SOLUTIONS FOR PART II

5. COMBINATORIAL REASONING

5.1. *When rolling n dice, the probability is $1/2$ that the sum of the numbers obtained is even.* There are 6^n equally likely outcomes; we show that in half of them the sum is even. For each of the 6^{n-1} ways to roll the first $n-1$ dice, there are six ways to roll the last die, and exactly three of them produce an even total. Thus there are $6^n/2$ ways to roll an even sum.

5.2. *Probabilities for the sum of two rolled dice.*

k	2	3	4	5	6	7	8	9	10	11	12
probability	$\frac{1}{36}$	$\frac{2}{36}$	$\frac{3}{36}$	$\frac{4}{36}$	$\frac{5}{36}$	$\frac{6}{36}$	$\frac{5}{36}$	$\frac{4}{36}$	$\frac{3}{36}$	$\frac{2}{36}$	$\frac{1}{36}$

5.3. *The numbers x and $14-x$ are equally likely to be the sum of the numbers facing up on two dice.* Whenever i, j are two dice rolls that sum to x, the numbers $7-i$ and $7-j$ are two dice rolls that sum to $14-x$, since $1 \le i \le 6$ implies that $1 \le 7-i \le 6$. Furthermore, the transformation is its own inverse. This establishes a bijection between the set of (ordered pair) dice rolls summing to x and the set of (ordered pair) dice rolls summing to $14-x$, so the two sets are equally likely when the individual ordered pairs are equally likely rolls.

5.4. *There are m^l words of length l from an alphabet of size m, and in $\prod_{i=1}^{l}(l+1-i)$ of them each letter is used at most once.* For each position in the word, a letter must be chosen. When repetitions are allowed, there are m choices at each of the l positions, regardless of earlier choices. When repetitions are forbidden, the number of ways to fill the ith position is $l+1-i$, regardless of how the earlier positions were filled. In each case, multiplying these factors counts the arrangements, by the product rule.

5.5. *Given n married couples, there are $n(n-1)$ ways to form pairs consisting of one man and one woman who are not married to each other.* We must choose one person of each type. Whichever type we choose first, we can choose such a person in n ways. Whichever person we choose, there are $n-1$ person of the opposite sex other than that person's spouse, and we choose one of those.

5.6. *There are $n!$ bijections from an n-element set A to an n-element set B.* List the elements of A in some order, as $\{a_1, \ldots, a_n\}$. The bijection assigns an element of B to each element of A. Furthermore, the assigned elements are distinct. The image of a_1 can be chosen in n ways. For each way to choose this, there are $n-1$ ways to choose the image of a_2. In general, for each way to choose the images of $a_1, \ldots, a_i$, there are $n-i$ ways to choose the image of a_{i+1}. By the product rule, the number of ways to form a bijection is $\prod_{i=0}^{n-1}(n-i)$.

5.7. *There are $12 \cdot 47 + 1 \cdot 48$ ways to pick two cards from a standard 52-card deck such that the first card is a spade and the second card is not an Ace.* There are 13 ways to start with a spade. If the spade is not the Ace, then there are 47 ways to pick the second card, since one non-Ace has been used. If the spade is the Ace, then there are 48 ways to pick the second card. Combining the two cases yields the answer $12 \cdot 47 + 48$

Alternatively, one can name a spade for the first card and a non-Ace for the second card, eliminating the cases where the same card is named twice. This yields $13 \cdot 48 - 12$, which equals the value above.

5.8. *The coefficient of x^4y^5 in the expansion of $(x+y)^9$ is $\binom{9}{4}$*, by the Binomial Theorem. The value is $\frac{9\cdot 8\cdot 7\cdot 6}{4\cdot 3\cdot 2\cdot 1}$, which equals 126.

5.9. *Probabilities in a 5-card hand.* We divide the number of hands with the desired property by $\binom{52}{5}$, the total number of possible hands.

a) Hands having at least three cards with the same rank. If we simply pick three cards of the same rank and then pick two other cards, we might get four of the same rank; such hands would be counted four times. Thus we count the two cases separately. By picking a rank and an extra card, there are $13 \cdot 48$ hands with four of a single rank. For the other case, we pick a rank, leave out one of that rank, and pick two cards of other ranks, in $13 \cdot 4 \cdot \binom{48}{2}$ ways. Thus the answer is $13 \cdot 48(1 + 2 \cdot 47)/\binom{52}{5}$.

b) Hands having at least two cards with the same rank. To the numerator in part (a), we could add on the hands having two but not three from a single rank. Note that we must avoid double-counting the hands having a pair from each of two ranks.

Alternatively, we can subtract from the total the hands having no pair of cards with the same rank. Since we pick five different ranks and one card from each, there are $\binom{13}{5}4^5$ of these, and the answer is $1 - \binom{13}{5}4^5/\binom{52}{5}$. Note that about half of the hands have no repeated ranks, since $\binom{13}{5}4^5/\binom{52}{5} = \frac{52\cdot 48\cdot 44\cdot 40\cdot 36}{52\cdot 51\cdot 50\cdot 49\cdot 48} = .50708$.

5.10. *In $2n$ coin flips, the probability of obtaining exactly n heads is $\binom{2n}{n}/2^{2n}$.* There are 2^{2n} lists of heads and tails, all equally likely. A list with n heads is determined by choosing locations for the n heads in the list. Thus $\binom{2n}{n}$ outcomes have n heads.

When $n = 10$, the value is $(19 \cdot 17 \cdot 13 \cdot 11)/2^{18}$ after cancellation. This equals approximately .176197.

5.11. *The most common difference between the rolls on two dice is 1.* Note that specified unordered pairs of distinct numbers appear in two ways out of 36, while specified pairs of equal numbers appear in only one way. Indexing the rows by the roll of the first die and the columns by the roll on the second die yield the following table of outcomes for the difference. Each position in the table has probability 1/36 of occurring. Collecting those with a particular difference into a single event shows that the differences 0,1,2,3,4,5 occur with probabilities $\frac{6}{36}, \frac{10}{36}, \frac{8}{36}, \frac{6}{36}, \frac{4}{36}, \frac{2}{36}$.

5.12. *The probability that three rolls of a die sum to 11 is* $1/8$. When the first roll is $1, 2, 3, 4, 5,$ or 6, the numbers of ways to throw the other two to reach a total of 11 are $3, 4, 5, 6, 5,$ or 4, respectively. Since each ordered triple occurs with probability $1/6^3$, the answer is thus $27/216$.

5.13. *The probabilities for the number of 6s in four rolls.* When we obtain a 6 exactly k times, there are five choices each for the remaining $4-k$ rolls. We pick the positions for the 6s in $\binom{4}{k}$ ways, and for each there are 5^{4-k} ways to complete the list. Thus the probability is $\binom{4}{k}5^{4-k}/6^4$.

k	0	1	2	3	4
instances	625	500	150	20	1
probability	.4823	.3858	.1157	.0154	.0008

5.14. *Probability of sum n in three selections from $[n]$ is $(n-1)(n-2)/(2n^3)$.* There are n^3 equally likely outcomes. The number of outcomes that sum to n is the number of solutions to $x_1 + x_2 + x_3 = n$ in positive integers.

Proof 1 (selections with repetition). The number of solutions is the number of solutions to $y_1 + y_2 + y_3 = n - 3$ in nonnegative integers. This equals the number of selections of $n-3$ elements from three types with repetition allowed, which is $\binom{n-1}{2}$, by Theorem 5.31. Thus the probability is $(n-1)(n-2)/(2n^3)$.

Proof 2 (summations). When $x_1 = i$, there are $n-i-1$ ways to assign the final two values, since x_2 can then take any value from 1 to $n-i-1$, which determines x_3. Thus the number of solutions is $\sum_{i=1}^{n-2}(n-i-1)$. The summands are the integers from 1 to $n-2$ (in reverse order), so the sum is $(n-1)(n-2)/2$.

5.15. *The size of the union of k pairwise disjoint finite sets $A_1, \ldots, A_k$ is the sum of their sizes.* We use induction on k. Basis step: $k = 1$. The one set A_1 is also the union, and its size is its size.

Induction step: $k > 1$. Let B be the union of $A_1, \ldots, A_{k-1}$. By the induction hypothesis, $|B| = \sum_{i=1}^{k-1} A_i$. Since A_k is disjoint from each of $A_1, \ldots, A_{k-1}$, also $A_k \cap B = \varnothing$. Now Corollary 4.41 states that $|A_k \cup B| = |A_k| + |B|$. Together, these yield $\left|\bigcup_{i=1}^k A_i\right| = \sum_{i=1}^k |A_i|$.

5.16. *The rule of product, from the rule of sum.* In the set T, elements are formed in k steps. Each element of T can be expressed as a k-tuple in which the ith coordinate lists the way in which the ith step is performed. We are given that the ith step can be performed in r_i ways, no matter how the earlier steps are performed. We use induction on k to prove that $|T| = \prod_{i=1}^k r_i$.

Basis step: $k = 1$. The elements of T are the ways to perform the step, so $|T| = r_1$.

Induction step: $k > 1$. We partition T into sets, depending on how the first $k-1$ steps are performed. The given condition implies that each set has size r_k. The induction hypothesis implies that there are $\prod_{i=1}^{k-1} r_i$ sets in the partition. Since each has size r_k, and the sets are pairwise disjoint, the rule of sum implies that $|T| = \prod_{i=1}^k r_i$.

5.17. *The only solution of $n! + m! = k!$ in positive integers is $n = m = 1$ and $k = 2$.* Suppose that $n! + m! = k!$; by symmetry, we may assume that $n \geq m$. Since $m! > 0$, we have $k! > n! \geq m!$. Using the definition of factorial, we divide the equation by $n!$ to obtain $1 + m!/n! = k(k-1)\cdots(n+1)$. Since 1 and $k(k-1)\cdots(n+1)$ are integers, $m!/n!$ must be an integer. Since $m \leq n$, this requires $m = n$. Now we have $2 = k(k-1)\cdots(n+1)$. This requires $n+1 \leq 2$ and $k = n+1$, leaving only the possibility $(n, m, k) = (1, 1, 2)$. This possibility is indeed a solution.

5.18. *Sets of six cards with at least one card in every suit.* The distributions over suits can be 3111 or 2211. In the first case, we pick the suit contributing three cards, pick the three cards, and pick one card from each of the others. In the second case, we pick the two suits contributing two cards, pick two cards from each, and pick one card each from the remaining two suits. In each case, the product rule applies to these choices. Thus the answer is $\binom{4}{1}\binom{13}{3}13^3 + \binom{4}{2}\binom{13}{2}^2 13^2$.

5.19. *Counting 6-digit numbers by the number of distinct digits.* Let k be the number of distinct digits. There are 9 such natural numbers with $k = 1$ (six copies of the same digit).

When $k = 2$, we pick the two digits and choose a sequence with these two digits, excluding the sequences with all of one type. Thus the answer is $\binom{10}{2}(2^6 - 2) = 45 \cdot 62 = 2790$.

When $k = 6$, we are arranging six elements from a set of size 10, so the count is $10 \cdot 9 \cdot 8 \cdot 7 \cdot 6 \cdot 5 = 151200$.

When $k = 5$, we pick the one repeated digit, pick its two positions, and arrange four of the remaining digits in the remaining positions. The count is $10\binom{6}{2} \cdot 9 \cdot 8 \cdot 7 \cdot 6 = 453600$.

When $k = 4$, we might use three of one digit or two each of two digits. In the first case, counting as in the case $k = 5$ yields $10\binom{6}{3} \cdot 9 \cdot 8 \cdot 7 = 100800$. In the second case, we pick the two repeats, pick two positions for each, and arranging two other digits in the remaining positions to get $\binom{10}{2}\binom{6}{2}\binom{4}{2} \cdot 8 \cdot 7 = 226800$. Altogether we have 327600 numbers with $k = 4$.

When $k = 3$, we can pick three numbers and form 6-tuples from that 3-set, subtracting the 6-tuples that don't use all the numbers. For a given three, there are $3 + 3(2^6 - 2)$ bad 6-tuples. Thus the answer is $\binom{10}{3}[3^6 - 3 \cdot 2^6 + 3] = 64800$.

As a check, $9 + 2790 + 64800 + 327600 + 453600 + 151200 = 999999$.

5.20. *$(n^5 - 5n^3 + 4n)/120$ is an integer whenever n is a positive integer.* The numerator of this fraction factors as $(n + 2)(n + 1)n(n - 1)(n - 2)$. For $n \in \{1, 2\}$, the value is 0. For $n > 2$, the numerator is the product of five consecutive natural numbers, so it suffices to show that the product of five consecutive natural numbers is divisible by 120.

Proof 1 (combinatorial proof). The number $(l+4)(l+3)(l+2)(l+1)l/5!$ is the number of ways to choose 5 items from a set of $l + 4$ distinct items. The more general statement that the product of any k consecutive positive integers is divisible by $k!$ follows by the same argument.

Proof 2 (divisibility). A number is divisible by 120 if and only if it is divisible by 5, by 3, and by 2^3. Thus it suffices to show that every product of five consecutive integers has these factors. Since the multiples of an integer t are spaced t apart, five consecutive integers contain exactly one number divisible by 5 and at least one divisible by 3. They also contain at least two numbers divisible by 2, and one of these is divisible by 4. Hence there are at least three powers of 2 in the product. Note that being divisible by 2 and by 4 does not imply that a number is divisible by 8.

Proof 3 (induction and divisibility). We prove by induction on n that $(n + 2)(n + 1)n(n - 1)(n - 2)$ is divisible by 120. The product is 0 when $n = 1$. For the induction step, suppose that the claim holds when $n = m$. To show that $(m + 3)(m + 2)(m + 1)m(m - 1)$ is divisible by 120, we show that this minus $(m+2)(m+1)m(m-1)(m-2)$ is divisible by 120. With the induction hypothesis, we conclude that the claim holds when $n = m + 1$.

The desired difference simplifies to $5(m + 2)(m + 1)m(m - 1)$. Thus it suffices to show that the product of four consecutive integers is divisible by 24. We could apply a divisibility analysis (as in Proof 2) or prove this statement itself by induction. The induction step would reduce to the statement that the product of three consecutive integers is divisible by 6. We could prove this using divisibility or induction, reducing to the statement that the product of two consecutive integers is divisible by 2. If we ever switch to the divisibility approach, then we use an argument like Proof 2.

The reduction to the next induction is always done in the same way. We can combine all the reductions into a single inductive proof (by induction on $k + l$) of the more general statement that the product of k consecutive natural numbers starting with l is divisible by $k!$ (see Exercise 7.21.)

5.21. *There are $\binom{m}{2}\binom{n}{2}$ rectangles of all sizes formed using segments in a grid with m horizontal lines and n vertical lines.* Each such rectangle is determined, uniquely, by choosing two vertical lines and two horizontal lines as boundaries.

5.22. *Every convex n-gon has $\binom{n}{4}$ pairs of crossing diagonals.*

Proof 1 (bijection). The direct proof is that every crossing pair of diagonals is determined by the four endpoints of the two diagonals, and this establishes a bijection from the set of crossing pairs of diagonals to the set of 4-tuples of vertices, since each 4-set of vertices can be matched up in exactly one way to produce a crossing pair of diagonals.

Proof 2 (summations). We count the crossings involving diagonals from one vertex. Let the vertices be $v_1, \ldots, v_n$ in order. The diagonal from v_n to v_k is crossed by $(k - 1)(n - k - 1)$ diagonals not involving v_n. Thus $\sum_{k=1}^{n-1}(k - 1)(n - k - 1)$ crossings involve v_n. This argument is valid for each vertex, so we can sum over the vertices and divide by the number of times each crossing is counted to conclude that the total number of crossings is $\frac{n}{4}\sum_{k=1}^{n-1}(k - 1)(n - k - 1)$. We need the sum

$$\sum_{k=1}^{n-1}(k - 1)(n - k - 1) = \binom{n}{3}$$

(also needed in an inductive proof). One can compute this by writing the summand as a polynomial and applying Propositions 4.7 and 4.16. Exercise 9.11 evaluates a more general sum by a combinatorial argument.

5.23. *Multiplicities of poker hands.*

a) One pair (two cards of equal rank and no others of equal rank). This occurs in $\binom{13}{1}\binom{4}{2}\binom{12}{3}4^3$ ways: pick the special rank, pick two cards from it, pick the three other ranks, pick one card each from those ranks.

b) Full house (two cards of equal rank and three cards of another rank). This occurs in $13 \cdot 12\binom{4}{2}\binom{4}{3}$ ways: pick the two ranks (order matters because the chosen ranks are distinguished by the number of cards they contribute), pick 2 cards from the first rank, pick three cards from the second rank.

c) Straight flush (five cards in sequence from the same suit). A straight flush is determined by choosing a suit and choosing the rank where the 5-card sequence starts. There are four suits and 10 starting values (10 J Q K A is the highest), so there are 40 such hands.

5.24. *Bridge distributions.* The probability of each distibution is the number of such hands divided by the total number of 13-card hands, $\binom{52}{13}$. For each distribution, we list the number of hands and the rank. To count the hands, we first assign the multiplicities to suits, then we choose the specified number of cards from each suit.

The number of ways to assign the multiplicities depends on how many times each multiplicity occurs. With four distinct multiplicities, there are 24 ways to assign them to suits. When three numbers arise (one repeated), as in 5440, there are 12 ways. With three suits of the same multiplicity, as in 4333, there are 4 ways (this is why this distribution ranks so low). Since 13 is odd, there cannot be four suits with the same multiplicity or two pairs with equal multiplicity.

distrib.	# hands	rank	distrib.	# hands	rank
4333	$4\binom{13}{4}\binom{13}{3}^3$	5 (10.5%)	7420	$24\binom{13}{7}\binom{13}{4}\binom{13}{2}\binom{13}{0}$	19 (0.36%)
4432	$12\binom{13}{4}^2\binom{13}{3}\binom{13}{2}$	1 (21.6%)	7510	$24\binom{13}{7}\binom{13}{5}\binom{13}{1}\binom{13}{0}$	23tie (0.11%)
4441	$4\binom{13}{4}^3\binom{13}{1}$	10 (3.0%)	7600	$12\binom{13}{7}\binom{13}{6}\binom{13}{0}^2$	30 (.0056%)
5332	$12\binom{13}{5}\binom{13}{3}^2\binom{13}{2}$	2 (15.5%)	8221	$12\binom{13}{8}\binom{13}{2}^2\binom{13}{1}$	21 (0.19%)
5422	$12\binom{13}{5}\binom{13}{4}\binom{13}{2}^2$	4 (10.6%)	8311	$12\binom{13}{8}\binom{13}{3}\binom{13}{1}^2$	22 (0.12%)
5431	$24\binom{13}{5}\binom{13}{4}\binom{13}{3}\binom{13}{2}$	3 (12.9%)	8320	$24\binom{13}{8}\binom{13}{3}\binom{13}{2}\binom{13}{0}$	23tie (0.12%)
5440	$12\binom{13}{5}\binom{13}{4}^2\binom{13}{0}$	13 (1.2%)	8410	$24\binom{13}{8}\binom{13}{4}\binom{13}{1}\binom{13}{0}$	26 (0.045%)
5521	$12\binom{13}{5}^2\binom{13}{2}\binom{13}{1}$	9 (3.2%)	8500	$12\binom{13}{8}\binom{13}{5}\binom{13}{0}^2$	31 (0.0031%)
5530	$12\binom{13}{5}^2\binom{13}{3}\binom{13}{0}$	14 (0.9%)			
6322	$12\binom{13}{6}\binom{13}{3}\binom{13}{2}^2$	6 (5.6%)	9211	$12\binom{13}{9}\binom{13}{2}\binom{13}{1}^2$	27 (0.018%)
6331	$12\binom{13}{6}\binom{13}{3}^2\binom{13}{1}$	8 (3.4%)	9220	$12\binom{13}{9}\binom{13}{2}^2\binom{13}{0}$	29 (.0082%)
6421	$24\binom{13}{6}\binom{13}{4}\binom{13}{2}\binom{13}{1}$	7 (4.7%)	9310	$24\binom{13}{9}\binom{13}{3}\binom{13}{1}\binom{13}{0}$	28 (0.010%)
6430	$24\binom{13}{6}\binom{13}{4}\binom{13}{3}\binom{13}{0}$	12 (1.3%)	9400	$12\binom{13}{9}\binom{13}{4}\binom{13}{0}^2$	33 (.00097%)
6511	$12\binom{13}{6}\binom{13}{5}\binom{13}{1}^2$	15 (0.71%)	10,1,1,1	$4\binom{13}{10}\binom{13}{1}^3$	34 (.00040%)
6520	$24\binom{13}{6}\binom{13}{5}\binom{13}{2}\binom{13}{0}$	16 (0.65%)	10,2,1,0	$24\binom{13}{10}\binom{13}{2}\binom{13}{1}\binom{13}{0}$	32 (.0011%)
6610	$12\binom{13}{6}^2\binom{13}{1}\binom{13}{0}$	25 (0.072%)	10,3,0,0	$12\binom{13}{10}\binom{13}{3}\binom{13}{0}^2$	35 (.00016%)
7222	$4\binom{13}{7}\binom{13}{2}^3$	17 (0.51%)	11,1,1,0	$12\binom{13}{11}\binom{13}{1}^2\binom{13}{0}$	36 (.000025%)
7321	$24\binom{13}{7}\binom{13}{3}\binom{13}{2}\binom{13}{1}$	11 (1.9%)	11,2,0,0	$12\binom{13}{11}\binom{13}{2}\binom{13}{0}^2$	37 (.000011%)
7330	$12\binom{13}{7}\binom{13}{3}^2\binom{13}{0}$	20 (0.26%)	12,1,0,0	$12\binom{13}{12}\binom{13}{1}\binom{13}{0}^2$	38 (.0000003%)
7411	$12\binom{13}{7}\binom{13}{4}\binom{13}{1}^2$	18 (0.39%)	13,0,0,0	4	39 (6×10^{-10}%)

5.25. *Inductive proof of $\binom{n}{k} = \frac{n!}{k!(n-k)!}$.* The formula holds for $n = 0$ under the convention that the "factorial" of a negative number is infinite. For $n > 1$, we apply Pascal's Formula and the induction hypothesis to obtain

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1} = \frac{(n-1)!}{k!(n-1-k)!} + \frac{(n-1)!}{(k-1)!(n-k)!} = \frac{n-k}{n}\frac{n!}{k!(n-k)!} + \frac{k}{n}\frac{n!}{k!(n-k)!} = \frac{n!}{k!(n-k)!}.$$

5.26. *The binomial theorem by induction on n.* For the basis step, we have $(x + y)^0 = 1 = \binom{0}{0}x^0y^0$. Now suppose that the expansion formula holds when the exponent is n. We consider the summation when the parameter is $n + 1$. The induction hypothesis tells us that $(x + y)^n = \sum_{k=0}^{n}\binom{n}{k}x^ky^{n-k}$. Since we want the expansion for $(x+y)^{n+1}$, we multiply both sides by $(x+y)$.

To simplify the resulting expression, we want want to combine the terms where the exponents on x agree and on y agree. Therefore, we shift the index in the first summation. We then use Pascal's Formula to combine corresponding terms in the two summations. For the terms that don't pair up, we have $\binom{n}{n} = 1 = \binom{n+1}{n+1}$ and $\binom{n}{0} = 1 = \binom{n+1}{0}$, so these become the top and bottom terms of the desired summation. The full computation is

$$\begin{aligned}
(x + y)^{n+1} &= (x + y)\sum_{k=0}^{n}\binom{n}{k}x^ky^{n-k}\\
&= \sum_{k=0}^{n}\binom{n}{k}x^{k+1}y^{n-k} + \sum_{k=0}^{n}\binom{n}{k}x^ky^{n+1-k}\\
&= \sum_{l=1}^{n+1}\binom{n}{l-1}x^ly^{n-(l-1)} + \sum_{k=0}^{n}\binom{n}{k}x^ky^{n+1-k}\\
&= x^{n+1} + \left(\sum_{k=1}^{n}\left[\binom{n}{k-1} + \binom{n}{k}\right]x^ky^{n+1-k}\right) + y^{n+1}\\
&= \sum_{k=0}^{n+1}\binom{n+1}{k}x^ky^{n+1-k}
\end{aligned}$$

This proof is a direct generalization of the computation that obtains the expansion of $(x + y)^3$ from the expansion of $(x + y)^2$, for example.

