Number Theory for Mathematical Contests

David A. SANTOS
dsantos@ccp.edu

August 13, 2005 REVISION

Contents

Preface

These notes started in the summer of 1993 when I was teaching Number Theory at the Center for Talented Youth Summer Program at the Johns Hopkins University. The pupils were between 13 and 16 years of age.

The purpose of the course was to familiarise the pupils with contest-type problem solving. Thus the majority of the problems are taken from well-known competitions:

AHSME	American High School Mathematics Examination
AIME	American Invitational Mathematics Examination
USAMO	United States Mathematical Olympiad
IMO	International Mathematical Olympiad
ITT	International Tournament of Towns
MMPC	Michigan Mathematics Prize Competition
$(UM)^2$	University of Michigan Mathematics Competition
Stanford	Stanford Mathematics Competition
Mandelbrot	Mandelbrot Competition

Firstly, I would like to thank the pioneers in that course: Samuel Chong, Nikhil Garg, Matthew Harris, Ryan Hoegg, Masha Sapper, Andrew Trister, Nathaniel Wise and Andrew Wong. I would also like to thank the victims of the summer 1994: Karen Acquista, Howard Bernstein, Geoffrey Cook, Hobart Lee, Nathan Lutchansky, David Ripley, Eduardo Rozo, and Victor Yang.

I would like to thank Eric Friedman for helping me with the typing, and Carlos Murillo for proofreading the notes.

Due to time constraints, these notes are rather sketchy. Most of the motivation was done in the classroom, in the notes I presented a rather terse account of the solutions. I hope some day to be able to give more coherence to these notes. No theme requires the knowledge of Calculus here, but some of the solutions given use it here and there. The reader not knowing Calculus can skip these problems. Since the material is geared to High School students (talented ones, though) I assume very little mathematical knowledge beyond Algebra and Trigonometry. Here and there some of the problems might use certain properties of the complex numbers.

A note on the topic selection. I tried to cover most Number Theory that is useful in contests. I also wrote notes (which I have not transcribed) dealing with primitive roots, quadratic reciprocity, diophantine equations, and the geometry of numbers. I shall finish writing them when laziness leaves my weary soul.

I would be very glad to hear any comments, and please forward me any corrections or remarks on the material herein.

David A. SANTOS
dsantos@ccp.edu

Legal Notice

This material may be distributed only subject to the terms and conditions set forth in the Open Publication License, version 1.0 or later (the latest version is presently available at

http://www.opencontent.org/openpub/ .

THIS WORK IS LICENSED AND PROVIDED “AS IS” WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE OR A WARRANTY OF NON-INFRINGEMENT.

THIS DOCUMENT MAY NOT BE SOLD FOR PROFIT OR INCORPORATED INTO COMMERCIAL DOCUMENTS WITHOUT EXPRESS PERMISSION FROM THE AUTHOR(S). THIS DOCUMENT MAY BE FREELY DISTRIBUTED PROVIDED THE NAME OF THE ORIGINAL AUTHOR(S) IS(ARE) KEPT AND ANY CHANGES TO IT NOTED.

Chapter 1

Preliminaries

1.1 Introduction

We can say that no history of mankind would ever be complete without a history of Mathematics. For ages numbers have fascinated Man, who has been drawn to them either for their utility at solving practical problems (like those of measuring, counting sheep, etc.) or as a fountain of solace.

Number Theory is one of the oldest and most beautiful branches of Mathematics. It abounds in problems that yet simple to state, are very hard to solve. Some number-theoretic problems that are yet unsolved are:

1. (Goldbach's Conjecture) Is every even integer greater than 2 the sum of distinct primes?
2. (Twin Prime Problem) Are there infinitely many primes p such that $p+2$ is also a prime?
3. Are there infinitely many primes that are 1 more than the square of an integer?
4. Is there always a prime between two consecutive squares of integers?

In this chapter we cover some preliminary tools we need before embarking into the core of Number Theory.

1.2 Well-Ordering

The set $\mathbb{N} = \{0,1,2,3,4,\ldots\}$ of natural numbers is endowed with two operations, addition and multiplication, that satisfy the following properties for natural numbers a, b, and c:

1. **Closure:** $a+b$ and ab are also natural numbers.
2. **Associative laws:** $(a+b)+c = a+(b+c)$ and $a(bc) = (ab)c$.
3. **Distributive law:** $a(b+c) = ab+ac$.
4. **Additive Identity:** $0+a = a+0 = a$
5. **Multiplicative Identity:** $1a = a1 = a$.

One further property of the natural numbers is the following.

1 Axiom (Well-Ordering Axiom) Every non-empty subset $\mathscr{S}$ of the natural numbers has a least element.

As an example of the use of the Well-Ordering Axiom, let us prove that there is no integer between 0 and 1.

2 Example Prove that there is no integer in the interval $]0;1[$.

Solution: Assume to the contrary that the set $\mathscr{S}$ of integers in $]0;1[$ is non-empty. Being a set of positive integers, it must contain a least element, say m. Now, $0 < m^2 < m < 1$, and so $m^2 \in \mathscr{S}$. But this is saying that $\mathscr{S}$ has a positive integer m^2 which is smaller than its least positive integer m. This is a contradiction and so $\mathscr{S} = \varnothing$.

We denote the set of all integers by $\mathbb{Z}$, i.e.,

$$\mathbb{Z} = \{\ldots -3, -2, -1, 0, 1, 2, 3, \ldots\}.$$

A rational number is a number which can be expressed as the ratio $\frac{a}{b}$ of two integers a, b, where $b \neq 0$. We denote the set of rational numbers by $\mathbb{Q}$. An **irrational number** is a number which cannot be expressed as the ratio of two integers. Let us give an example of an irrational number.

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

Solution: The proof is by contradiction. Suppose that $\sqrt{2}$ were rational, i.e., that $\sqrt{2} = \frac{a}{b}$ for some integers a, b. This implies that the set

$$\mathscr{A} = \{n\sqrt{2} : \text{ both } n \text{ and } n\sqrt{2} \text{ positive integers}\}$$

is nonempty since it contains a. By Well-Ordering $\mathscr{A}$ has a smallest element, say $j = k\sqrt{2}$. As $\sqrt{2} - 1 > 0$,

$$j(\sqrt{2} - 1) = j\sqrt{2} - k\sqrt{2} = (j - k)\sqrt{2}$$

is a positive integer. Since $2 < 2\sqrt{2}$ implies $2 - \sqrt{2} < \sqrt{2}$ and also $j\sqrt{2} = 2k$, we see that

$$(j - k)\sqrt{2} = k(2 - \sqrt{2}) < k(\sqrt{2}) = j.$$

Thus $(j - k)\sqrt{2}$ is a positive integer in $\mathscr{A}$ which is smaller than j. This contradicts the choice of j as the smallest integer in $\mathscr{A}$ and hence, finishes the proof.

4 Example Let a, b, c be integers such that $a^6 + 2b^6 = 4c^6$. Show that $a = b = c = 0$.

Solution: Clearly we can restrict ourselves to nonnegative numbers. Choose a triplet of nonnegative integers a, b, c satisfying this equation and with

$$\max(a, b, c) > 0$$

as small as possible. If $a^6 + 2b^6 = 4c^6$ then a must be even, $a = 2a_1$. This leads to $32a_1^6 + b^6 = 2c^6$. Hence $b = 2b_1$ and so $16a_1^6 + 32b_1^6 = c^6$. This gives $c = 2c_1$, and so $a_1^6 + 2b_1^6 = 4c_1^6$. But clearly $\max(a_1, b_1, c_1) < \max(a, b, c)$. This means that all of these must be zero.

5 Example (IMO 1988) If a, b are positive integers such that $\dfrac{a^2 + b^2}{1 + ab}$ is an integer, then $\dfrac{a^2 + b^2}{1 + ab}$ is a perfect square.

Solution: Suppose that $\dfrac{a^2 + b^2}{1 + ab} = k$ is a counterexample of an integer which is not a perfect square, with $\max(a, b)$ as small as possible. We may assume without loss of generality that $a < b$ for if $a = b$ then

$$0 < k = \frac{2a^2}{a^2 + 1} < 2,$$

which forces $k = 1$, a perfect square.

Now, $a^2 + b^2 - k(ab + 1) = 0$ is a quadratic in b with sum of the roots ka and product of the roots $a^2 - k$. Let b_1, b be its roots, so $b_1 + b = ka$ and $b_1 b = a^2 - k$.

As a, k are positive integers, supposing $b_1 < 0$ is incompatible with $a^2 + b_1^2 = k(ab_1 + 1)$. As k is not a perfect square, supposing $b_1 = 0$ is incompatible with $a^2 + 0^2 = k(0 \cdot a + 1)$. Also

$$b_1 = \frac{a^2 - k}{b} < \frac{b^2 - k}{b} < b.$$

Thus we have found another positive integer b_1 for which $\dfrac{a^2+b_1^2}{1+ab_1} = k$ and which is smaller than the smallest $\max(a,b)$. This is a contradiction. It must be the case, then, that k is a perfect square.

Practice

6 Problem Find all integer solutions of $a^3+2b^3=4c^3$.

7 Problem Prove that the equality $x^2+y^2+z^2=2xyz$ can hold for whole numbers x,y,z only when $x=y=z=0$.

1.3 Mathematical Induction

The Principle of Mathematical Induction is based on the following fairly intuitive observation. Suppose that we are to perform a task that involves a certain number of steps. Suppose that these steps must be followed in strict numerical order. Finally, suppose that we know how to perform the n-th task provided we have accomplished the $n-1$-th task. Thus if we are ever able to start the job (that is, if we have a base case), then we should be able to finish it (because starting with the base case we go to the next case, and then to the case following that, etc.).

Thus in the Principle of Mathematical Induction, we try to verify that some assertion $P(n)$ concerning natural numbers is true for some base case k_0 (usually $k_0=1$, but one of the examples below shows that we may take, say $k_0=33$.) Then we try to settle whether information on $P(n-1)$ leads to favourable information on $P(n)$.

We will now derive the Principle of Mathematical Induction from the Well-Ordering Axiom.

8 Theorem (Principle of Mathematical Induction) If a set$\mathscr{S}$ of non-negative integers contains the integer 0, and also contains the integer $n+1$ whenever it contains the integer n, then $\mathscr{S}=\mathbb{N}$.

> **Proof:** *Assume this is not the case and so, by the Well-Ordering Principle there exists a least positive integer k not in $\mathscr{S}$. Observe that $k>0$, since $0\in S$ and there is no positive integer smaller than 0. As $k-1<k$, we see that $k-1\in\mathscr{S}$. But by assumption $k-1+1$ is also in $\mathscr{S}$, since the successor of each element in the set is also in the set. Hence $k=k-1+1$ is also in the set, a contradiction. Thus $\mathscr{S}=\mathbb{N}$.* ❑

The following versions of the Principle of Mathematical Induction should now be obvious.

9 Corollary If a set $\mathscr{A}$ of positive integers contains the integer m and also contains $n+1$ whenever it contains n, where $n>m$, then $\mathscr{A}$ contains all the positive integers greater than or equal to m.

10 Corollary (Principle of Strong Mathematical Induction) If a set $\mathscr{A}$ of positive integers contains the integer m and also contains $n+1$ whenever it contains $m+1, m+2, \ldots, n$, where $n>m$, then $\mathscr{A}$ contains all the positive integers greater than or equal to m.

We shall now give some examples of the use of induction.

11 Example Prove that the expression

$$3^{3n+3}-26n-27$$

is a multiple of 169 for all natural numbers n.

Solution: For $n=1$ we are asserting that $3^6-53=676=169\cdot 4$ is divisible by 169, which is evident. Assume the assertion is true for $n-1, n>1$, i.e., assume that

$$3^{3n}-26n-1=169N$$

for some integer N. Then

$$3^{3n+3}-26n-27=27\cdot 3^{3n}-26n-27=27(3^{3n}-26n-1)+676n$$

which reduces to

$$27\cdot 169N+169\cdot 4n,$$

which is divisible by 169. The assertion is thus established by induction.

12 Example Prove that

$$(1+\sqrt{2})^{2n}+(1-\sqrt{2})^{2n}$$

is an even integer and that

$$(1+\sqrt{2})^{2n}-(1-\sqrt{2})^{2n}=b\sqrt{2}$$

for some positive integer b, for all integers $n\geq 1$.

Solution: We proceed by induction on n. Let $P(n)$ be the proposition: "$(1+\sqrt{2})^{2n}+(1-\sqrt{2})^{2n}$ is even and $(1+\sqrt{2})^{2n}-(1-\sqrt{2})^{2n}=b\sqrt{2}$ for some $b\in\mathbb{N}$." If $n=1$, then we see that

$$(1+\sqrt{2})^{2}+(1-\sqrt{2})^{2}=6,$$

an even integer, and

$$(1+\sqrt{2})^{2}-(1-\sqrt{2})^{2}=4\sqrt{2}.$$

Therefore $P(1)$ is true. Assume that $P(n-1)$ is true for $n>1$, i.e., assume that

$$(1+\sqrt{2})^{2(n-1)}+(1-\sqrt{2})^{2(n-1)}=2N$$

for some integer N and that

$$(1+\sqrt{2})^{2(n-1)}-(1-\sqrt{2})^{2(n-1)}=a\sqrt{2}$$

for some positive integer a.

Consider now the quantity

$$(1+\sqrt{2})^{2n}+(1-\sqrt{2})^{2n}=(1+\sqrt{2})^{2}(1+\sqrt{2})^{2n-2}+(1-\sqrt{2})^{2}(1-\sqrt{2})^{2n-2}.$$

This simplifies to

$$(3+2\sqrt{2})(1+\sqrt{2})^{2n-2}+(3-2\sqrt{2})(1-\sqrt{2})^{2n-2}.$$

Using $P(n-1)$, the above simplifies to

$$12N+2\sqrt{2}a\sqrt{2}=2(6N+2a),$$

an even integer and similarly

$$(1+\sqrt{2})^{2n}-(1-\sqrt{2})^{2n}=3a\sqrt{2}+2\sqrt{2}(2N)=(3a+4N)\sqrt{2},$$

and so $P(n)$ is true. The assertion is thus established by induction.

13 Example Prove that if k is odd, then 2^{n+2} divides

$$k^{2^n}-1$$

for all natural numbers n.

Solution: The statement is evident for $n=1$, as $k^2-1=(k-1)(k+1)$ is divisible by 8 for any odd natural number k because both $(k-1)$ and $(k+1)$ are divisible by 2 and one of them is divisible by 4. Assume that $2^{n+2}|k^{2^n}-1$, and let us prove that $2^{n+3}|k^{2^{n+1}}-1$. As $k^{2^{n+1}}-1=(k^{2^n}-1)(k^{2^n}+1)$, we see that 2^{n+2} divides $(k^{2n}-1)$, so the problem reduces to proving that $2|(k^{2n}+1)$. This is obviously true since k^{2n} odd makes $k^{2n}+1$ even.

14 Example (USAMO 1978) An integer n will be called *good* if we can write

$$n = a_1 + a_2 + \cdots + a_k,$$

where $a_1, a_2, \ldots, a_k$ are positive integers (not necessarily distinct) satisfying

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

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

Solution: We first prove that if n is good, then $2n+8$ and $2n+9$ are good. For assume that $n = a_1 + a_2 + \cdots + a_k$, and

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

Then $2n+8 = 2a_1 + 2a_2 + \cdots + 2a_k + 4 + 4$ and

$$\frac{1}{2a_1} + \frac{1}{2a_2} + \cdots + \frac{1}{2a_k} + \frac{1}{4} + \frac{1}{4} = \frac{1}{2} + \frac{1}{4} + \frac{1}{4} = 1.$$

Also, $2n+9 = 2a_1 + 2a_2 + \cdots + 2a_k + 3 + 6$ and

$$\frac{1}{2a_1} + \frac{1}{2a_2} + \cdots + \frac{1}{2a_k} + \frac{1}{3} + \frac{1}{6} = \frac{1}{2} + \frac{1}{3} + \frac{1}{6} = 1.$$

Therefore,

$$\text{if } n \text{ is good both } 2n+8 \text{ and } 2n+9 \text{ are good.} \tag{1.1}$$

We now establish the truth of the assertion of the problem by induction on n. Let $P(n)$ be the proposition "all the integers $n, n+1, n+2, \ldots, 2n+7$" are good. By the statement of the problem, we see that $P(33)$ is true. But (1.1) implies the truth of $P(n+1)$ whenever $P(n)$ is true. The assertion is thus proved by induction.

We now present a variant of the Principle of Mathematical Induction used by Cauchy to prove the Arithmetic-Mean-Geometric Mean Inequality. It consists in proving a statement first for powers of 2 and then interpolating between powers of 2.

15 Theorem (Arithmetic-Mean-Geometric-Mean Inequality) Let $a_1, a_2, \ldots, a_n$ be nonnegative real numbers. Then

$$\sqrt[n]{a_1 a_2 \cdots a_n} \leq \frac{a_1 + a_2 + \cdots + a_n}{n}.$$

Proof: *Since the square of any real number is nonnegative, we have*

$$(\sqrt{x_1} - \sqrt{x_2})^2 \geq 0.$$

Upon expanding,

$$\frac{x_1 + x_2}{2} \geq \sqrt{x_1 x_2}, \tag{1.2}$$

which is the Arithmetic-Mean-Geometric-Mean Inequality for $n = 2$. Assume that the Arithmetic-Mean-Geometric-Mean Inequality holds true for $n = 2^{k-1}, k > 2$, that is, assume that nonnegative real numbers $w_1, w_2, \ldots, w_{2^{k-1}}$ satisfy

$$\frac{w_1 + w_2 + \cdots + w_{2^{k-1}}}{2^{k-1}} \geq (w_1 w_2 \cdots w_{2^{k-1}})^{1/2^{k-1}}. \tag{1.3}$$

Using (1.2) with

$$x_1 = \frac{y_1 + y_2 + \cdots + y_{2^{k-1}}}{2^{k-1}}$$

and

$$x_2 = \frac{y_{2^{k-1}+1} + \cdots + y_{2^k}}{2^{k-1}},$$

we obtain that

$$\frac{\frac{y_1+y_2+\cdots+y_{2^{k-1}}}{2^{k-1}}+\frac{y_{2^{k-1}+1}+\cdots+y_{2^k}}{2^{k-1}}}{2} \geq \left((\frac{y_1+y_2+\cdots+y_{2^{k-1}}}{2^{k-1}})(\frac{y_{2^{k-1}+1}+\cdots+y_{2^k}}{2^{k-1}})\right)^{1/2}.$$

Applying (1.3) to both factors on the right hand side of the above , we obtain

$$\frac{y_1+y_2+\cdots+y_{2^k}}{2^k} \geq (y_1y_2\cdots y_{2^k})^{1/2^k}. \tag{1.4}$$

This means that the 2^{k-1}-th step implies the 2^k-th step, and so we have proved the Arithmetic-Mean-Geometric-Mean Inequality for powers of 2.

Now, assume that $2^{k-1} < n < 2^k$. Let

$$y_1 = a_1, y_2 = a_2, \ldots, y_n = a_n,$$

and

$$y_{n+1} = y_{n+2} = \cdots = y_{2^k} = \frac{a_1+a_2+\cdots+a_n}{n}.$$

Let

$$A = \frac{a_1+\cdots+a_n}{n} \text{ and } G = (a_1\cdots a_n)^{1/n}.$$

Using (1.4) we obtain

$$\frac{a_1+a_2+\cdots+a_n+(2^k-n)\frac{a_1+\cdots+a_n}{n}}{2^k} \geq \left(a_1a_2\cdots a_n(\frac{a_1+\cdots+a_n}{n})^{(2^k-n)}\right)^{1/2^k},$$

which is to say that

$$\frac{nA+(2^k-n)A}{2^k} \geq (G^nA^{2^k-n})^{1/2^k}.$$

This translates into $A \geq G$ or

$$(a_1a_2\cdots a_n)^{1/n} \leq \frac{a_1+a_2+\cdots+a_n}{n},$$

which is what we wanted.❑

16 Example Let s be a positive integer. Prove that every interval $[s;2s]$ contains a power of 2.

Solution: If s is a power of 2, then there is nothing to prove. If s is not a power of 2 then it must lie between two consecutive powers of 2, i.e., there is an integer r for which $2^r < s < 2^{r+1}$. This yields $2^{r+1} < 2s$. Hence $s < 2^{r+1} < 2s$, which gives the required result.

17 Example Let $\mathscr{M}$ be a nonempty set of positive integers such that $4x$ and $[\sqrt{x}]$ both belong to $\mathscr{M}$ whenever x does. Prove that $\mathscr{M}$ is the set of all natural numbers.

Solution: We will prove this by induction. First we will prove that 1 belongs to the set, secondly we will prove that every power of 2 is in the set and finally we will prove that non-powers of 2 are also in the set.

Since $\mathscr{M}$ is a nonempty set of positive integers, it has a least element, say a. By assumption $\llbracket\sqrt{a}\rrbracket$ also belongs to $\mathscr{M}$, but $\sqrt{a} < a$ unless $a = 1$. This means that 1 belongs to $\mathscr{M}$.

Since 1 belongs to $\mathscr{M}$ so does 4, since 4 belongs to $\mathscr{M}$ so does $4\cdot 4 = 4^2$, etc.. In this way we obtain that all numbers of the form $4^n = 2^{2n}, n = 1, 2, \ldots$ belong to $\mathscr{M}$. Thus all the powers of 2 raised to an even power belong to $\mathscr{M}$. Since the square roots belong as well to $\mathscr{M}$ we get that all the powers of 2 raised to an odd power also belong to $\mathscr{M}$. In conclusion, all powers of 2 belong to $\mathscr{M}$.

Assume now that $n \in \mathbb{N}$ fails to belong to $\mathscr{M}$. Observe that n cannot be a power of 2. Since $n \notin M$ we deduce that no integer in $A_1 = [n^2, (n+1)^2)$ belongs to $\mathscr{M}$, because every member of $y \in A_1$ satisfies $[\sqrt{y}] = n$. Similarly no member $z \in A_2 = [n^4, (n+1)^4)$ belongs to $\mathscr{M}$ since this would entail that z would belong to A_1, a contradiction. By induction we can show that no member in the interval $A_r = [n^{2^r}, (n+1)^{2^r})$ belongs to $\mathscr{M}$.

We will now show that eventually these intervals are so large that they contain a power of 2, thereby obtaining a contradiction to the hypothesis that no element of the A_r belonged to $\mathscr{M}$. The function

$$f: \begin{array}{ccc} \mathbb{R}_+^* & \rightarrow & \mathbb{R} \\ x & \mapsto & \log_2 x \end{array}$$

is increasing and hence $\log_2(n+1) - \log_2 n > 0$. Since the function

$$f: \begin{array}{ccc} \mathbb{R} & \rightarrow & \mathbb{R}_+^* \\ x & \mapsto & 2^{-x} \end{array}$$

is decreasing, for a sufficiently large positive integer k we have

$$2^{-k} < \log_2(n+1) - \log_2 n.$$

This implies that

$$(n+1)^{2^k} > 2n^{2^k}.$$

Thus the interval $[n^{2^k}, 2n^{2^k}]$ is totally contained in $[n^{2^k}, (n+1)^{2^k})$. But every interval of the form $[s, 2s]$ where s is a positive integer contains a power of 2. We have thus obtained the desired contradiction.

