integer s such that $a = b + sm$. Hence, $a = b + (st)n$, so $a \equiv b \pmod{n}$. **37.** **a)** Let $m = c = 2$, $a = 0$, and $b = 1$. Then $0 = ac \equiv bc = 2 \pmod{2}$, but $0 = a \not\equiv b = 1 \pmod{2}$. **b)** Let $m = 5$, $a = b = 3$, $c = 1$, and $d = 6$. Then $3 \equiv 3 \pmod{5}$ and $1 \equiv 6 \pmod{5}$, but $3^1 = 3 \not\equiv 4 \equiv 729 = 3^6 \pmod{5}$. **39.** By Exercise 38 the sum of two squares must be either $0 + 0 = 0$, $0 + 1 = 1$, or $1 + 1 = 2$, modulo 4, never 3, and therefore not of the form $4k + 3$. **41.** Because $a \equiv b \pmod{m}$, there exists an integer s such that $a = b + sm$, so $a - b = sm$. Then $a^k - b^k = (a - b)(a^{k-1} + a^{k-2}b + \cdots + ab^{k-2} + b^{k-1})$, $k \geq 2$, is also a multiple of m. It follows that $a^k \equiv b^k \pmod{m}$. **43.** To prove closure, note that $a \cdot_m b = (a \cdot b)$ **mod** m, which by definition is an element of $\mathbf{Z}_m$. Multiplication is associative because $(a \cdot_m b) \cdot_m c$ and $a \cdot_m (b \cdot_m c)$ both equal $(a \cdot b \cdot c)$ **mod** m and multiplication of integers is associative. Similarly, multiplication in $\mathbf{Z}_m$ is commutative because multiplication in $\mathbf{Z}$ is commutative, and 1 is the multiplicative identity for $\mathbf{Z}_m$ because 1 is the multiplicative identity for $\mathbf{Z}$. **45.** $0 +_5 0 = 0$, $0 +_5 1 = 1$, $0 +_5 2 = 2$, $0 +_5 3 = 3$, $0 +_5 4 = 4$; $1 +_5 1 = 2$, $1 +_5 2 = 3$, $1 +_5 3 = 4$, $1 +_5 4 = 0$; $2 +_5 2 = 4$, $2 +_5 3 = 0$, $2 +_5 4 = 1$; $3 +_5 3 = 1$, $3 +_5 4 = 2$; $4 +_4 4 = 3$ and $0 \cdot_5 0 = 0$, $0 \cdot_5 1 = 0$, $0 \cdot_5 2 = 0$, $0 \cdot_5 3 = 0$, $0 \cdot_5 4 = 0$; $1 \cdot_5 1 = 1$, $1 \cdot_5 2 = 2$, $1 \cdot_5 3 = 3$, $1 \cdot_5 4 = 4$; $2 \cdot_5 2 = 4$, $2 \cdot_5 3 = 1$, $2 \cdot_5 4 = 3$; $3 \cdot_5 3 = 4$, $3 \cdot_5 4 = 2$; $4 \cdot_5 4 = 1$ **47.** f is onto but not one-to-one (unless $d = 1$); g is neither.