5.27. *Equality of numbers of even and odd subsets,* by the Binomial Theorem. Let A be the set of even-sized subsets, and let B be the set of odd-sized subsets. The binomial coefficient $\binom{n}{k}$ counts the subsets of n of size k. Thus $|A| = \sum_{i\ge0}\binom{n}{2i}$ and $|B| = \sum_{i\ge0}\binom{n}{2i+1}$. We want to show that $\sum_{i\ge0}\binom{n}{2i} - \sum_{i\ge0}\binom{n}{2i+1} = 0$.

In the expansion $(1 + x)^n = \sum\binom{n}{k}x^k$ from the Binomial Theorem, we can count the sets of even size positively and the sets of odd size negatively by setting $x = -1$. The value of the sum becomes the total number of even subsets minus the total number of odd subsets. Setting $x = -1$ on both sides yields $\sum\binom{n}{k}(-1)^k = (1 - 1)^n = 0$. Thus the number of subsets of each type is the same. When $n = 0$, there is one even subset and no odd subsets, which motivates the convention in combinatorics that $0^0 = 1$.

5.28. *$x_1+\cdots+x_k\le n$ has $\binom{n+k}{k}$ solutions in nonnegative integers.*

Proof 1 (summation). We have counted solutions to $x_1+\cdots+x_k=m$ for each m, the number is $\binom{m+k-1}{k-1}$. Summing this over $0\le m\le n$ and applying the Summation Identity yields a total of $\binom{n+k}{k}$ solutions.

Proof 2 (transformation). Introduce an extra variable x_{k+1}. The desired solutions correspond to nonnegative integer solutions to $\sum_{i=1}^{k+1}x_i=n$. The number of solutions to the transformed equation with $k+1$ variables and sum n is $\binom{n+(k+1)-1}{(k+1)-1}=\binom{n+k}{k}$.

5.29. *The equation $x_1+\cdots+x_k=n$ has $\binom{n-1}{k-1}$ solutions in positive integers.*

Proof 1 (transformation). Solutions in positive integers to $\sum_{i=1}^{k}x_i=n$ correspond to solutions in nonnegative integers to $\sum_{i=1}^{k}y_i=n-k$, since subtracting 1 turns a positive integer into a nonnegative integer, and this is invertible. The model of selections with repetition then says that there are $\binom{(n-k)+k-1}{k-1}=\binom{n-1}{k-1}$ such solutions.

Proof 2 (direct bijection). In the model of dots and bars, each x_i counts the dots between successive bars. If there is at least one dot for each x_i, then the bars must be placed in *distinct* places between dots. Thus there are $n-1$ places in which bars can go, and we choose $k-1$ of them to determine a solution in positive integers.

5.30. *Proof by induction on n that $\sum_{i=0}^{n}\binom{i}{k}=\binom{n+1}{k+1}$ for all $n,k\in\mathbb{N}$.* If $n=1$, then the sum is $\binom{0}{k}+\binom{1}{k}$, which is 1 if $k=1$ and 0 if $k>1$. On the right side, $\binom{2}{k+1}$ is 1 if $k=1$ and 0 if $k>1$. Hence the identity holds when $n=1$. For the induction step, suppose that the identity holds when $n=m-1$ (and all k). For $n=m$, we then have $\sum_{i=0}^{n}\binom{i}{k}=\binom{n}{k}+\sum_{i=0}^{n-1}\binom{i}{k}=\binom{n}{k}+\binom{n}{k+1}=\binom{n+1}{k+1}$, where we have used the induction hypothesis and then Pascal's Formula (the binomial coefficient recurrence) in the last two steps.

5.31. *There are $(2n)!/(2^n n!)$ ways to partition $2n$ distinct people into pairs.*

Proof 1. There are $(2n)!$ ways to put the people in a linear order, and when we do this we can form pairs from the first two, the next two, and so on. However, this counts each partition into pairs exactly $2^n n!$ times, because we don't care which person of a pair is written first, and we don't care what order the pairs are written in.

Proof 2. There are $\binom{2n}{2}\binom{2n-2}{2}\cdots\binom{2}{2}$ ways to pick pairs successively, since the number of ways to pick the next pair doesn't depend on how the previous pairs were chosen. Divide this by $n!$, since all $n!$ orderings of the pairs yield the same partition. Regrouping the factors yields $(2n)!/(2^n n!)$.

Proof 3. There are $\binom{2n}{n}$ ways to pick n people to be assigned to distinct pairs. The remaining n people are paired with them according to some permutation, in $n!$ possible ways. This creates each partition into pairs 2^n

times, because in any subset of the pairs we can switch the choice of which member of the pair was in the original selected set.

Proof 4. Let a_n be the desired value. There are $2n-1$ ways to pair person 1 with another person. Every such choice can be extended to a partition into pairs by pairing up the remaining $2n-2$ people, which by definition can be done in a_{n-1} ways. Thus $a_n=(2n-1)a_{n-1}$ with $a_0=1$ (or $a_1=1$). By induction on n (or iterative substitution), $a_n=\prod_{i=1}^{n}(2i-1)$. Multiplying by 1 in the form $\prod_{i=1}^{n}2i/(2^n n!)$ yields the formula claimed.

5.32. *A combinatorial proof that $n^2=2\binom{n}{2}+n$.* Arrange n^2 dots in an n by n array. Of these, n dots have the same row and column index. For each choice of distinct indices i and j, there are two dots: positions (i,j) and (j,i).

5.33. *Summing the cubes.*

a) $m^3=6\binom{m}{3}+6\binom{m}{2}+m$. Beginning with the right side, we compute $m(m-1)(m-2)+3m(m-1)+m=m^3-3m^2+2m+3m^2-3m+m=m^3$.

b) $\sum_{i=1}^{n}i^3=(\frac{n(n+1)}{2})^2$. Using part (a) and the identity $\sum_{i=0}^{n}\binom{i}{k}=\binom{n+1}{k+1}$, we conclude that

$$\sum_{i=0}^{n}i^3=6\binom{n+1}{4}+6\binom{n+1}{3}+\binom{n+1}{2}=(n+1)n\left[\frac{6}{24}(n-1)(n-2)+\frac{6}{6}(n-1)+\frac{1}{2}\right]$$
$$=\frac{(n+1)n}{4}\left[(n^2-3n+2)+(4n-4)+2\right]=\left[\frac{n(n+1)}{2}\right]^2.$$

c) Combinatorial proof of part (a) by counting a set in two ways. Consider the 3-tuples of numbers, where each number is in $[m]$. There are m triples in which we use only one type of number. There are $6\binom{m}{2}$ triples in which we use two distinct numbers, because there are two ways to pick the value used only once after picking the pair used, and there are three positions in which the value used only once can be placed. Finally, there are $\binom{m}{3}$ ways to pick three values, and there are 6 orders in which the chosen values can be written. Thus the right side of part (a) counts the triples, grouped by how many distinct values are used.

5.34. *The number of cubes of all positive integer sizes formed by an n by n by n assembly of unit cubes is $\binom{n+1}{2}^2$.* In each of the three directions, the coordinates of a cube with sides of length $n+1-i$ can be chosen in i ways. Hence the desired value is $\sum_{i=1}^{n}i^3$ for cubes with positive integer sizes.

Using binomial coefficients, $i^3=6\binom{i}{3}+6\binom{i}{2}+\binom{i}{1}$. By the Summation Identity, $\sum_{i=1}^{n}i^3=6\binom{n+1}{4}+6\binom{n+1}{3}+\binom{n+1}{2}$. Extracting the common factor $(n+1)n$ leaves $\frac{1}{4}[(n-1)(n-2)+4(n-1)+2]$, which equals $(n+1)n/4$.

5.35. *Track meet with k^n contestants.*

a) $k-1$ divides k^n-1. In each group race, $k-1$ of the k runners are eliminated. At the end, k^n-1 of the k^n contestants have been eliminated in the races. Thus $k-1$ divides k^n-1.

b) The meet has $(k^n-1)/(k-1)$ races, since k^n-1 runners lose, and $k-1$ of them lose in each race and are eliminated.

5.36. *Combinatorial proof of $\binom{2n}{n} = 2\binom{2n-1}{n-1}$.* Count the n-subsets of $[2n]$ by whether the element $2n$ is included. If so, then $n-1$ elements must be added from the remaining $2n-1$ elements to complete the set. If not, then $n-1$ more elements must be omitted from the remaining $2n-1$ elements to complete the set left out.

5.37. *If n, k, l are natural numbers with $l \le k \le n$, then $\binom{n}{k}\binom{k}{l} = \binom{n}{l}\binom{n-l}{k-l}$.* Each side counts the set consisting of all possible ways to form, from a set of n people, a committee of size k and a subcommittee of size l within it. The left side groups this set according to the choice of the committee (pick the committee first and then pick the subcommittee from it). The right side groups it according to the choice of the subcommittee (pick the subcommittee first and then fill out the remainder of the committee from the remaining $n-l$ people. Similarly, both sides count the ternary sequences of length n with l twos and $k-l$ ones.

5.38. *A combinatorial proof that $\sum_{k=1}^{n} 2^{k-1} = 2^n - 1$.* The right side counts the nonempty subsets of $[n]$. There are 2^{k-1} such subsets having largest element k, because any subset of the numbers below k can be chosen to accompany it. Hence the left side also counts the nonempty subsets of $[n]$, grouped by the largest element in the subset.

5.39. *A combinatorial proof that $\sum_{k=0}^{n} k\binom{n}{k} = n2^{n-1}$.* The formula on the right counts the ways to choose a committee with chair from a set of n people, by first choosing the chair and then choosing a subset of the remaining people to complete the committee.

The sum on the right counts the same set by the size of the committee. To form a committee with k people, choose the k from the set of n people, and then choose the chair from the committee.

5.40. *A combinatorial proof that $\sum_{i=1}^{n-1} i = \binom{n}{2}$.* The right side counts all pairs of elements from the set $[n]$. When the larger of the two elements is $i+1$, there are i ways to complete the pair. Since every pair has its larger element in the set $\{2, \dots, n\}$, the sum counts all the pairs.

5.41. *A combinatorial proof that $\sum_{i=1}^{n}(i-1)(n-i) = \binom{n}{3}$.* The right side counts all triples of elements chosen from the set $[n]$. We can group these by the index of the middle element. When the middle element is i, we

can complete the triple by choosing one smaller element and one larger element, in any way. Since there are $i-1$ smaller elements and $n-i$ larger elements, the product rule says that the number of triples with i as the middle element. Since every triple has some middle element in $[n]$, the rule of sum then says that the sum on the left equals $\binom{n}{3}$.

5.42. $\sum_{i=0}^{k}\binom{m}{i}\binom{n}{k-i} = \binom{m+n}{k}$. The right side counts the ways to choose k elements from a set of $m+n$ distinct elements. Every such choice selects some number of elements from the first m and the remaining elements from the last n. The number of ways to select i elements from the first m is $\binom{m}{i}$, and the number of ways to select $k-i$ from the last n is $\binom{n}{k-i}$, independently. Hence the number of selections in which there are i elements chosen from the first m is $\binom{m}{i}\binom{n}{k-i}$. Summing over i counts all the selections.

5.43. $\sum_{i=-m}^{n}\binom{m+i}{r}\binom{n-i}{s} = \binom{m+n+1}{r+s+1}$. The right side counts selections of $r+s+1$ elements (without repetition) from $m+n+1$ distinct elements. With the $m+n+1$ elements listed in increasing order, the $r+1$th smallest element must occur at some value, say $m+i+1$ for $-m \le i \le n$. For each such choice of i, the corresponding term on the left counts the ways to choose the r smaller elements and the s larger elements.

Equivalently, the right side counts lattice walks from the origin to the point $(r+s+1, m+n-r-s)$. The left side counts these according to the height at which the step from $x=r$ to $x=r+1$ is made.

5.44. $\sum_{i=0}^{k}\binom{m+k-i-1}{k-i}\binom{n+i-1}{i} = \binom{m+n+k-1}{k}$. The right side counts selections of k elements with repetition allowed from $m+n$ types. The left side groups these by how many, say i, are selected from the first m types. This identity is the selections-with-repetition version of the Vandermonde convolution.

5.45. $\sum_{A\subseteq[n]}\sum_{B\subseteq[n]}|A\cap B| = n4^{n-1}$. Let S be the set of triples (x, A, B) such that $A, B \subseteq [n]$ and $x \in A\cap B$. For each choice of $A, B \subseteq [n]$, there are $|A\cap B|$ ways to choose x to complete a triple in S, so the sum counts S. For each of the n ways to choose an element $x \in [n]$, there are 2^{n-1} choices of A containing x and 2^{n-1} choices of B containing x, so also $|S| = n4^{n-1}$. Since both sides of the formula count S, they are equal.

5.46. $\sum_{S\subseteq[n]}\prod_{i\in S}1/i = n+1$. Consider the product $\prod_{i=1}^{n}(1+1/i)$. The expansion of this product has 2^n terms, since the ith factor can contribute 1 or $1/i$. For each $S \subseteq [n]$, there is a term $\prod_{i\notin S}1\prod_{i\in S}1/i$. Thus the desired sum equals $\prod_{i=1}^{n}(1+1/i) = \prod_{i=1}^{n}\frac{i+1}{i} = n+1$.

5.47. *If $f_m\colon \mathbb{N}\to\mathbb{N}$ is defined by $f_m(n) = \sum_{k=0}^{m}\binom{n}{k}$, then $f_m(n) = 2^n$ when $n \le m$, and this fails when $n = m+1$.* There are $\binom{n}{k}$ subsets of $[n]$ having size k. When this is summed over all k with $0 \le k \le n$, we have counted all subsets of $[n]$, and there are 2^n such subsets. When $k > n$, we have $\binom{n}{k} = 0$, since there are no subsets of $[n]$ with more than n elements. Thus

$$f_m(n) = \sum_{k=0}^{m} \binom{n}{k} = \sum_{k=0}^{n} \binom{n}{k} = 2^n \quad \text{when} \quad n \le m$$
$$f_m(n) = \sum_{k=0}^{m} \binom{n}{k} < \sum_{k=0}^{n} \binom{n}{k} = 2^n \quad \text{when} \quad n > m$$

5.48. *There are $n!$ chains of distinct subsets $A_0, A_1, \dots, A_n$ of $[n]$ su ch that $A_0 \subset A_1 \subset \cdots \subset A_n$.* Distinctness of the subsets requires them to have the distinct sizes $0, 1, \dots, n$. Thus each set adds an element to the previous set, and there are $n!$ orders in which this can be done. If repetitions are allowed, then each element can be added at any step or not at all, so in this case there are $(n+1)^n$ such chains.

5.49. *Parity and inverse for permutations.* The parity of the permutation is the parity of the number of pairs i, j such that $i < j$ and j appears earlier than i (these are *inversions*). To determine the inverse of permutation $a_1, \dots, a_n$, mapping i to a_i, we write the pairs (a_i, i) in increasing order of a_i and then keep only the second coordinate.

permutation	# inversions	parity	inverse
987654321	36	even	987654321
135792468	10	even	162738495
259148637	15	odd	418527963

5.50. *Correcting the labels Apples, Oranges, and Apples / Oranges.* We are told that *all* labels are wrong, so a permutation with no fixed point has been applied to the labels. The correct action is to select one piece of fruit from the bin labeled Apples/Oranges. Since the label is wrong, all fruit in that bin will be the same type as the selected piece; call this type B. A permutation of $[3]$ with no fixed point is a single cycle. Since the Apple/Orange label moved to Type B, it must be that the Type B label moved to the other pure bin, and that label moved to the Apple/Orange bin.

5.51. *When the Drummer Problem is changed by having three drummers who rotate, the final drummer cannot be determined from the initial permutation.* It suffices to present a permutation so that different ways of reaching the identity permutation at the end lead to different answers for the final drummer. When there are three couples, we might start with 321. If there is only one dance before the end, we reach 123 immediately and end with the second drummer. If we instead have three dances before the end, we might move to 231 and 213 before reaching 123 with the first drummer at the end.

5.52. *For $n > 1$, the number of even permutations of $[n]$ equals the number of odd permutations of $[n]$.* Every transposition changes the parity of a permutation. Thus interchanging the first two elements in the word form of the permutation maps the set of even permutations into the set of odd permutations. The map is injective and surjective, since we can obtain an even permutation mapping to a particular odd permutation uniquely by transposing the first two elements of the odd permutation. Thus the map is a bijection, and the two sets has the same size.

5.53. *Every permutation can be sorted using at most $n - 1$ transpositions.* For i from 1 to $n-1$ successively, perform the transposition that switches the element in position i with the element i, unless i is already in position i. After step i, all of $1, \dots, i$ are in their desired positions, and hence the later positions are a permutation of $\{i+1, \dots, n\}$. Thus after $n-1$ steps, the only position left for element n is position n.

The permutation $n\, n-1 \cdots 1$ needs at least $\lfloor n/2 \rfloor$ transpositions for sorting. The number of elements not in their desired positions is n (if n is even) or $n-1$ (if n is odd). Since each transposition places at most two elements into their desired positions, the number of transpositions needed is at least half the number of elements out of place, or $\lfloor n/2 \rfloor$.

5.54. *The minimum number of adjacent transpositions needed to transform a permutation f to the identity permutation is the number of inversions in f (pairs i, j with $i < j$ but i before j). Over all permutations of $[n]$, the maximum of this is $\binom{n}{2}$.* If f is not already sorted, then some adjacent pair of elements is an inversion ($n-1$ increases can only occur if f is $1\,2 \cdots n$). Transposing such an adjacent pair reduces the number of inversions by 1. Hence we can transform f to a permutation with no inversions at most by t transpositions, where t is the number of inversions in f. The only permutation with no inversions is the identity, so this sorts f.

Transposing two adjacent elements reduces the number of inversions by at most 1, so at least t transpositions are needed.

Over permutations of $[n]$, the number of transpositions needed is maximized by maximizing the number of inversions. This occurs when f is $n\, n-1 \cdots 1$, where it equals $\binom{n}{2}$.

5.55. *Bijection from the set A of permutations of $[n]$ to the set B of n-tuples $(b_1, \dots, b_n)$ such that $1 \le b_i \le i$ for each i.* Each permutation $a = a_1, \dots, a_n \in A$ is a list of numbers. For each i, the elements $1, \dots, i$ form a sublist of a. Let b_i be the position of i in the sublist consisting of $1, \dots, i$. Let $f(a)$ be the resulting list $b_1, \dots, b_n$. By construction, $1 \le b_i \le i$, so $f(a) \in B$.

To prove that f is a bijection, we describe a function $g\colon B \to A$. We build $g(b)$ from an empty list by inserting numbers in the order $1, \ldots, n$. Before inserting i, the list consists of $\{1, \ldots, i-1\}$. We insert i to have position b_i. After processing b, we have a permutation of $[n]$.

To prove that f and g are bijections, it suffices to show that they are injective (in fact $g = f^{-1}$), since A and B are finite and have the same size. First consider f. Given distinct permutations in A, there is some least value j such that the subpermutations using elements $1, \ldots, j$ are different (by the Well Ordering Property, since they differ when $j = n$. Since they are the same earlier but differ at the jth step, the corresponding values of b_j are different.

For g, if two elements of B differ first at the jth index ($b_j \neq b'_j$), then the subpermutations of $1, \ldots, j$ in the two image permutations are different.

5.56. *Among positive integers, the inequality $n! > 2^n$ holds if and only if $n \geq 4$.* By explicit computation, the inequality fails when $n \leq 3$, and $4! = 24 > 16 = 2^4$. This provides the basis for a proof by induction that $n! > 2^n$ when $n \geq 4$. For the induction step, suppose that $k! > 2^k$ for some positive integer k. We then have

$$(k+1)! = (k+1)k! > 2 \cdot k! > 2 \cdot 2^k = 2^{k+1}$$

and the inequality holds also when $n = k+1$.

5.57. For $n \in \mathbb{N}$, $\sum_{k=1}^{n} k \cdot k! = (n+1)! - 1$.

Proof 1 (induction on n). When $n = 1$, we have $1 \cdot 1! = 1 = 2! - 1$. For the induction step, suppose that the formula holds when $n = m$. When $n = m+1$, we separate the last term of the sum and apply the induction hypothesis to obtain

$$\begin{aligned} \sum_{k=1}^{m+1} k \cdot k! &= (m+1)(m+1)! + \sum_{k=1}^{m} k \cdot k! \\ &= [(m+2)! - (m+1)!] + [(m+1)! - 1] = (m+2)! - 1 \end{aligned}$$

Thus the formula also holds when $n = m+1$.

Proof 2 (combinatorial argument). The formula $(n+1)! - 1$ counts the permutations of $[n+1]$ except for the indentity permutation. The summation also counts this set, partitioned by letting $k+1$ be the highest value of i such that element i is not in position i. For such a permutation, element $k+2, \ldots, n+1$ are located in positions $k+2, \ldots, n+1$ (one choice only), and elements $1, \ldots, k+1$ are located in positions $1, \ldots, k+1$, forming some permutation of $[k+1]$ such that $k+1$ is not in the last position. To form such a permutation, take a permutation of $[k]$ and insert $k+1$ immediately preceding one of the k elements. There are $k \cdot k!$ ways to do this.

The identity permutation has no element out of place, so it is not counted in this sum. Any other permutation has an element out of place, and k is uniquely defined for it. Thus each non-identity permutation of $[n+1]$ is counted exactly once in the set, as desired.

5.58. *Permutations of* $[4]$ *and* $[5]$ *without fixed points.* Avoiding fixed points means that the cycles in the functional digraph have length at least 2.

With four elements, this requires a single 4-cycle or two 2-cycles. There are six 4-cycles (start at element 1 and visit the other three elements in some order) and there are three permutations consisting of two 2-cycles (pick the mate of one fixed element). The answer is 9.

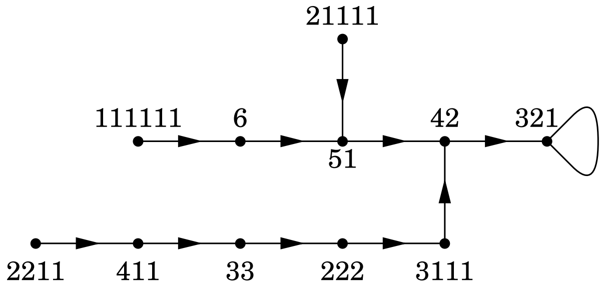
With five elements, we require a single 5-cycle or a 3-cycle and a 2-cycle. There are 24 5-cycles (start at element 1 and visit the other four elements in some order). There are 20 permutations consisting of a 3-cycle and 2-cycle (pick the 2-cycle in 10 ways, and form a 3-cycle on the remaining elements in two ways). The answer is 44.

5.59. *If $f\colon A \to A$, and n, k are natural numbers with $k < n$, then $f^n = f^k \circ f^{n-k}$.* We use induction on n. When $n = 2$, we have $k = 1$, and the formula $f^2 = f^1 \circ f^1$ is the definition of f^2. For the induction step, suppose that the claim is true when $n = m$; we prove that it also holds for $n = m+1$. For $k = 1$, again the definition of iteration yields $f^{m+1} = f^1 \circ f^m$. Now consider $1 < k < n+1$. Using the definition of iteration, the induction hypothesis, the associativity of composition, and the definition of iteration again, we have

$$f^{m+1} = f \circ f^m = f \circ (f^{k-1} \circ f^{m+1-k}) = (f \circ f^{k-1}) \circ f^{m+1-k} = f^k \circ f^{m+1-k}$$

5.60. *The Penny Problem function.* The function f takes a unit from each pile to make a new pile.

a) The functional digraph of f when $n = 6$.



b) The function f is injective and surjective when $n \leq 2$, and it is neither when $n \geq 3$. When $n = 1$, the set has size 1, and f is the identity. When $n = 2$, the set is $\{2, 11\}$, and f transposes the two elements.

