Intermediate Number Theory

Justin Stevens

FOURTH EDITION

Mathematics is the queen of sciences and number theory is the queen of mathematics.

– Carl Friedrich Gauss

Last Updated December 29, 2017.

CONTENTS

CHAPTER 1

THE ART OF PROOFS

§1.1 Well-Ordering Principle

The set of ***integers*** are $\mathbb{Z} = \{\cdots, -3, -2, -1, 0, 1, 2, 3, \cdots\}$. Properties of addition $(+)$ and multiplication $(\cdot)$ for integers a and b include:

(I) Closure: $a + b$ and $a \cdot b$ are both integers.

(II) Associativity: $a + (b + c) = (a + b) + c$ and $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.

(III) Commutativity: $a + b = b + a$ and $a \cdot b = b \cdot a$.

(IV) Identity: $a + 0 = a$ and $a \cdot 1 = a$.

(V) Distributivity: $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(a + b) \cdot c = a \cdot c + b \cdot c$.

(VI) Additive Inverse: $a + (-a) = 0$.

Positive integers are $\mathbb{Z}^+ = \{1, 2, 3, \cdots\}$. The additive inverses of the positive integers are the negative integers. The natural numbers, $\mathbb{N}$, consist of zero combined with the positive integers. They are equipped with an ordering relation; we write $a < b$ if $b - a$ is positive.

Example 1.1. Prove that $\min(a, b) + \max(a, b) = a + b$.

Proof. We have two cases to consider. If $a \leq b$, then we have $\min(a, b) = a$ and $\max(a, b) = b$. Otherwise, if $b < a$, then $\min(a, b) = b$ and $\max(a, b) = a$. Either way, the result holds. □

Axiom (Well-Ordering). Every non-empty subset of $\mathbb{Z}^+$ has a least element.

The well-ordering principle serves as a starting block from which we build up number theory.

Definition. $x \in S$ denotes "x belongs to set S" and $R \subset S$ denotes "R is a subset of S".

Example 1.2. Prove that there is no integer between 0 and 1.

Proof. Assume for the sake of contradiction that $S = \{c \in \mathbb{Z} \mid 0 < c < 1\}$, the set of integers between 0 and 1, is non-empty. Hence, S must have a smallest element, say m. However, we see that $m^2 \in \mathbb{Z}$ from closure over multiplication and $0 < m^2 < m < 1$. This contradicts the minimality of m, hence $S = \emptyset$ and there are no integers between 0 and 1. □

A ***rational number*** can be expressed in the form a/b where a and b are integers and $b \neq 0$. The rationals, $\mathbb{Q}$, are a field since all non-zero elements have a multiplicative inverse. They can be formally defined as an equivalence class of pairs of integers (a, b) with $b \neq 0$ and equivalence relation $(a_1, b_1) \sim (a_2, b_2)$ if and only if $a_1 b_2 = a_2 b_1$.

Example 1.3. Prove that the rational numbers are not well-ordered.

Proof. We must show that there is no lower bound to the rationals. Consider the set

$$S = \left\{ \frac{1}{n} \text{ for } n \in \mathbb{Z}^+ \right\}.$$

As n grows larger the set approaches 0. This lower bound, however, is never reached. □

An ***irrational number*** cannot be expressed as the ratio of two integers. Around 500 BC, Pythagoras founded a religion called Pythagoreanism. The followers thought numbers explained everything in life, from nature to music. According to legend, Hippasus was a Pythagorean who was an excellent mathematician. While looking at the pentagram, he took the measure of the length of several sides and found the ratio was an irrational number, the golden ratio.

Two quantities are in the golden ratio if their ratio is the same as the ratio of their sum to the larger of the two quantities: $(a + b)/a = a/b \stackrel{\text{def}}{=} \varphi$. Letting $\varphi = a/b$ in the equation, we see

$$1 + \frac{1}{\varphi} = \varphi \implies \varphi^2 - \varphi - 1 = 0.$$

Using the quadratic formula, $\varphi = \frac{1+\sqrt{5}}{2}$. The other root is $\psi = \frac{1-\sqrt{5}}{2}$.

Example 1.4. Prove that $\sqrt{2}$ is irrational.

Proof by Contradiction. For positive integers a and b, let $\sqrt{2} = \dfrac{a}{b}$. Consider the set

$$X = \{k\sqrt{2} : \text{both } k \text{ and } k\sqrt{2} \text{ are positive integers}\}.$$

Since $a = b\sqrt{2}$, X is non-empty. Let the smallest element of X be $m = n\sqrt{2}$. Consider

$$m\sqrt{2} - m = m\sqrt{2} - n\sqrt{2} = (m - n)\sqrt{2}.$$

Since $m\sqrt{2} - m = 2n - m$ is a positive integer, we have $m\sqrt{2} - m \in X$. However,

$$(m - n)\sqrt{2} = \left(n\sqrt{2} - n\right)\sqrt{2} < n\sqrt{2}.$$

Therefore, $m\sqrt{2} - m$ is an element of X that is less than m, contradiction. □

The ***reals***, $\mathbb{R}$, consist of all rational and irrational numbers, therefore $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$.

§1.2 Induction

Induction is a popular proof technique used in mathematics. We begin with an example.

Example 1.5. Prove the identity $1 + 2 + 2^2 + 2^3 + \cdots + 2^n = 2^{n+1} - 1$.

