Do the following exercises from the text:
Chapter 2 (Section 2.3): 2, 12, 17(a)-(b), 23

2. Prove that $1^3 + 2^3 + \cdots + n^3 = \dfrac{n^2(n+1)^2}{4}$ for all $n \in \mathbb{N}$.

Proof. The proof is by induction on n. For $n \in \mathbb{N}$, let $S(n)$ be the statement

$$1^3 + 2^3 + \cdots + n^3 = \frac{n^2(n+1)^2}{4}.$$

Then $S(1)$ is the statement $1^3 = \dfrac{1^2(1+1)^2}{4}$, which is true since $1^3 = 1$ and $\dfrac{1^2(1+1)^2}{4} = 1$.

For the induction step, assume that $S(k)$ is true for some $k \geq 1$. Thus, we are assuming that

$$1^3 + 2^3 + \cdots + k^3 = \frac{k^2(k+1)^2}{4}.$$

Add $(k+1)^3$ to both sides of this equation to get

$$\begin{aligned} 1^3 + 2^3 + \cdots + k^3 + (k+1)^3 &= \frac{k^2(k+1)^2}{4} + (k+1)^3 \\ &= \frac{k^2(k+1)^2 + 4(k+1)^3}{4} \\ &= \frac{(k+1)^2(k^2 + 4(k+1))}{4} \\ &= \frac{(k+1)^2(k+2)^2}{4}. \end{aligned}$$

This shows that the truth of $S(k)$ implies the truth of $S(k+1)$. Hence, by the induction principle, $S(n)$ is true for all $n \in N$. $\square$

12. Show that the power set of any set X with exactly n elements has 2^n elements.

Proof. Use induction on the number n of elements of X. For $n \in \mathbb{N}$ let $S(n)$ be the statement: "Any set X with n elements has a power set $\mathcal{P}(X)$ with exactly 2^n elements."

For the base step of the induction argument, let X be any set with exactly 1 element, say $X = \{a\}$. Then the only subsets of X are the empty set $\emptyset$ and the entire set $X = \{a\}$. Thus $|\mathcal{P}(X)| = 2 = 2^1 = 2^{|X|}$, so the base case is true. For the induction step, assume that $k \in \mathbb{N}$ is arbitrary and that any set X with $|X| = k$ has $|\mathcal{P}(X)| = 2^k$.

Let X be any set with $|X| = k+1$, and count the number of subsets of X. Suppose $X = \{a_1, \ldots, a_k, a_{k+1}\}$. The subsets of X are of two types. First, there are all of the subsets of X that do not contain a_{k+1}, which consist of all subsets of $\{a_1, \ldots, a_k\}$. By the induction hypothesis, there are 2^k subsets of $\{a_1, \ldots, a_k\}$, so there are 2^k subsets of X that do not contain a_{k+1}. Then there are the subsets of X that do contain the element a_{k+1}. Every such subset of X has the form $Y \cup \{a_{k+1}\}$, where Y is a subset of X that does not contain a_{k+1}. Since our induction hypothesis is that there are 2^k subsets Y of $X \setminus \{a_1, \ldots, a_k\}$, there are also 2^k subsets of X that contain a_{k+1}. Hence, we conclude that there are $2^k + 2^k = 2 \cdot 2^k = 2^{k+1}$ subsets of X. Thus, we have shown that the truth of statement $S(k)$ implies the truth of statement $S(k+1)$. By the induction principle, $S(n)$ is true for all $n \in \mathbb{N}$. $\square$

17. The Fibonacci numbers are defined inductively by $f_1 = 1$, $f_2 = 1$, and $f_{n+2} = f_{n+1} + f_n$ for $n \in \mathbb{N}$.

    (a) Prove that $f_n < 2^n$ for all $n \in \mathbb{N}$.

    Proof. Use induction on n. Let $S(n)$ be the statement: "$f_n < 2^n$." For the base case, $f_1 = 1 < 2 = 2^1$ so $S(1)$ is true. Also, $S(2)$ is true since $f_2 = 1 < 2^2$. We will use the strong induction principle. Thus our induction hypothesis is that $f_k < 2^k$ for $1 \le k \le n$. Thus, let $n \ge 2$ be given. By the induction hypothesis and the definition of f_n,

    $$f_n = f_{n-1} + f_{n-2} < 2^{n-1} + 2^{n-2} < 2^{n-1} + 2^{n-1} = 2 \cdot 2^{n-1} = 2^n.$$

    By the strong induction principle, $S(n)$ is true for all $n \in \mathbb{N}$. $\square$

    (b) Prove that $f_{n+1}f_{n-1} = f_n^2 + (-1)^n$ for all $n \ge 2$.