When $n \geq 3$, f maps both (n) and $(2, 1, 1, \ldots, 1, 1, 1)$ into the element $(n-1, 1)$. Furthermore, these two elements are distinct when $n \geq 3$, so f is not injective.

When $n \geq 3$, the element $(1, \ldots, 1)$ is not in the image. Since it has only 1s, any element mapping to it has only one pile. The only element with one pile is a pile of n, and its image is $(n-1, 1)$, which is not all 1s.

5.61. *There is a 3-cycle in the functional digraph of $f\colon \mathbb{R} \to \mathbb{R}$ defined by $f(x) = 1/(ax+b)$ for $x \neq -b/a$ and $f(-b/a) = (-1/b) - (b/a)$ if and only if $a + b^2 = 0$.* Such 3-cycles correspond to points x such that $f(f(f(x))) = x$ and that $f(x) \neq x$. The solutions to $x = 1/(ax+b)$ are the solutions to $ax^2 + bx - 1 = 0$ (given that $x \neq -b/a$).

Note that $f(-b/a)$ has been chosen so that $f(f(-b/a)) = -b/a$. This is a 2-cycle and as long as $x \notin \{-b/a, -(a+b^2)/(ab)\}$ we can use the formula $f(x) = 1/(ax+b)$.

Given that $f(x) = \frac{1}{ax+b}$, we have $f(f(x)) = \frac{ax+b}{a+b(ax+b)}$. Now

$$f(f(f(x))) = \frac{1}{a\frac{ax+b}{a+b(ax+b)} + b} = \frac{a + b(ax+b)}{a(ax+b) + ab + b^2(ax+b)}.$$

Setting $x = f(f(f(x)))$ yields $xa(ax+b) + xab + xb^2(ax+b) = a + b(ax+b)$, which simplifies to $x(a+b^2)(ax+b) = a + b^2$. If $a + b^2 \neq 0$, then we obtain $ax^2 + bx - 1 = 0$, which is precisely the condition for $x = f(x)$. Therefore, a 3-cycle can occur only when $a + b^2 = 0$.

When $a + b^2 = 0$, the formula for $f(f(x))$ simplifies to $\frac{ax+b}{abx}$. Applying f again yields

$$f(f(f(x))) = \frac{1}{a\frac{ax+b}{abx} + b} = \frac{bx}{ax + b + b^2x} = x.$$

Therefore, when $a + b^2 = 0$, every point not in $\{0, -b/a\}$ lies on a 3-cycle.

We leave the analysis for $f(x) = \frac{cx+d}{ax+b}$ and $ad \neq bc$ to the reader.

5.62. *Partitions of integers.*

a) The partitions of 6 are 6, 51, 42, 411, 33, 321, 3111, 222, 2211, 21111, 111111.

b) The number of partitions of n with k parts equals the number of partitions of n with largest part k. A partition $l = l_1, l_2, \cdots$ of n can be viewed as n pennies in piles, with the size of each pile being one of the parts. Each pile has a penny at the bottom level; each penny is at level i it there are $i-1$ pennies below it in its pile. If p_i is the number of pennies at level i (this is the same as the number of piles with at least i pennies), then $p_1 \geq p_2 \geq \cdots$. Thus the list $p = p_1, p_2, \cdots$ is also a partition of n. Applying the same procedure to p yields the original partition l. Thus this transformation is a bijection from the set of partitions of n to itself. The partition l has k parts (piles) if and only if the largest part (p_1) in the corresponding partition p is k. Thus the bijection restricts to a partition from the set of partitions of n with k parts to the set of partitions of n with largest part k. Thus these two sets have the same size.

5.63. *The number of partitions of n into distinct parts equals the number of partitions of n into odd parts.* Given a partition of n into distinct parts, we define a corresponding partition of n into odd parts. This map will be a bijection, proving that the two sets have the same size. We use the fact that each positive integer can be expressed in a unique way as an odd number times a power of two.

Let $p = p_1, p_2, \cdots$ be a partition of n into distinct parts. For each p_i, we write $p_i = (2k_i + 1)2^{j_i}$, with k_i and j_i uniquely determined. Form a new partition by including, for each i, 2^{j_i} parts of size $2k_i + 1$. Since these new parts sum to p_i, doing this for each i produces a partition of n into odd parts. Note that distinct parts (such as 10 and 40) may both yield odd parts of the same size (such as two 5's and eight 5's), but the multiplicities of these parts will be different powers of 2.

To invert the map and retrieve the original partition p from a partition of n into odd parts, let l be the number of parts of size $2k+1$. The number l has a unique expression as a sum of powers of 2. For each power of 2 used in the binary expansion of l, combine that many copies of k into a single part for the partition p. When the original transformation is applied to p, the number of copies of $2k+1$ produced is the sum of distinct powers of 2, and the unique binary expansion of l identifies these powers.

5.64. *For $n, k \in \mathbb{N}$, there is exactly one choice of integers $m_1 \ldots m_k$ such that $0 \leq m_1 < m_2 < \cdots < m_k$ and $n = \binom{m_1}{1} + \binom{m_2}{2} + \cdots + \binom{m_k}{k}$ (called the k-nomial representation).*

Proof 1 (strong induction on n). For $n = 0$, the unique solution is $m_i = i - 1$ for $1 \leq i \leq k$. For $n > 0$, let m_k be the largest integer t such that $\binom{t}{k} \leq n$. We claim that combining this with the unique $(k-1)$-representation of $n' = n - \binom{m_k}{k}$ yields the unique k-representation of n.

First, observe that the resulting m_{k-1} in the representation of N is less than m_k. Otherwise, $n' > \binom{m_k}{k-1}$, which yields $n > \binom{m_k}{k} + \binom{m_{k-1}}{k-1} = \binom{m_k+1}{k}$, contradicting the choice of m_k. Thus the numbers we have chosen do form a k-representation of n.

For uniqueness, it suffices to show that m_k is uniquely determined, because the induction hypothesis implies that n' has a unique $(k-1)$-representation to complete the k-representation of n. If we choose a value larger than m_k, then by the choice of m_k we already total more than n. If we choose a value less than m_k, then the most we can get is $\binom{m_k-1}{k}$ from the top term and $\sum_{i=1}^{k-1}\binom{m_k-1-i}{k-i}$ from the lower terms. Thus the total is at most

$$\sum_{i=0}^{k-1}\binom{m_k-1-i}{k-i}=\sum_{i=0}^{k-1}\binom{m_k-1-i}{m_k-1-k}\le\sum_{j=m_k-k}^{m_k-1}\binom{j}{m_k-1-k}=\binom{m_k}{m_k-k}-1<\binom{m_k}{k}$$

Since $n\ge\binom{m_k}{k}$, the bound above prohibits alternative expressions.

Proof 2. (ordinary induction on n). Consider a k-representation of n using $m_1,\dots,m_k$. Let j be the maximum index such that $m_1,\dots,m_j$ are consecutive; either $j=k$ or $m_{j+1}>m_j+1$. We have

$$\sum_{i=1}^{j}\binom{m_1+i-1}{i}=\sum_{i=1}^{j}\binom{m_1+i-1}{m_1-1}=\binom{m_1+j}{m_1}-1=\binom{m_1+j}{j}-1=\binom{m_j+1}{j}-1$$

Thus we obtain a k-representation of $n+1$ by replacing m_j with m_j+1 and setting m_i to $i-1$ for $1\le i<j$. As in the first proof, we must also show uniqueness; this also can be done on the bottom end.

5.65. *Polynomials with rational coefficients that map integers to integers.* Let I be the set of polynomials with this property.

a) If $p,q\in I$ and $n\in\mathbb{Z}$, then $p+q\in I$ and $n\cdot p\in I$. Polynomials are real-valued functions, and we have defined the sum $f+g$ of real-valued functions by adding their values at each point of the domain. Hence $p+q$ maps the integer m to the integer $p(m)+q(m)$, but we also must verify that $p+q$ is a polynomial! Fortunately, if $p(x)=\sum a_ix^i$ and $q(x)=\sum b_ix^i$, then the polynomial $h(x)=\sum(a_i+b_i)x^i$ has the same value as $p+q$ at every point x, so $p+q$ is this polynomial. Similarly, $np(m)$ is an integer, and the function $n\cdot p$ is the same as the polynomial $\sum(n\cdot a_i)x^i$.

b) The polynomials $\binom{x}{j}$ and $\sum_{j=0}^{k}n_j\binom{x}{j}$ belong to I if $\{n_j\}\subseteq\mathbb{Z}$. Note that $\binom{x}{j}=\frac{1}{j!}x(x-1)\cdots(x-j+1)$ is a polynomial; we can obtain the coefficients by multiplying out the factors. If $j=0$, the value of the product with no factors is 1, and this is the polynomial whose value is 0 everywhere. Note that when x is an integer, $\binom{x}{j}$ is a product of integers and hence is an integer. This makes sense, because we recognize $\binom{x}{j}$ as the number of ways to choose j elements from x distinct elements, when x is an integer. Now $\sum_{j=0}^{k}n_j\binom{x}{j}$ is a sum of integer multiples of polynomials in I. By part (a) (and induction on k), the resulting polynomial is also in I.

c) If f is any polynomial of degree k with rational coefficients, then f c an be written in the form $\sum_{j=0}^{k}b_j\binom{x}{j}$, where the b_j's are rational . Let $f=\sum_{j=0}^{k}c_jx^j$. If $k=0$, then $f=c_0\binom{x}{0}$. For $k>0$, we complete the proof by induction on k. Let $b_k=c_kk!$, so that $f(x)-b_k\binom{x}{k}$ is a polynomial of degree at most $k-1$. By the induction hypothesis, we can choose rational numbers $b_0,\dots,b_{k-1}$ so that $f(x)-b_k\binom{x}{k}=\sum_{j=0}^{k-1}b_j\binom{x}{j}$. Since b_k as defined is also a rational number, we have expressed $f(x)=\sum_{j=0}^{k}b_j\binom{x}{j}$ in the desired form.

d) $f\in I$ if and only if $f(x)=\sum_{j=0}^{k}b_j\binom{x}{j}$, where the b_j's are integers. By part (b), we know that any function of this form belongs to I. Conversely, suppose $f\in I$, and let k be the degree of f. By part (c), we know that $f(x)=\sum_{j=0}^{k}b_j\binom{x}{j}$, where the b_j's are rational numbers. We prove that each b_j is in fact an integer, by induction on j. For $j=0$, evaluate f at 0; the result, which is an integer because $f\in I$, also equals $\sum_{j=0}^{k}b_j\binom{0}{j}=b_0$. Hence b_0 must be an integer. For the induction step, assume that $0<r\le k$ and we have proved that $b_0,\dots,b_{r-1}$ are integers. We have $f(r)=\sum_{j=0}^{k}b_j\binom{r}{j}$. The only nonzero terms are those with $j\le r$, so we have $f(r)=\sum_{j=0}^{r}b_j\binom{r}{j}$, or $b_r=f(r)-\sum_{j=0}^{r-1}b_j\binom{r}{j}$. The right-hand side is a sum of products of integers, so b_r is an integer, which completes the induction.

6. DIVISIBILITY

6.1. *The phrase "Let n be relatively prime" makes no sense* because relative primality is considered only for pairs of numbers.

6.2. *When p is a prime number, the integers are relatively prime to p are all integers that are not divisible by p.* Since p has no factors other than itself and 1, the integer multiples of p are the only numbers having a common factor with p other than 1.

6.3. *The numbers relatively prime to* 0 *are* ±1. Since 0 is divisible by every integer, the numbers whose greatest common divisor with 0 is 1 are ±1.

6.4. *If* $\gcd(a,b)=1$*, then* $\gcd(na,nb)=n$.

Proof 1 (integer combinations). By Theorem 6.12, the set of integer combinations of na and nb is the set of multiples of $\gcd(na,nb)$. If k is an integer combination of na and nb, then $k=rna+snb=n(ra+sb)$ for some integers r,s. Thus all integer combinations of a and b are multiples of n. Conversely, each integer multiple tn is an integer combination of a and b, since $\gcd(a,b)=1$ yields r,s such that $ra+sb=1$, and then $tn=t(ra+sb)n=(rtn)a+(stn)b$. Thus the set of integer combinations is the set of multiples of n, and we have $n=\gcd(a,b)$.

Proof 2 (unique prime factorization). In the prime factorization of $\gcd(r, s)$, the exponent on each prime is the minimum of its exponents in the prime factorizations of r and s. On the other hand, the prime factorization of rs sums the exponents in the prime factorizations of r and s. Taking the minimum of the exponents on corresponding primes in na and nb will yield just the prime factorization of n, since the prime factorizations of a and b have no nonzero exponents for corresponding primes.

6.5. *Application of the Euclidean Algorithm to the input* $(5n, 2n)$. The next pair is $(2n, n)$ and then $(n, 0)$, so the greatest common divisor is n.

6.6. *Application of the Euclidean Algorithm to the input* $(n + 1, n)$. The next pair is $(n, 1)$ and then $(1, 0)$, so it takes two steps.

6.7. *61 is an integer combination of 9 and 16 but not of 9 and 15.* Since 3 divides both 9 and 15, the distibutive law implies that all integer combinations of 9 and 15 are divisible by 3, which does not include 61. On the other hand, 9 and 16 are relatively prime, so every integer is an integer combination of them. The combination $61 = (61 \cdot 4)16 - (61 \cdot 7)16$ is found by the method of Example 6.20, but also $61 = 1\dot{1}6 + 5 \cdot 9$.

6.8. *The Euclidean Algorithm.*

a) $\gcd(126, 224) = 14$. The successive pairs in applying the Euclidean algorithm are $(224, 126)$, $(126, 98)$, $(98, 28)$, $(28, 14)$, $(14, 0)$. Working backward, $14 = 98 - 3 \cdot 28$, $28 = 126 - 98$, $98 = 224 - 126$. Thus $14 = 98 - 3(126 - 98) = 4 \cdot 98 - 3 \cdot 126 = 4(224 - 126) - 3 \cdot 126 = 4 \cdot 224 - 7 \cdot 126$.

b) $\gcd(221, 299) = 13$. The pairs are $(299, 221)$, $(221, 78)$, $(78, 65)$, $(65, 13)$, $(13, 0)$. Working backward, $13 = 78 - 65$, $65 = 221 - 2 \cdot 78$, $78 = 299 - 221$. Thus $13 = 78 - 65 = 78 - (221 - 2 \cdot 78) = 3 \cdot 78 - 221 = 3(299 - 221) - 221 = 3 \cdot 299 - 4 \cdot 221$.

6.9. *Solution of Diophantine equations.*

a) $17x + 13y = 200$. Since $gcd(17, 13) = 1$, solutions exist. The Euclidean algorithm computes $17 - 13 = 4$, $13 - 3 \cdot 4 = 1$. Since $13 - 3 \cdot (17 - 13) = 1$, we have $-3 \cdot 17 + 4 \cdot 13 = 1$. Multiplying by 200 yields the solution $x = -600$, $y = 800$. The complete set of solution pairs is $\{(x, y)\colon x = -600 + 13k, y = 800 - 17k, k \in \mathbb{Z}\}$.

b) $21x + 15y = 93$. Solutions exist only if $\gcd(21, 15)$ divides 93. The Euclidean algorithm computes $21 - 15 = 6$ and $15 - 2 \cdot 6 = 3$. Since 3 divides 15 and 21, $\gcd(21, 15) = 3$, and solutions exist. Furthermore, $15 - 2(21 - 15) = 3$, so $21 \cdot (-2) + 15 \cdot 3 = 3$. Multiplying by 31 yields the solution $x = -62$, $y = 93$. To obtain the other solutions, we increase x by the smallest integer n such that $21n$ is a multiple of 15. This will be the least common multiple of 21 and 15, which is $21 \cdot 15/3$. Hence we can alter x by multiples of 5 and y by corresponding multiples of 7. The complete set

of solution pairs is $\{(5n - 62, 93 - 7n)\colon n \in \mathbb{Z}\}$. Any initial pair can be used instead of $(-62, 93)$, such as $(x, y) = (3, 2)$. We used $(-62, 93)$ since it is the pair generated by the algorithm.

c) $60x + 42y = 104$. Since $\gcd(60, 42) = 6$ and 104 is not divisible by 6, there are no integer solutions.

d) $588x + 231y = 63$. Solutions require that the greatest common divisor of 588 and 231 divides 63. From the Euclidean algorithm, we have $\gcd(588, 231) = \gcd(231, 126) = \gcd(126, 105) = \gcd(105, 21) = \gcd(21, 0) = 21$. Since $63 = 3 \cdot 21$, solutions exist. Since $126 = 588 - 2 \cdot 231$, $105 = 231 - 126$, and $21 = 126 - 105$, we can substitute back in to find that $21 = 2 \cdot 588 - 5 \cdot 231$. Thus $588 \cdot 6 + 231 \cdot (-15) = 63$, and $(x, y) = (6, -15)$ is a solution pair. Since $588/21 = 28$ and $231/21 = 11$, the full set of solutions is $\{(6 + 11n, -15 - 28n)\colon n \in \mathbb{Z}\}$. We could also obtain this from the reduced equation $28x + 11y = 3$ after finding $\gcd(588, 231)$.

6.10. *The first ten multiples of 7 end in different digits (in base 10), but those of 8 do not.* The multiples of 7 are 7, 14, 21, 28, 35, 42, 49, 56, 63, with distinct last digits. Since 8 is even, its multiples cannot end in odd digits.

6.11. *Given equal (nonzero) numbers of each type of American coin (pennies, nickels, dimes, quarters, half-dollars) yielding a whole dollar total, the minimum value is \$91. Without pennies, the minimum is \$9. With pennies and nickels omitted, the minimum is \$17.* If there are x of each coin, then the total amount in cents is $x(1 + 5 + 10 + 25 + 50) = 91x$. If this amount is divisible by 100, then x must be divisible by 100, since 91 is relatively prime to 100. Hence the smallest nonzero solution occurs when $x = 100$. If pennies are omitted, then the total is $90x$, and $x = 10$ suffices. If pennies and nickels are omitted, then the total is $85x$, and $x = 20$ is needed.

6.12. *If a parking meter contains the same number of dimes and quarters, totaling a nonzero whole number of dollars, then the minimum number of coins is* If there are k dimes and k quarters, then the total value in cents is $35k$. If the total is a whole number n of dollars, then we require $35k = 100n$, which reduces to $7k = 20n$. Since 7 divides $7k$, it must also divide $20n$. Since 7 and 20 are relatively prime, we conclude that 7 divides n. The smallest positive integer divisible by 7 is 7. This is achievable using 20 dimes and 20 quarters, so the smallest possible number of coins is 40.

6.13. *If a parking meter can hold k quarters, $2k$ nickels, and $4k$ dimes, then the values of k such that the total amount of money is a whole number of dollars are the positive multiples of 4.* If the total is a whole number n of dollars, then $25k + 5(2k) + 10(4k) = 100n$, or $75k = 100n$. This reduces to $3k = 4n$. When n is an integer, this requires that $3k$ is divisible by 4. Since 3 and 4 are relatively prime, this requires $4|k$. Furthermore when $k = 4l$

the total is $300l$, which yields $3l$ dollars. Thus the complete set of solutions for k is the set of positive multiples of 4.

6.14. *If a parking meter accepts only dimes and quarters and has twice as many dimes as quarters, and if the total amount of money is a nonzero whole number of dollars, then the smallest possible number of quarters is 20.* Let n denote the number of quarters present. By hypothesis there are $2n$ dimes, and the total number of cents is $20n + 25n$. The total also equals m dollars, for some positive integer m, so $45n = 100m$. We can reduce this to $9n = 20m$ without changing the set of solutions. Now the right side is divisible by 20, so the left side must also be divisible by 20. Since 20 has no common factors with 9, 20 must divide n. The value $n = 20$ satisfies all requirements, and the minimum possible amount of money is $9.

6.15. *Nine American coins are needed to achieve totals of 1 through 99 cents, but the choice of coins is not unique.* Let i denote a value from 1 to 99 to be expressed as a sum of some number of 1s, 5s, 10s, 25s, and 50s. To obtain all values that are not multiples of 5, at least four 1s are needed. If more than four 1s are used for any i, then having an extra 5 available instead of an extra 1 would still permit a sum of i, so some smallest solution has exactly four 1s.

It now suffices to express the multiples of 5. A single 5 is needed, but if more than one 5 is ever used i, then having an extra 10 instead still permit a sum of i, so some smallest solution has exactly one 5.

Now we need only consider the multiples of 10, having exactly one 5 and four 1s in our smallest solution. Two 10s are now needed to achieve 10 and 20. To achieve 30, we must add another 10 or a 25. Our total is now at most 54, so we will need at least one more coin after that. If we add one 25 and one 50 as these two coins, then we are finished, and we have argued that no smaller number of coins suffices. Our values are 1,1,1,1,5,10,10,25,50.

We can achieve everything else up to 49 by using $30 = 25 + 5$, $35 = 25 + 10$, $40 = 25 + 10 + 5$, and $45 = 25 + 10 + 10$ (plus 1s as needed), and then the higher values can be expressed using the 50.

The solution is not unique, since 1,1,1,1,5,5,10,25,50 also works with the same number of coins, using $20 = 10 + 5 + 5$ and $45 = 25 + 10 + 5 + 5$.

Given the freedom to choose any values, only seven are needed, since 1,2,4,8,16,32,64 can express all numbers through 127. Six coins do not suffice, because there are only 2^6 configurations with six coins (each coin is used or not used in any sum), so only 64 different totals (including 0) can be achieved. Hence seven is the minimum with unrestricted values.

6.16. *If $b, a \in \mathbb{N}$, then exactly one pair (k, r) of nonnegative integers satisfies $0 \le r \le a-1$ and $b = ka+r$.* Fix a, and call a pair (k, r) such that $b = ka+r$ a *representation* of b. We use (strong) induction on b. If $1 \le b < a$, then $(0, r)$ is a representation. Since numbers representable using $k \ge 1$ are at least a,, every representation of b has $k = 0$ and hence requires $r = b$.

If $b \ge a$, then every realization has $k \ge 1$. Thus the realizations of b correspond bijectively to the representations of $b-a$ with the coefficient of a smaller by 1. By the induction hypothesis, there is a unique representation of $b - a$, and hence there is a unique representation of b.

6.17. *For $a, b \in \mathbb{N}$, $\gcd(a + b, a - b) = \gcd(2a, a - b) = \gcd(a + b, 2b)$.* If d divides two numbers, then d also divides their difference and their sum, by the distributive law. Hence $d|(a + b)$ and $d|(a - b)$ imply $d|(2b)$ and $d|(2a)$. Also $d|(2a)$ and $d|(a - b)$ imply $d|(a + b)$, and using this also yields $d|(2b)$. Also $d|(a + b)$ and $d|(2b)$ imply $d|(a - b)$, and using this also yields $d|(2a)$. Thus the three sets of common divisors (and hence the greatest common divisors) are the same.

6.18. *If $\gcd(a, b) = 1$, then $\gcd(a^2, b^2) = 1$, but $\gcd(a, 2b)$ may be 1 or 2.* Squaring doubles each exponent in the prime factorization. If no primes have nonzero exponents in the factorization of both a and b, then doubling the exponents does not change this. Doubling b adds 1 to the exponent on 2 in the prime factorization, so it changes the gcd if a is even and b is odd.