Practice

18 Problem Prove that $11^{n+2} + 12^{2n+1}$ is divisible by 133 for all natural numbers n.

19 Problem Prove that

$$1 - \frac{x}{1!} + \frac{x(x-1)}{2!} - \frac{x(x-1)(x-2)}{3!}$$
$$+ \cdots + (-1)^n \frac{x(x-1)(x-2)\cdots(x-n+1)}{n!}$$

equals

$$(-1)^n \frac{(x-1)(x-2)\cdots(x-n)}{n!}$$

for all non-negative integers n.

20 Problem Let $n \in \mathbb{N}$. Prove the inequality

$$\frac{1}{n+1} + \frac{1}{n+2} + \cdots + \frac{1}{3n+1} > 1.$$

21 Problem Prove that

$$\underbrace{\sqrt{2+\sqrt{2+\cdots+\sqrt{2}}}}_{n \text{ radical signs}} = 2\cos\frac{\pi}{2^{n+1}}$$

for $n \in \mathbb{N}$.

22 Problem Let $a_1 = 3, b_1 = 4$, and $a_n = 3^{a_{n-1}}, b_n = 4^{b_{n-1}}$ when $n > 1$. Prove that $a_{1000} > b_{999}$.

23 Problem Let $n \in \mathbb{N}, n > 1$. Prove that

$$\frac{1 \cdot 3 \cdot 5 \cdots (2n-1)}{2 \cdot 4 \cdot 6 \cdots (2n)} < \frac{1}{\sqrt{3n+1}}.$$

24 Problem Prove that if n is a natural number, then

$$1 \cdot 2 + 2 \cdot 5 + \cdots + n \cdot (3n-1) = n^2(n+1).$$

25 Problem Prove that if n is a natural number, then

$$1^2 + 3^2 + 5^2 + \cdots + (2n-1)^2 = \frac{n(4n^2-1)}{3}.$$

26 Problem Prove that

$$\frac{4^n}{n+1} < \frac{(2n)!}{(n!)^2}$$

for all natural numbers $n > 1$.

27 Problem Prove that the sum of the cubes of three consecutive positive integers is divisible by 9.

28 Problem If $|x| \neq 1, n \in \mathbb{N}$ prove that

$$\frac{1}{1+x} + \frac{2}{1+x^2} + \frac{4}{1+x^2} + \frac{8}{1+x^8} + \cdots + \frac{2^n}{1+x^{2^n}}$$

equals

$$\frac{1}{x-1} + \frac{2^{n+1}}{1-x^{2^{n+1}}}.$$

29 Problem Is it true that for every natural number n the quantity n^2+n+41 is a prime? Prove or disprove!

30 Problem Give an example of an assertion which is *not* true for any positive integer, yet for which the induction step holds.

31 Problem Give an example of an assertion which is true for the first two million positive integers but fails for every integer greater than 2000000.

32 Problem Prove by induction on n that a set having n elements has exactly 2^n subsets.

33 Problem Prove that if n is a natural number,

$$n^5/5+n^4/2+n^3/3-n/30$$

is always an integer.

34 Problem (Halmos)) Every man in a village knows instantly when another's wife is unfaithful, but never when his own is. Each man is completely intelligent and knows that every other man is. The law of the village demands that when a man can PROVE that his wife has been unfaithful, he must shoot her before sundown the same day. Every man is completely law-abiding. One day the mayor announces that there is at least one unfaithful wife in the village. The mayor always tells the truth, and every man believes him. If in fact there are exactly forty unfaithful wives in the village (but that fact is not known to the men,) what will happen after the mayor's announcement?

35 Problem

1. Let $a_1, a_2, \ldots a_n$ be positive real numbers with
$$a_1 \cdot a_2 \cdots a_n = 1.$$
Use induction to prove that
$$a_1 + a_2 + \cdots + a_n \geq n,$$
with equality if and only if $a_1 = a_2 = \cdots = a_n = 1$.
2. Use the preceding part to give another proof of the Arithmetic-Mean-Geometric-Mean Inequality.
3. Prove that if $n > 1$, then
$$1 \cdot 3 \cdot 5 \cdots (2n-1) < n^n.$$
4. Prove that if $n > 1$ then
$$n\left((n+1)^{1/n}-1\right) < 1+\frac{1}{2}+\cdots+\frac{1}{n}.$$
5. Prove that if $n > 1$ then
$$1+\frac{1}{2}+\cdots+\frac{1}{n} < n\left(1-\frac{1}{(n+1)^{1/n}}+\frac{1}{n+1}\right).$$
6. Given that u, v, w are positive, $0 < a \leq 1$, and that $u+v+w=1$, prove that
$$\left(\frac{1}{u}-a\right)\left(\frac{1}{v}-a\right)\left(\frac{1}{w}-a\right) \geq 27-27a+9a^2-a^3.$$
7. Let $y_1, y_2, \ldots, y_n$ be positive real numbers. Prove the *Harmonic-Mean- Geometric-Mean Inequality:*
$$\frac{n}{\frac{1}{y_1}+\frac{1}{y_2}+\cdots+\frac{1}{y_n}} \leq \sqrt[n]{y_1 y_2 \cdots y_n}.$$
8. Let $a_1, \ldots, a_n$ be positive real numbers, all different. Set $s = a_1 + a_2 + \cdots + a_n$.
    (a) Prove that
    $$(n-1)\sum_{1\leq r\leq n}\frac{1}{s-a_r} < \sum_{1\leq r\leq n}\frac{1}{a_r}.$$
    (b) Deduce that
    $$\frac{4n}{s} < s\sum_{1\leq r\leq n}\frac{1}{a_r(s-a_r)} < \frac{n}{n-1}\sum_{1\leq r\leq n}\frac{1}{a_r}.$$

36 Problem Suppose that $x_1, x_2, \ldots, x_n$ are nonnegative real numbers with

$$x_1 + x_2 + \cdots + x_n \leq 1/2.$$

Prove that

$$(1-x_1)(1-x_2)\cdots(1-x_n) \geq 1/2.$$

37 Problem Given a positive integer n prove that there is a polynomial T_n such that $\cos nx = T_n(\cos x)$ for all real numbers x. T_n is called the n-th *Tchebychev Polynomial*.

38 Problem Prove that

$$\frac{1}{n+1}+\frac{1}{n+2}+\cdots+\frac{1}{2n} > \frac{13}{24}$$

for all natural numbers $n > 1$.

39 Problem In how many regions will a sphere be divided by n planes passing through its centre if no three planes pass through one and the same diameter?

40 Problem (IMO 1977) Let $f, f : \mathbb{N} \mapsto \mathbb{N}$ be a function satisfying

$$f(n+1) > f(f(n))$$

for each positive integer n. Prove that $f(n) = n$ for each n.

41 Problem Let $F_0(x) = x, F(x) = 4x(1-x), F_{n+1}(x) = F(F_n(x)), n = 0, 1, \ldots.$ Prove that

$$\int_0^1 F_n(x)\,dx = \frac{2^{2n-1}}{2^{2n}-1}.$$

(Hint: Let $x = \sin^2\theta$.)

1.4 Fibonacci Numbers

The *Fibonacci numbers* f_n are given by the recurrence

$$f_0 = 0,\ f_1 = 1,\ f_{n+1} = f_{n-1} + f_n,\ n \geq 1. \tag{1.5}$$

Thus the first few Fibonacci numbers are 0, 1, 1, 2, 3, 5, 8, 13, 21, ... A number of interesting algebraic identities can be proved using the above recursion.

42 Example Prove that

$$f_1 + f_2 + \cdots + f_n = f_{n+2} - 1.$$

Solution: We have

$$\begin{array}{ll} f_1 & = f_3 - f_2 \\ f_2 & = f_4 - f_3 \\ f_3 & = f_5 - f_4 \\ \vdots & \vdots \\ f_n & = f_{n+2} - f_{n+1} \end{array}$$

Summing both columns,

$$f_1 + f_2 + \cdots + f_n = f_{n+2} - f_2 = f_{n+2} - 1,$$

as desired.

43 Example Prove that

$$f_1 + f_3 + f_5 + \cdots + f_{2n-1} = f_{2n}.$$

Solution: Observe that

$$\begin{array}{lcl} f_1 & = & f_2 - f_0 \\ f_3 & = & f_4 - f_2 \\ f_5 & = & f_6 - f_4 \\ \vdots & \vdots & \vdots \\ f_{2n-1} & = & f_{2n} - f_{2n-2} \end{array}$$

Adding columnwise we obtain the desired identity.

44 Example Prove that

$$f_1^2 + f_2^2 + \cdots + f_n^2 = f_n f_{n+1}.$$

Solution: We have

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

Thus

$$f_{n+1}f_n - f_n f_{n-1} = f_n^2,$$

which yields

$$f_1^2+f_2^2+\cdots+f_n^2=f_nf_{n+1}.$$

45 Theorem (Cassini's Identity)

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

Proof: *Observe that*

$$\begin{aligned} f_{n-1}f_{n+1}-f_n^2 &= (f_n-f_{n-2})(f_n+f_{n-1})-f_n^2 \\ &= -f_{n-2}f_n-f_{n-1}(f_{n-2}-f_n) \\ &= -(f_{n-2}f_n-f_{n-1}^2) \end{aligned}$$

Thus if $v_n=f_{n-1}f_{n+1}-f_n^2$, we have $v_n=-v_{n-1}$. This yields $v_n=(-1)^{n-1}v_1$ which is to say

$$f_{n-1}f_{n+1}-f_n^2=(-1)^{n-1}(f_0f_2-f_1^2)=(-1)^n.$$

❑

46 Example (IMO 1981) Determine the maximum value of

$$m^2+n^2,$$

where m,n are positive integers satisfying $m,n\in\{1,2,3,\ldots,1981\}$ and

$$(n^2-mn-m^2)^2=1.$$

Solution: Call a pair (n,m) *admissible* if $m,n\in\{1,2,\ldots,1981\}$ and $(n^2-mn-m^2)^2=1$.

If $m=1$, then $(1,1)$ and $(2,1)$ are the only admissible pairs. Suppose now that the pair (n_1,n_2) is admissible, with $n_2>1$. As $n_1(n_1-n_2)=n_2^2\pm 1>0$, we must have $n_1>n_2$.

Let now $n_3=n_1-n_2$. Then $1=(n_1^2-n_1n_2-n_2^2)^2=(n_2^2-n_2n_3-n_3^2)^2$, making (n_2,n_3) also admissible. If $n_3>1$, in the same way we conclude that $n_2>n_3$ and we can let $n_4=n_2-n_3$ making (n_3,n_4) an admissible pair. We have a sequence of positive integers $n_1>n_2>\ldots$, which must necessarily terminate. This terminates when $n_k=1$ for some k. Since $(n_{k-1},1)$ is admissible, we must have $n_{k-1}=2$. The sequence goes thus $1,2,3,5,8,\ldots,987,1597$, i.e., a truncated Fibonacci sequence. The largest admissible pair is thus (1597, 987) and so the maximum sought is 1597^2+987^2.

Let $\tau=\dfrac{1+\sqrt{5}}{2}$ be the Golden Ratio. Observe that $\tau^{-1}=\dfrac{\sqrt{5}-1}{2}$. The number τ is a root of the quadratic equation $x^2=x+1$. We now obtain a closed formula for f_n. We need the following lemma.

47 Lemma If $x^2=x+1,n\geq 2$ then we have $x^n=f_nx+f_{n-1}$.

Proof: *We prove this by induction on n. For $n=2$ the assertion is a triviality. Assume that $n>2$ and that $x^{n-1}=f_{n-1}x+f_{n-2}$. Then*

$$\begin{aligned} x^n &= x^{n-1}\cdot x \\ &= (f_{n-1}x+f_{n-2})x \\ &= f_{n-1}(x+1)+f_{n-2}x \\ &= (f_{n-1}+f_{n-2})x+f_{n-1} \\ &= f_nx+f_{n-1} \end{aligned}$$

❑

48 Theorem (Binet's Formula) The n-th Fibonacci number is given by

$$f_n=\frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^n-\left(\frac{1-\sqrt{5}}{2}\right)^n\right)$$

$n=0,2,\ldots.$

Proof: *The roots of the equation* $x^2 = x+1$ *are* $\tau = \dfrac{1+\sqrt{5}}{2}$ *and* $1-\tau = \dfrac{1-\sqrt{5}}{2}$. *In virtue of the above lemma,*

$$\tau^n = \tau f_n + f_{n-1}$$

and

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

Subtracting

$$\tau^n - (1-\tau)^n = \sqrt{5}f_n,$$

from where Binet's Formula follows.❑

49 Example (Cesàro) Prove that

$$\sum_{k=0}^{n}\binom{n}{k}2^k f_k = f_{3n}.$$

Solution: Using Binet's Formula,

$$\begin{aligned}\sum_{k=0}^{n}\binom{n}{k}2^k f_k &= \sum_{k=0}^{n}\binom{n}{k}2^k\frac{\tau^k-(1-\tau)^k}{\sqrt{5}}\\ &= \frac{1}{\sqrt{5}}\left(\sum_{k=0}^{n}\binom{n}{k}\tau^k - \sum_{k=0}^{n}\binom{n}{k}2^k(1-\tau)^k\right)\\ &= \frac{1}{\sqrt{5}}\left((1+2\tau)^n-(1+2(1-\tau))^n\right).\end{aligned}$$

As $\tau^2 = \tau+1, 1+2\tau = \tau^3$. Similarly $1+2(1-\tau) = (1-\tau)^3$. Thus

$$\sum_{k=0}^{n}\binom{n}{k}2^k f_k = \frac{1}{\sqrt{5}}\left((\tau)^{3n}+(1-\tau)^{3n}\right) = f_{3n},$$

as wanted.

The following theorem will be used later.

50 Theorem If $s \geq 1, t \geq 0$ are integers then

$$f_{s+t} = f_{s-1}f_t + f_s f_{t+1}.$$

Proof: *We keep t fixed and prove this by using strong induction on s. For* $s = 1$ *we are asking whether*

$$f_{t+1} = f_0 f_t + f_1 f_{t+1},$$

which is trivially true. Assume that $s > 1$ *and that* $f_{s-k+t} = f_{s-k-1}f_t + f_{s-k}f_{t+1}$ *for all k satisfying* $1 \leq k \leq s-1$. *We have*

$$\begin{aligned} f_{s+t} &= f_{s+t-1}+f_{s+t-2} && \text{by the Fibonacci recursion,}\\ &= f_{s-1+t}+f_{s-2+t} && \text{trivially,}\\ &= f_{s-2}f_t + f_{s-1}f_{t+1} + f_{s-3}f_t + f_{s-2}f_{t+1} && \text{by the inductive assumption}\\ &= f_t(f_{s-2}+f_{s-3}) + f_{t+1}(f_{s-1}+f_{s-2}) && \text{rearranging,}\\ &= f_t f_{s-1} + f_{t+1}f_s && \text{by the Fibonacci recursion.}\end{aligned}$$

This finishes the proof.❑

Practice

51 Problem Prove that

$$f_{n+1}f_n - f_{n-1}f_{n-2} = f_{2n-1},\ n > 2.$$

52 Problem Prove that

$$f_{n+1}^2 = 4f_nf_{n-1} + f_{n-2}^2,\ n > 1.$$

53 Problem Prove that

$$f_1f_2 + f_2f_3 + \cdots + f_{2n-1}f_{2n} = f_{2n}^2.$$

54 Problem Let N be a natural number. Prove that the largest n such that $f_n \leq N$ is given by

$$n = \left\lfloor\!\!\left\lfloor \frac{\log\left(N + \frac{1}{2}\right)\sqrt{5}}{\log\left(\frac{1+\sqrt{5}}{2}\right)} \right\rfloor\!\!\right\rfloor.$$

55 Problem Prove that $f_n^2 + f_{n-1}^2 = f_{2n+1}$.

56 Problem Prove that if $n > 1$,

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

57 Problem Prove that

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

58 Problem Prove that

$$\sum_{n=2}^{\infty}\frac{1}{f_{n-1}f_{n+1}} = 1.$$

Hint: What is

$$\frac{1}{f_{n-1}f_n} - \frac{1}{f_nf_{n+1}}?$$

59 Problem Prove that

$$\sum_{n=1}^{\infty}\frac{f_n}{f_{n+1}f_{n+2}} = 1.$$

60 Problem Prove that

$$\sum_{n=0}^{\infty}1/f_{2^n} = 4 - \tau.$$

61 Problem Prove that

$$\sum_{n=1}^{\infty}\arctan\frac{1}{f_{2n+1}} = \pi/4.$$

62 Problem Prove that

$$\lim_{n\to\infty}\frac{f_n}{\tau^n} = \frac{1}{\sqrt{5}}.$$

63 Problem Prove that

$$\lim_{n\to\infty}\frac{f_{n+r}}{f_n} = \tau^r.$$

64 Problem Prove that

$$\sum_{k=0}^{n}\frac{1}{f_{2^k}} = 2 + \frac{f_{2^n-2}}{f_{2^n}}.$$

Deduce that

$$\sum_{k=0}^{\infty}\frac{1}{f_{2^k}} = \frac{7-\sqrt{5}}{2}.$$

65 Problem (Cesàro) Prove that

$$\sum_{k=0}^{n}\binom{n}{k}f_k = f_{2n}.$$

66 Problem Prove that

$$\sum_{n=1}^{\infty}\frac{f_n}{10^n}$$

is a rational number.

67 Problem Find the exact value of

$$\sum_{k=1}^{1994}(-1)^k\binom{1995}{k}f_k.$$

68 Problem Prove the converse of Cassini's Identity: If k and m are integers such that $|m^2 - km - k^2| = 1$, then there is an integer n such that $k = \pm f_n, m = \pm f_{n+1}$.

1.5 Pigeonhole Principle

The Pigeonhole Principle states that if $n+1$ pigeons fly to n holes, there must be a pigeonhole containing at least two pigeons. This apparently trivial principle is very powerful. Let us see some examples.

69 Example (Putnam 1978) Let A be any set of twenty integers chosen from the arithmetic progression $1,4,\ldots,100$. Prove that there must be two distinct integers in A whose sum is 104.

Solution: We partition the thirty four elements of this progression into nineteen groups $\{1\},\{52\}$, $\{4,100\}$, $\{7,97\}$, $\{10,94\}$, $\ldots\{49,55\}$. Since we are choosing twenty integers and we have nineteen sets, by the Pigeonhole Principle there must be two integers that belong to one of the pairs, which add to 104.

70 Example Show that amongst any seven distinct positive integers not exceeding 126, one can find two of them, say a and b, which satisfy

$$b < a \leq 2b.$$

Solution: Split the numbers $\{1,2,3,\ldots,126\}$ into the six sets

$$\{1,2\},\{3,4,5,6\},\{7,8,\ldots,13,14\},\{15,16,\ldots,29,30\},$$

$$\{31,32,\ldots,61,62\} \text{ and } \{63,64,\ldots,126\}.$$

By the Pigeonhole Principle, two of the seven numbers must lie in one of the six sets, and obviously, any such two will satisfy the stated inequality.

71 Example Given any set of ten natural numbers between 1 and 99 inclusive, prove that there are two disjoint nonempty subsets of the set with equal sums of their elements.

Solution: There are $2^{10}-1=1023$ non-empty subsets that one can form with a given 10-element set. To each of these subsets we associate the sum of its elements. The maximum value that any such sum can achieve is $90+91+\cdots+99=945<1023$. Therefore, there must be at least two different subsets that have the same sum.

72 Example No matter which fifty five integers may be selected from

$$\{1,2,\ldots,100\},$$

prove that one must select some two that differ by 10.

Solution: First observe that if we choose $n+1$ integers from any string of $2n$ consecutive integers, there will always be some two that differ by n. This is because we can pair the $2n$ consecutive integers

$$\{a+1,a+2,a+3,\ldots,a+2n\}$$

into the n pairs

$$\{a+1,a+n+1\},\{a+2,a+n+2\},\ldots,\{a+n,a+2n\},$$

and if $n+1$ integers are chosen from this, there must be two that belong to the same group.

So now group the one hundred integers as follows:

$$\{1,2,\ldots 20\},\{21,22,\ldots,40\},$$

$$\{41,42,\ldots,60\},\ \{61,62,\ldots,80\}$$

and

$$\{81,82,\ldots,100\}.$$

If we select fifty five integers, we must perforce choose eleven from some group. From that group, by the above observation (let $n=10$), there must be two that differ by 10.

73 Example (AHSME 1994) Label one disc “**1**”, two discs “**2**”, three discs “**3**”, ..., fifty discs “**50**”. Put these $1+2+3+\cdots+50 = 1275$ labeled discs in a box. Discs are then drawn from the box at random without replacement. What is the minimum number of discs that must me drawn in order to guarantee drawing at least ten discs with the same label?

Solution: If we draw all the $1+2+\cdots+9 = 45$ labelled “**1**”, ..., “**9**” and any nine from each of the discs “**10**”, ..., “**50**”, we have drawn $45+9\cdot 41 = 414$ discs. The 415-th disc drawn will assure at least ten discs from a label.

74 Example (IMO 1964) Seventeen people correspond by mail with one another—each one with all the rest. In their letters only three different topics are discussed. Each pair of correspondents deals with only one of these topics. Prove that there at least three people who write to each other about the same topic.

Solution: Choose a particular person of the group, say Charlie. He corresponds with sixteen others. By the Pigeonhole Principle, Charlie must write to at least six of the people of one topic, say topic I. If any pair of these six people corresponds on topic I, then Charlie and this pair do the trick, and we are done. Otherwise, these six correspond amongst themselves only on topics II or III. Choose a particular person from this group of six, say Eric. By the Pigeonhole Principle, there must be three of the five remaining that correspond with Eric in one of the topics, say topic II. If amongst these three there is a pair that corresponds with each other on topic II, then Eric and this pair correspond on topic II, and we are done. Otherwise, these three people only correspond with one another on topic III, and we are done again.

75 Example Given any seven distinct real numbers $x_1, \ldots x_7$, prove that we can always find two, say a, b with

$$0 < \frac{a-b}{1+ab} < \frac{1}{\sqrt{3}}.$$

Solution: Put $x_k = \tan a_k$ for a_k satisfying $-\frac{\pi}{2} < a_k < \frac{\pi}{2}$. Divide the interval $(-\frac{\pi}{2}, \frac{\pi}{2})$ into six non-overlapping subintervals of equal length. By the Pigeonhole Principle, two of seven points will lie on the same interval, say $a_i < a_j$. Then $0 < a_j - a_i < \frac{\pi}{6}$. Since the tangent increases in $(-\pi/2, \pi/2)$, we obtain

$$0 < \tan(a_j - a_i) = \frac{\tan a_j - \tan a_i}{1+\tan a_j \tan a_i} < \tan\frac{\pi}{6} = \frac{1}{\sqrt{3}},$$

as desired.

