Solution Manual for
A First Course in Abstract Algebra, with Applications
Third Edition
by Joseph J. Rotman

Exercises for Chapter 1

1.1 True or false with reasons.

(i) There is a largest integer in every nonempty set of negative integers.

Solution. True. If C is a nonempty set of negative integers, then

$$-C = \{-n : n \in C\}$$

is a nonempty set of positive integers. If $-a$ is the smallest element of $-C$, which exists by the Least Integer Axiom, then $-a \leq -c$ for all $c \in C$, so that $a \geq c$ for all $c \in C$.

(ii) There is a sequence of 13 consecutive natural numbers containing exactly 2 primes.

Solution. True. The integers 48 through 60 form such a sequence; only 53 and 59 are primes.

(iii) There are at least two primes in any sequence of 7 consecutive natural numbers.

Solution. False. The integers 48 through 54 are 7 consecutive natural numbers, and only 53 is prime.

(iv) Of all the sequences of consecutive natural numbers not containing 2 primes, there is a sequence of shortest length.

Solution. True. The set C consisting of the lengths of such (finite) sequences is a nonempty subset of the natural numbers.

(v) 79 is a prime.

Solution. True. $\sqrt{79} < \sqrt{81} = 9$, and 79 is not divisible by 2, 3, 5, or 7.

(vi) There exists a sequence of statements $S(1), S(2), \ldots$ with $S(2n)$ true for all $n \geq 1$ and with $S(2n-1)$ false for every $n \geq 1$.

Solution. True. Define $S(2n-1)$ to be the statement $n \neq n$, and define $S(2n)$ to be the statement $n = n$.

(vii) For all $n \geq 0$, we have $n \leq F_n$, where F_n is the nth Fibonacci number.

Solution. True. We have $0 = F_0$, $1 = F_1$, $1 = F_2$, and $2 = F_3$. Use the second form of induction with base steps $n = 2$ and $n = 3$ (verifying the inductive step will show why we choose these numbers). By the inductive hypothesis, $n - 2 \leq F_{n-2}$ and $n - 1 \leq F_{n-1}$. Hence, $2n - 3 \leq F_n$. But $n \leq 2n - 3$ for all $n \geq 3$, as desired.

(viii) If m and n are natural numbers, then $(mn)! = m!n!$.

Solution. False. If $m = 2 = n$, then $(mn)! = 24$ and $m!n! = 4$.

1.2 **(i)** For any $n \geq 0$ and any $r \neq 1$, prove that

$$1 + r + r^2 + r^3 + \cdots + r^n = (1 - r^{n+1})/(1 - r).$$

Solution. We use induction on $n \geq 1$. When $n = 1$, both sides equal $1 + r$. For the inductive step, note that

$$\begin{aligned}[1 + r + r^2 + r^3 + \cdots + r^n] + r^{n+1} &= (1 - r^{n+1})/(1 - r) + r^{n+1} \\ &= \frac{1 - r^{n+1} + (1 - r)r^{n+1}}{1 - r} \\ &= \frac{1 - r^{n+2}}{1 - r}.\end{aligned}$$

(ii) Prove that

$$1 + 2 + 2^2 + \cdots + 2^n = 2^{n+1} - 1.$$

Solution. This is the special case of the geometric series when $r = 2$; hence, the sum is $(1 - 2^{n+1})/(1 - 2) = 2^{n+1} - 1$. One can also prove this directly, by induction on $n \geq 0$.

1.3 Show, for all $n \geq 1$, that 10^n leaves remainder 1 after dividing by 9.

Solution. This may be rephrased to say that there is an integer q_n with $10^n = 9q_n + 1$. If we define $q_1 = 1$, then $10 = q_1 + 1$, and so the base step is true.

For the inductive step, there is an integer q_n with

$$\begin{aligned}10^{n+1} = 10 \times 10^n &= 10(9q_n + 1) \\ &= 90q_n + 10 = 9(10q_n + 1) + 1.\end{aligned}$$

Define $q_{n+1} = 10q_n + 1$, which is an integer.

1.4 Prove that if $0 \leq a \leq b$, then $a^n \leq b^n$ for all $n \geq 0$.

Solution. *Base step.* $a^0 = 1 = b^0$, and so $a^0 \leq b^0$.

Inductive step. The inductive hypothesis is

$$a^n \leq b^n.$$

Since a is positive, Theorem 1.4(i) gives $a^{n+1} = aa^n \leq ab^n$; since b is positive, Theorem 1.4(i) now gives $ab^n \leq bb^n = b^{n+1}$.

1.5 Prove that $1^2 + 2^2 + \cdots + n^2 = \frac{1}{6}n(n+1)(2n+1) = \frac{1}{3}n^3 + \frac{1}{2}n^2 + \frac{1}{6}n$.

Solution. The proof is by induction on $n \geq 1$. When $n = 1$, the left side is 1 and the right side is $\frac{1}{3} + \frac{1}{2} + \frac{1}{6} = 1$.

For the inductive step,

$$\begin{aligned}[1^2 + 2^2 + \cdots + n^2] + (n+1)^2 &= \tfrac{1}{3}n^3 + \tfrac{1}{2}n^2 + \tfrac{1}{6}n + (n+1)^2 \\ &= \tfrac{1}{3}(n+1)^3 + \tfrac{1}{2}(n+1)^2 + \tfrac{1}{6}(n+1),\end{aligned}$$

after some elementary algebraic manipulation.

1.6 Prove that $1^3 + 2^3 + \cdots + n^3 = \frac{1}{4}n^4 + \frac{1}{2}n^3 + \frac{1}{4}n^2$.

Solution. *Base step*: When $n = 1$, both sides equal 1.

Inductive step:

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

Expanding gives

$$\tfrac{1}{4}n^4 + \tfrac{3}{2}n^3 + \tfrac{13}{4}n^2 + 3n + 1,$$

which is

$$\tfrac{1}{4}(n+1)^4 + \tfrac{1}{2}(n+1)^3 + \tfrac{1}{4}(n+1)^2.$$

1.7 Prove that $1^4 + 2^4 + \cdots + n^4 = \frac{1}{5}n^5 + \frac{1}{2}n^4 + \frac{1}{3}n^3 - \frac{1}{30}n$.

Solution. The proof is by induction on $n \geq 1$. If $n - 1$, then the left side is 1, while the right side is $\frac{1}{5} + \frac{1}{2} + \frac{1}{3} - \frac{1}{30} = 1$ as well.

For the inductive step,

$$\left[1^4 + 2^4 + \cdots + n^4\right] + (n+1)^4 = \tfrac{1}{5}n^5 + \tfrac{1}{2}n^4 + \tfrac{1}{3}n^3 - \tfrac{1}{30}n + (n+1)^4.$$

It is now straightforward to check that this last expression is equal to

$$\tfrac{1}{5}(n+1)^5 + \tfrac{1}{2}(n+1)^4 + \tfrac{1}{3}(n+1)^3 - \tfrac{1}{30}(n+1).$$

1.8 Find a formula for $1+3+5+\cdots+(2n-1)$, and use mathematical induction to prove that your formula is correct.

Solution. We prove by induction on $n \geq 1$ that the sum is n^2.

Base Step. When $n = 1$, we interpret the left side to mean 1. Of course, $1^2 = 1$, and so the base step is true.

Inductive Step.

$$\begin{aligned}1 + 3 + 5 + \cdots + (2n-1) + (2n+1) &\\ &= 1 + 3 + 5 + \cdots + (2n-1)] + (2n+1) \\ &= n^2 + 2n + 1 \\ &= (n+1)^2.\end{aligned}$$

1.9 Find a formula for $1 + \sum_{j=1}^{n} j!j$, and use induction to prove that your formula is correct.

Solution. A list of the sums for $n = 1, 2, 3, 4, 5$ is $2, 6, 24, 120, 720$. These are factorials; better, they are $2!, 3!, 4!, 5!, 6!$. We have been led to the guess

$$S(n) : 1 + \sum_{j=1}^{n} j!j = (n+1)!.$$

We now use induction to prove that the guess is *always* true. The base step $S(1)$ has already been checked; it is on the list. For the inductive step, we must prove

$$S(n+1) : 1 + \sum_{j=1}^{n+1} j!j = (n+2)!.$$

Rewrite the left side as

$$\left[1 + \sum_{j=1}^{n} j!j\right] + (n+1)!(n+1).$$

By the inductive hypothesis, the bracketed term is $(n+1)!$, and so the left side equals

$$\begin{aligned}(n+1)! + (n+1)!(n+1) &= (n+1)![1 + (n+1)] \\ &= (n+1)!(n+2) \\ &= (n+2)!.\end{aligned}$$

By induction, $S(n)$ is true for all $n \geq 1$.

1.10 (***M. Barr***) There is a famous anecdote describing a hospital visit of G. H. Hardy to Ramanujan. Hardy mentioned that the number 1729 of the taxi he had taken to the hospital was not an interesting number. Ramanujan disagreed, saying that it is the smallest positive integer that can be written as the sum of two cubes in two different ways.

(i) Prove that Ramanujan's statement is true.

Solution. First, 1729 is the sum of two cubes in two different ways:

$$1729 = 1^3 + 12^3; \qquad 1927 = 9^3 + 10^3.$$

Second, no smaller number n has this property. If $n = a^3 + b^3$, then $a, b \leq 12$. It is now a matter of checking all pairs $a^3 + b^3$ for such a and b.

(ii) Prove that Ramanujan's statement is false.
Solution. One must pay attention to hypotheses. Consider a^3+b^3 if b is negative:

$$728 = 12^3 + (-10^3) = 9^3 + (-1)^3.$$

1.11 Derive the formula for $\sum_{i=1}^{n} i$ by computing the area $(n+1)^2$ of a square with sides of length $n+1$ using Figure 1.1.
Solution. Compute the area A of the square in two ways. On the one hand, $A = (n+1)^2$. On the other hand, $A = |D| + 2|S|$, where D is the diagonal and S is the "staircase." Therefore,

$$|S| = \tfrac{1}{2}\Big[(n+1)^2 - (n+1)\Big] = \tfrac{1}{2}n(n+1).$$

But $|S|$ is the sum we are seeking.

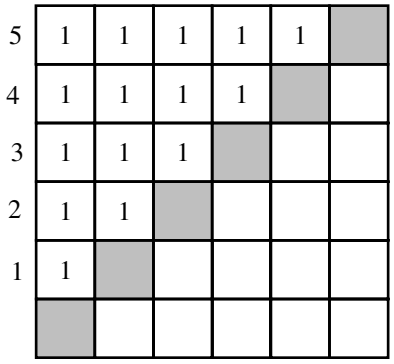


Figure 1.1
$1 + 2 + \cdots + n = \frac{1}{2}(n^2 + n)$

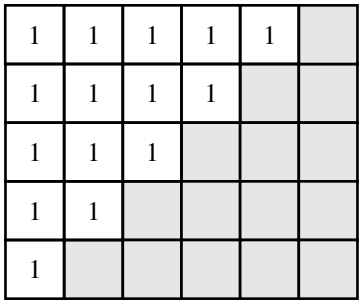


Figure 1.2
$1 + 2 + \cdots + n = \frac{1}{2}n(n+1)$

1.12 **(i)** Derive the formula for $\sum_{i=1}^{n} i$ by computing the area $n(n+1)$ of a rectangle with height $n+1$ and base n, as pictured in Figure 1.2.
Solution. Compute the area R of the rectangle in two ways. On the one hand, $R = n(n+1)$. On the other hand, $R = 2|S|$, where S is the shaded region (whose area is what we seek).

