15. procedure *Cantor permutation*(n, i: integers with $n \geq 1$ and $0 \leq i < n!$)

```
x := n
for j := 1 to n
  p_j := 0
for k := 1 to n − 1
begin
  c := ⌊x/(n − k)!⌋; x := x − c(n − k)!; h := n
  while p_h ≠ 0
    h := h − 1
  for j := 1 to c
  begin
    h := h − 1
    while p_h ≠ 0
      h := h − 1
  end
  p_h := n − k + 1
end
h := 1
while p_h ≠ 0
  h := h + 1
p_h := 1
  {p_1 p_2 ··· p_n is the permutation corresponding
   to i}
```

Supplementary Exercises

1. a) 151,200 **b)** 1,000,000 **c)** 210 **d)** 5005 **3.** 3^{100} **5.** 24,600 **7. a)** 4,060 **b)** 2688 **c)** 25,009,600 **9. a)** 192 **b)** 301 **c)** 300 **d)** 300 **11.** 639 **13.** The maximum possible sum is 240, and the minimum possible sum is 15. So the number of possible sums is 226. Because there are 252 subsets with five elements of a set with 10 elements, by the pigeonhole principle it follows that at least two have the same sum. **15. a)** 50 **b)** 50 **c)** 14 **d)** 5 **17.** Let $a_1, a_2, \ldots, a_m$ be the integers, and let $d_i = \sum_{j=1}^{i} a_j$. If $d_i \equiv 0 \pmod{m}$ for some i, we are done. Otherwise d_1 **mod** m, d_2 **mod** $m, \ldots, d_m$ **mod** m are m integers with values in $\{1, 2, \ldots, m-1\}$. By the pigeonhole principle $d_k = d_l$ for some $1 \leq k < l \leq m$. Then $\sum_{j=k+1}^{l} a_j = d_l - d_k \equiv 0 \pmod{m}$. **19.** The decimal expansion of the rational number a/b can be obtained by division of b into a, where a is written with a decimal point and an arbitrarily long string of 0s following it. The basic step is finding the next digit of the quotient, namely, $\lfloor r/b \rfloor$, where r is the remainder with the next digit of the dividend brought down. The current remainder is obtained from the previous remainder by subtracting b times the previous digit of the quotient. Eventually the dividend has nothing but 0s to bring down. Furthermore, there are only b possible remainders. Thus, at some point, by the pigeonhole principle, we will have the same situation as had previously arisen. From that point onward, the calculation must follow the same pattern. In particular, the quotient will repeat. **21. a)** 125,970 **b)** 20 **c)** 141,120,525 **d)** 141,120,505 **e)** 177,100 **f)** 141,078,021 **23. a)** 10 **b)** 8 **c)** 7 **25.** 3^n **27.** $C(n+2, r+1) = C(n+1, r+1) + C(n+1, r) = 2C(n+1, r+1) - C(n+1, r+1) + C(n+1, r) = 2C(n+1, r+1) - (C(n, r+1) + C(n, r)) + (C(n, r) + C(n, r-1)) = 2C(n+1, r+1) - C(n, r+1) + C(n, r-1)$ **29.** Substitute $x = 1$ and $y = 3$ into the Binomial Theorem. **31.** $C(n+1, 5)$ **33.** 3,491,888,400 **35.** 5^{24} **37. a)** 45 **b)** 57 **c)** 12 **39. a)** 386 **b)** 56 **c)** 512 **41.** 0 if $n < m$; $C(n-1, n-m)$ if $n \geq m$ **43. a)** 15,625 **b)** 202 **c)** 210 **d)** 10

45. procedure *next permutation* (n: positive integer, $a_1, a_2, \ldots, a_r$: positive integers not exceeding n with $a_1 a_2 \ldots a_r \neq nn \ldots n$)

```
i := r
while a_i = n
begin
  a_i := 1
  i := i − 1
end
a_i := a_i + 1
{a_1 a_2 ... a_r is the next permutation in lexicographic
  order}
```