76 Example (Canadian Math Olympiad 1981) Let $a_1, a_2, \ldots, a_7$ be nonnegative real numbers with

$$a_1 + a_2 + \ldots + a_7 = 1.$$

If

$$M = \max_{1\le k\le 5} a_k + a_{k+1} + a_{k+2},$$

determine the minimum possible value that $\mathscr{M}$ can take as the a_k vary.

Solution: Since $a_1 \le a_1+a_2 \le a_1+a_2+a_3$ and $a_7 \le a_6+a_7 \le a_5+a_6+a_7$ we see that $\mathscr{M}$ also equals

$$\max_{1\le k\le 5} \{a_1, a_7, a_1+a_2, a_6+a_7, a_k+a_{k+1}+a_{k+2}\}.$$

We are thus taking the maximum over nine quantities that sum $3(a_1+a_2+\cdots+a_7) = 3$. These nine quantities then average $3/9 = 1/3$. By the Pigeonhole Principle, one of these is $\ge 1/3$, i.e. $M \ge 1/3$. If $a_1 = a_1+a_2 = a_1+a_2+a_3 = a_2+a_3+a_4 = a_3+a_4+a_5 = a_4+a_5+a_6 = a_5+a_6+a_7 = a_7 = 1/3$, we obtain the 7-tuple $(a_1, a_2, a_3, a_4, a_5, a_6, a_7) = (1/3, 0, 0, 1/3, 0, 0, 1/3)$, which shows that $M = 1/3$.

Practice

77 Problem (AHSME 1991) A circular table has exactly sixty chairs around it. There are N people seated at this table in such a way that the next person to be seated must sit next to someone. What is the smallest possible value of N?

Answer: 20.

78 Problem Show that if any five points are all in, or on, a square of side 1, then some pair of them will be at most at distance $\sqrt{2}/2$.

79 Problem (Eötvös, 1947) Prove that amongst six people in a room there are at least three who know one another, or at least three who do not know one another.

80 Problem Show that in any sum of non-negative real numbers there is always one number which is at least the average of the numbers and that there is always one member that it is at most the average of the numbers.

81 Problem We call a set “sum free” if no two elements of the set add up to a third element of the set. What is the maximum size of a sum free subset of $\{1,2,\ldots,2n-1\}$.

Hint: Observe that the set $\{n+1,n+2,\ldots,2n-1\}$ of $n+1$ elements is sum free. Show that any subset with $n+2$ elements is not sum free.

82 Problem (MMPC 1992) Suppose that the letters of the English alphabet are listed in an arbitrary order.

1. Prove that there must be four consecutive consonants.

2. Give a list to show that there need not be five consecutive consonants.

3. Suppose that all the letters are arranged in a circle. Prove that there must be five consecutive consonants.

83 Problem (Stanford 1953) Bob has ten pockets and forty four silver dollars. He wants to put his dollars into his pockets so distributed that each pocket contains a different number of dollars.

1. Can he do so?

2. Generalise the problem, considering p pockets and n dollars. The problem is most interesting when
$$n=\frac{(p-1)(p-2)}{2}.$$
Why?

84 Problem No matter which fifty five integers may be selected from
$$\{1,2,\ldots,100\},$$
prove that you must select some two that differ by 9, some two that differ by 10, some two that differ by 12, and some two that differ by 13, but that you need not have any two that differ by 11.

85 Problem Let $mn+1$ different real numbers be given. Prove that there is either an increasing sequence with at least $n+1$ members, or a decreasing sequence with at least $m+1$ members.

86 Problem If the points of the plane are coloured with three colours, show that there will always exist two points of the same colour which are one unit apart.

87 Problem Show that if the points of the plane are coloured with two colours, there will always exist an equilateral triangle with all its vertices of the same colour. There is, however, a colouring of the points of the plane with two colours for which no equilateral triangle of side 1 has all its vertices of the same colour.

88 Problem Let $r_1,r_2,\ldots,r_n,n>1$ be real numbers of absolute value not exceeding 1 and whose sum is 0. Show that there is a non-empty proper subset whose sum is not more than $2/n$ in size. Give an example in which any subsum has absolute value at least $\dfrac{1}{n-1}$.

89 Problem Let $r_1,r_2,\ldots,r_n$ be real numbers in the interval $[0,1]$. Show that there are numbers $\varepsilon_k, 1\le k\le n, \varepsilon_k=-1,0,1$ not all zero, such that
$$\left|\sum_{k=1}^{n}\varepsilon_k r_k\right|\le\frac{n}{2^n}.$$

90 Problem (USAMO, 1979) Nine mathematicians meet at an international conference and discover that amongst any three of them, at least two speak a common language. If each of the mathematicians can speak at most three languages, prove that there are at least three of the mathematicians who can speak the same language.

91 Problem (USAMO, 1982) In a party with 1982 persons, amongst any group of four there is at least one person who knows each of the other three. What is the minimum number of people in the party who know everyone else?

92 **Problem (USAMO, 1985)** There are n people at a party. Prove that there are two people such that, of the remaining $n-2$ people, there are at least $\lfloor\!\lfloor n/2 \rfloor\!\rfloor - 1$ of them, each of whom knows both or else knows neither of the two. Assume that "knowing" is a symmetrical relationship.

93 **Problem (USAMO, 1986)** During a certain lecture, each of five mathematicians fell asleep exactly twice. For each pair of these mathematicians, there was some moment when both were sleeping simultaneously. Prove that, at some moment, some three were sleeping simultaneously.

94 **Problem** Let $\mathscr{P}_n$ be a set of $\lfloor\!\lfloor en! \rfloor\!\rfloor + 1$ points on the plane. Any two distinct points of $\mathscr{P}_n$ are joined by a straight line segment which is then coloured in one of n given colours. Show that at least one monochromatic triangle is formed.

(Hint: $e = \sum_{n=0}^{\infty} 1/n!$.)

Chapter 2

Divisibility

2.1 Divisibility

95 Definition If $a \neq 0, b$ are integers, we say that a *divides* b if there is an integer c such that $ac = b$. We write this as $a|b$.

If a does not divide b we write $a \not| b$. The following properties should be immediate to the reader.

96 Theorem 1. If a,b,c,m,n are integers with $c|a, c|b$, then $c|(am+nb)$.

2. If x,y,z are integers with $x|y, y|z$ then $x|z$.

Proof: *There are integers s,t with $sc = a, tc = b$. Thus*

$$am+nb = c(sm+tn),$$

giving $c|(am+bn)$.

Also, there are integers u,v with $xu = y, yv = z$. Hence $xuv = z$, giving $x|z$.

It should be clear that if $a|b$ and $b \neq 0$ then $1 \leq |a| \leq |b|$.❑

97 Example Find all positive integers n for which

$$n+1|n^2+1.$$

Solution: $n^2+1 = n^2-1+2 = (n-1)(n+1)+2$. This forces $n+1|2$ and so $n+1 = 1$ or $n+1 = 2$. The choice $n+1 = 1$ is out since $n \geq 1$, so that the only such n is $n = 1$.

98 Example If $7|3x+2$ prove that $7|(15x^2-11x-14.)$.

Solution: Observe that $15x^2-11x-14 = (3x+2)(5x-7)$. We have $7s = 3x+2$ for some integer s and so

$$15x^2-11x-14 = 7s(5x-7),$$

giving the result.

Among every two consecutive integers there is an even one, among every three consecutive integers there is one divisible by 3, etc.The following theorem goes further.

99 Theorem The product of n consecutive integers is divisible by $n!$.

Proof: *Assume first that all the consecutive integers $m+1, m+2, \ldots, m+n$ are positive. If this is so, the divisibility by $n!$ follows from the fact that binomial coefficients are integers:*

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

If one of the consecutive integers is 0, then the product of them is 0, and so there is nothing to prove. If all the n consecutive integers are negative, we multiply by $(-1)^n$, and see that the corresponding product is positive, and so we apply the first result.❑

100 Example Prove that $6|n^3-n$, for all integers n.

Solution: $n^3-n=(n-1)n(n+1)$ is the product of 3 consecutive integers and hence is divisible by $3!=6$.

101 Example (Putnam 1966) Let $0 < a_1 < a_2 < \ldots < a_{mn+1}$ 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.

Solution: Let, for each $1 \leq k \leq mn+1, n_k$ denote the length of the longest chain, starting with a_k and each dividing the following one, that can be selected from $a_k, a_{k+1}, \ldots, a_{mn+1}$. If no n_k is greater than n, then the are at least $m+1$ n_k's that are the same. However, the integers a_k corresponding to these n_k's cannot divide each other, because $a_k|a_l$ implies that $n_k \geq n_l+1$.

102 Theorem If $k|n$ then $f_k|f_n$.

Proof: *Letting $s=kn, t=n$ in the identity $f_{s+t}=f_{s-1}f_t+f_sf_{t+1}$ we obtain*

$$f_{(k+1)n}=f_{kn+n}=f_{n-1}f_{kn}+f_nf_{kn+1}.$$

It is clear that if $f_n|f_{kn}$ then $f_n|f_{(k+1)n}$. Since $f_n|f_{n\cdot 1}$, the assertion follows.❑

Practice

103 Problem Given that $5|(n+2)$, which of the following are divisible by 5

$$n^2-4,\ n^2+8n+7,\ n^4-1, n^2-2n?$$

104 Problem Prove that n^5-5n^3+4n is always divisible by 120.

105 Problem Prove that

$$\frac{(2m)!(3n)!}{(m!)^2(n!)^3}$$

is always an integer.

106 Problem Demonstrate that for all integer values n,

$$n^9-6n^7+9n^5-4n^3$$

is divisible by 8640.

107 Problem Prove that if $n>4$ is composite, then n divides $(n-1)!$.
(Hint: Consider, separately, the cases when n is and is not a perfect square.)

108 Problem Prove that there is no prime triplet of the form $p, p+2, p+4$, except for $3, 5, 7$.

109 Problem Prove that for $n \in \mathbb{N}$, $(n!)!$ is divisible by $n!^{(n-1)!}$

110 Problem (AIME 1986) What is the largest positive integer n for which

$$(n+10)|(n^3+100)?$$

(Hint: $x^3+y^3=(x+y)(x^2-xy+y^2)$.)

111 Problem (Olimpíada matemática española, 1985) If n is a positive integer, prove that $(n+1)(n+2)\cdots(2n)$ is divisible by 2^n.

2.2 Division Algorithm

112 Theorem (Division Algorithm) If a,b are positive integers, then there are unique integers q,r such that $a = bq + r, 0 \leq r < b$.

> **Proof:** *We use the Well-Ordering Principle. Consider the set* $\mathscr{S} = \{a - bk : k \in \mathbb{Z} \text{ and } a \geq bk\}$. *Then* $\mathscr{S}$ *is a collection of nonnegative integers and* $\mathscr{S} \neq \varnothing$ *as* $a - b \cdot 0 \in \mathscr{S}$. *By the Well-Ordering Principle,* $\mathscr{S}$ *has a least element, say* r. *Now, there must be some* $q \in \mathbb{Z}$ *such that* $r = a - bq$ *since* $r \in \mathscr{S}$. *By construction,* $r \geq 0$. *Let us prove that* $r < b$. *For assume that* $r \geq b$. *Then* $r > r - b = a - bq - b = a - (q+1)b \geq 0$, *since* $r - b \geq 0$. *But then* $a - (q+1)b \in \mathscr{S}$ *and* $a - (q+1)b < r$ *which contradicts the fact that* r *is the smallest member of* $\mathscr{S}$. *Thus we must have* $0 \leq r < b$. *To show that* r *and* q *are unique, assume that* $bq_1 + r_1 = a = bq_2 + r_2, 0 \leq r_1 < b, 0 \leq r_2 < b$. *Then* $r_2 - r_1 = b(q_1 - q_2)$, *that is* $b|(r_2 - r_1)$. *But* $|r_2 - r_1| < b$, *whence* $r_2 = r_1$. *From this it also follows that* $q_1 = q_2$. *This completes the proof.* ❑

It is quite plain that $q = \llbracket a/b \rrbracket$, where $\llbracket a/b \rrbracket$ denotes the integral part of a/b.

It is important to realise that given an integer $n > 0$, the Division Algorithm makes a partition of all the integers according to their remainder upon division by n. For example, every integer lies in one of the families $3k, 3k+1$ or $3k+2$ where $k \in \mathbb{Z}$. Observe that the family $3k+2, k \in \mathbb{Z}$, is the same as the family $3k-1, k \in \mathbb{Z}$. Thus

$$\mathbb{Z} = A \cup B \cup C$$

where

$$A = \{\ldots, -9, -6, -3, 0, 3, 6, 9, \ldots\}$$

is the family of integers of the form $3k, k \in \mathbb{Z}$,

$$B = \{\ldots -8, -5, -2, 1, 4, 7, \ldots\}$$

is the family of integers of the form $3k+1, k \in \mathbb{Z}$ and

$$C = \{\ldots -7, -4, -1, 2, 5, 8, \ldots\}$$

is the family of integers of the form $3k-1, k \in \mathbb{Z}$.

113 Example (AHSME 1976) Let r be the remainder when $1059, 1417$ and 2312 are divided by $d > 1$. Find the value of $d - r$.

Solution: By the Division Algorithm, $1059 = q_1 d + r, 1417 = q_2 d + r, 2312 = q_3 d + r$, for some integers q_1, q_2, q_3. From this, $358 = 1417 - 1059 = d(q_2 - q_1), 1253 = 2312 - 1059 = d(q_3 - q_1)$ and $895 = 2312 - 1417 = d(q_3 - q_2)$. Hence $d|358 = 2 \cdot 179, d|1253 = 7 \cdot 179$ and $7|895 = 5 \cdot 179$. Since $d > 1$, we conclude that $d = 179$. Thus (for example) $1059 = 5 \cdot 179 + 164$, which means that $r = 164$. We conclude that $d - r = 179 - 164 = 15$.

114 Example Show that $n^2 + 23$ is divisible by 24 for infinitely many n.

Solution: $n^2 + 23 = n^2 - 1 + 24 = (n-1)(n+1) + 24$. If we take $n = 24k \pm 1, k = 0, 1, 2, \ldots$, all these values make the expression divisible by 24.

115 Definition A *prime* number p is a positive integer greater than 1 whose only positive divisors are 1 and p. If the integer $n > 1$ is not prime, then we say that it is *composite.*

For example, 2, 3, 5, 7, 11, 13, 17, 19 are prime, 4, 6, 8, 9, 10, 12, 14, 15, 16, 18, 20 are composite. The number 1 is neither a prime nor a composite.

116 Example Show that if $p > 3$ is a prime, then $24|(p^2 - 1)$.

Solution: By the Division Algorithm, integers come in one of six flavours: $6k, 6k\pm 1, 6k\pm 2$ or $6k+3$. If $p > 3$ is a prime, then p is of the form $p = 6k\pm 1$ (the other choices are either divisible by 2 or 3). But $(6k\pm 1)^2 - 1 = 36k^2 \pm 12k = 12k(3k-1)$. Since either k or $3k-1$ is even, $12k(3k-1)$ is divisible by 24.

117 Example Prove that the square of any integer is of the form $4k$ or $4k+1$.

Solution: By the Division Algorithm, any integer comes in one of two flavours: $2a$ or $2a+1$. Squaring,

$$(2a)^2 = 4a^2, \ (2a+1)^2 = 4(a^2+a)+1)$$

and so the assertion follows.

118 Example Prove that no integer in the sequence

$$11, 111, 1111, 11111, \ldots$$

is the square of an integer.

Solution: The square of any integer is of the form $4k$ or $4k+1$. All the numbers in this sequence are of the form $4k-1$, and so they cannot be the square of any integer.

119 Example Show that from any three integers, one can always choose two so that a^3b-ab^3 is divisible by 10.

Solution: It is clear that $a^3b-ab^3 = ab(a-b)(a+b)$ is always even, no matter which integers are substituted. If one of the three integers is of the form $5k$, then we are done. If not, we are choosing three integers that lie in the residue classes $5k\pm 1$ or $5k\pm 2$. Two of them must lie in one of these two groups, and so there must be two whose sum or whose difference is divisible by 5. The assertion follows.

120 Example Prove that if $3|(a^2+b^2)$, then $3|a$ and $3|b$

Solution: Assume $a = 3k\pm 1$ or $b = 3m\pm 1$. Then $a^2 = 3x+1, b^2 = 3y+1$. But then $a^2+b^2 = 3t+1$ or $a^2+b^2 = 3s+2$, i.e., $3 \not| (a^2+b^2)$.

Practice

121 Problem Prove the following extension of the Division Algorithm: if a and $b \neq 0$ are integers, then there are unique integers q and r such that $a = qb+r, 0 \leq r < |b|$.

122 Problem Show that if a and b are positive integers, then there are unique integers q and r, and $\varepsilon = \pm 1$ such that $a = qb+\varepsilon r, -\frac{b}{2} < r \leq \frac{b}{2}$.

123 Problem Show that the product of two numbers of the form $4k+3$ is of the form $4k+1$.

124 Problem Prove that the square of any odd integer leaves remainder 1 upon division by 8.

125 Problem Demonstrate that there are no three consecutive odd integers such that each is the sum of two squares greater than zero.

126 Problem Let $n > 1$ be a positive integer. Prove that if one of the numbers $2^n-1, 2^n+1$ is prime, then the other is composite.

127 Problem Prove that there are infinitely many integers n such that $4n^2+1$ is divisible by both 13 and 5.

128 Problem Prove that any integer $n > 11$ is the sum of two positive composite numbers.

Hint: Think of $n-6$ if n is even and $n-9$ if n is odd.

129 Problem Prove that 3 never divides n^2+1.

130 Problem Show the existence of infinitely many natural numbers x, y such that $x(x+1)|y(y+1)$ but

$$x \nmid y \text{ and } (x+1) \nmid y,$$

and also

$$x \nmid (y+1) \text{ and } (x+1) \nmid (y+1).$$

Hint: Try $x = 36k+14, y = (12k+5)(18k+7)$.

2.3 Some Algebraic Identities

In this section we present some examples whose solutions depend on the use of some elementary algebraic identities.

131 Example Find all the primes of the form n^3-1, for integer $n>1$.

Solution: $n^3-1 = (n-1)(n^2+n+1)$. If the expression were prime, since n^2+n+1 is always greater than 1, we must have $n-1=1$, i.e. $n=2$. Thus the only such prime is 7.

132 Example Prove that n^4+4 is a prime only when $n=1$ for $n \in \mathbb{N}$.

Solution: Observe that

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

Each factor is greater than 1 for $n>1$, and so n^4+4 cannot be a prime.

133 Example Find all integers $n \geq 1$ for which n^4+4^n is a prime.

Solution: The expression is only prime for $n=1$. Clearly one must take n odd. For $n \geq 3$ odd all the numbers below are integers:

$$\begin{aligned} n^4+2^{2n} &= n^4+2n^22^n+2^{2n}-2n^22^n \\ &= (n^2+2^n)^2-\left(n2^{(n+1)/2}\right)^2 \\ &= (n^2+2^n+n2^{(n+1)/2})(n^2+2^n-n2^{(n+1)/2}). \end{aligned}$$

It is easy to see that if $n \geq 3$, each factor is greater than 1, so this number cannot be a prime.

134 Example Prove that for all $n \in \mathbb{N}$, n^2 divides the quantity

$$(n+1)^n-1.$$

Solution: If $n=1$ this is quite evident. Assume $n>1$. By the Binomial Theorem,

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

and every term is divisible by n^2.

135 Example Prove that if p is an odd prime and if

$$\frac{a}{b} = 1+1/2+\cdots+1/(p-1),$$

then p divides a.

Solution: Arrange the sum as

$$1+\frac{1}{p-1}+\frac{1}{2}+\frac{1}{p-2}+\cdots+\frac{1}{(p-1)/2}+\frac{1}{(p+1)/2}.$$

After summing consecutive pairs, the numerator of the resulting fractions is p. Each term in the denominator is $< p$. Since p is a prime, the p on the numerator will not be thus cancelled out.

136 Example Prove that

$$\boxed{x^n-y^n=(x-y)(x^{n-1}+x^{n-2}y+x^{n-3}y^2+\cdots+xy^{n-2}+y^{n-1})}$$

Thus $x-y$ **always divides** x^n-y^n.

Solution: We may assume that $x \neq y, xy \neq 0$, the result being otherwise trivial. In that case, the result follows at once from the identity

$$\sum_{k=0}^{n-1} a^k = \frac{a^n-1}{a-1}\ a \neq 1,$$

upon letting $a = x/y$ and multiplying through by y^n.

☞ *Without calculation we see that* $8767^{2345}-8101^{2345}$ *is divisible by* 666.

137 Example (Eőtvős 1899) Show that

$$2903^n-803^n-464^n+261^n$$

is divisible by 1897 for all natural numbers n.

Solution: By the preceding problem, 2903^n-803^n is divisible by $2903-803=2100=7\cdot 300=$, and 261^n-464^n is divisible by $261-464=-203=7\cdot(-29)$. Thus the expression $2903^n-803^n-464^n+261^n$ is divisible by 7. Also, 2903^n-464^n is divisible by $2903-464=9\cdot 271$ and 261^n-803^n is divisible by $-542=(-2)271$. Thus the expression is also divisible by 271. Since 7 and 271 have no prime factors in common, we can conclude that the expression is divisible by $7\cdot 271=1897$.

138 Example ($(UM)^2C^4$ 1987**)** Given that 1002004008016032 has a prime factor $p > 250000$, find it.

Solution: If $a = 10^3, b = 2$ then

$$1002004008016032 = a^5+a^4b+a^3b^2+a^2b^3+ab^4+b^5=\frac{a^6-b^6}{a-b}.$$

This last expression factorises as

$$\begin{aligned}\frac{a^6-b^6}{a-b} &= (a+b)(a^2+ab+b^2)(a^2-ab+b^2)\\ &= 1002\cdot 1002004\cdot 998004\\ &= 4\cdot 4\cdot 1002\cdot 250501\cdot k,\end{aligned}$$

where $k < 250000$. Therefore $p = 250501$.

139 Example (Grünert, 1856) If x, y, z, n are natural numbers $n \geq z$, then the relation

$$x^n+y^n=z^n$$

does not hold.

Solution: It is clear that if the relation $x^n+y^n=z^n$ holds for natural numbers x,y,z then $x<z$ and $y<z$. By symmetry, we may suppose that $x<y$. So assume that $x^n+y^n=z^n$ and $n\geq z$. Then

$$z^n-y^n=(z-y)(z^{n-1}+yz^{n-2}+\cdots+y^{n-1})\geq 1\cdot nx^{n-1}>x^n,$$

contrary to the assertion that $x^n+y^n=z^n$. This establishes the assertion.

140 Example Prove that for n odd,

$$x^n+y^n=(x+y)(x^{n-1}-x^{n-2}y+x^{n-3}y^2-+-\cdots+-xy^{n-2}+y^{n-1}).$$

Thus **if n is odd, $x+y$ divides x^n+y^n.**

Solution: This is evident by substituting $-y$ for y in example 1.11 and observing that $(-y)^n=-y^n$ for n odd.

