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: $(a + b)/a = a/b \overset{\text{def}}{=} \varphi$. 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 $n=k$:

$$1+2+2^2+2^3+\cdots+2^k = 2^{k+1}-1. \tag{Hypothesis}$$

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

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

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

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 $F_{\text{max}} \leq K+1$. If $F_{\text{max}} = K+1$, then we are clearly done. Otherwise, $F_{\text{max}} < K+1 < F_{\text{max}+1}$, therefore

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

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

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

Since $F_{a_m} < F_{\text{max}-1}$ 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,

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

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

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

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:

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

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 $\frac{1}{1\cdot 2}+\frac{1}{2\cdot 3}+\cdots+\frac{1}{n(n+1)}=\frac{n}{n+1}$ 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 $\frac{n^5}{5}+\frac{n^4}{2}+\frac{n^3}{3}-\frac{n}{30}$ is always an integer.

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

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

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

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

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

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

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

1.25$\star$ (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$\star$ (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.

CHAPTER 2

DIVISIBILITY THEORY

§2.1 Basic Theorems

Definition. For integers n and $d \neq 0$, d divides n, written $d \mid n$, if and only if there exists an integer q such that $n = dq$. This is equivalent to saying n is a multiple of d.

For every integer n, the definition directly implies $1 \mid n$, $n \mid 0$, and $n \mid n$.

Theorem 2.1. Properties of divisibility over the integers include:

(1) **Transitive:** $d \mid m$ and $m \mid n$ implies $d \mid n$.

(2) **Linear Combinations:** $d \mid n_1$ and $d \mid n_2$ implies $d \mid n_1\alpha_1 + n_2\alpha_2$ for integers α_1, α_2.

(3) **Cancellation:** $dc \mid nc$ implies $d \mid n$.

(4) **Anti-symmetry:** $d \mid n$ and $n \mid d$ implies $|n| = |d|$.

Proof. We prove (1) and (2), leaving (3) and (4) as exercises.

(1) Since $d \mid m$, there exists $q \in \mathbb{Z}$ with $m = qd$. Similarly, $n = q'm$ for $q' \in \mathbb{Z}$. Hence,

$$n = q'm = q'(qd) = d(q'q) \implies d \mid n.$$

(2) Since $d \mid n_1$, there exists $q_1 \in \mathbb{Z}$ with $n_1 = q_1 d$. Similarly, $n_2 = q_2 d$ for $q_2 \in \mathbb{Z}$. Hence,

$$\begin{aligned} n_1\alpha_1 + n_2\alpha_2 &= (q_1 d)\,\alpha_1 + (q_2 d)\,\alpha_2 \\ &= d\,(q_1\alpha_1 + q_2\alpha_2)\,. \end{aligned}$$

Hence, $d \mid n_1\alpha_1 + n_2\alpha_2$. These numbers are called linear combinations of n_1 and n_2. □

Example 2.1 (AIME)**.** Find the sum of all positive two-digit integers that are divisible by each of their digits.

Solution. Let the number be $N = 10a+b$. The first condition gives $a \mid b$ while the second condition gives $b \mid 10a$, therefore $b = a$, $b = 2a$, or $b = 5a$. Therefore, $N = 11a$, $N = 12a$, or $N = 15a$.

- If $N = 11a$, then we have a sum of $11\left(\frac{9\cdot 10}{2}\right) = 11 \cdot 45 = 495$.
- If $N = 12a$, then $N = 12, 24, 36, 48$ for a sum of 120.
- If $N = 15a$, then $N = 15$ for a sum of 15.

Hence, the total is $495 + 120 + 15 = \boxed{630}$. □

Example 2.2. Prove that if $d \mid n$ and $(d+1) \mid n$, then $(d^2 + d) \mid n$.

Solution. From the given conditions, there exists integers r and s such that

$$n = dr = (d+1)\,s.$$

Taking the reciprocal of these equations and subtracting gives

$$\frac{1}{d} - \frac{1}{d+1} = \frac{r}{n} - \frac{s}{n} \implies \frac{1}{d(d+1)} = \frac{r-s}{n}.$$

Therefore, we conclude that $(d^2 + d) \mid n$. □

Example 2.3. Prove that if $d \mid n$, then $F_d \mid F_n$.

Proof. Note $F_d \mid F_{d\cdot 1}$. Let $s = qd$ and $t = d$ in the identity $F_{s+t} = F_{s+1}F_t + F_sF_{t-1}$:

$$F_{qd+d} = F_{qd+1}F_d + F_{qd}F_{d-1}.$$

If F_d divides F_{qd}, it also divides their linear combination, $F_{(q+1)d}$. The result follows by induction. □

Example 2.4. Prove that that the product of n consecutive integers is divisible by $n!$.

Solution. For positive m, we consider the Binomial coefficient

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

Since the left-hand side is an integer, $n!$ divides the product of n consecutive positive integers. If any of the consecutive integers is 0, then the product is 0, and we are done. Otherwise, if the n consecutive integers are all negative, we multiply by $(-1)^n$ to reduce to the positive case. □

Exercises

2.1.1. Find all three-digit odd numbers that are divisible by each of their distinct digits.

2.1.2. Prove the cancellation and anti-symmetry properties of divisibility.

2.1.3. Prove that $n^5 - 5n^3 + 4n$ is always divisible by 120 for all integers n.

2.1.4. Prove that if d divides every integer in the sequence $n_1, n_2, \cdots, n_k$, then

$$d \mid n_1\alpha_1 + n_2\alpha_2 + \cdots + n_k\alpha_k, \quad \alpha_j \in \mathbb{Z}.$$

§2.2 Primes and Algebraic Identities

Definition. A prime is a number $p > 1$ whose only positive divisors are 1 and itself.

Definition. A composite number n can be written as $n = ab$ for $a > 1$ and $b > 1$.

Since divisors of composites come in pairs, if $d \nmid n$ for $2 \le d \le \lfloor \sqrt{n} \rfloor$, then n is prime.

Sieve (Eratosthenes). Write the numbers 1 to N in a grid. For all primes $p \le \sqrt{N}$, cross out the multiples $2p, 3p, 4p, \cdots$. The numbers that remain are the primes less than N.

Example 2.5. Find all primes less than or equal to 100.

Solution. We show the completed grid using the Sieve of Eratosthenes:

	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	49	~~50~~
~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	77	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~
91	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~

Example 2.6 (PUMaC). If p, q, and r are primes such that $pqr = 7(p+q+r)$, find $p+q+r$.

Solution. We see that at least one of the primes must be 7, say p. Simplifying using SFFT,

$$qr = q + r + 7 \implies (q-1)(r-1) = 8.$$

Therefore, $(q, r) = (5, 3)$ or $(q, r) = (3, 5)$. Hence, $p + q + r = 3 + 5 + 7 = \boxed{15}$. □

Example 2.7. Find all primes p such that $16p + 1$ is a perfect cube.

Solution. Let $16p + 1 = n^3$ for some integer n. Using difference of cubes,

$$16p = n^3 - 1 = (n-1)\left(n^2 + n + 1\right).$$

Since $n^2 + n + 1$ is odd, we must have $16 \mid n - 1$, therefore $n - 1 = 16k$ for some integer k:

$$p = k\left(n^2 + n + 1\right).$$

Since $n^2 + n + 1 > 1$, we must have $k = 1$, so $n = 17$. We then find $p = 17^2 + 17 + 1 = \boxed{307}$. □

Example 2.8. Find all integers a and b such that $a^4 + 4b^4$ is prime.

Solution. Complete the square by adding $4a^2b^2$ to both sides: $\left(a^2 + 2b^2\right)^2 = a^4 + 4a^2b^2 + 4b^4$. Rearranging this equation and using difference of squares:

$$\begin{aligned} a^4 + 4b^4 &= \left(a^2 + 2b^2\right)^2 - (2ab)^2 \\ &= \left(a^2 - 2ab + 2b^2\right)\left(a^2 + 2ab + 2b^2\right) \\ &= \left[(a-b)^2 + b^2\right]\left[(a+b)^2 + b^2\right]. \end{aligned}$$

If $a^4 + 4b^2$ is prime, then one factor must be 1 and the other a prime, so $|a| = |b| = 1$. □

The factorization used in the above problem is known as the **Sophie Germain Identity**.

Example 2.9 (MPfG). Find the unique five-digit prime divisor of 104060465.

Solution. We see $101^4 = 104060401$. Therefore, using the Sophie-Germain identity,

$$\begin{aligned} 104060465 &= 101^4 + 64 = 101^4 + 4 \cdot 2^4 \\ &= \left(101^2 - 2 \cdot 101 \cdot 2 + 2 \cdot 2^2\right)\left(101^2 + 2 \cdot 101 \cdot 2 + 2 \cdot 2^2\right) \\ &= 9805 \cdot 10613. \end{aligned}$$

The answer is hence $\boxed{10613}$. □

Example 2.10. (a) Prove $x^n - y^n = (x-y)\left(x^{n-1} + x^{n-2}y + \cdots + y^{n-1}\right)$ for natural n.

(b) Prove $x^n + y^n = (x+y)\left(x^{n-1} - x^{n-2}y + \cdots + y^{n-1}\right)$ for odd n.

Proof. (a) We use the geometric series formula $\displaystyle\sum_{k=0}^{n-1} r^k = \frac{r^n - 1}{r - 1}$ with $r = \dfrac{x}{y}$:

$$1 + \frac{x}{y} + \cdots + \frac{x^{n-2}}{y^{n-2}} + \frac{x^{n-1}}{y^{n-1}} = \frac{x^n/y^n - 1}{x/y - 1}$$

Multipying both sides by y^{n-1}:

$$y^{n-1} + xy^{n-2} + \cdots + x^{n-2}y + x^{n-1} = \frac{x^n - y^n}{x - y}.$$

Multiplying by $x - y$ gives the difference of nth power factorization.

(b) Substitute $-y$ for y in the above factorization when n is odd. □

For $n = 3$, this is the familiar sum and difference of cubes factorization.

Example 2.11 (UMich). Find a prime factor $p > 250000$ of 1002004008016032.

Solution. If $x = 1000$ and $y = 2$, then the given number is $N = x^5 + x^4y + x^3y^2 + x^2y^3 + xy^4 + y^5$. Using the factorization for $n = 6$ along with sum and difference of cubes,

$$\begin{aligned} N &= \frac{1000^6 - 2^6}{1000 - 2} \\ &= 2^5 \cdot \frac{\left(500^3 - 1\right)\left(500^3 + 1\right)}{500 - 1} \\ &= 2^5 \cdot \frac{(500 - 1)\left(500^2 + 500 + 1\right)(500 + 1)\left(500^2 - 500 + 1\right)}{500 - 1}. \end{aligned}$$

The only prime factor of this number that satisfies $p > 250000$ is $500^2 + 500 + 1 = \boxed{250501}$. □

Example 2.12. Prove that if $2^n - 1$ is prime for $n \geq 2$, then n must be prime.

Proof by Contradiction. If n is composite, let $n = cd$ for $c > 1$ and $d > 1$, so

$$\begin{aligned} 2^{cd} - 1 &= \left(2^c - 1\right)\left(2^{c(d-1)} + \cdots + 2^{2c} + 2^c + 1\right) \\ &= \left(2^d - 1\right)\left(2^{d(c-1)} + \cdots + 2^{2d} + 2^d + 1\right). \end{aligned}$$

However, then $2^n - 1$ is also composite, contradiction. Thus, n must be prime. □

Definition. Primes of the form $M_p = 2^p - 1$ are called **Mersenne primes**.

There are currently 49 known Mersenne primes. As of this writing, the largest known prime is a Mersenne prime, $2^{74,207,281} - 1$. This number has an astonishing $22,338,618$ digits!

Example 2.13. Find a factor of $2^{33} - 2^{19} - 2^{17} - 1$ that lies between 1000 and 5000.