Proof. We begin by testing the identity for small values of n:

$$1 = 2 - 1, \quad 1 + 2 = 4 - 1, \quad 1 + 2 + 4 = 8 - 1.$$

We now assume the identity is true for an arbitrary $n = k$:

$$1 + 2 + 2^2 + 2^3 + \cdots + 2^k = 2^{k+1} - 1. \qquad \text{(Hypothesis)}$$

Adding the next power of 2 to both sides of our assumption:

$$\begin{aligned}\left[1 + 2 + 2^2 + \cdots + 2^k\right] + 2^{k+1} &= \left[2^{k+1} - 1\right] + 2^{k+1} \\ &= 2^{k+2} - 1.\end{aligned}$$

Therefore, we have proven that if the identity is true for $n = k$, then it is also true for $n = k + 1$. Imagining the natural numbers as dominoes, we knock down the first domino ($n = 0$) and every domino knocks down the next one. Therefore, the identity is true for all natural numbers n. □

Principle (Mathematical Induction). To prove a statement P for all positive integers at least n_0,

(1) **Base Case:** Show $P(n_0)$.

(2) **Inductive Step:** Show $P(k)$ implies $P(k + 1)$ for any positive integer $k \geq n_0$.

Proof by Contradiction. Assume that $S = \{n \mid P(n) \text{ is false}\}$ is non-empty. Let the least element of S be m. Observe that $n_0 \notin S$, therefore $m > n_0$. Furthermore, by minimality, $m - 1 \notin S$. However by the inductive step, $P(m - 1)$ implies $P(m)$, contradiction. □

Example 1.6. Prove the sum of cubes identity

$$1^3 + 2^3 + 3^3 + \cdots + n^3 = \left[\frac{n(n+1)}{2}\right]^2.$$

Proof by Induction. When $n = 1$, $1 = 1^2$. We assume the formula is true for $n = k$, hence

$$1^3 + 2^3 + 3^3 + \cdots + k^3 = \left[\frac{k(k+1)}{2}\right]^2. \qquad \text{(Hypothesis)}$$

Adding the next cube to both sides of our assumption gives:

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

This is the sum of cubes formula for $n = k+1$, hence the identity holds for all positive integers. □

Exercises

1.2.1. Prove that the sum of the first n positive odd integers is n^2.

1.2.2. Prove the geometric series formula for all positive integers n,

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

§1.3 Pascal's Triangle and Fibonacci Numbers

Definition. The factorial of a positive n is recursively defined by $n! = n \cdot (n-1)!$ and $0! = 1$. In other words, it equals the product of all positive integers less than or equal to n.

For example, $6! = 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 720$. We also define the binomial coefficient $\binom{n}{k} = \dfrac{n!}{k!(n-k)!}$.

Theorem 1.1 (Pascal's Identity).

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

Proof. By the definition of binomial coefficients and factorials,

$$\begin{aligned}
\binom{n-1}{k-1} + \binom{n-1}{k} &= \frac{(n-1)!}{(k-1)!(n-k)!} + \frac{(n-1)!}{k!(n-k-1)!} \\
&= (n-1)! \left(\frac{k}{k!(n-k)!} + \frac{n-k}{k!(n-k)!} \right) \\
&= (n-1)! \left(\frac{n}{k!(n-k)!} \right) \\
&= \frac{n!}{k!(n-k)!} = \binom{n}{k}.
\end{aligned}$$

□

Using Pascal's identity along with induction, we can prove the following result:

Theorem 1.2 (Binomial Theorem).

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k.$$

You will be asked to prove this in an exercise. We now introduce a famous recurrence.

Definition. The Fibonacci numbers are defined by $F_1 = 1, F_2 = 1$, and $F_{n+2} = F_{n+1} + F_n$. Every number is the sum of the two preceeding terms. The first several Fibonacci numbers are

$$1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, \cdots.$$

The Fibonacci numbers have many beautiful and surprising properties.

Example 1.7. Consider a board of length n. How many ways are there to tile this board with squares (length 1) and dominoes (length 2)?

Solution. Let $f(n)$ be the number of tilings of an n-board. We can compute $f(1) = 1$ and $f(2) = 2$. Depending on if we begin with a square or domino, we either have a $n-1$ or a $n-2$ board remaining:

$$f(n) = f(n-1) + f(n-2).$$

This is exactly the Fibonacci recurrence with a shifted index of 1. Hence, $f(n) = F_{n+1}$. □

Example 1.8. Prove that for all positive integers n,

$$F_1 + F_2 + F_3 + \cdots + F_n = F_{n+2} - 1.$$

Proof by Induction. When $n = 1$, $1 = 2 - 1$. Assuming the identity for $n = k$, we have

$$F_1 + F_2 + F_3 + \cdots + F_k = F_{k+2} - 1. \qquad \text{(Hypothesis)}$$

We add the next Fibonacci number, F_{k+1}, to both sides of our assumption (in parenthesis):

$$\begin{aligned}[F_1 + F_2 + F_3 + \cdots + F_k] + F_{k+1} &= [F_{k+2} - 1] + F_{k+1} \\ &= F_{k+3} - 1.\end{aligned}$$

This is the identity for $n = k + 1$, hence by induction, our proof is complete. □

Example 1.9. Prove that the diagonal sum of Pascal's triangle are Fibonacci numbers,

$$F_{n+1} = \sum_{k\geq 0} \binom{n-k}{k} = \binom{n}{0} + \binom{n-1}{1} + \binom{n-2}{2} + \cdots.$$