6.19. *If n, k, j are natural numbers with $j \le k \le n$, then $\binom{n}{k}$ and $\binom{n}{j}$ are not relatively prime.* Exercise 5.37states that $\binom{n}{k}\binom{k}{j} = \binom{n}{j}\binom{n-j}{k-j}$ (Both sides count the ways to form, from a set of n people, a committee of size k and a subcommittee of size l within it.)

Since $\binom{n}{j}$ divides the product on the right in part (a), it also divides the product on the left. If $\binom{n}{k}$ and $\binom{n}{j}$ are relatively prime, then on the left $\binom{n}{j}$ must divide $\binom{k}{j}$. This is a contradiction, since $\binom{n}{j}$ is larger than $\binom{k}{j}$.

6.20. *If p and q are relatively prime, then $2\sum_{i=1}^{q-1} \lfloor ip/q \rfloor = (p - 1)(q - 1)$.* The integer points $\{(i, j)\colon 1 \le i \le q - 1$ and $1 \le j \le p - 1\}$ form a rectangle of $(p - 1)(q - 1)$ points. Since $\gcd(p, q) = 1$, none of these points lie on the line from $(0, 0)$ to (q, p), so exactly half of the points lie below the line. The summation counts the points below the line; there are $\lfloor ip/q \rfloor$ of these with horizontal coordinate i.

For arbitrary $p, q \in \mathbb{N}$, the general formula becomes $(p - 1)(q - 1) - \gcd(p, q) + 1$, because the points on the diagonal line are counted twice by doubling the sum. There are $\gcd(p, q)$ such points before the point (q, p).

6.21. *If $x \in \mathbb{R}$, then $\lfloor -x \rfloor = -\lceil x \rceil$.* The greatest integer less than or equal to $-x$ is the first integer that is at least $|x|$ from 0 in the negative direction.

This is the negative of the first integer that is at least $|x|$ from 0 in the positive direction, which is $\lceil x \rceil$.

If $x \in \mathbb{Z}$ and $n \in \mathbb{N}$, then $\lceil x/k \rceil = \lfloor (x + k - 1)/k \rfloor$. Let $z = \lceil x/k \rceil$; we show that $\lfloor (x + k - 1)/k \rfloor = z$. If $\lceil x/k \rceil = z$, then $z - (k - 1)/k \le x/k \le z$, since the integer x must be a multiple of $1/k$ that is bigger than $z - 1$. Adding $(k-1)/k$ to both inequalities yields $z \le (x+k-1)/k \le z+(k-1)/k < z + 1$. Thus $(x + k - 1)/k \in [z, z + 1)$, and $\lfloor (x + k - 1)/k \rfloor = z$.

It follows also that $\lfloor x/k \rfloor = \lceil (x - k + 1)/k \rceil$ by applying the above statement about $\lceil y/k \rceil$ when $y = x - k + 1$.

6.22. *The integer k is at least 3 and satisfies $(k - 2)|(2k)$ if and only if $k \in \{3, 4, 6\}$.* By direct computation, the numbers 3, 4, 6 satisfy the requirements. The condition $(k - 2)|(2k)$ is equivalent to $\gcd(k - 2, 2k) = k - 2$. One step of the Euclidean algorithm yields the pair $(k + 2, k - 2)$. If $k \ge 6$, then the next pair is $(k-2, 4)$, and thereafter the gcd will be less than $k-2$ unless $k - 2 = 4$. For $k < 6$, we test the possibilities 3, 4, 5 for k.

6.23. *If $p > 0$ and $\{p, p + 2, p + 4\}$ are all prime, then $p = 3$.* The numbers $p, p+2, p+4$ belong to distinct congruence classes modulo 3. Hence exactly one of them is divisible by 3. Hence if all three numbers are prime, then 3 is in the set. Since 1 by definition is not a prime number, the only case in which all three are prime is $\{3, 5, 7\}$.

6.24. *Divisibility properties for functions on $\mathbb{N}$.*

a) 3 divides $4^n - 1$. **Proof 1** (induction). For $n = 1$, we have $4 - 1 = 3$. Suppose that the claim holds when $n = k$. By the induction hypothesis, 3 divides $4^k - 1$, which means that we can write $4^k - 1 = 3r$ for some integer r. Now we compute $4^{k+1} - 1 = 4(4^k) - 1 = 4(3r + 1) - 1 = 12r + 3 = 3(4r + 1)$. We have written $4^{k+1} - 1$ as a multiple of 3 also, which completes the induction step.

Proof 2 (geometric sum). Always $\sum_{i=0}^{n-1} q^i = (q^n - 1)/(q - 1)$. For $q = 4$, the left side is an integer, and thus the right side also must be an integer. Thus $4^n - 1$ is divisible by 3.

b) 6 divides $f(n) = n^3 + 5n$. **Proof 1** (induction). For $n = 1$, we have $f(1) = 1 + 5 = 6$. Suppose that the claim holds when $n = k$. By the distributive law, showing that $f(k + 1) - f(k)$ is divisible by 6 will yield the claim also for $n = k + 1$. Let $g(n) = f(n + 1) - f(n)$; we compute $g(n) = 3n^2 + 3n + 6$. This is divisible by 3. If it is also divisible by 2, then it will be divisible by 6. If n is even, then every term of $g(n)$ is even. If n is odd, then both $3n^2$ and $3n$ are products of odd numbers, so $g(n)$ is odd plus odd plus even and is even. In each case, we have the desired result.

Proof 2 (prime factors). Since 6 divides $6n$, by the distributive law it suffices to show that 6 divides $n^3 - n$. Observe that $n^3 - n = (n + 1)n(n - 1)$. Since three consecutive integers always contain an even number and a multiple of 3, the product is divisible by 6.

6.25. *If $a_1 = 1$, $a_2 = 1$, and $a_{n+1} = a_n + 2a_{n-1}$ for $n \ge 2$, then a_n is divisible by 3 if and only if n is divisible by 3.* We use induction on the subscript. For the basis step, we have $a_1 = 1$, $a_2 = 1$, $a_3 = 3$, as desired. We need to verify three values in the basis step, because the induction step uses the value three before in its hypothesis. For the induction step, it suffices to prove that for $n \ge 1$, the number a_{n+3} is divisible by 3 if and only if a_n is divisible by 3. We have $a_{n+3} = a_{n+2} + 2a_{n+1} = 3a_{n+1} + 2a_n$. Since $3a_{n+1}$ is divisible by 3 and 2 is not divisible by 3 and 3 is prime, we conclude the desired statement.

6.26. *If $n \in \mathbb{N}$, then $(n - 1)^3 + n^3 + (n + 1)^3$ is divisible by 9.*

Proof 1 (multiples of 3). Expanding the summands yields $3n^3 + 6n$, which is divisible by 3. Hence it suffices to show that 3 also divides $n^3 + 2n$. This differs by a multiple of 3 from $n^3 - n$, which equals $(n+1)n(n-1)$. Since three consecutive integers include a multiple of 3, the product is divisible by 3, and the original number is divisible by 9. (There is also a somewhat tedious proof by iterated induction.)

Proof 2 (remainders). In every set of three consecutive natural numbers, one number is a multiple of 3, and the other two are one above and one below multiples of 3. The cube of the multiple of 3 is divisible by 9, so it suffices to show that the sum of the other two cubes is divisible by 9. More generally, we show that the sum of the cubes of $3k - 1$ and $3l + 1$ is divisible by 9 for all integers k, l. We have $(3k - 1)^3 + (3l + 1)^3 = 27k^3 - 27k^2 + 9k - 1 + 27l^3 + 27l^2 + 9l + 1$. After canceling $-1 + 1$, all remaining terms are divisible by 9, so the claim holds.

Proof 3 (induction). For $n = 1$, the sum equals 9, which is divisible by 9. Suppose that the claim holds when $n = k$. It then suffices to prove that the difference between the sum for $n = k + 1$ and the sum for $n = k$ is divisible by 9. This difference is $(k+2)^3 - (k-1)^3$, which equals $9k^2 + 9k + 9$ and has 9 as a factor.

6.27. *The function $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ defined by $f(x, y) = 3^{x-1}(3y - 1)$ is not surjective.* The number 1 is not achievable using any x, y. If 1 is the product of two natural numbers, they must both equal 1, but $3y - 1$ cannot equal 1 for any natural number y.

6.28. *If $\gcd(a, b) = 1$, and $a|n$ and $b|n$, then $ab|n$.* Consider the prime factorizations of n, a, b. The hypotheses imply that the factorizations of a and b use distinct prime factors of n, with powers no greater than in the factorization of n. Hence the product of all the prime factors of a and b, with their multiplicities in those factorizations, still divides n.

6.29. *The product of the least common multiple and greatest common divisor of a and b is $a \cdot b$.* For each prime p_i, let the exponents of p_i in the prime factorization of a and b be a_i and b_i, respectively. Let $d = \gcd(a, b)$ and $m = \operatorname{lcm}(a, b)$. Since d is the gcd, the exponent of p_i in the prime factorization of d must be $\min\{a_i, b_i\}$, and similarly the exponent of p_i in the prime factorization of m must be $\max\{a_i, b_i\}$. Thus the sum of the exponents in the prime factorizations of d and m is $a_i + b_i$. This means that the exponent on each prime in the prime factorization of $d \cdot m$ is the same as the exponent on that prime in the prime factorization of $a \cdot b$.

6.30. $(2n)!/(2^n n!)$ *is an odd number.* The computation below shows that $(2n)!$ equals $2^n n!$ times an odd number.

$$(2n)! = \prod_{i=1}^{n}(2i)\prod_{i=1}^{n}(2i-1) = 2^n \prod_{i=1}^{n} i \prod_{i=1}^{n}(2i-1) = 2^n n! \prod_{i=1}^{n}(2i-1).$$

The ratio also counts the ways to place $2n$ people into pairs, which is the product of the first n odd numbers, $\prod_{i=1}^{n}(2i-1)$, proved by induction on n.

6.31. *Divisibility properties of integer solutions to $a^2 + b^2 = c^2$.*

a) At least one of $\{a, b\}$ is even. We use proof by contradiction. Consider a solution with a, b both odd. Now a^2, b^2 are both odd, and $a^2 + b^2$ is even. This makes c^2 even, which requires c even. Hence c^2 is divisible by 4. Since a, b are odd, we can write $a = 2k + 1$ and $b = 2l + 1$ for some integers k, l. We compute $a^2 + b^2 = (2k + 1)^2 + (2l + 1)^2 = 4k^2 + 4k + 4l^2 + 4l + 2$. This number is not divisible by 4, contradicting our conclusion that $4|c^2$.

b) If c is divisible by 3, then a and b are both divisible by 3. Consider a solution with c divisible by 3. If a or b is divisible by 3, then by the distributive property the other must also be divisible by 3. Hence both are divisible by 3 or neither is divisible by 3. If an integer is not divisible by 3, then its square is one more than a multiple of 3, since $(3k-1)^2 = 9k^2-6k+1$ and $(3k+1)^2 = 9k^2+6k+1$. Hence if neither of a, b is a multiple of 3, then a^2+b^2 is 2 more than a multiple of 3 (by the distributive property). This is impossible, since we have assumed that their sum is divisible by 3. Hence a, b must both be divisible by 3.

6.32. *All but one jelly bean can be extracted if and only if the difference between the amounts x, y in the two jars is not a multiple of 3.* (Pressing the lever of a jar with at least two beans extracts one bean and moves another to the other jar). Experimentation with small examples suggests the stated conjecture: winning positions include (1,0), (2,0), (2,1), and losing positions include (1,1), (3,0). These verify the statement when $x + y$ is at most 3.

We use induction on $x + y$ to complete the proof. Each move decreases the sum by one, so it suffices to prove that making a move does not change whether the two numbers differ by a multiple of three. Starting with (x, y) leads next to $(x + 1, y - 2)$ or $(x - 2, y + 1)$. The difference between the two numbers changes by three, so the claim holds.

6.33. *If abc is a 3-digit natural number (in base 10), then the 6-digit number $abcabc$ has at least three distinct prime factors.* Since $abcabc = 1001 \cdot abc$, it suffices to show that 1001 has three distinct prime factors. In fact, $1001 = 7 \cdot 11 \cdot 13$.

6.34. *The set of prime numbers is not finite.* Suppose that the set S of prime numbers is finite. Let N be the product of the numbers in S. Since N is divisible by each number in S and these numbers are at least 2, $N + 1$ is not divisible by any of them. Since the smallest factor of $N + 1$ that is greater than 1 is a prime number, there is some prime number not in S. The contradiction implies that S is not finite.

6.35. *Construction of a set of n consecutive positive integers that are not prime.* Let $x = (n + 1)! + 2$. Since $(n + 1)!$ is divisible by all of $2, \ldots, n + 1$, we have $(n + 1)! + i$ divisible by i for $i \in \{2, \ldots, n + 1$. These are the n consecutive numbers $x, x + 1, \ldots, x + n - 1$.

6.36. *Primes and factorials.*

a) The exponent of a prime p in the prime factorization of $k!$ is $\lfloor k/p \rfloor + \lfloor k/p^2 \rfloor + \lfloor k/p^3 \rfloor + \cdots$. The exponent is the number of times p appears in the factorization. We write the prime factorization as $k! = \prod p_i^{a_i}$ and compute each a_i. Every pth natural number is divisible by p, so there are $\lfloor k/p \rfloor$ multiples of p as factors in $k!$. However, each multiple of p^2 contributes an extra factor of p, and there are $\lfloor k/p^2 \rfloor$ multiples of p^2 as factors in $k!$. Now each multiple of p^3 contributes yet another factor, etc. The last (nonzero) term in the sum corresponds to the largest power of p that is at most k.

In particular, the exponent of 5 in the prime factorization of 250! is 62, since $\lfloor 250/5 \rfloor + \lfloor 250/25 \rfloor + \lfloor 250/125 \rfloor = 50 + 10 + 2$.

b) The product of any k consecutive natural numbers is divisible by $k!$. To show that a number is divisible by $k!$, it suffices to show that the number has at least as many copies of each prime in its factorization as $k!$ does. If we take k consecutive numbers, we obtain at least $\lfloor k/p \rfloor$ multiples of p (maybe one extra if we start just below a multiple of p). As above, we also get at least $\lfloor k/p^2 \rfloor$ extra contributions for multiples of p^2, and so on. Because this is true for each prime p, we have as many factors of each p in the product of k consecutive numbers as in the product $k!$.

c) Combinatorial proof of (b). The product of the k consecutive natural numbers $n(n+1)\cdots(n+k-1)$ is exactly $k!$ times $\binom{n}{k}$, the number of ways to choose a subset of size k from a set of size $n + k - 1$. Since $\binom{n}{k}$ is an integer, $n(n + 1)\cdots(n + k - 1)$ is divisible by $k!$.

6.37. *Inductive proof of Fermat's Little Theorem.* Let p be a prime number.

a) If $1 \le i \le p-1$, then $\binom{p}{i}$ is divisible by p. **Proof 1** (prime factorization). The binomial coefficient $\binom{p}{i}$ is an integer m; consider its prime factorization. In the formula $m = p!/[i!(p-i)!]$, the factors in the denominator must cancel with some of those in the numerator to leave an integer. The factor p in the numerator cannot be canceled by any of those in the denominator, because they are all natural numbers less than p, and p is not divisible by any natural number except itself and 1.

Proof 2 (properties of primes). We have $m = p(p-1)\cdots(p-i+1)/i!$. Hence p divides $m \cdot i!$. Since p is prime, p therefore divides m or $i!$. If p divides $i!$, then it must divide some number between 1 and i, which cannot happen when $i < p$. Hence p must divide m, as desired.

b) If $n \in \mathbb{N}$, then $n^p - n$ is divisible by p. We use induction on n. For $n = 1$, $n^p - n = 0$, which is divisible by p. For the inductive step, suppose $n^p - n$ is divisible by p. Then $(n+1)^p - (n+1) = \sum_{i=0}^{p} \binom{p}{i} n^i - (n+1) = (n^p - n) + \sum_{i=1}^{p-1} \binom{p}{i} n^i$. By the induction hypothesis and part (a), both $n^p - n$ and the terms in the sum are divisible by p, so the total is divisible by p, as desired.

6.38. *If x, y, k are nonnegative integers and k is not a power of 2, then $x^k + y^k$ is not prime.*

If $k = lm$ with l odd and m an integer, then $x^k + y^k = (x^m)^l - (-y^m)^l$. Because we know the factorization $u^l - v^l = (u-v)(\sum_{i=1}^{l} u^{l-i} v^{i-1})$, we can let $u = x^m$ and $v = -y^m$ and write $x^k + y^k = (x^m + y^m)(\sum_{i=1}^{l} x^{m(l-i)} y^{m(i-1)} (-1)^{i-1})$.

If $l > 1$, this expresses $x^k + y^k$ as the product of two other integers, so it proves that $x^k + y^k$ is not prime, except in the special case that $l = k$ and $x + y = 1$. However, this case cannot occur when x and y are both nonnegative unless $\{x, y\} = \{1, 0\}$, in which case $x^k + y^k = 1$, which we do not consider prime. There is one other exception: if $x = y = 1$, then $x^k + y^k = 2$, which is prime.

If $2^n + 1$ is prime and n is not a power of 2, then n is prime. In the special case $x = 2$, $y = 1$, $k = n$, the contrapositive of the statement proved above is that if $2^n + 1$ is prime, then n is a power of 2.

6.39. *If $2^n - 1$ is prime, then n is prime.* We prove the contrapositive. If n is not prime, then $n = a \cdot b$, where a, b both are greater than 1 and less than n. Since $y^{a \cdot b} = (y^a)^b$, the identity $x^b - 1 = (x-1)\sum_{i=0}^{b-1} x^i$ yields

$$2^{a \cdot b} - 1 = (2^a - 1)(2^{a(b-1)} + 2^{a(b-2)} + \cdots + 2^a + 1).$$

Since $a > 1$, we have $2^a - 1 > 1$. Since $b > 1$, the second factor has at least two terms, so it also exceeds 1. Thus we have expressed $2^n - 1$ as a product of two natural numbers greater than 1, proving that $2^n - 1$ is not prime.

6.40. *If $2^n - 1$ is prime, then $2^{n-1}(2^n - 1)$ is perfect (equal to the sum of its proper divisors).* With $2^n - 1$ being prime, the proper divisors are $\{2^k\colon 0 \le k \le n-1\}$ and $\{2^k(2^n - 1)\colon 0 \le k \le n-2\}$. Summing them yields

$$2^{n-1} + [1 + (2^n - 1)] \sum_{k=0}^{n-2} 2^k = 2^{n-1} + 2^n(2^{n-1} - 1) = 2^{n-1}(2^n - 1).$$

6.41. *Pólya's proof for infinitude of primes.* Let $a_n = 2^{2^n} + 1$.

If $n < m$, then a_n divides $a_m - 2$. We use induction on m for fixed n. Note that

$$a_m - 2 = \left(2^{2^{m-1}}\right)^2 - 1 = \left(2^{2^{m-1}} + 1\right)\left(2^{2^{m-1}} - 1\right)$$

If $m = n + 1$, then the first factor in the product is a_n; this completes the basis step. If $m > n + 1$, then by the induction hypothesis, a_n divides the second factor; this completes the induction step.

a_n and a_m have no common factors if $n \ne m$. We may assume that $n < m$. Since a_n divides $a_m - 2$, every common factor divides 2. Since a_n is odd, this means there is no common integer factor larger than 1.

There are infinitely many primes. Each a_m has a prime factor that is not in the set of prime factors of $\{a_1, \ldots, a_{m-1}\}$. Hence there is no bound on the number of primes obtained in this way.

6.42. *Last digits in base 10 representations.* Let $f(n)$ be the number of distinct last digits in the base 10 representations of multiples of n.

last digit	last digit of kn, where $k =$	
of n	1 2 3 4 5 6 7 8 9 10	$f(n)$
1	1 2 3 4 5 6 7 8 9 0	10
2	2 4 6 8 0 2 4 6 8 0	5
3	3 6 9 2 5 8 1 4 7 0	10
4	4 8 2 6 0 4 8 2 6 0	5
5	5 0 5 0 5 0 5 0 5 0	2
6	6 2 8 4 0 6 2 8 4 0	5
7	7 4 1 8 5 2 9 6 3 0	10
8	8 6 4 2 0 8 6 4 2 0	5
9	9 8 7 6 5 4 3 2 1 0	10
0	0 0 0 0 0 0 0 0 0 0	1

6.43. *Alternative algorithm for gcd.* Let a and b be positive integers that are not both even. When one of $\{a, b\}$ is even and positive, divide it by 2. When a, b are both odd, replace the larger number by the difference. When one number becomes 0, the other number is the gcd of the original pair.

We use induction on the sum of the numbers, but we include all pairs $(n, 0)$ in the basis. For these numbers, the algorithm correctly reports that the gcd is n. For pairs with both numbers nonzero, the induction hypothesis tells us that the algorithm terminates when applied to the next pair and correctly reports its gcd. Thus it suffices to show that the gcd for the original pair is the same as the gcd for the new pair.

Consider the pairs $(2k, 2l + 1)$ and $(k, 2l + 1)$. Neither pair has 2 as a common divisor, since $2l + 1$ is odd. An odd number divides $2k$ if and only if it divides k. Thus the common divisors of the two pairs are the same.

Consider the pairs (a, b) and (b, c), where $c = a - b$. By manipulating the equality and applying the distributive law, if a number divides two of $\{a, b, c\}$, then it also divides the third. Thus again the two pairs have the same common divisors.

Since the operations applied do not change the set of common divisors, they do not change the least common divisor.

6.44. *An inductive procedure for computing the q-ary representation of n.*

1) If $1 \le n \le q - 1$, then the q-ary expansion of n is $a_0 = n$.

2) If $n \ge q$, then let $n = kq + r$, where r is an integer in $\{0, \dots, q - 1\}$, and let $b_m, \dots, b_0$ be the q-ary expansion of k. The q-ary expansion of n is $a_{m+1}, \dots, a_0$, where $a_0 = r$ and $a_i = b_{i-1}$ for $i > 0$.

We use induction on n. When $n < q$, the representation with n alone in the last place has value n. When $n \ge q$, we are given $\sum_{i=0}^{m} b_i q^i = k$, where $n = kq + r$. By construction, we have $0 \le a_i \le q - 1$, so it suffices to show that the representation evaluates to n. We have

$$\sum_{i=0}^{m+1} a_i q^i = a_0 + q \sum_{i=1}^{m+1} b_{i-1} q^{i-1} = r + qk = n.$$

Computation of base 5 representation of 729. Since $729 = 145 \cdot 5 + 4$, we append 4 to the base 5 representation of 145. Since $145 = 29 \cdot 5 + 0$, we append 0 to the base 5 representation of 29. Since $29 = 5 \cdot 5 + 4$, we append 4 to the base 5 representation of 5. Since $5 = 1 \cdot 5 + 0$, we append 0 to the base 5 representation of 1. Since $1 \le 5 - 1$, we use 1 as the base 5 representation of 1. Hence the base 5 representation of 729 is $10404_{(5)}$.

6.45. *Given 500 seven-ounce weights, 500 thirteen-ounce weights, and a balance scale, an object can be tested for weighing 500 ounces.* The question is whether 500 can be expressed as an integer combination of 7's and 13's without using more than five hundred of either. The coefficients can be positive or negative according to whether the known weights are put on the same side or the opposite side of the balance as the unknown weight.

Solutions to $7x + 13y = 500$ exist, since 7 and 13 are relatively prime. The Euclidean algorithm yields an expression for 1, via $13 - 7 = 6$, $7 - 6 = 1$, so $1 = 7 - (13 - 7) = 7(2) - 13(1)$. Hence 500 of the 13-ounce weights on the same side as the unknown weight and 1000 of the 7-ounce weights on the opposite side will balance.