Section 4.2

1. **a)** 1110 0111 **b)** 1 0001 1011 0100 **c)** 1 0111 11010110 1100 **3.** **a)** 31 **b)** 513 **c)** 341 **d)** 26,896 **5.** **a)** 1 0111 1010 **b)** 11 1000 0100 **c)** 1 0001 0011 **d)** 101 0000 1111 **7.** **a)** 1000 0000 1110 **b)** 1 0011 0101 1010 1011 **c)** 10101011 1011 1010 **d)** 1101 1110 1111 1010 11001110 1101 **9.** 1010 1011 1100 1101 1110 1111 **11.** $(\text{B7B})_{16}$ **13.** Adding up to three leading 0s if necessary, write the binary expansion as $(\dots b_{23}b_{22}b_{21}b_{20}b_{13}b_{12}b_{11}b_{10}b_{03}b_{02}b_{01}b_{00})_2$. The value of this numeral is $b_{00} + 2b_{01} + 4b_{02} + 8b_{03} + 2^4 b_{10} + 2^5 b_{11} + 2^6 b_{12} + 2^7 b_{13} + 2^8 b_{20} + 2^9 b_{21} + 2^{10} b_{22} + 2^{11} b_{23} + \cdots$, which we can rewrite as $b_{00} + 2b_{01} + 4b_{02} + 8b_{03} + (b_{10} + 2b_{11} + 4b_{12} + 8b_{13}) \cdot 2^4 + (b_{20} + 2b_{21} + 4b_{22} + 8b_{23}) \cdot 2^8 + \cdots$. Now $(b_{i3}b_{i2}b_{i1}b_{i0})_2$ translates into the hexadecimal digit h_i. So our number is $h_0 + h_1 \cdot 2^4 + h_2 \cdot 2^8 + \cdots = h_0 + h_1 \cdot 16 + h_2 \cdot 16^2 + \cdots$, which is the hexadecimal expansion $(\dots h_1 h_1 h_0)_{16}$. **15** Adding up to two leading 0s if necessary, write the binary expansion as $(\dots b_{22}b_{21}b_{20}b_{12}b_{11}b_{10}b_{02}b_{01}b_{00})_2$. The value of this numeral is $b_{00} + 2b_{01} + 4b_{02} + 2^3 b_{10} + 2^4 b_{11} + 2^5 b_{12} + 2^6 b_{20} + 2^7 b_{21} + 2^8 b_{22} + \cdots$, which we can rewrite as $b_{00} + 2b_{01} + 4b_{02} + (b_{10} + 2b_{11} + 4b_{12}) \cdot 2^3 + (b_{20} + 2b_{21} + 4b_{22}) \cdot 2^6 + \cdots$. Now $(b_{i2}b_{i1}b_{i0})_2$ translates into the octal digit h_i. So our number is $h_0 + h_1 \cdot 2^3 + h_2 \cdot 2^6 + \cdots = h_0 + h_1 \cdot 8 + h_2 \cdot 8^2 + \cdots$, which is the octal expansion $(\dots h_1 h_1 h_0)_8$. **17.** 1 1101 1100 1010 1101 0001, $1273)_8$ **19.** Convert the given octal numeral to binary, then convert from binary to hexadecimal using Example 7. **21.** **a)** 1011 1110, 10 0001 0000 0001 **b)** 1 1010 1100, 1011 0000 0111 0011 **c)** 100 1001 1010, 101 0010 1001 0110 0000 **d)** 110 0000 0000, 1000 0000 0001 1111 1111 **23.** **a)** 1132, 144,305 **b)** 6273, 2,134,272 **c)** 2110, 1,107,667 **d)** 57,777, 237,326,216 **25.** 436 **27.** 27 **29.** The binary expansion of the integer is the unique such sum. **31.** Let $a = (a_{n-1}a_{n-2} \dots a_1 a_0)_{10}$. Then $a = 10^{n-1}a_{n-1} + 10^{n-2}a_{n-2} + \cdots + 10a_1 + a_0 \equiv a_{n-1} + a_{n-2} + \cdots + a_1 + a_0 \pmod{3}$, because

$10^j \equiv 1 \pmod{3}$) for all nonnegative integers j. It follows that $3 \mid a$ if and only if 3 divides the sum of the decimal digits of a. **33.** Let $a = (a_{n-1}a_{n-2}\ldots a_1a_0)_2$. Then $a = a_0 + 2a_1 + 2^2a_2 + \cdots + 2^{n-1}a_{n-1} \equiv a_0 - a_1 + a_2 - a_3 + \cdots \pm a_{n-1} \pmod{3}$. It follows that a is divisible by 3 if and only if the sum of the binary digits in the even-numbered positions minus the sum of the binary digits in the odd-numbered positions is divisible by 3. **35. a)** -6 **b)** 13 **c)** -14 **d)** 0 **37.** The one's complement of the sum is found by adding the one's complements of the two integers except that a carry in the leading bit is used as a carry to the last bit of the sum. **39.** If $m \ge 0$, then the leading bit a_{n-1} of the one's complement expansion of m is 0 and the formula reads $m = \sum_{i=0}^{n-2} a_i 2^i$. This is correct because the right-hand side is the binary expansion of m. When m is negative, the leading bit a_{n-1} of the one's complement expansion of m is 1. The remaining $n-1$ bits can be obtained by subtracting $-m$ from $111\ldots1$ (where there are $n-1$ 1s), because subtracting a bit from 1 is the same as complementing it. Hence, the bit string $a_{n-2}\ldots a_0$ is the binary expansion of $(2^{n-1}-1) - (-m)$. Solving the equation $(2^{n-1}-1) - (-m) = \sum_{i=0}^{n-2} a_i 2^i$ for m gives the desired equation because $a_{n-1} = 1$. **41. a)** -7 **b)** 13 **c)** -15 **d)** -1 **43.** To obtain the two's complement representation of the sum of two integers, add their two's complement representations (as binary integers are added) and ignore any carry out of the leftmost column. However, the answer is invalid if an overflow has occurred. This happens when the leftmost digits in the two's complement representation of the two terms agree and the leftmost digit of the answer differs. **45.** If $m \ge 0$, then the leading bit a_{n-1} is 0 and the formula reads $m = \sum_{i=0}^{n-2} a_i 2^i$. This is correct because the right-hand side is the binary expansion of m. If $m < 0$, its two's complement expansion has 1 as its leading bit and the remaining $n-1$ bits are the binary expansion of $2^{n-1} - (-m)$. This means that $(2^{n-1}) - (-m) = \sum_{i=0}^{n-2} a_i 2^i$. Solving for m gives the desired equation because $a_{n-1} = 1$. **47.** $4n$

```
49. procedure Cantor($x$: positive integer)
      $n := 1; f := 1$
      while $(n + 1) \cdot f \le x$
        $n := n + 1$
        $f := f \cdot n$
      $y := x$
      while $n > 0$
        $a_n := \lfloor y/f \rfloor$
        $y := y - a_n \cdot f$
        $f := f/n$
        $n := n - 1$
      $\{x = a_n n! + a_{n-1}(n-1)! + \cdots + a_1 1!\}$
```