Solution. The left-hand side is the number of tilings of an n-board. If there are k dominoes in a tiling, then there are $n - 2k$ squares for a total of $n - k$ tiles. The number of ways to select k of these to be dominoes is $\binom{n-k}{k}$. Therefore, there are $f(n) = F_{n+1} = \sum_{k\geq 0} \binom{n-k}{k}$ tilings. □

Example 1.10 (Binet's Formula)**.** Recall $\varphi = \frac{1+\sqrt{5}}{2}$ is the golden ratio and $\psi = \frac{1-\sqrt{5}}{2}$. Prove

$$F_n = \frac{\varphi^n - \psi^n}{\sqrt{5}}.$$

Proof by Induction. For base cases, $F_1 = (\varphi - \psi)/\sqrt{5} = 1$ and $F_2 = (\varphi^2 - \psi^2)/\sqrt{5} = 1$. Furthermore, φ and ϕ are roots of the quadratic $x^2 - x - 1 = 0$, therefore

$$\begin{aligned}\varphi^k &= \varphi^{k-1} + \varphi^{k-2} \\ \psi^k &= \psi^{k-1} + \psi^{k-2}.\end{aligned}$$

Assume Binet's formula for $n = k-2$ and $n = k-1$. From the definition of Fibonacci numbers,

$$\begin{aligned} F_k &= F_{k-1} + F_{k-2} \\ &= \frac{\varphi^{k-1} - \psi^{k-1}}{\sqrt{5}} + \frac{\varphi^{k-2} - \psi^{k-2}}{\sqrt{5}} \\ &= \frac{\varphi^{k-1} + \varphi^{k-2}}{\sqrt{5}} - \frac{\psi^{k-1} + \psi^{k-2}}{\sqrt{5}} \\ &= \frac{\varphi^k - \psi^k}{\sqrt{5}}. \end{aligned}$$

This is Binet's formula for k, hence we have proven the identity by induction. □

Exercises

1.3.1. Prove the following identies using the Binomial Theorem:

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

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

(iii) $\binom{n}{0} + 2\binom{n}{1} + 2^2\binom{n}{2} + \cdots + 2^n\binom{n}{n} = 3^n$.

1.3.2. Prove the following Fibonacci identites:

(i) $F_1 + F_3 + F_5 + \cdots + F_{2n-1} = F_{2n}$.

(ii) $F_1^2 + F_2^2 + \cdots + F_n^2 = F_n F_{n+1}$.

1.3.3. Prove the Binomial Theorem using induction.

§1.4 Strong Induction and Recursion

Principle (Strong Mathematical Induction). To prove a statement P for all positive integers $\geq n_0$,

(1) **Base Case:** Show $P(n_0)$.

(2) **Inductive Step:** Show $P(n_0), P(n_0+1), \cdots, P(k)$ implies $P(k+1)$ for any integer $k \geq n_0$.

Example 1.11 (Zeckendorf). Prove every positive integer N can be represented as the unique sum of non-consecutive Fibonacci numbers. In other words, there exists a unique $\{a_j\}_{j=0}^{m}$ with

$$N = \sum_{j=0}^{m} F_{a_j}, \quad a_0 \geq 2 \text{ and } a_{j+1} > a_j + 1.$$

Proof by Strong Induction. For the base case of $N = 1$, the unique representation sum is $1 = F_2$. Now, assume that every every integer up to K can be written as the unique sum of distinct non-consecutive Fibonacci numbers. Let $F_{\max}$ be the largest Fibonacci number such that $F_{\max} \leq K+1$. If $F_{\max} = K+1$, then we are clearly done. Otherwise, $F_{\max} < K+1 < F_{\max+1}$, therefore

$$0 < (K+1) - F_{\max} < F_{\max+1} - F_{\max} = F_{\max-1}. \tag{$\star$}$$

By our hypothesis, there exists a sequence $\{a_j\}_{j=0}^{m}$ with $a_{j+1} > a_j + 1$ such that

$$K + 1 - F_{\max} = \sum_{j=0}^{m} F_{a_j}.$$

Since $F_{a_m} < F_{\max-1}$ by $(\star)$, adding $F_{\max}$ to both sides produces a valid representation for $K+1$.

For uniqueness, we require the following lemma, whose proof is left as an exercise:

Lemma. *The sum of any set of distinct, non-consecutive Fibonacci numbers whose largest member is F_j is strictly less than the next larger Fibonacci number F_{j+1}.*

For the sake of contradiction, let $K+1$ be the smallest integer with two representations:

$$\begin{aligned} K+1 &= F_{a_1} + F_{a_2} + \cdots + F_{a_m} \\ &= F_{b_1} + F_{b_2} + \cdots + F_{b_l}. \end{aligned}$$

Without loss of generality, assume that $a_m \geq b_l$. If $a_m > b_l$, then our Lemma shows

$$\begin{aligned} K+1 &= F_{b_1} + F_{b_2} + \cdots + F_{b_l} \\ &< F_{b_l+1} - 1 \\ &\leq F_{a_m} - 1 \\ &< F_{a_1} + F_{a_2} + \cdots + F_{a_m} \\ &= K+1. \end{aligned}$$

This is a contradiction, therefore $a_m = b_l$. By our hypothesis, $K+1-F_{a_m} = K+1-F_{b_l}$ has a unique representation, so adding the values back, $K+1$ also has a unique representation. □

The method of subtracting the largest Fibonacci number is known as a **greedy strategy**.