Solution. Observe that for $a = 2^{11}, b = -2^6$, and $c = -1$,

$$2^{33} - 2^{19} - 2^{17} - 1 = 2^{33} - 2^{18} - 1 - 3 \cdot 2^{17} = a^3 + b^3 + c^3 - 3abc.$$

Since $a^3 + b^3 + c^3 - 3abc = (a + b + c)\left(a^2 + b^2 + c^2 - ab - bc - ca\right)$, the desired divisor is

$$a + b + c = 2^{11} - 2^6 - 1 = 2048 - 64 - 1 = \boxed{1983}.$$

□

Exercises

2.2.1. (Mandelbrot) Jayne writes the integers from 1 to 2000 on a piece of paper. She erases all the multiples of 3, then all the multiples of 5, and so on, erasing all the multiples of each odd prime. How many numbers are left when she finishes?

2.2.2. (ARML) Find all primes p such that $p^{1994} + p^{1995}$ is a perfect square.

2.2.3. (ARML) Find the largest divisor of 1001001001 less than 10000.

2.2.4. Prove that if $d \mid n$, then for positive integers x and y, $x^d - y^d \mid x^n - y^n$.

§2.3 Division Algorithm

Algorithm 2.2 (Division Algorithm). For $n \in \mathbb{Z}$ and $d \in \mathbb{Z}^+$, there exists q and r such that

$$n = dq + r, \quad 0 \le r < d$$

Proof. For proving the existence of the quotient and remainder, consider the progression:

$$\{\cdots, n-3d, n-2d, n-d, n, n+d, n+2d, n+3d, \cdots\}.$$

Let the smallest non-negative member of this arithmetic progression be $r_{\min} = n - dq$. Assume for the sake of contradiction that $r_{\min} \ge d$. Then, we simply subtract d from the value of r to produce $r' = n - d(q+1) \ge 0$. Since $r' < r_{\min}$, we have found a smaller non-negative member of the progression than r, contradiction. Therefore, $0 \le r_{\min} < d$.

The second part of this proof is to show that the quotient and remainder are unique. Assume for the sake of contradiction that n can be represented in two ways:

$$n = dq_1 + r_1 = dq_2 + r_2 \implies d(q_1 - q_2) = r_2 - r_1.$$

This implies that $r_2 - r_1$ is a multiple of d. However, $-d < r_2 - r_1 < d$ since $0 \le r_1, r_2 < d$. Therefore, if $r_2 - r_1$ is a multiple of d, we must have $r_2 - r_1 = 0 \implies r_2 = r_1$ and $q_2 = q_1$. □

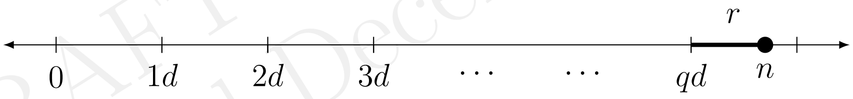

Figure 2.1: If $d \nmid n$, then n will always lie between two ticks on the number line.

Example 2.14 (AHSME). Let r be the remainder when each of the numbers $1059, 1417$, and 2312 are divided by an integer $d > 1$. Find d and r.

Solution. By the division algorithm, there exists three integer quotients q_1, q_2, and q_3 with

$$1059 = dq_1 + r, \quad 1417 = dq_2 + r, \quad 2312 = dq_3 + r.$$

We subtract the equations in pairs:

$$358 = d(q_2 - q_1),\ 895 = d(q_3 - q_2),\ 1253 = d(q_3 - q_1).$$

Hence, d must divide $358 = 2 \cdot 179,\ 895 = 5 \cdot 179$, and $1253 = 7 \cdot 179$, so $d = \boxed{179}$. Dividing 1059 by 179 shows $1059 = 179 \cdot 5 + 164$, therefore the remainder is $r = \boxed{164}$. □

Another application of the division algorithm is different forms of numbers. For integer k, define A to be the set of numbers of the form $3k$, B to be $3k+1$, and C to be $3k+2$. Notice that these sets make up the entirety of the integers, therefore $A \cup B \cup C = \mathbb{Z}$.

Example 2.15. Prove that every perfect square is of the form $3k$ or $3k+1$.

Solution. We break this into three cases based on the remainder when we divide n by 3. If $n = 3m$, then $n^2 = (3m)^2 = 9m^2 = 3(3m^2)$, which is of the form $3k$. Otherwise,

$$n^2 = (3m+1)^2 = 9m^2 + 6m + 1 = 3\left(3m^2 + 2m\right) + 1$$
$$n^2 = (3m+2)^2 = 9m^2 + 12m + 4 = 3\left(3m^2 + 4m + 1\right) + 1.$$

In both cases, we conclude that n^2 is of the form $3k+1$. □

Example 2.16. Prove that $n^9 - 6n^7 + 9n^5 - 4n^3$ is divisible by 8640 for all integers $n \geq 1$.

Proof. We begin by factorizing the polynomial:

$$\begin{aligned} n^9 - 6n^7 + 9n^5 - 4n^3 &= n^3\left(n^6 - 6n^4 + 9n^2 - 4\right) \\ &= n^3\left(n^2 - 1\right)\left(n^4 - 5n^2 + 4\right) \\ &= n^3\left(n^2 - 1\right)\left(n^2 - 1\right)\left(n^2 - 4\right) \\ &= (n-2)(n-1)^2 n^3 (n+1)^2 (n+2). \end{aligned}$$

Since $8640 = 2^6 \cdot 3^3 \cdot 5^1$, we break the problem into the prime divisors:

- 5^1: We have 5 consecutive integers in the product, so the product is divisible by 5.
- 3^3: If $n = 3k$, then n^3 has three factors of 3. If $n = 3k+1$, then $(n-1)^2(n+2)$ has three factors of 3. Finally, if $n = 3k+2$, then $(n-2)(n+1)^2$ has three factors of 3.
- 2^6: If $n = 4k$, then $(n-2)n^3(n+2)$ has eight factors of 3. If $n = 4k+2$, then it has seven factors of 3. If $n = 4k+1$ or $n = 4k+3$, then $(n-1)^2(n+1)^2$ has six factors of 3.

For every prime, we've proven the polynomial has enough factors to be divisible by 8640. □

Example 2.17 (TAG$_5$)**.** Let there be n coins and two players A and B, with A making the first move. Each player may in turn take-away either $1, 2, 3, 4$, or 5 coins from the pile. The winner is the player who removes the final coin(s). Determine the winning strategy for general n.

Solution. If $6 \mid n$ and player A takes s coins, player B takes $6 - s$ coins to reduce the pile by 6. Player B can repeat this strategy until there are $1 \leq r \leq 5$ coins remaining to win. Else if $6 \nmid n$, player A can take r coins to leave $n' = n - r$ coins where $6 \mid n'$ to win using the strategy above. □

Exercises

2.3.1. Find the greatest three digit integer that leaves a remainder of 7 upon division by 13.

2.3.2. (AHSME) Let S be a subset of $\{1, 2, 3, ..., 50\}$ such that no pair of distinct elements in S has a sum divisible by 7. What is the maximum number of elements in S?

2.3.3. Euclid divides 2017 by every positive integer up to 1000 using the division algorithm and records the remainder. What is the largest remainder Euclid writes down?

2.3.4. Prove the product of two numbers of the form $4k+3$ is of the form $4k+1$.

§2.4 Modular Arithmetic

Concept (Modular Arithmetic). We define the quotient group $\mathbb{Z}_m$ by:

- The mod m residues are the remainders upon division by m, $0, 1, 2, \cdots, m-1$.
- Integers a and b are said to be congruent mod m if they have the same residue:

$$a = q_1 m + r$$
$$b = q_2 m + r,$$

  where q_1, q_2, and r are integers with $0 \le r < m$.

- This is written as $a \equiv b \pmod{m}$ and is equivalent to $m \mid a - b$.

We see that if $a \equiv b \pmod{m}$, then $a - b = mq$ for some integer q, implying $a = b + mq$.

Theorem 2.3. If $a_1 \equiv a_2 \pmod{m}$ and $b_1 \equiv b_2 \pmod{m}$, then

$$a_1 + b_1 \equiv a_2 + b_2 \pmod{m}, \quad a_1 b_1 \equiv a_2 b_2 \pmod{m}.$$

Proof. By definition, there exists integers q_a and q_b such that $a_1 = a_2 + mq_a$ and $b_1 = b_2 + mq_b$. Adding these equations gives

$$a_1 + b_1 = a_2 + mq_a + b_2 + mq_b \equiv a_2 + b_2 \pmod{m}.$$

Multiplying these equations gives

$$a_1 b_1 \equiv (a_2 + mq_a)(b_2 + mq_b) = a_2 b_2 + mq_a b_2 + mq_b a_2 + m^2 q_a q_b \equiv a_2 b_2 \pmod{m}.$$ □

Example 2.18. Compute the units digit of $1! + 2! + 3! + 4! + 5! + \cdots + 100!$.

Solution. Since $5! = 120 \equiv 0 \pmod{10}$, every term after that cancels, so the units digit is

$$1! + 2! + 3! + 4! + 5! \cdots + 100! \equiv 1 + 2 + 6 + 4 + 0 + \cdots + 0 \equiv \mathbf{3} \pmod{10}.$$ □

Example 2.19 (AIME). Find the remainder when $9 \times 99 \times \cdots \times \underbrace{99\cdots9}_{\text{999 9's}}$ is divided by 1000.

Solution. After the second term, every number is -1 mod 1000, so the product is

$$9 \times 99 \times 999 \cdots \times \underbrace{99\cdots9}_{\text{999 9's}} \equiv 9 \cdot 99 \cdot (-1)^{997} \equiv -891 \equiv \mathbf{109} \pmod{1000}.$$ □

Theorem 2.4 (Modulo Exponentiation). If $a_1 \equiv a_2 \pmod{m}$, then $a_1^n \equiv a_2^n \pmod{m}$.

We can prove this by repeatedly multiplying together the congruence $a_1 \equiv a_2 \pmod{m}$.

Example 2.20. Compute the remainder when 6^{203} is divided by 37.

Solution. Observe that $6^2 \equiv 36 \equiv -1 \pmod{37}$. Therefore,

$$6^{203} \equiv \left(6^2\right)^{101} \cdot 6^1 \equiv (-1)^{101} \cdot 6^1 \equiv \boxed{31} \pmod{37}.$$ □

Example 2.21. Compute the units digit of $3^{7^{11}}$.

Solution. Observe the following relations for nonnegative integer n:

$$\begin{aligned}
n \equiv 0 \pmod{4} &\implies 3^n \equiv 1 \pmod{10}\\
n \equiv 1 \pmod{4} &\implies 3^n \equiv 3 \pmod{10}\\
n \equiv 2 \pmod{4} &\implies 3^n \equiv 9 \pmod{10}\\
n \equiv 3 \pmod{4} &\implies 3^n \equiv 7 \pmod{10}.
\end{aligned}$$

We therefore wish to find the remainder when 7^{11} is divided by 4:

$$7^{11} \equiv (-1)^{11} \equiv -1 \equiv 3 \pmod{4} \implies 3^{7^{11}} \equiv 3^3 \equiv \mathbf{7} \pmod{10}.$$ □

Example 2.22 (ARML). Find a divisor between 2000 and 3000 of $85^9 - 21^9 + 6^9$.

Solution. Let $N = 85^9 - 21^9 + 6^9$. Since $85 \equiv 21 \pmod{64}$, we see that $85^9 \equiv 21^9 \pmod{64}$. Furthermore, 6^9 is divisible by 64, so N is divisible by 64. Similarly $21 \equiv 6 \pmod{5}$, so

$$N \equiv 0 - 6^9 + 6^9 \equiv 0 \pmod{5}.$$

Finally, since $85 \equiv 1 \pmod{7}$ and $6 \equiv -1 \pmod{7}$, we see that

$$N \equiv 1^9 - 0 + (-1)^9 \equiv 0 \pmod{7}.$$

Therefore, the desired divisor between 2000 and 3000 is $2^6 \cdot 5^1 \cdot 7^1 = \mathbf{2240}$. □

Example 2.23 (AMC 10). Compute the last three digits of 2011^{2011}.

Solution. Since $2011 \equiv 11 \pmod{1000}$, we work mod 1000 and use the Binomial Theorem:

$$\begin{aligned}
2011^{2011} &\equiv (10+1)^{2011}\\
&\equiv 10^{2011} + \cdots + \binom{2011}{2}10^2 + \binom{2011}{1}10^1 + \binom{2011}{0}\\
&\equiv \frac{2011 \cdot 2010}{2}10^2 + 2011 \cdot 10^1 + 1\\
&\equiv 11 \cdot 5 \cdot 100 + 110 + 1\\
&\equiv \boxed{661} \pmod{1000}.
\end{aligned}$$ □

Example 2.24. Find the largest factor of 2 in the prime factorization of $\lfloor \frac{14^{30}}{7^{15}-1} \rfloor$.