51. First step: $c = 0, d = 0, s_0 = 1$; second step: $c = 0, d = 1, s_1 = 0$; third step: $c = 1, d = 1, s_2 = 0$; fourth step: $c = 1, d = 1, s_3 = 0$; fifth step: $c = 1, d = 1, s_4 = 1$; sixth step: $c = 1, s_5 = 1$

```
53. procedure subtract($a, b$: positive integers, $a > b$,
        $a = (a_{n-1}a_{n-2}\ldots a_1a_0)_2$,
        $b = (b_{n-1}b_{n-2}\ldots b_1b_0)_2$)
      $B := 0$ {$B$ is the borrow}
      for $j := 0$ to $n - 1$
        if $a_j \ge b_j + B$ then
          $s_j := a_j - b_j - B$
          $B := 0$
        else
          $s_j := a_j + 2 - b_j - B$
          $B := 1$
      {$(s_{n-1}s_{n-2}\ldots s_1s_0)_2$ is the difference}
```

```
55. procedure compare($a, b$: positive integers,
      $a = (a_na_{n-1}\ldots a_1a_0)_2$,
      $b = (b_nb_{n-1}\ldots b_1b_0)_2$)
      $k := n$
      while $a_k = b_k$ and $k > 0$
        $k := k - 1$
      if $a_k = b_k$ then print "$a$ equals $b$"
      if $a_k > b_k$ then print "$a$ is greater than $b$"
      if $a_k < b_k$ then print "$a$ is less than $b$"
```

57. $O(\log n)$ **59.** The only time-consuming part of the algorithm is the **while** loop, which is iterated q times. The work done inside is a subtraction of integers no bigger than a, which has $\log a$ bits. The result now follows from Example 9.

Section 4.3

1. 29, 71, 97 prime; 21, 111, 143 not prime **3. a)** $2^3 \cdot 11$ **b)** $2 \cdot 3^2 \cdot 7$ **c)** 3^6 **d)** $7 \cdot 11 \cdot 13$ **e)** $11 \cdot 101$ **f)** $2 \cdot 3^3 \cdot 5 \cdot 7 \cdot 13 \cdot 37$ **5.** $2^8 \cdot 3^4 \cdot 5^2 \cdot 7$

```
7.  procedure primetester($n$ : integer greater than 1)
      $isprime$ := true
      $d := 2$
      while $isprime$ and $d \le \sqrt{n}$
        if $n$ mod $d = 0$ then $isprime$ := false
        else $d := d + 1$
      return $isprime$
```

9. Write $n = rs$, where $r > 1$ and $s > 1$. Then $2^n - 1 = 2^{rs} - 1 = (2^r)^s - 1 = (2^r - 1)((2^r)^{s-1} + (2^r)^{s-2} + (2^r)^{s-3} + \cdots + 1)$. The first factor is at least $2^2 - 1 = 3$ and the second factor is at least $2^2 + 1 = 5$. This provides a factoring of $2^n - 1$ into two factors greater than 1, so $2^n - 1$ is composite. **11.** Suppose that $\log_2 3 = a/b$ where $a, b \in \mathbf{Z}^+$ and $b \ne 0$. Then $2^{a/b} = 3$, so $2^a = 3^b$. This violates the fundamental theorem of arithmetic. Hence, $\log_2 3$ is irrational. **13.** 3, 5, and 7 are primes of the desired form. **15.** 1, 7, 11, 13, 17, 19, 23, 29 **17. a)** Yes **b)** No **c)** Yes **d)** Yes **19.** Suppose that n is not prime, so that $n = ab$, where a and b are integers greater than 1. Because $a > 1$, by the identity in the hint, $2^a - 1$ is a factor of $2^n - 1$ that is greater than 1, and the second factor in this identity is also greater than 1. Hence, $2^n - 1$ is not prime. **21. a)** 2 **b)** 4 **c)** 12 **23.** $\phi(p^k) = p^k - p^{k-1}$ **25. a)** $3^5 \cdot 5^3$ **b)** 1 **c)** 23^{17} **d)** $41 \cdot 43 \cdot 53$ **e)** 1 **f)** 1111 **27. a)** $2^{11} \cdot 3^7 \cdot 5^9 \cdot 7^3$ **b)** $2^9 \cdot 3^7 \cdot 5^5 \cdot 7^3 \cdot 11 \cdot 13 \cdot 17$ **c)** 23^{31} **d)** $41 \cdot 43 \cdot 53$ **e)** $2^{12}3^{13}5^{17}7^{21}$ **f)** Undefined **29.** gcd (92928, 123552) $=$ 1056; lcm(92928, 123552) $=$ 10,872,576; both products are 11,481,440,256. **31.** Because $\min(x, y) + \max(x, y) = x + y$, the exponent of p_i in the prime factorization of $\gcd(a, b) \cdot \operatorname{lcm}(a, b)$ is the sum of the exponents of p_i in the prime factorizations of a and b. **33. a)** 6 **b)** 3 **c)** 11 **d)** 3 **e)** 40 **f)** 12 **35.** 9 **37.** By Exercise 36 it follows that $\gcd(2^b - 1, (2^a - 1) \textbf{ mod } (2^b - 1)) = \gcd(2^b - 1, 2^{a \textbf{ mod } b} - 1)$. Because the exponents involved in the calculation are b and a **mod** b, the same as the quantities involved in computing $\gcd(a, b)$, the steps used by the Euclidean algorithm to compute $\gcd(2^a - 1, 2^b - 1)$ run in parallel to those used to compute $\gcd(a, b)$ and show that $\gcd(2^a - 1, 2^b - 1) = 2^{\gcd(a,b)} - 1$. **39. a)** $1 = (-1) \cdot 10 + 1 \cdot 11$ **b)** $1 = 21 \cdot 21 + (-10) \cdot 44$ **c)** $12 = (-1) \cdot 36 + 48$ **d)** $1 = 13 \cdot 55 + (-21) \cdot 34$ **e)** $3 = 11 \cdot 213 + (-20) \cdot 117$ **f)** $223 = 1 \cdot 0 + 1 \cdot 223$ **g)** $1 = 37 \cdot 2347 + (-706) \cdot 123$ **h)** $2 = 1128 \cdot 3454 + (-835) \cdot 4666$ **i)** $1 = 2468 \cdot 9999 + (-2221) \cdot 11111$ **41.** $(-3) \cdot 26 + 1 \cdot 91 = 13$ **43.** $34 \cdot 144 + (-55) \cdot 89 = 1$