47. We must show that if there are $R(m, n-1) + R(m-1, n)$ people at a party, then there must be at least m mutual friends or n mutual enemies. Consider one person; let's call him Jerry. Then there are $R(m-1, n) + R(m, n-1) - 1$ other people at the party, and by the pigeonhole principle there must be at least $R(m-1, n)$ friends of Jerry or $R(m, n-1)$ enemies of Jerry among these people. First let's suppose there are $R(m-1, n)$ friends of Jerry. By the definition of R, among these people we are guaranteed to find either $m-1$ mutual friends or n mutual enemies. In the former case, these $m-1$ mutual friends together with Jerry are a set of m mutual friends; and in the latter case, we have the desired set of n mutual enemies. The other situation is similar: Suppose there are $R(m, n-1)$ enemies of Jerry; we are guaranteed to find among them either m mutual friends or $n-1$ mutual enemies. In the former case, we have the desired set of m mutual friends, and in the latter case, these $n-1$ mutual enemies together with Jerry are a set of n mutual enemies.

CHAPTER 6

Section 6.1

1. 1/13 **3.** 1/2 **5.** 1/2 **7.** 1/64 **9.** 47/52 **11.** $1/C(52, 5)$ **13.** $1 - [C(48, 5)/C(52, 5)]$ **15.** $C(13, 2) C(4, 2)C(4, 2)C(44, 1)/C(52, 5)$ **17.** $10{,}240/C(52, 5)$ **19.** $1{,}302{,}540/C(52, 5)$ **21.** 1/64 **23.** 8/25 **25. a)** $1/C(50, 6) = 1/15{,}890{,}700$ **b)** $1/C(52, 6) = 1/20{,}358{,}520$ **c)** $1/C(56, 6) = 1/32{,}468{,}436$ **d)** $1/C(60, 6) = 1/50{,}063{,}860$ **27. a)** 139,128/319,865 **b)** 212, 667/511,313 **c)** 151,340/386,529 **d)** 163,647/446,276 **29.** $1/C(100, 8)$ **31.** 3/100 **33. a)** 1/7,880,400 **b)** 1/8,000,000 **35. a)** 9/19 **b)** 81/361 **c)** 1/19 **d)** 1,889,568/2,476,099 **e)** 48/361 **37.** Three dice **39.** The door the contestant chooses is chosen at random without knowing where the prize is, but the door chosen by the host is not chosen at random, because he always avoids opening the door with the prize. This makes any argument based on symmetry invalid. **41. a)** $671/1296$ **b)** $1 - 35^{24}/36^{24}$; no **c)** Yes