(ii) (***Alhazen***) For fixed $k \geq 1$, use Figure 1.3 to prove

$$(n+1)\sum_{i=1}^{n} i^k = \sum_{i=1}^{n} i^{k+1} + \sum_{i=1}^{n}\Big(\sum_{p=1}^{i} p^k\Big).$$

Solution. As indicated in Figure 1.3, a rectangle with height $n+1$ and base $\sum_{i=1}^{n} i^k$ can be subdivided so that the shaded staircase has area $\sum_{i=1}^{n} i^{k+1}$, while the area above it is

$$1^k + (1^k + 2^k) + (1^k + 2^k + 3^k) + \cdots + (1^k + 2^k + \cdots + n^k).$$

One can prove this, for fixed k, by induction on $n \geq 1$.

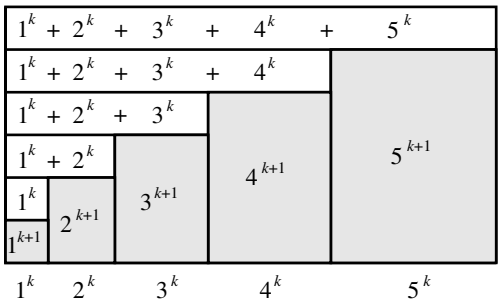


Figure 1.3 Alhazan's Dissection

(iii) Given the formula $\sum_{i=1}^{n} i = \frac{1}{2}n(n+1)$, use part (ii) to derive the formula for $\sum_{i=1}^{n} i^2$.

Solution.

$$\begin{aligned}(n+1)\sum_{i=0}^{n} i &= \sum_{i=0}^{n} i^2 + \sum_{i=0}^{n}\Big(\sum_{p=0}^{i} p\Big)\\ &= \sum_{i=0}^{n} i^2 + \sum_{i=0}^{n} \tfrac{1}{2} i(i+1)\\ &= \sum_{i=0}^{n} i^2 + \tfrac{1}{2}\sum_{i=0}^{n} i^2 + \tfrac{1}{2}\sum_{i=0}^{n} i.\end{aligned}$$

Therefore,

$$(n+1-\tfrac{1}{2})\sum_{i=0}^{n} i = \tfrac{3}{2}\sum_{i=0}^{n} i^2,$$

and so

$$\begin{aligned}\sum_{i=0}^{n} i^2 &= \tfrac{2}{3}(n+\tfrac{1}{2})\tfrac{1}{2}n(n+1)\\ &= \tfrac{1}{3}\tfrac{1}{2}(2n+1)n(n+1)\\ &= \tfrac{1}{6}(2n+1)n(n+1).\end{aligned}$$

1.13 **(i)** Prove that $2^n > n^3$ for all $n \geq 10$.

Solution. *Base step*. $2^{10} = 1024 > 10^3 = 1000$. (Note that $2^9 = 512 < 9^3 = 729$.)

Inductive step Note that $n \geq 10$ implies $n \geq 4$. The inductive hypothesis is $2^n > n^3$; multiplying both sides by 2 gives

$$\begin{aligned} 2^{n+1} = 2 - 2^n &> 2n^3 \\ &= n^3 + n^3 \\ &\geq n^3 + 4n^2 \\ &= n^3 + 3n^2 + n^2 \\ &> n^3 + 3n^2 + 4n \\ &= n^3 + 3n^2 + 3n + n \\ &\geq n^3 + 3n^2 + 3n + 1 \\ &= (n+1)^3. \end{aligned}$$

(ii) Prove that $2^n > n^4$ for all $n \geq 17$.

Solution. *Base step*. $2^{17} = 131,072 > 17^4 = 83,521$. (Note that $16^4 = (2^4)^4 = 2^{16}$.)

Inductive step. Note that $n \geq 17$ implies $n \geq 7$. The inductive hypothesis is $2^n > n^4$; multiplying both sides by 2 gives

$$\begin{aligned} 2^{n+1} = 2 - 2^n &> 2n^4 \\ &= n^4 + n^4 \\ &\geq n^4 + 5n^3 \\ &\geq n^4 + 4n^3 + n^3 \\ &\geq n^4 + 4n^3 + 7n^2 \\ &\geq n^4 + 4n^3 + 6n^2 + n^2 \\ &\geq n^4 + 4n^3 + 6n^2 + 5n \\ &\geq n^4 + 4n^3 + 6n^2 + 4n + 1 = (n+1)^4. \end{aligned}$$

1.14 Around 1350, N. Oresme was able to sum the series $\sum_{n=1}^{\infty} n/2^n$ by dissecting the region in Figure 1.4 in two ways. Let A_n be the vertical rectangle with base $\frac{1}{2^n}$ and height n, so that area$(A_n) = n/2^n$, and let B_n be horizontal rectangle with base $\frac{1}{2^n} + \frac{1}{2^{n+1}} + \cdots$ and height 1. Prove that $\sum_{n=1}^{\infty} n/2^n = 2$.

Solution. You may assume that $\sum_{n=0}^{\infty} ar^n = a/(1-r)$ if $0 \leq r < 1$. Now compute the area using $\sum A_n = \sum B_n$.

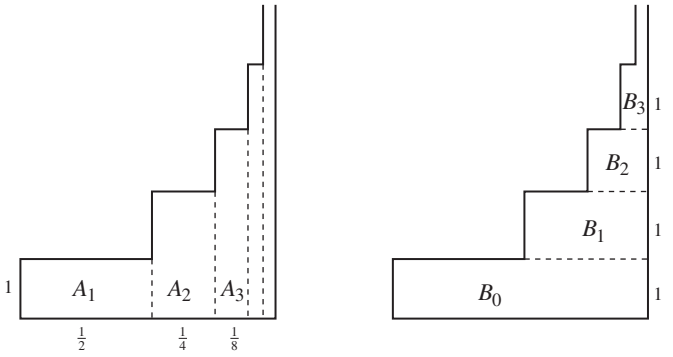


Figure 1.4 Oresme's Dissections

1.15 Let $g_1(x), \ldots, g_n(x)$ be differentiable functions, and let $f(x)$ be their product: $f(x) = g_1(x) \cdots g_n(x)$. Prove, for all integers $n \geq 2$, that the derivative

$$f'(x) = \sum_{i=1}^{n} g_1(x) \cdots g_{i-1}(x) g_i'(x) g_{i+1}(x) \cdots g_n(x).$$

Solution. *Base step*. If $n = 2$, this is the usual product rule for derivatives.

Inductive step. Define $h(x) = g_1(x) \cdots g_n(x) = f(x)/g_{n+1}(x)$. Rewrite what has to be shown:

$$f'(x) = \sum_{j=1}^{n+1} \frac{g_j'(x) f(x)}{g_j(x)}.$$

Now

$$\begin{aligned} f'(x) &= (h(x) g_{n+1}(x))' \\ &= h'(x) g_{n+1}(x) + h(x) g_{n+1}'(x) \\ &= \sum = 1_{i=1} \left[\frac{g_i'(x) h(x)}{g_i(x)} \right] g_{n+1}(x) + \left[\frac{f(x)}{g_{n+1}(x)} \right] g_n' \\ &= \sum_{j=1}^{n+1} \frac{g_j'(x) f(x)}{g_j(x)}. \end{aligned}$$

1.16 Prove, for every $n \in \mathbb{N}$, that $(1 + x)^n \geq 1 + nx$ whenever $x \in \mathbb{R}$ and $1 + x > 0$.

Solution. We prove the inequality by induction on $n \geq 1$. The base step $n = 1$ says $1 + x \geq 1 + x$, which is obviously true. For the inductive step,

we record the inductive hypothesis:

$$(1+x)^n \geq 1+nx.$$

Multiplying both sides of this inequality by the positive number $1+x$ preserves the inequality:

$$\begin{aligned}(1+x)^{n+1} &= (1+x)(1+x)^n \\ &\geq (1+x)(1+nx) \\ &= 1+(n+1)x+nx^2 \\ &\geq 1+(n+1)x,\end{aligned}$$

because $nx^2 \geq 0$.

1.17 Prove that every positive integer a has a unique factorization $a = 3^k m$, where $k \geq 0$ and m is not a multiple of 3.

Solution. Model your solution on the proof of Proposition 1.14. Replace "even" by "multiple of 3" and "odd" by "not a multiple of 3." We prove this by the second form of induction on $a \geq 1$. The base step $n = 1$ holds, for $1 = 3^0 \cdot 1$ is a factorization of the desired kind.

For the inductive step, let $a \geq 1$. If a is not a multiple of 3, then $a = 3^0 a$ is a good factorization. If $a = 3b$, then $b < a$, and so the inductive hypothesis gives $k \geq 0$ and an integer c not divisible by 3 such that $b = 3^k c$. It follows that $a = 3b = 3^{k+1}c$, which is a factorization of the desired kind. We have proved the existence of a factorization.

To prove uniqueness, suppose that $n = 3^k m = 3^t m'$, where both k and t are nonnegative and both m and m' are not multiples of 3; it must be shown that $k = t$ and $m = m'$. We may assume that $k \geq t$. If $k > t$, then canceling 3^t from both sides gives $3^{k-t}m = m'$. Since $k - t > 0$, the left side is a multiple of 3 while the right side is not; this contradiction shows that $k = t$. We may thus cancel 3^k from both sides, leaving $m = m'$.

1.18 Prove that $F_n < 2^n$ for all $n \geq 0$, where $F_0, F_1, F_2, \ldots$ is the Fibonacci sequence.

Solution. The proof is by the second form of induction.

Base step:

$F_0 = 0 < 1 = 2^0$ and $F_1 = 1 < 2 = 2^1$. (There are two base steps because we will have to use two predecessors for the inductive step.)

Inductive step:

If $n \geq 2$, then

$$\begin{aligned} F_n &= F_{n-1} + F_{n-2} \\ &< 2^{n-1} + 2^{n-2} \quad \text{(by inductive hypothesis)} \\ &< 2^{n-1} + 2^{n-1} \\ &= 2 \cdot 2^{n-1} \\ &= 2^n. \end{aligned}$$

By induction, $F_n < 2^n$ for all $n \geq 0$.

Notice that the second form is the appropriate induction here, for we are using two predecessors, $S(n-2)$ and $S(n-1)$, to prove $S(n)$.