Solution. We begin by computing $14^{30} \pmod{7^{15}-1}$. Since $7^{15} \equiv 1 \pmod{7^{15}-1}$, we have

$$14^{30} = 2^{30}7^{30} = 2^{30}\left(7^{15}\right)^2 \equiv 2^{30} \pmod{7^{15}-1}.$$

Furthermore, $2^{30} = 4^{15} < 7^{15} - 1$, therefore the greatest integer function is

$$\lfloor \frac{14^{30}}{7^{15}-1} \rfloor = \frac{14^{30} - 2^{30}}{7^{15}-1}.$$

We can now factor and use difference of squares:

$$\frac{14^{30} - 2^{30}}{7^{15}-1} = \frac{2^{30}\left(7^{30}-1\right)}{7^{15}-1} = 2^{30}\left(7^{15}+1\right).$$

Notice $7^{15} + 1 \equiv (-1)^{15} + 1 \equiv 0 \pmod 8$. However, since $7^2 = 49 \equiv 1 \pmod{16}$,

$$7^{15} + 1 \equiv \left(7^2\right)^7 7^1 + 1 \equiv 8 \pmod{16}.$$

Hence, there are 3 factors of 2 in $7^{15} + 1$. Therefore, the answer is $30 + 3 = \boxed{33}$. □

Example 2.25. A repunit is a number consisting only of the digit 1, such as 111 and 11111. Let n be a number relatively prime to 10. Prove that there is a repunit divisible by n.

Proof by Contradiction. Let a repunit with j digits be denoted a_j. Assume that there are no repunits divisible by n, hence there are $n-1$ possible remainders when we divide a_j by n. Considering an infinite number of repunits by the pigeonhole principle, two must have the same remainder upon division by n, say a_i and a_j for $j > i$. However, then

$$a_j - a_i = \underbrace{111\cdots111}_{j\text{ 1's}} - \underbrace{11\cdots11}_{i\text{ 1's}} = 10^i \cdot \underbrace{11\cdots11}_{j-i\text{ 1's}} = 10^i a_{j-i}.$$

Since a_j and a_i have the same remainder, n divides their difference. Furthermore, n is relatively prime to 10, so $n \mid a_{j-i}$, contradiction. Therefore, we can always find a repunit divisible by n. □

Exercises

2.4.1. Prove that if $a_1 \equiv a_2 \pmod m$ and $d \mid m$, then $a_1 \equiv a_2 \pmod d$.

2.4.2. (a) Find the remainder when 5^{1337} is divided by 31.

(b) Find the remainder when 2^{2001} is divided by $2^7 - 1$. (*Source: HMMT*)

2.4.3. Prove that for all natural numbers n, $2^{4n} + 10n - 1$ is divisible by 25.

2.4.4. Prove that if $a \equiv b \pmod n$, then $a^n \equiv b^n \pmod{n^2}$.

§2.5 Base Numbers

Definition. When writing numbers using the first b whole numbers (i.e. $0, 1, 2, \cdots, b-1$), we are using base b. We can think of base conversions as different ways of grouping numbers.

In general, we write a number n in base b as

$$n = (d_k d_{k-1} \cdots d_2 d_1 d_0)_b = d_k b^k + d_{k-1} b^{k-1} + \cdots + d_2 b^2 + d_1 b + d_0, \quad 0 \le d_i < b.$$

For example, to convert 2017 to base 8, we repeatedly divide using the division algorithm:

$$2017 = 8 \cdot 252 + \mathbf{1}, \quad 252 = 8 \cdot 31 + \mathbf{4}, \quad 31 = 8 \cdot 3 + \mathbf{7}, \quad 3 = 8 \cdot 0 + \mathbf{3}.$$

Therefore, $2017 = 8 \cdot 252 + 1 = 8\,(8 \cdot 31 + 4) + 1 = 8\,(8\,(8 \cdot 3 + 7) + 4) + 1 = 3741_8$.

Algorithm 2.5 (Base Conversion). To express a decimal number n in base b, we repeatedly divide n by b using the division algorithm, stopping when the quotient is 0:

$$\begin{aligned} n &= b \cdot q_0 + r_0 \\ q_0 &= b \cdot q_1 + r_1 \\ q_1 &= b \cdot q_2 + r_2 \\ &\cdots \\ q_{k-2} &= b \cdot q_{k-1} + r_{k-1} \\ q_{k-1} &= b \cdot 0 + r_k. \end{aligned}$$

Then n is the result of appending the remainders in reverse order, $(r_k r_{k-1} r_{k-2} \cdots r_2 r_1 r_0)_b$.

Another algorithm employs a greedy startegy by continually subtracting the largest power of b that goes into n. For bases that are greater than 10, we use letters to represent digits. For example, in base 16, we use A, B, C, D, E, F to represent values ten to fifteen.

Example 2.26. Convert 11110011_2 to base 16 and 25681_9 to base 3.

Solution. For the first part, we group the bits in fours to see

$$11110011_2 = \left(2^7 + 2^6 + 2^5 + 2^4\right) + \left(2^1 + 2^0\right) = 15 \cdot 2^4 + 3 = \boxed{F3_{16}}.$$

For the second part, since $9 = 3^2$,

$$\begin{aligned} 25681_9 &= 2 \cdot 9^4 + 5 \cdot 9^3 + 6 \cdot 9^2 + 8 \cdot 9^1 + 1 \cdot 9^0 \\ &= 2 \cdot 3^8 + 5 \cdot 3^6 + 6 \cdot 3^4 + 8 \cdot 3^2 + 1 \cdot 3^0. \end{aligned}$$

Converting $5, 6$, and 8 to base 3 gives:

$$\begin{aligned} &= \mathbf{2} \cdot 3^8 + (3 + 2) \cdot 3^6 + (3 \cdot 2) \cdot 3^4 + (3 \cdot 2 + 2) \cdot 3^2 + \mathbf{1} \cdot 3^0 \\ &= \mathbf{2} \cdot 3^8 + \mathbf{1} \cdot 3^7 + \mathbf{2} \cdot 3^6 + \mathbf{2} \cdot 3^5 + \mathbf{2} \cdot 3^3 + \mathbf{2} \cdot 3^2 + \mathbf{1} \cdot 3^0 \\ &= \boxed{212202201_3}. \end{aligned}$$

We could also directly convert each digit to base 3: $2 = 2_3, 5 = 12_3$, $6 = 20_3$, $8 = 22_3$, $1 = 01_3$. □

Example 2.27. Convert 100_{b+1}, 1000_{b+1}, and 10000_{b+1} to base b.

Solution. Using the Binomial Theorem,

$$\begin{aligned} 100_{b+1} &= (b+1)^2 = b^2 + 2b + 1 = \mathbf{121_b} \\ 1000_{b+1} &= (b+1)^3 = b^3 + 3b^2 + 3b + 1 = \mathbf{1331_b} \\ 10000_{b+1} &= (b+1)^4 = b^4 + 4b^3 + 6b^2 + 4b^2 + 1 = \mathbf{14641_b}. \end{aligned}$$ □

Example 2.28 (AIME)**.** Call N a *7-10-double* if the digits of the base-7 representation of N form a base-10 number that is twice N. For example, $51 = 102_7$. What is the largest *7-10-double*?

Solution. Let the base 7 representation of the *7-10-double* be $N = (a_k a_{k-1} \cdots a_2 a_1 a_0)_7$. Hence,

$$(a_k a_{k-1} \cdots a_2 a_1 a_0)_{10} = 2\,(a_k a_{k-1} \cdots a_2 a_1 a_0)_7\,.$$

Observe that for $k \geq 3$, we have $10^k \gg 2 \cdot 7^k$, so we try $k = 2$:

$$100a_2 + 10a_1 + a_0 = 98a_2 + 14a_1 + 2a_0 \implies 2a_2 = 4a_1 + a_0.$$

To maximize N, we let $a_2 = 6$, giving $a_1 = 3$ and $a_0 = 0$. Therefore, $N = 630_7 = \mathbf{315}$. □

Example 2.29 (ARML)**.** Let $N_b = 1_b + 2_b + \cdots + 100_b$ for an integer $b > 2$. Compute the number of values of b for which the sum of the squares of the digits of N_b is at most 512.

Solution. We convert every term in the sum for N_b to decimal:

$$N_b = 1 + 2 + \cdots + b^2 = \frac{b^2(b^2+1)}{2} = \frac{b^4}{2} + \frac{b^2}{2}.$$

If b is even, $N_b = \frac{b}{2}b^3 + \frac{b}{2}b = \left(\frac{b}{2}0\frac{b}{2}0\right)_b$. Since the sum of the squares of the digits is at most 512,

$$\left(\frac{b}{2}\right)^2 + \left(\frac{b}{2}\right)^2 = \frac{b^2}{2} \leq 512 \implies b^2 \leq 1024 \implies 4 \leq b \leq 32.$$

There are **15** even values of b in this range. If b is odd, then $N_b = \frac{b-1}{2}b^3 + \frac{b+1}{2}b^2 = \left(\frac{b-1}{2}\frac{b+1}{2}00\right)_b$, so

$$\left(\frac{b-1}{2}\right)^2 + \left(\frac{b+1}{2}\right)^2 \leq 512 \implies \frac{b^2+1}{2} \leq 512 \implies 3 \leq b \leq 31.$$

There are **15** odd values of b in this range. In conclusion, there are $15 + 15 = \boxed{30}$ values for b. □

Example 2.30 (AIME)**.** The increasing sequence $1, 3, 4, 9, 10, 12, 13, \cdots$ consists of all those positive integers which are exponent powers of 3 or sums of distinct powers of 3. Find the 100th term of this sequence.

Solution. We create a table of the powers of 3 used for the first several terms:

k	kth term	3^2	3^1	3^0
1	**1**	0	0	1
2	**3**	0	1	0
3	**4**	0	1	1
4	**9**	1	0	0
5	**10**	1	0	1
6	**12**	1	1	0
7	**13**	1	1	1

We see $100 = 64 + 32 + 4 = 1100100_2$. Since the 1's and 0's actually correspond to powers of 3, the 100^{th} term of the sequence is

$$3^6 + 3^5 + 3^2 = \mathbf{981}.$$

□

Fractional bases are very similar to normal bases, except they include negative exponents.

Example 2.31. Convert the decimal number 7/16 to base 6.

Solution. Let the base 6 representation of the decimal number 7/16 be

$$\frac{7}{16} = \frac{a_1}{6} + \frac{a_2}{6^2} + \frac{a_3}{6^3} + \frac{a_4}{6^4} + \cdots.$$

We multiply this equation by 6 and write the left hand side as a mixed number:

$$\frac{42}{16} = 2 + \frac{10}{16} = a_1 + \frac{a_2}{6} + \frac{a_3}{6^2} + \frac{a_4}{6^3} + \cdots.$$

Therefore, $a_1 = \mathbf{2}$. We now convert 10/16 to base 6 using the same method:

$$\frac{60}{16} = 3 + \frac{12}{16} = a_2 + \frac{a_3}{6} + \frac{a_4}{6^2} + \cdots.$$

Hence, $a_2 = \mathbf{3}$. Since $12/16 = 4/6 + 3/36$, $a_3 = \mathbf{4}$ and $a_4 = \mathbf{3}$. Hence, $7/16 = \boxed{.2343_6}$. □

Example 2.32 (AIME)**.** A rational number written in base eight is $\underline{ab}.\underline{cd}$, where all digits are nonzero. The same number in base twelve is $\underline{bb}.\underline{ba}$. Find the base-ten number $\underline{abc}$.