Section 6.2

1. $p(T) = 1/4$, $p(H) = 3/4$ **3.** $p(1) = p(3) = p(5) = p(6) = 1/16$; $p(2) = p(4) = 3/8$ **5.** $9/49$ **7. a)** $1/2$ **b)** $1/2$ **c)** $1/3$ **d)** $1/4$ **e)** $1/4$ **9. a)** $1/26!$ **b)** $1/26$ **c)** $1/2$ **d)** $1/26$ **e)** $1/650$ **f)** $1/15{,}600$ **11.** Clearly, $p(E \cup F) \ge p(E) = 0.7$. Also, $p(E \cup F) \le 1$. If we apply Theorem 2 from Section 6.1, we can rewrite this as $p(E) + p(F) - p(E \cap F) \le 1$, or $0.7 + 0.5 - p(E \cap F) \le 1$. Solving for $p(E \cap F)$ gives $p(E \cap F) \ge 0.2$. **13.** Because $p(E \cup F) = p(E) + p(F) - p(E \cap F)$ and $p(E \cup F) \le 1$, it follows that $1 \ge p(E) + p(F) - p(E \cap F)$. From this inequality we conclude that $p(E) + p(F) \le 1 + p(E \cap F)$. **15.** We will use mathematical induction to prove that the inequality holds for $n \ge 2$. Let $P(n)$ be the statement that $p(\bigcup_{j=1}^{n} E_j) \le \sum_{j=1}^{n} p(E_j)$. *Basis step:* $P(2)$ is true because $p(E_1 \cup E_2) = p(E_1) + p(E_2) - p(E_1 \cap E_2) \le p(E_1) + p(E_2)$. *Inductive step:* Assume that $P(k)$ is true. Using the basis case and the inductive hypothesis, it follows that $p(\bigcup_{j=1}^{k+1} E_j) \le p(\bigcup_{j=1}^{k} E_j) + p(E_{k+1}) \le \sum_{j=1}^{k+1} p(E_j)$. This shows that $P(k+1)$ is true, completing the proof by mathematical induction. **17.** Because $E \cup \overline{E}$ is the entire sample space S, the event F can be split into two disjoint events: $F = S \cap F = (E \cup \overline{E}) \cap F = (E \cap F) \cup (\overline{E} \cap F)$, using the distributive law. Therefore, $p(F) = p((E \cap F) \cup (\overline{E} \cap F)) = p(E \cap F) + p(\overline{E} \cap F)$, because these two events are disjoint. Subtracting $p(E \cap F)$ from both sides, using the fact that $p(E \cap F) = p(E) \cdot p(F)$ (the hypothesis that E and F are independent), and factoring, we have $p(F)[1 - p(E)] = p(\overline{E} \cap F)$. Because $1 - p(E) = p(\overline{E})$, this says that $p(\overline{E} \cap F) = p(\overline{E}) \cdot p(F)$, as desired. **19. a)** $1/12$ **b)** $1 - \frac{11}{12} \cdot \frac{10}{12} \cdot \cdots \cdot \frac{13-n}{12}$ **c)** 5 **21.** 614 **23.** $1/4$ **25.** $3/8$ **27. a)** Not independent **b)** Not independent **c)** Not independent **29.** $3/16$ **31. a)** $1/32 = 0.03125$ **b)** $0.49^5 \approx 0.02825$ **c)** 0.03795012 **33. a)** $5/8$ **b)** 0.627649 **c)** 0.6431 **35. a)** p^n **b)** $1 - p^n$ **c)** $p^n + n \cdot p^{n-1} \cdot (1-p)$ **d)** $1 - [p^n + n \cdot p^{n-1} \cdot (1-p)]$ **37.** $p(\bigcup_{i=1}^{\infty} E_i)$ is the sum of $p(s)$ for each outcome s in $\bigcup_{i=1}^{\infty} E_i$. Because the E_is are pairwise disjoint, this is the sum of the probabilities of all the outcomes in any of the E_is, which is what $\sum_{i=1}^{\infty} p(E_i)$ is. (We can rearrange the summands and still get the same answer because this series converges absolutely.) **39. a)** $\overline{E} = \bigcup_{j=1}^{\binom{m}{k}} F_j$, so the given inequality now follows from Boole's Inequality (Exercise 15). **b)** The probability that a particular player not in the jth set beats all k of the players in the jth set is $(1/2)^k = 2^{-k}$. Therefore, the probability that this player does not do so is $1 - 2^{-k}$, so the probability that all $m - k$ of the players not in the jth set are unable to boast of a perfect record against everyone in the jth set is $(1 - 2^{-k})^{m-k}$. That is precisely $p(F_j)$. **c)** The first inequality follows immediately, because all the summands are the same and there are $\binom{m}{k}$ of them. If this probability is less than 1, then it must be possible that $\overline{E}$ fails, i.e., that E happens. So there is a tournament that meets the conditions of the problem as long as the second inequality holds. **d)** $m \ge 21$ for $k = 2$, and $m \ge 91$ for $k = 3$

41.
```
procedure probabilistic prime (n, k)
composite := false
i := 0
while composite = false and i < k
begin
  i := i + 1
  choose b uniformly at random with 1 < b < n
  apply Miller's test to base b
  if n fails the test then composite := true
end
if composite = true then print ("composite")
else print ("probably prime")
```