Example 1.12. The Ackermann function is a recursive function defined by

$$A(m,n) = \begin{cases} n+1, & \text{if } m = 0 \\ A(m-1,1), & \text{if } n = 0 \\ A(m-1, A(m,n-1)) & \text{otherwise.} \end{cases}$$

Prove that for every natural n, (i) $A(1,n) = n+2$, (ii) $A(2,n) = 2n+3$, (iii) $A(3,n) = 2^{n+3} - 3$.

Proof by Induction. We use these three examples to build up the Ackermann function.

(i) When $n = 0$, $A(1,0) = A(0,1) = 2$. If $A(1,k) = k+2$ for a positive integer k. Then,

$$A(1,k+1) = A(0, A(1,k)) = A(0,k+2) = k+2+1 = k+3.$$

(ii) When $n = 0$, $A(2,0) = A(1,1) = 3$. Assume $A(2,k) = 2k+3$ for a positive integer k. Then,

$$A(2,k+1) = A(1, A(2,k)) = A(1, 2k+3) = (2k+3)+2 = 2(k+1)+3.$$

(iii) When $n = 0$, $A(3,0) = A(2,1) = 5$. Assume $A(3,k) = 2^{k+3} - 3$ for $k \in \mathbb{Z}$. Then,

$$A(3,k+1) = A(2, A(2,k)) = A(2, 2^{k+3} - 3) = 2 \cdot \left(2^{k+3} - 3\right) + 3 = 2^{k+4} - 3. \qquad \square$$

In computability theory, the Ackermann function was the earliest-discovered total computable function that is not primitive recursive, meaning it can't be rewritten using for loops. It is often used as a benchmark of a compiler's ability to optimize deep recursion. To compute larger values of the function, we introduce notation first discovered by Donald Knuth in 1976.

Definition. Knuth's up-arrow notation is a method of notation for very large integers.

- Single arrow is exponentiation: $a \uparrow n = a^n$.
- Double arrow is iterated exponentiation, known as tetration:

$$a \uparrow\uparrow n = \underbrace{a \uparrow (a \uparrow (a \uparrow (\cdots a \uparrow a))}_{n\ a's}.$$

  For example, $2 \uparrow\uparrow 4 = 2 \uparrow (2 \uparrow (2 \uparrow (2 \uparrow 2))) = 2^{2^{2^2}} = 65536$.

- Triple arrow is iterated tetration:

$$a \uparrow\uparrow\uparrow n = \underbrace{a \uparrow\uparrow (a \uparrow\uparrow (a \uparrow\uparrow (\cdots a \uparrow\uparrow a)))}_{n\ a's}.$$

- In general, we define the up-arrow notation recursively as

$$a \uparrow^n b = \begin{cases} 1 & \text{if } n \geq 1 \text{ and } b = 0 \\ a \uparrow^{n-1} (a \uparrow^n (b-1)) & \text{otherwise.} \end{cases}$$

For $m = 4$, $A(4, n) = 2 \uparrow\uparrow^{m-n}(n + 3) - 3$. For example, $A(4, 0) = 13$, $A(4, 1) = 65533$, and

$$A(4, 2) = 2^{2^{2^{2}}} - 3 = 2^{65536} - 3.$$

This has 19729 decimal digits! In general, we can prove $A(m, n) = 2 \uparrow^{m-2} (n + 3) - 3$.

Definition. Graham's number is the enormous number g_{64} in the recursive definition

$$g_n = \begin{cases} 3 \uparrow\uparrow\uparrow\uparrow 3, & n = 1 \\ 3 \uparrow^{g_{n-1}} 3, & n \geq 2. \end{cases}$$

Notice the number of arrows in each subsequent layer is the value of the layer proceeding it.

To begin to understand the depth of Graham's number, we show the first several power towers:

$$3 = 3, \quad 3^3 = 27, \quad 3^{3^3} = 7,625,597,484,987.$$

We define the *sun tower* as $3 \uparrow\uparrow\uparrow 3 = 3 \uparrow\uparrow (3 \uparrow\uparrow 3) = 3 \uparrow\uparrow 3^{3^3}$, a power tower with 7.6 trillion 3's. Then, $g_1 = 3 \uparrow\uparrow\uparrow (3 \uparrow\uparrow\uparrow 3)$ is the result of applying the function $x \mapsto 3 \uparrow\uparrow x$ a sun tower amount of times beginning with $x = 1$. Finally, Graham's number is a stacked up-arrow tower:

$$G = \left.\begin{array}{c} 3\underbrace{\uparrow\uparrow \cdots\cdots\cdots\cdots \uparrow} 3 \\ 3\underbrace{\uparrow\uparrow \cdots\cdots\cdots\cdots \uparrow} 3 \\ \vdots \\ 3\underbrace{\uparrow\uparrow \cdots\cdots \uparrow} 3 \\ 3 \uparrow\uparrow\uparrow\uparrow 3 \end{array}\right\} 64 \text{ layers}$$

Exercises

1.4.1. Prove the Principle of Strong Induction from the well-ordering principle

1.4.2. (Fibonacci Nim) Let there be n coins and two players A and B. On the first move, a player is not allowed to take all of the coins, and on each subsequent move, the number of coins removed can be any number that is at most twice the previous move. The winner is the player who removes the final chip(s). Determine the winning strategy for general n.