45.
```
procedure extended Euclidean($a$, $b$: positive integers)
    $x := a$
    $y := b$
    $oldolds := 1$
    $olds := 0$
    $oldoldt := 0$
    $oldt := 1$
    while $y \neq 0$
        $q := x$ div $y$
        $r := x$ mod $y$
        $x := y$
        $y := r$
        $s := oldolds - q \cdot olds$
        $t := oldoldt - q \cdot oldt$
        $oldolds := olds$
        $oldoldt := oldt$
        $olds := s$
        $oldt := t$
    {$\gcd(a, b)$ is $x$, and $(oldolds)a + (oldoldt)b = x$}
```

47. a) $a_n = 1$ if n is prime and $a_n = 0$ otherwise. **b)** a_n is the smallest prime factor of n with $a_1 = 1$. **c)** a_n is the number of positive divisors of n. **d)** $a_n = 1$ if n has no divisors that are perfect squares greater than 1 and $a_n = 0$ otherwise. **e)** a_n is the largest prime less than or equal to n. **f)** a_n is the product of the first $n - 1$ primes. **49.** Because every second integer is divisible by 2, the product is divisible by 2. Because every third integer is divisible by 3, the product is divisible by 3. Therefore the product has both 2 and 3 in its prime factorization and is therefore divisible by $3 \cdot 2 = 6$. **51.** $n = 1601$ is a counterexample. **53** Setting $k = a + b + 1$ will produce the composite number $a(a + b + 1) + b = a^2 + ab + a + b = (a + 1)(a + b)$. **55.** Suppose that there are only finitely many primes of the form $4k + 3$, namely $q_1, q_2, \ldots, q_n$, where $q_1 = 3$, $q_2 = 7$, and so on. Let $Q = 4q_1q_2 \cdots q_n - 1$. Note that Q is of the form $4k + 3$ (where $k = q_1q_2 \cdots q_n - 1$). If Q is prime, then we have found a prime of the desired form different from all those listed. If Q is not prime, then Q has at least one prime factor not in the list $q_1, q_2, \ldots, q_n$, because the remainder when Q is divided by q_j is $q_j - 1$, and $q_j - 1 \neq 0$. Because all odd primes are either of the form $4k + 1$ or of the form $4k + 3$, and the product of primes of the form $4k + 1$ is also of this form (because $(4k + 1)(4m + 1) = 4(4km + k + m) + 1$), there must be a factor of Q of the form $4k + 3$ different from the primes we listed. **57.** Given a positive integer x, we show that there is exactly one positive rational number m/n (in lowest terms) such that $K(m/n) = x$. From the prime factorization of x, read off the m and n such that $K(m/n) = x$. The primes that occur to even powers are the primes that occur in the prime factorization of m, with the exponents being half the corresponding exponents in x; and the primes that occur to odd powers are the primes that occur in the prime factorization of n, with the exponents being half of one more than the exponents in x.