1.19 If F_n denotes the nth term of the Fibonacci sequence, prove that

$$\sum_{n=1}^{m} F_n = F_{m+2} - 1.$$

Solution. By Theorem 1.15, we have $F_n = \frac{1}{\sqrt{5}}(\alpha^n - \beta^n)$ for all n. Hence,

$$\begin{aligned} \sum_{n=1}^{m} F_n &= \sum_{n=1}^{m} \tfrac{1}{\sqrt{5}}(\alpha^n - \beta^n) \\ &= \tfrac{1}{\sqrt{5}} \sum_{n=1}^{m} (\alpha^n - \beta^n) \\ &= \tfrac{1}{\sqrt{5}} \Big(\Big[\frac{1-\alpha^{m+1}}{1-\alpha} - 1 \Big] - \Big[\frac{1-\beta^{m+1}}{1-\beta} - 1 \Big] \Big). \end{aligned}$$

Now $\alpha(\alpha - 1) = 1$, so that $1/(1-\alpha) = -\alpha$; similarly, $1/(1-\beta) = -\beta$. Therefore,

$$\begin{aligned} \sum_{n=1}^{m} F_n &= \tfrac{1}{\sqrt{5}} \Big(\Big[\frac{1-\alpha^{m+1}}{1-\alpha} - 1 \Big] - \Big[\frac{1-\beta^{m+1}}{1-\beta} - 1 \Big] \Big) \\ &= \tfrac{1}{\sqrt{5}} \Big((-\alpha)[(1-\alpha^{m+1}) - 1] - [(-\beta)(1-\beta^{m+1}) - 1] \Big) \\ &= \tfrac{1}{\sqrt{5}} [-(\alpha - \beta) + (\alpha^{m+2} - \beta^{m+2})]. \end{aligned}$$

This is the desired formula, for $\frac{1}{\sqrt{5}}(\alpha - \beta) = 1$ and $\frac{1}{\sqrt{5}}(\alpha^{m+2} - \beta^{m+2}) = F_{m+2}$.

1.20 Prove that $4^{n+1} + 5^{2n-1}$ is divisible by 21 for all $n \geq 1$.

Solution. We use the second form of induction.

Base Step. If $n = 1$, then

$$4^{n+1} + 5^{2n-1} = 16 + 5 = 21,$$

which is obviously divisible by 21. Since our inductive step will involve two predecessors, we are obliged to check the case $n = 2$. But $4^3 + 5^3 = 64 + 125 = 189 = 21 \times 9$.

Inductive Step.

$$\begin{aligned} 4^{n+2} + 5^{2n+1} &= 4 \cdot 4^{n+1} + 5^2 \cdot 5^{2n-1} \\ &= 4 \cdot 4^{n+1} + (4 \cdot 5^{2n-1} - 4 \cdot 5^{2n-1}) + 5^2 \cdot 5^{2n-1} \\ &= 4(4^{n+1} + 5^{2n-1}) + 5^{2n-1}(5^2 - 4). \end{aligned}$$

Now the last term is divisible by 21; the first term, by the inductive hypothesis, and the second because $5^2 - 4 = 21$.

1.21 For any integer $n \geq 2$, prove that there are n consecutive composite numbers. Conclude that the gap between consecutive primes can be arbitrarily large.

Solution. The proof has nothing to do with induction. If $2 \leq a \leq n + 1$, then a is a divisor of $(n + 1)!$; say, $(n + 1)! = da$ for some integer d. It follows that $(n + 1)! + a = (d + 1)a$, and so $(n + 1)! + a$ is composite for all a between 2 and $n + 1$.

1.22 Prove that the first and second forms of mathematical induction are equivalent; that is, prove that Theorem 1.4 is true if and only if Theorem 1.12 is true.

Solution. Absent.

1.23 (***Double Induction***) Let $S(m, n)$ be a doubly indexed family of statements, one for each $m \geq 0$ and $n \geq 0$. Suppose that

(i) $S(0, 0)$ is true;

(ii) if $S(m, 0)$ is true, then $S(m + 1, 0)$ is true;

(iii) if $S(m, n)$ is true for all $m \geq 0$, then $S(m, n+1)$ is true for all $m \geq 0$.

Prove that $S(m, n)$ is true for all $m \geq 0$ and $n \geq 0$.

Solution. Conditions (i) and (ii) are the hypotheses needed to prove, by (ordinary) induction that the statements $S(m, 0)$ are true for all $m \geq 0$.

Now consider the statements

$$T(n) : S(m, n) \text{ is true for all } m \geq 0.$$

We prove that all the statements $T(n)$ are true by induction on $n \geq 0$. The base step has been proved above, and condition (iii) is precisely what is needed for the inductive step.

1.24 Use double induction to prove that

$$(m+1)^n > mn$$

for all $m, n \geq 0$.

Solution. According to Exercise 1.23, there are three things to verify.

(i) $S(0,0)$: $(0+0)^0 = 1 \cdot 0$.

(ii) $S(m,0) \Rightarrow S(m+1,0)$: if $(m+1)^0 > m$, then $(m+2)^0 > (m+1)\cdot 0 = 0$?

(iii) $S(m,n) \Rightarrow S(m,n+1)$: does $(m+1)^n > mn$ imply $(m+1)^{n+1} > m(n+1)$? Yes, because

$$\begin{aligned}(m+1)^{n+1} &= (m+1)(m+1)^n \\ &> (m+1)mn \\ &= m^2n + mn \\ &> mn + m,\end{aligned}$$

for $m^2n \geq mn$ and $mn \geq m$.

Notice that $2^n > n$ is the special case $S(0,n)$.

1.25 For every acute angle θ, i.e., $0° < \theta < 90°$, prove that

$$\sin\theta + \cot\theta + \sec\theta \geq 3.$$

Solution. That θ is an acute angle implies that the numbers $\sin\theta$, $\cot\theta$, and $\sec\theta$ are all positive. The inequality of the means gives

$$\left[\tfrac{1}{3}(\sin\theta + \cot\theta + \sec\theta)\right]^3 \geq \sin\theta\cot\theta\sec\theta.$$

Now

$$\sin\theta\cot\theta\sec\theta = \sin\theta\frac{\cos\theta}{\sin\theta}\frac{1}{\cos\theta} = 1,$$

so that $\left[\tfrac{1}{3}(\sin\theta + \cot\theta + \sec\theta)\right]^3 \geq 1$ and

$$\tfrac{1}{3}(\sin\theta + \cot\theta + \sec\theta) \geq 1.$$

Therefore, $\sin\theta + \cot\theta + \sec\theta \geq 3$.

1.26 *Isoperimetric Inequality.*

(i) Let p be a positive number. If Δ is an equilateral triangle with perimeter $p = 2s$, prove that $\text{area}(\Delta) = s^2/\sqrt{27}$.

Solution. This is an elementary fact of high school geometry.

(ii) Of all the triangles in the plane having perimeter p, prove that the equilateral triangle has the largest area.

Solution. Use ***Heron's formula***: if a triangle T has area A and sides of lengths a, b, c, then

$$A^2 = s(s-a)(s-b)(s-c),$$

where $s = \frac{1}{2}(a+b+c)$. The inequality of the means gives

$$\left[\frac{(s-a)+(s-b)+(s-c)}{3}\right]^3 \geq (s-a)(s-b)(s-c) = \frac{A^2}{s},$$

with equality holding if and only if $s-a = s-b = s-c$. Thus, equality holds if and only if $a = b = c$, which is to say T is equilateral.

1.27 Prove that if $a_1, a_2, \ldots, a_n$ are positive numbers, then

$$(a_1 + a_2 + \cdots + a_n)(1/a_1 + 1/a_2 + \cdots + 1/a_n) \geq n^2.$$

Solution. By the inequality of the means, $[(a_1 + a_2 + \cdots + a_n)/n]^n \geq a_1 \cdots a_n$ and $[(1/a_1 + 1/a_2 + \cdots + 1/a_n)/n]^n \geq 1/a_1 \cdots 1/a_n$. Now use the general fact that if $p \geq q > 0$ and $p' \geq q' > 0$, then $pp' \geq qq'$ to obtain $(a_1 + a_2 + \cdots + a_n)/n]^n[(1/a_1 + 1/a_2 + \cdots + 1/a_n)/n]^n \geq (a_1 \cdots a_n)(1/a_1 \cdots 1/a_n)$. But the right side is $a_1 \cdots a_n(1/a_1) \cdots (1/a_n) = 1$, so that

$$(a_1 + a_2 + \cdots + a_n)/n]^n[(1/a_1 + 1/a_2 + \cdots + 1/a_n)/n]^n \geq 1.$$

Taking nth roots gives $(a_1+a_2+\cdots+a_n)(1/a_1+1/a_2+\cdots+1/a_n) \geq n^2$.

1.28 True or false with reasons.

(i) For all integers r with $0 < r < 7$, the binomial coefficient $\binom{7}{r}$ is a multiple of 7.

Solution. True.

(ii) For any positive integer n and any r with $0 < r < n$, the binomial coefficient $\binom{n}{r}$ is a multiple of n.

Solution. False.

(iii) Let D be a collection of 10 different dogs, and let C be a collection of 10 different cats. There are the same number of quartets of dogs as there are sextets of cats.

Solution. True.

(iv) If q is a rational number, then $e^{2\pi iq}$ is a root of unity.

Solution. True.

(v) Let $f(x) = ax^2 + bx + c$, where a, b, c are real numbers. If z is a root of $f(x)$, then $\overline{z}$ is also a root of $f(x)$.
Solution. True.

(vi) Let $f(x) = ax^2 + bx + c$, where a, b, c are complex numbers. If z is a root of $f(x)$, then $\overline{z}$ is also a root of $f(x)$.
Solution. False.

(vii) The primitive 4th roots of unity are i and $-i$.
Solution. True.

1.29 Prove that the binomial theorem holds for complex numbers: if u and v are complex numbers, then

$$(u+v)^n = \sum_{r=0}^{n} \binom{n}{r} u^{n-r} v^r.$$

Solution. The proof of the binomial theorem for real numbers used only properties of the three operations: addition, multiplication, and division. These operations on complex numbers have exactly the same properties. (Division enters in only because we chose to expand $(a+b)^n$ by using the formula for $(1+x)^n$; had we not chosen this expository path, then division would not have been used. Thus, the binomial theorem really holds for commutative rings.)

1.30 Show that the binomial coefficients are "symmetric":

$$\binom{n}{r} = \binom{n}{n-r}$$

for all r with $0 \le r \le n$.
Solution. By Lemma 1.17, both $\binom{n}{r}$ and $\binom{n}{n-r}$ are equal to

$$\frac{n!}{r!(n-r)!}.$$

1.31 Show, for every n, that the sum of the binomial coefficients is 2^n:

$$\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{n} = 2^n.$$

Solution. By Corollary 1.19, if $f(x) = (1+x)^n$, then there is the expansion

$$f(x) = \binom{n}{0} + \binom{n}{1}x + \binom{n}{2}x^2 + \cdots + \binom{n}{n}x^n.$$

Evaluating at $x = 1$ gives the answer, for $f(1) = (1+1)^n = 2^n$.

1.32 **(i)** Show, for every $n \geq 1$, that the "alternating sum" of the binomial coefficients is zero:

$$\binom{n}{0} - \binom{n}{1} + \binom{n}{2} - \cdots + (-1)^n \binom{n}{n} = 0.$$

Solution. If $f(x) = (1+x)^n$, then $f(-1) = (1-1)^n = 0$; but the expansion is the alternating sum of the binomial coefficients.

(ii) Use part (i) to prove, for a given n, that the sum of all the binomial coefficients $\binom{n}{r}$ with r even is equal to the sum of all those $\binom{n}{r}$ with r odd.

Solution. By part (i),

$$\binom{n}{0} - \binom{n}{1} + \binom{n}{2} - \cdots \pm \binom{n}{n} = 0.$$

Since the sign of $\binom{n}{r}$ is $(-1)^r$, the terms $\binom{n}{r}$ with r even are positive while those with r odd are negative. Just put those coefficients with negative coefficient on the other side of the equation.