1.4.3. The McCarthy 91 function is a recursive function defined by

$$M(n) = \begin{cases} n - 10, & \text{if } n > 100 \\ M(M(n + 11)), & \text{if } n \leq 100. \end{cases}$$

Prove that $M(n) = 91$ for all integers $n \leq 100$.

§1.5 Review Problems

1.13. Prove that $\dfrac{1}{1\cdot 2}+\dfrac{1}{2\cdot 3}+\cdots+\dfrac{1}{n(n+1)}=\dfrac{n}{n+1}$ for all positive integers n.

1.14. Prove that $1\cdot 1!+2\cdot 2!+3\cdot 3!+\cdots+n\cdot n!=(n+1)!-1$ for all positive integers n.

1.15. Prove that if n is a positive integer, then $\dfrac{n^5}{5}+\dfrac{n^4}{2}+\dfrac{n^3}{3}-\dfrac{n}{30}$ is always an integer.

1.16. In this problem, we will prove $1^2+2^2+3^2+\cdots+n^2=\dfrac{n(n+1)(2n+1)}{6}$.

(i) Prove that $1+2+3+\cdots+n=\dbinom{n+1}{2}$.

(ii) Prove that $\dbinom{2}{2}+\dbinom{3}{2}+\dbinom{4}{2}+\cdots+\dbinom{n}{2}=\dbinom{n+1}{3}$ for $n\geq 2$.

(iii) From part (i) and (ii), deduce the sum of squares formula.

1.17. Prove that $\dbinom{n}{k}\dbinom{k}{r}=\dbinom{n}{r}\dbinom{n-r}{k-r}$ if $n\geq k\geq r\geq 0$.

1.18. Prove that $\dbinom{n}{1}+2\dbinom{n}{2}+3\dbinom{n}{3}+\cdots+n\dbinom{n}{n}=n2^{n-1}$.

1.19. Define a_n by $a_0=2$, $a_1=8$, and $a_n=8a_{n-1}-15a_{n-2}$ for $n\geq 2$. Prove that $a_n=3^n+5^n$.

1.20. For real x, define $x_n=x^n+\frac{1}{x^n}$. Find x_2, x_3, x_4, and x_5 in terms of x_1.

1.21. Prove that if x_1 is an integer, then x_n is always an integer for all natural n.

1.22. Prove the Lemma used in Example 1.11.

1.23⋆ Prove that $F_{s+t}=F_{s+1}F_t+F_sF_{t-1}$ for integers $s\geq 0$ and $t\geq 1$.

1.24⋆ (Cassini's Identity) Prove that $F_{n+1}F_{n-1}-F_n^2=(-1)^n$.

1.25⋆ (USAMO) We call an integer n *good* if we can write $n=a_1+a_2+\cdots+a_k$, where $a_1, a_2, \cdots, a_k$ are positive integers (not necessarily distinct) satisfying

$$\frac{1}{a_1}+\frac{1}{a_2}+\cdots+\frac{1}{a_k}=1.$$

Given the integers 33 through 73 are good, prove that every integer ≥ 33 is good.

1.26⋆ (Putnam) Prove that every positive integer is a sum of one or more numbers of the form 2^r3^s, where r and s are nonnegative integers and no summand divides another.

APPENDIX A

SOLUTIONS

§A.1 The Art of Proofs Solutions

Exercises for Section 1.2

1.2.1 When $n = 1$, $1 = 1^2$. Assume the identity holds for $n = k$, therefore

$$1 + 3 + 5 + \cdots + (2k - 1) = k^2. \qquad \text{(Hypothesis)}$$

We add the next odd number to both sides of the hypothesis:

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

Therefore, the identity holds for all positive integers n by induction.

1.2.2 When $n = 1$, $1 = 1$. Assume the geometric series holds for $n = k$, therefore

$$1 + r + r^2 + \cdots + r^{k-1} = \frac{r^k - 1}{r - 1}. \qquad \text{(Hypothesis)}$$

We add the next term to both sides of the hypothesis:

$$\begin{aligned}\left[1 + r + r^2 + \cdots + r^{k-1}\right] + r^k &= \left[\frac{r^k - 1}{r - 1}\right] + r^k \\ &= \frac{r^k - 1 + r^{k+1} - r^k}{r - 1} \\ &= \frac{r^{k+1} - 1}{r - 1}.\end{aligned}$$

Therefore, the geometric series formula holds for all positive integers n by induction.

Exercises for Section 1.3

1.3.1 (i) When $x = y = 1$ in the Binomial Theorem, we have

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

(ii) When $x = 1$ and $y = -1$ in the Binomial Theorem, we have

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

(iii) When $x = 1$ and $y = 2$ in the Binomial Theorem, we have

$$(1+2)^n = \sum_{k=0}^{n} \binom{n}{k} 1^{n-k} 2^k = \binom{n}{0} + 2\binom{n}{1} + 2^2\binom{n}{2} + \cdots = 3^n.$$

1.3.2 (i) When $n = 1$, $F_1 = F_2$. Assume the identity holds for $n = k$, therefore

$$F_1 + F_3 + F_5 + \cdots + F_{2k-1} = F_{2k}. \qquad \text{(Hypothesis)}$$

Adding the next odd Fibonacci term to our hypothesis:

$$\begin{aligned}[F_1 + F_3 + F_5 + \cdots + F_{2k-1}] + F_{2k+1} &= [F_{2k}] + F_{2k+1} \\ &= F_{2k+2}.\end{aligned}$$

Therefore, the Fibonacci identity holds for all positive integers n by induction.