Section 4.4

1. $15 \cdot 7 = 105 \equiv 1 \pmod{26}$ **3.** 7 **5. a)** 7 **b)** 52 **c)** 34 **d)** 73 **7.** Suppose that b and c are both inverses of a modulo m. Then $ba \equiv 1 \pmod{m}$ and $ca \equiv 1 \pmod{m}$. Hence, $ba \equiv ca \pmod{m}$. Because $\gcd(a, m) = 1$ it follows by Theorem 7 in Section 4.3 that $b \equiv c \pmod{m}$. **9.** 8 **11. a)** 67 **b)** 88 **c)** 146 **13.** 3 and 6 **15.** Let $m' = m/\gcd(c, m)$. Because all the common factors of m and c are divided out of m to obtain m', it follows that m' and c are relatively prime. Because m divides $ac - bc = (a - b)c$, it follows that m' divides $(a - b)c$. By Lemma 3 in Section 4.3, we see that m' divides $a - b$, so $a \equiv b \pmod{m'}$. **17.** Suppose that $x^2 \equiv 1 \pmod{p}$. Then p divides $x^2 - 1 = (x + 1)(x - 1)$. By Lemma 2 it follows that $p \mid x + 1$ or $p \mid x - 1$, so $x \equiv -1 \pmod{p}$ or $x \equiv 1 \pmod{p}$. **19. a)** Suppose that $ia \equiv ja \pmod{p}$, where $1 \leq i < j < p$. Then p divides $ja - ia = a(j - i)$. By Theorem 1, because a is not divisible by p, p divides $j - i$, which is impossible because $j - i$ is a positive integer less than p. **b)** By part (a), because no two of $a, 2a, \ldots, (p - 1)a$ are congruent modulo p, each must be congruent to a different number from 1 to $p - 1$. It follows that $a \cdot 2a \cdot 3a \cdot \cdots \cdot (p - 1) \cdot a \equiv 1 \cdot 2 \cdot 3 \cdot \cdots \cdot (p - 1) \pmod{p}$. It follows that $(p - 1)! \cdot a^{p-1} \equiv p - 1 \pmod{p}$. **c)** By Wilson's theorem and part (b), if p does not divide a, it follows that $(-1) \cdot a^{p-1} \equiv -1 \pmod{p}$. Hence, $a^{p-1} \equiv 1 \pmod{p}$. **d)** If $p \mid a$, then $p \mid a^p$. Hence, $a^p \equiv a \equiv 0 \pmod{p}$. If p does not divide a, then $a^{p-1} \equiv a \pmod{p}$, by part (c). Multiplying both sides of this congruence by a gives $a^p \equiv a \pmod{p}$. **21.** All integers of the form $323 + 330k$, where k is an integer **23.** All integers of the form $53 + 60k$, where k is an integer

25.

```
procedure $chinese(m_1, m_2, \ldots, m_n$ : relatively
        prime positive integers ; $a_1, a_2, \ldots, a_n$ : integers)
$m := 1$
for $k := 1$ to $n$
    $m := m \cdot m_k$
for $k := 1$ to $n$
    $M_k := m/m_k$
    $y_k := M_k^{-1}$ mod $m_k$
$x := 0$
for $k := 1$ to $n$
    $x := x + a_k M_k y_k$
while $x \geq m$
    $x := x - m$
return $x$ {the smallest solution to the system
        $\{x \equiv a_k \pmod{m_k}, k = 1, 2, \ldots, n\}$}
```