Solution. Equating the integer parts, $8a + b = 12b + b \implies a = 3/2b$, so $(a, b) = (3, 2)$ or $(6, 4)$. Similarly, equating the fractional parts,

$$\frac{c}{8} + \frac{d}{64} = \frac{b}{12} + \frac{3/2b}{144} = \frac{3b}{32}.$$

Multiplying by 64 gives $8c+d = 6b$. If $b = 4$, then $(c, d) = (3, 0)$. However the digits are given to be non-zero. If $b = 2$, then $(c, d) = (1, 4)$ and we see $12.34_8 = 22.21_{12}$, so the answer is $abc = \mathbf{321}$. □

Example 2.33. Convert $1/(b - 1)$ to base b.

Solution. Using the infinite geometric series formula, we see that

$$\frac{1}{b} + \frac{1}{b^2} + \frac{1}{b^3} + \cdots = \frac{1/b}{1 - 1/b} = \frac{1}{b-1}.$$

Therefore, $1/(b - 1) = \mathbf{1} \cdot b^{-1} + \mathbf{1} \cdot b^{-2} + \mathbf{1} \cdot b^{-3} + \cdots = 0.\overline{\mathbf{1}}_b$. □

Example 2.34 (AHSME)**.** Call a positive real number special if it has a decimal representation that consists entirely of digits 0 and 7. For example, $\frac{700}{99} = 7.\overline{07} = 7.070707\cdots$ and 77.007 are special numbers. Find the smallest n such that 1 can be written as a sum of n special numbers?

Solution. Call numbers whose decimal representation consists solely of digits 0 and 1 super-special. We wish to find super-special numbers that sum to $1/7 = 0.\overline{142857}$. One example is

$$.111111,\ .011111,\ .010111,\ .010111,\ .000111,\ .000101,\ .000101,\ .000100.$$

Assume for the sake of contradiction that we can represent $1/7$ as the sum of less than 8 super-special numbers. However, since the addition won't have any carry over, each digit is simply the number of super-special numbers that have a 1 in the place, so the answer is **8**. □

Exercises

2.5.1. In balanced ternary, the digits have values $-1, 0$, and 1. For example, $11 = 3^2 + 3^1 - 3^0$. Find the sum of the exponents used in the balanced ternary representation of 2000.

2.5.2. Prove that 10101 is composite in any number base.

2.5.3. (HMMT) Let S be the set of integers of the form $2^x + 2^y + 2^z$, where x, y, z are pairwise distinct non-negative integers. Determine the 100th smallest element of S.

2.5.4. (AIME) Find the positive integer n such that there exists a single digit d with

$$\frac{n}{810} = 0.d25d25d25\cdots.$$

§2.6 Divisibility Rules

Below is a list of the divisibility rules up until 11.

- 2 - Last digit is even.
- 3 - Sum of the digits is divisible by 3.
- 4 - Number formed by last two digits is divisible by 4.
- 5 - Last digit is either 0 or 5.
- 6 - Divisibility rules for both 2 and 3 hold.
- 7 - Truncate the units digit of N, double that, and subtract it from the rest of the number. Repeat the process if necessary. Check to see if the final number obtained is divisible by 7.
- 8 - Number formed by the last three digits is divisible by 8.
- 9 - Sum of the digits is divisible by 9.
- 10 - The number ends in 0.
- 11 - Alternating sum of digits is divisible by 11.

In this section, we will focus on the rules for $7, 9$, and 11.

Example 2.35. Prove that a number is divisible by 9 if and only if the sum of its digits is.

Proof. Notice $10 \equiv 1 \pmod 9$. Considering the decimal form of a number,

$$\begin{aligned} n &= 10^k a_k + 10^{k-1} a_{k-1} + \cdots + 10^2 a_2 + 10^1 a_1 + a_0 \\ &\equiv 1^k a_k + 1^{k-1} a_{k-1} + \cdots + 1^2 a_2 + 1^1 a_1 + a_0 \\ &\equiv a_k + a_{k-1} + \cdots + a_2 + a_1 + a_0 \pmod 9. \end{aligned}$$

Hence n is divisible by 9 if and only if the sum of its digits is. □

Example 2.36 (AHSME)**.** The two-digit integers from 19 to 92 are written consecutively to form the larger number $N = 19202122\ldots909192$. Find the largest power of 3 that evenly divides N.

Solution. Let $f(n)$ denote the sum of the digits of n. By the divisibility rule for 9,

$$\begin{aligned} f(N) = f(19) + f(20) + f(21) + \cdots + f(92) &\equiv 19 + 20 + 21 + \cdots + 92 \pmod 9 \\ &\equiv 74\left(\frac{111}{2}\right) \\ &\equiv 3 \cdot 37^2 \equiv 3 \pmod 9. \end{aligned}$$

Therefore, the highest power of 3 that evenly divides N is $\boxed{3^1}$. □

Example 2.37. Prove that a number is divisible by 11 iff the alternating sum of its digits is.

Proof. Notice $10 \equiv -1 \pmod{11}$. Considering the decimal form of a number,

$$\begin{aligned} n &= 10^k a_k + 10^{k-1} a_{k-1} + \cdots + 10^2 a_2 + 10^1 a_1 + a_0 \\ &\equiv (-1)^k a_k + (-1)^{k-1} a_{k-1} + \cdots + (-1)^2 a_2 + (-1)^1 a_1 + a_0 \\ &\equiv a_0 - a_1 + a_2 - a_3 + \cdots + (-1)^k a_k \pmod{11}. \end{aligned}$$

Hence n is divisible by 11 if and only if the alternating sum of its digits is. □

Example 2.38 (PuMaC)**.** If $17! = 355687ab8096000$, find a and b.

Solution. We use both the divisibility rule for 9 and 11:

$$\begin{aligned} a + b + 57 \equiv 0 \pmod 9 &\implies a + b \equiv 6 \pmod 9 \\ a - b + 9 \equiv 0 \pmod{11} &\implies a - b \equiv 2 \pmod 9. \end{aligned}$$

The solution to this system of congruences is $(a, b) = \boxed{(4, 2)}$. □

Example 2.39. Find a and b such that the seven-digit number $21358ab$ is divisible by 99.

Solution. Observe that $10^2 \equiv 1 \pmod{99}$, therefore

$$\begin{aligned} 21358ab &= 2 \cdot 100^3 + 13 \cdot 100^2 + 58 \cdot 100 + 10a + b \\ &\equiv 2 + 13 + 58 + 10a + b \\ &\equiv 73 + 10a + b \equiv 0 \pmod{99}. \end{aligned}$$

Therefore, $10a + b = 26$ and $(a, b) = \boxed{(2, 6)}$. □

Example 2.40. Prove a number is divisible by 7 if and only if the result of truncating the units digit of the number and subtracting twice that from the rest of the number is also divisible by 7.

Proof. Let $N = 10a + x$ have units digit x. Multiplying by 5,

$$5N = 50a + 5x \equiv a - 2x \pmod{7}.$$

Therefore, 7 divides $a - 2x$ if and only if 7 divides N. □

Example 2.41. Prove that if a three-digit integer abc is divisible by 37, then its cyclic permutations are also divisible by 37. For example, 481, 814, and 148 are all divisible by 37.

Proof. We are given $100a+10b+c \equiv 0 \pmod{37}$ Since $10^3 \equiv 1 \pmod{37}$, multiplying by 10 gives

$$1000a + 100b + 10c \equiv 100b + 10c + a \equiv bca \equiv 0 \pmod{37}.$$

Similarly, multiplying our new congruence by 10 gives

$$1000b + 100c + 10a \equiv 100c + 10a + b \equiv cab \equiv 0 \pmod{37}.$$

Therefore, the cyclic permutations of abc are also divisible by 37. □

Example 2.42. (USAMO) Prove that for every positive integer n, there exists an n-digit number divisible by 5^n all of whose digits are odd.

Solution. We use induction. We begin by showing the first 4 base cases: $5, 75, 375, 9375$.

Assume that the k digit number $N = a_1a_2a_3 \cdots a_k$ is divisible by 5^k, hence $N = 5^kA$. We show that for one value of $i \in \{1, 3, 5, 7, 9\}$ the number below is divisible by 5^{k+1}:

$$N_i = ia_1a_2a_3 \cdots a_k = i \cdot 10^k + 5^kA = 5^k\left(i \cdot 2^k + A\right).$$

Since $\{1, 3, 5, 7, 9\}$ is a complete residue system, there exists an odd i with $i \cdot 2^k + A \equiv 0 \pmod{5}$. For this value of i, N_i is a $k + 1$-digit number divisible by 5^{k+1} all of whose digits are odd. □

Exercises

2.6.1. A number is selected at random from the set of all five-digit numbers whose sum of digits is equal to 43. What is the probability that this number is divisible by 11?

2.6.2. Prove that a number is divisible by 2^k if and only if the last k digits are.

2.6.3. Modifying the coefficients in the divisibility rule for 7 gives rules for other primes:

(a) Prove the divisibility rule for 13 replaces $-2x$ with $+4x$.

(b) Find the prime p whose divisibility rule replaces $-2x$ with $-3x$.

2.6.4. (HMMT) Find the digit N for which 91 divides $12345N789$.

§2.7 Polynomials

A polynomial for a variable x is an expression of the form

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0.$$

The constants $a_n, a_{n-1}, \cdots, a_1, a_0$ are the **coefficients**. $a_n \neq 0$ is the leading coefficient and a_0 is the constant coefficient. A polynomial is said to be **monic** if the leading coefficient is 1. n is the **degree** of the polynomial, denoted $\deg(f)$. By convention, the degree of $f(x) = 0$ is undefined.

Theorem 2.6. To divide $n(x)$ by $d(x)$, there exists a unique quotient $q(x)$ and remainder $r(x)$:

$$n(x) = d(x)q(x) + r(x), \quad \deg(r) < \deg(d) \text{ or } r(x) = 0.$$

Proof. To prove the existence, we repeatedly eliminate the leading term of $r(x)$ to decrease its degree until $\deg(r) < \deg(d)$. To prove uniqueness suppose that for quotients q_1 and q_2,

$$\begin{aligned} n(x) &= d(x) \cdot q_1(x) + r_1(x) \\ n(x) &= d(x) \cdot q_2(x) + r_2(x), \end{aligned}$$

where $\deg(r_1) < \deg(d)$ (or $r_1 = 0$) and $\deg(r_2) < \deg(d)$ (or $r_2 = 0$). Subtracting and rearranging,

$$d(x)\left(q_2(x) - q_1(x)\right) = r_1(x) - r_2(x).$$

However, since $q_1(x)$ and $q_2(x)$ are distinct, we have

$$\deg\left[d(x)(q_1(x) - q_2(x)\right] \geq \deg(d(x)).$$

On the other hand, $\deg(r_2(x) - r_1(x)) < \deg(d)$, therefore $r_1(x) = r_2(x)$ and $q_2(x) = q_1(x)$. □

Theorem 2.7 (Remainder Theorem). The remainder when $f(x)$ is divided by $x-a$ is $f(a)$.

Proof. Since $x-a$ is linear, there exists a constant remainder r upon division:

$$f(x) = (x-a)q(x) + r.$$

Substituting $x=a$ into this expression gives $f(a) = (a-a)\,q(a) + r \implies f(a) = r$. □

Example 2.43 (AIME). Find the largest integer n such that n^3+100 is divisible by $n+10$.

Solution. The remainder when we divide $p(n) = n^3+100$ by $n-(-10)$ is

$$r = p(-10) = -10^3 + 100 = -900.$$

Since $n+10$ divides the remainder, the largest value of n is when $n+10 = 900$ or $n = \boxed{890}$. □

If the remainder when we divide $f(x)$ by $d(x)$ is 0, then we say $d(x)$ is a factor of $f(x)$.

Theorem 2.8 (Factor Theorem). $f(x)$ has a factor of $x-c$ if and only if $f(c) = 0$.

Proof. If $x-c$ is a factor of $f(c)$, then $f(x) = (x-c)q(x)$ for some $q(x)$. Substituting $x=c$ gives

$$f(c) = (c-c)q(c) = 0 \cdot q(c) = 0.$$

If $f(c) = 0$, then the remainder when we divide $f(x)$ by $x-c$ is 0, so $x-c$ is a factor of $f(x)$. □

Euler discovered that n^2+n+41 generates 40 consecutive primes for $0 \le n \le 39$. However, $40^2+40+41 = 41^2$. Euler's polynomial is prime for 86 of the first 100 natural numbers.

Example 2.44 (Legendre). Prove that there is no nonconstant polynomial with integral coefficients that produces primes for every integer n.