    Proof. The proof is by induction on n. For $n \ge 2$ let $S(n)$ be the statement:

    $$f_{n+1}f_{n-1} = f_n^2 + (-1)^n.$$

    The statement $S(2)$ is true since, for $n = 2$, $f_{n+1}f_{n-1} = f_n^2 + (-1)^n$ is the statement $f_3 f_1 = f_2^2 + (-1)^2$ which is $2 \cdot 1 = 1^2 + 1$ which is true.
    Now assume that $k \ge 2$ and that $S(k)$ is true, that is, assume $f_{k+1}f_{k-1} = f_k^2 + (-1)^k$. Rewrite this as

    $$f_k^2 - f_{k+1}f_{k-1} = -(-1)^k = (-1)^{k-1}$$

    . Now consider the left hand side with k replaced by $k+1$. Then, using the recursive definitions of f_{k+1} and f_{k+2},

    $$\begin{aligned} f_{k+1}^2 - f_{k+2}f_k &= f_{k+1}(f_k + f_{k-1}) - f_{k+2}f_k \\ &= f_k(f_{k+1} - f_{k+2}) + f_{k+1}f_{k-1} \\ &= f_k(-f_k) + f_{k+1}f_{k-1} \\ &= -(f_k^2 - f_{k+1}f_{k-1}) \\ &= (-1)(-1)^{k-1} \\ &= (-1)^k. \end{aligned}$$

    Thus, if $S(k)$ is true for some $k \ge 2$, then $S(k+1)$ is also true. By the principle of induction, $S(n)$ is true for all $n \ge 2$. $\square$

23. Define the least common multiple of two nonzero integers a and b to be the nonnegative integer m such that both a and b divide m, and if a and b both divide any other integer n, then m also divides n. Prove that there exists a unique least common multiple of for any two nonzero integers a and b.

    Proof. Suppose a and b are nonzero integers. Let

    $$S = \{n \in \mathbb{Z} : n > 0,\ a \mid n \text{ and } b \mid n\}.$$

    $S \neq \emptyset$ since a and b both divide ab and $-(ab)$, and one of these two integers is positive. Since S is a nonempty subset of $\mathbb{N}$, it has a smallest element m. We claim that m is a least common multiple of a and b. By the definition of S, $a \mid m$ and $b \mid m$. Now let n be any positive integer such that $a \mid n$ and $b \mid n$. We need to show that $m \mid n$. To see this, divide n by m to get $n = mq + r$ where $0 \leq r < m$. Since $r = n - mq$ is a linear combination of m and n, and since a divides both m and n it follows that $a \mid r$. Similarly $b \mid r$. If $r > 0$, it follows that $r \in S$ and $r < m$, which contradicts that m is the smallest element of S. Thus, $r = 0$ and $n = mq$ so that $m \mid n$.

    To show that the least common multiple is unique, suppose that m and m' are both least common multiples. Then, $m \mid m'$ and $m' \mid m$, so that $m' = \pm m$ and since both are positive, $m = m'$. ☐

Supplemental Problems:

1. Show that any positive integer $n \geq 12$ can be written as a linear combination $3u + 7v$ for nonnegative integers u, v.

    ▶ **Solution.** Thus, the question is if any positive integer $n \geq 12$ can be written as $n = 3u + 7v$ for some nonnegative integers u and v. Thus, let $S(n)$ be the statement $n = 3u + 7v$ for some nonnegative integers u and v. Since $12 = 3 \cdot 4 + 0 \cdot 7$, $S(12)$ is true. Now assume that $S(k)$ is true for some $k \geq 12$. Then $k = 3u + 7v$ for some nonnegative integers u and v.

    Case 1: $v = 0$. In this case $u \geq 4$ since $k \geq 12$. Then $k+1 = 3(u-2)+7$ and $u-2 > 0$.

    Case 2: $v = 1$. In this case $u \geq 2$ since $k = 3u + 7 \cdot 1 \geq 12$. Thus, as in case 1, $k + 1 = 3(u - 2) + 7 \cdot 2$.

    Case 3: $v \geq 2$. In this case, $k + 1 = 3(u + 5) + 7(v - 2)$.