However, we do not have 1000 7-ounce weights. We can cancel thirteen 7-ounce weights with seven 13-ounce weights enough times to reduce the coefficients below 500. For example, canceling 650 7-ounce weights with 350 13-ounce weights leads to $(350)7 - (150)13 = 500$.

If the weights are six-ounce and nine-ounce weights, then only multiples of 3 can be balanced, which doesn't include 500.

6.46. *There are four solutions to $70x + 28y = 518$ in positive integers.* We first divide the equation by 14 to obtain the reduced equation $5x + 2y = 37$ with the same set of solution pairs. Since $5(1) + 2(-2) = 1$, there is a solution with $x = 37$ and $y = -74$. Since $\gcd(5, 2) = 1$, the full set of integer solutions is $\{(x, y)\colon x = 37 - 2k, y = -74 + 5k, k \in \mathbb{Z}\}$.

In order to have both coordinates of the solution positive, we need $37 - 2k > 0$ and $-74 + 5k > 0$, which requires $14.8 < k < 18.5$. Thus we obtain positive solutions precisely when $k \in \{15, 16, 17, 18\}$. The resulting solutions are $\{(7, 1), (5, 6), (3, 11), (1, 16)\}$.

6.47. *Integer solutions to $\frac{1}{60} = \frac{x}{5} + \frac{y}{12}$.* Clearing fractions yields $1 = 12x + 5y$, which has the solution $(x, y) = (-2, 5)$. Since $\gcd(12, 5) = 1$, the full set of integer solutions is $\{(x, y)\colon x = -2 + 5k, y = 5 - 12k, k \in \mathbb{Z}\}$.

6.48. *Integer solutions to $ax + by = c$ when $a, b, c \in \mathbb{Z}$ and $\gcd(a, b)$ divides c.* Let $d = \gcd(a, b)$. The integer solutions to $ax + by = c$ are also the integer solutions to $(a/d)x + (b/d)y = (c/d)$. The hypothesis implies that $a/d, b/d, c/d$ are all integers, and therefore we can apply the methods of diophantine equations to find the integer solutions to the new equation.

Since a/d and b/d are relatively prime, there are integers m, n such that $m(a/d) + n(b/d) = 1$. We obtain one solution (x_0, y_0) by setting $x_0 = m(c/d)$ and $y_0 = n(c/d)$. The set of integer solutions is then $\{(x_0 + kb/d, y_0 - ka/d)\colon k \in \mathbb{Z}\}$, again because a/d and b/d are relatively prime.

6.49. *Pocketfuls of t pennies/nickels/dimes with value s cents.* Let a, b, c be the multiplicities of the three types. Multiple solutions a, b, c and a', b', c for smallest s will not both have positive amounts of the same type of coin, since coins could be canceled to obtain a smaller multiple solution. Converting dimes into pennies and nickels increases the number of coins, and converting pennies into nickels and dimes decreases the number.

Hence the minimal multiple solution arises by converting nickels into the same total number of pennies and dimes. We require $5b = a' + 10c'$ and $b = a' + c'$, which becomes $4b = 9c'$. We can convert 9 nickels into 4 dimes and 5 pennies. Since $\gcd(4, 9) = 1$, there is no smaller solution, and the answer is $s = 45$.

6.50. *A "reciprocal" dart board problem.*

a) There are no natural numbers m and n such that $7/17 = 1/m + 1/n$. If they exist, then the larger of $1/m$ and $1/n$ must exceed $7/34$ but be less than $7/17$. Thus $3 \le \min\{m, n\} \le 7$. For $m \in \{3, 4, 5, 6, 7\}$, the value $7/17 - 1/m$ is not the reciprocal of an integer, so there is no solution.

b) If p is prime, then the values k for which there exist $m, n \in \mathbb{N}$ such that $\frac{k}{p} = \frac{1}{m} + \frac{1}{n}$ are $2p$, p, 2, 1, and all divisors of $p+1$. Writing the equation as $kmn = p(m + n)$, we conclude that p divides at least one of $\{k, m, n\}$. If $p|k$, then k/p is an integer, and $k/p \le 2$ since m and n are integers; the two possibilities are achieved by $(m, n) = (1, 1)$ and $(m, n) = (2, 2)$. If $p|m$ and $p|n$, then $k = 1/a + 1/b$ for some $a, b \in \mathbb{N}$, which implies $k \le 2$. We can achieve $k = 2$ by $(m, n) = (p, p)$ and $k = 1$ by $(m, n) = (2p, 2p)$. In the remaining cases, we may assume that p divides m but not n or k.

Suppose $m = ap$. From $kapn = p(ap + n)$, we obtain $(ka - 1)n = ap$. Hence $p|(ka - 1)$; let $ka - 1 = bp$. Now $nbp = ap$, which implies $nb = a$. The original equation becomes $knbpn = p(nbp + n)$, which reduces to $knb = bp + 1$. Since these are multiples of b, we obtain $b = 1$. Now $kn = p + 1$, which implies $k|(p + 1)$. Furthermore, setting $(m, n) = (p\frac{p+1}{k}, \frac{p+1}{k})$ makes any such k achievable.

6.51. *The Coconuts Problem.* Let $x - 4$ be the original number of coconuts. Since $x - 5$ is divisible by 5, also x is divisible by 5. The amount remaining for the second sailor is $(4/5)(x - 5) = (4/5)x - 4$ is the amount for the second sailor. Since he also discards one, we conclude that $(4/5)x$ is divisible by 5, and $(4/5)^2x - 4$ coconuts confront the third sailor. After three more iterations, we find that x is divisible by $5^5 = 3125$, which implies there are at least 3121 coconuts originally. For the number 3121 itself, five iterations of subtract 1 and multiply by $(4/5)$ leaves a number (1020) that is divisible by 5, so 3121 is the answer.

6.52. *The Postage Stamp Problem with two values and at most s stamps.* We wish to be able to post envelopes costing 1 cent through n cents, for the maximum n. We must have a stamp of value 1 to get started. Let m be the value of the other stamp. (Comment: the more general problem in which d different values are allowed is unsolved.)

a) The best m is at most $s + 1$. If $m > s + 1$, then the maximum n we can reach is s. Thus we consider only $m \le s + 1$.

b) If $2 \le m \le s + 1$, then the smallest weight that cannot be posted is $m(s + 3 - m) - 1$. The amounts we can achieve are those of the form $k = qm + r$, where q, r are nonnegative and have sum at most s. Let q, r be obtained be the division algorithm. For $k < m(s + 3 - m)$, we have $q = \lfloor k/m \rfloor \le s + 2 - m$ and $r < m \le s + 1$. Thus $q + r \le s + 1$, with equality only when $q = s + 2 - m$ and $r = m - 1$, which are the values for $k = m(s + 3 - m) - 1$. Thus we can post each weight less than this.

To show that this is optimal, consider $m(s + 3 - m) - 1$. This number is one less than a multiple of m. Hence achieving it with ones and m's requires using at least $m - 1$ ones. After $m - 1$ ones, the remaining total is $m(s + 2 - m)$. Since we get at most m more cents with each additional stamp, at least $s + 2 - m$ more stamps are needed. Hence the total number of stamps needed is at least $(m - 1) + (s + 2 - m) = s + 1$, which exceeds the number of stamps allowed on the envelope.

The best choice of m is $\lceil s/2 \rceil + 1$. Since the maximum n is $m(s + 3 - m) - 2$, we choose m to maximize $m(s + 3 - m)$. As discussed in Chapter 1, this occurs when $m = (s + 3)/2$. This is the answer when s is odd: choose $m = (s + 3)/2$, achieving all values up to $(s + 3)^2/4 - 2$. When s is even, this choice is not allowed; the integer maximizing $m(s + 3 - m)$ is then $(s + 2)/2$.

6.53. *A card game winnable by the second player.* Cards labeled $1, \ldots, 2n$ are shuffled and dealt so that players A and B each receive n cards. Starting with A, play alternates between the two players. At each play, a player adds one of his or her remaining cards to the running total x. The first player who makes x divisible by $2n + 1$ wins.

For every possible deal, there is a strategy that player B can follow to win. It suffices to show that B can always make it impossible for A to win on the next move. Note that A cannot win on the first move. When B is about to play in round i, B has $n - i + 1$ cards remaining, and A has $n - i$ cards remaining. Player B must ensure that the total does not become m less than a multiple of $2n + 1$, where m is any of the cards still held by A. Hence B must ensure that the total avoids $n - i$ congruence classes. Since B holds $n - i + 1$ cards, which put the total into $n - i + 1$ different congruence classes modulo $2n + 1$, B has a card whose contribution to the total avoids all the dangerous classes. Hence B can keep A from winning. To prove that B must eventually win, observe that the sum of all the cards is $n(2n + 1)$, which is divisible by $2n + 1$.

6.54. *Transforming triples to generate 0.* The rule: if r, s are members of the current triple, with $r \le s$, then these numbers can be replaced by $2r$ and $s - r$. We show that if all three numbers are positive, then we can perform a list of moves to eventually produce a triple with a number smallest than the current smallest number.

We start with $x \le y \le z$. By the division algorithm, we can write $y = mx + b$ with $0 \le b < x$. By finding the largest power of 2 that does not exceed x, we can write $y = (2^n + a)x + b$, where $0 \le a < 2^n$ and $0 \le b < x$. We will arrange to reach the triple $2^{n+1}x, b, z - (2^n - a - 1)x$, which has the same sum. Since $b < x$, this allows us to proceed by strong induction.

We successively double the first entry $n+1$ times, subtracting the first entry from the second or third as appropriate, depending on the binary expansion of a. We must ensure that the second and third entries remain larger than the first during this process. At the jth step, for $1 \le j \le n$, we subtract the first entry $(2^{j-1}x)$ from the second if a has 2^{j-1} in its binary expansion; otherwise we subtract it from the third entry. At the $n+1$th step, we subtract from the second entry.

If these operations follow the rules, then we have subtracted $y-b$ from the second entry. From the sum of the last two entries we have subtracted $x\sum_{j=1}^{n+1} 2^{j-1} = x(2^{n+1}-1)$. Thus the third entry becomes $(2^n - a - 1)x$.

The operations are all valid if the last subtraction from each entry is valid, since the first entry successively grows and the others decrease. Before the last step, the first entry is $2^n x$ and the second is $y - ax$. Since $y - ax = 2^n x + b \ge 2^n x$, the operation is valid. The last subtraction from the third entry is at most $2^{n-1}x$, and before performing this we have subtracted at most $(2^{n-1}-1)x$ from it. Since $z \ge y \ge 2^n x$, we have $z - (2^{n-1}-1)x \ge y - 2^{n-1}x \ge 2^{n-1}x$, and again the operation is valid.

6.55. *If S is an ideal in $\mathbb{Z}$, then $S = d\mathbb{Z}$ for some $d \in \mathbb{Z}$.* First suppose $S = \{0\}$; this set S satisfies the definition of an ideal and has the desired form $S = 0\mathbb{Z}$. Any other ideal S contains a nonzero integer x. Also S contains $-x$, and one of $\{x, -x\}$ is positive, so S contains a natural number. By the Well Ordering Property, S has a least positive element m.

We prove that $S = m\mathbb{Z}$. Since S is an ideal and $m \in S$, the second property of ideals implies $m\mathbb{Z} \subseteq S$. Hence it suffices to show $S \subseteq m\mathbb{Z}$, meaning that every element of S is a multiple of m. If some $x \in S$ is not a multiple of m, then also $-x$ is a member of S that is not a multiple of m. Hence we may assume S contains a positive integer x that is not a multiple of m. By applying the Division Algorithm to x and m, we can write $x = km + r$ for some integers k, r with $1 \le r < m$; we know $r \ne 0$ because x is not divisible by m. Since $x, m \in S$ and $r = x - km$, we have $r \in S$. This contradicts the choice of m as the least positive element of S, and hence there is no $x \in S$ that is not a multiple of m.

6.56. *Greatest common divisors for polynomials.* We subtract a multiple of the polynomial of smaller degree to seek the greatest common divisor, since when $p = fq + r$, a polynomial is a common divisor of p and q if and only if it is a common divisor of q and r.

a) $(3x^3 + x + 1, x^2) \to (x^2, x+1) \to (x+1, -1) \to (-1, 1) \to (1, 0)$. These are relatively prime.

b) $(x^3 + 2x^2 + 2x + 1, x^2 + x) \to (x^2 + x, x^2 + 2x + 1) \to (x^2 + x, x + 1) \to (x+1, 0)$. The greatest common divisor is $x + 1$.

c) $(x^3 - x - 2x^2 + 2, x^3 - 3x - 2) \to (x^3 - 3x - 2, -2x^2 + 2x + 4) \to (-2x^2 + 2x + 4, x^2 - x - 2) \to (x^2 - x - 2, 0)$. The greatest common divisor is $x^2 - x - 2$.

6.57. $\deg(p+q) \le \max(\deg(p), \deg(q))$. The sum of two polynomials p and q is the polynomial whose coefficients are the sums of the corresponding coefficients in p and q. If a power of x has coefficient 0 in both, then it has coefficient 0 in the sum, and hence $\deg(p+q) \le \max(\deg(p), \deg(q))$. Strict inequality occurs when p and q have the same degree and the leading coefficient of p is the negative of the leading coefficient of q.

6.58. *When $a, b \in \mathbb{R}[x]$ and $b \ne 0$, the polynomials q, r such that $a = qb + r$ and* $\deg(r) < \deg(b)$ *(or $r = 0$) are unique.* We use induction on the degree of a. Basis step: $\deg a = 0$. Here $q = 0$ and $r = a$ if $\deg b > 0$; otherwise $q = a/b$ and $r = 0$ if $\deg b = 0$.

Induction step: $\deg a > 0$. Since the degree of the product of two polynomials is the sum of their degrees, $\deg a < \deg b$ forces $q = 0$ and then $r = a$.

Hence we may assume that $\deg a \ge \deg b$. Now we must have $\deg q = \deg a - \deg b$. Hence qb is a polynomial of degree $\deg a$ (let $k = \deg a$). Since r and r' have lower degree, $qb + r = a$ determines the leading coefficient of q; call it c. Let $a' = a - cx^k b$; this polynomial has smaller degree than a. By the induction hypothesis q' and r' such that $a' = q'b + r'$ are uniquely determined. Also $\deg q' < k$. Now q must be $cx^k + q'$, and r must be r'.

6.59. *Every nonconstant $a \in \mathbb{R}[x]$ is a product of irreducible polynomials, and the factorization is unique except for reordering and multiplication by units.* We use strong induction on the degree. Let m be a polynomial of smallest degree that does not have such a unique factorization. This implies that m is not irreducible, so we can write $m = ab$, where a and b are polynomials of lower degree. Combining factorizations of a and b yields a factorization of m, so it remains to show uniqueness.

If m has two factorizations into irreducible polynomials, then we write $c\prod p_i^{a_i} = m = c'\prod q_j^{b_j}$, where c and c' are units and all polynomials have leading coefficient 1. If some p_i and q_j are equal, then deleting one of each from the factorizations yields a polynomial of smaller degree with two factorizations. Hence we may assume that there is no such repetition.

Since p_1 divides $q_1(m/q_1)$, by Lemma 6.29 p_1 must divide q_1 or m/q_1. If p_1 divides q_1, then they are equal since q_1 is irreducible, but we have forbidden equality. If p_1 divides m/q_1, then we write $m/q_1 = p_1 r$. Now m/q_1 has the factorization $cq_1^{b_1-1}\prod_{i>j} q_j^{b_j}$, and another factorization consisting of p_1 and a factorization of r. Since the first factorization omits p_1, and the second contains p_1, m/q_1 is a counterexample of smaller degree. Hence there is no smallest-degree counterexample.

6.60. *Unique factorization of natural numbers, by the logic of Exercise 6.59.* If the claim fails, let m be the smallest natural number that does not have a unique factorization. This implies that m is not prime, so we can write $m = ab$, where a and b are less than m. Combining factorizations of a and b yields a factorization of m, so it remains to show uniqueness.

Suppose that m has two prime factorizations. We may write $\prod p_i^{a_i} = m = \prod q_j^{b_j}$. If some p_i and q_j are equal, then deleting one of each from the factorizations yields a smaller number with two factorizations. Hence we may assume that there is no such repetition.

Since p_1 divides $q_1(m/q_1)$, by ?? p_1 must divide q_1 or m/q_1. If p_1 divides q_1, then they are equal since q_1 is prime, but we have forbidden equality. If p_1 divides m/q_1, then we write $m/q_1 = p_1 r$. Now m/q_1 has the factorization $cq_1^{b_1-1} \prod_{i>j} q_j^{b_j}$, and another factorization consisting of p_1 and a factorization of r. Since the first factorization omits p_1, and the second contains p_1, m/q_1 is a counterexample of smaller degree. Hence there is no smallest-degree counterexample.

6.61. *The set $\mathbb{R}[x, y]$ of polynomials in two variables has ideals that are not principal.* Consider the set S of polynomials p such that $p(0, 0) = 0$. Every constant multiple of such a polynomial and every sum of two such polynomials is also in S, so S is an ideal. The set S contains both p_1 and p_2 defined by $p_1(x, y) = x$ and $p_2(x, y) = y$, but there is no nonconstant element of S that divides both, so S is not a principal ideal.

6.62. *If a and b are polynomials with no nonconstant common factor, then then same holds for the pairs a^2, b^2 and $a, 2b$.* If an irreducible polynomial p divides a product, then it divides one of the factors (Lemma 6.29). Thus if p divides both $a \cdot a$ and $b \cdot b$, then it must divide both a and b. Therefore a^2 and b^2 have no nonconstant common factor.

For the second pair, multiplication by a constant does not change the nonconstant factors.

6.63. *If $ab = 1$ for $a, b \in \mathbb{R}[x]$, then a and b are constants.* If a or b has positive degree, then ab has positive degree and does not equal 1.

6.64. *A polynomial in $\mathbb{Z}[x]$ whose factors lie in $\mathbb{R}[x]$ but not in $\mathbb{Z}[x]$.* One example is $x^2 - 2$. The point is that a polynomial can be irreducible over Z[x] while being reducible over R[x].

6.65. *For real numbers $A, B, C \in \mathbb{R}$ with $A \neq 0$, a necessary and sufficient condition for $Ax^2 + Bx + C$ to be irreducible in $\mathbb{R}[x]$ is $B^2 - 4AC < 0$.* Any real numbers r, s that satisfy $Ax^2 + Bx + C = A(x - r)(x - s)$ are provided by the quadratic formula, $(-B \pm \sqrt{B^2 - 4AC})/(2A)$. Such real numbers exist if and only if $B^2 - 4AC \geq 0$; otherwise, the polynomial is irreducible.

7. MODULAR ARITHMETIC

7.1. *Cancellation of factors modulo n.* When a, b, x, n are positive integers, "$ax \equiv bx \pmod{n}$" does not imply "$a \equiv b \pmod{n}$". For a counterexample, note that $2 \cdot 3 \equiv 4 \cdot 3 \pmod{6}$, but $2 \not\equiv 4 \pmod{6}$. With the added condition that x and n are relatively prime, the implication becomes true. The reason is that $ax \equiv bx \pmod{n}$ means that n divides $x(a - b)$. Since x and n are relatively prime, Proposition 6.6 implies that n divides $a - b$, so $a \equiv bmodn$.

7.2. *Divisibility conditions.* An integer written in base 10 is divisible by 5 if and only if the last digit is 0 or 5. It is divisible by 2 if and only if the last digit is even. The last digit does not determine whether it is divisible by 3, since 3 is divisible by 3 but 13 is not.

7.3. *The regular sleeper.* If the person goes to sleep 17 hours after rising and sleeps eight hours each day, then she goes to sleep one hour later each day. After 24 days, she has risen at each possible hour. If she goes to sleep after 18 hours, then she rises two hours later each day. Since 24 is even, she cannot change the parity of the hour at which she rises.

7.4. *If two natural numbers have the same number of copies of each digit in their decimal expansions, then they differ by a multiple of 9.* Differing by a multiple of 9 is equivalent to belonging to the same congruence class modulo 9. Since $10^n \equiv 1^n \equiv 1 \pmod{9}$, the sum of the digits in the base 10 representation of n is congruent to n modulo 9. Two numbers that have the same number of copies of each digit in their decimal expansions have the same sum of digits.

7.5. *The congruence class of 10^n modulo 11 is $(-1)^n$, and hence $654321 \equiv -3 \pmod{11}$.* The first statement follows from the fact that the congruence class of kl is the congruence class of the product of any representatives of the classes of k and l. Hence we can use -1 instead of 10 in forming the product n times. For the subsequent computation,

$$\begin{aligned} 654321 &\equiv 6(-1)^5 + 5(-1)^4 + 4(-1)^3 + 3(-1)^2 + 2(-1)^1 + (-1)^0 \\ &\equiv -6 + 5 - 4 + 3 - 2 + 1 \equiv -3 \pmod{11}. \end{aligned}$$

7.6. *Remainders modulo 8: $9^{1000} \equiv 1 \pmod{8}$, $10^{1000} \equiv 0 \pmod{8}$, $11^{1000} \equiv 1 \pmod{8}$.* Determining the last digit in the base 8 expansion is the same as finding the remainder class modulo 8. Since $9 \equiv 1 \pmod{8}$, 9^{1000} has the same remainder as 1^{1000}. Since $10 = 2 \cdot 5$, 10^{1000} is a multiple of $2^3 = 8$, so its remainder is 0. Since $11 \equiv 3 \pmod{8}$,

$$11^{1000} \equiv (3^2)^{500} \equiv 1^{500} \equiv 1 \pmod{8}.$$

7.7. *When the remainders modulo m of the numbers $1^2, 2^2, \dots, (m-1)^2$ are listed in order, the list is symmetric around the center,* because $m - j \equiv -j \pmod{m}$, and $(m-j)^2 \equiv (-j)^2 \equiv (-1)^2 j^2 \equiv j^2 \pmod{m}$.

7.8. *If k is an odd number, then $k^2 - 1$ is divisible by 8.* We factor $k^2 - 1$ as $(k+1)(k-1)$ and observe that both of these factors are even, with one of them divisible by 4.

One can also compute with congruence classes: k is congruent to one of $1, 3, 5, 7$ modulo 8. In these cases, $1^2 - 1 \equiv 0 \pmod{8}$, $3^2 - 1 \equiv 9 - 1 \equiv 0 \pmod{8}$, $5^2 - 1 \equiv 25 - 1 \equiv 0 \pmod{8}$, and $7^2 - 1 \equiv 49 - 1 \equiv 0 \pmod{8}$.

7.9. $2^{100} \equiv 3 \pmod{13}$. By Fermat's Little Theorem, $2^{12} \equiv 1 \pmod{13}$. Hence $2^{100} \equiv (2^{12})^4 \cdot 2^4 \equiv 1 \cdot 16 \equiv 3 \pmod{13}$.

7.10. *The common citizenship relation.* If people were restricted to be citizens of only one country, then this would be an equivalence relation, with one equivalence class for each country. However, there are people who hold dual citizenship. They satisfy the relation with citizens of each of the two countries, although people of one country need not be citizens of the same country with people of the other country. The relation fails to be transitive.

7.11. *Equivalence relations R on a set S.*

a) $S = \mathbb{N} - \{1\}$; $(x, y) \in R$ if and only if x and y have a common factor bigger than 1. This is not an equivalence relation. It satisfies the reflexive and symmetric properties but not the transitive property: $(2, 6) \in R$ and $(6, 3) \in R$, but $(2, 3) \notin R$.

b) $S = \mathbb{R}$; $(x, y) \in R$ if and only if there exists $n \in \mathbb{Z}$ such that $x = 2^n y$. This is an equivalence relation. Reflexive property: $x = 2^0 x$. Symmetric property: if $x = 2^n y$, then $y = 2^{-n} x$. Transitive property: if $x = 2^n y$ and $y = 2^m z$, then $x = 2^{n+m} z$.