Proof. Suppose that there is such a polynomial with integer coefficients and $a_k \neq 0$:

$$f(n) = a_k n^k + a_{n-1} k^{n-1} + \cdots + a_2 n^2 + a_1 n + a_0.$$

For a fixed value of n_0, let $f(n_0) = p$ be a prime. For a variable integer t consider

$$\begin{aligned} f(n_0+tp) &= a_k\left(n_0+tp\right)^k + a_{k-1}\left(n_0+tp\right)^{k-1} + \cdots + a_2\left(n_0+tp\right)^2 + a_1\left(n_0+tp\right) + a_0 \\ &\equiv a_k n_0^k + a_{k-1} n_0^{k-1} + \cdots + a_2 n_0^2 + a_1 n_0 + a_0 \\ &\equiv f(n_0) \equiv 0 \pmod{p}. \end{aligned}$$

Since f always generates primes, $f(n_0+tp) = p$. However, then the polynomial $g(n) = f(n)-p$ has infinite roots, contradiction. Therefore there is no nonconstant prime producing polynomial. □

While there is no prime-producing polynomial, in 1947, it was proven that there exists a positive real number r such that $\lfloor r^{3^n} \rfloor$ is prime for all natural numbers n. The value r is known as Mills' constant and its value is unknown, however, assuming the Riemann hypothesis, $r \approx 1.306378\ldots$

Example 2.45 (AIME)**.** Find integers a and b such that x^2-x-1 is a factor of $ax^{17}+bx^{16}+1$.

Solution. We know φ and ψ are the roots of x^2-x-1. Since $\varphi^2=\varphi+1$, we see that

$$\begin{aligned}\varphi^3&=\varphi^2+\varphi=2\varphi+1\\ \varphi^4&=\varphi^3+\varphi^2=3\varphi+2\\ \varphi^5&=\varphi^4+\varphi^3=5\varphi+3.\end{aligned}$$

These coefficients are Fibonacci numbers! We can prove by induction that $\varphi^n=F_n\varphi+F_{n-1}$. Since x^2-x-1 divides $ax^{17}+bx^{16}+1$, φ must also be a root of $ax^{17}+bx^{16}+1$. Therefore,

$$a\varphi^{17}+b\varphi^{16}+1=a\left(F_{17}\varphi+F_{16}\right)+b\left(F_{16}\varphi+F_{15}\right)+1=0.$$

Hence, $aF_{17}+bF_{16}=0$ and $aF_{16}+bF_{15}+1=0$. We solve $a=F_{16}=\mathbf{987}$ and $b=-F_{17}=\mathbf{-1597}$. We can verify the second equation by Cassini's identity: $F_{16}^2-F_{15}F_{17}=-1$. □

Example 2.46 (Mandelbrot)**.** Determine the positive integer a such that $x^8+5x^6+13x^4+20x^2+36$ is evenly divisible by x^2-x+a.

Solution. Let $n(x)=x^8+5x^6+13x^4+20x^2+36$ and $d(x)=x^2-x+a$, so

$$n(x)=d(x)q(x)\text{ for }q(x)\in\mathbb{Z}[x].$$

Since a is the constant term of $d(x)$, it must divide 36. Substituting $x=1$ into the equation,

$$n(1)=d(1)\cdot q(1)\implies 75=a\cdot q(1).$$

Since $a\mid 75$, $a\mid 36$, and a is positive, $a=1$ or $a=3$. Substituting $x=-2$ gives

$$n(-2)=d(-2)\cdot q(-2)\implies 900=(a+6)\cdot q(-2).$$

Since $7\nmid 900$, we must have $a=\mathbf{3}$. Using long division, we verify

$$x^8+5x^6+13x^4+20x^2+36=\left(x^2-x+3\right)\left(x^6+x^5+3x^4+4x^2+4x+12\right).$$ □

Exercises

2.7.1. Find a constant c such that $x^4+3x^3+cx^2+6x-4$ is evenly divisible by $x-2$.

2.7.2. Find the quotient $q(x)$ and remainder $r(x)$ upon dividing $x^6+2x^5+3x^3+1$ by x^3+x^2-1.

2.7.3. Prove that if $d(x)$ is a factor of $f(x)$, then every root of $d(x)$ is also a root of $f(x)$.

§2.8 Review Problems

2.47. Prove that if n is an integer, then $1 + (-1)^n (2n - 1)$ is a multiple of 4.

2.48. (AMC 10) For each positive integer $m > 1$, let $P(m)$ denote the greatest prime factor of m. Find all n such that both $P(n) = \sqrt{n}$ and $P(n+48) = \sqrt{n+48}$.

2.49. Express $2^{22} + 1$ as the product of two four-digit numbers.

2.50. Find all positive integers $n < 17$ for which $n! + (n+1)! + (n+2)!$ is a multiple of 49.

2.51. (Duke) Find the sum of all integers n such that $n^2 + 2n + 2$ divides $n^3 + 4n^2 + 4n - 14$.

2.52. (ARML) Compute the largest prime factor of

$$3(3(3(3(3(3(3(3(3(3(3+1)+1)+1)+1)+1)+1)+1)+1)+1)+1)+1.$$

2.53. (Putnam) Determine the prime members of the sequence $101, 10101, 1010101, \cdots$.

2.54. Prove that the sum $1^k + 2^k + 3^k + \cdots + n^k$ is divisible by $1 + 2 + 3 + \cdots + n$ for all odd k.

2.55. Determine all values of n such that $1^2 + 2^2 + 3^2 + \cdots + n^2$ is divisible by $1 + 2 + 3 + \cdots + n$.

2.56. Find the remainder when $1^3 + 2^3 + 3^3 + \cdots + 100^3$ is divided by 9.

2.57. (AHSME) If the base 8 representation of a perfect square is $ab3c$ where $a \neq 0$, find c.

2.58. (AHSME) Given $0 \leq x_0 < 1$, let

$$x_n = \begin{cases} 2x_{n-1} & \text{if } 2x_{n-1} < 1 \\ 2x_{n-1} - 1 & \text{if } 2x_{n-1} \geq 1 \end{cases}$$

for all integers $n > 0$. For how many x_0 is it true that $x_0 = x_5$?

2.59. (HMMT) Let Q be a polynomial $Q(x) = a_0 + a_1 x + \cdots + a_n x^n$, where $a_0, \ldots, a_n$ are nonnegative integers. Given that $Q(1) = 4$ and $Q(5) = 152$, find $Q(6)$.

2.60. (AHSME) Let the product $(12)(15)(16)$, each factor written in base b, equal 3146 in base b. Let $s = 12 + 15 + 16$, each term expressed in base b. Find the value of s in base b.

2.61. Prove that every six-digit number of the form $abcabc$ is divisible by $7, 11$, and 13.

2.62. (HMMT) What is the smallest 5-digit palindrome that is a multiple of 99?

2.63. Prove that every number in the sequence $16, 1156, 111556, \cdots$ is a perfect square.

2.64. Prove that every positive integer m divides infinitely many Fibonacci numbers.

2.65. (AHSME) A set of consecutive positive integers beginning with 1 is written on a blackboard. When one number is erased, the arithmetic mean of the remaining numbers is $35\frac{7}{17}$. Find it.

2.66. (AMC 12) Call a number "prime-looking" if it is composite but not divisible by 2, 3, or 5. The three smallest prime-looking numbers are 49, 77, and 91. There are 168 prime numbers less than 1000. How many prime-looking numbers are there less than 1000?

2.67. Find the positive integer m such that the polynomial $p^3 + 2p + m$ divides $p^{12} - p^{11} + 3p^{10} + 11p^3 - p^2 + 23p + 30$.

§2.9 Challenge Problems

2.68. Fermat numbers are of the form $f_n = 2^{2^n} + 1$ for natural n.

(a) $f_0 = 3, f_1 = 5, f_2 = 17, f_3 = 257$, and $f_4 = 65537$ are primes. Prove 641 divides $2^{32} + 1$.

(b) Prove that if $2^n + 1$ is prime for a positive integer n, then it is a Fermat number.

2.69$\star$ For an integer k in base 10, let $z(k)$ be the number of zeroes that appear in the binary representation of k. Let $S_n = \sum_{k=1}^{n} z(k)$. Compute S_{256}.

2.70$\star$ (AIME) Let $T = \{9^k : k \text{ is an integer}, 0 \leq k \leq 4000\}$. Given that 9^{4000} has 3817 digits and that its first (leftmost) digit is 9, how many elements of T have 9 as their leftmost digit?

2.71. (IMO) Let $f(n)$ denote the sum of the digits of n and $N = 4444^{4444}$. Find $f(f(f(N)))$.

2.72$\star$ (APMO) For any positive integer n, let $S(n)$ be the sum of digits in the decimal representation of n. Any positive integer obtained by removing one or more digits from the right-hand end of the decimal representation of n is called a stump of n. Let $T(n)$ be the sum of all stumps of n. Prove that $n = S(n) + 9T(n)$.

2.73$\star$ (USAMO) Prove that there is no polynomial P with integer coefficients such that there exists integers a, b, c with $P(a) = b, P(b) = c$, and $P(c) = a$.

2.74$\star$ Prove that for all positive integer pairs (a, b) with $b > 2$, $2^b - 1$ does not divide $2^a + 1$.

2.75$\star$ (IMO) Find all integers a, b, c with $1 < a < b < c$ such that

$$(a-1)(b-1)(c-1)$$

divides $abc - 1$.

2.76$\star$ (IMO) Find all pairs of positive integers such that $xy^2 + y + 7$ divides $x^2y + x + y$.

2.77$\star$ (Putnam) Let $0 < a_1 < a_2 < \cdots < a_{mn+1}$ be $mn+1$ integers. Prove that you can find either $m+1$ of them no one of which divides any other, or $n+1$ of them, each dividing the following.

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

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

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

$$1 + r + r^2 + \cdots + r^{k-1} = \frac{r^k - 1}{r - 1}. \tag{Hypothesis}$$

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

$$F_1 + F_3 + F_5 + \cdots + F_{2k-1} = F_{2k}. \tag{Hypothesis}$$

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

$$F_1^2 + F_2^2 + \cdots + F_k^2 = F_k F_{k+1}. \tag{Hypothsis}$$

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

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

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 $n - 1$:

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

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,

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

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

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

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 $3^s \le n < 3^{s+1}$. 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.

§A.2 Divisibility and Congruences Solutions

Exercises for Section 2.1

2.1.1 Observe that if 9 is amongst the digits, then the digits must sum to 18, however, this is impossible by parity. If 3 is included, then one of the other digits must be 1 mod 3 and the other 2 mod 3. Therefore, possible candidates are **315**, **135**, 375, or **735**, however, $7 \nmid 375$. If 3 is excluded, then the number must be **175** or 715, however $7 \nmid 715$. The answer is $\boxed{135, 175, 315, 735}$.

2.1.2 We complete the proof of Theorem 2.1:

(3) Since $dc \mid nc$, there exists an integer q with $nc = q\,(dc)$. Therefore $n = dq$, implying $d \mid n$.

(4) Since $d \mid n$ and $n \mid d$, there exists integers q and q' with $n = dq$ and $d = nq'$. Substituting,

$$n = nq'q \implies q'q = 1.$$

Therefore $|q'| = |q| = 1$ and we conclude $|n| = |d|$.

2.1.3 Factoring the polynomial using difference of squares,

$$\begin{aligned} n^5 - 5n^3 + 4n &= n\left(n^4 - 5n^2 + 4\right) \\ &= n\left(n^2 - 4\right)\left(n^2 - 1\right) \\ &= n\,(n-2)\,(n+2)\,(n-1)\,(n+1)\,. \end{aligned}$$

Therefore, since it is the product of 5 consecutive integers, $n^5 - 5n^3 + 4n$ is divisible by $5! = 120$.

2.1.4 Since $d \mid n_j$ for every $1 \le j \le k$, there exists an integer q_j such that $n_j = q_j d$:

$$\begin{aligned} n_1\alpha_1 + n_2\alpha_2 + \cdots + n_k\alpha_k &= q_1 d\alpha_1 + q_2 d\alpha_2 + \cdots + q_k d\alpha_k \\ &= d\left(\sum_{1 \le j \le k} q_j\alpha_j\right). \end{aligned}$$

By the definition of divisibility, $d \mid n_1\alpha_1 + n_2\alpha_2 + \cdots + n_k\alpha_k$.