(ii) When $n = 1$, $F_1^2 = F_1 F_2$. Assume the identity holds for $n = k$, therefore

$$F_1^2 + F_2^2 + \cdots + F_k^2 = F_k F_{k+1}. \qquad \text{(Hypothsis)}$$

Adding the square of the next Fibonacci number to our hypothesis:

$$\begin{aligned}\left[F_1^2 + F_2^2 + \cdots + F_k^2\right] + F_{k+1}^2 &= [F_k F_{k+1}] + F_{k+1}^2 \\ &= F_{k+1}\left(F_k + F_{k+1}\right) \\ &= F_{k+1} F_{k+2}.\end{aligned}$$

Therefore, the Fibonacci identity holds for all positive integers n by induction.

1.3.3 When $n = 1$, $(x+y)^1 = x + y$. Assuming the Binomial Theorem for $n - 1$:

$$(x+y)^{n-1} = \sum_{k=0}^{n-1} \binom{n-1}{k} x^{n-k-1} y^k. \qquad \text{(Hypothesis)}$$

Multiplying by $x+y$, we see that

$$\begin{aligned}
(x+y)^n &= (x+y)(x+y)^{n-1} \\
&= (x+y)\left[\sum_{k=0}^{n-1}\binom{n-1}{k}x^{n-k-1}y^k\right] \\
&= \sum_{k=0}^{n-1}\binom{n-1}{k}x^{n-k}y^k + \sum_{k=0}^{n-1}\binom{n-1}{k}x^{n-k-1}y^{k+1} \\
&= \sum_{k=0}^{n-1}\binom{n-1}{k}x^{n-k}y^k + \sum_{k'=1}^{n}\binom{n-1}{k'-1}x^{n-k'}y^{k'} && (k'=k+1) \\
&= x^n + \sum_{k=1}^{n-1}\left[\binom{n-1}{k}+\binom{n-1}{k-1}\right]x^{n-k}y^k + y^n \\
&= x^n + \sum_{k=1}^{n-1}\binom{n}{k}x^{n-k}y^k + y^n. && \text{(Pascal's Identity)}
\end{aligned}$$

Therefore, the Binomial Theorem holds for all positive integers n.

Exercises for Section 1.4

1.4.1 Assume that $S = \{n \mid P(n) \text{ is false}\}$ is non-empty. Let the least element of S be m. Observe that $n_0 \notin S$, therefore $m > n_0$. Furthermore, since m is the smallest element of S, $P(n)$ is true for all $n_0 \le n \le m-1$. However, by the inductive step, this implies $P(m)$ is also true, contradiction.

1.4.3 We use strong induction. For a base case, if $90 \le k < 101$, then $k+11 > 100$, so

$$M(k) = M(M(k+11)) = M(k+11-10) = M(k+1).$$

Therefore, $M(90) = M(91) = \cdots = M(100) = M(101) = 101-10 = 91$. We now use induction on blocks of 11 numbers. Assume that $M(k) = 91$ for $a \le k < a+11$. Then, for $a-11 \le k < a$,

$$M(k) = M(M(k+11)) = M(91) = 91.$$

Since we established the base case $a = 90$, $M(k) = 91$ for any k in such a block. Letting a be multiples of 10, there are no holes between the blocks, hence $M(k) = 91$ for all integers $k \le 100$.

Review Problems

1.13 When $n = 1$, $1/2 = 1/2$. We now assume the identity holds for $n = k$, therefore

$$\frac{1}{1\cdot 2} + \frac{1}{2\cdot 3} + \cdots + \frac{1}{k(k+1)} = \frac{k}{k+1}. \qquad \text{(Hypothesis)}$$

We add the next fraction to both sides of our assumption:

$$\begin{aligned}
\left[\frac{1}{1\cdot 2} + \frac{1}{2\cdot 3} + \cdots + \frac{1}{k(k+1)}\right] + \frac{1}{(k+1)(k+2)} &= \frac{k}{k+1} + \frac{1}{(k+1)(k+2)} \\
&= \frac{k^2+2k+1}{(k+1)(k+2)} \\
&= \frac{k+1}{k+2}.
\end{aligned}$$

Therefore, the identity holds for all positive integers by induction. Alternatively,

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

1.14 When $n = 1$, $1 = 2! - 1$. We now assume the identity holds for $n = k$, therefore

$$1 \cdot 1! + 2 \cdot 2! + 3 \cdot 3! + \cdots + k \cdot k! = (k+1)! - 1 \qquad \text{(Hypothesis)}$$

We add the next factorial to both sides of our hypothesis:

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

Therefore, the identity holds for all positive integers by induction.

1.15 When $n = 1$, $1/5 + 1/2 + 1/3 - 1/30 = 1$. Assume that $k^5/5 + k^4/2 + k^3/3 - k/30$ is an integer for an arbitrary k. We expand the expression for $n = k + 1$ using the Binomial Theorem:

$$\frac{k^5 + 5k^4 + 10k^3 + 10k^2 + 5k + 1}{5} + \frac{k^4 + 4k^3 + 6k^2 + 4k + 1}{2} - \frac{k^3 + 3k^2 + 3k + 1}{3} - \frac{k+1}{30}.$$

With some algebraic manipulation, this expression is equivalent to

$$\left(\frac{k^5}{5} + \frac{k^4}{2} + \frac{k^3}{3} - \frac{k}{30}\right) + \left(k^4 + 2k^3 + 2k^2 + k + 2k^3 + 3k^2 + 2k + k^2 + k + 1\right),$$

which is an integer by the induction hypothesis.