7.12. *When S is the disjoint union of sets $A_1, \dots, A_k$, the relation R consisting of pairs $(x, y) \in S \times S$ such that x and y belong to the same member of $\{A_1, \dots, A_k\}$ is an equivalence relation on S.*

Reflexive property: x and x belong to the same set A_i.

Symmetric property: If x and y belong to A_i, then y and x belong to A_i.

Transitive property: If x and y belong to A_i, and y and z belong to A_j, then $i = j$ since y belongs to only one set. This implies that x and z belong to the same set A_i.

7.13. *When C is a fixed subset of S, the relation R defined on the set of subsets of S by $(A, B) \in R$ if and only if $A \cap C = B \cap C$ is an equivalence relation.* The reflexive property holds because $A \cap C = A \cap C$. The symmetric property holds because $A \cap C = B \cap C$ implies $B \cap C = A \cap C$. The transitive property holds because $A \cap C = B \cap C$ and $B \cap C = D \cap C$ imply $A \cap C = D \cap C$, by the transitivity of equality.

7.14. *The relation R defined by "$(g, h) \in R$ if and only if $g - h \in O(f)$" is an equivalence relation on the set of functions from $\mathbb{R}$ to $\mathbb{R}$.* Reflexive property: $(g, g) \in R$ by choosing any positive constants c, a, since $|g(x) - g(x)| = 0 \le c|f(x)|$ for all $x \in \mathbb{R}$. Symmetric property: consider $(g, h) \in R$, with constants c, a such that $|g(x) - h(x)| \le c|f(x)|$ for $x > a$. Since $|h(x) - g(x)| = |g(x) - h(x)|$, the same choice c, a shows that $h - g \in R$.

Transitive property: Suppose that $g - h \in R$ using constants c, a and that $h - j \in R$ using constants c', a'. We have

$$\begin{aligned} |g(x) - j(x)| &= |g(x) - h(x) + h(x) - j(x)| \le |g(x) - h(x)| + |h(x) - j(x)| \\ &\le c|f(x)| + c'|f(x)| = (c + c')|f(x)| \end{aligned}$$

for $x > \max\{a, a'\}$. Thus $g - j \in R$, using constants $c + c'$ and $\max\{a, a'\}$.

7.15. *Symmetry plus transitivity does not imply reflexivity.* "Consider $x \in S$. If $(x, y) \in R$, then the symmetric property implies that $(y, x) \in R$. Now the transitive property applied to (x, y) and (y, x) implies that $(x, x) \in R$." This argument assumes the existence of an element y different from x such that $(x, y) \in R$; there need not be such an element.

7.16. *Every year (including leap years) has at least one Friday the 13th.* It suffices to prove that every year has a month that begins on a Sunday. To prove this, it suffices to prove that for every year and every day of the week, some month during the year begins on that day of the week. We treat the days of the week as integers modulo 7. If the jth month has 31 days, then the $j + 1$th month starts in the class 3 later than the start of the jth month. Similarly, the shift is 2, 1, 0 for months of length 30,29,28, respectively. Suppose January 1 is in class k. We consider two cases, since in leap years February has 29 days instead of 28. The months then begin in congruence classes modulo 7 as indicated below:

	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec
usual	k	$k+3$	$k+3$	$k+6$	$k+1$	$k+4$	$k+6$	$k+2$	$k+5$	k	$k+3$	$k+5$
leap	k	$k+3$	$k+4$	k	$k+2$	$k+5$	k	$k+3$	$k+6$	$k+1$	$k+4$	$k+6$

Since the values $k, k+1, k+2, k+3, k+4, k+5, k+6$ all appear in each list, we conclude that in each year, each congruence class occurs as the start of some month.

Comments. 1) all congruence classes occur after February. Thus the problem can be solved using only one case by considering only the portion of the year beginning on March 1. 2) the maximum number of occurrences of the same class is 3. Hence the maximum number of Friday the 13ths in a year is 3, which occurs in leap years that start on Sunday and in non-leap years that start on Thursday.

7.17. *n^3+5n is divisible by 6 for every $n \in \mathbb{N}$.*

a) Proof 1 (induction). For $n = 1$, $n^3 + 5n = 6$, which is divisible by 6. For the induction step, suppose $m^3 + 5m$ is divisible by 6. Then $(m+1)^3 + 5(m+1) = (m^3 + 5m) + (3m^2 + 3m) + (6)$. The quantity inside each parenthesis is divisible by 6, the first by the induction hypothesis, the second since $3m^2 + 3m = 3m(m+1)$ has 3 and an even number as factors, and the third since $6|6$. Hence the distributive property implies $6|[(m+1)^3 + 5(m+1)]$, which completes the induction step.

b) Proof 2 (modular arithmetic). Since $5 \equiv -1 \pmod{6}$, we have $n^3 + 5n \equiv n^3 - n \equiv (n+1)n(n-1) \pmod{6}$. Since three consecutive integers always contain an even number and a multiple of 3, their product is divisible by 6. Thus $n^3 + 5n$ is also divisible by 6.

c) Proof 3 (binomial coefficients). Since $\binom{n}{3} = n(n-1)(n-2)/6$, we have $n^3 = 6\binom{n}{3} + 3n^2 - 2n$. Hence $n^3 + 5n = 6\binom{n}{3} + 3n(n+1)$. Since $\binom{n}{3}$ is an integer, the first term is a multiple of 6, and the second has 3 and an even number as factors and is also a multiple of 6.

7.18. *Solution to $2n^2 + n \equiv 0 \pmod{p}$ when p is an odd prime.* We factor $2n^2 + n$ as $n(2n+1)$ and ask when the product is a multiple of p. Since p is prime, this occurs if and only if n is a multiple of p or $n \equiv (p-1)/2 \pmod{p}$.

7.19. *If $m, n, p \in \mathbb{Z}$ and 5 divides $m^2 + n^2 + p^2$, then 5 divides at least one of $\{m, n, p\}$.* If 5 divides $m^2 + n^2 + p^2$, then these three numbers belong to congruence classes modulo 5 that sum to a multiple of 5. The congruence classes modulo 5 that contain squares of integers can be found by squaring representatives of the five classes. Since $0^2 \equiv 0 \pmod{5}$, $1^2 \equiv 1 \pmod{5}$, $2^2 \equiv 4 \equiv -1 \pmod{5}$, $3^2 \equiv 4 \equiv -1 \pmod{5}$, and $4^2 \equiv 1 \pmod{5}$, the only congruence classes modulo 5 that contain squares are $1, 0, -1$.

If we do not use congruence class 0 (multiples of 5), then the possibilities for sums of three squares (modulo 5) are (three 1's), (two 1's and a -1), (one 1 and two -1's), (three -1's). In these four cases, the sums are congruent to $3, 1, -1, -3$, respectively. Hence if the sum of three squares is divisible by 5, at least one of the squares must be divisible by 5. If a prime divides $k \cdot k$, then it must also divide k, so we conclude that at least one of $\{m, n, p\}$ is divisible by 5.

7.20. *$k^n - 1$ is divisible by $k - 1$ for all positive integers k, n with $k \geq 2$.* Since $k \equiv 1 \pmod{k-1}$, we have $k^n - 1 \equiv 1^n - 1 \equiv 0 \pmod{k-1}$.

7.21. *The product of any k consecutive natural numbers is divisible by $k!$.* Let $a_k(n) = \prod_{i=0}^{k-1}(n+i)$. We prove by induction on $n+k$ that $a_k(n)$ is divisible by $k!$ when $k, n \in \mathbb{N}$.

Proof 1 (induction on $n + k$). Basis step ($\min\{n, k\} = 1$). We have $a_1(n) = n$ (divisible by 1!), and $a_k(1) = k!$ (divisible by $k!$).

Induction step: Applying the distributive law to the last factor, we have $a_k(n) = a_k(n-1) + ka_{k-1}(n)$. By the induction hypothesis, $k!$ divides $a_k(n-1)$ and $(k-1)!$ divides $a_{k-1}(n)$. Thus $k!$ divides both and their sum.

Proof 2 (combinatorial argument). We show that $a_k(n)/k!$ is an integer, by showing that it counts a set. In particular, $a_k(n)/k! = \binom{n+k-1}{k}$; the ratio is the formula for the number of k-element subsets of a set of size $n + k - 1$.

7.22. *There are infinitely many primes of the form $4n+3$ and infinitely many primes of the form $6n + 5$, where $n \in \mathbb{N}$.* Suppose that $m \equiv -1 \pmod{4}$. The congruence class of a number is the product of the congruence classes of its factors. Thus the factors of m are all congruence to 1 or -1 modulo 4, with an odd number of them congruent to -1. Thus every number congruent to $-1 \pmod{4}$ has a prime factor congruent to $-1 \pmod{4}$.

Similarly, suppose that $m \equiv -1 \pmod{6}$. Again m has only odd factors. Since $3 \cdot 3 \equiv 1 \cdot 1 \equiv 1 \pmod{6}$ and $3 \cdot 1 \equiv 3 \pmod{6}$, an odd number of factors used in producing m as a product must be congruent to $-1 \pmod{6}$.

Suppose there are finitely many primes congruent to -1 modulo k, where $k \in \{4, 6\}$. Let N be the product of all these primes, and let N' be the next number above N that is congruent to $-1 modulok$. Since $N' - N$ is 2 or 4, N' is not divisible by any of the prime factors of N. Thus N' is another prime congruent to -1 modulo k.

7.23. *Palindromic integers.* The congruence class of 10^n modulo 11 is $(-1)^n$, since $10 \equiv -1 \pmod{11}$. (Equivalently, $10^n \equiv 1 \pmod{11}$ if n is even and $10^n \equiv 10 \pmod{11}$ if n is odd.) If n is a palindrome of even length ($2l$ digits), then $n = \sum_{i=0}^{2l-1} a_i 10^i$ with $a_i = a_{2l-1-i}$. Since $i + (2l - 1 - i)$ is odd, the parity of i is opposite to the parity of $2l - 1 - i$. Therefore, $10^i + 10^{2l-1-i} \equiv 0 \pmod{11}$. Since $a_i = a_{2l-1-i}$, grouping the terms in pairs yields

$$n = \textstyle\sum_{i=0}^{l-1} a_i(10^i + 10^{2l-1-i}) \equiv \sum_{i=0}^{l-1} a_i \cdot 0 \equiv 0 \pmod{11}.$$

The proof for divisibility by $k + 1$ of natural numbers whose base k representation is a palindrome of even length is the same as the proof above for $k = 10$; simply replace each "10" by "k" and each "11" by "$k + 1$".

7.24. *The function $f : \mathbb{Z}_n \to \mathbb{Z}_n$ defined by $f(x) = x^2$ is injective only when $n \leq 2$.* If $n > 2$, then -1 and 1 are different classes, $f(-1) = f(1)$.

7.25. *Powers of 10, modulo 7.*

$$10^1 \equiv 3 \pmod{7}.$$
$$10^2 \equiv 3^2 \equiv 2 \pmod{7}.$$
$$10^3 \equiv 10^2 10 \equiv 3 \cdot 2 \equiv 6 \pmod{7}.$$
$$10^4 \equiv 10^3 10 \equiv 6 \cdot 3 \equiv 4 \pmod{7}.$$
$$10^5 \equiv 10^4 10 \equiv 4 \cdot 3 \equiv 5 \pmod{7}.$$
$$10^6 \equiv 10^5 10 \equiv 5 \cdot 3 \equiv 1 \pmod{7}.$$

7.26. $\{123654, 321654\}$ *is the set of 6-digit integers whose set of digits is* $\{1, 2, 3, 4, 5, 6\}$ *and for each* i *the number formed by the first* i *digits is divisible by* i. Let the digits of the number be $abcdef$ in order. Since 0 is not in the set of allowed digits, $5|abcde$ implies $e = 5$. Similarly, the three even digits must be $\{b, d, f\}$. There is no further restriction on f, since the sum of the digits is 15, which is divisible by 3. The first three digits are $\{1, 3, b\}$, where $b \in \{2, 4, 6\}$. Since $1 + 3 \equiv 1 \pmod 3$, we must have $b \equiv 2 \pmod 3$ to have $3|abc$; the only such choice for b is 2. Now, with c odd, we must have $d \equiv 2 \pmod 4$ to have $4|abcd$, and the only remaining choice for this is $d = 6$. We have eliminated all possibilities except 123654 and 321654, and both of these work.

7.27. *The unique natural number whose base 10 representation is a permutation of* $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 0\}$ *such that the first* i *digits form the base 10 representation of a number divisible by* i, *for* $1 \le i \le 10$, *is* 3816547290.

Let the base 10 representation of n be $a_1a_2 \cdots a_{10}$ as a string from left to right. Let n_j be the integer whose base 10 representation is the first j digits of the base 10 representation of n, read from left to right. Since n_{10} is divisible by 10, $a_{10} = 0$. Since n_5 is divisible by 5 and 0 is taken, $a_5 = 5$. With $a_{10} = 0$, n_9 imposes no constraint. Also n_1 imposes no constraint.

All of a_2, a_4, a_6, a_8 are even, and thus all of a_1, a_3, a_7, a_9 are odd.

Since $4|100$, the 2-digit number a_3a_4 must be divisible by 4. Since a_3 is odd, we conclude that $a_4 \in \{2, 6\}$.

Since a_6 is even and $8|200$, the 2-digit number a_7a_8 must be divisible by 8. Since a_7 is odd, we conclude that $a_7a_8 \in \{16, 32, 72, 96\}$. Thus $\{a_4, a_8\} = \{2, 6\}$ and $\{a_2, a_6\} = \{4, 8\}$

Since n_3 is divisible by 3, the first three digits sum to a multiple of 3. Since n_6 is divisible by 6, the digits $a_4a_5a_6$ must also sum to a multiple of 3. For $a_4a_5a_6$ this leaves the two cases 258 and 654.

If $a_4a_5a_6 = 258$, then $a_8 = 6$ and $a_2 = 4$. This and divisibility of n_3 by 3 requires $a_1 + a_3 \equiv -1 \pmod 3$. Since $a_5 = 5$, the only remaining pair of odd digits with this property is $\{1, 7\}$. With $a_8 = 6$, this forces $a_7 = 9$ and hence $a_9 = 3$. We are left with the two possibilities 1472589630 and 7412589630. The first requires $7|2589$, and the second requires $7|412589$. Since $7|2590$, the first fails. Also $7|412580$, so the second fails.

The last case is $a_4a_5a_6 = 654$. Now $a_8 = 2$ and $a_2 = 8$. This and divisibility of n_3 by 3 requires $a_1 + a_3 \equiv 1 \pmod 3$. The possibilities for $\{a_1, a_3\}$ are now $\{1, 3\}$, $\{1, 9\}$, and $\{3, 7\}$. The last of these is out, since $a_8 = 2$ requires $a_7 \in \{3, 7\}$. The remaining possibilities are now 1836547290, 3816547290, 1896543270, 1896547230, 9816543270, and 9816547230. Again all requirements are now satisfied except $7|n_7$. Using any test for divisibility by 7 to check this leaves 3816547290 as the only solution.

7.28. *Test for divisibility by 7.*

a) (by reducing powers of 10). Each power of 10 is 10 times the previous power, which is congruent to 3 times the previous power when reduced modulo 7. We thus have $10 \equiv 3 \pmod 7$, $10^2 \equiv 3 \cdot 3 \equiv 2 \pmod 7$, $10^3 \equiv 2 \cdot 3 \equiv -1 \pmod 7$, $10^4 \equiv -1 \cdot 3 \equiv -3 \pmod 7$, and $10^5 \equiv -3 \cdot 3 \equiv -2 \pmod 7$. Using the decimal representation, we therefore obtain

$$535801 \equiv 5(-2) + 3(-3) + 5(-1) + 8(2) + 0(3) + 1(1) \equiv -7 \equiv 0 \pmod 7.$$

b) (by remainders) If $f(n)$ *is formed by subtracting twice the last digit in the decimal representation of* n *from the number formed by the remaining digits, then* $7|n$ *if and only if* $7|f(n)$. Let a be the last digit in the decimal representation of n. By the construction of $f(n)$ from n, we have $n = 10[f(n)+2a]+a = 10f(n)+21a$. Since $7|(21a)$, we have $7|(n-10f(n))$. Hence $7|n$ if and only if $7|[10f(n)]$. Since $10f(n)$ is a multiple of $f(n)$, $7|f(n)$ implies $7|[10f(n)]$. Conversely, if $7|[10f(n)]$, then $7|f(n)$ because 7 and 10 are relatively prime. Hence $7|[10f(n)]$ if and only if $7|f(n)$. By transitivity of implication, $7|n$ if and only if $7|f(n)$. Applying this to 535801, we have

$$7|535801 \Leftrightarrow 7|53578 \Leftrightarrow 7|5341 \Leftrightarrow 7|532 \Leftrightarrow 7|49.$$

Since 7 divides 49, we conclude that $7|535801$, which agrees with part (a).

7.29. *Test for divisibility by* n, *generalizing Exercise 7.28).* For a positive integer n, let $f(n)$ be the integer formed by subtracting j times the last base 10 digit of n from the number formed by the remaining digits.

If s *is not divisible by 2 or 5 and* $10j \equiv -1 \pmod s$, *then* n *is divisible by* s *if and only if* $f(n)$ *is divisible by* n. Let a be the last digit in the decimal representation of n. By the construction of $f(n)$ from n, we have $n = 10[f(n) + ja] + a = 10f(n) + (10j + 1)a$. Since $10j \equiv -1 \pmod s$, we have $s|(n - 10f(n))$. Hence $s|n$ if and only if $s|[10f(n)]$. Since $10f(n)$ is a multiple of $f(n)$, $s|f(n)$ implies $s|[10f(n)]$. Conversely, if $s|[10f(n)]$, then $s|f(n)$ because s and 10 are relatively prime. Hence $s|[10f(n)]$ if and only if $s|f(n)$. By transitivity of implication, $s|n$ if and only if $s|f(n)$.

Tests for divisiblity by 17 and 19, applied to 323. Both 17 and 19 satisfy the conditions for s, so it suffices to find j such that $10 \equiv -1 \pmod s$. When $s = 17$, we set $j = 5$, since $50 \equiv -1 \pmod{17}$. When $s = 19$, we set $j = -2$, since $-20 \equiv -1 \pmod{19}$.

For divisibility by 17, replace 323 with $32 - 5 \cdot 3 = 17$, which is divisible by 17. For divisibility by 19, replace 323 with $32 + 2 \cdot 3 = 38$, which is divisible by 19. Hence 323 is divisible by both 17 and 19; it is their product.

7.30. *Primes and threes.*

a) The sum of the digits in the base 10 representation of a natural number n *is a multiple of 3 if and only if* n *is a multiple of 3.* Since

$10 \equiv 1 \pmod 3$, $10^i \equiv 1 \pmod 3$ for $i \in \mathbb{N}$. If $n = \sum_{i=0}^{k} a_i 10^i$, this implies $n \equiv \sum_{i=0}^{k} a_i \pmod 3$. Hence n is divisible by 3 if and only if $\sum_{i=0}^{k} a_i$ is divisible by 3.

b) If $x+1$ and $x-1$ are primes, then $6|x$ or $x = 4$. The case $x = 4$ is an exception; otherwise we may assume $x - 1 \neq 3$. Since there is only one even prime, $x+1$ and $x-1$ must be odd, so $2|x$. Since $x - 1 \neq 3$, neither of $x-1, x+1$ is divisible by 3. Since exactly one of every three consecutive integers is divisible by 3, this implies $3|x$. Together, $2|x$ and $3|x$ imply $6|x$.

c) If $x+1$ and $x-1$ are primes, then their concatenation is not prime unless the concatenation is 53. Since $\{3, 5\}$ is an exception, we may henceforth assume $\{x-1, x+1\} \neq \{3, 5\}$. We know by (b) that x is divisible by 3. By (a), this implies that the digits of $x-1$ sum to one less than a multiple of 3, and the digits of $x+1$ sum to one more than a multiple of 3. Together, the digits of the concatenation therefore sum to a multiple of 3. By (a), the concatenation is therefore divisible by 3 and not prime.

7.31. *If $n = m^2 + 1$ for some $m \in \mathbb{N}$, then k is a square if and only if $-k$ is a square modulo n.* If k is a square, then $k \equiv j^2 \pmod n$ for some integer j. Since $n = m^2 + 1$, we have $m^2 \equiv -1 \pmod n$. Thus $-k \equiv m^2 j^2 \equiv (mj)^2 \pmod n$, and $-k$ is all a square. The converse follows in the same way starting from $-k$.

7.32. *If $n \in \mathbb{N}$, $a, b \in \mathbb{Z}$, and $d = \gcd(a, n)$, then there is no congruence class $\overline{x}$ (modulo n) that solves the congruence equation $\overline{ax} = \overline{b}$ unless d divides b, in which case there are d solutions.* The meaning of the equation in classes is that $\overline{x}$ is a solution if and only if $ax + ny = b$ for some $y \in \mathbb{Z}$. Since d divides a and n, there is no solution unless $d|b$. Suppose $d|b$. Now we know $ax + ny = b$ has infinitely many integer solutions, and the set of solutions (x, y) is $\{(x_0 + (n/d)m, y_0 - (a/d)m) \colon m \in \mathbb{Z}\}$, where (x_0, y_0) is one solution (see Exercise 6.27). We need to know how many congruence classes modulo n contain elements of $\{x_0 + (n/d)m\}$. The numbers m_1 and m_2 give the same congruence class modulo n for $x_0 + (n/d)m$ if and only if m_1 and m_2 differ by a multiple of d. Hence there are d classes that solve the equation.

7.33. *Deserting soldiers.* Out of 1500 soldiers, the number x of soldiers that remain satisfies $x \equiv 1 \pmod 5$, $x \equiv 3 \pmod 7$, and $x \equiv 3 \pmod{11}$. With a_i and n_i as indicated in the table below, we apply the procedure in the proof of the Chinese Remainder Theorem:

i	a_i	n_i	N_i	$N_i \pmod{n_i}$	y_i
1	1	5	77	2	3
2	3	7	55	-1	-1
3	3	11	35	2	6

Applying the Chinese Remainder Theorem, we obtain an integer satisfying all three congruence conditions by computing

$$\sum a_i N_i y_i = (1)(77)(3) + (3)(55)(-1) + (3)(35)(6) = 231 - 165 + 630 = 696.$$

(Checking the resulting congruences is important for eliminating arithmetic errors!!!) The set of solutions is the set of integers that differ from 696 by a multiple of N, where $N = 5 \cdot 7 \cdot 11 = 385$. Since only a few soldiers deserted, the number remaining should be the largest integer less than 1500 that is congruent to 696 modulo 385. Since $696 + 2 \cdot 385 = 1466$, we conclude that 34 soldiers deserted.

7.34. *The number -13 is the unique integer with absolute value at most 252 that is congruent to $1 \pmod 7$, $3 \pmod 8$, and $5 \pmod 9$.* Since 7, 8, and 9 are pairwise relatively prime, we can apply the Chinese Remainder Theorem. The product is 504, and the products N_i without each n_i are $\{72, 63, 56\}$. We seek the multiplicative inverse y_i of $N_i \pmod{n_i}$. First, $72 \equiv 2 \pmod 7$, with inverse 4 ($2 \cdot 4 = 8 \equiv 1 \pmod 7$). Also, $63 \equiv -1 \pmod 8$, with inverse -1. Finally, $56 \equiv 2 \pmod 9$, with inverse 5. The numbers $N_i y_i$ are $\{288, -63, 280\}$. We set

$$x = \sum a_i N_i y_i = 288 - 3 \cdot 63 + 5 \cdot 280 = 1499 \equiv -13 \pmod{504}.$$

The number -13 is in the desired classes modulo each of $\{7, 8, 9\}$.