141 Example Show that 1001 divides

$$1^{1993}+2^{1993}+3^{1993}+\cdots+1000^{1993}.$$

Solution: Follows at once from the previous problem, since each of $1^{1993}+1000^{1993},2^{1993}+999^{1993},\ldots,500^{1993}+501^{1993}$ is divisible by 1001.

142 Example (S250) Show that for any natural number n, there is another natural number x such that each term of the sequence

$$x+1,x^x+1,x^{x^x}+1,\ldots$$

is divisible by n.

Solution: It suffices to take $x=2n-1$.

143 Example Determine infinitely many pairs of integers (m,n) such that $\mathscr{M}$ and n share their prime factors and $(m-1,n-1)$ share their prime factors.

Solution: Take $m=2^k-1,n=(2^k-1)^2,k=2,3,\ldots$. Then m,n obviously share their prime factors and $m-1=2(2^{k-1}-1)$ shares its prime factors with $n-1=2^{k+1}(2^{k-1}-1)$.

Practice

144 Problem Show that the integer

$$\underbrace{1\ldots1}_{91\text{ ones}}$$

is composite.

145 Problem Prove that $1^{99}+2^{99}+3^{99}+4^{99}$ is divisible by 5.

146 Problem Show that if $|ab|\neq 1$, then a^4+4b^4 is composite.

147 Problem Demonstrate that for any natural number n, the number

$$\underbrace{1\cdots\cdots1}_{2n\ 1's}-\underbrace{2\cdots\ 2}_{n\ 2's}$$

is the square of an integer.

148 Problem Let $0\leq a<b$.

1. Prove that $b^n((n+1)a-nb)<a^{n+1}$.
2. Prove that for $n=1,2,\ldots,$

$$\left(1+\frac{1}{n}\right)^n<\left(1+\frac{1}{n+1}\right)^{n+1}\quad n=1,2,\ldots.$$

3. Show that

$$\frac{b^{n+1}-a^{n+1}}{b-a}>(n+1)a.$$

4. Show that
$$\left(1+\frac{1}{n}\right)^{n+1} > \left(1+\frac{1}{n+1}\right)^{n+2} \quad n = 1,2,\ldots.$$

149 Problem If a, b are positive integers, prove that
$$(a+1/2)^n + (b+1/2)^n$$
is an integer only for finitely many positive integers n.

150 Problem Prove that $100|11^{10}-1$.

151 Problem Let A and B be two natural numbers with the same number of digits, $A > B$. Suppose that A and B have more than half of their digits on the sinistral side in common. Prove that
$$A^{1/n} - B^{1/n} < \frac{1}{n}$$
for all $n = 2,3,4,\ldots$.

152 Problem Demonstrate that every number in the sequence
$$49, 4489, 444889, 44448889, \ldots, \underbrace{4\cdots\cdots4}_{n\ 4's}\underbrace{8\cdots\ 8}_{n-1\ 8's}9,$$
is the square of an integer.

153 Problem (Polish Mathematical Olympiad) Prove that if n is an even natural number, then the number $13^n + 6$ is divisible by 7.

154 Problem Find, with proof, the unique square which is the product of four consecutive odd numbers.

155 Problem Prove that the number $2222^{5555} + 5555^{2222}$ is divisible by 7.

(Hint: Consider
$$2222^{5555} + 4^{5555} + 5555^{2222} - 4^{2222} + 4^{2222} - 4^{5555}.)$$

156 Problem Prove that if $a^n + 1, 1 < a \in \mathbb{N}$, is prime, then a is even and n is a power of 2. Primes of the form $2^{2^k} + 1$ are called *Fermat primes*.

157 Problem Prove that if $a^n - 1, 1 < a \in \mathbb{N}$, is prime, then $a = 2$ and n is a prime. Primes of the form $2^n - 1$ are called *Mersenne primes*.

158 Problem (Putnam, 1989) How many primes amongst the positive integers, written as usual in base-ten are such that their digits are alternating 1's and 0's, beginning and ending in 1?

159 Problem Find the least value achieved by $36^k - 5^k, k = 1,2,\ldots$.

160 Problem Find all the primes of the form $n^3 + 1$.

161 Problem Find a closed formula for the product
$$P = (1+2)(1+2^2)(1+2^{2^2})\cdots(1+2^{2^n}).$$
Use this to prove that for all positive integers n, $2^{2^n} + 1$ divides
$$2^{2^{2^n}+1} - 2.$$

162 Problem Let $a > 1$ be a real number. Simplify the expression
$$\sqrt{a+2\sqrt{a-1}} + \sqrt{a-2\sqrt{a-1}}.$$

163 Problem Let a, b, c, d be real numbers such that
$$a^2 + b^2 + c^2 + d^2 = ab + bc + cd + da.$$
Prove that $a = b = c = d$.

164 Problem Let a, b, c be the lengths of the sides of a triangle. Show that
$$3(ab+bc+ca) \leq (a+b+c)^2 \leq 4(ab+bc+ca).$$

165 Problem (ITT, 1994) Let a, b, c, d be complex numbers satisfying
$$a+b+c+d = a^3+b^3+c^3+d^3 = 0.$$
Prove that a pair of the a, b, c, d must add up to 0.

166 Problem Prove that the product of four consecutive natural numbers is never a perfect square.

Hint: What is $(n^2+n-1)^2$?

167 Problem Let $k \geq 2$ be an integer. Show that if n is a positive integer, then n^k can be represented as the sum of n successive odd numbers.

168 Problem (Catalan) Prove that
$$1 - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} + \cdots + \frac{1}{2n-1} - \frac{1}{2n}$$

equals

$$\frac{1}{n+1}+\frac{1}{n+2}+\cdots+\frac{1}{2n}.$$

169 Problem (IMO, 1979) If a, b are natural numbers such that

$$\frac{a}{b}=1-\frac{1}{2}+\frac{1}{3}-\frac{1}{4}+\cdots-\frac{1}{1318}+\frac{1}{1319},$$

prove that $1979|a$.

170 Problem (Polish Mathematical Olympiad) A *triangular number* is one of the form $1+2+\ldots+n, n \in \mathbb{N}$. Prove that none of the digits $2,4,7,9$ can be the last digit of a triangular number.

171 Problem Demonstrate that there are infinitely many square triangular numbers.

172 Problem (Putnam, 1975) Supposing that an integer n is the sum of two triangular numbers,

$$n=\frac{a^2+a}{2}+\frac{b^2+b}{2},$$

write $4n+1$ as the sum of two squares, $4n+1=x^2+y^2$ where x and y are expressed in terms of a and b.

Conversely, show that if $4n+1=x^2+y^2$, then n is the sum of two triangular numbers.

173 Problem (Polish Mathematical Olympiad) Prove that amongst ten successive natural numbers, there are always at least one and at most four numbers that are not divisible by any of the numbers $2,3,5,7$.

174 Problem Show that if k is odd,

$$1+2+\cdots+n$$

divides

$$1^k+2^k+\cdots+n^k.$$

175 Problem Are there five consecutive positive integers such that the sum of the first four, each raised to the fourth power, equals the fifth raised to the fourth power?

Chapter 3

Congruences. $\mathbb{Z}_n$

3.1 Congruences

The notation $a \equiv b \mod n$ is due to Gauß, and it means that $n|(a-b)$. It also indicates that a and b leave the same remainder upon division by n. For example, $-8 \equiv -1 \equiv 6 \equiv 13 \mod 7$. Since $n|(a-b)$ implies that $\exists k \in \mathbb{Z}$ such that $nk = a-b$, we deduce that $a \equiv b \mod n$ if and only if there is an integer k such that $a = b+nk$.

We start by mentioning some simple properties of congruences.

176 Lemma Let $a,b,c,d,m \in \mathbb{Z}, k \in$ with $a \equiv b \mod m$ and $c \equiv d \mod m$. Then

1. $a+c \equiv b+d \mod m$
2. $a-c \equiv b-d \mod m$
3. $ac \equiv bd \mod m$
4. $a^k \equiv b^k \mod m$
5. If f is a polynomial with integral coefficients then $f(a) \equiv f(b) \mod m$.

> **Proof:** *As $a \equiv b \mod m$ and $c \equiv d \mod m$, we can find $k_1, k_2 \in \mathbb{Z}$ with $a = b+k_1m$ and $c = d+k_2m$. Thus $a \pm c = b \pm d + m(k_1 \pm k_2)$ and $ac = bd + m(k_2b + k_1d)$. These equalities give (1), (2) and (3). Property (4) follows by successive application of (3), and (5) follows from (4).* ❑

Congruences $\mod 9$ can sometimes be used to check multiplications. For example $875961 \cdot 2753 \neq 2410520633$. For if this were true then

$$(8+7+5+9+6+1)(2+7+5+3) \equiv 2+4+1+0+5+2+0+6+3+3 \mod 9.$$

But this says that $0 \cdot 8 \equiv 8 \mod 9$, which is patently false.

177 Example Find the remainder when 6^{1987} is divided by 37.

Solution: $6^2 \equiv -1 \mod 37$. Thus $6^{1987} \equiv 6 \cdot 6^{1986} \equiv 6(6^2)^{993} \equiv 6(-1)^{993} \equiv -6 \equiv 31 \mod 37$.

178 Example Prove that 7 divides $3^{2n+1} + 2^{n+2}$ for all natural numbers n.

Solution: Observe that $3^{2n+1} \equiv 3 \cdot 9^n \equiv 3 \cdot 2^n \mod 7$ and $2^{n+2} \equiv 4 \cdot 2^n \mod 7$. Hence

$$3^{2n+1} + 2^{n+2} \equiv 7 \cdot 2^n \equiv 0 \mod 7,$$

for all natural numbers n.

179 Example Prove the following result of Euler: $641|(2^{32}+1)$.

Solution: Observe that $641 = 2^7 \cdot 5 + 1 = 2^4 + 5^4$. Hence $2^7 \cdot 5 \equiv -1 \mod 641$ and $5^4 \equiv -2^4 \mod 641$. Now, $2^7 \cdot 5 \equiv -1 \mod 641$ yields $5^4 \cdot 2^{28} = (5 \cdot 2^7)^4 \equiv (-1)^4 \equiv 1 \mod 641$. This last congruence and $5^4 \equiv -2^4 \mod 641$ yield $-2^4 \cdot 2^{28} \equiv 1 \mod 641$, which means that $641|(2^{32}+1)$.

180 Example Find the perfect squares $\mod 13$.

Solution: First observe that we only have to square all the numbers up to 6, because $r^2 \equiv (13-r)^2 \mod 13$. Squaring the nonnegative integers up to 6, we obtain $0^2 \equiv 0, 1^2 \equiv 1, 2^2 \equiv 4, 3^2 \equiv 9, 4^2 \equiv 3, 5^2 \equiv 12, 6^2 \equiv 10 \mod 13$. Therefore the perfect squares mod 13 are 0, 1, 4, 9, 3, 12, and 10.

181 Example Prove that there are no integers with $x^2 - 5y^2 = 2$.

Solution: If $x^2 = 2 - 5y^2$, then $x^2 \equiv 2 \mod 5$. But 2 is not a perfect square $\mod 5$.

182 Example Prove that $7|(2222^{5555} + 5555^{2222})$.

Solution: $2222 \equiv 3 \mod 7$, $5555 \equiv 4 \mod 7$ and $3^5 \equiv 5 \mod 7$. Now $2222^{5555} + 5555^{2222} \equiv 3^{5555} + 4^{2222} \equiv (3^5)^{1111} + (4^2)^{1111} \equiv 5^{1111} - 5^{1111} \equiv 0 \mod 7$.

183 Example Find the units digit of 7^{7^7}.

Solution: We must find $7^{7^7} \mod 10$. Now, $7^2 \equiv -1 \mod 10$, and so $7^3 \equiv 7^2 \cdot 7 \equiv -7 \equiv 3 \mod 10$ and $7^4 \equiv (7^2)^2 \equiv 1 \mod 10$. Also, $7^2 \equiv 1 \mod 4$ and so $7^7 \equiv (7^2)^3 \cdot 7 \equiv 3 \mod 4$, which means that there is an integer t such that $7^7 = 3 + 4t$. Upon assembling all this,

$$7^{7^7} \equiv 7^{4t+3} \equiv (7^4)^t \cdot 7^3 \equiv 1^t \cdot 3 \equiv 3 \mod 10.$$

Thus the last digit is 3.

184 Example Prove that every year, including any leap year, has at least one Friday 13-th.

Solution: It is enough to prove that each year has a Sunday the 1st. Now, the first day of a month in each year falls in one of the following days:

Month	Day of the year	mod 7
January	1	1
February	32	4
March	60 or 61	4 or 5
April	91 or 92	0 or 1
May	121 or122	2 or 3
June	152 or 153	5 or 6
July	182 or183	0 or 1
August	213 or 214	3 or 4
September	244 or 245	6 or 0
October	274 or 275	1 or 2
November	305 or 306	4 or 5
December	335 or 336	6 or 0

(The above table means that, depending on whether the year is a leap year or not, that March 1st is the 50th or 51st day of the year, etc.) Now, each remainder class modulo 7 is represented in the third column, thus each year, whether leap or not, has at least one Sunday the 1st.

185 Example Find infinitely many integers n such that $2^n + 27$ is divisible by 7.

Solution: Observe that $2^1 \equiv 2, 2^2 \equiv 4, 2^3 \equiv 1, 2^4 \equiv 2, 2^5 \equiv 4, 2^6 \equiv 1 \mod 7$ and so $2^{3k} \equiv 1 \mod 3$ for all positive integers k. Hence $2^{3k} + 27 \equiv 1 + 27 \equiv 0 \mod 7$ for all positive integers k. This produces the infinitely many values sought.

186 Example Are there positive integers x, y such that $x^3 = 2^y + 15$?

Solution: No. The perfect cubes $\mod 7$ are 0, 1, and 6. Now, every power of 2 is congruent to 1, 2, or 4 $\mod 7$. Thus $2^y + 15 \equiv 2, 3,$ or $5 \mod 7$. This is an impossibility.

187 Example Prove that $2^k - 5, k = 0, 1, 2, \ldots$ never leaves remainder 1 when divided by 7.

Solution: $2^1 \equiv 2, 2^2 \equiv 4, 2^3 \equiv 1 \mod 7$, and this cycle of three repeats. Thus $2^k - 5$ can leave only remainders 3, 4, or 6 upon division by 7.

188 Example (AIME, 1994) The increasing sequence

$$3, 15, 24, 48, \ldots,$$

consists of those positive multiples of 3 that are one less than a perfect square. What is the remainder when the 1994-th term of the sequence is divided by 1000?

Solution: We want $3 | n^2 - 1 = (n-1)(n+1)$. Since 3 is prime, this requires $n = 3k+1$ or $n = 3k-1, k = 1, 2, 3, \ldots$. The sequence $3k+1, k = 1, 2, \ldots$ produces the terms $n^2 - 1 = (3k+1)^2 - 1$ which are the terms at even places of the sequence of $3, 15, 24, 48, \ldots$. The sequence $3k-1, k = 1, 2, \ldots$ produces the terms $n^2 - 1 = (3k-1)^2 - 1$ which are the terms at odd places of the sequence $3, 15, 24, 48, \ldots$. We must find the 997th term of the sequence $3k+1, k = 1, 2, \ldots$. Finally, the term sought is $(3(997)+1)^2 - 1 \equiv (3(-3)+1)^2 - 1 \equiv 8^2 - 1 \equiv 63 \mod 1000$. The remainder sought is 63.

189 Example (USAMO, 1979) Determine all nonnegative integral solutions

$$(n_1, n_2, \ldots, n_{14})$$

if any, apart from permutations, of the Diophantine equation

$$n_1^4 + n_2^4 + \cdots + n_{14}^4 = 1599.$$

Solution: There are no such solutions. All perfect fourth powers $\mod 16$ are $\equiv 0$ or $1 \mod 16$. This means that

$$n_1^4 + \cdots + n_{14}^4$$

can be at most $14 \mod 16$. But $1599 \equiv 15 \mod 16$.

190 Example (Putnam, 1986) What is the units digit of

$$\left\lfloor \frac{10^{20000}}{10^{100}+3} \right\rfloor?$$

Solution: Set $a - 3 = 10^{100}$. Then $[(10^{20000})/10^{100}+3] = [(a-3)^{200}/a] = [\frac{1}{a}\sum_{k=0}^{200}\binom{200}{k}a^{200-k}(-3)^k] = \sum_{k=0}^{199}\binom{200}{k}a^{199-k}(-3)^k$. Since $\sum_{k=0}^{200}(-1)^k\binom{200}{k} = 0, (3)^{199}\sum_{k=0}^{199}(-1)^k\binom{200}{k} = -3^{199}$. As $a \equiv 3 \mod 10$,

$$\sum_{k=0}^{199}\binom{200}{k}a^{199-k}(-3)^k \equiv 3^{199}\sum_{k=0}^{199}(-1)^k\binom{200}{k} \equiv -3^{199} \equiv 3 \mod 10.$$

191 Example Prove that for any $a,b,c \in \mathbb{Z}, n \in \mathbb{N}, n > 3$, there is an integer k such that $n \not|(k+a), n \not|(k+b), n \not|(k+c)$.

Solution: The integers a,b,c belong to at most three different residue classes $\mod n$. Since $n > 3$, we have more than three distinct residue classes. Thus there must be a residue class, say k for which $-k \not\equiv a, -k \not\equiv b, -k \not\equiv c, \mod n$. This solves the problem.

192 Example (Putnam, 1973) Let $a_1, a_2, \ldots, a_{2n+1}$ be a set of integers such that if any one of them is removed, the remaining ones can be divided into two sets of n integers with equal sums. Prove that $a_1 = a_2 = \ldots = a_{2n+1}$.

Solution: As the sum of the $2n$ integers remaining is always even, no matter which of the a_k be taken, all the a_k must have the same parity. The property stated in the problem is now shared by $a_k/2$ or $(a_k - 1)/2$, depending on whether they are all even, or all odd. Thus they are all congruent $\mod 4$. Continuing in this manner we arrive at the conclusion that the a_k are all congruent $\mod 2^k$ for every k, and this may only happen if they are all equal.

193 Example Prove that

$$(kn)! \equiv 0 \mod \prod_{r=0}^{n-1}(n+r)$$

if $n,k \in \mathbb{N}, n \geq k \geq 2$.

Solution: $(kn)! = M(n-1)!n(n+1)\cdots(2n-1)$ for some integer $M \geq 1$. The assertion follows.

194 Example Let

$$n!! = n!\left(1/2! - 1/3! + \cdots + (-1)^n/n!\right).$$

Prove that for all $n \in \mathbb{N}, n > 3$,

$$n!! \equiv n! \mod (n-1).$$

Solution: We have

$$\begin{aligned} n! - n!! &= n(n-1)(n-2)!(1 - 1/2! \\ &\qquad + \cdots + (-1)^{n-1}/(n-1)! + (-1)^n/n!) \\ &= (n-1)\left(m + (-1)^{n-1}n/(n-1) + (-1)^n/(n-1)\right) \\ &= (n-1)\left(m + (-1)^n\right), \end{aligned}$$

where $\mathscr{M}$ is an integer, since $(n-2)!$ is divisible by $k!, k \leq n-2$.

195 Example Prove that

$$\sum_{k=0}^{6n+2}\binom{6n+2}{2k}3^k \equiv 0, 2^{3n+1}, -2^{3n+1} \mod 2^{3n+2}$$

when n is of the form $2k, 4k+3$ or $4k+1$ respectively.

Solution: Using the Binomial Theorem,

$$2S := 2\sum_{k=0}^{3n+1}\binom{6n+2}{2k}3^k = (1+\sqrt{3})^{6n+2} + (1-\sqrt{3})^{6n+2}.$$

Also, if n is odd, with $a = 2+\sqrt{3}, b = 2-\sqrt{3}$,

$$\begin{aligned} \frac{1}{2}(a^{3n+1} + b^{3n+1}) &= \sum_{r=0}^{\frac{3n+1}{2}}\binom{3n+1}{2r}2^{3n+1-2r}3^r. \\ &\equiv 3^{(3n+1)/2} \mod 4 \\ &\equiv (-1)^{(n-1)/2} \mod 4. \end{aligned}$$

As $2S = 2^{3n+1}(a^{3n+1}+b^{3n+1})$, we have, for odd n,

$$S \equiv (-1)^{(n-1)/2}2^{3n+1} \mod 2^{3n+3}.$$

If n is even,

$$\begin{aligned}\frac{1}{2}(a^{3n+1}+b^{3n+1}) &= \sum_{2r\leq 3n}\binom{3n+1}{2r+1}2^{2r+1}3^{3n-2r}\\ &\equiv 2(6n+1)3^{3n} \mod 8\\ &\equiv 4n+2 \mod 8.\end{aligned}$$

So for even $n, S \equiv 2^{3n+2}2n+1 \mod 2^{3n+4}$.

Practice

196 Problem Find the number of all $n, 1 \leq n \leq 25$ such that $n^2+15n+122$ is divisible by 6.

(Hint: $n^2+15n+122 \equiv n^2+3n+2 = (n+1)(n+2) \mod 6.$)

197 Problem (AIME 1983) Let $a_n = 6^n + 8^n$. Determine the remainder when a_{83} is divided by 49.

198 Problem (Polish Mathematical Olympiad) What digits should be put instead of x and y in $30x0y03$ in order to give a number divisible by 13?

199 Problem Prove that if $9|(a^3+b^3+c^3)$, then $3|abc$, for integers a, b, c.

200 Problem Describe all integers n such that $10|n^{10}+1$.

201 Problem Prove that if

$$a-b, a^2-b^2, a^3-b^3, a^4-b^4, \ldots$$

are all integers, then a and b must also be integers.

202 Problem Find the last digit of 3^{100}.

203 Problem (AHSME 1992) What is the size of the largest subset S of $\{1, 2, \ldots, 50\}$ such that no pair of distinct elements of S has a sum divisible by 7?

204 Problem Prove that there are no integer solutions to the equation $x^2 - 7y = 3$.

205 Problem Prove that if $7|a^2+b^2$ then $7|a$ and $7|b$.

206 Problem Prove that there are no integers with

$$800000007 = x^2+y^2+z^2.$$

207 Problem Prove that the sum of the decimal digits of a perfect square cannot be equal to 1991.

208 Problem Prove that

$$7|4^{2^n}+2^{2^n}+1$$

for all natural numbers n.

209 Problem Prove that 5 never divides

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

210 Problem Prove that if p is a prime, $\binom{n}{p} - [\frac{n}{p}]$ is divisible by p, for all $n \geq p$.

211 Problem How many perfect squares are there $\mod 2^n$?

212 Problem Prove that every non-multiple of 3 is a perfect power of 2 $\mod 3^n$.

213 Problem Find the last two digits of 3^{100}.

214 Problem (USAMO, 1986) What is the smallest integer $n > 1$, for which the root-mean-square of the first n positive integers is an integer?