1.16 (i) When $n = 1$, $1 = 1$. We now assume the identity holds for $n = k$, therefore

$$1 + 2 + 3 + \cdots + k = \binom{k+1}{2}. \qquad \text{(Hypothesis)}$$

Adding the next integer to both sides of our hypothesis:

$$\begin{aligned}[1 + 2 + 3 + \cdots + k] + k + 1 &= \binom{k+1}{2} + k + 1 \\ &= \binom{k+2}{2}.\end{aligned}$$

The last step follows from either Pascal's identity or simple algebraic manipulation.

(ii) When $n = 2$, $\binom{2}{2} = \binom{3}{3}$. We now assume the identity holds for $n = k$, therefore

$$\binom{2}{2} + \binom{3}{2} + \binom{4}{2} + \cdots + \binom{k}{2} = \binom{k+1}{3}. \qquad \text{(Hypothesis)}$$

Adding the next binomial to both sides of our hypothesis:

$$\begin{aligned}\left[\binom{2}{2} + \binom{3}{2} + \binom{4}{2} + \cdots + \binom{k}{2}\right] + \binom{k+1}{2} &= \binom{k+1}{3} + \binom{k+1}{2} \\ &= \binom{k+2}{3}. \qquad \text{(Pascal's Identity)}\end{aligned}$$

Therefore, the identity holds for all $n \geq 2$ by induction.

(iii) Observe that $k^2 = 2\binom{k}{2} + k$. Therefore,

$$\begin{aligned}\sum_{k=1}^{n} k^2 &= \sum_{k=1}^{n} \left[2\binom{k}{2} + k\right] \\ &= 2\binom{n+1}{3} + \binom{n+1}{2} \\ &= 2\frac{(n+1)n(n-1)}{6} + \frac{(n+1)n}{2} \\ &= \frac{n(n+1)(2n+1)}{6}.\end{aligned}$$

1.17 We see that the left hand side is

$$\binom{n}{k}\binom{k}{r} = \frac{n!}{k!(n-k)!} \cdot \frac{k!}{r!(k-r)!} = \frac{n!}{(n-k)!r!(k-r)!}.$$

Similarly, the right hand side is

$$\binom{n}{r}\binom{n-r}{k-r} = \frac{n!}{r!(n-r)!} \cdot \frac{(n-r)!}{(k-r)!(n-k)!} = \frac{n!}{(n-k)!r!(k-r)!}.$$

Therefore the identity is proven.

1.18 Each term in our sum is equivalent to

$$\begin{aligned}k\binom{n}{k} &= k\left(\frac{n!}{k!(n-k)!}\right) \\ &= \frac{n!}{(k-1)!(n-k)!} = n\binom{n-1}{k-1}.\end{aligned}$$

Therefore, we can rewrite the summation as

$$\begin{aligned}\binom{n}{1} + 2\binom{n}{2} + 3\binom{n}{3} + \cdots + n\binom{n}{n} &= n\left[\binom{n-1}{0} + \binom{n-1}{1} + \cdots + \binom{n-1}{n-1}\right] \\ &= n2^{n-1}.\end{aligned}$$

1.19 We see $a_0 = 3^0 + 5^0 = 2$ and $a_1 = 3^1 + 5^1 = 8$. Assume the formula holds for $n = k-2$ and $n = k-1$. We then show it holds for $n = k$. Note that 3 and 5 are roots of $x^2 - 8x + 15 = 0$, hence

$$3^k = 8 \cdot 3^{k-1} - 15 \cdot 3^{k-2}, \quad 5^k = 8 \cdot 5^{k-1} - 15 \cdot 5^{k-2}.$$

Using these identities along with the inductive hypothesis,

$$\begin{aligned}a_k &= 8a_{k-1} - 15a_{k-2} \\ &= 8\left(3^{k-1} + 5^{k-1}\right) - 15\left(3^{k-2} + 5^{k-2}\right) \\ &= 3^k + 5^k.\end{aligned}$$

1.20 Squaring x_1, we see $x_1^2 = \left(x + \frac{1}{x}\right)^2 = x^2 + 2 + \frac{1}{x^2}$, therefore $x_2 = \boldsymbol{x_1^2 - 2}$. Cubing x_1, we see

$$x_1^3 = \left(x + \frac{1}{x}\right)^3 = x^3 + 3x + \frac{3}{x} + \frac{1}{x^3} \implies x_3 = \boldsymbol{x_1^3 - 3x_1}.$$

Squaring the equation for x_2 gives an expression for x_4:

$$x_2^2 = \left(x^2 + \frac{1}{x^2}\right)^2 = x^4 + 2 + \frac{1}{x^4} \implies x_4 = x_2^2 - 2 = \boldsymbol{x_1^4 - 4x_1^2 + 2}.$$

Finally, to find x_5, we multiply x_1 by x_4 to get a recursive relation,

$$x_1 x_4 = \left(x + \frac{1}{x}\right)\left(x^4 + \frac{1}{x^4}\right) = x^5 + \frac{1}{x^5} + x^3 + \frac{1}{x^3} \implies x_5 = x_1 x_4 - x_3 = \boldsymbol{x_1^5 - 5x_1^3 + 5x_1}.$$