27. All integers of the form $16 + 252k$, where k is an integer **29.** Suppose that p is a prime appearing in the prime factorization of $m_1 m_2 \cdots m_n$. Because the m_is are relatively prime, p is a factor of exactly one of the m_is, say m_j. Because m_j divides $a - b$, it follows that $a - b$ has the factor p in its prime factorization to a power at least as large as the power to which it appears in the prime factorization of m_j. It follows that $m_1 m_2 \cdots m_n$ divides $a - b$, so $a \equiv b \pmod{m_1 m_2 \cdots m_n}$. **31.** $x \equiv 1 \pmod 6$ **33.** 7 **35.** $a^{p-2} \cdot a = a \cdot a^{p-2} = a^{p-1} \equiv 1 \pmod p$ **37. a)** By Fermat's little theorem, we have $2^{10} \equiv 1 \pmod{11}$. Hence, $2^{340} = (2^{10})^{34} = 1^{34} = 1 \pmod{11}$. **b)** Because $32 \equiv 1 \pmod{31}$, it follows that $2^{340} = (2^5)^{68} = 32^{68} \equiv 1^{68} = 1 \pmod{31}$. **c)** Because 11 and 31 are relatively prime, and $11 \cdot 31 = 341$, it follows by parts (a) and (b) and Exercise 29 that $2^{340} \equiv 1 \pmod{341}$. **39. a)** 3, 4, 8 **b)** 983 **41.** Suppose that q is an odd prime with $q \mid 2^p - 1$. By Fermat's little theorem, $q \mid 2^{q-1} - 1$. From Exercise 37 in Section 4.3, $\gcd(2^p - 1, 2^{q-1} - 1) = 2^{\gcd(p, q-1)} - 1$. Because q is a common divisor of $2^p - 1$ and $2^{q-1} - 1$, $\gcd(2^p - 1, 2^{q-1} - 1) > 1$. Hence, $\gcd(p, q - 1) = p$, because the only other possibility, namely, $\gcd(p, q - 1) = 1$, gives us $\gcd(2^p - 1, 2^{q-1} - 1) = 1$. Hence, $p \mid q - 1$, and therefore there is a positive integer m such that $q - = mp$. Because q is odd, m must be even, say, $m = 2k$, and so every prime divisor of $2^p - 1$ is of the form $2kp + 1$. Furthermore, the product of numbers of this form is also of this form. Therefore, all divisors of $2^p - 1$ are of this form. **43.** M_{11} is not prime; M_{17} is prime. **45.** First, $2047 = 23 \cdot 89$ is composite. Write $2047 - 1 = 2046 = 2 \cdot 1023$, so $s = 1$ and $t = 1023$ in the definition. Then $2^{1023} = (2^{11})^{93} = 2048^{93} \equiv 1^{93} = 1 \pmod{2047}$, as desired. **47.** We must show that $b^{2820} \equiv 1 \pmod{2821}$ for all b relatively prime to 2821. Note that $2821 = 7 \cdot 13 \cdot 31$, and if $\gcd(b, 2821) = 1$, then $\gcd(b, 7) = \gcd(b, 13) = \gcd(b, 31) = 1$. Using Fermat's little theorem we find that $b^6 \equiv 1 \pmod 7$, $b^{12} \equiv 1 \pmod{13}$, and $b^{30} \equiv 1 \pmod{31}$. It follows that $b^{2820} \equiv (b^6)^{470} \equiv 1 \pmod 7$, $b^{2820} \equiv (b^{12})^{235} \equiv 1 \pmod{13}$, and $b^{2820} \equiv (b^{30})^{94} \equiv 1 \pmod{31}$. By Exercise 29 (or the Chinese remainder theorem) it follows that $b^{2820} \equiv 1 \pmod{2821}$, as desired. **49. a)** If we multiply out this expression, we get $n = 1296m^3 + 396m^2 + 36m + 1$. Clearly $6m \mid n - 1$, $12m \mid n - 1$, and $18m \mid n - 1$. Therefore, the conditions of Exercise 48 are met, and we conclude that n is a Carmichael number. **b)** Letting $m = 51$ gives $n = 172{,}947{,}529$. **51.** $0 = (0, 0)$, $1 = (1, 1)$, $2 = (2, 2)$, $3 = (0, 3)$, $4 = (1, 4)$, $5 = (2, 0)$, $6 = (0, 1)$, $7 = (1, 2)$, $8 = (2, 3)$, $9 = (0, 4)$, $10 = (1, 0)$, $11 = (2, 1)$, $12 = (0, 2)$, $13 = (1, 3)$, $14 = (2, 4)$ **53.** We have $m_1 = 99$, $m_2 = 98$, $m_3 = 97$, and $m_4 = 95$, so $m = 99 \cdot 98 \cdot 97 \cdot 95 = 89{,}403{,}930$. We find that $M_1 = m/m_1 = 903{,}070$, $M_2 = m/m_2 = 912{,}285$, $M_3 = m/m_3 = 921{,}690$, and $M_4 = m/m_4 = 941{,}094$. Using the Euclidean algorithm, we compute that $y_1 = 37$, $y_2 = 33$, $y_3 = 24$, and $y_4 = 4$ are inverses of M_k modulo m_k for $k = 1, 2, 3, 4$, respectively. It follows that the solution is $65 \cdot 903{,}070 \cdot 37 + 2 \cdot 912{,}285 \cdot 33 + 51 \cdot 921{,}690 \cdot 24 + 10 \cdot 941{,}094 \cdot 4 = 3{,}397{,}886{,}480 \equiv 537{,}140 \pmod{89{,}403{,}930}$. **55.** $\log_2 5 = 16$, $\log_2 6 = 14$ **57.** $\log_3 1 = 0$, $\log_3 2 = 14$, $\log_3 3 = 1$, $\log_3 4 = 12$, $\log_3 5 = 5$, $\log_3 6 = 15$, $\log_3 7 = 11$, $\log_3 8 = 10$, $\log_3 9 = 2$, $\log_3 10 = 3$, $\log_3 11 = 7$, $\log_3 12 = 13$, $\log_3 13 = 4$, $\log_3 14 = 9$, $\log_3 15 = 6$, $\log_3 16 = 8$ **59.** Assume that s is a solution of $x^2 \equiv a \pmod p$. Then because $(-s)^2 = s^2$, $-s$ is also a solution. Furthermore, $s \not\equiv -s \pmod p$. Otherwise, $p \mid 2s$, which implies that $p \mid s$, and this implies, using the original assumption, that $p \mid a$, which is a contradiction. Furthermore, if s and t are incongruent solutions modulo p, then because $s^2 \equiv t^2 \pmod p$, $p \mid s^2 - t^2$. This implies that $p \mid (s + t)(s - t)$, and by Lemma 3 in Section 4.3, $p \mid s - t$ or $p \mid s + t$, so $s \equiv t \pmod p$ or $s \equiv -t \pmod p$. Hence, there are at most two solutions. **61.** The value of $\left(\frac{a}{p}\right)$ depends only on whether a is a quadratic residue modulo p, that is, whether $x^2 \equiv a \pmod p$ has a solution. Because this depends only on the equivalence class of a modulo p, it follows that $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$ if $a \equiv b \pmod p$. **63.** By Exercise 62, $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = a^{(p-1)/2} b^{(p-1)/2} = (ab)^{(p-1)/2} \equiv \left(\frac{ab}{p}\right) \pmod p$. **65.** $x \equiv 8, 13, 22$, or $27 \pmod{35}$ **67.** Compute r^e **mod** p for $e = 0, 1, 2, \ldots, p - 2$ until we get the answer a. Worst case and average case time complexity are $O(p \log p)$.