Note. The root mean square of n numbers $a_1, a_2, \ldots, a_n$ is defined to be

$$\left(\frac{a_1^2+a_2^2+\cdots+a_n^2}{n}\right)^{1/2}.$$

215 Problem Find all integers $a, b, c, a > 1$ and all prime numbers p, q, r which satisfy the equation

$$p^a = q^b + r^c$$

$(a, b, c, p, q, r$ need not necessarily be different).

216 Problem Show that the number 16 is a perfect 8-th power mod p for any prime p.

217 Problem (IMO, 1975) Let $a_1, a_2, a_3, \ldots$ be an increasing sequence of positive integers. Prove that for every $s \geq 1$ there are infinitely many a_m that can be written in the form $a_m = xa_s + ya_t$ with positive integers x and y and $t > s$.

218 Problem For each integer $n > 1$, prove that $n^n - n^2 + n - 1$ is divisible by $(n-1)^2$.

219 Problem Let x and $a_i, i = 0, 1, \ldots, k$ be arbitrary integers. Prove that

$$\sum_{i=0}^{k} a_i (x^2 + 1)^{3i}$$

is divisible by $x^2 \pm x + 1$ if and only if $\sum_{i=0}^{k} (-1)^i a_i$ is divisible by $x^2 \pm x + 1$.

220 Problem ($(UM)^2C^9$ 1992) If x, y, z are positive integers with

$$x^n + y^n = z^n$$

for an odd integer $n \geq 3$, prove that z cannot be a prime-power.

3.2 Divisibility Tests

Working base-ten, we have an ample number of rules of divisibility. The most famous one is perhaps the following.

221 Theorem (Casting-out 9's) A natural number n is divisible by 9 if and only if the sum of it digits is divisible by 9.

> **Proof:** *Let* $n = a_k 10^k + a_{k-1} 10^{k-1} + \cdots + a_1 10 + a_0$ *be the base-10 expansion of* n*. As* $10 \equiv 1 \mod 9$, *we have* $10^j \equiv 1 \mod 9$. *It follows that* $n = a_k 10^k + \cdots + a_1 10 + a_0 \equiv a_k + \cdots + a_1 + a_0$, *whence the theorem.* ❏

222 Example (AHSME, 1992) The two-digit integers from 19 to 92 are written consecutively in order to form the integer

$$192021222324 \cdots 89909192.$$

What is the largest power of 3 that divides this number?

Solution: By the casting-out-nines rule, this number is divisible by 9 if and only if

$$19 + 20 + 21 + \cdots + 92 = 37^2 \cdot 3$$

is. Therefore, the number is divisible by 3 but not by 9.

223 Example (IMO, 1975) When 4444^{4444} is written in decimal notation, the sum of its digits is A. Let B be the sum of the digits of A. Find the sum of the digits of B. (A and B are written in decimal notation.)

Solution: We have $4444 \equiv 7 \mod 9$, and hence $4444^3 \equiv 7^3 \equiv 1 \mod 9$. Thus $4444^{4444} = 4444^{3(1481)} \cdot 4444 \equiv 1 \cdot 7 \equiv 7 \mod 9$. Let C be the sum of the digits of B.

By the casting-out 9's rule, $7 \equiv 4444^{4444} \equiv A \equiv B \equiv C \mod 9$. Now, $4444 \log_{10} 4444 < 4444 \log_{10} 10^4 = 17776$. This means that 4444^{4444} has at most 17776 digits, so the sum of the digits of 4444^{4444} is at most $9 \cdot 17776 = 159984$, whence $A \leq 159984$. Amongst all natural numbers ≤ 159984 the one with maximal digit sum is 99999, so it follows that $B \leq 45$. Of all the natural numbers ≤ 45, 39 has the largest digital sum, namely 12. Thus the sum of the digits of B is at most 12. But since $C \equiv 7 \mod 9$, it follows that $C = 7$.

A criterion for divisibility by 11 can be established similarly. For let $n = a_k 10^k + a_{k-1} 10^{k-1} + \cdots + a_1 10 + a_0$. As $10 \equiv -1 \mod 11$, we have $10^j \equiv (-1)^j \mod 11$. Therefore $n \equiv (-1)^k a_k + (-1)^{k-1} a_{k-1} + \cdots - a_1 + a_0 \mod 11$, that is, n is divisible by 11 if and only if the alternating sum of its digits is divisible by 11. For example, $912282219 \equiv 9 - 1 + 2 - 2 + 8 - 2 + 2 - 1 + 9 \equiv 7 \mod 11$ and so 912282219 is not divisible by 11, whereas $8924310064539 \equiv 8 - 9 + 2 - 4 + 3 - 1 + 0 - 0 + 6 - 4 + 4 - 3 + 9 \equiv 0 \mod 11$, and so 8924310064539 is divisible by 11.

224 Example (Putnam, 1952) Let

$$f(x)=\sum_{k=0}^{n} a_k x^{n-k}$$

be a polynomial of degree n with integral coefficients. If a_0, a_n and $f(1)$ are all odd, prove that $f(x)=0$ has no rational roots.

Solution: Suppose that $f(a/b)=0$, where a and b are relatively prime integers. Then $0=b^n f(a/b)=a_0b^n+a_1b^{n-1}a+\cdots+a_{n-1}ba^{n-1}+a_na^n$. By the relative primality of a and b it follows that $a|a_0, b|a_n$, whence a and b are both odd. Hence

$$a_0b^n+a_ab^{n-1}a+\cdots+a_{n-1}ba^{n-1}+a_na^n \equiv a_0+a_1+\cdots+a_n = f(1)\equiv 1 \mod 2,$$

but this contradicts that a/b is a root of f.

Practice

225 Problem (AHSME 1991) An n-digit integer is *cute* if its n digits are an arrangement of the set $\{1,2,\ldots,n\}$ and its first k digits form an integer that is divisible by k for all $k, 1\leq k\leq n$. For example, 321 is a cute three-digit number because 1 divides 3, 2 divides 32, and 3 divides 321. How many cute six-digit integers are there?

Answer: 2.

226 Problem How many ways are there to roll two distinguishable dice to yield a sum that is divisible by three?

Answer: 12.

227 Problem Prove that a number is divisible by $2^k, k\in\mathbb{N}$ if and only if the number formed by its last k digits is divisible by 2^k. Test whether

$$90908766123456789999872$$

is divisible by 8.

228 Problem An old receipt has faded. It reads 88 chickens at the total of $\$x4.2y$, where x and y are unreadable digits. How much did each chicken cost?

Answer: 73 cents.

229 Problem Five sailors plan to divide a pile of coconuts amongst themselves in the morning. During the night, one of them wakes up and decides to take his share. After throwing a coconut to a monkey to make the division come out even, he takes one fifth of the pile and goes back to sleep. The other four sailors do likewise, one after the other, each throwing a coconut to the monkey and taking one fifth of the remaining pile. In the morning the five sailors throw a coconut to the monkey and divide the remaining coconuts into five equal piles. What is the smallest amount of coconuts that could have been in the original pile?

Answer: 15621

230 Problem Prove that a number which consists of 3^n identical digits is divisible by 3^n. For example, 111 111 111 is divisible by 9.

231 Problem ($(UM)^2C^8$ 1991) Suppose that $a_0, a_1, \ldots a_n$ are integers with $a_n\neq 0$, and let

$$p(x)=a_0+a_1x+\cdots+a_nx^n.$$

Suppose that x_0 is a rational number such that $p(x_0)=0$. Show that if $1\leq k\leq n$, then

$$a_kx_0+a_{k+1}x_0^2+\cdots+a_nx^{n-k+1}$$

is an integer.

232 Problem 1953 digits are written in a circular order. Prove that if the 1953-digit numbers obtained when we read these digits in dextrogyral sense beginning with one of the digits is divisible by 27, then if we read these digits in the same direction beginning with any other digit, the new 1953-digit number is also divisible by 27.

233 Problem (Lagrange) Prove that

$$f_{n+60}\equiv f_n \mod 10.$$

Thus the last digit of a Fibonacci number recurs in cycles of length 60.

234 Problem Prove that

$$f_{2n+1}\equiv f_{n+1}^2 \mod f_n^2.$$

3.3 Complete Residues

The following concept will play a central role in our study of integers.

235 Definition If $a \equiv b \mod n$ then b is called a *residue* of a modulo n. A set $a_1, a_2, \ldots a_n$ is called a *complete residue system* modulo n if for every integer b there is exactly one index j such that $b \equiv a_j \mod n$.

It is clear that given any finite set of integers, this set will form a complete set of residues modulo n if and only if the set has n members and every member of the set is incongruent modulo n. For example, the set $\mathscr{A} = \{0,1,2,3,4,5\}$ forms a complete set of residues $\mod 6$, since any integer x is congruent to one and only one member of $\mathscr{A}$. Notice that the set $\mathscr{B} = \{-40,6,7,15,22,35\}$ forms a complete residue set $\mod 6$, but the set $\mathscr{C} = \{-3,-2,-1,1,2,3\}$ does not, as $-3 \equiv 3 \mod 6$.

$+_3$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

Table 3.1: Addition Table for $\mathbb{Z}_3$

$+_6$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

Table 3.2: Addition Table for $\mathbb{Z}_6$

Tied up with the concept of complete residues is that of $\mathbb{Z}_n$. As an example, let us take $n = 3$. We now let 0 represent all those integers that are divisible by 3, 1 represent all those integers that leave remainder 1 upon division by 3, and 2 all those integers that leave remainder 2 upon division by 3, and consider the set $\mathbb{Z}_3 = \{0,1,2\}$. We define addition in $\mathbb{Z}_3$ as follows. Given $\mathsf{a}, \mathsf{b} \in \mathbb{Z}_3$ we consider $a + b \mod 3$. Now, there is $c \in \{0,1,2\}$ such that $a + b \equiv c \mod 3$. We then define $\mathsf{a} +_3 \mathsf{b}$ to be equal to c. Table 3.3 contains all the possible additions.

We observe that $\mathbb{Z}_3$ together with the operation $+_3$ as given in Table 3.3 satisfies the following properties:

1. The element $\mathsf{0} \in \mathbb{Z}_3$ is an *identity element* for $\mathbb{Z}_3$, i.e. $\mathsf{0}$ satisfies $\mathsf{0} +_3 \mathsf{a} = \mathsf{a} +_3 \mathsf{0} = \mathsf{a}$ for all $\mathsf{a} \in \mathbb{Z}_3$

2. Every element $\mathsf{a} \in \mathbb{Z}_3$ has an *additive inverse* b, i.e., an element such that $\mathsf{a} +_3 \mathsf{b} = \mathsf{b} +_3 \mathsf{a} = \mathsf{0}$. We denote the additive inverse of a by $-\mathsf{a}$. In $\mathbb{Z}_3$ we note that $-\mathsf{0} = \mathsf{0}, -\mathsf{1} = \mathsf{2}, -\mathsf{2} = \mathsf{1}$.

3. The operation addition in $\mathbb{Z}_3$ is *associative*, that is, for all $\mathsf{a}, \mathsf{b}, \mathsf{c} \in \mathbb{Z}_3$ we have $\mathsf{a} +_3 (\mathsf{b} +_3 \mathsf{c}) = (\mathsf{a} +_3 \mathsf{b}) +_3 \mathsf{c}$.

We then say that $< \mathbb{Z}_3, +_3 >$ forms a *group* and we call it the *group of residues under addition* $\mod 3$.

Similarly we define $< \mathbb{Z}_n, +_n >$, as the *group of residues under addition* $\mod n$. As a further example we present the addition table for $< \mathbb{Z}_6, +_6 >$ on Table (1.2). We will explore later the multiplicative structure of $\mathbb{Z}_n$.

Practice

236 Problem Construct the addition tables for $\mathbb{Z}_8$ and $\mathbb{Z}_9$.

237 Problem How many distinct ordered pairs $(\mathsf{a}, \mathsf{b}) \neq (\mathsf{0}, \mathsf{0})$ are in $\mathbb{Z}_{12}$ such that $\mathsf{a} +_{12} \mathsf{b} = \mathsf{0}$?

Chapter 4

Unique Factorisation

4.1 GCD and LCM

If $a,b \in \mathbb{Z}$, not both zero, the largest positive integer that divides both a,b is called the *greatest common divisor of a and b.* This is denoted by (a,b) or sometimes by $\gcd(a,b)$. Thus if $d|a$ and $d|b$ then $d|(a,b)$, because any common divisor of a and b must divide the largest common divisor of a and b. For example, $(68,-6)=2, \gcd(1998,1999)=1$.

If $(a,b)=1$, we say that a and b are *relatively prime or coprime.* Thus if a,b are relatively prime, then they have no factor greater than 1 in common.

If a,b are integers, not both zero, the smallest positive integer that is a multiple of a,b is called the *least common multiple of a and b.* This is denoted by $[a,b]$. We see then that if $a|c$ and if $b|c$, then $[a,b]|c$, since c is a common multiple of both a and b, it must be divisible by the smallest common multiple of a and b.

The most important theorem related to gcd's is probably the following.

238 Theorem (Bachet-Bezout Theorem) The greatest common divisor of any two integers a,b can be written as a linear combination of a and b, i.e., there are integers x,y with

$$(a,b)=ax+by.$$

Proof: *Let* $\mathscr{A}=\{ax+by|ax+by>0, x,y\in\mathbb{Z}\}$. *Clearly one of* $\pm a, \pm b$ *is in* $\mathscr{A}$, *as both* a,b *are not zero. By the Well Ordering Principle,* $\mathscr{A}$ *has a smallest element, say* d. *Therefore, there are* x_0,y_0 *such that* $d=ax_0+by_0$. *We prove that* $d=(a,b)$. *To do this we prove that* $d|a, d|b$ *and that if* $t|a, t|b$, *then* $t|d$.

We first prove that $d|a$. *By the Division Algorithm, we can find integers* $q,r, 0\leq r<d$ *such that* $a=dq+r$. *Then*

$$r=a-dq=a(1-qx_0)-by_0.$$

If $r>0$, *then* $r\in\mathscr{A}$ *is smaller than the smaller element of* $\mathscr{A}$, *namely* d, *a contradiction. Thus* $r=0$. *This entails* $dq=a$, *i.e.* $d|a$. *We can similarly prove that* $d|b$.

Assume that $t|a, t|b$. *Then* $a=tm, b=tn$ *for integers* m,n. *Hence* $d=ax_0+bx_0=t(mx_0+ny_0)$, *that is,* $t|d$. *The theorem is thus proved.* ❑

☞ *It is clear that any linear combination of* a,b *is divisible by* (a,b).

239 Lemma (Euclid's Lemma) If $a|bc$ and if $(a,b)=1$, then $a|c$.

Proof: *As* $(a,b)=1$, *by the Bachet-Bezout Theorem, there are integers* x,y *with* $ax+by=1$. *Since* $a|bc$, *there is an integer* s *with* $as=bc$. *Then* $c=c\cdot 1=cax+cby=cax+asy$. *From this it follows that* $a|c$, *as wanted.*❑

240 Theorem If $(a,b)=d$, then

$$(\frac{a}{d},\frac{b}{d})=1.$$

Proof: *By the Bachet-Bezout Theorem, there are integers* x,y *such that* $ax+by=d$. *But then* $(a/d)x+(b/d)y=1$, *and* $a/d, b/d$ *are integers. But this is a linear combination of* $a/d, b/d$ *and so* $(a/d, b/d)$ *divides this linear combination, i.e., divides 1. We conclude that* $(a/d, b/d)=1$.❑

241 Theorem Let c be a positive integer. Then

$$(ca,cb)=c(a,b).$$

Proof: *Let* $d_1=(ca,cb)$ *and* $d_2=(a,b)$. *We prove that* $d_1|cd_2$ *and* $cd_2|d_1$. *As* $d_2|a$ *and* $d_2|b$, *then* $cd_2|ca, cd_2|cb$. *Thus* cd_2 *is a common divisor of ca and cb and hence* $d_1|cd_2$. *By the Bachet-Bezout Theorem we can find integers* x,y *with* $d_1=acx+bcy=c(ax+by)$. *But* $ax+by$ *is a linear combination of* a,b *and so it is divisible by* d_2. *There is an integer s then such that* $sd_2=ax+by$. *It follows that* $d_1=csd_2$, *i.e.,* $cd_2|d_1$. ❑

☞ *It follows similarly that* $(ca,cb)=|c|(a,b)$ *for any non-zero integer c.*

242 Lemma For nonzero integers a, b, c,

$$(a,bc)=(a,(a,b)c).$$

Proof: *Since* $(a,(a,b)c)$ *divides* $(a,b)c$ *it divides bc. Thus* $\gcd(a,(a,b)c)$ *divides a and bc and hence* $\gcd(a,(a,b)c)|\gcd(a,bc)$. *On the other hand,* (a,bc) *divides a and bc, hence it divides ac and bc. Therefore* (a,bc) *divides* $(ac,bc)=c(a,b)$. *In conclusion,* (a,bc) *divides a and* $c(a,b)$ *and so it divides* $(a,(a,b)c)$. *This finishes the proof.*❑

243 Theorem $(a^2,b^2)=(a,b)^2$.

Proof: *Assume that* $(m,n)=1$. *Using the preceding lemma twice,*

$$(m^2,n^2)=(m^2,(m^2,n)n)=(m^2,(n,(m,n)m)n).$$

As $(m,n)=1$, *this last quantity equals* (m^2,n). *Using the preceding problem again,*

$$(m^2,n)=(n,(m,n)m)=1.$$

Thus $(m,n)=1$ *implies* $(m^2,n^2)=1$.

By Theorem 240,

$$\left(\frac{a}{(a,b)},\frac{b}{(a,b)}\right)=1,$$

and hence

$$\left(\frac{a^2}{(a,b)^2},\frac{b^2}{(a,b)^2}\right)=1.$$

By Theorem 241, upon multiplying by $(a,b)^2$, *we deduce*

$$(a^2,b^2)=(a,b)^2,$$

which is what we wanted.❑

244 Example Let $(a,b)=1$. Prove that $(a+b,a^2-ab+b^2)=1$ or 3.

Solution: Let $d=(a+b,a^2-ab+b^2)$. Now d divides

$$(a+b)^2-a^2+ab-b^2=3ab.$$

Hence d divides $3b(a+b)-3ab=3b^2$. Similarly, $d|3a^2$. But then $d|(3a^2,3b^2)=3(a^2,b^2)=3(a,b)^2=3$.

245 Example Let $a, a \neq 1, m, n$ be positive integers. Prove that

$$(a^m - 1, a^n - 1) = a^{(m,n)} - 1.$$

Solution: Set $d = (m,n), sd = m, td = n$. Then $a^m - 1 = (a^d)^s - 1$ is divisible by $a^d - 1$ and similarly, $a^n - 1$ is divisible by $a^d - 1$. Thus $(a^d - 1)|(a^m - 1, a^n - 1)$. Now, by the Bachet-Bezout Theorem there are integers x, y with $mx + ny = d$. Notice that x and y must have opposite signs (they cannot obviously be both negative, since then d would be negative. They cannot both be positive because then $d \geq m + n$, when in fact we have $d \leq m, d \leq n$). So, assume without loss of generality that $x > 0, y \leq 0$. Set $t = (a^m - 1, a^n - 1)$. Then $t|(a^{mx} - 1)$ and $t|(a^{-ny} - 1)$. Hence, $t|((a^{mx} - 1) - a^d(a^{-ny} - 1)) = a^d - 1$. The assertion is established.

246 Example (IMO, 1959) Prove that the fraction $\dfrac{21n+4}{14n+3}$ is irreducible for every natural number n.

Solution: $2(21n+4) - 3(14n+3) = -1$. Thus the numerator and the denominator have no common factor greater than 1.

247 Example (AIME, 1985) The numbers in the sequence

$$101, 104, 109, 116, \ldots$$

are of the form $a_n = 100 + n^2, n = 1, 2, \ldots$. For each n let $d_n = (a_n, a_{n+1})$. Find $\max\limits_{n \geq 1} d_n$.

Solution: We have the following: $d_n = (100 + n^2, 100 + (n+1)^2) = (100 + n^2, 100 + n^2 + 2n + 1) = (100 + n^2, 2n + 1)$. Thus $d_n|(2(100+n^2) - n(2n+1)) = 200 - n$. Therefore $d_n|(2(200-n) + (2n+1)) = 401$. This means that $d_n|401$ for all n. Could it be that large? The answer is yes, for let $n = 200$, then $a_{200} = 100 + 200^2 = 100(401)$ and $a_{201} = 100 + 201^2 = 40501 = 101(401)$. Thus $\max\limits_{n \geq 1} d_n = 401$.

248 Example Prove that if m and n are natural numbers and m is odd, then $(2^m - 1, 2^n + 1) = 1$.

Solution: Let $d = (2^m - 1, 2^n + 1)$. It follows that d must be an odd number, and $2^m - 1 = kd, 2^n + 1 = ld$, for some natural numbers k, l. Therefore, $2^{mn} = (kd+1)^n = td + 1$, where $t = \sum\limits_{j=0}^{n-1} \binom{n}{j} k^{n-j} d^{n-j-1}$. In the same manner, $2^{mn} = (ld - 1)^m = ud - 1$, where we have used the fact that m is odd. As $td + 1 = ud - 1$, we must have $d|2$, whence $d = 1$.

249 Example Prove that there are arbitrarily long arithmetic progressions in which the terms are pairwise relatively prime.

Solution: The numbers $km! + 1, k = 1, 2, \ldots, m$ form an arithmetic progression of length m and common difference $m!$. Suppose that $d|(lm! + 1), d|(sm! + 1), 1 \leq l < s \leq m$. Then $d|(s(lm! + 1) - l(sm! + 1)) = (s - l) < m$. Thus $1 \leq d < m$ and so, $d|m!$. But then $d|(sm! + 1 - sm!) = 1$. This means that any two terms of this progression are coprime.

250 Example Prove that any two consecutive Fibonacci numbers are relatively prime.

Solution: Let $d = (f_n, f_{n+1})$. As $f_{n+1} - f_n = f_{n-1}$ and d divides the sinistral side of this equality, $d|f_{n-1}$. Thus $d|(f_n - f_{n-1}) = f_{n-2}$. Iterating on this process we deduce that $d|f_1 = 1$ and so $d = 1$.
Aliter: By Cassini's Identity $f_{n-1}f_{n+1} - f_n^2 = (-1)^n$. Thus $d|(-1)^n$, i.e., $d = 1$.

251 Example Prove that

$$(f_m, f_n) = f_{(n,m)}.$$

Solution: Set $d = (f_n, f_m), c = f_{(m,n)}, a = (m,n)$. We will prove that $c|d$ and $d|c$.

Since $a|m$ and $a|n$, $f_a|f_m$ and $f_a|f_n$ by Theorem 102. Thus

$$f_a|(f_m, f_m),$$

i.e., $c|d$.