Section 6.3

NOTE: In the answers for Section 6.3, all probabilities given in decimal form are rounded to three decimal places. **1.** $3/5$ **3.** $3/4$ **5.** 0.481 **7. a)** 0.999 **b)** 0.324 **9. a)** 0.740 **b)** 0.260 **c)** 0.002 **d)** 0.998 **11.** 0.724 **13.** $3/17$ **15. a)** $1/3$ **b)** $p(M = j \mid W = k) = 1$ if i, j, and k are distinct; $p(M = j \mid W = k) = 0$ if $j = k$ or $j = i$; $p(M = j \mid W = k) = 1/2$ if $i = k$ and $j \ne i$ **c)** $2/3$ **d)** You should change doors, because you now have a $2/3$ chance to win by switching. **17.** The definition of conditional probability tells us that $p(F_j \mid E) = p(E \cap F_j)/p(E)$. For the numerator, again using the definition of conditional probability, we have $p(E \cap F_j) = p(E \mid F_j)p(F_j)$, as desired. For the denominator, we show that $p(E) = \sum_{i=1}^{n} p(E \mid F_i)p(F_i)$. The events $E \cap F_i$ partition the event E; that is, $(E \cap F_{i_1}) \cap (E \cap F_{i_2}) = \emptyset$ when $i_i \ne i_2$ (because the F_i's are mutually exclusive), and $\bigcup_{i=1}^{n}(E \cap F_{i_i}) = E$ (because the $\bigcup_{i=1}^{n} F_i = S$). Therefore, $p(E) = \sum_{i=1}^{n} p(E \cap F_i) = \sum_{i=1}^{n} p(E \mid F_i)p(F_i)$. **19.** No **21.** Yes **23.** By Bayes' Theorem, $p(S \mid E_1 \cap E_2) = p(E_1 \cap E_2 \mid S)p(S)/[p(E_1 \cap E_2 \mid S)p(S) + p(E_1 \cap E_2 \mid \overline{S})p(\overline{S})]$. Because we are assuming no prior knowledge about whether a message is or is not spam, we set $p(S) = p(\overline{S}) = 0.5$, and so the equation above simplifies to $p(S \mid E_1 \cap E_2) = p(E_1 \cap E_2 \mid S)/[p(E_1 \cap E_2 \mid S) + p(E_1 \cap E_2 \mid \overline{S})]$. Because of the assumed independence of E_1, E_2, and S, we have $p(E_1 \cap E_2 \mid S) = p(E_1 \mid S) \cdot p(E_2 \mid S)$, and similarly for $\overline{S}$.