Exercises for Section 2.2

2.2.1 By the Sieve of Eratosthenes, Jane will erase every integer with an odd factor. Therefore, the numbers that remain are the powers of 2, 2^n. Since $2^{11} = 2048$, we must have $0 \le n \le 10$, for a total of $\boxed{11}$ values.

2.2.2 We factor $p^{1994} + p^{1995} = p^{1994}\,(1 + p)$. Since 1994 is even, $p + 1$ must be a perfect square:

$$p = n^2 - 1 = (n-1)\,(n+1)\,, \text{ for integer } n.$$

For this to be a prime, we must have $n - 1 = 1 \implies n = 2$ and $p = \boxed{3}$.

2.2.3 We factor $N = 1001001001 = (10^3+1)(10^6+1)$. From the sum of cubes formula,

$$\begin{aligned} N &= \left[(10+1)\left(10^2-10+1\right)\right]\left[\left(10^2+1\right)\left(10^4-10^2+1\right)\right] \\ &= (11\cdot 91)(101\cdot 9901) \\ &= 7\cdot 11\cdot 13\cdot 101\cdot 9901. \end{aligned}$$

The largest divisor less than 10000 is $\boxed{9901}$.

2.2.4 Let $n = dq$ for some integer q. Then,

$$\begin{aligned} x^n - y^n &= x^{dq} - y^{dq} \\ &= \left(x^d\right)^q - \left(y^d\right)^q \\ &= \left(x^d - y^d\right)\left(x^{d\cdot(q-1)} + x^{d\cdot(q-2)}y^d + \cdots + y^{d\cdot(q-1)}\right). \end{aligned}$$

Therefore, $x^d - y^d \mid x^n - y^n$ when $d \mid n$.

Exercises for Section 2.3

2.3.1 Let the three digit integer be $N = 13K + 7$. We solve the inequality:

$$13K + 7 < 1000 \implies 13K < 993 \implies K < 77.$$

Therefore, the largest N is when $K = 76$, giving $N = 13\cdot 76 + 7 = \boxed{995}$.

2.3.2 We group the numbers in the list based upon their remainder when dividing by 7:

$$\begin{aligned} 7k &: \{7,14,21,28,35,42,49\} \\ 7k+1 &: \{1,8,15,22,29,36,43,50\} \\ 7k+2 &: \{2,9,16,23,30,37,44\} \\ 7k+3 &: \{3,10,17,24,31,38,45\} \\ 7k+4 &: \{4,11,18,25,32,39,46\} \\ 7k+5 &: \{5,12,19,26,33,40,47\} \\ 7k+6 &: \{6,13,20,27,34,41,48\}. \end{aligned}$$

We can have a maximum of **1** number that is $7k$, **8** numbers that are $7k+1$, **7** numbers that are $7k+2$, and **7** numbers that are $7k+3$. The answer is hence $1+8+7+7 = \boxed{23}$.

2.3.3 From the division algorithm, $2017 = dq + r$ for $0 \le r \le d-1$. We condition on the quotient.

- If $q = 1$, then $2017 = d + r \le 2d - 1 \implies d \ge 1009$. However, d is at most 1000.
- If $q = 2$, then $2017 = 2d + r \le 3d - 1 \implies d \ge 673$. For $d = 673$, we see that

$$2017 = 673\cdot 2 + \mathbf{671}.$$

As the quotient increases, the remainder decreases. Therefore, the largest remainder is $r = \boxed{671}$.

2.3.4 Let the two numbers be $4m+3$ and $4n+3$. Expanding their product, we see

$$(4m+3)(4n+3) = 16mn + 12m + 12n + 9 = 4(4mn + 3m + 3n + 2) + 1,$$

which is of the form $4k+1$.

Exercises for Section 2.4

2.4.1 Since $a_1 \equiv a_2 \pmod{m}$, by definition, $m \mid a_1 - a_2$. Furthermore, $d \mid m$, therefore by the transitive property of divisibility, $d \mid a_1 - a_2$. This then implies $a_1 \equiv a_2 \pmod{d}$.

2.4.2 (a) Note that $5^3 = 125 \equiv 1 \pmod{31}$. Therefore, since $1337 \equiv 2 \pmod{3}$,

$$5^{1337} \equiv 5^2 \equiv \boxed{25} \pmod{31}.$$

(b) Note that $2^7 \equiv 1 \pmod{2^7 - 1}$. Therefore, since $2001 \equiv 6 \pmod{7}$,

$$2^{2001} \equiv 2^6 \equiv \boxed{64} \pmod{2^7 - 1}.$$

2.4.3 Rewriting the expression and using the Binomial Theorem,

$$\begin{aligned}
2^{4n} + 10n - 1 &= 16^n + 10n - 1 \\
&= (15+1)^n + 10n - 1 \\
&= \left[15^n + \binom{n}{1}15^{n-1} + \cdots + \binom{n}{n-2}15^2 + \binom{n}{n-1}15 + 1\right] + 10n - 1 \\
&\equiv [0 + 15n + 1] + 10n - 1 \equiv 0 \pmod{25}.
\end{aligned}$$

2.4.4 We use our difference of nth powers factorization:

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

Since $a \equiv b \pmod{n}$, the first term in the product is divisible by n. Furthermore,

$$a^{n-1} + a^{n-2}b + \cdots + b^{n-1} \equiv \underbrace{b^{n-1} + b^{n-1} + \cdots + b^{n-1}}_{\text{n terms}} \equiv 0 \pmod{n}.$$

Therefore, the second term is also divisible by n, implying the product is divisible by n^2.

Exercises for Section 2.5

2.5.1 In base 3, $2000 = 2\cdot 3^6 + 2\cdot 3^5 + 2\cdot 3^3 + 2$. Observe that $2\cdot 3^k = 3^{k+1} - 3^k$, so

$$2000 = \left(3^7 - 3^6\right) + \left(3^6 - 3^5\right) + \left(3^4 - 3^3\right) + (3-1) = 3^7 - 3^5 + 3^4 - 3^3 + 3 - 1.$$

Therefore, the sum of exponents used is $7 + 5 + 4 + 3 + 1 + 0 = \boxed{20}$.

2.5.2 Let the base be b. Using difference of squares,

$$\begin{aligned}
10101_b &= b^4 + b^2 + 1 \\
&= \left(b^2+1\right)^2 - b^2 \\
&= \left(b^2 - b + 1\right)\left(b^2 + b + 1\right).
\end{aligned}$$

Since $b \geq 2$, both factors are at least 3, therefore, the number is composite.

2.5.3 WLOG say $x > y > z$. For $x = k$, we see that $y, z \in \{0, 1, \cdots, k-1\}$ for a total of $\binom{k}{2}$ ways to choose y and z. We repeat this procedure until $x = 8$, giving the sum

$$\binom{2}{2} + \binom{3}{2} + \binom{4}{2} + \cdots + \binom{8}{2} = 84.$$

Therefore, $(x, y, z) = (8, 7, 6)$ is the 84th element of the set. Now, we desire to find the 16th smallest element for $x = 9$. We see that for $y = 1$ to $y = 5$, there are $1 + 2 + 3 + 4 + 5 = 15$ pairs. Therefore, the 100th smallest element is $(x, y, z) = (9, 6, 0)$ giving $2^9 + 2^6 + 2^0 = \boxed{577}$.

2.5.4 Using the formula for a sum of an infinite geometric series,

$$\begin{aligned}\frac{n}{810} &= \frac{100d + 25}{10^3} + \frac{100d + 25}{10^6} + \cdots \\ &= \frac{100d + 25}{999}.\end{aligned}$$

We isolate the equation for n and simplify:

$$n = \frac{810}{999}(100d + 25) = \frac{30}{37} \cdot 25(4d + 1).$$

Hence $37 \mid 4d + 1$, so $d = 9$. Then, $n = 30 \cdot 25 = \boxed{750}$.

Exercises for Section 2.6

2.6.1 Let such a five-digit number be $\underline{abcde}$. Since $43 = 5 \cdot 9 - 2$, the digits must either consist of 4 nines and 1 seven or 3 nines and 2 eights. Therefore, there are $\binom{5}{1} + \binom{5}{2} = 15$ such numbers. By the divisibility rule for 11, $a - b + c - d + e$ must be divisible by 11. The maximum value is

$$a - b + c - d + e = 2(a + c + e) - (a + b + c + d + e) \le 2 \cdot 27 - 43 = 11,$$

with equality holding when $a = b = c = 9$. Therefore, we must have $(b, d) = (7, 9), (8, 8), (9, 7)$ for a total of 3 numbers that are divisible by 11. The probability is $3/15 = \boxed{1/5}$.

2.6.2 Let the decimal form be $N = a_m a_{m-1} \cdots a_1 a_0$. Reducing mod 2^k, we see

$$\begin{aligned}N &= 10^m a_m + 10^{m-1} a_{m-1} + \cdots + 10^1 a_1 + a_0 \\ &\equiv 10^{k-1} a_{k-1} + 10^{k-2} a_{k-2} + \cdots + a_1 + a_0 \\ &\equiv a_{k-1} a_{k-2} a_{k-3} \cdots a_1 a_0 \pmod{2^k}.\end{aligned}$$

Therefore, n is divisible by 2^k if and only if the last k digits are.

2.6.3 (a) Let $N = 10a + x$ have units digit x. Multiplying by 4,

$$4N = 40a + 4x \equiv a + 4x \pmod{13}.$$

Therefore, we conclude that 13 divides N if and only if 13 divides $a + 4x$.

(b) We desire to find a prime p such that $p \mid 10a + x$ implies $p \mid a - 3x$. Note

$$10a + x - 10\,(a - 3x) = 31x,$$

therefore $p \mid 31$ by the linear combination theorem. Hence, $p = \boxed{31}$.

2.6.4 Since $1001 = 7 \cdot 11 \cdot 13$, we see $10^3 \equiv -1 \pmod{91}$. Now,

$$\begin{aligned} 123450789 &= 123 \cdot 10^6 + 450 \cdot 10^3 + 789 \\ &\equiv 123 \cdot 1 + 450 \cdot -1 + 789 \cdot 1 \\ &\equiv 32 + 5 + 61 \\ &\equiv 98 \equiv 7 \pmod{91}. \end{aligned}$$

Therefore, $12345N789 \equiv 7 + 1000N \equiv 7 - N \equiv 0 \pmod{91} \implies N = \boxed{7}$.

Exercises for Section 2.7

2.7.1 Let $f(x) = x^4 + 3x^3 + cx^2 + 6x - 4$. By the factor theorem, we must have $f(2) = 0$, hence

$$f(2) = 16 + 24 + 4c + 12 - 4 = 0 \implies 4c + 48 = 0 \implies c = \boxed{-12}.$$

2.7.2 We divide the leading terms of the two polynomials: $x^6/x^3 = x^3$. Hence,

$$x^6 + 2x^5 + 3x^3 + 1 = \left(x^3 + x^2 - 1\right) \cdot x^3 + \left(x^5 + 4x^3 + 1\right)$$

To eliminate the quintic term, we divide x^5 by x^3: $x^5/x^3 = x^2$ and add to our quotient:

$$x^6 + 2x^5 + 3x^3 + 1 = \left(x^3 + x^2 - 1\right) \cdot \left(x^3 + x^2\right) + \left(-x^4 + 4x^3 + x^2 + 1\right)$$

To remove the quartic term, we divide $-x^4$ by x^3: $-x^4/x^3 = -x$ and add to our quotient:

$$x^6 + 2x^5 + 3x^3 + 1 = \left(x^3 + x^2 - 1\right) \cdot \left(x^3 + x^2 - x\right) + \left(5x^3 + x^2 - x + 1\right)$$

To remove the cubic term, we divide $5x^3$ by x^3: $5x^3/x^3 = 5$ and add to our quotient:

$$x^6 + 2x^5 + 3x^3 + 1 = \left(x^3 + x^2 - 1\right) \cdot \left(x^3 + x^2 - x + 5\right) + \left(-4x^2 - x + 6\right)$$

Therefore, $q(x) = \boxed{x^3 + x^2 - x + 5}$ and $r(x) = \boxed{-4x^2 - x + 6}$.