Now, by the Bachet-Bezout Theorem, there are integers x, y such that $xm+yn=a$. Observe that x, y cannot be both negative, otherwise a would be negative. As $a|n, a|m$ we have $a \leq n, a \leq m$. They cannot be both positive since then $a = xm+yn \geq m+n$, a contradiction. Thus they are of opposite signs, and we assume without loss of generality that $x \leq 0, y > 0$.

Observe that

$$f_{yn} = f_{a-xm} = f_{a-1}f_{-xm} + f_a f_{-xm+1}$$

upon using the identity

$$f_{s+t} = f_{s-1}f_t + f_s f_{t+1}$$

of Theorem 50. As $n|yn, m|(-xm)$, we have that $f_n|f_{yn}$, $f_m|f_{-xm}$. This implies that $(f_n, f_m)|f_{yn}$ and $(f_n, f_m)|f_{-xm}$. Hence

$$(f_n, f_m)|f_a f_{-xm+1}.$$

We saw earlier that $(f_n, f_m)|f_{-xm}$. If it were the case that

$$(f_n, f_m)|f_{-xm+1},$$

then (f_n, f_m) would be dividing two consecutive Fibonacci numbers, a contradiction to the preceding problem in the case when $(f_n, f_m) > 1$. The case $= 1$ is a triviality. Therefore $(f_n, f_m)|f_a$, which is what we wanted to prove.

252 Example Prove that no odd Fibonacci number is ever divisible by 17.

Solution: Let $d = (17, f_n)$, which obviously must be odd. Then $(17, f_n) = (34, f_n) = (f_9, f_n) = f_{(9,n)} = f_1, f_3$ or f_9. This means that $d = (17, f_n) = 1, 2$ or 34. This forces $d = 1$.

253 Example The *Catalan number of order n* is defined as

$$C_n = \frac{1}{n+1}\binom{2n}{n}.$$

Prove that C_n is an integer for all natural numbers n.

Solution: By the binomial absorption identity,

$$\frac{2n+1}{n+1}\binom{2n}{n} = \binom{2n+1}{n+1}.$$

Since $2n+1$ and $n+1$ are relatively prime, and since the dextral side is an integer, it must be the case that $n+1$ divides $\binom{2n}{n}$.

254 Example Let n be a natural number. Find the greatest common divisor of

$$\binom{2n}{1}, \binom{2n}{3}, \ldots, \binom{2n}{2n-1}.$$

Solution: Since

$$\sum_{k=1}^{n}\binom{2n}{2k-1} = 2^{2n-1},$$

the gcd must be of the form 2^a. Since the gcd must divide $\binom{2n}{1} = 2n$, we see that it has divide 2^{l+1}, where l is the largest power of 2 that divides n. We claim that 2^{l+1} divides all of them. We may write $n = 2^l m$, where $\mathscr{M}$ is odd. Now,

$$\binom{2^{l+1}m}{2k-1} = \frac{2^{l+1}m}{2k-1}\binom{2^{l+1}m-1}{2k-2}.$$

But $2k-1 \not| 2^{l+1}$ for $k > 1$. This establishes the claim.

255 Example Let any fifty one integers be taken from amongst the numbers $1, 2, \ldots, 100$. Show that there are two that are relatively prime.

Solution: Arrange the 100 integers into the 50 sets

$$\{1,2\},\{3,4\},\{5,6\}\ldots,\{99,100\}.$$

Since we are choosing fifty one integers, there must be two that will lie in the same set. Those two are relatively prime, as consecutive integers are relatively prime.

256 Example Prove that any natural number $n > 6$ can be written as the sum of two integers greater than 1, each of the summands being relatively prime.

Solution: If n is odd, we may choose $a = 2, b = n-2$. If n is even, then is either of the form $4k$ or $4k+2$. If $n = 4k$, then take $a = 2k+1, b = 2k-1$. These two are clearly relatively prime (why?). If $n = 4k+2, k > 1$ take $a = 2k+3, b = 2k-1$.

257 Example How many positive integers ≤ 1260 are relatively prime to 1260?

Solution: As $1260 = 2^2 \cdot 3^2 \cdot 5 \cdot 7$, the problem amounts to finding those numbers less than 1260 which are not divisible by 2, 3, 5, or 7. Let A denote the set of integers ≤ 1260 which are multiples of 2, B the set of multiples of 3, etc. By the Inclusion-Exclusion Principle,

$$\begin{aligned}|A\cup B\cup C\cup D| &= |A|+|B|+|C|+|D| \\ &\quad -|A\cap B|-|A\cap C|-|A\cap D| \\ &\quad -|B\cap C|-|B\cap D|-|C\cap D| \\ &\quad +|A\cap B\cap C|+|A\cap B\cap D|+|A\cap C\cap D| \\ &\quad +|B\cap C\cap D|-|A\cap B\cap C\cap D| \\ &= 630+420+252+180-210-126-90-84 \\ &\quad -60-36+42+30+18+12-6=972.\end{aligned}$$

The number of integers sought is then $1260-972 = 288$.

Practice

258 Problem Show that

$$(a,b)[a,b] = ab$$

for all natural numbers a, b.

259 Problem Find lcm $(23!41!, 29!37!)$.

260 Problem Find two positive integers a, b such that

$$a^2+b^2 = 85113, \text{ and lcm } (a,b) = 1764.$$

261 Problem Find $a, b \in \mathbb{N}$ with $(a,b) = 12, [a,b] = 432$.

262 Problem Prove that $(a,b)^n = (a^n, b^n)$ for all natural numbers n.

263 Problem Let $a \in \mathbb{N}$. Find, with proof, all $b \in \mathbb{N}$ such that

$$(2^b - 1) | (2^a + 1).$$

264 Problem Show that $(n^3 + 3n + 1, 7n^3 + 18n^2 - n - 2) = 1$.

265 Problem Let the integers a_n, b_n be defined by the relation

$$a_n + b_n\sqrt{2} = (1 + \sqrt{2})^n, \; n \in \mathbb{N}.$$

Prove that $\gcd(a_n, b_n) = 1 \; \forall \; n$.

266 Problem Prove or disprove the following two propositions:

1. If $a, b \in \mathbb{N}, a < b$, then in any set of b consecutive integers there are two whose product is divisible by ab.
2. If $a, b, c, \in \mathbb{N}, a < b < c$, then in any set of c consecutive integers there are three whose product is divisible by abc.

267 Problem Let $n, k, n \geq k > 0$ be integers. Prove that the greatest common divisor of the numbers

$$\binom{n}{k}, \binom{n+1}{k}, \ldots, \binom{n+k}{k}$$

is 1.

(Hint: Prove

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

268 Problem Let $F_n = 2^{2^n} + 1$ be the n-th *Fermat number.* Find (F_n, F_m).

269 Problem Find the greatest common divisor of the sequence

$$16^n + 10n - 1, \; n = 1, 2, \ldots.$$

270 Problem Demonstrate that $(n! + 1, (n+1)! + 1) = 1$.

271 Problem Prove that any natural number $n > 17$ can be written as $n = a + b + c$ where a, b, c are pairwise relatively prime natural numbers each exceeding 1.

(Hint: Consider $n \mod 12$. Write two of the summands in the form $6k + s$ and the third summand as a constant.)

272 Problem Prove that there are no positive integers $a, b, n > 1$ with

$$(a^n - b^n) | (a^n + b^n).$$

273 Problem Prove that the binomial coefficients have the following hexagonal property:

$$\gcd\left(\binom{n-1}{k-1}, \binom{n}{k+1}, \binom{n+1}{k}\right)$$

equals

$$\gcd\left(\binom{n-1}{k}, \binom{n+1}{k+1}, \binom{n}{k-1}\right).$$

274 Problem (Putnam, 1974) Call a set of integers *conspiratorial* if no three of them are pairwise relatively prime. What is the largest number of elements in any conspiratorial subset of the integers 1 through 16?

4.2 Primes

Recall that a *prime number* is a positive integer greater than 1 whose only positive divisors are itself and 1. Clearly 2 is the only even prime and so 2 and 3 are the only consecutive integers which are prime. An integer different from 1 which is not prime is called *composite.* It is clear that if $n > 1$ is composite then we can write n as $n = ab, 1 < a \leq b < n, a, b \in \mathbb{N}$.

275 Theorem If $n > 1$, then n is divisible by at least one prime.

> **Proof:** *Since $n > 1$, it has at least one divisor > 1. By the Well Ordering Principle, n must have a least positive divisor greater than 1, say q. We claim that q is prime. For if not then we can write q as $q = ab, 1 < a \leq b < q$. But then a is a divisor of n greater than 1 and smaller than q, which contradicts the minimality of q.*❑

276 Theorem (Euclid) There are infinitely many primes.

> **Proof:** *Let $p_1, p_2, \ldots p_k$ be a list of primes. Construct the integer*
>
> $$n = p_1 p_2 \cdots p_k + 1.$$

This integer is greater than 1 *and so by the preceding problem, it must have a prime divisor* p*. Observe that* p *must be different from any of* $p_1, p_2, \ldots, p_k$ *since* n *leaves remainder* 1 *upon division by any of the* p_i*. Thus we have shown that no finite list of primes exhausts the set of primes, i.e., that the set of primes is infinite.*❑

277 Lemma The product of two numbers of the form $4k+1$ is again of that form.

Proof: $(4a+1)(4b+1) = 4(4ab+a+b)+1.$❑

278 Theorem There are infinitely many primes of the form $4n+3$.

Proof: *Any prime either equals* 2*, or is of the form* $4k \pm 1$*. We will show that the collection of primes of the form* $4k-1$ *is inexhaustible. Let*

$$\{p_1, p_2, \ldots p_n\}$$

be any finite collection of primes of the form $4k-1$*. Construct the number*

$$N = 4p_1p_2\cdots p_n - 1.$$

Since each p_k *is* $\geq 3, N \geq 11$*. Observe that* N *is not divisible by any of the primes in our collection. Now either* N *is a prime, in which case it is a prime of the form* $4k-1$ *not on the list, or it is a product of primes. In the latter case, all of the prime factors of* N *cannot be of the form* $4k+1$*, for the product of any two primes of this form is again of this form, in view of the preceding problem. Thus* N *must be divisible by some prime of the form* $4k-1$ *not on the list. We have thus shown that given any finite list of primes of the form* $4k-1$ *we can always construct an integer which is divisible by some prime of the form* $4k-1$ *not on that list. The assertion follows.* ❑

279 Example Prove that there are arbitrarily long strings that do not contain a prime number.

Solution: Let $k \in \mathbb{N}, k \geq 2$. Then each of the numbers

$$k!+2, \ldots, k!+k$$

is composite.

280 Theorem If the positive integer n is composite, then it must have a prime factor p with $p \leq \sqrt{n}$.

Proof: *Suppose that* $n = ab, 1 < a \leq b < n$*. If both* a *and* b *are* $> \sqrt{n}$*, then* $n = ab > \sqrt{n}\sqrt{n} = n$*, a contradiction. Thus* n *has a factor* $\neq 1$ *and* $\leq \sqrt{n}$*, and hence a prime factor, which is* $\leq \sqrt{n}$*.* ❑

281 Example Find the number of prime numbers ≤ 100.

Solution: Observe that $\sqrt{100} = 10$. By the preceding theorem, all the composite numbers in the range $10 \leq n \leq 100$ have a prime factor amongst $2, 3, 5$, or 7. Let A_m denote the multiples of $\mathscr{M}$ which are ≤ 100. Then $|A_2| = 50, |A_3| = 33, |A_5| = 20, |A_7| = 14, |A_6| = 16, |A_{10}| = 10, |A_{14}| = 7, |A_{15}| = 6, |A_{21}| = 4, |A_{35}| = 2, |A_{30}| = 3, |A_{42}| = 2, |A_{70}| = 1, |A_{105}| = 0, |A_{210}| = 0$. Thus the number of primes ≤ 100 is

$$\begin{aligned}
&= 100 - (\text{ number of composites } \leq 1) - 1 \\
&= 4 + 100 - \text{ multiples of 2, 3, 5, or } 7 \leq 100 - 1 \\
&= 4 + 100 - (50+33+20+14) + (16+10+7+6+4+2) \\
&\quad -(3+2+1+0) - 0 - 1 \\
&= 25,
\end{aligned}$$

where we have subtracted the 1, because 1 is neither prime nor composite.

282 Lemma If p is a prime, $\binom{p}{k}$ is divisible by p for all $0 < k < p$.

Proof:

$$\binom{p}{k} = \frac{p(p-1)\cdots(p-k+1)}{k!}$$

yields

$$k!\binom{p}{k} = p(p-1)\cdots(p-k+1),$$

whence $p|k!\binom{p}{k}$. *Now, as* $k < p, p \not| k!$. *By Euclid's Lemma, it must be the case that* $p|\binom{p}{k}$.❑

283 Example Prove that if p is a prime, then p divides $2^p - 2$.

Solution: By the Binomial Theorem:

$$2^p - 2 = (1+1)^p - 2 = \binom{p}{1} + \binom{p}{2} + \cdots + \binom{p}{p-1},$$

as $\binom{p}{0} = \binom{p}{p} = 1$. By the preceding lemma, p divides each of the terms on the dextral side of the above. This establishes the assertion.

Practice

284 Problem Prove that there are infinitely many primes of the form $6n+5$.

285 Problem Use the preceding problem to show that there are infinitely many primes p such that $p-2$ is not a prime.

286 Problem If p and q are consecutive odd primes, prove that the prime factorisation of $p+q$ has at least three (not necessarily distinct) primes.

287 Problem

1. Let p be a prime and let $n \in \mathbb{N}$. Prove, by induction on n, that $p|(n^p - n)$.
2. Extend this result to all $n \in \mathbb{Z}$.
3. Prove *Fermat's Little Theorem*: if $p \not| n$, then $p|(n^{p-1} - 1)$.
4. Prove that $42|n^7 - n, n \in \mathbb{Z}$.
5. Prove that $30|n^5 - n, n \in \mathbb{Z}$.

288 Problem Let p be an odd prime and let $(a,b) = 1$. Prove that

$$\left(a+b, \frac{a^p + b^p}{a+b}\right) \text{ divides } p.$$

289 Problem Prove that $3, 5, 7$ is the only prime triplet of the form $p, p+2, p+4$.

290 Problem Let $n > 2$. Prove that if one of the numbers $2^n - 1$ and $2^n + 1$ is prime, then the other is composite.

4.3 Fundamental Theorem of Arithmetic

Consider the integer 1332. It is clearly divisible by 2 and so we obtain $1332 = 2 \cdot 666$. Now, 666 is clearly divisible by 6, and so $1332 = 2 \cdot 2 \cdot 3 \cdot 111$. Finally, 111 is also divisible by 3 and so we obtain $1332 = 2 \cdot 2 \cdot 3 \cdot 3 \cdot 37$. We cannot further decompose 1332 as a product of positive integers greater than 1, as all $2, 3, 37$ are prime. We will show now that such decomposition is always possible for a positive integer greater than 1.

291 Theorem Every integer greater than 1 is a product of prime numbers.

Proof: *Let $n > 1$. If n is a prime, then we have nothing to prove. Assume that n is composite and let q_1 be its least proper divisor. By Theorem 4.5, q_1 is a prime. Set $n = q_1 n_1, 1 < n_1 < n$. If n_1 is a prime, then we arrived at the result. Otherwise, assume that n_1 is composite, and let q_2 be its least prime divisor, as guaranteed by Theorem 4.5.*

> *We can write then $n = q_1 q_2 n_2, 1 < n_2 < n_1 < n$. Continuing the argument, we arrive at a chain $n > n_1 > n_2 \cdots > 1$, and this process must stop before n steps, as n is a positive integer. Eventually we then have $n = q_1 q_2 \cdots q_s$.* ❑

We may arrange the prime factorisation obtained in the preceding Theorem as follows,

$$n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}, \ \ a_1 > 0, a_2 > 0, \ldots, a_k > 0,$$

$$p_1 < p_2 < \cdots < p_k,$$

where the p_j are primes. We call the preceding factorisation of n, the *canonical factorisation* of n. For example $2^3 3^2 5^2 7^3$ is the canonical factorisation of 617400.

292 Theorem (Fundamental Theorem of Arithmetic) Every integer > 1 can be represented as a product of primes in only one way, apart from the order of the factors.

> **Proof:** *We prove that a positive integer greater than 1 can only have one canonical factorisation. Assume that*
>
> $$n = p_1^{a_1} p_2^{a_2} \cdots p_s^{a_s} = q_1^{b_1} q_2^{b_2} \cdots q_t^{b_t}$$
>
> *are two canonical factorisations of n. By Euclid's Lemma (example 1.2) we conclude that every p must be a q and every q must be a p. This implies that $s = t$. Also, from $p_1 < p_2 < \cdots < p_s$ and $q_1 < q_2 < \cdots < q_t$ we conclude that $p_j = q_j, 1 \leq j \leq s$.*
>
> *If $a_j > b_j$ for some j then, upon dividing by $p_j^{b_j}$, we obtain*
>
> $$p_1^{a_1} p_2^{a_2} \cdots p_j^{a_j - b_j} \cdots p_s^{a_s} = p_1^{b_1} p_2^{b_2} \cdots p_{j-1}^{b_{j-1}} p_{j+1}^{b_{j+1}} \cdots p_s^{b_s},$$
>
> *which is impossible, as the sinistral side is divisible by p_j and the dextral side is not. Similarly, the alternative $a_j < b_j$ for some j is ruled out and so $a_j = b_j$ for all j. This finishes the proof.* ❑

It is easily seen, by the Fundamental Theorem of Arithmetic, that if a has the prime factorisation $a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}$ and b has the prime factorisation $b = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n}$, (it may be the case that some of the a_k and some of the b_k are zero) then

$$(a,b) = p_1^{\min(a_1,b_1)} p_2^{\min(a_2,b_2)} \cdots p_n^{\min(a_n,b_n)}. \tag{4.1}$$

and also

$$[a,b] = p_1^{\max(a_1,b_1)} p_2^{\max(a_2,b_2)} \cdots p_n^{\max(a_n,b_n)}. \tag{4.2}$$

Since $x + y = \max(x,y) + \min(x,y)$, it clearly follows that

$$ab = (a,b)[a,b].$$

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

Solution: Assume that $\sqrt{2} = a/b$ with relatively prime natural numbers a, b. Then $2b^2 = a^2$. The sinistral side of this last equality has an odd number of prime factors (including repetitions), whereas the dextral side has an even number of prime factors. This contradicts the Fundamental Theorem of Arithmetic.

294 Example Prove that if the polynomial

$$p(x) = a_0 x^n + a_1 x^{n-1} + \cdots + a_{n-1} x + a_n$$

with integral coefficients assumes the value 7 for four integral values of x, then it cannot take the value 14 for any integral value of x.

Solution: First observe that the integer 7 can be decomposed into at most three different integer factors $7 = -7(1)(-1)$. Assume that $p(a_k) - 7 = 0$ for distinct $a_k, 1 \leq k \leq 4$. Then

$$p(x) - 7 = (x - a_1)(x - a_2)(x - a_3)(x - a_4)q(x)$$

for a polynomial q with integer coefficients. Assume that there is an integer $\mathscr{M}$ with $p(m) = 14$. Then

$$7 = p(m) - 7 = (m - a_1)(m - a_2)(m - a_3)(m - a_4)q(m).$$

Since the factors $m - a_k$ are all distinct, we have decomposed the integer 7 into at least four different factors. This is impossible, by the Fundamental Theorem of Arithmetic.

295 Example Prove that the product of three consecutive integers is never a perfect power (i.e., a perfect square or a perfect cube, etc.).

Solution: Let the integer be $(n-1)n(n+1) = (n^2 - 1)n$. Since $n^2 - 1$ and n are relatively prime, by the Fundamental Theorem of Arithmetic, $n^2 - 1$ is a perfect kth power $(k \geq 2)$ and n is also a perfect kth power. But then, $n^2 - 1$ and n^2 would be *consecutive* perfect kth powers, sheer nonsense.

296 Example Prove that $m^5 + 3m^4n - 5m^3n^2 - 15m^2n^3 + 4mn^4 + 12n^5$ is never equal to 33.

Solution: Observe that

$$\begin{aligned} & m^5 + 3m^4n - 5m^3n^2 - 15m^2n^3 + 4mn^4 + 12n^5 \\ & = (m - 2n)(m - n)(m + n)(m + 2n)(m + 3n). \end{aligned}$$

Now, 33 can be decomposed as the product of at most four different integers $33 = (-11)(3)(1)(-1)$. If $n \neq 0$, the factors in the above product are all different. They cannot be multiply to 33, by the Fundamental Theorem of Arithmetic, as 33 is the product of 4 different factors and the expression above is the product of 5 different factors for $n \neq 0$.. If $n = 0$, the product of the factors is m^5, and 33 is clearly not a fifth power.

297 Example Prove that the sum

$$S = 1/2 + 1/3 + 1/4 + \cdots + 1/n$$

is never an integer.

Solution: Let k be the largest integer such that $2^k \leq n$, and P the product of all the odd natural numbers not exceeding n. The number $2^{k-1}PS$ is a sum, all whose terms, except for $2^{k-1}P\dfrac{1}{2^k}$, are integers.

298 Example Prove that there is exactly one natural number n for with $2^8 + 2^{11} + 2^n$ is a perfect square.

Solution: If $k^2 = 2^8 + 2^{11} + 2^n = 2304 + 2^n = 48^2 + 2^n$, then $k^2 - 48^2 = (k - 48)(k + 48) = 2^n$. By unique factorisation, $k - 48 = 2^s, k + 48 = 2^t, s + t = n$. But then $2^t - 2^s = 96 = 3 \cdot 2^5$ or $2^s(2^{t-s} - 1) = 3 \cdot 2^5$. By unique factorisation, $s = 5, t - s = 2$, giving $s + t = n = 12$.

299 Example Prove that in any set of 33 distinct integers with prime factors amongst $\{5, 7, 11, 13, 23\}$, there must be two whose product is a square.

Solution: Any number in our set is going to have the form

$$5^a 7^b 11^c 13^d 23^f.$$

Thus to each number in the set, we associate a vector (a, b, c, d, f). These vectors come in 32 different flavours, according to the parity of the components. For example (even, odd, odd, even, odd) is one such class. Since we have 33 integers, two (at least) will have the same parity in their exponents, and the product of these two will be a square.

300 Example (IMO, 1985) Given a set $\mathscr{M}$ of 1985 distinct positive integers, none with a prime factor greater than 26, prove that $\mathscr{M}$ contains a subset of four distinct elements whose product is the fourth power of an integer.

Solution: Any number in our set is going to be of the form

$$2^a 3^b 5^c 7^d 11^f 13^g 17^h 19^j 23^k.$$

Thus if we gather 513 of these numbers, we will have two different ones whose product is a square.