Section 6.4

1. 2.5 **3.** $5/3$ **5.** $336/49$ **7.** 170 **9.** $(4n+6)/3$ **11.** $50{,}700{,}551/10{,}077{,}696 \approx 5.03$ **13.** 6 **15.** $p(X \ge j) = \sum_{k=j}^{\infty} p(X = k) = \sum_{k=j}^{\infty} (1-p)^{k-1} p = p(1-p)^{j-1} \sum_{k=0}^{\infty} (1-p)^k = p(1-p)^{j-1}/(1-(1-p)) = (1-p)^{j-1}$ **17.** 2302 **19.** $(7/2) \cdot 7 \ne 329/12$ **21.** $p + (n-1)p(1-p)$ **23.** $5/2$ **25. a)** 0 **b)** n **27. a)** We are told that X_1 and X_2 are independent. To see that X_1 and X_3 are independent, we enumerate the eight possibilities for (X_1, X_2, X_3) and find that $(0,0,0), (1,0,1), (0,1,1), (1,1,0)$ each have probability $1/4$ and the others have probability 0 (because of the definition of X_3). Thus, $p(X_1 = 0 \wedge X_3 = 0) = 1/4$, $p(X_1 = 0) = 1/2$, and $p(X_3 = 0) = 1/2$, so it is true that $p(X_1 = 0 \wedge X_3 = 0) = p(X_1 = 0)p(X_3 = 0)$. Essentially the same calculation shows that $p(X_1 = 0 \wedge X_3 = 1) = p(X_1 = 0)p(X_3 = 1)$, $p(X_1 = 1 \wedge X_3 = 0) = p(X_1 = 1)p(X_3 = 0)$, and $p(X_1 = 1 \wedge X_3 = 1) = p(X_1 = 1)p(X_3 = 1)$. Therefore by definition, X_1 and X_3 are independent. The same reasoning shows that X_2 and X_3 are independent. To see that X_3 and $X_1 + X_2$ are not independent, we observe that $p(X_3 = 1 \wedge X_1 + X_2 = 2) = 0$. But $p(X_3 = 1)p(X_1 + X_2 = 2) = (1/2)(1/4) = 1/8$. **b)** We see from the calculation in part (a) that X_1, X_2, and X_3 are all Bernoulli random variables, so the variance of each is $(1/2)(1/2) = 1/4$. Therefore, $V(X_1) + V(X_2) + V(X_3) = 3/4$. We use the calculations in part (a) to see that $E(X_1 + X_2 + X_3) = 3/2$, and then $V(X_1 + X_2 + X_3) = 3/4$. **c)** In order to use the first part of Theorem 7 to show that $V((X_1 + X_2 + \cdots + X_k) + X_{k+1}) = V(X_1 + X_2 + \cdots + X_k) + V(X_{k+1})$ in the inductive step of a proof by mathematical induction, we would have to know that $X_1 + X_2 + \cdots + X_k$ and X_{k+1} are independent, but we see from part (a) that this is not necessarily true. **29.** $1/100$ **31.** $E(X)/a = \sum_r (r/a) \cdot p(X = r) \geq \sum_{r \geq a} 1 \cdot p(X = r) = p(X \geq a)$ **33. a)** $10/11$ **b)** 0.9984 **35. a)** Each of the $n!$ permutations occurs with probability $1/n!$, so $E(X)$ is the number of comparisons, averaged over all these permutations. **b)** Even if the algorithm continues $n - 1$ rounds, X will be at most $n(n - 1)/2$. It follows from the formula for expectation that $E(X) \leq n(n - 1)/2$. **c)** The algorithm proceeds by comparing adjacent elements and then swapping them if necessary. Thus, the only way that inverted elements can become uninverted is for them to be compared and swapped. **d)** Because $X(P) \geq I(P)$ for all P, it follows from the definition of expectation that $E(X) \geq E(I)$. **e)** This summation counts 1 for every instance of an inversion. **f)** This follows from Theorem 3. **g)** By Theorem 2 with $n = 1$, the expectation of $I_{j,k}$ is the probability that a_k precedes a_j in the permutation. This is clearly $1/2$ by symmetry. **h)** The summation in part (f) consists of $C(n, 2) = n(n - 1)/2$ terms, each equal to $1/2$, so the sum is $n(n - 1)/4$. **i)** From part (a) and part (b) we know that $E(X)$, the object of interest, is at most $n(n - 1)/2$, and from part (d) and part (h) we know that $E(X)$ is at least $n(n - 1)/4$, both of which are $\Theta(n^2)$. **37.** 1 **39.** $V(X + Y) = E((X + Y)^2) - E(X + Y)^2 = E(X^2 + 2XY + Y^2) - [E(X) + E(Y)]^2 = E(X^2) + 2E(XY) + E(Y^2) - E(X)^2 - 2E(X)E(Y) - E(Y)^2 = E(X^2) - E(X)^2 + 2[E(XY) - E(X)E(Y)] + E(Y^2) - E(Y)^2 = V(X) + 2\,\mathrm{Cov}(X, Y) + V(Y)$ **41.** $[(n - 1)/n]^m$ **43.** $(n - 1)^m/n^{m-1}$