    Thus, if $k \geq 12$ and $k = 3u + 7v$, then $k + 1 = 3u' + 7v'$ so that if $S(k)$ is true, then so is $S(k+1)$. By the principle of mathematical induction, $S(k)$ is true for all $k \geq 12$. ◀

2. Compute the gcd of $m = -231$ and $n = 150$ and express it as a linear combination of m and n.

▶ **Solution.** Use the Euclidean Algorithm:

$$\begin{aligned} -231 &= (-2) \cdot 150 + 69 \\ 150 &= 2 \cdot 69 + 12 \\ 69 &= 5 \cdot 12 + 9 \\ 12 &= 1 \cdot 9 + 3 \\ 9 &= 3 \cdot 3 + 0 \end{aligned}$$

Thus $\gcd(-231,\, 150) = 3$. Reversing the process gives

$$\begin{aligned} 3 &= 12 - 9 = 12 - (69 - 5 \cdot 12) = 6 \cdot 12 - 69 = 6(150 - 2 \cdot 69) - 69 \\ &= 6 \cdot 150 - 13 \cdot 69 = 6 \cdot 150 - 13(-231 + 2 \cdot 150) \\ &= (-20) \cdot 150 + (-13)(-231). \end{aligned}$$

◀

3. Let $A = \begin{bmatrix} 2 & 1 \\ 0 & 2 \end{bmatrix}$. Using mathematical induction, show that $A^n = \begin{bmatrix} 2^n & n2^{n-1} \\ 0 & 2^n \end{bmatrix}$ for all positive integers n.

▶ **Solution.** Let $S(n)$ be the statement $A^n = \begin{bmatrix} 2^n & n2^{n-1} \\ 0 & 2^n \end{bmatrix}$.

Since $A^1 = A = \begin{bmatrix} 2 & 1 \\ 0 & 2 \end{bmatrix} = \begin{bmatrix} 2^1 & 1 \cdot 2^{1-1} \\ 0 & 2^1 \end{bmatrix}$, it follows that $S(1)$ is a true statement.

For the inductive step, assume that $S(k)$ is true. That is, assume that $k \geq 1$ and $A^k = \begin{bmatrix} 2^k & k2^{k-1} \\ 0 & 2^k \end{bmatrix}$. Then

$$\begin{aligned} A^{k+1} &= A^k \cdot A \\ &= \begin{bmatrix} 2^k & k2^{k-1} \\ 0 & 2^k \end{bmatrix} \cdot \begin{bmatrix} 2 & 1 \\ 0 & 2 \end{bmatrix} \\ &= \begin{bmatrix} 2^k \cdot 2 & 2^k + k2^{k-1} \cdot 2 \\ 0 & 2^k \cdot 2 \end{bmatrix} \\ &= \begin{bmatrix} 2^{k+1} & (k+1)2^k \\ 0 & 2^{k+1} \end{bmatrix}. \end{aligned}$$

The last matrix is of the form $\begin{bmatrix} 2^n & n2^{n-1} \\ 0 & 2^n \end{bmatrix}$ for $n = k+1$. Hence $S(k+1)$ is a true statement whenever $S(k)$ is true. It follows from the principle of mathematical induction that $S(n)$ is true for all $n \geq 1$, i.e., the proposed formula for A^n is valid for all $n \geq 1$. ◀

4. Prove that $2^n > n^3$ for every integer $n \geq 10$.

▶ **Solution.** Let $S(n)$ be the statement $2^n > n^3$. If $n = 10$, then $2^{10} = 1024 > 1000 = 10^3$ so $S(10)$ is a true statement.

For the inductive step, assume that $S(k)$ is true for some $k \geq 10$. Thus, we are assuming that $2^k > k^3$. Then

$$\begin{aligned} 2^{k+1} &= 2 \cdot 2^k > 2k^3 = k^3 + k^3 = k^3 + k \cdot k^2 \\ &> k^3 + 7k^2 = k^3 + 3k^2 + 3k^2 + k^2 > k^3 + 3k^2 + 3k + 1 = (k+1)^3. \end{aligned}$$

Reading from the beginning to the end of this chain of inequalities, we see that if $k \geq 10$ and $2^k > k^3$, then it follows that $2^{k+1} > (k+1)^3$. Thus, if $S(k)$ is true for some $k \geq 10$, then $S(k+1)$ is also true. By the principle of mathematical induction, it follows that $S(n)$ is true for all $n \geq 10$. ◀