1.33 Prove that if $n \geq 2$, then

$$\sum_{r=1}^{n} (-1)^{r-1} r \binom{n}{r} = 0.$$

Solution. Again, consider $f(x) = (1+x)^n$. There are two ways to describe its derivative $f'(x)$. On the one hand, $f'(x) = n(1+x)^{n-1}$. On the other hand, we can do term-by-term differentiation:

$$f'(x) = \sum_{r=1}^{n} r \binom{n}{r} x^{r-1}.$$

Evaluating at $x = -1$ gives $f'(-1) = n(1-1)^{n-1} = 0$, since $n - 1 \geq 1$. On the other hand, we can use the expansion to see

$$f'(-1) = \sum_{r=1}^{n} (-1)^{r-1} r \binom{n}{r}.$$

1.34 If $1 \leq r \leq n$, prove that

$$\binom{n}{r} = \frac{n}{r} \binom{n-1}{r-1}.$$

Solution. Absent.

1.35 Let $\varepsilon_1, \ldots, \varepsilon_n$ be complex numbers with $|\varepsilon_j| = 1$ for all j, where $n \geq 2$.

(i) Prove that

$$\Big|\sum_{j=1}^{n} \varepsilon_j\Big| \leq \sum_{j=1}^{n} |\varepsilon_j| = n.$$

Solution. The triangle inequality gives $|u + v| \leq |u| + |v|$ for all complex numbers u and v, with no restriction on their norms. The inductive proof is routine.

(ii) Prove that there is equality,

$$\Big|\sum_{j=1}^{n} \varepsilon_j\Big| = n,$$

if and only if all the ε_j are equal.

Solution. The proof is by induction on $n \geq 2$.

For the base step, suppose that $|\varepsilon_1 + \varepsilon_2| = 2$. Therefore,

$$\begin{aligned} 4 &= |\varepsilon_1 + \varepsilon_2|^2 \\ &= (\varepsilon_1 + \varepsilon_2) \cdot (\varepsilon_1 + \varepsilon_2) \\ &= |\varepsilon_1|^2 + 2\varepsilon_1 \cdot \varepsilon_2 + |\varepsilon_2|^2 \\ &= 2 + 2\varepsilon_1 \cdot \varepsilon_2. \end{aligned}$$

Therefore, $2 = 1 + \varepsilon_1 \cdot \varepsilon_2$, so that

$$\begin{aligned} 1 &= \varepsilon_1 \cdot \varepsilon_2 \\ &= |\varepsilon_1||\varepsilon_2| \cos\theta \\ &= \cos\theta, \end{aligned}$$

where θ is the angle between ε_1 and ε_2 (for $|\varepsilon_1| = 1 = |\varepsilon_2|$). Therefore, $\theta = 0$ or $\theta = \pi$, so that $\varepsilon_2 = \pm\varepsilon_1$. We cannot have $\varepsilon_2 = -\varepsilon_1$, for this gives $|\varepsilon_1 + \varepsilon_2| = 0$.

For the inductive step, let $|\sum_{j=1}^{n+1} \varepsilon_j| = n + 1$. If $|\sum_{j=1}^{n} \varepsilon_j| < n$, then part (i) gives

$$\Big|\big(\sum_{j=1}^{n} \varepsilon_j\big) + \varepsilon_{n+1}\Big| \leq \Big|\sum_{j=1}^{n} \varepsilon_j\Big| + 1 < n + 1,$$

contrary to hypothesis. Therefore, $|\sum_{j=1}^{n} \varepsilon_j| = n$, and so the inductive hypothesis gives $\varepsilon_1, \ldots, \varepsilon_n$ all equal, say to ω. Hence, $\sum_{j=1}^{n} \varepsilon_j = n\omega$, and so

$$|n\omega + \varepsilon_{n+1}| = n + 1.$$

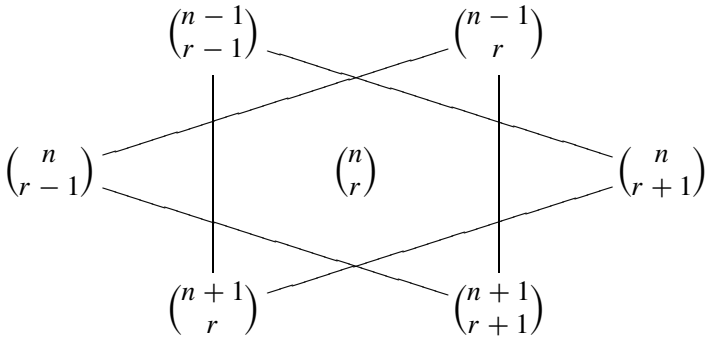
The argument concludes as that of the base step.

$$\begin{aligned}(n+1)^2 &= (n\omega + \varepsilon_{n+1}) \cdot (n\omega + \varepsilon_{n+1}) \\ &= n^2 + 2n\omega \cdot \varepsilon_{n+1} + 1,\end{aligned}$$

so that $\omega \cdot \varepsilon_{n+1} = 1$. By the base step, $\omega = \varepsilon_{n+1}$, and the proof is complete.

1.36 (***Star of David***) Prove, for all $n > r \geq 1$, that

$$\binom{n-1}{r-1}\binom{n}{r+1}\binom{n+1}{r} = \binom{n-1}{r}\binom{n}{r-1}\binom{n+1}{r+1}.$$



Solution. Using Pascal's formula, one sees that both sides are equal to

$$\frac{(n-1)!n!(n+1)!}{(r-1)!r!(r+1)!(n-r-1)!(n-r)!(n-r+1)!}.$$

1.37 For all odd $n \geq 1$, prove that there is a polynomial $g_n(x)$, all of whose coefficients are integers, such that

$$\sin(nx) = g_n(\sin x).$$

Solution. From De Moivre's theorem,

$$\cos nx + i \sin nx = (\cos x + i \sin x)^n,$$

we have

$$\begin{aligned}\sin nx &= \text{Im } (\cos x + i \sin x)^n \\ &= \text{Im } \Big(\sum_{r=0}^{n} \binom{n}{r} i^r \sin^r x \cos^{n-r} x\Big).\end{aligned}$$

Write $n = 2m + 1$. Only odd powers of i are imaginary, so that, if $r = 2k + 1$,

$$\sin nx = \sum_{0 \le k \le m} \binom{n}{2k+1} (-1)^k \sin^{2k+1} x \cos^{2(m-k)} x.$$

But

$$\cos^{2(m-k)} x = (\cos^2 x)^{m-k} = (1 - \sin^2 x)^{m-k},$$

and so we have expressed $\sin nx$ as a polynomial in $\sin x$.

1.38 **(i)** What is the coefficient of x^{16} in $(1 + x)^{20}$?

Solution. Pascal's formula gives $\binom{20}{16} = 4845$.

(ii) How many ways are there to choose 4 colors from a palette containing paints of 20 different colors?

Solution. Pascal's formula gives $\binom{20}{4} = 4845$. One could also have used part (i) and Exercise 1.30.

1.39 Give at least two different proofs that a set X with n elements has exactly 2^n subsets.

Solution. There are many proofs of this. We offer only three.

Algebraic.

Let $X = \{a_1, a_2, \ldots, a_n\}$. We may describe each subset S of X by a *bitstring*; that is, by an n-tuple

$$(\epsilon_1, \epsilon_2, \ldots, \epsilon_n),$$

where

$$\epsilon_i = \begin{cases} 0 & \text{if } a_i \text{ is not in } S \\ 1 & \text{if } a_i \text{ is in } S. \end{cases}$$

(after all, a set is determined by the elements comprising it). But there are exactly 2^n such n-tuples, for there are two choices for each coordinate.

Combinatorial.

Induction on $n \ge 1$ (taking base step $n = 0$ is also fine; the only set with 0 elements is $X = \varnothing$, which has exactly one subset, itself). If X has just one element, then there are two subsets: $\varnothing$ and X. For the inductive step, assume that X has $n + 1$ elements, of which one is colored red, the other n being blue. There are two types of subsets S: those that are solid blue; those that contain the red. By induction, there are 2^n solid blue subsets; denote them by B. But, there are as many subsets R containing the red as there are solid blue subsets: each R arises by adjoining the red element to a solid blue subset, namely, $B = R - \{\text{red}\}$ (even the singleton subset consisting of the red element alone arises in this way, by adjoining the red element to $\varnothing$). Hence, there are $2^n + 2^n = 2^{n+1}$ subsets.

Binomial Coefficients.

If X has n elements, then the number of its subsets is the sum of the number of 0-subsets (there is only 1, the empty set), the number of 1-subsets, the number of 2-subsets, etc. But $\binom{n}{r}$ is the number of r-subsets, as we have seen in the text, and so the total number of subsets is the sum of all the binomial coefficients, which is 2^n, by Exercise 1.31.

1.40 A weekly lottery asks you to select 5 different numbers between 1 and 45. At the week's end, 5 such numbers are drawn at random, and you win the jackpot if all your numbers match the drawn numbers. What is your chance of winning?

Solution. The answer is "45 choose 5", which is $\binom{45}{5} = 1,221,759$. The odds against your winning are more than a million to one.

1.41 Assume that "term-by-term" differentiation holds for power series: if $f(x) = c_0+c_1x+c_2x^2+\cdots+c_nx^n+\cdots$, then the power series for the derivative $f'(x)$ is

$$f'(x) = c_1 + 2c_2x + 3c_3x^2 + \cdots + nc_nx^{n-1} + \cdots .$$

(i) Prove that $f(0) = c_0$.

Solution. $f(0) = c_0$, for all the other terms are 0. (If one wants to be fussy–this is the wrong course for analytic fussiness–then the partial sums of the series form the constant sequence $c_0, c_0, c_0, \ldots$.)

(ii) Prove, for all $n \geq 0$, that

$$f^{(n)}(x) = n!c_n + (n+1)!c_{n+1}x + x^2g_n(x),$$

where $g_n(x)$ is some power series .

Solution. This is a straightforward proof by induction on $n \geq 0$. The base step is obvious; for the inductive step, just observe that $f^{n+1}(x) = (f^{(n)}(x))'$. As $f^{(n)}(x)$ is a power series, by assumption, its derivative is computed term by term.

(iii) Prove that $c_n = f^{(n)}(x)(0)/n!$ for all $n \geq 0$. (Of course, this is Taylor's formula.)

Solution. If $n = 0$, then our conventions that $f^{(0)}(x) = f(x)$ and $0! = 1$ give the result. For the inductive step, use parts (i) and (ii).

1.42 (***Leibniz***) Prove that if f and g are C^∞-functions, then

$$(fg)^{(n)}(x) = \sum_{k=0}^{n} \binom{n}{k} f^{(k)}(x) \cdot g^{(n-k)}(x).$$

Solution. The proof is by induction on $n \geq 1$.