Section 4.5

1. 91, 57, 21, 5 **3. a)** 7, 19, 7, 7, 18, 0 **b)** Take the next available space **mod** 31. **5.** 1, 5, 4, 1, 5, 4, 1, 5, 4, … **7.** 2, 6, 7, 10, 8, 2, 6, 7, 10, 8, … **9.** 2357, 5554, 8469, 7239, 4031, 2489, 1951, 8064 **11.** 2, 1, 1, 1, … **13.** Only string (d) **15.** 4 **17.** Correctly, of course **19. a)** Not valid **b)** Valid **c)** Valid **d)** Not valid **21. a)** No **b)** 5 **c)** 7 **d)** 8 **23.** Transposition errors involving the last digit **25. a)** Yes **b)** No **c)** Yes **d)** No **27.** Transposition errors will be detected if and only if the transposed digits are an odd number of positions apart and do not differ by 5. **29. a)** Valid **b)** Not valid **c)** Valid **d)** Valid **31.** Yes, as long as the two digits do not differ by 7 **33. a)** Not valid **b)** Valid **c)** Valid **d)** Not valid **35.** The given congruence is equivalent to $3d_1 + 4d_2 + 5d_3 + 6d_4 + 7d_5 + 8d_6 + 9d_7 + 10d_8 \equiv 0 \pmod{11}$. Transposing adjacent digits x and y (with x on the left) causes the left-hand side to increase by $x - y$. Because $x \not\equiv y \pmod{11}$, the congruence will no longer hold. Therefore errors of this type are always detected.

Section 4.6

1. a) GR QRW SDVV JR **b)** QB ABG CNFF TB **c)** QX UXM AHJJ ZX **3. a)** KOHQV MCIF GHSD **b)** RVBXP TJPZ NBZX **c)** DBYNE PHRM FYZA **5. a)** SURRENDER NOW **b)** BE MY FRIEND **c)** TIME FOR FUN **7.** TO SLEEP PERCHANCE TO DREAM **9.** ANY SUFFICIENTLY ADVANCED TECHNOLOGY IS INDISTINGUISHABLE FROM MAGIC **11.** $p = 7c + 13$ **mod** 26 **13.** $a = 18$, $b = 5$ **15.** BEWARE OF MARTIANS **17.** Presumably something like an affine cipher **19.** HURRICANE **21.** The length of the key may well be the greatest common divisor of the distances between the starts of the repeated string (or a factor of the gcd). **23.** Suppose we know both $n = pq$ and $(p-1)(q-1)$. To find p and q, first note that $(p-1)(q-1) = pq - p - q + 1 = n - (p+q) + 1$. From this we can find $s = p + q$. Because $q = s - p$, we have $n = p(s - p)$. Hence, $p^2 - ps + n = 0$. We now can use the quadratic formula to find p. Once we have found p, we can find q because $q = n/p$. **25.** 2545 2757 1211 **27.** SILVER **29.** Alice sends 5^8 **mod** $23 = 16$ to Bob. Bob sends 5^5 **mod** $23 = 20$ to Alice. Alice computes 20^8 **mod** $23 = 6$ and Bob computes 16^5 **mod** $23 = 6$. The shared key is 6. **31.** 2186 2087 1279 1251 0326 0816 1948 **33.** Alice can decrypt the first part of Cathy's message to learn the key, and Bob can decrypt the second part of Cathy's message, which Alice forwarded to him, to learn the key. No one else besides Cathy can learn the key, because all of these communications use secure private keys.