2.7.3 Since $d(x) \mid f(x)$, $f(x) = d(x)q(x)$. Let r be an arbitrary root of $d(x)$. Then,

$$f(r) = d(r) \cdot q(r) = 0 \cdot q(r) = 0,$$

thus r is also a root of $f(x)$.

Review Problems

2.47 The value of $(-1)^n$ depends on the parity of n. Therefore, we we have two cases:

(i) n is even. Then, $n = 2k$ for some integer k. Substituting this into the expression:

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

(ii) n is odd. Then, $n = 2k+1$ for some integer k. Substituting this into the expression:

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

2.48 We see that $n = p^2$ and $n + 48 = q^2$ for primes p and q. By difference of squares,

$$q^2 - p^2 = (q+p)(q-p) = 48.$$

If $q + p = 24$ and $q - p = 2$, then $(q, p) = \mathbf{(13, 11)}$. For $q + p = 12$ and $q - p = 4$, $(q, p) = (8, 4)$ and for $q + p = 8$ and $q - p = 6$, $(q, p) = (7, 1)$. Neither are prime solutions, hence $n = 11^2 = \boxed{121}$.

2.49 We complete the square:

$$\begin{aligned} 2^{22} + 1 &= \left(2^{11} + 1\right)^2 - \left(2^6\right)^2 \\ &= \left(2^{11} + 1 - 2^6\right)\left(2^{11} + 1 + 2^6\right) \\ &= 1985 \cdot 2113. \end{aligned}$$

The desired four-digit numbers are $\boxed{1985}$ and $\boxed{2113}$.

2.50 Factoring, we see

$$n! + (n+1)! + (n+2)! = n!\left[1 + (n+1) + (n+1)(n+2)\right] = n!\,(n+2)^2.$$

The expression is divisible by 49 if and only if $7 \mid n+2$ or $49 \mid n!$. The first condition happens when $n = 5$ or $n = 12$ and the second when $n \geq 14$. Therefore, the answers are $\boxed{5, 12, 14, 15, 16}$.

2.51 From the division algorithm for polynomials,

$$n^3 + 4n^2 + 4n - 14 = (n^2 + 2n + 2)(n + 2) + (-2n - 18).$$

When $n^2 + 2n + 2$ divides $n^3 + 4n^2 + 4n - 14$, it must also divide the remainder above, $-2n - 18$. If $|-2n - 18| \geq |n^2 + 2n + 2|$, then $-4 \leq n \leq 4$. Testing values shows $n = \mathbf{-4, -2, -1, 0, 1, 4}$. Alternatively, if $-2n - 18 = 0$, then $n = \mathbf{-9}$. The sum of all n is hence $\boxed{-11}$.

2.52 Using the sum of a geometric series formula and factoring,

$$\begin{aligned}3^{11}+3^{10}+3^9+\cdots+3^0 &= \frac{3^{12}-1}{2}\\ &= \frac{\left(3^6-1\right)\left(3^6+1\right)}{2}\\ &= \frac{\left(3^3-1\right)\left(3^3+1\right)\left(3^6+1\right)}{2}\\ &= \frac{26\cdot 28\cdot 730}{2}.\end{aligned}$$

Since $26 = 2\cdot 13$, $28 = 2^2\cdot 7$, and $730 = 2\cdot 5\cdot 73$, the largest prime factor is $\boxed{73}$.

2.53 Let k_n represent the member of the sequence with n 1's. From grouping terms, we see that 101 divides k_{2n}, therefore, the only prime with an even index is $\boxed{101}$. Furthermore,

$$\begin{aligned}k_{2n+1} = 1+10^2+10^4+\cdots+10^{4n} &= \frac{10^{4n+2}-1}{99}\\ &= \left(\frac{10^{2n+1}+1}{11}\right)\left(\frac{10^{2n+1}-1}{9}\right).\end{aligned}$$

Since both of these are integers greater than 1, no member of the sequence is prime for odd indices.

2.54 Recall that $1+2+\cdots+n = n(n+1)/2$. Let S be the sum of the odd k^{th} powers. Multiplying the divisibility by 2 and using the converse of Example 2.2, we must prove $n \mid 2S$ and $n+1 \mid 2S$. To prove $n+1$ divides the sum, we group it into pairs that sum to $n+1$:

$$2S = \left(1^k+n^k\right)+\cdots+\left(d^k+(n+1-d)^k\right)+\cdots+\left(n^k+1\right).$$

To prove n divides the sum, we group it into pairs that add to n:

$$2S = \left(1^k+(n-1)^k\right)+\cdots+\left(d^k+(n-d)^k\right)+\cdots+\left((n-1)^k+1\right)+2n^k.$$

Since $x+y \mid x^k+y^k$ for odd k, we have proven $n \mid 2S$ and $n+1 \mid 2S$.

2.55 Recall the sum of squares formula $1^2+2^2+3^2+\cdots+n^2 = n(n+1)(2n+1)/6$. Therefore,

$$n(n+1)/2 \mid n(n+1)(2n+1)/6.$$

Using the cancellation property, this is equivalent to $3 \mid 2n+1$, hence $n \equiv \boxed{1 \pmod 3}$.

2.56 Clearly $(3n)^3 \equiv 0 \pmod 9$. Using the Binomial Theorem,

$$\begin{aligned}(3n+1)^3 &= 27n^3+27n^2+9n+1 \equiv 1 \pmod 9\\ (3n+2)^3 &= 27n^3+54n+36n+8 \equiv 8 \pmod 9.\end{aligned}$$

Therefore, every group of 3 sums to 0 mod 9. Hence,

$$\begin{aligned}1^3+2^3+3^3+\cdots+99^3+100^3 &= \sum_{k=0}^{32}\left[(3k+1)^3+(3k+2)^3+(3k+3)^3\right]+100^3\\ &\equiv 0+1\equiv 1 \pmod 9.\end{aligned}$$

Another method uses the sum of cubes formula:

$$\begin{aligned}1^3+2^3+3^3+\cdots+100^3 &= \left(\frac{100\cdot 101}{2}\right)^2\\ &= 50^2\cdot 101^2\\ &\equiv 5^2\cdot 2^2\equiv 10^2\equiv 1 \pmod 9).\end{aligned}$$

2.57 Converting to decimal,

$$ab3c_8 = 512a+64b+24+c = 8\left(64a+8b+3+c\right).$$

If c is even, then $64a+8b+3+c$ is odd. However, 8 only has three factors of 2, hence $ab3c_8$ cannot be a perfect square. Furthermore, we see all odd perfect squares are 1 mod 8. Indeed,

$$(2n+1)^2 = 4n^2+4n+1 = 4n(n+1)+1.$$

Since one of n and $n+1$ is even, this entire quantity is 1 mod 8. Therefore, $c=\boxed{1}$.

2.58 In binary, the given recursion is equivalent to right shifting the decimal by 1. Let

$$x_0 = \sum\frac{a_k}{2^k} = .\left(a_1a_2a_3a_4a_5\cdots\right)_2.$$

If $a_1=0$, then $x_1=2x_0$ and if $a_1=1$, then $x_1=2x_0-1$. Either way, $x_1=.\left(a_2a_3a_4a_5a_6\cdots\right)_2$. To determine x_5, we right shift by 5 bits: $x_5=.\left(a_6a_7a_8a_9a_{10}\cdots\right)_2$. Since $x_0=x_5$, x_0 must repeat with $a_1a_2a_3a_4a_5$ as the repeating block. There are 2 choices per digit, so we have $2^5=32$ blocks. However, if $a_1=a_2=a_3=a_4=a_5=1$, then $x_0=1$, so the answer is $32-1=\boxed{31}$.

2.59 Since $Q(1)=4$, the sum of the coefficients equals 4. Converting 152 to base 5, we see $152=1102_5$, so $Q(x)=x^3+x^2+2$. Therefore, $Q(6)=216+36+2=\boxed{254}$.

2.60 We are given that $12_b\cdot 15_b\cdot 16_b=3146_b$. Converting back to decimal,

$$\begin{aligned}(b+2)(b+5)(b+6) &= 3b^3+b^2+4b+6\\ b^3+13b^2+52b+60 &= 3b^3+b^2+4b+6\\ 0 &= 2b^3-12b^2-48b-54\end{aligned}$$

Dividing by 2, $b^3-6b^2-24b-27=0$. Since the digit 6 is used, $b\geq 7$. We see $b=9$ is the only real root of the cubic, therefore $s=12_9+15_9+16_9=\boxed{44_9}$.

2.61 Let N be such a number. Grouping the terms,

$$\begin{aligned} n = abcabc &= 10^5 \cdot a + 10^4 \cdot b + 10^3 \cdot c + 10^2 \cdot a + 10^1 \cdot b + c \\ &= \left(10^5 + 10^2\right) \cdot a + \left(10^4 + 10^1\right) \cdot b + \left(10^3 + 1\right) \cdot c \\ &= 1001 \cdot (100a + 10b + c)\,. \end{aligned}$$

Since $1001 = 7 \cdot 11 \cdot 13$, we conclude that $abcabc$ is divisible by $7, 11$, and 13.

2.62 Observe that a 5-digit palindrome is of the form

$$XYZYX = 10000X + 1000Y + 100Z + 10Y + X = 10001X + 1010Y + 100Z.$$

Notice $99 \mid 9999$ and $99 \mid 990$, so $10001 \equiv 2 \pmod{99}$ and $1010 \equiv 20 \pmod{99}$. Therefore,

$$10001X + 1010Y + 100Z \equiv 2X + 20Y + Z \equiv 0 \pmod{99}.$$

Since X, Y, and Z are all digits, $0 \le X, Y, Z \le 9$, so $2X + 20Y + Z = 99$ or $2X + 20Y + Z = 198$.

- In the first case, the smallest palindrome we obtain is when $Y = 4$ giving $2X + Z = 19$. We must have $Z = 9 \implies X = 5$, giving the palindrome 54945.
- In the second case, the smallest palindrome we obtain is when $Y = 9$ giving $2x + Z = 18$. We must have $Z = 8 \implies X = 5$, giving the palindrome 59895.

The smaller of the two cases is $\boxed{54945}$.

2.63 By the geometric series formula, we see that a sequence k 1's equals

$$\underbrace{11\cdots111}_{k\ 1's} = 10^{k-1} + 10^{k-2} + \cdots + 10^2 + 10^1 + 1 = \frac{10^k - 1}{9}.$$

Therefore, we can write every number in the sequence in the form

$$\begin{aligned} \underbrace{11\cdots111}_{k \text{ 1's}}\underbrace{55\cdots55}_{k-1 \text{ 1's}}6 &= \frac{10^k\left(10^k - 1\right)}{9} + \frac{50\left(10^{k-1} - 1\right)}{9} + 6 \\ &= \frac{10^{2k} + 4 \cdot 10^k + 4}{9} \\ &= \left(\frac{10^k + 2}{3}\right)^2. \end{aligned}$$

Since $10^k + 2 \equiv 1 + 2 \equiv 0 \pmod{3}$, every term in the sequence is the square of an integer.

2.64 We make a list of the possible pairs of consecutive Fibonacci numbers, (F_{k+2}, F_{k+1}) for nonnegative integers k. This list is infinite, but reduced modulo m, there are only m^2 distinct pairs. Therefore, by the pigeonhole principle, two pairs must be equal. Then, by induction, we see that the entire sequence is periodic modulo m. Hence, there exists an integer $d > 2$ such that

$$(F_{d+2}, F_{d+1}) \equiv (1, 1) \pmod{m} \implies F_d \equiv F_{d+2} - F_{d+1} \equiv 0 \pmod{m}.$$

We know $F_d \mid F_{qd}$, hence $F_{qd} \equiv 0 \pmod{m}$ for infinite values of q.