If n = 1, then the equation is precisely the product rule of Calculus: $(fg)' = f'g + fg'$. For the inductive step, we have

$$\begin{aligned}(fg)^{n+1} &= [(fg)^n]' \\ &= \Big[\sum_{k=0}^{n}\binom{n}{k} f^k g^{n-k}\Big]' \\ &= \sum_{k=0}^{n}\binom{n}{k}\Big[f^k g^{n-k}\Big]' \\ &= \sum_{k=0}^{n}\binom{n}{k}\Big[f^{k+1} g^{n-k} + f^k g^{n-k+1}\Big] \\ &= \sum_{k=0}^{n}\binom{n}{k} f^{k+1} g^{n-k} + \sum_{k=0}^{n}\binom{n}{k} f^k g^{n-k+1}.\end{aligned}$$

Rewrite this last expression without the sigma notation:

$$\begin{aligned}&\binom{n}{0} f^0 g^{n+1} + \binom{n}{1} f^1 g^n + \cdots + \binom{n}{k} f^k g^{n-k+1} + \cdots \\ &\quad + \binom{n}{0} f^1 g^n + \cdots + \binom{n}{k-1} f^k g^{n-k+1} \cdots .\end{aligned}$$

The coefficient of $f^k g^{n-k+1}$ is thus $\binom{n}{k-1} + \binom{n}{k} = \binom{n+1}{k}$, by Lemma 1.17, as desired.

1.43 Find $\sqrt{i}$.

Solution. By De Moivre's theorem, since $i = e^{i\pi/2}$, we have

$$\sqrt{i} = e^{i\pi/4} = \cos \pi/4 + i \sin \pi/4 = \tfrac{\sqrt{2}}{2} + i\tfrac{\sqrt{2}}{2}.$$

1.44 **(i)** If $z = r[\cos\theta + i \sin\theta]$, show that

$$w = \sqrt[n]{r}\,[\cos(\theta/n) + i \sin(\theta/n)]$$

is an nth root of z, where $r \geq 0$.

Solution. By De Moivre's theorem,

$$\begin{aligned}w_n &= (\sqrt[n]{r})^n([\cos(\theta/n) + i \sin(\theta/n)])^n \\ &= r[\cos(\theta) + i \sin(\theta)].\end{aligned}$$

(ii) Show that every nth root of z has the form $\zeta^k w$, where ζ is a primitive nth root of unity and $k = 0, 1, 2, \ldots, n-1$.

Solution. If $a^n = z = b^n$, then $1 = a^n/b^n = (a/b)^n$. Therefore, a/b is an nth root of unity, and so $a/b = \zeta^k$ for some k; that is, $a = \zeta^k b$. In particular, if $b = w$, then $b = \zeta^k w$.

1.45 **(i)** Find $\sqrt{8 + 15i}$.

Solution. The polar coordinates of (8, 15) are (17, 62°), and $\sin 31° \approx .515$ and $\cos 31° \approx .857$. Hence, $8+15i \approx 17(\cos 62°+i \sin 62°)$, and so
$\sqrt{8 + 15i} \approx 17(\cos 31°+i \sin 31°) \approx 3.533+2.123i$. (Of course, the other square root is the negative of this one.)

(ii) Find all the fourth roots of $8 + 15i$.

Solution. $\sin 15.5° \approx .267$ and $\cos 15.5° \approx .967$. Hence,

$$\sqrt[4]{8 + 15i} = \sqrt[4]{17}(\cos 15.5° + i \sin 15.5°) \approx 1.964 + 542i.$$

By Exercise 1.44, the other fourth roots are obtained by multiplying this one by i, -1, and $-i$.

1.46 True or false with reasons.

(i) $6 \mid 2$.

Solution. False.

(ii) $2 \mid 6$.

Solution. True.

(iii) $6 \mid 0$.

Solution. True.

(iv) $0 \mid 6$.

Solution. False.

(v) $0 \mid 0$.

Solution. True.

(vi) $(n, n + 1) = 1$ for every natural number n.

Solution. True.

(vii) $(n, n + 2) = 2$ for every natural number n.

Solution. False.

(viii) If b and m are positive integers, then $b \mid m$ if and only if the last b-adic digit d_0 of m is 0.

Solution. True.

(ix) 113 is a sum of distinct powers of 2.

Solution. True.

(x) If a and b are natural numbers, there there are natural numbers s and t with $\gcd(a, b) = sa + tb$.

Solution. False.

1.47 Given integers a and b (possibly negative) with $a \neq 0$, prove that there exist unique integers q and r with $b = qa + r$ and $0 \leq r < |a|$.

Solution. We have already proved this when $a > 0$ and $b \geq 0$. Assume now that $a > 0$ and $b < 0$. Now $-b > 0$, and so there are integers q and r with $-b = qa + r$ and $0 \leq r < a$; it follows that $b = -qb - r$. If $r = 0$, we are done; if $r > 0$, then $b = (-q - 1)a + (a - r)$ and $0 < a - r < a$ (by Proposition A.2(ii), $-r < 0$ implies $a - r < a$.

Now assume that $a < 0$, so that $-a > 0$ (and so $|a| = -a$. By what we have proved so far, there are integers q and r with $b = q(-a) + r$, where $0 \leq r < -a$; that is, $b = (-q)a + r$, where $0 \leq r < |a|$.

1.48 Prove that $\sqrt{2}$ is irrational using Proposition 1.14 instead of Euclid's lemma.

Solution. Assume, on the contrary, that $\sqrt{2} = a/b$, where a and b are integers. By Proposition 1.14, we have $a = 2^k m$ and $b = 2^\ell n$, where $k, \ell \geq 0$ and m, n are odd. If $k \geq \ell$, then we may cancel to obtain $\sqrt{2} = 2^{k-\ell} m/n$; otherwise, $\sqrt{2} = m/2^{\ell-k} m$. We may assume, therefore, that $\sqrt{2} = a/b$ where at least one of a or b is odd. Squaring and cross-multiplying, we have $2b^2 = a^2$. Hence, a^2 is even; it follows that a itself is even, for odd $\times$ odd is odd. Write $a = 2c$, so that $2b^2 = a^2 = 4c^2$. Thus, $b^2 = 2c^2$, which implies, as above, that b is even. This contradicts the fact that at least one of a or b is odd.

1.49 Let $p_1, p_2, p_3, \ldots$ be the list of the primes in ascending order: $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, and so forth. Define $f_k = p_1 p_2 \cdots p_k + 1$ for $k \geq 1$. Find the smallest k for which f_k is not a prime.

Solution. f_1, f_2, f_3, f_4, and f_5 are prime, but

$$f_6 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 30031 = 59 \cdot 509.$$

1.50 Prove that if d and d' are nonzero integers, each of which divides the other, then $d' = \pm d$.

Solution. Assume that $d = ad'$ and $d' = bd$. Then

$$d = ad' = abd,$$

so that canceling d gives $1 = ab$. As a and b are nonzero integers, $|a| \geq 1$ and $|b| \geq 1$. But $1 = |ab| = |a|\,|b|$ gives $|a| = 1 = |b|$. Hence, $a = 1 = b$ or $a = -1 = b$.

1.51 If ζ is a root of unity, prove that there is a positive integer d with $\zeta^d = 1$ such that whenever $\zeta^k = 1$, then $d \mid k$.

Solution. Define $I = \{k \text{ in } \mathbb{Z} : \zeta^k = 1\}$. Of course, I is a subset of $\mathbb{Z}$, and it contains positive numbers because ζ is a root of unity. Observe that

(i) If k is in I and u is in $\mathbb{Z}$, then uk is in I:
If k is in I, then $\zeta^k = 1$. Hence, $\zeta^{uk} = (\zeta^k)^u = 1^u = 1$, and so uk is in I.

(ii) If k, ℓ are in I, then $k + \ell$ is in I:
If k, ℓ are in I, then $\zeta^k = 1 = \zeta^\ell$, so that $1 = \zeta^k\zeta^\ell = \zeta^{k+\ell}$; hence, $k + \ell$ is in I.

It now follows from Corollary 1.37 that there is a positive number d in I, i.e., $\zeta^d = 1$, such that every k in I is a multiple of d; that is, if $\zeta^k = 1$, then $d \mid k$.

1.52 Show that every positive integer m can be written as a sum of distinct powers of 2; show, moreover, that there is only one way in which m can so be written.
Solution. In base 2, the only digits are 0 and 1. If we neglect the binary digits 0, then every positive integer is uniquely a sum of powers of 2.

1.53 Find the b-adic digits of 1000 for $b = 2$, 3, 4, 5, and 20.
Solution.

$$\begin{aligned} \text{base } 2: &\quad 1000 = 1111101000 \\ \text{base } 3: &\quad 1000 = 1101001 \\ \text{base } 4: &\quad 1000 = 33220 \\ \text{base } 5: &\quad 1000 = 13000 \\ \text{base } 20: &\quad 1000 = 2\theta, \end{aligned}$$

where θ is a symbol denoting the new digit "ten."

1.54 **(i)** Prove that if n is ***squarefree*** (i.e., $n > 1$ and n is not divisible by the square of any prime), then $\sqrt{n}$ is irrational.
Solution. We rewrite the proof of Proposition 1.14. Suppose, on the contrary, that $\sqrt{n}$ is rational, where n is squarefree; that is, $\sqrt{n} = a/b$. We may assume that a/b is in lowest terms; that is, $(a, b) = 1$. Squaring, $a^2 = nb^2$. Let p be a prime divisor of n, so that $n = pq$. Since n is squarefree, $(p, q) = 1$. By Euclid's lemma, $p \mid a$, so that $a = pm$, hence $p^2m^2 = a^2 = pqb^2$, and $pm^2 = qb^2$. By Euclid's lemma, $p \mid b$, contradicting $(a, b) = 1$.

(ii) Prove that $\sqrt[3]{2}$ is irrational.
Solution. Assume that $\sqrt[3]{4} = a/b$, where $(a, b) = 1$. Then $4b^3 = a^3$, so that a is even; say, $a = 2m$. Hence $4b^3 = 8m^3$; canceling, $b^3 = 2m^3$, forcing b to be even. This contradicts $(a, b) = 1$.

1.55 **(i)** Find $d = \gcd(12327, 2409)$, find integers s and t with $d = 12327s + 2409t$, and put the fraction 2409/12327 in lowest terms.

Solution. One uses the Euclidean algorithm to get: $(12327, 2409) = 3$ and $3 = 12327 \cdot 299 - 2409 \cdot 1530$; the fraction 2409/12327 = 803/4109 is in lowest terms.

(ii) Find $d = \gcd(7563, 526)$, and express d as a linear combination of 7563 and 526.

Solution. The Euclidean algorithm gives

$$(7563, 526) = 1 \text{ and } 1 = 532 - 526 - 37 - 7563.$$

(iii) Find $d = \gcd(73122, 7404621)$ and express d as a linear combination of 73122 and 7404621.

Solution. Here are the equations of the Euclidean algorithm:

$$\begin{aligned} 7404621 &= 101 \cdot 73122 + 19299 \\ 73122 &= 3 \cdot 19299 + 15225 \\ 19299 &= 1 \cdot 15225 + 4074 \\ 15225 &= 3 \cdot 4074 + 3003 \\ 4074 &= 1 \cdot 3003 + 1071 \\ 3003 &= 2 \cdot 1071 + 861 \\ 1071 &= 1 \cdot 861 + 210 \\ 861 &= 4 \cdot 210 + 21 \\ 210 &= 10 \cdot 21. \end{aligned}$$

We conclude that the gcd is 21. Following the algorithm in the text, we find that

$$21 = 34531 \cdot 73122 - 341 \cdot 7404621.$$

1.56 Let a and b be integers, and let $sa + tb = 1$ for s, t in $\mathbb{Z}$. Prove that a and b are relatively prime.

Solution. If $sa + tb = 1$, then any common divisor of a and b must divide 1; hence, a and b are relatively prime.