7.35. *A solution to $x \equiv 3 \pmod 6$, $x \equiv 4 \pmod 7$, $x \equiv 5 \pmod 8$ can be found by transforming the problem to congruences modulo 3, 7, and 8.* The Chinese Remainder Theorem requires relatively prime moduli, which 6 and 8 are not. Nevertheless, since $x \equiv 3 \pmod 6$ if and only if both $x \equiv 1 \pmod 2$ and $x \equiv 0 \pmod 3$, replacing $x \equiv 3 \pmod 6$ with these two congruences does not change the solutions. Now 2 and 8 are not relatively prime, but $x \equiv 5 \pmod 8$ requires x to be odd, so we can drop the condition $x \equiv 1 \pmod 2$. Thus the original problem is equivalent to $x \equiv 0 \pmod 3$, $x \equiv 4 \pmod 7$, $x \equiv 5 \pmod 8$. (With $x \equiv 4 \pmod 6$ in the original problem instead of $x \equiv 3 \pmod 6$, there would be no solution.)

The smallest positive solution is 165. This number has the desired remainders modulo 3, 7, 8, and consecutive numbers with these remainder differ by $3 \cdot 7 \cdot 8 = 168$, since 3, 7, 8 are relatively prime.

7.36. *If n is congruent to $x \pmod a$, to $y \pmod b$, and to $z \pmod c$, then the set of such integers is $\{n + kl \colon k \in \mathbb{Z}\}$, where l is the least common multiple of a, b, and c.* The numbers described are those whose difference from n is a multiple of a, b, and c. Thus m satisfies all the congruences if and only if $m - n$ is a multiple of a, b, and c.

7.37. *Completion of the Newspaper Problem (Solution 7.32).* The check for x dollars and y cents is paid as y dollars and x cents, with x and y between 0 and 99. With a newspaper costing k cents, we are given $100y + x - k = 2(100x + y)$, or $98y - 199x = k$.

Setting (dollars,cents) pairs equivalent when they represent the same amount yields $(y, x - k)$ equivalent to $(2x, 2y)$, which leads to $y = 2x + n$ and $x - k = 2y - 100n$ for some $n \in \mathbb{Z}$. Eliminating y produces $3x + k = 98n$.

Modulo 3, this equation becomes $k \equiv 2n \pmod 3$. Since $y = 2x + n$, the parameter n is at most 99. With $x = (98n - k)/3$, n must be positive.

When k is a multiple of 3, also n must be. In this case, $n \geq 3$ yields $x \geq 98 - k/3$ and $y \geq 199 - 2k/3$. Since $y \leq 99$, we have $k \geq 150$. Thus the existence of a solution when $3|k$ requires that the newspaper cost at least \$1.50. Each increase of 3 in k decreases x by 1 and y by 2, until $k = 294$. We can then use $n = 6$ to find solutions for higher multiples of 3.

For each n, there is a range of values of k (congruent to $2n$ modulo 3) for which solutions can be found. The restriction $99 \geq y = \frac{1}{3}(199n - 2k)$ yields the lower bound on k, and the restriction $0 \leq x = \frac{1}{3}(98n - k)$ yields the upper bound. In particular, we obtain solutions for $99.5n - 148.5 \leq k \leq 98n$ when $k \equiv 2n \pmod 3$ and $1 \leq n \leq 99$.

When $k \equiv 0 \pmod 3$, we need $n =\equiv 0 \pmod 3$, and the Note that in each congruence class there are gaps. The highest k for $n = 3$ is \$2.94, but the next multiple of 3 such that a solution exists is \$4.50. The smallest newspaper costs in each congruence class for which the problem is solvable are \$1.50, \$.52, and \$.02, yielding the check values \$48.99, \$48.98, and \$48.97. The largest are \$97.02, \$96.04, and \$95.06, yielding the check values \$0.99, \$0.98, and \$0.97.

7.38. *For $n > 2$, there are $(n-1)!/2$ distinguishable ways to form a necklace fr om n distinguishable beads.* **Proof 1** (counting argument). Beginning at some point on the necklace, there are $n!$ ways to write down the beads in order, but $2n$ of these come from the same necklace, since each point we start at gives us a different ordering for the same necklace, as does going counterclockwise instead of clockwise. With $2n$ permutations for each necklace, altogether there are $n!/(2n) = (n-1)!/2$ necklaces.

Proof 2 (induction). When $n = 3$, each bead neighbors the other two, and there is only one necklace. For $n > 3$, we obtain n-bead necklaces from $(n-1)$-bead necklaces by inserting bead n in one of $n - 1$ possible positions. By the induction hypothesis, there are $(n-2)!/2$ necklaces with $n - 1$ beads; thus we have created $(n-1)!/2$ objects. Since a necklace is determined by listing the two neighbors of each bead, these $(n-1)!/2$ objects correspond to distinct necklaces. Deleting bead n from an n-bead necklace leaves an $(n-1)$-bead necklace; thus we have counted all necklaces with n beads.

7.39. *Equivalence classes under rotation for hats with n feathers from k types, where n is prime.* Hats x and y are indistinguishable when we can rotate x into y. We can rotate x into itself by the 0 degree rotation, so the relation is reflexive. If rotating x by n degrees yields y, then rotating y by $-n$ degrees yields x, so the relation is symmetric. The composition of rotating x into y and y into z rotates x into z, so the relation is transitive. Thus indistinguishability is an equivalence relation and partitions the set of all hats with n feathers from k types into equivalence classes. We want to count the classes.

Given a hat, record the feather-types in order from any point. Since there are always k choices for the type of the next feather, there are k^n possible resulting lists. Of these lists, k use only one color of bead. All other list can be rotated in n ways to obtain equivalent list. We claim that when n is prime, these n lists are distinct. If so, then the $k^n - k$ non-constant orderings fall into equivalence classes of size n, making the number of equivalence classes $k + (k^n - k)/n$. (This also yields a combinatorial proof that n divides $k^n - k$ when n is prime.)

Let x be the list from a nonconstant hat. If the n rotations of x are not all distinct, then some list y appears twice. If y occurs when we shift x by i or by j, then shifting y by $a = j - i$ positions leaves y unchanged. Hence shifting y by any multiple of a positions also leaves it unchanged. Since n is prime, some multiple of a is congruent to $1 \pmod n$, say $aq = rn + 1$. Shifting by $rn + 1$ positions has the same effect as shifting by 1. Thus shifting y by one position leaves it unchanged. This requires that each entry in y is the same as the next, so y must be a constant ordering. We have proved the contrapositive of the desired statement.

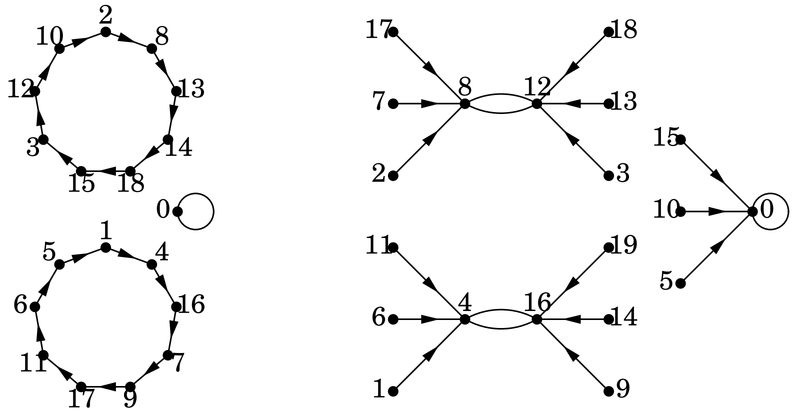
7.40. *There are $(k^n + k^{\lceil n/2 \rceil})/2$ distinguishable ways to paint a a stick partitioned into n equal segments when k colors are available.* Since the same coloring can be viewed forward or backward, the colorings group into equivalence classes of sizes 1 and 2. Altogether there are k^n colorings of the fixed stick. We count each class once if we add on the number of classes of size 1 and then divide by 2.

A coloring is equivalent only to itself if and only if it looks the same from both ends. Thus specifying the colors of the first $\lceil n/2 \rceil$ positions determines the rest. We can specify such a coloring in $k^{\lceil n/2 \rceil}$ ways.

7.41. Define f and g from $\mathbb{Z}_n$ to $\mathbb{Z}_n$ by $f(x) \equiv (x + a) \pmod n$ and $g(x) \equiv ax \pmod n$.

a) The functional digraph of f is a collection of d cycles of length n/d, where $d = \gcd(a, n)$. Since addition modulo n has additive inverses, the functional digraph is a collection of pairwise disjoint cycles. The length of each cycle is the minimum number of times a must be added to obtain a multiple of n. That multiple is the least common multiple of a and n, so the length is $\mathrm{lcm}\,(n,a)/a$. Since $\gcd(n,a)\mathrm{lcm}\,(n,a) = na$, the length is n/d.

b) Digraphs for g *when* $(n,a) = (19,4)$ *and when* $(n,a) = (20,4)$.



The digraph consists of one loop plus cycles of equal length whenever n is prime (see Chapter 6). This fails when n is not prime, although when n and a are relatively prime the function is still injective and the digraph consists of cycles. Roughly speaking, the divisors of n lie on shorter cycles than the non-divisors of n.

7.42. *Orbits in* $\mathbb{Z}_{13}$ *under multiplication.*

multiplier	partition	order
1	(1)(2)(3)(4)(5)(6)(7)(8)(9)(10)(11)(12)	1
2	(2,4,8,3,6,12,11,9,5,10,7,1)	12
3	(3,9,1)(2,6,5)(4,12,10)(7,8,11)	3
4	(4,3,12,9,10,1)(2,8,6,11,5,7)	6
5	(5,12,8,1)(2,10,11,3)(4,7,9,6)	4
6	(6,10,8,9,2,12,7,3,5,4,11,1)	12
7	(7,10,5,9,11,12,6,3,8,4,2,1)	12
8	(8,12,5,1)(2,3,11,10)(4,6,9,7)	4
9	(9,3,1)(2,5,6)(4,10,12)(7,11,8)	3
10	(10,9,12,3,4,1)(2,7,5,11,6,8)	6
11	(11,4,5,3,7,12,2,9,8,10,6,1)	12
12	(12,1)(2,11)(3,10)(4,9)(5,8)(6,7)	2

7.43. *Short proof of Fermat's Little Theorem.* When a and p are relatively prime, we have proved that $\{a, 2a, \dots, (p-1)a\}$ have distinct remainders modulo p. Thus the product $\prod_{i=1}^{p-1} i_a$ is congruent to the product $\prod_{i=1}^{p-1} i$

modulo p. In other words, $(p-1)!a^{p-1} \equiv (p-1)! \pmod p$. Since p is prime, $(p-1)!$ is relatively prime to p, and thus $(p-1)!$ has a multiplicative inverse modulo p. Multiplying both sides of the congruence by this inverse has the effect of canceling $(p-1)!$, and we conclude that $a^{p-1} \equiv 1 \pmod p$.

7.44. *341 divides* $2^{341}-2$*, although 341 is not prime* (and hence the converse to Fermat's Little Theorem is false). The number 341 is the product of the primes 11 and 31. A number is divisible by the product of two primes if and only if it is divisible by each of them. Hence it suffices to prove that 2^{341} has remainder 2 modulo 11 and has remainder 2 modulo 31. For each computation, we use Fermat's Little Theorem.

$$2^{341} \equiv (2^{11})^{31} \equiv 2^{31} \equiv 2\cdot(2^{10})^3 \equiv 2\cdot 1^3 \equiv 2(\pmod{11}).$$

$$2^{341} \equiv (2^{31})^{11} \equiv 2^{11} \equiv 2\cdot(2^5)(2^5) \equiv 2\cdot 32\cdot 32 \equiv 2\cdot 1\cdot 1(\pmod{31}).$$

Alternatively, without using Fermat's Little Theorem, notice that $2^{10} = 1024$, which is $3\cdot 341+1$. Hence $2^{10} \equiv 1 \pmod{341}$, and we compute directly

$$2^{341} = (2^{10})^{34}\cdot 2 \equiv 1^{34}\cdot 2 \equiv 2 \pmod{341}.$$

7.45. *A polynomial congruent to 0.* Given a positive integer m, let $\prod_{i=1}^k p_i^{a_i}$ be the prime factorization of m. Let $f(x) = \prod_{i=1}^k (x^{p_i} - x)^{a_i}$. For every $x \in \mathbb{Z}$, we have $x^{p_i} - x$ divisible by p_i. Hence $f(x)$ is divisible by all the prime factors of m, with sufficient multiplicity, so $m|f(x)$.

7.46. *Equivalence classes under cyclic shifts.* Let R be the relation on $[a]^p$ defined by putting $(x,y) \in R$ if the p-tuple y arises from x by a cyclic shift.

a) R is an equivalence relation. Every p-tuple is a cyclic shift of itself, so R is reflexive. The inverse of a cyclic shift is a cyclic shift, so R is symmetric. The composition of two cyclic shifts is a cyclic shift, so R is transitive. Hence R is an equivalence relation.

b) If p is prime and $a \in \mathbb{N}$, then p divides $a^p - a$. To obtain a set S of size $a^p - a$, we discard from $[a]^p$ the a elements that use only one value. Each forms an equivalence class of size 1 under R. If the remaining equivalence classes partition S into sets of size p, then p divides $[a]^p - a$.

If $x \in S$, then p cyclic shifts apply to x, so each class has size at most p. Suppose that some class has size less than p In shifting an element by $0, 1, \dots, p-1$ positions to obtain all members of the class, some member must appear twice. If y appears when we shift x by i or by j, then shifting y by $j-i$ positions does not change it. Let $b = j-i$; shifting y by any multiple of b positions also leaves it unchanged. By Lemma 7.27, 1 is a multiple of b modulo p. We conclude that shifting y by one position leaves it unchanged. This requires that each entry in y is the same as the next, but we explicitly omitted such p-tuples from S. The contradiction implies that R partitions S into equivalence classes of size p.

c) (Fermat's Theorem) If p is prime and a is not a multiple of p, then $a^{p-1} \equiv 1 \pmod p$. Since we may choose any representative of a congruence class for modular computation, part (b) holds for every integer a. We have proved that p divides $a^p - a$, which means $a^p \equiv a \pmod p$. Since p does not divide a, Corollary 7.28 provides the multiplicative inverse b such that $ab \equiv 1 \pmod p$. Note that $a^p b = a^{p-1}ab \equiv a^{p-1} \pmod p$. Multiplying both sides of $a^p \equiv a \pmod p$ by b yields $a^{p-1} \equiv 1 \pmod p$.

7.47. *If p is an odd prime, then* $2(p-3)! \equiv -1(\pmod p)$. If p is prime, then Wilson's Theorem implies $(p-1)! \equiv -1(\pmod p)$. But, $(p-1)! = (p-1)(p-2)(p-3)!$. If $p > 2$, then $(p-1)(p-2) \equiv (-1)(-2) \equiv 2 \pmod p$. Hence $2(p-3)! \equiv (p-1)! \equiv -1(\pmod p)$ if p is an odd prime.

7.48. *If $(p-1)! \equiv -1 \pmod p$, then p is prime.* (This is the converse of Wilson's Theorem.) If $n = 4$, then $(n-1)! \equiv 2 \pmod n$. We prove that if n is not prime and not equal to 4, then $(n-1)! \equiv 0(\pmod n)$. If n is not a prime and is not the square of a prime, then n is the product of two distinct natural numbers a, b that are less than n (for example, let a be a prime factor of n, and let $b = n/a$). Since a, b are both factors of $(n-1)!$, $(n-1)!$ is divisible by $a \cdot b = n$. If $n = p^2$ where p is prime and $p > 2$, then p and $2p$ are both less than n, so $(n-1)!$ is divisible by $p \cdot 2p = 2n$, and hence $(n-1)!$ is divisible by n.

7.49. *The set of permutations of $[n]$, viewed as a set of functions from $[n]$ to $[n]$, forms a group under the operation of composition.* Composition is a binary operation, with the composition of two bijections from $[n]$ to $[n]$ being itself a bijection from $[n]$ to $[n]$.

The identity permutation is the identity element for the group.

Composition of functions is associative (Proposition 4.32).

Every permutation $f\colon [n] \to [n]$ is a bijection. Every bijection has an inverse as a function. The inverse function for f is another bijection from $[n]$ to $[n]$, and thus it is a permutation of $[n]$ whose composition with f is the identity permutation.

7.50. *The set S of polynomials of degree k with coefficients in $\mathbb{Z}_p$ is a group under addition modulo p.* This addition is a binary operation on the set; the definitions of addition of polynomials and addition modulo p imply that the sum of two elements of S is in S. The identity element is the polynomial with coefficients all $\overline{0}$. The inverse of $f \in S$ is the polynomial whose coefficients are the inverses in $\mathbb{Z}_p$ of the coefficients of f. Associativity of addition of elements of S follows from the associativity of addition modulo p for each coefficient.

7.51. *For every element x of a group G, there is a unique element y such that* $y \circ x = 1$. The definition of group in the text requires the existence of an element y, called the *inverse* of x, such that $y \circ x = 1 = x \circ y$. If there is another element y' such that $1 = y' \circ x$, then we compose both sides of the equation with y and apply associativity to obtain

$$y = 1 \circ y = (y' \circ x) \circ y = y' \circ (x \circ y) = y' \circ 1 = y'.$$

7.52. *The function $f_y\colon G \to G$ defined by $f_y(x) = y \circ x$ is surjective, given that G is a group under the operation $\circ$.* Since G is a group, it has an element y^{-1} such that $y \circ y^{-1}$ is the identity element. Given $w \in G$, let $x = y^{-1} \circ w$. Now $f_y(x) = y \circ (y^{-1} \circ w)$. Using associativity, we have $f_y(x) = (y \circ y^{-1}) \circ w = w$. Since w was arbitrary, f is surjective. A function from a finite set to itself that is surjective is also injective (since the image of a surjective function is at least as large as the domain) and hence is bijective.

7.53. *The order of a group element divides the order of the group.* The *order* of a finite group G is $|G|$, and the identity element is written as 1 when the group operation is represented as multiplication. The *order* of an element $x \in G$ is the least k such that $x^k = 1$.

Note first that every $x \in G$ has a well-defined order. Successive composition of x must yield a repetition, $x^i = x^j$ with $0 \le i < j$. Cancellation using multiplications by x^{-1} yields $x^{j-i} = 1$. Hence there is a least such k.

For $y \in G$, let $S_y = \{y, yx, yx^2, \ldots, yx^{k-1}\}$, where k is the order of x. The set S_y consists of k distinct elements; if $yx^i = yx^j$ for some $0 \le i < j < k$, then $x^{j-i} = 1$, which contradicts the definition of k.

Let R be the relation on G that consists of the ordered pairs (y, z) such that $z \in S_y$. Since $y \in S_y$, R is reflexive. Since $z = yx^i$ implies $zx^{k-i} = y$, R is symmetric. Since $y = wx^i$ and $z = yx^j$ yield $z = wx^{i+j}$, and the $i + j$ can be reduced to the value between 0 and $k-1$ that is congruent to it modulo k (by eliminating the factor x^k, if necessary), R is transitive.

Thus R is an equivalence relation on G. By construction, S_y is of the equivalence class of y under R, so the sets of the form S_y for $y \in G$ are the equivalence classes of R. Since the equivalence classes partition G and we have shown that they all have size k, we conclude that k divides $|G|$.

8. THE RATIONAL NUMBERS

8.1. *Given that x is rational and a, b, c are irrational,*

a) $x + a$ is irrational - TRUE. Otherwise, a is a difference of rational numbers, which must be rational.

b) xa is rational - FALSE. If x is zero, the xa is zero, which is rational. (For $x \neq 0$, the statement would be true.)

c) $a \cdot b \cdot c$ is irrational - FALSE. Let $a = b = c = 2^{1/3}$.

d) $(x + a)(x + b)$ is irrational - FALSE. Let $a = \sqrt{2}$ and $b = -\sqrt{2}$.

8.2. *If f is a polynomial with rational coefficients, then there is a polynomial with integer coefficients that has the same zeros as f.* Let m be the least common multiple (the product also works) of the denominators of the coefficients of f when they are written in lowest terms. Let g be the polynomial whose coefficients are m times the coefficients of f. By the choice of m, g has integer coefficients. By the distributive law, the value $g(x)$ is m times the value $f(x)$. Thus $f(x) = 0$ if and only if $g(x) = 0$.

8.3. *$a, b, c \in \mathbb{Q}$ with $a \neq 0$, and $ax^2 + bx + c = 0$ has two solutions, then the product of the solutions is rational.* If r and s are the solutions, then $x - r$ and $x - s$ are factors of $x^2 + (b/a)x + (c/a)$. Thus $(x - r)(x - s) = x^2 - (r + s)x + rs = x^2 + (b/a)x + (c/a)$. Since polynomials are equal only when their corresponding coefficients are equal, we have $rs = c/a$, and thus rs is rational.

8.4. *Explanation of restriction on the definition of a line.* The line $L(a, b)$ determined by integers a and b is $\{(x, y) \in \mathbb{R}^2 \colon bx = ay\}$. We require that a and b are not both 0, because otherwise the set of solutions would be the set of all points in the plane.

8.5. *The image of the function $f \colon \mathbb{R} \to \mathbb{R}^2$ defined by $f(t) = \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right)$ is the circle of radius 1 centered at the origin.* Theorem 8.12 states that $x^2 + y^2 = 1$ if and only if there exists a real number t such that

$$(x, y) = \left(\frac{1 - t^2}{1 + t^2}, \frac{2t}{1 + t^2}\right).$$

8.6. *The line of slope m through (p, q) is defined parametrically by $\{(p + t, q + mt) \colon t \in \mathbb{R}\}$.* A point (x, y) is on the line of slope m through (p, q) if and only if $\frac{y-q}{x-p} = m$. We rewrite this as $y - q = m(x - p)$ and let $t = x - p$. This yields $x = p + t$ and $y = q + mt$.

8.7. *Examples of Pythagorean triples.* Pythagorean triples with no common factors arise as $(r^2 - s^2, 2rs, r^2 + s^2)$ or $(2rs, r^2 - s^2, r^2 + s^2)$. The given examples arise with parameter values as indicated below:

$(5, 12, 13)$	$(8, 15, 17)$	$(7, 24, 25)$	$(20, 21, 29)$	$(9, 40, 41)$
$r = 3$	$r = 4$	$r = 4$	$r = 5$	$r = 5$
$s = 2$	$s = 1$	$s = 3$	$s = 2$	$s = 4$

8.8. *The equation $1/x + 1/y = 1/(x + y)$ has no solution in real numbers.*

Proof 1 (contradiction & ad hoc argument). Suppose x, y is a solution; we may assume $x, y \neq 0$. Multiplying both sides by $xy(x + y)$ yields $(x + y)^2 = xy$. Since the left side of this is positive, xy must be positive. The equation $(x + y)^2 = xy$ also can be rewritten as $x^2 + xy + y^2 = 0$, but now we have 0 as the sum of three positive numbers. There are many other ways to manipulate the equation to obtain a contradiction, but this one is particularly short.

Proof 2 ("lowest terms"). Rewriting the equation as $x^2 + xy + y^2 = 0$, suppose $x = p/q$ and $y = r/s$ are a solution with x and y in lowest terms. Multiplying by $q^2 s^2$, we have $p^2 s^2 + pqrs + r^2 q^2 = 0$. Letting $a = ps$ and $b = qr$, we have $a^2 + ab + b^2 = 0$ for the integers a, b. We earlier proved that this equation has no integer solutions except $a = b = 0$. This exercise has extended the proof to show that even when rational numbers are allowed, this equation has no solutions except $a = b = 0$.

8.9. *A fraction is in lowest terms if and only if its denominator is the smallest positive denominator among all fractions representing the same rational number.* First we prove sufficiency, by the contrapositive method. If a, b have a common factor m, then we can write $a = cm$ and $b = dm$, and we conclude $c/d = a/b$ by the definition of the equivalence relation. Hence we can replace a/b by c/d and have a smaller denominator. For necessity, suppose a and b are relatively prime and $a/b = c/d$ with $d > 0$. It suffices to prove $b \leq d$. From $ad = bc$, we conclude that b divides ad. Since a and b are relatively prime, this requires $b|d$, which implies $b \leq d$.