Supplementary Exercises

1. The actual number of miles driven is $46518 + 100000k$ for some natural number k. **3.** 5, 22, -12, -29 **5.** Because $ac \equiv bc \pmod m$ there is an integer k such that $ac = bc + km$. Hence, $a - b = km/c$. Because $a - b$ is an integer, $c \mid km$. Letting $d = \gcd(m, c)$, write $c = de$. Because no factor of e divides m/d, it follows that $d \mid m$ and $e \mid k$. Thus $a - b = (k/e)(m/d)$, where $k/e \in \mathbf{Z}$ and $m/d \in \mathbf{Z}$. Therefore $a \equiv b \pmod{m/d}$. **7.** Proof of the contrapositive: If n is odd, then $n = 2k + 1$ for some integer k. Therefore $n^2 + 1 = (2k+1)^2 + 1 = 4k^2 + 4k + 2 \equiv 2 \pmod 4$. But perfect squares of even numbers are congruent to 0 modulo 4 (because $(2m)^2 = 4m^2$), and perfect squares of odd numbers are congruent to 1 or 3 modulo 4, so $n^2 + 1$ is not a perfect square. **9.** n is divisible by 8 if and only if the binary expansion of n ends with 000. **11.** We assume that someone has chosen a positive integer less than 2^n, which we are to guess. We ask the person to write the number in binary, using leading 0s if necessary to make it n bits long. We then ask "Is the first bit a 1?", "Is the second bit a 1?", "Is the third bit a 1?", and so on. After we know the answers to these n questions, we will know the number, because we will know its binary expansion. **13.** $(a_n a_{n-1} \ldots a_1 a_0)_{10} = \sum_{k=0}^{n} 10^k a_k \equiv \sum_{k=0}^{n} a_k \pmod 9$ because $10^k \equiv 1 \pmod 9$ for every nonnegative integer k. **15.** Because for all $k \le n$, when Q_n is divided by k the remainder will be 1, it follows that no prime number less than or equal to n is a factor of Q_n. Thus by the fundamental theorem of arithmetic, Q_n must have a prime factor greater than n. **17.** Take $a = 10$ and $b = 1$ in Dirichlet's theorem. **19.** Every number greater than 11 can be written as either $8 + 2n$ or $9 + 2n$ for some $n \ge 2$. **21.** Assume that every even integer greater than 2 is the sum of two primes, and let n be an integer greater than 5. If n is odd, write $n = 3 + (n - 3)$ and decompose $n - 3 = p + q$ into the sum of two primes; if n is even, then write $n = 2 + (n - 2)$ and decompose $n - 2 = p + q$ into the sum of two primes. For the converse, assume that every integer greater than 5 is the sum of three primes, and let n be an even integer greater than 2. Write $n + 2$ as the sum of three primes, one of which is necessarily 2, so $n + 2 = 2 + p + q$, whence $n = p + q$. **23.** Recall that a nonconstant polynomial can take on the same value only a finite number of times. Thus f can take on the values 0 and ± 1 only finitely many times, so if there is not some y such that $f(y)$ is composite, then there must be some x_0 such that $\pm f(x_0)$ is prime, say p. Look at $f(x_0 + kp)$. When we plug $x_0 + kp$ in for x in the polynomial and multiply it out, every term will contain a factor of p except for the terms that form $f(x_0)$. Therefore $f(x_0 + kp) = f(x_0) + mp = (m \pm 1)p$ for some integer m. As k varies, this value can be 0, p, or $-p$ only finitely many times; therefore it must be a composite number for some values of k. **25.** 1 **27.** 1 **29.** If not, then suppose that $q_1, q_2, \ldots, q_n$ are all the primes of the form $6k + 5$. Let $Q = 6q_1q_2 \cdots q_n - 1$. Note that Q is of the form $6k + 5$, where $k = q_1q_2 \cdots q_n - 1$. Let $Q = p_1p_2 \cdots p_t$ be the prime factorization of Q. No p_i is 2, 3, or any q_j, because the remainder when Q is divided by 2 is 1, by 3 is 2, and by q_j is $q_j - 1$. All odd primes other than 3 are of the form $6k + 1$ or $6k + 5$, and the product of primes of the form $6k + 1$ is also of this form. Therefore at least one of the p_i's must be of the form $6k + 5$, a contradiction. **31.** The product of numbers of the form $4k + 1$ is of the form $4k + 1$, but numbers of this form might have numbers not of this form as their only prime factors. For example, $49 = 4 \cdot 12 + 1$, but the prime factorization of 49 is $7 \cdot 7 = (4 \cdot 1 + 3)(4 \cdot 1 + 3)$. **33. a)** Not mutually relatively prime **b)** Mutually relatively prime **c)** Mutually relatively prime **d)** Mutually relatively prime **35** 1 **37.** $x \equiv 28 \pmod{30}$ **39.** By the Chinese remainder theorem, it suffices to show that $n^9 - n \equiv 0 \pmod 2$, $n^9 - n \equiv 0 \pmod 3$, and $n^9 - n \equiv 0 \pmod 5$. Each in turn follows from applying Fermat's little theorem. **41.** By Fermat's little theorem, $p^{q-1} \equiv 1 \pmod q$ and clearly $q^{p-1} \equiv 0 \pmod q$. Therefore $p^{q-1} + q^{p-1} \equiv 1 + 0 = 1 \pmod q$. Similarly, $p^{q-1} + q^{p-1} \equiv 1 \pmod p$. It follows from the Chinese remainder theorem that $p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$. **43.** If a_i is changed from x to y, then the change in the left-hand side of the congruence is either $y - x$ or $3(y - x)$, modulo 10, neither of which can be 0 because 1 and