1.57 If $d = (a, b)$, prove that a/d and b/d are relatively prime.

Solution. Absent.

1.58 Prove that if $(r, m) = 1 = (r', m)$, then $(rr', m) = 1$.

Solution. Since $(r, m) = 1$, we have $ar + bm = 1$; since $(r', m) = 1$, we have $sr' + tm = 1$. Multiplying,

$$1 = (ar + bm)(sr' + tm) = (as)rr' + (art + bsr' + btm)m.$$

Therefore, 1 is a linear combination of rr' and m; as 1 is obviously the smallest positive linear combination, it must be their gcd.

1.59 Let a, b and d be integers. If $d = sa + tb$, where s and t are integers, find infinitely many pairs of integers (s_k, t_k) with $d = s_k a + t_k b$.
Solution. If $d = sa + tb$, and if we define $s_k = s + kb$ and $t_k = t - ka$, then $d = s_k a + t_k b$ for all k.

1.60 If a and b are relatively prime and if each divides an integer n, prove that their product ab also divides n.
Solution. Assume that $(a, b) = 1$ and $n = ak = b\ell$. By Corollary 1.40, $b \mid ak$ implies $b \mid k$. Thus, $k = bk'$ and so $n = ak = abk'$.

1.61 Prove, for any (possibly negative) integers a and b, that $(b, a) = (b-a, a)$.
Solution. If c is a common divisor of a and b, then $c \mid a$ and $c \mid b$; hence, $c \mid b-a$, and c is a common divisor of a and $b-a$. This does not yet show that the two gcd's are equal. However, if c' is a common divisor of a and $b - a$, then $c' \mid b$, for $b = a + (b - a)$. Hence, c' is a common divisor of a and b. It now follows that the two gcd's are equal.

1.62 If $a > 0$, prove that $a(b, c) = (ab, ac)$. [One must assume that $a > 0$ lest $a(b, c)$ be negative.]
Solution. Let $(b, c) = d$. Clearly, ad is a common divisor of ab and ac. Now let k be a common divisor of ab and ac. It suffices to prove that $k \mid ad$. If $sb + tc = d$, then $asb + atc = ad$, and $k \mid ad$ because it divides each of the summands on the left. As we mentioned in the exercise, the only reason to assume that $a > 0$ is to guarantee that $a(b, c)$ be positive.

1.63 Prove that the following pseudocode implements the Euclidean algorithm.

```
Input: a, b
Output: d
d := b;    s := a
WHILE s > 0 DO
   rem := remainder after dividing d by s
   d := s
   s := rem
END WHILE
```

Solution. The idea is to show that a proof of the Euclidean algorithm can be constructed by following the steps of the algorithm.

1.64 If F_n denotes the nth term of the Fibonacci sequence 0, 1, 1, 2, 3, 5, 8, ..., prove, for all $n \geq 1$, that F_{n+1} and F_n are relatively prime.
Solution. The hint refers to the fact, which is the key step in antanairesis, that $(a, b) = (a - b, b)$ whenever $a > b$. The proof is by induction on $n \geq 1$. The base step $n = 1$ is true, for $(F_2, F_1) = (1, 1) = 1$. For the

inductive step, use antanairesis and the defining recurrence,

$$\begin{aligned}(F_{n+2}, F_{n+1}) &= (F_{n+1} - F_n, F_{n+1}) \\ &= (F_n, F_{n+1}) = 1.\end{aligned}$$

Here is a proof that is a variation of the same idea. Let $n \geq 1$ be the smallest integer for which F_{n+1} and F_n have gcd $d > 1$. We note that $n > 1$ because $(F_2, F_1) = (1, 1) = 1$, and so $n - 1 \geq 1$. But if d is a common divisor of F_{n+1} and F_n, then d divides $F_{n-1} = F_{n+1} - F_n$, so that $(F_n, F_{n-1}) \neq 1$. This contradicts n being the smallest index for which $(F_{n+1}, F_n) \neq 1$.

1.65 **(i)** Show that if d is the greatest common divisor of $a_1, a_2, \ldots, a_n$, then $d = \sum t_i a_i$, where t_i is in $\mathbb{Z}$ for all i with $1 \leq i \leq n$.

Solution. The set I of all linear combinations $\sum t_i a_i$ of $a_1, a_2, \ldots, a_n$, where t_i is in $\mathbb{Z}$ for $1 \leq i \leq n$, satisfies the conditions of Corollary 1.37. If d is the smallest positive element in I, then the proof of Theorem 1.35 can be modified to show that d is the gcd.

(ii) Prove that if c is a common divisor of $a_1, a_2, \ldots, a_n$, then $c \mid d$.

Solution. The proof of Corollary 1.40 generalizes easily.

1.66 **(i)** Show that (a, b, c), the gcd of a, b, c, is equal to $(a, (b, c))$.

Solution. It suffices to prove that any common divisor of a, b, c is a common divisor of a and (b, c), and conversely. But each of these statements is easy to prove.

(ii) Compute $(120, 168, 328)$.

Solution.

$$(120, 168, 328) = (120, (328, 168)) = (120, 8) = 8$$

1.67 **(i)** Consider a complex number $z = q + ip$, where $q > p$ are positive integers. Prove that

$$(q^2 - p^2, 2qp, q^2 + p^2)$$

is a Pythagorean triple by showing that $|z^2| = |z|^2$.

Solution. If $z = q + ip$, then $|z^2| = |z|^2$, by part (i). Now $z^2 = (q^2 - p^2) + i2qp$, so that $|z^2| = (q^2 - p^2)^2 + (2qp)^2$. On the other hand, $|z|^2 = (q^2 + p^2)^2$. Thus, if we define $a = q^2 - p^2$, $b = 2qp$, and $c = q^2 + p^2$, then $a^2 + b^2 = c^2$ and (a, b, c) is a Pythagorean triple.

(ii) Show that the Pythagorean triple $(9, 12, 15)$ (which is not primitive) is not of the type given in part (i).

Solution. Suppose there are q and p for (9, 12, 15). Then $2qp = 12$ and $qp = 6$. Since $q > p$ are positive integers, the only possibilities are $q = 6$ and $p = 1$ or $q = 3$ and $p = 2$. The first possibility gives the Pythagorean triple (12, 35, 37) while the second gives the Pythagorean triple (5, 12, 13).

(iii) Using a calculator which can find square roots but which can display only 8 digits, show that

$$(19597501, 28397460, 34503301)$$

is a Pythagorean triple by finding q and p.

Solution. If q and p exist, then we have

$$q^2 + p^2 = 34503301$$
$$q^2 - p^2 = 19597501.$$

Therefore, $2p^2 = 14905800$ and $p^2 = 7452900$. Hence, $p = 2730$. Finally, $2qp = 28397460$, and so $q = 5201$. Since we were able to find q and p, the original trio does form a Pythagorean triple.

1.68 True or false with reasons.

(i) $|2^{19} - 3^{12}| < \frac{1}{2}$.

Solution. False.

(ii) If $r = p_1^{g_1} \cdots p_n^{g_n}$, where the p_i are distinct primes and the g_i are integers, then r is an integer if and only if all the g_i are nonnegative.

Solution. True.

(iii) The least common multiple $[2^3 \cdot 3^2 \cdot 5 \cdot 7^2, 3^3 \cdot 5 \cdot 13] = 2^3 \cdot 3^5 \cdot 5^2 \cdot 7^2 \cdot 13/45$.

Solution. True.

(iv) If a and b are positive integers which are not relatively prime, then there is a prime p with $p \mid a$ and $p \mid b$.

Solution. True.

(v) If a and b are relatively prime, then $(a^2, b^2) = 1$.

Solution. True.

1.69 **(i)** Find gcd(210, 48) using factorizations into primes.

Solution. $210 = 2^1 \cdot 3^1 \cdot 5^1 \cdot 7^1$ and $48 = 2^4 \cdot 3^1 \cdot 5^0 \cdot 7^0$, so that $(210, 48) = 2^1 \cdot 3^1 \cdot 5^0 \cdot 7^0 = 6$.

(ii) Find gcd(1234, 5678).

Solution. $1234 = 2 \cdot 617$ (the reader is expected to prove that 617 is prime, using $\sqrt{617} < 25$) and $5678 = 2 \cdot 17 \cdot 167$, so that the gcd $= 2$.

1.70 **(i)** Prove that an integer $m \geq 2$ is a perfect square if and only if each of its prime factors occurs an even number of times.

Solution. If $m = a^2$ and $a = p_1^{e_1} \cdots p_n^{e_n}$, then $m = p_1^{2e_1} \cdots p_n^{2e_n}$. Conversely, if $m = p_1^{2e_1} \cdots p_n^{2e_n}$, then $m = a^2$, where $a = p_1^{e_1} \cdots p_n^{e_n}$.

(ii) Prove that if m is a positive integer for which $\sqrt{m}$ is rational, then m is a perfect square. Conclude that if m is not a perfect square, then $\sqrt{m}$ is irrational.

Solution. Let $m = p_1^{e_1} \cdots p_n^{e_n}$. If m is not a perfect square, then at least one of the e_i is odd. If $\sqrt{m} = a/b$, then $mb^2 = a^2$. The exponent of p_i on the left is odd while the exponent of p_i on the right is even, and this is a contradiction.

1.71 If a and b are positive integers with $(a, b) = 1$, and if ab is a square, prove that both a and b are squares.

Solution. Since a and b are relatively prime, the sets of primes occurring in the factorization of a and of b are disjoint. Hence, if ab is a square, then all the exponents e_i in $ab = p_1^{e_1} \cdots p_n^{e_n}$ are even, and hence all the exponents arising from the primes in a (or in b) are even as well. Therefore, both a and b are perfect squares.

1.72 Let $n = p^r m$, where p is a prime not dividing an integer $m \geq 1$. Prove that $p \nmid \binom{n}{p^r}$.

Solution. Write $a = \binom{n}{p^r}$. By Pascal's formula:

$$a = \binom{n}{p^r} = \frac{n!}{(p^r)!(n - p^r)!}.$$

Cancel the factor $(n - p^r)!$ and cross-multiply, obtaining:

$$a(p^r)! = n(n-1)(n-2)\cdots(n - p^r + 1).$$

Thus, the factors on the right side, other than $n = p^r m$, have the form $n - i = p^r m - i$, where $1 \leq i \leq p^r - 1$. Similarly, the factors in $(p^r)!$, other than p^r itself, have the form $p^r - i$, for i in the same range: $1 \leq i \leq p^r - 1$.

If $p^e \mid p^r m - i$, where $e \leq r$ and $i \geq 1$, then $p^r m - i = bp^e$; hence, $p^e \mid i$; there is a factorization $i = p^e j$. Therefore, $p^r - i = p^e(p^{r-e} - j)$.

A similar argument shows that if $p^e \mid p^r - i$ for $i \geq 1$, then $p^e \mid p^r m - i$. By the fundamental theorem of arithmetic, the total number of factors p occurring on each side must be the same. Therefore, the total number of p's dividing ap^r must equal the total number of p's dividing $p^r m$. Since $p \nmid m$, the highest power of p dividing $p^r m$ is p^r, and so the highest power of p dividing ap^r is p^r; that is, $p \nmid a = \binom{p^r m}{p^r} = \binom{n}{p^r}$, as desired.