2.65 Let the number of consecutive integers be n and $1 \leq k \leq n$ be the erased number. The smallest possible arithmetic mean occurs when $k = n$ is removed, giving an average of $\frac{n}{2}$. The largest occurs when $k = 1$ is removed, giving an average of $\frac{n+2}{2}$. We have the inequality

$$\frac{n}{2} \leq 35\frac{7}{17} \leq \frac{n+2}{2} \implies n \leq 70\frac{14}{17} \leq n+2.$$

Since we average $n-1$ numbers after removing one, $17 \mid n-1$, hence $n = 69$. Therefore,

$$\frac{1/2 \cdot 69 \cdot 70 - k}{68} = 35\frac{7}{17} \implies k = \boxed{7}.$$

2.66 Let S_n denote the numbers ≤ 1000 divisible by n. We divide the numbers into five sets:

$$\{1\},\ \{S_2\},\ \{S_3\},\ \{S_5\},\ \{\text{primes not including } 2, 3, 5\},\ \{\text{prime-looking}\}.$$

By complimentary counting, the number of prime-looking numbers is $1000 - 165 - 1 - |S_2 \cup S_3 \cup S_5|$. Notice that $2, 3$, and 5 are prime. We calculate $S_2 \cup S_3 \cup S_5$ using PIE:

$$\begin{aligned}|S_2 \cup S_3 \cup S_5| &= \lfloor\frac{1000}{2}\rfloor + \lfloor\frac{1000}{3}\rfloor + \lfloor\frac{1000}{5}\rfloor - \lfloor\frac{1000}{6}\rfloor - \lfloor\frac{1000}{10}\rfloor - \lfloor\frac{1000}{15}\rfloor + \lfloor\frac{1000}{30}\rfloor \\ &= 500 + 333 + 200 - 166 - 100 - 66 + 33 = 734.\end{aligned}$$

The number of prime-looking numbers is hence $1000 - 165 - 1 - 734 = \boxed{100}$.

Challenge Problems

2.68 (a) Observe that $2^{16} = 65536 \equiv 154 \pmod{641}$. Therefore,

$$2^{32} + 1 = 65536^2 + 1 \equiv 154^2 + 1 = 23717 = 641 \cdot 37 \equiv 0 \pmod{641}.$$

An alternative proof involves manipulating the equation $641 = 2^7 \cdot 5 + 1 = 2^4 + 5^4$.

(b) Suppose $n = 2^r \cdot s$ for some nonnegative integer r and positive odd integer $s > 1$. Then,

$$2^n + 1 = \left(2^{2^r}\right)^s + 1 = \left(2^{2^r} + 1\right)\left(2^{2^r\cdot(s-1)} - \cdots + 2^{2^r\cdot 2} - 2^{2^r} + 1\right).$$

However, then $2^n + 1$ is composite. Thus, n cannot have an odd prime factor, so $n = 2^r$.

2.69 The three-digit binary numbers are $100_2, 101_2, 110_2$, and 111_2. After the first digit, the rest of the digits are evenly split between zeros and ones, hence there are $2 \cdot \frac{1}{2} \cdot 2^2 = 4$ zeros. In general, for an m-digit binary number, there are $m-1$ digits after the initial 1 for a total of 2^{m-1} integers. The proportion of zeroes for every digit is $\frac{1}{2}$, hence we have $(m-1) \cdot \frac{1}{2} \cdot 2^{m-1}$ zeros in total. Therefore,

$$S_{255} = 1 \cdot 1 + 2 \cdot 2 + 3 \cdot 4 + 4 \cdot 8 + 5 \cdot 16 + 6 \cdot 32 + 7 \cdot 64 = 769.$$

Adding the 8 zeroes in 256, our answer is $S_{256} = 769 + 8 = \boxed{777}$.

2.70 Note 9^{4000} has 3816 more digits than 9^0. Furthermore, 9^n has one more digit than 9^{n-1} except in the case that 9^n starts with a 9 (implying 9^{n-1} starts with a 1). Hence, computing 9^n from 9^{n-1} for $1 \leq n \leq 4000$, there are $4000 - 3816 = \boxed{184}$ instances when the digits do not increase. Since $9^0 = 1$, this is exactly the number of elements of T with leading digit 9.

2.71 For every positive integer n, $f(n) \equiv n \pmod{9}$. Therefore,

$$f(f(f(n))) \equiv f(f(n)) \equiv f(n) \equiv n \pmod{9}.$$

We desire to compute $4444^{4444} \pmod{9}$. Since $4444 \equiv 7 \pmod{9}$ and $7^3 \equiv 1 \pmod{9}$,

$$4444^{4444} \equiv 7^{4444} \equiv 7^1 \equiv 7 \pmod{9}.$$

Notice $4444^{4444} < 10^{4 \cdot 4444} = 10^{17776}$. Therefore, 4444^{4444} has at most 17776 digits, so

$$f(n) < 9 \cdot 17776 = 159984.$$

Furthermore, $f(f(n))$ is maximized when $f(n) = 99999$ giving $f(f(n)) = 9 \cdot 5 = 45$. Finally, $f(f(f(n))) \leq f(39) = 12$. Since $f(f(f(n))) \equiv 7 \pmod{9}$, we must have $f(f(f(N))) = \boxed{7}$.

2.72 Let $n = d_k d_{k-1} \cdots d_2 d_1 d_0 = \sum_{i=0}^{k} 10^i d_i$, where d_i are the digits of n. Observe that the result of removing the first m digits is $U_m(n) = \sum_{i=m}^{k} 10^{i-m} d_i$. Therefore,

$$T(n) = \sum_{m=1}^{k} U_m(n) = \sum_{m=1}^{k} \sum_{i=m}^{k} 10^{i-m} d_i.$$

By the geometric series formula, the coefficient of an arbitrary digit d_j is

$$10^{j-1} + 10^{j-2} + \cdots + 10 + 1 = \frac{10^j - 1}{9}.$$

Therefore, $T(n) = \displaystyle\sum_{j=0}^{k} \left(\frac{10^j - 1}{9} \right) d_j$. Finally, we see that

$$S(n) + 9T(n) = \sum_{j=0}^{k} \left(1 + 9 \cdot \frac{10^j - 1}{9} \right) d_j = \sum_{j=0}^{k} 10^j d_j = n.$$

2.73 We begin by proving that for integers m and n, $m - n \mid P(m) - P(n)$.

Proof. Let $P(x) = a_r x^r + a_{r-1} x^{r-1} + \cdots + a_1 x + a_0$. Then,

$$\begin{aligned} P(m) - P(n) &= \left(a_r m^r + a_{r-1} m^{r-1} + \cdots + a_1 m + a_0\right) - \left(a_r n^r + a_{r-1} n^{r-1} + \cdots + a_1 n + a_0\right) \\ &= a_r \left(m^r - n^r\right) + a_{r-1} \left(m^{r-1} - n^{r-1}\right) + \cdots + a_1 \left(m - n\right). \end{aligned}$$

Since $m - n \mid m^s - n^s$ for all exponents s, the identity is established. □

Assume for the sake of contradiction there exists such a polynomial. Then,

$$a - b \mid P(a) - P(b) = b - c \mid P(b) - P(c) = c - a \mid P(c) - P(a) = a - b.$$

Therefore $|a - b| = |b - c| = |c - a| = k$ for some constant k. However,

$$0 = (a - b) + (b - c) + (c - a) = mk,$$

where m is one of $-3, -1, 1$, or 3. Hence $k = 0$, implying $a = b = c$, contradiction.

2.74 Assume that $2^b - 1 \mid 2^a + 1$ for some integer pair (a, b). Since $a > b > 2$, we write $a = bq + r$, where $0 \leq r \leq b - 1$ using the division algorithm. Furthermore, $2^b \equiv 1 \pmod{2^b - 1}$, therefore

$$2^a \equiv 2^{bq} 2^r \equiv 2^r \equiv -1 \pmod{2^b - 1} \implies 2^b - 1 \mid 2^r + 1.$$

However, $2^r + 1 \leq 2^{b-1} + 1 < 2^b - 1$ for $b > 2$, therefore, this is a contradiction.

2.75 Set $x = a - 1, y = b - 1$, and $z = c - 1$ where $1 \leq x \leq y \leq z$. Therefore,

$$(x+1)(y+1)(z+1) - 1 = xyz + yz + xz + xy + z + y + x.$$

Let $f(x, y, z)$ be the quotient of divisibility. Expanding and simplifying, we see that

$$f(x, y, z) = \frac{yz + xz + xy + z + y + x}{xyz} = \frac{1}{x} + \frac{1}{y} + \frac{1}{z} + \frac{1}{xy} + \frac{1}{xz} + \frac{1}{yz}.$$

Furthermore, f is decreasing in the variables x, y, z, hence the maximum value is

$$f(1, 2, 3) = 2\frac{5}{6} \implies f(x, y, z) \in \{1, 2\}.$$

Furthermore, $f(3, 4, 5) = \frac{59}{60} < 1$, therefore x is either 1 or 2. We finish with casework.
If $x = 1$, then $f(1, y, z) = 1 + \frac{1}{y} + \frac{1}{z} + \frac{1}{y} + \frac{1}{z} + \frac{1}{yz} = 2$. Multiplying by yz and using SFFT,

$$yz = 2y + 2z + 1 \implies (y - 2)(z - 2) = 5 \implies (y, z) = (3, 7).$$

If $x = 2$, since $f(2, 3, 4) = \frac{35}{24} < 2$, we must have

$$f(2, y, z) = \frac{1}{2} + \frac{1}{y} + \frac{1}{z} + \frac{1}{2y} + \frac{1}{2z} + \frac{1}{yz} = 1.$$

Multiplying by $2yz$ and simplifying using Simon's Favourite Factoring Trick,

$$yz = 3y + 3z + 2 \implies (y - 3)(z - 3) = 11 \implies (y, z) = (4, 14).$$

Adding 1 to the triples found above gives $(a, b, c) = \boxed{(2, 4, 8), (3, 5, 15)}$.

2.76 We find a linear combination of $xy^2 + y + 7$ and $x^2y + x + y$ that cancels several terms:

$$y\left(x^2y + x + y\right) - x\left(xy^2 + y + 7\right) = y^2 - 7x.$$

Hence $xy^2 + y + 7 \mid y^2 - 7x$. Since the LHS is positive, we have three cases:

- $y^2 - 7x > 0$. We arrive at a contradiction since $xy^2 + y + 7 > y^2 > y^2 - 7x$.
- $y^2 - 7x = 0$. We have the solution $(x, y) = \boldsymbol{(7m^2, 7m)}$ for some positive integer m.
- $y^2 - 7x < 0$. Since $7x - y^2$ is positive, we multiply by -1:

$$xy^2 + y + 7 \mid y^2 - 7x \implies xy^2 + y + 7 \mid 7x - y^2.$$

Now, $xy^2 + y + 7 \leq 7x - y^2$. Comparing the coefficient of x shows $y^2 \leq 7 \implies y = 1, 2$.

  - If $y = 1$, then $x + 8 \mid 7x - 1$. Since $7\,(x + 8) - (7x - 1) = 57$, we see $x + 8 \mid 57$. The divisors of 57 are $1, 3, 19, 57$, so $x = 11$ or $x = 49$ yielding $(x, y) = \mathbf{(11, 1), (49, 1)}$.
  - If $y = 2$, then $4x + 9 \mid 7x - 4$. However, $2(4x + 9) = 8x + 18 > 7x - 4$, therefore, the quotient must be 1. However, $4x + 9 = 7x - 4$ has no integer solutions.

The solutions are hence $(x, y) = \boxed{(11, 1), (49, 1), (7m^2, 7m)}$.

2.77 Assume neither sequence exists. We poset the sequence using the ordering

$$a_m \prec a_n \;\leftrightarrow\; a_m < a_n, a_m \mid a_n.$$

Define a function $f : \mathcal{N}_{mn+1} \to \mathcal{N}_m \times \mathcal{N}_n$ with $f(t) = (x_t, y_t)$, where x_t is the largest chain beginning with a_t, while y_t is the largest decreasing anti-chain beginning with a_t. There are mn possible values of f, hence by the pigeonhole principle, there exists indices $j < k$ with $f(j) = f(k)$.

However, if $a_j \mid a_k$, then $x_j \geq x_k + 1$. Otherwise, if $a_j \nmid a_k$, then $a_k \succ a_j$, hence $y_k \geq y_j + 1$. Both inequalities contradict $f(j) = f(k)$, therefore, our original assumption was false. Hence, we can find either a chain of length $m + 1$ or an anti-chain of length $n + 1$.

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/.