8.10. *If a/m and b/n are rational numbers in lowest terms, then $(an + bm)/(mn)$ is in lowest terms if and only if m and n are relatively prime.* If m, n have a common factor, then it also divides $an + bm$, and $(an + bm)/(mn)$ is not in lowest terms.

Suppose that m, n have no common factor. To show that $(an + bm)/(mn)$ is in lowest terms, we prove that every prime number d dividing mn does not divide $an + bm$. Since m, n have no common factor, d must divide m or n (this is why we take d to be a prime factor). By symmetry, we may suppose that $d|m$. Since a/m is in lowest terms, d does not divide a. Now d divides bm but not a or n, so it cannot divide $an + bm$.

8.11. *If x and y are real numbers such that $x/y = \sqrt{2}$, then $(2y - x)/(x - y) = \sqrt{2}$.* Dividing numerator and denominator by y, we obtain

$$\frac{2y - x}{x - y} = \frac{2 - x/y}{x/y - 1} = \frac{2 - \sqrt{2}}{\sqrt{2} - 1} = \frac{\sqrt{2}(\sqrt{2} - 1)}{\sqrt{2} - 1} = \sqrt{2}.$$

8.12. *If a, b, c, d are positive integers with $a/b < c/d$, then $a/b < (a+c)/(b+d) < c/d$.* Since a, b, c, d are positive, $a/b < c/d$ is equivalent to $ad < bc$. Adding ab or cd to both sides yields $a(b+d) < b(a+c)$ or $d(a+c) < c(b+d)$, respectively, which are equivalent to $a/b < (a+c)/(b+d)$ and $(a+c)/(b+d) < c/d$, respectively. In terms of batting averages, this says that a single player's average over the full season is between his averages over two disjoint parts of the season. In terms of slopes of lines, this says that the slope of the sum of two vectors in the first quadrant, placed at the origin, is between the slopes of the two vectors.

8.13. *If a, b, c, d are positive integers with $a \le c \le d$ and $c/d \le a/b$, then $b - a \le d - c$.* From $c/d \le a/b$, we obtain $bc \le ad$. Subtracting ac from both sides yields $bc - ac \le ad - ac$, or $(b-a)c \le (d-c)a$. Since $a \le c$, we have $(b-a)cle(d-c)c$, and now we cancel c to obtain the desired inequality.

This conclusion does not always hold if $a \le d < c$ and $c/d \le a/b$. Consider the example $(a, b, c, d) = (2, 1, 5, 3)$. Now $a \le d < c$ becomes $2 \le 3 < 5$, and $c/d \le a/b$ becomes $5/3 \le 2/1$, but $b - a = -1$ and $d - c = -2$.

8.14. *The graph of the set of points in $S = \{(x, y) \in \mathbb{R}^2 \colon x^2 - y^2 = 1\}$ with positive first coordinate is the right branch of a hyperbola, located between the rays $y = x$ in the first quadrant and $y = -x$ in the fourth quadrant and asymptotic to these two rays.* Sketching the points solving the equation suggests the description given.

Solving for one variable in terms of the other parametrizes the solutions to $f(x, y) = c$, but we seek a parametrization that maps rational values of the parameter into rational points. (This is useful in later applications; for example, ratios of polynomials can be integrated.)

As done for the circle in the text, we seek a rational parametrization using the slope of the line between (x, y) and $(-1, 0)$. With $y = t(x+1)$, the values $-1 < t < 1$ are the valid range of the parameter. Substituting $y = t(x+1)$ in $x^2 - y^2 = 1$ yields $x^2(1-t^2) - 2t^2x - (1+t^2) = 1$. Solving for x by the quadratic formula yields $x = (t^2 \pm 1)/(1-t^2)$. Since $|t| < 1$ and we consider only $x > 0$, the parametrization is

$$\left\{\left(\frac{1+t^2}{1-t^2}, \frac{2t}{1-t^2}\right) \colon -1 < t < 1\right\}.$$

8.15. *Symmetry considerations in the geometric proof of the Pythagorean Theorem.* The outer square has sides of length $a + b$. Breaking each side into segments of lengths a and b and drawing segments to connect the breakpoints creates four triangles. Each triangle has sides of lengths a and b separated by a right angle, so we can obtain each triangle from the others by rotating around the center of the figure (the triangles are *congruent*). Thus the third sides are equal and the areas are equal. The rotational symmetry also implies that the angles of the central quadrilateral are equal. Since they are equal and sum to 360 degrees, they are right angles, and the central quadrilateral is a square.

8.16. *The Billiard Problem.* Suppose the ball starts along a line with a rational slope $s = m/n$ in lowest terms. The integer points on the line L along which the ball starts are $\{(x, y) \in \mathbb{Z} \times \mathbb{Z} \colon y = (m/n)x\}$; these are the integer solutions to $ny = mx$. The positive point on this line that is closest to the origin is (n, m). The coordinates of the closest point must be relatively prime, since otherwise dividing out a common factor yields a closer integer point on the line. Conversely, since m, n are relatively prime, each solution (x, y) to $ny = mx$ must satisfy $n|x$ and $m|y$.

Consider the path P that the ball follows until it hits a corner. We claim that the total horizontal distance is n and the total vertical distance is m. In other words, when P is laid out along L, it extends from $(0, 0)$ to (n, m). After the ball travels one unit to the right, it bounces and starts heading left. Correspondingly, L crosses the line $x = 1$. With the ith bounce of P off a vertical boundary, L crosses the line $x = i$. Similarly, with the jth bounce of P off a horizontal boundary, L crosses the line $y = j$. The ball reaches a corner when L reaches (n, m), since this is when it simultaneously reaches a vertical integer line and a horizontal integer line. By the correspondence between bounces and crossings of grid lines, the corner is on the line $x = 1$ if and only if n is odd, and it is on the line $y = 1$ if and only if m is odd. Hence the ball ends at $(1, 1)$, $(1, 0)$, $(0, 1)$ if and only if the parities of n and m are (odd,odd), (odd,even), or (even,odd), respectively. It never ends at (0,0), because that would require n, m both even, which cannot happen since $\gcd(m, n) = 1$.

8.17. *The set of rational numbers is countable.* Specifying a bijection from $\mathbb{Q}$ to $\mathbb{N}$ is equivalent to listing the elements of $\mathbb{Q}$ in order, indexed by $\mathbb{N}$, so that each rational number appears exactly once. We use for each rational number the canonical representative p/q in lowest terms.

Since each rational number x is represented by a unique pair (p, q) of integers in this way, it has a specific integer value of $f(x) = |p| + |q|$. We list the rational numbers x in increasing order of $f(x)$. We can do this because for each n there are finitely many rational numbers with $f(x) = n$. In fact, there are at most $2n - 1$, since for each such x the value of p is an integer between $-n + 1$ and $n - 1$, and then q is $n - |p|$.

So, for each $n \in \mathbb{N}$ in increasing order, we list the rational numbers with $f(x) = n$ in increasing order of p, skipping those where p and $n - |p|$ have a common factor, since those are not in lowest terms and occur earlier. This lists each rational number exactly once, so it is a bijection.

8.18. *No prime number has a rational square root.* Suppose that p is prime and $x^2 = p$ has a rational solution. We may choose $x = r/s$ in lowest terms, which implies that r, s are relatively prime integers. From $x^2 = p$ we obtain $r^2 = ps^2$. Since p divides the right side, we also have $p|r^2$, which implies $p|r$ since p is prime (a prime dividing the product of two numbers must divide one of the factors). Now $p|r$ yields $p^2|r^2$. Since $r^2 = ps^2$, we also have $p^2|(p_s^2)$. By canceling like factors, we obtain $p|s^2$. Reasoning as before, we conclude that $p|s$. Now we have p as a common factor of r and s, which contradicts the choice of r/s in lowest terms.

8.19. *If an integer n has a rational square root, then n is the square of an integer.* Suppose that $x^2 = n$ has a rational root $x = r/s$ in lowest terms. Since r and s are relatively prime, also r^2 and s^2 are relatively prime. ("Relatively prime" means that r and s have no common prime factors. Squaring doubles the exponents on prime factors but doesn't change the set of prime factors, so r^2 and s^2 are also relatively prime.)

The equation yields $r^2 = ns^2$. Thus s^2 divides r^2. Since r^2 and s^2 are relatively prime, this requires that $s^2 = 1$. Thus $s = 1$, and x is an integer.

8.20. *Solutions to $f(x) = 0$ when $f(x) = x^6 + cx^5 + 1$ and c is an integer.*

a) When $c = 2$, -1 is a solution; when $c = -2$, 1 is a solution. $(-1)^6 + 2(-1)^5 + 1 = 0$, and $1^6 - 2(1)^5 + 1 = 0$.

b) When $c \neq \pm 2$, there are no rational solutions. If there is a rational solution, written as p/q in lowest terms, then $p|1$ and $q|1$, by the Rational Zeros Theorem. Hence the only candidates are ± 1. When $x = \pm 1$, $x^6 + 1 = 2$. Hence $cx^5 = -2$, which requires $c \in \{2, -2\}$ when $x \in \{1, -1\}$.

8.21. *Solutions to $f(x) = 0$ when $f(x) = 2x^3 + x^2 + x + 2$.* If there is a rational solution, written as p/q in lowest terms, then $p|2$ and $q|2$, by the Rational Zeros Theorem. Hence the candidates are $\{\pm 2, \pm 1, \pm 1/2\}$. With all coefficients of f positive, no positive x is a zero. Among the negative candidates, only -1 is a zero. We factor $f(x) = 2x^3 + x^2 + x + 2 = (x + 1)(2x^2 - x + 2)$. By the quadratic formula, the polynomial $f(x)/(x + 1)$ has no real zeros, since $(-1)^2 - 4 \cdot 2 \cdot 2 < 0$. This is suggested by graphing the function: the function does not cross the horizontal axis when x is positive, and on the negative side it seems to crosses only at $x = -1$.

8.22. *The Rational Zeros Theorem implies that the kth root of an integer is not a rational number unless the kth root is an integer.* The Rational Zeros Theorem states that every rational solution to the polynomial equation $\sum_{i=0}^{k} c_i x^i = 0$ with integer coefficients, when written as $x = p/q$ in lowest terms, satisfies $q|c_k$ and $p|c_0$. The kth root of an integer m satisfies the equation $x^k - m = 0$. Here the coefficients are $c_k = 1$ and $c_0 = m$. The theorem implies that $q|1$, which implies that $x = p/q$ is an integer.

8.23. *$ax^2 + bx + c = 0$ has no rational solution for odd integers a, b, c.*

Proof 1 (parity). Let p/q be a rational solution in lowest terms. The quadratic formula yields $p/q = (-b \pm \sqrt{b^2 - 4ac}/(2a)$. After clearing fractions, we have $2ap + bq = \pm q\sqrt{b^2 - 4ac}$. Squaring both sides yields $4a^2p^2 + 4abpq + b^2q^2 = q^2b^2 - 4acq$, which simplifies to $a^2p^2 + abpq + qac = 0$. Since p/q is in lowest terms, p and q are both odd or are one odd and one even. In each case, there are an odd number of odd terms among $\{a^2p^2, abpq, qac\}$ if a, b, c are all odd, so they can't sum to 0. The contradiction proves that no such soluion exists, as in Theorem 2.3.

Proof 2 (properties of square roots and divisibility). If $(-b \pm \sqrt{b^2 - 4ac})/(2a)$ is rational when a, b, c are integers, then $\sqrt{b^2 - 4ac}$ must be rational. Since all rational square roots of integers are integers (Theorem 8.14), we have $b^2 - 4ac = d^2$ for some integer d. Since b is odd, d^2 and d are odd. Consider $4ac = b^2 - d^2$. Since every odd square is congruent to 1 modulo 8, we have $4ac$ divisible by 8, which implies that a or c is even.

8.24. *Without using the Rational Zeros Theorem, all rational zeros of a polynomial with integer coefficients and leading coefficient 1 are integers.* We generalize the proof of Theorem 8.14. Let $p(x) = \sum_{i=0}^{d} c_i x^{d-i}$ with each $c_i \in \mathbb{Z}$ and $c_0 = 1$. Let m/n be a rational zero of p, expressed in lowest terms, and suppose that $n > 1$; we obtain a contradiction. Note that evaluating p at m/n and multiplying by n^d yields $m^d + \sum_{i=1}^{d} n^i c_i m^{d-i} = 0$, and each term in the sum has n as a factor.

By the Division Algorithm, we can write m as $nq + r$ with $0 < r < n$. Using $r = m - nq$, we compute

$$\frac{m^{d-1}}{n^{d-1}} = \frac{m^{d-1}r}{n^{d-1}r} = \frac{m^d - m^{d-1}nq}{n^{d-1}r} = \frac{-nm^{d-1}(c_1 - q) - \sum_{i=2}^{d} n^i c_i m^{d-i}}{n^{d-1}r}$$
$$= \frac{-m^{d-1}(c_1 - q) - \sum_{i=2}^{d} n^{i-1} c_i m^{d-i}}{n^{d-2}r}$$

We have succeeded in canceling a factor of n from the numerator and denominator, and yet the remaining numerator and denominator are both integers. However, $n^{d-2}r < n^{d-1}$, since $r < n$. We have thus expressed m^{d-1}/n^{d-1} as a rational number with denominator smaller than n^{d-1}. Since m and n have no common factors, the Fundamental Theorem of Arithmetic (unique prime factorization), implies that m^{d-1}/n^{d-1} is already a rational number in lowest terms. The contradiction implies that $n = 1$, and a rational zero must be an integer.

8.25. *A Pythagorean triple in increasing order that cannot be written in the form $(r^2 - s^2, 2rs, r^2 + s^2)$ for integers r, s.* In a primitive Pythagorean triple, r and s have opposite parity, and hence $r^2 - s^2$ is odd. Thus all primitive Pythagorean triples in which the smallest number is even have this property. An example is $(8, 15, 17)$.

8.26. *Every integer greater than 2 belongs to a Pythagorean triple not containing 0.* The Pythagorean triples are the triples of the form $(r^2 - s^2, 2rs, r^2 + s^2)$, where $r, s \in \mathbb{Z}$, and the integer multiples of such triples. The even integer $2k$ belongs to the Pythagorean triple $(k^2 - 1, 2k, k^2 + 1)$ formed by setting $r = k$ and $s = 1$. The odd integer $2k - 1$ belongs to the Pythagorean triple $(2k - 1, 2k^2 - 2k, 2k^2 - 2k + 1)$ formed by setting $r = k$ and $s = k - 1$.

8.27. *The sum of Pythagorean triples (a, b, c) and (u, v, w) (under componentwise addition) is a Pythagorean triple if and only if $av = bu$.* Suppose that $a^2 + b^2 = c^2$ and $u^2 + v^2 = w^2$. Note that $(a + u)^2 + (b + v)^2 = c^2 + 2au + 2bv + w^2$. Thus the sum is a Pythagorean triple if and only if $au + bv = cw$.

Sufficiency. Suppose that $av = bu$. It suffices to show that $au + bv = cw$. Since both are positive, it suffices to show that their squares are equal. Note that $a^2v^2 + b^2u^2 = 2aubv$ when $av = bu$. Thus

$$(cw)^2 = c^2w^2 = (a^2 + b^2)(u^2 + v^2) = a^2u^2 + b^2u^2 + a^2v^2 + b^2v^2 = (au + bv)^2.$$

Necessity. If the sum is a Pythagorean triple, then we have $au + bv = cw$. Squaring both sides yields $(au + bv)^2 = (a^2 + b^2)(u^2 + v^2)$. Canceling $a^2u^2 + v^2v^2$ yields $a^2v^2 + b^2u^2 = 2aubv$, which is equivalent to $(av - bu)^2 = 0$. This requires $av = bu$.

Alternative geometric viewpoint. The length of the segment from the origin to (a, b) is c, and the length of the segment from the origin to (u, v) is w. In order for the sum to be a Pythagorean triple, the length of the segment from the origin to $(a + u, b + v)$ must be $c + w$. This holds only if the first two segments are collinear, which requires $a/b = u/v$ (for b, v nonzero), or $av = bu$.

8.28. *Probability and Pythagorean triples.* Let x and y be integers chosen at random from [20] (each with probability $1/20$, independently).

a) The probability that $x^2 + y^2$ is the square of an integer is $7/200$. The Pythagorean triples with $a, b \le 20$ are $(3, 4, 5)$, $(6, 8, 10)$, $(9, 12, 15)$, $(12, 16, 20)$, $(15, 20, 25)$, $(5, 12, 13)$, $(8, 15, 17)$. Thus there are 14 choices for (x, y) such that $x^2 + y^2$ is the square of an integer.

b) The probability that x and y belong to a Pythagorean triple is $21/200$. Each Pythagorean triple with $a, b, c \le 20$ yields six successful choices for (x, y), and there are two more from $(15, 20, 25)$. Thus there are 42 successful choices.

8.29. *Alternative proof of characterization of Pythagorean triples.* Let (a, b, c) be a Pythagorean triple such that a, b, c have no common factor (thus $\gcd(a, b) = \gcd(b, c) = \gcd(a, c) = 1$).

a) Exactly one of a and b is even. If both are even, then c^2 and also c are even, and a, b, c have the common factor 2. If neither is even, then a^2 and b^2 are congruent to 1 modulo 4, and c^2 is congruent to 2 modulo 4, but all even squares are divisible by 4.

b) If a is the even member of $\{a, b\}$, then $(c + b)/2$ and $(c - b)/2$ are relatively prime and are squares of integers. We may let $a = 2x$, where x is an integer. Since b and c are odd, both $(c + b)/2$ and $(c - b)/2$ are integers. Now $4x^2 = c^2 - b^2$ yields $x^2 = \frac{c+b}{2}\frac{c-b}{2}$. Since $\gcd(b, c) = 1$, also $(c + b)/2$ and $(c - b)/2$ have no common factors. Since their product is a square and they are relatively prime, each must be a square.

c) Letting $y^2 = (c - b)/2$ and $z^2 = (c + b)/2$, we have the parametrization $a = 2yz$, $b = z^2 - y^2$, and $c = z^2 + y^2$. The linear system $c + b = 2z^2$ and $c - b = 2y^2$ yields b and c. Now $x^2 = y^2z^2$ and $a = 2x$ yields $a = 2yz$.

8.30. *Solution of the general cubic equation.* Consider the equation $ax^3 + bx^2 + cx + d = 0$ with $a \ne 0$ and $a, b, c, d \in \mathbb{R}$.

a) Change of variables $x = s(y + t)$ to reduce to solving $y^3 + Ay + B = 0$; set $s = a^{-1/3}$ and $t = -b/(3as)$. With $x = s(y + t)$, we have

$$ax^3 + bx^2 + cx + d = as^3(y^3 + 3y^2t + 3yt^2 + t^3) + bs^2(y^2 + 2yt + t^2) + cs(y + t) + d.$$

Requiring this to equal $y^3 + Ay + B$ yields linear equations for s and t to make the coefficients of y^3 and y^2 be 1 and 0. These are $as^3 = 1$ and $3as^3t + bs^2 = 0$. We set $s = a^{-1/3}$ and $t = -b/(3as)$. These yield $A = -3t^2 + cs$ and $B = -2t^3 + cst + d$.

b) Change of variables $y = z + r/z$ to reduce $y^3 + Ay + B = 0$ to a quadratic equation in z^3; set $r = -A/3$. With $y = z + r/z$ (and assuming that $z \ne 0$), we have

$$y^3 + Ay + B = z^3 + 3zr + 3r^2/z + r^3/z^3 + Az + Ar/z + B.$$

Since the equation is $y^3 + Ay + B = 0$, we can multiply by z^3 to obtain $(z^3)^2 + (3r + A)z^4 + Bz^3 + (3r^2 + Ar)z^2 + r^3 = 0$. Choosing $r = -A/3$ reduces this to $(z^3)^2 + Bz^3 + r^3 = 0$.

c) Solution of the general cubic. We solve the quadratic in part (b) to obtain $z^3 = \frac{1}{2}(-B \pm \sqrt{B^2 - 4r^2})$, where $r = -A/3$ and A and B are determined from a, b, c, d as described in part (a). Taking the cube roots of these values to obtain z, we then set $y = z + r/z$ and $x = s(y + t)$. To be sure of obtaining all solutions for z, we must introduce the complex cube roots of z^3.

8.31. *If $f\colon \mathbb{Q}^* \to \mathbb{Q}^*$ (where $\mathbb{Q}^* = \mathbb{Q} - \{0\}$) such that $f(x+y) = \frac{f(x)f(y)}{f(x)+f(y)}$ for all $x, y \in \mathbb{Q}^*$, and $c = f(1)$, then $f(w) = c/w$ for $w \in \mathbb{Q}^*$.* Taking the reciprocal of both sides of the equation for f and letting $g(x) = 1/f(x)$ yields $g(x)g(y)[g(x)^{-1} + g(y)^{-1}] = g(x+y)$, and thus $g(y) + g(x) = g(x+y)$ for all $x, y \in \mathbb{Q}^*$. Letting also $g(0) = 0$ makes g a function defined on $\mathbb{Q}$ that satisfies the hypothesis of Theorem 8.21. By that theorem, $g(wx) = wg(x)$ for $w, x \in \mathbb{Q}$. For $w \neq 0$, we then have $f(w) = 1/g(w) = 1/(wg(1)) = c/w$.

8.32. *The watch with indistinguishable hands.* The watch stops between midnight and noon. We want to know whether the time can be determined from the positions of the hands.

a) If the watch has hour, minute, and second hands, then the answer is YES. Let the positions of the hour, minute, and second hands as a fraction of the way around the dial from 12 be given by x, y, z, respectively. We have $0 \le x, y, z < 1$, and there are integers $0 \le m < 12$ and $0 \le n < 60$ such that $12x = m + y$ and $60y = n + z$. An ambiquity means that analogous equations with integers i, j in place of m, n hold after some nonidentity permutation of x, y, z.

First consider the transposition (x, y). Using the additional equation $12y = i + x$, we have $144y = 12(i+x) = 12i + m + y$. Thus $y = (12i+m)/143$, and hence $x = (m+y)/12 = (12m+i)/143$. Incorporating the second hand, we have $y - x = \frac{n+z}{60} - \frac{j+z}{60} = \frac{n-j}{60}$, and also $y - x = \frac{12i+m}{143} - \frac{12m+i}{143} = \frac{11(i-m)}{143} = \frac{i-m}{13}$. Since 13 and 60 are relatively prime, this forces $y - x$ to be an integer. Hence $x = y$ and there is no ambiguity.

Since the hour hand determines the time by itself, the transposition (y, z) cannot yield an ambiguity. The transposition (x, z) leaves the minute hand unchanged. Since the minute hand determines the second hand, this forces $x = z$ and there is no ambiguity.

Finally, we consider 3-cycles. As (x, y, z) and (x, z, y) are inverses, we need only consider one of them. Suppose $12z = i + x$ and $60x = j + y$. Then $j + y = 5(12x) = 5(m + y)$, and hence $4y = j - 5m$. But now $n + z = 60y = 15(j - 5m) \in \mathbb{Z}$. This requires $z = 0$. Since z is the position of the hour hand in the second reading, this requires $x = y = z = 0$. If the event was *strictly* between midnight and noon, then this possibility is excluded.

b) If the watch has only hour and minute hands, then the answer is NO. Again consider the transposition (x, y). Using the additional equation $12y = i + x$, we have $144y = 12(i+x) = 12i + m + y$. Thus $y = (12i+m)/143$, and hence $x = (m+y)/12 = (12m+i)/143$. If there is no second hand, then every choice of i different from m yields an ambiguous time.