1.73 **(i)** For all rationals a and b, prove that

$$\|ab\|_p = \|a\|_p \|b\|_p \quad \text{and} \quad \|a+b\|_p \leq \max\{\|a\|_p, \|b\|_p\}.$$

Solution. If $a = p^e p_1^{e_1} \cdots p_n^{e_n}$ and $b = p^f p_1^{f_1} \cdots p_n^{f_n}$, then

$$ab = p^{e+f} p_1^{e_1+f_1} \cdots p_n^{e_n+f_n}.$$

Hence

$$\|ab\|_p = p^{-e-f} = p^{-e} p^{-f} = \|a\|_p \|b\|_p.$$

Assume $e \leq f$, so that $-f \leq -e$ and $\|a\|_p = \max\{\|a\|_p, \|b\|_p\}$.

$$\begin{aligned} a + b &= p^e p_1^{e_1} \cdots p_n^{e_n} + p^f p_1^{f_1} \cdots p_n^{f_n} \\ &= p^e \left(p_1^{e_1} \cdots p_n^{e_n} + p^{f-e} p_1^{f_1} \cdots p_n^{f_n} \right). \end{aligned}$$

If $u = p_1^{e_1} \cdots p_n^{e_n} + p^{f-e} p_1^{f_1} \cdots p_n^{f_n}$, then either $u = 0$ or $\|u\|_p = p^{-0} = 1$. In the first case, $\|a+b\|_p = 0$, and the result is true. Otherwise,

$$\begin{aligned} \|a+b\|_p = p^{-e}\|u\|_p &= \|a\|_p \|u\|_p \\ &\leq \|a\|_p = \max\{\|a\|_p, \|b\|_p\}. \end{aligned}$$

(ii) For all rationals a, b, prove $\delta_p(a,b) \geq 0$ and $\delta_p(a,b) = 0$ if and only if $a = b$.

Solution. $\delta_p(a,b) \geq 0$ because $\|c\|p \geq 0$ for all c. If $a = b$, then $\delta_p(a,b) = \|a-b\|p = \|0\|p = 0$; conversely, if $\delta_p(a,b) = 0$, then $a - b = 0$ because 0 is the only element c with $\|c\|_p = 0$.

(iii) For all rationals a, b, prove that $\delta_p(a,b) = \delta_p(b,a)$.

Solution. $\delta_p(a,b) = \delta_p(b,a)$ because

$$\|-c\|p = \|-1\|p\|c\|_p = \|c\|_p.$$

(iv) For all rationals a, b, c, prove $\delta_p(a, b) \leq \delta_p(a, c) + \delta_p(c, b)$.
Solution. $\delta_p(a, b) \leq \delta_p(a, c) + \delta_p(c, b)$ because

$$\begin{aligned}\delta_p(a, b) = \|a - b\|_p &= \|(a - c) + (c - b)\|_p \\ &\leq \max\{\|a - c\|_p, \|c - b\|_p\} \\ &\|a - c\|_p + \|c - b\|_p \\ &= \delta_p(a, c) + \delta_p(c, b).\end{aligned}$$

(v) If a and b are integers and $p^n \mid (a - b)$, then $\delta_p(a, b) \leq p^{-n}$. (Thus, a and b are "close" if $a - b$ is divisible by a "large" power of p.)
Solution. If $p^n \mid a - b$, then $a - b = p^n u$, where u is an integer. But $\|u\|_p \leq 1$ for every integer u, so that

$$\delta_(a, b) = \|a - b\|_p = \|p^n u\|_p = \|p^n\|_p \|u\|_p \leq p^{-n}.$$

At this point, one could assign a project involving completions, p-adic integers, and p-adic numbers.

1.74 Let a and b be in $\mathbb{Z}$. Prove that if $\delta_p(a, b) \leq p^{-n}$, then a and b have the same first n p-adic digits, $d_0, \ldots, d_{n-1}$.
Solution. This follows from the fact that $p^n \mid a$ if and only if the first p-adic digits $d_0, \ldots, d_{n-1}$ are all 0.

1.75 Prove that an integer $M \geq 0$ is the lcm of $a_1, a_2, \ldots, a_n$ if and only if it is a common multiple of $a_1, a_2, \ldots, a_n$ which divides every other common multiple.
Solution. Consider the set I of all the common multiples of $a_1, a_2, \ldots, a_n$. It is easy to check that I satisfies the hypotheses of Corollary 1.37, so that every number m in I is a multiple of d, where d is the smallest positive element in I. Since each a_i is in I, d is a common multiple; if m is any common multiple, then m is in I and hence $d \mid m$.

Conversely, if d is a common multiple dividing every common multiple m, then $d \leq |m|$.

1.76 **(i)** Give another proof of Proposition 1.56, $[a, b](a, b) = |ab|$, without using the Fundamental Theorem of Arithmetic.
Solution. The result is easy if either $a = 0$ or $b = 0$. Otherwise, if $(a, b) = d$, then $a = da'$ and $b = db'$, where $(a', b') = 1$. Now ab/d is an integer, and it is a common multiple of a and b:

$$ab/d = a(b/d) = b(a/d).$$

Next, we show that if c is a common multiple, then ab/d divides c. By hypothesis, $c = am = b\ell$. Now $c = am = da'm$ and

$c = b\ell = db'\ell$, so that $a'm = b'\ell$. Thus, a' divides $b'\ell$; as $(a', b') = 1$, we have a' divides ℓ, by Corollary 1.40. Write $\ell = a'k$, and observe that

$$c = db'\ell = db'a'k = (db')(da')k/d = [ab/d]k.$$

Therefore, $ab/d = [a, b]$, and so $[a, b](a, b) = ab$.

(ii) Find $[1371, 123]$.

Solution. $[1371, 123] = 1371 \cdot 123/(1371, 123)$. By the Euclidean algorithm, $(1371, 123) = 3$, and so $[1371, 123] = 56, 211$.

1.77 True or false with reasons.

(i) If a and m are integers with $m > 0$, then $a \equiv i \bmod m$ for some integer i with $0 \leq i \leq m - 1$.

Solution. True.

(ii) If a, b and m are integers with $m > 0$, then $a \equiv b \bmod m$ implies $(a + b)^m \equiv a^m + b^m \bmod m$.

Solution. False.

(iii) If a is an integer, then $a^6 \equiv a \bmod 6$.

Solution. False.

(iv) If a is an integer, then $a^4 \equiv a \bmod 4$.

Solution. False.

(v) 5263980007 is a perfect square.

Solution. False.

(vi) There is an integer n with $n \equiv 1 \bmod 100$ and $n \equiv 4 \bmod 1000$.

Solution. False.

(vii) There is an integer n with $n \equiv 1 \bmod 100$ and $n \equiv 4 \bmod 1001$.

Solution. True.

(viii) If p is a prime and $m \equiv n \bmod p$, then $a^m \equiv a^n \bmod p$ for every natural number a.

Solution. False.

1.78 Find all the integers x which are solutions to each of the following congruences:

(i) $3x \equiv 2 \bmod 5$.

Solution. $x \equiv 4 \bmod 5$.

(ii) $7x \equiv 4 \bmod 10$.

Solution. $x \equiv 12 \bmod 10$.

(iii) $243x + 17 \equiv 101 \bmod 725$.

Solution. The Euclidean algorithm gives $1 = 182 \cdot 243 - 61 \cdot 725$.

$$243x + 17 \equiv 101 \bmod 725 \text{ gives } 243x \equiv 84 \bmod 725.$$

Hence $x \equiv 182 \cdot 84 = 15288 \equiv 63 \bmod 725$.

(iv) $4x + 3 \equiv 4 \bmod 5$.

Solution. $x \equiv 4 \bmod 5$.

(v) $6x + 3 \equiv 4 \bmod 10$.

Solution. $6x + 3 \equiv 4 \bmod 10$ is the same problem as $6x \equiv 1 \bmod 10$. There are no solutions. The candidates for x are all r with $0 \leq r \leq 9$, and multiplying each of them by 6 never gives 1 mod 10. (Of course, $(6, 10) \neq 1$.)

(vi) $6x + 3 \equiv 1 \bmod 10$.

Solution. $6x + 3 \equiv 1 \bmod 10$ is the same problem as $6x \equiv 8 \bmod 10$. This congruence does have solutions. If $6x - 8 = 10m$, then $3x - 4 = 5m$, and so this gives a new congruence $3x \equiv 4 \bmod 5$ or $x \equiv 8 \equiv 3 \bmod 5$. Thus, $x = \ldots - 2, 3, 8, 13, \ldots$; there are two possible solutions mod10, namely, $x \equiv 3 \bmod 10$ and $x \equiv 8 \bmod 10$.

1.79 Let m be a positive integer, and let m' be an integer obtained from m by rearranging its (decimal) digits (e.g., take $m = 314159$ and $m' = 539114$). Prove that $m - m'$ is a multiple of 9.

Solution. By casting out 9s, a number is divisible by 9 if and only if the sum of its (decimal) digits is divisible by 9. But m and m' have the same set of digits, for one is just a permutation of the other, and so the sum of their digits is the same. Hence, one is divisible by 9 if and only if the other one is.

1.80 Prove that a positive integer n is divisible by 11 if and only if the alternating sum of its digits is divisible by 11.

Solution. Since $10 \equiv -1 \bmod 11$,

$$a = d_k 10^k + \cdots + d_1 10 + d_0 \equiv d_k(-1)^k + \cdots - d_1 + d_0.$$

1.81 What is the remainder after dividing 10^{100} by 7?

Solution. Use Corollary 1.67 after noting that $100 = 2 \cdot 7^2 + 2$ (of course, this says that 100 has 7-adic digits 202). Hence

$$10^{100} \equiv 3^{100} \equiv 3^4 = 81 \equiv 4 \bmod 7.$$

1.82 **(i)** Prove that $10q+r$ is divisible by 7 if and only if $q-2r$ is divisible by 7.

Solution. If $10q + r \equiv 0 \bmod 7$, then $15q + 5r \equiv 0 \bmod 7$, and so $q - 2r \equiv 0 \bmod 7$. Conversely, if $q - 2r \equiv 0 \bmod 7$, then $3q - 6r \equiv 0 \bmod 7$, hence $3q + r \equiv 0 \bmod 7$, and so $10q + r \equiv 0 \bmod 7$.

(ii) Given an integer a with decimal digits $d_k d_{k-1} \ldots d_0$, define

$$a' = d_k d_{k-1} \cdots d_1 - 2d_0.$$

Show that a is divisible by 7 if and only if some one of a', a'', a''',... is divisible by 7.

Solution. If $a = 10b + d_0$, then $a' = b - 2d_0$. By part (i), $a \equiv 0 \bmod 7$ if and only if $a' \equiv 0 \bmod 7$. Now repeat.

1.83 **(i)** Show that $1000 \equiv -1 \bmod 7$.

Solution. Dividing 1000 by 7 leaves remainder $6 \equiv -1 \bmod 7$.