1.21 Since x_1 is an integer, x_2, x_3, x_4, and x_5 are all integers. Inspired by our work for x_5,

$$x_1 a_{k-1} = \left(x + \frac{1}{x}\right)\left(x^{k-1} + \frac{1}{x^{k-1}}\right) = x^k + x^{k-2} + \frac{1}{x^{k-2}} + \frac{1}{x^k}.$$

Assume that x_{k-1} and x_{k-2} are both integers. Then, $x_k = x_1 a_{k-1} - a_{k-2}$ is also an integer. By induction, since we showed several base cases, x_n is an integer for all positive integers n.

1.23 Shifting the indices, we desire to prove $f(s+t) = f(s)f(t) + f(s-1)f(t-1)$. The LHS is the number of tilings of an $(s+t)$-board. We condition on if there is a domino at s in our tiling:

(i) If there is no domino at s, we have $f(s)f(t)$ tilings of the $(s+t)$-board.

(ii) If there is a domino at s, we have $f(s-1)f(t-1)$ tilings of the $(s+t)$-board.

Therefore, we have established that $f(s+t) = f(s)f(t) + f(s-1)f(t-1)$.

1.24 Notice $\varphi\psi = -1$ and $\varphi - \psi = \sqrt{5}$. Using Binet's formula and algebraic manipulation,

$$\begin{aligned} F_{n+1}F_{n-1} - F_n^2 &= \frac{1}{5}\left[\left(\varphi^{n+1} - \psi^{n+1}\right)\left(\varphi^{n-1} - \psi^{n-1}\right) - \left(\varphi^n - \psi^n\right)^2\right] \\ &= \frac{1}{5}\left[-\varphi^{n+1}\psi^{n-1} - \psi^{n+1}\varphi^{n-1} + 2\varphi^n\psi^n\right] \\ &= -\frac{1}{5}(\varphi\psi)^{n-1}\left(\varphi^2 - 2\varphi\psi + \psi^2\right) \\ &= -\frac{1}{5}(-1)^{n-1}(\varphi - \psi)^2 \\ &= (-1)^n. \end{aligned}$$

1.25 We use induction. Observe that if n is good, then

$$\frac{1}{2a_1} + \cdots + \frac{1}{2a_k} + \frac{1}{4} + \frac{1}{4} = \frac{1}{2} + \frac{1}{4} + \frac{1}{4} = 1 \implies 2n+8 \text{ is good.}$$
$$\frac{1}{2a_1} + \cdots + \frac{1}{2a_k} + \frac{1}{3} + \frac{1}{6} = \frac{1}{2} + \frac{1}{3} + \frac{1}{6} = 1 \implies 2n+9 \text{ is good.}$$

Let $P(n)$ be the proposition "all the integers $n, n+1, n+2, \cdots, 2n+7$ are good". The base case $P(33)$ is given. If k is good, then $2k+8$ and $2k+9$ are also good, hence $P(k) \implies P(k+1)$.

1.26 We use strong induction. For a base case, 1 is obvious. Assume every integer up to n can be written in this form. We then show that n can also be by breaking it into two cases:

- If n is even, then $n/2$ can be written as a sum by hypothesis. Multiplying every term in this sum by 2 gives the desired representation for n. For example, $5 = 2 + 3$ and $10 = 4 + 6$.
- If n is odd, then find s such that $3^s \leq n < 3^{s+1}$. Clearly if $3^s = n$, then we are done. If $3^s < n$, then let $n' = (n - 3^s)/2$. Since n' is an integer, it can be written as a sum. Notice the powers of 3 in the representation of n' are less than 3^s since

$$n' = \frac{n - 3^s}{2} < \frac{3^{s+1} - 3^s}{2} = 3^s.$$

  Multiplying the representation of n' by 2 gives one for $2n'$. We know none of the terms of this sum are divisible by 3^s. Also since they are all even, none divide 3^s. Putting together the representations for $2n'$ with 3^s gives a valid representation for n.

BIBLIOGRAPHY

[1] A. J. Cole and A. J. T. Davie. A game based on the euclidean algorithm and a winning strategy for it. *The Mathematical Gazette*, 53(386):354–357, 1969.

[2] Matthew Crawford. *Introduction to Number Theory*. Art of Problem Solving, 2nd edition.

[3] Titu Andreescu and Dorin Andrica. *Number Theory: Structures, Examples, and Problems*. Birkhäuser.

[4] Thomas Koshy. *Elementary Number Theory with Applications*. Academic Press, 1st edition.

[5] David Burton. *Elementary Number Theory*. McGraw-Hill Education, 6th edition.

[6] Ivan Niven, Herbert S. Zuckerman, and Hugh L. Montgomery. *An Introduction to the Theory of Numbers*. John Wiley & Sons, 5th edition.

[7] David A. Santos. *Number Theory for Mathematical Contests*. 2005.

[8] G. H. Hardy and E. M. Wright. *An Introduction to the Theory of Numbers*. Oxford Mathematics, 6th edition.

[9] Arthur Benjamin and Jennifer Quinn. *Proofs that Really Count*. The Mathematical Association of America.

[10] Chris Caldwell. The prime pages. https://primes.utm.edu/.