Start weeding out squares. Since we have $1985 > 513$ numbers, we can find a pair of distinct a_1, b_1 such that $a_1 b_1 = c_1^2$. Delete this pair. From the 1983 integers remaining, we can find a pair of distinct a_2, b_2 such that $a_2 b_2 = c_2^2$. Delete this pair. From the 1981 integers remaining, we can find a pair a_3, b_3 such that $a_3 b_3 = c_3^2$. We can continue this operation as long as we have at least 513 integers. Thus we may perform this operation $n+1$ times, were n is the largest positive integer such that $1985 - 2n \geq 513$, i.e., $n = 736$. Therefore, we are able to gather 737 pairs a_k, b_k such that $a_k b_k = c_k^2$. Now, the 737 numbers c_k have all their prime factors smaller than 26, and since $737 > 513$, we may find two distinct c_m say c_i and $c_j, i \neq j$, such that $c_i c_j = a^2$, a perfect square. But then $c_i c_j = a^2$ implies that $a_i b_i a_j b_j = a^4$, a fourth power. Thus we have found four distinct numbers in our set whose product is a fourth power.

301 Example Let any fifty one integers be taken from amongst the numbers $1, 2, \ldots, 100$. Show that there must be one that divides some other.

Solution: Any of the fifty one integers can be written in the form $2^a m$, where m is odd. Since there are only fifty odd integers between 1 and 100, there are only fifty possibilities for m. Thus two (at least) of the integers chosen must share the same odd part, and thus the smaller will divide the larger.

302 Example (USAMO 1972) Prove that

$$\frac{[a,b,c]^2}{[a,b][b,c][c,a]} = \frac{(a,b,c)^2}{(a,b)(b,c)(c,a)}.$$

Solution: Put

$$a = \prod p_k^{\alpha_k},\ b = \prod p_k^{\beta_k},\ c = \prod p_k^{\gamma_k},$$

with primes p_k. The assertion is equivalent to showing

$$\begin{aligned} &2\max(\alpha_k, \beta_k, \gamma_k) - \max(\alpha_k, \beta_k) - \max(\alpha_k, \gamma_k) - \max(\beta_k, \gamma_k) \\ &= 2\min(\alpha_k, \beta_k, \gamma_k) - \min(\alpha_k, \beta_k) - \min(\alpha_k, \gamma_k) - \min(\beta_k, \gamma_k). \end{aligned}$$

By symmetry, we may assume, without loss of generality, that $\alpha_k \geq \beta_k \geq \gamma_k$. The equation to be established reduces thus to the identity

$$2\alpha_k - \alpha_k - \alpha_k - \beta_k = 2\gamma_k - \beta_k - \gamma_k - \gamma_k.$$

303 Example Prove that $n = 24$ is the largest natural number divisible by all integral $a, 1 \leq a \leq \sqrt{n}$.

Solution: Suppose n is divisible by all the integers $\leq \sqrt{n}$. Let $p_1 = 2, p_2 = 3, \ldots, p_l$ be all the primes $\leq \sqrt{n}$, and let k_j be the unique integers such that $p_j^{k_j} \leq \sqrt{n} < p_j^{k_j+1}$. Clearly $n^{l/2} < p_1^{k_1+1} p_2^{k_2+1} \cdots p_l^{k_l+1}$. Let $\operatorname{lcm}(1, 2, 3, \ldots, \llbracket \sqrt{n} \rrbracket - 1, \llbracket \sqrt{n} \rrbracket) = K$. Clearly then $K = p_1^{k_1} p_2^{k_2} \cdots p_l^{k_l}$. Hence $p_1^{k_1+1} p_2^{k_2+1} \cdots p_l^{k_l+1} \leq K^2$ and thus $n^{l/2} < K^2$. By hypothesis, n must be divisible by K and so $K \leq n$. Consequently, $n^{l/2} < n^2$. This implies that $l < 4$ and so $n < 49$. By inspection, we see that the only valid values for n are $n = 2, 4, 6, 8, 12, 24$.

304 Example (Irving Kaplansky) A positive integer n has the property that for $0 < l < m < n$,

$$S = l + (l+1) + \ldots + m$$

is never divisible by n. Prove that this is possible if and only if n is a power of 2.

Solution: Set $n = s2^k$ with s odd. If $s = 1, 2S = (l+m)(m-l+1)$, which has one factor even and one factor odd, cannot be divisible by $2n = 2^{k+1}$, since, its even factor is less than $2n$. But if $s > 1$, then S is divisible by n, with $0 < l < m < n$, if we take

$$m = (s + 2^{k+1} - 1)/2$$

and

$$l = \begin{cases} 1 + m - 2^{k+1}, & s > 2^{k+1}, \\ 1 + m - s, & s < 2^{k+1}. \end{cases}$$

305 Example Let $0 < a_1 < a_2 < \cdots < a_k \leq n$, where $k > \lfloor\frac{n+1}{2}\rfloor$, be integers. Prove that

$$a_1 + a_j = a_r$$

is soluble.

Solution: The $k-1$ positive integers $a_i - a_1, 2 \leq i \leq k$, are clearly distinct. These, together with the k given distinct a's, give $2k - 1 > n$ positive integers, each not greater than n. Hence, at least one of the integers is common to both sets, so that at least once $a_r - a_1 = a_j$.

The sequence $\lfloor n/2\rfloor + 1, \lfloor n/2\rfloor + 2, \ldots, n$, shows that for $k = \lfloor (n+1)/2\rfloor$ the result is false.

306 Example Let $0 < a_1 < a_2 < \cdots < a_n \leq 2n$ be integers such that the least common multiple of any two exceeds $2n$. Prove that $a_1 > \lfloor\frac{2n}{3}\rfloor$.

Solution: It is clear that no one of the numbers can divide another (otherwise we would have an lcm $\leq 2n$). Hence, writing $a_k = 2^{t_k}A_k$, A_k odd, we see that all the A_k are different. Since there are n of them, they coincide in some order with the set of all positive odd numbers less than $2n$.

Now, consider $a_1 = 2^{t_1}A_1$. If $a_1 \leq \lfloor 2n/3\rfloor$, then $3a_1 = 2^{t_1}3A_1 \leq 2n$, and $3A_1 < 2n$. Since $3A_1$ would then be an odd number $< 2n$, $3A_1 = A_j$ for some j, and $a_j = 2^{t_j}3A_1$. Thus either $[a_1, a_j] = 2^{t_1}3A_1 = 3a_1 \leq 2n$, or $[a_1, a_j] = 2^{t_j}3A_1 = a_j \leq 2n$. These contradictions establish the assertion.

307 Example (Putnam, 1980) Derive a formula for the number of quadruples (a, b, c, d) such that

$$3^r7^s = [a, b, c] = [b, c, d] = [c, d, a] = [d, a, b].$$

Solution: By unique factorisation, each of a, b, c, d must be of the form $3^m7^n, 0 \leq m \leq r, 0 \leq n \leq s$. Moreover, $\mathscr{M}$ must equal r for at least two of the four numbers, and n must equal s for at least two of the four numbers. There are $\binom{4}{2}r^2 = 6r^2$ ways of choosing exactly two of the four numbers to have exponent r, $\binom{4}{3}r = 4r$ ways of choosing exactly three to have exponent r and $\binom{4}{4} = 1$ of choosing the four to have exponent r. Thus there is a total of $1 + 4r + 6r^2$ of choosing at least two of the four numbers to have exponent r. Similarly, there are $1 + 4s + 6s^2$ ways of choosing at least two of the four numbers to have exponent s. The required formula is thus

$$(1 + 4r + 6r^2)(1 + 4s + 6s^2).$$

Practice

308 Problem Prove that $\log_{10} 7$ is irrational.

309 Problem Prove that

$$\frac{\log 3}{\log 2}$$

is irrational.

310 Problem Find the smallest positive integer such that $n/2$ is a square and $n/3$ is a cube.

311 Problem How many integers from 1 to 10^{20} inclusive, are not perfect squares, perfect cubes, or perfect fifth powers?

312 Problem Prove that the sum

$$1/3+1/5+1/7+\cdots+1/(2n+1)$$

is never an integer.

(Hint: Look at the largest power of $3 \le n$).

313 Problem Find $\min\limits_{k\ge 1} 36^k - 5^k$.

(Hint: Why is $36^k - 1 - 5^k \neq 0$?)

314 Problem (AIME 1987) Find the number of ordered triples (a,b,c) of positive integers for which $[a,b] = 1000, [b,c] = [a,c] = 2000$.

315 Problem Find the number of ways of factoring 1332 as the product of two positive relatively prime factors each greater than 1. Factorisations differing in order are considered the same.

Answer: 3.

316 Problem Let $p_1, p_2, \ldots, p_t$ be different primes and $a_1, a_2, \ldots a_t$ be natural numbers. Find the number of ways of factoring $p_1^{a_1}p_2^{a_2}\cdots p_t^{a_t}$ as the product of two positive relatively prime factors each greater than 1. Factorisations differing in order are considered the same.

Answer: $2^{t-1}-1$.

317 Problem Let $n = p_1^{a_1}p_2^{a_2}\cdots p_t^{a_t}$ and $m = p_1^{b_1}p_2^{b_2}\cdots p_t^{b_t}$, the p's being different primes. Find the number of the common factors of m and n.

Answer:

$$\prod_{k=1}^{t}(1+\min(a_k,b_k)).$$

318 Problem (USAMO 1973) Show that the cube roots of three distinct prime numbers cannot be three terms (not necessarily consecutive) of an arithmetic progression.

319 Problem Let $2 = p_1, 3 = p_2, \ldots$ be the primes in their natural order and suppose that $n \ge 10$ and that $1 < j < n$. Set

$$N_1 = p_1p_2\cdots p_{j-1}-1, N_2 = 2p_1p_2\cdots p_{j-1}-1, \ldots$$

and

$$N_{p_j} = p_jp_1p_2\cdots p_{j-1}-1$$

Prove

1. Each $p_i, j \le i \le n$, divides at most one of the $N_{p_k}, 1 \le k \le j$
2. There is a $j, 1 < j < n$, for which $p_j > n-j+1$.
3. Let s be the smallest j for which $p_j > n-j+1$. There is a $t, 1 \le t \le p_s$, such that all of $p_1, \ldots p_n$ fail to divide $tp_1p_2\cdots p_{s-1}-1$, and hence $p_{n+1} < p_1p_2\cdots p_s$.
4. The s above is > 4 and so $p_{s-1}-2 \ge s$ and $p_1p_2\cdots p_s < p_{s+1}\cdots p_n$.
5. (Bonse's Inequality) For $n \ge 4$, $p_{n+1}^2 < p_1\cdots p_n$.

320 Problem Prove that 30 is the only integer n with the following property: if $1 \le t \le n$ and $(t,n) = 1$, then t is prime.

321 Problem (USAMO 1984)

1. For which positive integers n is there a finite set S_n of n distinct positive integers such that the geometric mean of any subset of S_n is an integer?
2. Is there an *infinite* set S of distinct positive integers such that the geometric mean of any finite subset of S is an integer.

322 Problem

1. **(Putnam 1955)** Prove that there is no triplet of integers (a,b,c), except for $(a,b,c) = (0,0,0)$ for which
$$a+b\sqrt{2}+c\sqrt{3} = 0.$$
2. **(Putnam 1980)** Prove that there exist integers a, b, c, not all zero and each of absolute value less than a million, such that
$$|a+b\sqrt{2}+c\sqrt{3}| < 10^{-11}.$$
3. **(Putnam 1980)** Let a,b,c be integers, not all zero and each of absolute value less than a million. Prove that
$$|a+b\sqrt{2}+c\sqrt{3}| > 10^{-21}.$$

323 Problem (Eőtvős 1906) Let $a_1, a_2, \ldots, a_n$ be any permutation of the numbers $1, 2, \ldots, n$. Prove that if n is odd, the product

$$(a_1-1)(a_2-2)\cdots(a_n-n)$$

is an even number.

324 Problem Prove that from any sequence formed by arranging in a certain way the numbers from 1 to 101, it is always possible to choose 11 numbers (which must not necessarily be consecutive members of the sequence) which form an increasing or a decreasing sequence.

325 Problem Prove that from any fifty two integers it is always to choose two, whose sum, or else, whose difference, is divisible by 100.

326 Problem Prove that from any one hundred integers it is always possible to choose several numbers (or perhaps, one number) whose sum is divisible by 100.

327 Problem Given n numbers $x_1, x_2, \ldots, x_n$ each of which is equal to ± 1, prove that if

$$x_1x_2 + x_2x_3 + \cdots + x_nx_1 = 0,$$

then n is a multiple of 4.

Chapter 5

Linear Diophantine Equations

5.1 Euclidean Algorithm

We now examine a procedure that avoids factorising two integers in order to obtain their greatest common divisor. It is called the *Euclidean Algorithm* and it is described as follows. Let a,b be positive integers. After using the Division Algorithm repeatedly, we find the sequence of equalities

$$\begin{array}{lcll} a & = & bq_1+r_2, & 0<r_2<b,\\ b & = & r_2q_2+r_3 & 0<r_3<r_2,\\ r_2 & = & r_3q_3+r_4 & 0<r_4<r_3,\\ \vdots & \vdots & \vdots & \vdots\\ r_{n-2} & = & r_{n-1}q_{n-1}+r_n & 0<r_n<r_{n-1},\\ r_{n-1} & = & r_nq_n. & \end{array} \tag{5.1}$$

The sequence of remainders will eventually reach a r_{n+1} which will be zero, since $b,r_2,r_3,\ldots$ is a monotonically decreasing sequence of integers, and cannot contain more than b positive terms.

The Euclidean Algorithm rests on the fact, to be proved below, that $(a,b)=(b,r_2)=(r_2,r_3)=\cdots=(r_{n-1},r_n)=r_n$.

328 Theorem Prove that if a,b,n are positive integers, then

$$(a,b)=(a+nb,b).$$

Proof: *Set $d=(a,b), c=(a+nb,b)$. As $d|a, d|b$, it follows that $d|(a+nb)$. Thus d is a common divisor of both $(a+nb)$ and b. This implies that $d|c$. On the other hand, $c|(a+nb), c|b$ imply that $c|((a+nb)-nb)=a$. Thus c is a common divisor of a and b, implying that $c|d$. This completes the proof.* ❑

329 Example Use Theorem 328 to find $(3456,246)$.

Solution: $(3456,246)=(13\cdot 246+158,246)=(158,246)$, by the preceding example. Now, $(158,246)=(158,158+88)=(88,158)$. Finally, $(88,158)=(70,88)=(18,70)=(16,18)=(2,16)=2$. Hence $(3456,246)=2$.

330 Theorem If r_n is the last non-zero remainder found in the process of the Euclidean Algorithm, then

$$r_n=(a,b).$$

Proof: *From equations 5.1*

$$\begin{array}{rcl} r_2 & = & a-bq_1 \\ r_3 & = & b-r_2q_2 \\ r_4 & = & r_2-r_3q_3 \\ \vdots & \vdots & \vdots \\ r_n & = & r_{n-2}-r_{n-1}q_{n-1} \end{array}$$

Let $r=(a,b)$. From the first equation, $r|r_2$. From the second equation, $r|r_3$. Upon iterating the process, we see that $r|r_n$.

But starting at the last equation 5.1 and working up, we see that $r_n|r_{n-1}, r_n|r_{n-2}, \ldots r_n|r_2, r_n|b, r_n|a$. Thus r_n is a common divisor of a and b and so $r_n|(a,b)$. This gives the desired result. ❑

331 Example Find $(23,29)$ by means of the Euclidean Algorithm.

Solution: We have

$$29 = 1\cdot 23+6,$$

$$23 = 3\cdot 6+5,$$

$$6 = 1\cdot 5+1,$$

$$5 = 5\cdot 1.$$

The last non-zero remainder is 1, thus $(23,29)=1$.

An equation which requires integer solutions is called a *diophantine equation*. By the Bachet-Bezout Theorem, we see that the linear diophantine equation

$$ax+by=c$$

has a solution in integers if and only if $(a,b)|c$. The Euclidean Algorithm is an efficient means to find a solution to this equation.

332 Example Find integers x,y that satisfy the linear diophantine equation

$$23x+29y=1.$$

Solution: We work upwards, starting from the penultimate equality in the preceding problem:

$$1 = 6-1\cdot 5,$$

$$5 = 23-3\cdot 6,$$

$$6 = 29\cdot 1-23.$$

Hence,

$$\begin{array}{rcl} 1 & = & 6-1\cdot 5 \\ & = & 6-1\cdot(23-3\cdot 6) \\ & = & 4\cdot 6-1\cdot 23 \\ & = & 4(29\cdot 1-23)-1\cdot 23 \\ & = & 4\cdot 29-5\cdot 23. \end{array}$$

This solves the equation, with $x=-5, y=4$.

333 Example Find integer solutions to

$$23x+29y=7.$$

Solution: From the preceding example, $23(-5)+29(4)=1$. Multiplying both sides of this equality by 7,

$$23(-35)+29(28)=7,$$

which solves the problem.

334 Example Find infinitely many integer solutions to

$$23x+29y=1.$$

Solution: By Example 332, the pair $x_0=-5, y_0=4$ is a solution. We can find a family of solutions by letting

$$x=-5+29t,\ y=4-23t,\ \ t\in\mathbb{Z}.$$

335 Example Can you find integers x, y such that $3456x+246y=73$?

Solution: No. $(3456,246)=2$ and $2\not|73$.

336 Theorem Assume that a, b, c are integers such that $(a,b)|c$. Then given any solution (x_0,y_0) of the linear diophantine equation

$$ax+by=c$$

any other solution of this equation will have the form

$$x=x_0+t\frac{b}{d},\ y=y_0-t\frac{a}{d},$$

where $d=(a,b)$ and $t\in\mathbb{Z}$.

Proof: *It is clear that if (x_0,y_0) is a solution of $ax+by=c$, then $x=x_0+tb/d, y=y_0-ta/d$ is also a solution. Let us prove that any solution will have this form.*

Let (x',y') satisfy $ax'+by'=c$. As $ax_0+by_0=c$ also, we have

$$a(x'-x_0)=b(y_0-y').$$

Dividing by $d=(a,b)$,

$$\frac{a}{d}(x'-x_0)=\frac{b}{d}(y_0-y').$$

Since $(a/d,b/d)=1$, $\frac{a}{d}|(y_0-y')$, in virtue of Euclid's Lemma. Thus there is an integer t such that $t\frac{a}{d}=y_0-y'$, that is, $y=y_0-ta/d$. From this

$$\frac{a}{d}(x'-x_0)=\frac{b}{d}t\frac{a}{d},$$

which is to say $x'=x_0+tb/d$. This finishes the proof. ❑

337 Example Find all solutions in integers to

$$3456x+246y=234.$$

Solution: By inspection, $3456(-1)+246(15)=234$. By Theorem 336, all the solutions are given by $x=-1+123t, y=15-1728t, t\in\mathbb{Z}$.

Practice

338 Problem Find the following:

1. $(34567,987)$
2. $(560,600)$
3. $(4554,36)$
4. $(8098643070,8173826342)$

339 Problem Solve the following linear diophantine equations, provided solutions exist:

1. $24x+25y=18$

2. $3456x+246y=44$

3. $1998x+2000y=33$

340 Problem Prove that the area of the triangle whose vertices are $(0,0),(b,a),(x,y)$ is

$$\frac{|by-ax|}{2}.$$

341 Problem A woman pays \$2.78 for some bananas and eggs. If each banana costs \$0.69 and each egg costs \$0.35, how many eggs and how many bananas did the woman buy?

5.2 Linear Congruences

We recall that the expression $ax \equiv b \mod n$ means that there is $t \in \mathbb{Z}$ such that $ax = b+nt$. Hence, the congruencial equation in x, $ax \equiv b \mod n$ is soluble if and only if the linear diophantine equation $ax+ny=b$ is soluble. It is clear then that the congruence

$$ax \equiv b \mod n$$

has a solution if and only if $(a,n)|b$.

342 Theorem Let a, b, n be integers. If the congruence $ax \equiv b \mod n$ has a solution, then it has (a,n) incongruent solutions mod n.

Proof: *From Theorem 336 we know that the solutions of the linear diophantine equation $ax+ny=b$ have the form $x = x_0+nt/d, y = y_0-at/d, d = (a,n), t \in \mathbb{Z}$, where x_0, y_0 satisfy $ax_0+ny=b$. Letting t take on the values $t = 0,1,\ldots((a,n)-1)$, we obtain (a,n) mutually incongruent solutions, since the absolute difference between any two of them is less than n. If $x = x_0+nt'/d$ is any other solution, we write t' as $t' = qd+r, 0 \leq r < d$. Then*

$$\begin{aligned} x &= x_0+n(qd+r)/d \\ &= x_0+nq+nr/d \\ &\equiv x_0+nr/d \mod n. \end{aligned}$$

Thus every solution of the congruence $ax \equiv b \mod n$ is congruent $\mod n$ to one and only one of the d values $x_0+nt/d, 0 \leq t \leq d-1$. Thus if there is a solution to the congruence, then there are d incongruent solutions mod n.❑

343 Example Find all solutions to the congruence $5x \equiv 3 \mod 7$

Solution: Notice that according to Theorem 342, there should only be one solution $\mod 7$, as $(5,7)=1$. We first solve the linear diophantine equation $5x+7y=1$. By the Euclidean Algorithm

$$\begin{aligned} 7 &= 5\cdot 1+2 \\ 5 &= 2\cdot 2+1 \\ 2 &= 2\cdot 1. \end{aligned}$$

Hence,

$$\begin{aligned} 1 &= 5-2\cdot 2 \\ 2 &= 7-5\cdot 1, \end{aligned}$$

which gives

$$1 = 5-2\cdot 2 = 5-2(7-5\cdot 1) = 5\cdot 3-7\cdot 2.$$

Whence $3 = 5(9)-7(6)$. This gives $5\cdot 9 \equiv 3 \mod 7$ which is the same as $5\cdot 2 \equiv 3 \mod 7$. Thus $x \equiv 2 \mod 7$.

344 Example Solve the congruence

$$3x \equiv 6 \mod 12.$$

Solution: As $(3,12)=3$ and $3|6$, the congruence has three mutually incongruent solutions. By inspection we see that $x=2$ is a solution. By Theorem 336, all the solutions are thus of the form $x=2+4t, t\in\mathbb{Z}$. By letting $t=0,1,2$, the three incongruent solutions modulo 12 are $t=2,6,10$.

We now add a few theorems and definitions that will be of use in the future.

345 Theorem Let x, y be integers and let a, n be non-zero integers. Then

$$ax\equiv ay \mod n$$

if and only if

$$x\equiv y \mod \frac{n}{(a,n)}.$$

Proof: *If $ax\equiv ay \mod n$ then $a(x-y)=sn$ for some integer s. This yields*

$$(x-y)\frac{a}{(a,n)}=s\frac{n}{(a,n)}.$$

Since $(a/(a,n),n/(a,n))=1$ by Theorem 240, we must have

$$\frac{n}{(a,n)}|(x-y),$$

by Euclid's Lemma (Lemma 239). This implies that

$$x\equiv y \mod \frac{n}{(a,n)}.$$

Conversely if $x\equiv y \mod \dfrac{n}{(a,n)}$ implies

$$ax\equiv ay \mod \frac{an}{(a,n)},$$

upon multiplying by a. As (a,n) divides a, the above congruence implies a fortiori that $ax-ay=tn$ for some integer t. This gives the required result.❑

Theorem 345 gives immediately the following corollary.