(ii) Show that if $a = r_0 + 1000r_1 + 1000^2 r_2 + \cdots$, then a is divisible by 7 if and only if $r_0 - r_1 + r_2 - \cdots$ is divisible by 7.

Solution. If $a = r_0 + 1000r_1 + 1000^2 r_2 + \cdots$, then

$$a \equiv r_0 + (-1)r_1 + (-1)^2 r_2 + \cdots = r_0 - r_1 + r_2 - \cdots \bmod 7.$$

Hence a is divisible by 7 if and only if $r_0 - r_1 + r_2 - \cdots$ is divisible by 7.

1.84 For a given positive integer m, find all integers r with $0 < r < m$ such that $2r \equiv 0 \bmod m$

Solution. The answer depends on the parity of m.

1.85 Prove that there are no integers x, y, and z such that $x^2 + y^2 + z^2 = 999$.

Solution. Now $999 \equiv 7 \bmod 8$. But no sum of three numbers, with repetitions allowed, taken from $\{0, 1, 4\}$, adds up to 7. This is surely true if a 4 is not used, while if a 4 is used, then the largest sum one can get which is under 8 is 6.

1.86 Prove that there is no perfect square a^2 whose last two digits are 35.

Solution. If a is a positive integer, then

$$a = d_0 + 10d_1 + 100d_2 + \cdots + 10^n d_n,$$

where $0 \le d_i \le 9$ for all i. Therefore, $a \equiv d_0 + 10d_1 \bmod 100$. In particular, the last two digits of a are 35 if and only if $a \equiv 35 \bmod 100$.

Let b be a positive integer with $b^2 \equiv 35 \bmod 100$. Now the last digit of b must be 5 (otherwise the last digit of b^2 would not be 5), and so

$b \equiv 5 \bmod 10$. Hence, $b = 5 + 10q$. and so $b^2 \equiv (5 + 10q)^2 \bmod 100$. But

$$(5 + 10q)^2 = 25 + 2 \cdot 5 \cdot q + 100q^2 \equiv 25 \bmod 100,$$

and so the last two digits of b^2 are 25, not 35. Therefore, no such b exists.

(More is true. We have proved that if the last digit of a perfect square is 5, then its last two digits are 25.)

1.87 If x is an odd number not divisible by 3, prove that $x^2 \equiv 1 \bmod 24$.
Solution. Here are two ways to proceed. The odd numbers < 24 not divisible by 3 are 1, 5, 7, 11, 13, 17, 19, 23; square each mod 24.

Alternatively, Example 1.161 says that the squares mod 8 are 0, 1, and 4. Now $x^2 - 1$ is divisible by 24 if and only if it is divisible by 3 and by 8 (as 3 and 8 are relatively prime). If x is to be odd, then $x \equiv 0 \bmod 3$ or $x \equiv 2 \bmod 3$; looking at x mod 8, the hypothesis eliminates those x with $x^2 \equiv 0 \bmod 8$ or $x^2 \equiv 4 \bmod 8$.

1.88 Prove that if p is a prime and if $a^2 \equiv 1 \bmod p$, then $a \equiv \pm 1 \bmod p$.
Solution. By Euclid's lemma, if p divides $a^2 - 1 = (a + 1)(a - 1)$, then p divides $a + 1$ or p divides $a - 1$; that is, $a \equiv \pm 1 \bmod p$.

1.89 Consider the congruence $ax \equiv b \bmod m$ when $\gcd(a, m) = d$. Show that $ax \equiv b \bmod m$ has a solution if and only if $d \mid b$.
Solution. If x_0 is a solution of $ax \equiv b \bmod m$, then $ax_0 - b = my$ for some integer y. Now $a = da'$ and $m = dm'$, by hypothesis, and so $da'x_o - b = dm'y$. It follows that $d \mid b$.

Conversely, suppose that $b = db'$. Then the congruence is

$$da'x \equiv db' \bmod dm'.$$

Note that $(a', m') = (a/d, m/d) = 1$, because d is the gcd (a, m). Therefore, the congruence $a'x \equiv b' \bmod m'$ has a solution, say, u, and hence du is a solution of the original congruence.

1.90 Solve the congruence $x^2 \equiv 1 \bmod 21$.
Solution. If $x^2 \equiv 1 \bmod 21$, then $21 \mid (x^2 - 1)$; that is, $21 \mid (x+1)(x-1)$. Hence, $3 \mid (x + 1)(x - 1)$ and $7 \mid (x + 1)(x - 1)$. By Euclid's lemma, $x \equiv \pm 1 \bmod 3$ and $x \equiv \pm 1 \bmod 7$. Thus, x is not a multiple of 3, while the candidates from the other congruences are 1, 8, 15, and 6, 13, 20. Thus, there are 4 solutions: [1], [8], [13], and [20].

1.91 Solve the simultaneous congruences:

(i) $x \equiv 2 \bmod 5$ and $3x \equiv 1 \bmod 8$;
Solution. $x \equiv 27 \bmod 40$.

(ii) $3x \equiv 2 \bmod 5$ and $2x \equiv 1 \bmod 3$.
Solution. $x \equiv 14 \bmod 15$.

1.92 Find the smallest positive integer which leaves remainder 4, 3, 1 after dividing by 5, 7, 9, respectively.
Solution. That the desired integer x satisfies three congruences:

$$x \equiv 4 \bmod 5; \quad x \equiv 3 \bmod 7; \quad x \equiv 1 \bmod 9.$$

By the Chinese remainder theorem, the first two congruences give

$$x \equiv 24 \bmod 35.$$

Now use the Chinese remainder theorem for the system

$$x \equiv 24 \bmod 35$$
$$x \equiv 1 \bmod 9$$

(which is possible because $(35, 9) = 1$. We obtain $x \equiv 199 \bmod 315$. Thus, 199 is the smallest such solution.

1.93 How many days are there between Akbal 13 and Muluc 8 in the Mayan tzolkin calendar?
Solution. Akbal is month 3 and Muluc is month 9. If x is the intervening number of days, then

$$x \equiv 13 - 8 \bmod 13$$
$$x \equiv 3 - 9 \bmod 20.$$

The Chinese remainder theorem gives $x \equiv 174 \bmod 260$ (and so the number of intervening days is either 174 or 86).

1.94 **(i)** Show that $(a + b)^n \equiv a^n + b^n \bmod 2$ for all a and b and for all $n \geq 1$.
Solution. If a is even, then $a + b \equiv b \bmod 2$ and $(a + b)^n \equiv b^n \equiv a^n + b^n \bmod 2$ for all n; a similar argument holds if b is even. If both a and b are odd, then $a \equiv 1 \equiv b \bmod 2$; hence, $a + b \equiv 1 + 1 \equiv 0 \bmod 2$ and $(a + b)^n \equiv 0 \bmod 2$, while $a^n + b^n \equiv 1 + 1 = 0 \bmod 2$.

(ii) Show that $(a + b)^2 \not\equiv a^2 + b^2 \bmod 3$.
Solution. If $a = 1 = b$, then $(a + b)^2 \equiv 4 \equiv 1 \bmod 3$, while $a^2 + b^2 \equiv 2 \bmod 3$.

1.95 Solve the linear system

$$x \equiv 12 \bmod 25$$
$$x \equiv 2 \bmod 30.$$

Solution. Absent.

1.96 Let m, m' be positive integers, let $d = (m, m')$, and let $b \equiv b' \bmod d$. Prove that any two solutions of the system

$$x \equiv b \bmod m$$
$$x \equiv b' \bmod m'$$

are congruent mod ℓ, where $\ell = \text{lcm}\{m, m'\}$.
Solution. Absent.

1.97 On a desert island, five men and a monkey gather coconuts all day, then sleep. The first man awakens and decides to take his share. He divides the coconuts into five equal shares, with one coconut left over. He gives the extra one to the monkey, hides his share, and goes to sleep. Later, the second man awakens and takes his fifth from the remaining pile; he too finds one extra and gives it to the monkey. Each of the remaining three men does likewise in turn. Find the minimum number of coconuts originally present.
Solution. Here are the equations arising from the story. Let C be the number of coconuts.

$$C = 5a + 1 \tag{1}$$
$$4a = 5b + 1 \tag{2}$$
$$4b = 5c + 1 \tag{3}$$
$$4c = 5d + 1 \tag{4}$$
$$4d = 5e + 1 \tag{5}$$

We work from the bottom up. Since $4d$ occurs in the last equation and $5d$ occurs in equation (4) above it, rewrite the latter as

$$16c = 5 \cdot 4d + 4.$$

Hence,

$$16c = 5 \cdot (5e + 1) + 4 = 25e + 9.$$

Now go up to the next equation (3), which we multiply by 16:

$$64b = 5(16c) + 16 = 5(25e + 9) + 16 = 125e + 61.$$

Go up again after multiplying by 64:

$$256a = 5(64b) + 64 = 5(125e + 61) + 64 = 625e + 369.$$

Finally, multiply equation (1) by 256 to get

$$256C = 5(256a) + 256 = 5(625e + 369) + 256 = 3125e + 2101.$$

Thus,

$$256C \equiv 2101 \bmod 3125.$$

Were the hint, "Try -4 coconuts," not given, one would proceed to solve this congruence, taking note of the fact that $(256, 3125) = 1$. But $C = -4$ is a solution of this congruence, and so $C \equiv -4 \bmod 3125$; that is, every number of the form $3125k - 4$ is a solution. The minimum value for C is thus 3121 coconuts.

1.98 A suspect said that he had spent the Easter holiday April 21, 1893, with his ailing mother; Sherlock Holmes challenged his veracity at once. How could the great detective have been so certain?
Solution. April 21, 1893, fell on Friday, and so this date could not have been Easter Sunday.

1.99 How many times in 1900 did the first day of a month fall on a Tuesday?
Solution. The year $y = 1900$ was not a leap year, and

$$g(y) \equiv [19/4] - 38 \equiv -34 \equiv 1 \bmod 7.$$

We seek the number of solutions to $3 \equiv 1 + j(m) + 1 \bmod 7$; that is, $j(m) \equiv 1 \bmod 7$. For the interval March through December, there is only one such month, namely, August. But we still have to check January and February, for they behave as if they occurred in 1899. Now $g(1899) \equiv 0 \bmod 7$, and the congruence is

$$3 \equiv 1 + j(m) \bmod 7 \text{ or } j(m) \equiv 2 \bmod 7.$$

As $j(\text{January}) = 0$ and $j(\text{February}) = 3$, neither of these months gives a solution, and so only August 1, 1900, fell on a Tuesday.

1.100 On what day of the week did February 29, 1896 fall? Conclude from your method of solution that no extra fuss is needed to find leap days.
Solution. March 1, 1896, fell on a Sunday, and so February 29, 1896, fell on a Saturday.

1.101

(i) Show that 1987 had three Friday 13s.
Solution. The following dates fell on Friday in 1986: February 13, March 13, and November 13.

(ii) Show, for any year $y > 0$, that $g(y) - g(y-1) = 1$ or 2, where $g(y) = y + \lfloor y/4 \rfloor - \lfloor y/100 \rfloor + \lfloor y/400 \rfloor$.
Solution. The following dates fell on Friday in 1986: February 13, March 13, and November 13.

(iii) Can there be a year with exactly one Friday 13?
Solution. Yes. For example, October 13, 1988, fell on a Friday, but no other 13th of the month fell on Friday.