Supplementary Exercises

1. $1/109{,}668$ **3. a)** $1/C(52, 13)$ **b)** $4/C(52, 13)$ **c)** $2{,}944{,}656/C(52, 13)$ **d)** $35{,}335{,}872/C(52, 13)$ **5. a)** $9/2$ **b)** $21/4$ **7. a)** 9 **b)** $21/2$ **9. a)** 8 **b)** $49/6$ **11. a)** $n/2^{n-1}$ **b)** $p(1 - p)^{k-1}$, where $p = n/2^{n-1}$ **c)** $2^{n-1}/n$ **13.** $\frac{(m-1)(n-1)+\gcd(m,n)-1}{mn-1}$ **15. a)** $2/3$ **b)** $2/3$ **17.** $1/32$ **19. a)** The probability that one wins 2^n dollars is $1/2^n$, because that happens precisely when the player gets $n - 1$ tails followed by a head. The expected value of the winnings is therefore the sum of 2^n times $1/2^n$ as n goes from 1 to infinity. Because each of these terms is 1, the sum is infinite. In other words, one should be willing to wager any amount of money and expect to come out ahead in the long run. **b)** \$9, \$9 **21. a)** $1/3$ when $S = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$, $A = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$, and $B = \{1, 2, 3, 4\}$; $1/12$ when $S = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$, $A = \{4, 5, 6, 7, 8, 9, 10, 11, 12\}$, and $B = \{1, 2, 3, 4\}$ **b)** 1 when $S = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$, $A = \{4, 5, 6, 7, 8, 9, 10, 11, 12\}$, and $B = \{1, 2, 3, 4\}$; $3/4$ when $S = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$, $A = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$, and $B = \{1, 2, 3, 4\}$ **23. a)** $p(E_1 \cap E_2) = p(E_1)p(E_2)$, $p(E_1 \cap E_3) = p(E_1)p(E_3)$, $p(E_2 \cap E_3) = p(E_2)p(E_3)$, $p(E_1 \cap E_2 \cap E_3) = p(E_1)p(E_2)p(E_3)$ **b)** Yes **c)** Yes; yes **d)** Yes; no **e)** $2^n - n - 1$ **25.** $V(aX + b) = E((aX + b)^2) - E(aX + b)^2 = E(a^2X^2 + 2abX + b^2) - [aE(X) + b]^2 = E(a^2X^2) + E(2abX) + E(b^2) - [a^2E(X)^2 + 2abE(X) + b^2] = a^2E(X^2) + 2abE(X) + b^2 - a^2E(X)^2 - 2abE(X) - b^2 = a^2[E(X^2) - E(X)^2] = a^2V(X)$ **27.** To count every element in the sample space exactly once, we must include every element in each of the sets and then take away the double counting of the elements in the intersections. Thus $p(E_1 \cup E_2 \cup \cdots \cup E_m) = p(E_1) + p(E_2) + \cdots + p(E_m) - p(E_1 \cap E_2) - p(E_1 \cap E_3) - \cdots - p(E_1 \cap E_m) - p(E_2 \cap E_3) - p(E_2 \cap E_4) - \cdots - p(E_2 \cap E_m) - \cdots - p(E_{m-1} \cap E_m) = qm - (m(m - 1)/2)r$, because $C(m, 2)$ terms are being subtracted. But $p(E_1 \cup E_2 \cup \cdots \cup E_m) = 1$, so we have $qm - [m(m - 1)/2]r = 1$. Because $r \geq 0$, this equation tells us that $qm \geq 1$, so $q \geq 1/m$. Because $q \leq 1$, this equation also implies that $[m(m - 1)/2]r = qm - 1 \leq m - 1$, from which it follows that $r \leq 2/m$. **29. a)** We purchase the cards until we have gotten one of each type. That means we have purchased X cards in all. On the other hand, that also means that we purchased X_0 cards until we got the first type we got, and then purchased X_1 more cards until we got the second type we got, and so on. Thus, X is the sum of the X_j's. **b)** Once j distinct types have been obtained, there are $n - j$ new types available out of a total of n types available. Because it is equally likely that we get each type, the probability of success on the next purchase (getting a new type) is $(n - j)/n$. **c)** This follows immediately from the definition of geometric distribution, the definition of X_j, and part (b). **d)** From part (c) it follows that $E(X_j) = n/(n - j)$. Thus by the linearity of expectation and part (a), we have $E(X) = E(X_0) + E(X_1) + \cdots + E(X_{n-1}) = \frac{n}{n} + \frac{n}{n-1} + \cdots + \frac{n}{1} = n\left(\frac{1}{n} + \frac{1}{n-1} + \cdots + \frac{1}{1}\right)$. **e)** About 224.46 **31.** $24 \cdot 13^4/(52 \cdot 51 \cdot 50 \cdot 49)$

CHAPTER 7

Section 7.1

1. a) 2, 12, 72, 432, 2592 **b)** 2, 4, 16, 256, 65,536 **c)** 1, 2, 5, 11, 26 **d)** 1, 1, 6, 27, 204 **e)** 1, 2, 0, 1, 3