346 Corollary If $ax\equiv ay \mod n$ and $(a,n)=1$, then $x\equiv y \mod n$.

Practice

347 Problem Solve the congruence $50x\equiv 12 \mod 14$.

348 Problem How many x, $38\leq x\leq 289$ satisfy

$$3x\equiv 8 \mod 11?$$

5.3 A theorem of Frobenius

If $(a,b)=d>1$ then the linear form $ax+by$ skips all non-multiples of d. If $(a,b)=1$, there is always an integer solution to $ax+by=n$ regardless of the integer n. We will prove the following theorem of Frobenius that tells un when we will find nonnegative solutions to $ax+by=n$.

349 Theorem (Frobenius) Let a,b be positive integers. If $(a,b)=1$ then the number of positive integers m that cannot be written in the form $ar+bs=m$ for nonnegative integers r, s equals $(a-1)(b-1)/2$.

Proof: *Let us say that an integer n is* attainable *if there are nonnegative integers r,s with $ar+bs=n$. Consider the infinite array*

$$\begin{array}{ccccccc} 0 & 1 & 2 & \ldots & k & \ldots & a-1 \\ a & a+1 & a+2 & \ldots & a+k & \ldots & 2a-1 \\ 2a & 2a+1 & 2a+2 & \ldots & 2a+k & \ldots & 3a-1 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \end{array}$$

The columns of this array are arithmetic progressions with common difference a. The numbers directly below a number n have the form $n+ka$ where k is a natural number. Clearly, if n is attainable, so is $n+ka$, implying thus that if an integer n is attainable so is every integer directly below it. Clearly all multiples of b are attainable. We claim that no two distinct multiples of b, vb and wb with $0 \leq v,w \leq a-1$ can belong to the same column. If this were so then we would have $vb \equiv wb \mod a$. Hence $a(v-w) \equiv 0 \mod a$. Since $(a,b)=1$ we invoke Corollary 5.1 to deduce $v-w \equiv 0 \mod a$. Since $0 \leq v,w \leq a-1$, we must have $v=w$.

Now we show that any number directly above one of the multiples $vb, 0 \leq v \leq a-1$ is non-attainable. For a number directly above vb is of the form $vb-ka$ for some natural number k. If $vb-ka$ were attainable, then $ax+by=vb-ka$ for some nonnegative integers x,y. This yields $by \leq ax+by = vb-ka < vb$. Hence, $0 \leq y < v < a$. This implies that $y \not\equiv v \mod b$. On the other hand, two numbers on the same column are congruent $\mod a$. Therefore we deduce $vb \equiv bv-ka \equiv ax+by \mod a$ which yields $bv \equiv by \mod a$. By Corollary 346 we obtain $v \equiv y \mod a$. This contradicts the fact that $0 \leq y < v < a$.

Thus the number of unattainable numbers is precisely the numbers that occur just above a number of the form $vb, 0 \leq v \leq a-1$. Now, on the j-th column, there are $(vb-j)/a$ values above vb. Hence the number of unattainable numbers is given by

$$\sum_{v=0}^{a-1}\sum_{j=0}^{a-1} \frac{vb-j}{a} = \frac{(a-1)(b-1)}{2},$$

as we wanted to show.❑

The greatest unattainable integer occurs just above $(a-1)b$, hence the greatest value that is not attainable is $(a-1)b-a$, which gives the following theorem.

350 Theorem Let a,b be relatively prime positive integers. Then the equation

$$ax+by=n$$

is unsoluble in nonnegative integers x,y for $n=ab-a-b$. If $n>ab-a-b$, then the equation is soluble in nonnegative integers.

351 Example (Putnam, 1971) A game of solitaire is played as follows. After each play, according to the outcome, the player receives either a or b points, ($a,b \in \mathbb{N}, a > b$), and his score accumulates from play to play. It has been noticed that there are thirty five non-attainable scores and that one of these is 58. Find a and b.

Solution: The attainable scores are the nonnegative integers of the form $ax+by$. If $(a,b)>1$, there are infinitely many such integers. Hence $(a,b)=1$. By Theorem 349, the number of non-attainable scores is $(a-1)(b-1)/2$. Therefore, $(a-1)(b-1)=70=2(35)=5(14)=7(10)$. The conditions $a>b, (a,b)=1$ yield the two possibilities $a=71, b=2$ and $a=11, b=8$. As $58=0\cdot 71+2\cdot 29$, the first alternative is dismissed. The line $11x+8y=58$ passes through $(6,-1)$ and $(-2,10)$ and thus it does not pass through a lattice point in the first quadrant. The unique solution is $a=11, b=8$.

352 Example (AIME, 1994) Ninety-four bricks, each measuring $4'' \times 10'' \times 19''$, are to be stacked one on top of another to form a tower 94 bricks tall. Each brick can be oriented so it contributes $4''$ or $10''$ or $19''$ to the total height of the tower. How many different tower heights can be achieved using all 94 of the bricks?

Solution: Let there be x,y,z bricks of height $4'', 10''$, and $19''$ respectively. We are asking for the number of different sums

$$4x+10y+19z$$

with the constraints $x \geq 0, y \geq 0, z \geq 0, x+y+z=94$.

Now, $4x+10y+19z \leq 19 \cdot 94 = 1786$. Letting $x = 94-y-z$, we count the number of different nonnegative integral solutions to the inequality $376+3(2y+5z) \leq 1786, y+z \leq 94$, that is $2y+5z \leq 470, y+z \leq 94$. By Theorem 350, every integer $\geq (2-1)(5-1) = 4$ can be written in the form $2y+5z$, and the number of exceptions is $(2-1)(5-1)/2 = 2$, namely $n=1$ and $n=3$. Thus of the 471 nonnegative integers $n \leq 470$, we see that 469 can be written in the form $n = 2y+5z$. Using $x = 96-x-y$, $n, 4 \leq n \leq 470$ will be "good" only if we have $470-n = 3x+5z$. By Theorem 349 there are $(3-1)(5-1)/2 = 4$ exceptions, each ≤ 8, namely $n = 1,2,4,7$. This means that 463, 466, 468, and 469 are not representable in the form $4x+10y+19z$. Then every integer $n, 0 \leq n \leq 470$ except for 1, 3, 463, 466, 468, and 469 can be thus represented, and the number of different sums is $471-6 = 465$.

353 Example

1. Let $(n,1991) = 1$. Prove that $\dfrac{n}{1991}$ is the sum of two positive integers with denominator < 1991 if an only if there exist integers m,a,b with

$$(*) \quad 1 \leq m \leq 10,\ a \geq 1,\ b \geq 1,\ mn = 11a+181b.$$

2. Find the largest positive rational with denominator 1991 that cannot be written as the sum of two positive rationals each with denominators less than 1991.

Solution: (a) If $(*)$ holds then $\dfrac{n}{1991} = \dfrac{a}{181m} + \dfrac{b}{11m}$ does the trick. Conversely, if $\dfrac{n}{1991} = \dfrac{a}{r} + \dfrac{b}{s}$ for $a,b \geq 1, (a,r) = (b,s) = 1$, and $r,s < 1991$, we may suppose $r = 181r_1, s = 11s_1$ and then $nr_1s_1 = 11as_1 + 181br_1$, which leads to $r_1|11as_1$ and so $r_1|s_1$. Similarly, $s_1|r_1$, whence $r_1 = s_1 = m$, say, and $(*)$ follows.
(b) Any $n > 170, (n,1991) = 1$ satisfies $(*)$ with $b=1$ and $\mathscr{M}$ such that mn is of the form $mn \equiv 181 \mod 11$. For $mn > 181$ except if $m = 1, n \leq 180$; but then n would not be of the form $n \equiv 181 \mod 11$.

But $n = 170$ does not satisfy $(*)$; for we would have $170 \equiv 181b \mod 11$, so $b \equiv m \mod 11$, which yields $b \geq m$, but $170m < 181$. The answer is thus $170/1991$.

Practice

354 Problem Let a,b,c be positive real numbers. Prove that there are at least $c^2/2ab$ pairs of integers (x,y) satisfying

$$x \geq 0, y \geq 0,\ ax+by \leq c.$$

355 Problem (AIME, 1995) What is largest positive integer that is not the sum of a positive integral multiple of 42 and a positive composite integer?

356 Problem Let $a > 0, b > 0, (a,b) = 1$. Then the number of nonnegative solutions to the equation $ax+by = n$ is equal to

$$[\frac{n}{ab}] \text{ or } [\frac{n}{ab}]+1.$$

(Hint: $[s]-[t] = [s-t]$ or $[s-t]+1$.)

357 Problem Let $a,b \in \mathbb{N}, (a,b) = 1$. Let $S(n)$ denote the number of nonnegative solutions to

$$ax+by = n.$$

Evaluate

$$\lim_{n\to\infty} \frac{S(n)}{n}.$$

358 Problem (IMO, 1983) Let a,b,c be pairwise relatively prime integers. Demonstrate that $2abc-ab-bc-ca$ is the largest integer not of the form

$$bcx+acy+abz, \qquad x \geq 0, y \geq 0, z \geq 0.$$

5.4 Chinese Remainder Theorem

In this section we consider the case when we have multiple congruences. Consider the following problem: find an integer x which leaves remainder 2 when divided by 5, is divisible by 7, and leaves remainder 4 when divided by 11. In the language of congruences we are seeking x such that

$$\begin{array}{rcll} x & \equiv & 2 & \mod 5, \\ x & \equiv & 0 & \mod 7, \\ x & \equiv & 4 & \mod 11. \end{array}$$

One may check that $x = 147$ satisfies the requirements, and that in fact, so does the parametric family $x = 147 + 385t, t \in \mathbb{Z}$.

We will develop a method to solve congruences like this one. The method is credited to the ancient Chinese, and it is thus called the *Chinese Remainder Theorem.*

359 Example Find x such that

$$x \equiv 3 \mod 5 \text{ and } x \equiv 7 \mod 11.$$

Solution: Since $x = 3 + 5a$, we have $11x = 33 + 55a$. As $x = 7 + 11b$, we have $5x = 35 + 55b$. Thus $x = 11x - 10x = 33 - 70 + 55a - 110b$. This means that $x \equiv -37 \equiv 18 \mod 55$. One verifies that all the numbers $x = 18 + 55t, t \in \mathbb{Z}$ verify the given congruences.

360 Example Find a number n such that when divided by 4 leaves remainder 2, when divided by 5 leaves remainder 1, and when divided by 7 leaves remainder 1.

Solution: We want n such that

$$\begin{array}{rcl} n \equiv & 2 & \mod 4, \\ n \equiv & 1 & \mod 5, \\ n \equiv & 1 & \mod 7. \end{array}$$

This implies that

$$\begin{array}{rcl} 35n \equiv & 70 & \mod 140, \\ 28n \equiv & 28 & \mod 140, \\ 20n \equiv & 20 & \mod 140. \end{array}$$

As $n = 21n - 20n$, we have $n \equiv 3(35n - 28n) - 20n \equiv 3(70 - 28) - 20 \equiv 106 \mod 140$. Thus all $n \equiv 106 \mod 140$ will do.

361 Theorem (Chinese Remainder Theorem) Let $m_1, m_2, \ldots m_k$ be pairwise relatively prime positive integers, each exceeding 1, and let $a_1, a_2, \ldots a_k$ be arbitrary integers. Then the system of congruences

$$\begin{array}{rcll} x & \equiv & a_1 & \mod m_1 \\ x & \equiv & a_2 & \mod m_2 \\ \vdots & \vdots & \vdots & \\ x & \equiv & a_k & \mod m_k \end{array}$$

has a unique solution modulo $m_1 m_2 \cdots m_k$.

Proof: *Set $P_j = m_1 m_2 \cdots m_k / m_j, 1 \leq j \leq k$. Let Q_j be the inverse of $P_j \mod m_j$, i.e., $P_j Q_j \equiv 1 \mod m_j$, which we know exists since all the m_i are pairwise relatively prime. Form the number*

$$x = a_1 P_1 Q_1 + a_2 P_2 Q_2 + \cdots + a_k P_k Q_k.$$

This number clearly satisfies the conditions of the theorem. The uniqueness of the solution modulo $m_1 m_2 \cdots m_k$ can be easily established. ❑

362 Example Can one find one million consecutive integers that are not square-free?

Solution: Yes. Let $p_1, p_2, \ldots, p_{1000000}$ be a million different primes. By the Chinese Remainder Theorem, there exists a solution to the following system of congruences.

$$\begin{array}{ccccc} x & \equiv & -1 & \mod & p_1^2, \\ x & \equiv & -2 & \mod & p_2^2, \\ \vdots & \vdots & \vdots & \vdots & \\ x & \equiv & -1000000 & \mod & p_{1000000}^2. \end{array}$$

The numbers $x+1, x+2, \ldots, x+1000000$ are a million consecutive integers, each of which is divisible by the square of a prime.

Practice

363 Problem Solve the following systems:

1. $x \equiv -1 \mod 4$; $x \equiv 2 \mod 5$
2. $4x \equiv 3 \mod 7$; $x \equiv 10 \mod 11$
3. $5x \equiv 2 \mod 8$; $3x \equiv 2 \mod 9$; $x \equiv 0 \mod 11$

364 Problem (USAMO 1986)

1. Do there exist fourteen consecutive positive integers each of which is divisible by one or more primes $p, 2 \leq p \leq 11$?
2. Do there exist twenty-one consecutive integers each of which is divisible by one or more primes $p, 2 \leq p \leq 13$?

Chapter 6

Number-Theoretic Functions

6.1 Greatest Integer Function

The largest integer not exceeding x is denoted by $\lfloor x \rfloor$ or $\lfloor x \rfloor$. We also call this function the *floor* function. Thus $\lfloor x \rfloor$ satisfies the inequalities $x-1 < \lfloor x \rfloor \leq x$, which, of course, can also be written as $\lfloor x \rfloor \leq x < \lfloor x \rfloor + 1$. The fact that $\lfloor x \rfloor$ is the *unique* integer satisfying these inequalities, is often of use. We also utilise the notation $\{x\} = x - \lfloor x \rfloor$, to denote the fractional part of x, and $||x|| = \min_{n \in \mathbb{Z}} |x-n|$ to denote the distance of a real number to its nearest integer. A useful fact is that we can write any real number x in the form $x = \lfloor x \rfloor + \{x\}, 0 \leq \{x\} < 1$.

The greatest integer function enjoys the following properties:

365 Theorem Let $\alpha, \beta \in \mathbb{R}, a \in \mathbb{Z}, n \in \mathbb{N}$. Then

1. $\lfloor \alpha + a \rfloor = \lfloor \alpha \rfloor + a$
2. $\lfloor \frac{\alpha}{n} \rfloor = \lfloor \frac{\lfloor \alpha \rfloor}{n} \rfloor$
3. $\lfloor \alpha \rfloor + \lfloor \beta \rfloor \leq \lfloor \alpha + \beta \rfloor \leq \lfloor \alpha \rfloor + \lfloor \beta \rfloor + 1$

Proof:

1. *Let $m = \lfloor \alpha + a \rfloor$. Then $m \leq \alpha + a < m + 1$. Hence $m - a \leq \alpha < m - a + 1$. This means that $m - a = \lfloor \alpha \rfloor$, which is what we wanted.*
2. *Write α/n as $\alpha/n = \lfloor \alpha/n \rfloor + \theta, 0 \leq \theta < 1$. Since $n\lfloor \alpha/n \rfloor$ is an integer, we deduce by (1) that*

   $$\lfloor \alpha \rfloor = \lfloor n\lfloor \alpha/n \rfloor + n\theta \rfloor = n\lfloor \alpha/n \rfloor + \lfloor n\theta \rfloor.$$

   Now, $0 \leq \lfloor n\theta \rfloor \leq n\theta < n$, and so $0 \leq \lfloor n\theta \rfloor / n < 1$. If we let $\Theta = \lfloor n\theta \rfloor / n$, we obtain

   $$\frac{\lfloor \alpha \rfloor}{n} = \lfloor \frac{\alpha}{n} \rfloor + \Theta, \quad 0 \leq \Theta < 1.$$

   This yields the required result.
3. *From the inequalities $\alpha - 1 < \lfloor \alpha \rfloor \leq \alpha, \beta - 1 < \lfloor \beta \rfloor \leq \beta$ we get $\alpha + \beta - 2 < \lfloor \alpha \rfloor + \lfloor \beta \rfloor \leq \alpha + \beta$. Since $\lfloor \alpha \rfloor + \lfloor \beta \rfloor$ is an integer less than or equal to $\alpha + \beta$, it must be less than or equal to the integral part of $\alpha + \beta$, i.e. $\lfloor \alpha + \beta \rfloor$. We obtain thus $\lfloor \alpha \rfloor + \lfloor \beta \rfloor \leq \lfloor \alpha + \beta \rfloor$. Also, $\alpha + \beta$ is less than the integer $\lfloor \alpha \rfloor + \lfloor \beta \rfloor + 2$, so its integer part $\lfloor \alpha + \beta \rfloor$ must be less than $\lfloor \alpha \rfloor + \lfloor \beta \rfloor + 2$, but $\lfloor \alpha + \beta \rfloor < \lfloor \alpha \rfloor + \lfloor \beta \rfloor + 2$ yields $\lfloor \alpha + \beta \rfloor \leq \lfloor \alpha \rfloor + \lfloor \beta \rfloor + 1$. This proves the inequalities.*

❑

366 Example Find a non-zero polynomial $P(x,y)$ such that

$$P(\lfloor\lfloor 2t\rfloor\rfloor, \lfloor\lfloor 3t\rfloor\rfloor) = 0$$

for all real t.

Solution: We claim that $3[2t] - 2[3t] = 0, \pm 1$ or -2. We can then take

$$P(x,y) = (3x-2y)(3x-2y-1)(3x-2y+1)(3x-2y+2).$$

In order to prove the claim, we observe that $\lfloor\lfloor x\rfloor\rfloor$ has unit period, so it is enough to prove the claim for $t \in [0,1)$. We divide $[0,1)$ as

$$[0,1) = [0,1/3) \cup [1/3,1/2) \cup [1/2,2/3) \cup [2/3,1).$$

If $t \in [0,1/3)$, then both $\lfloor\lfloor 2t\rfloor\rfloor$ and $\lfloor\lfloor 3t\rfloor\rfloor$ are $= 0$, and so $3\lfloor\lfloor 2t\rfloor\rfloor - 2\lfloor\lfloor 3t\rfloor\rfloor = 0$. If $t \in [1/3,1/2)$ then $[3t] = 1$ and $[2t] = 0$, and so $3\lfloor\lfloor 2t\rfloor\rfloor - 2\lfloor\lfloor 3t\rfloor\rfloor = -2$. If $t \in [1/2,2/3)$, then $[2t] = 1, [3t] = 1$, and so $3\lfloor\lfloor 2t\rfloor\rfloor - 2\lfloor\lfloor 3t\rfloor\rfloor = 1$. If $t \in [2/3,1)$, then $\lfloor\lfloor 2t\rfloor\rfloor = 1, \lfloor\lfloor 3t\rfloor\rfloor = 2$, and $3\lfloor\lfloor 2t\rfloor\rfloor - 2\lfloor\lfloor 3t\rfloor\rfloor = -1$.

367 Example Describe all integers n such that $1 + \lfloor\lfloor\sqrt{2n}\rfloor\rfloor \Big| 2n$.

Solution: Let $2n = m(1 + \lfloor\lfloor\sqrt{2n}\rfloor\rfloor)$. If $m \leq \lfloor\lfloor\sqrt{2n}\rfloor\rfloor - 1$ then $2n \leq (\lfloor\lfloor\sqrt{2n}\rfloor\rfloor - 1)(\lfloor\lfloor\sqrt{2n}\rfloor\rfloor + 1) = \lfloor\lfloor\sqrt{2n}\rfloor\rfloor^2 - 1 \leq 2n - 1 < 2n$, a contradiction. If $m \geq \lfloor\lfloor\sqrt{2n}\rfloor\rfloor + 1$, then $2n \geq (\lfloor\lfloor\sqrt{2n}\rfloor\rfloor^2 + 1)^2 \geq 2n + 1$, another contradiction. It must be the case that $m = \lfloor\lfloor\sqrt{2n}\rfloor\rfloor$.

Conversely, let $n = \dfrac{l(l+1)}{2}$. Since $l < \sqrt{2n} < l+1, l = \lfloor\lfloor\sqrt{2n}\rfloor\rfloor$. So all the integers with the required property are the triangular numbers.

368 Example Prove that the integers

$$\lfloor\lfloor \left(1+\sqrt{2}\right)^n \rfloor\rfloor$$

with n a nonnegative integer, are alternately even or odd.

Solution: By the Binomial Theorem

$$(1+\sqrt{2})^n + (1-\sqrt{2})^n = 2\sum_{0 \leq k \leq n/2} (2)^k \binom{n}{2k} := 2N,$$

an even integer. Since $-1 < 1 - \sqrt{2} < 0$, it must be the case that $(1-\sqrt{2})^n$ is the fractional part of $(1+\sqrt{2})^n$ or $(1+\sqrt{2})^n + 1$ depending on whether n is odd or even, respectively. Thus for odd n, $(1+\sqrt{2})^n - 1 < (1+\sqrt{2})^n + (1-\sqrt{2})^n < (1+\sqrt{2})^n$, whence $(1+\sqrt{2})^n + (1-\sqrt{2})^n = \lfloor\lfloor(1+\sqrt{2})^n\rfloor\rfloor$, always even, and for n even $2N := (1+\sqrt{2})^n + (1-\sqrt{2})^n = \lfloor\lfloor(1+\sqrt{2})^n\rfloor\rfloor + 1$, and so $\lfloor\lfloor(1+\sqrt{2})^n\rfloor\rfloor = 2N - 1$, always odd for even n.

369 Example Prove that the first thousand digits after the decimal point in

$$(6+\sqrt{35})^{1980}$$

are all 9's.

Solution: Reasoning as in the preceding problem,

$$(6+\sqrt{35})^{1980} + (6-\sqrt{35})^{1980} = 2k,$$

an even integer. But $0<6-\sqrt{35}<1/10$, (for if $\frac{1}{10}<6-\sqrt{35}$, upon squaring $3500<3481$, which is clearly nonsense), and hence $0<(6-\sqrt{35})^{1980}<10^{-1980}$ which yields

$$2k-1+\underbrace{0.9\ldots9}_{\text{1979 nines}}=2k-\frac{1}{10^{1980}}<(6+\sqrt{35})^{1980}<2k,$$

This proves the assertion of the problem.

370 Example (Putnam 1948) If n is a positive integer, demonstrate that

$$\lfloor\sqrt{n}+\sqrt{n+1}\rfloor=\lfloor\sqrt{4n+2}\rfloor.$$

Solution: By squaring, it is easy to see that

$$\sqrt{4n+1}<\sqrt{n}+\sqrt{n+1}<\sqrt{4n+3}.$$

Neither $4n+2$ nor $4n+3$ are squares since squares are either congruent to 0 or 1 mod 4, so

$$\lfloor\sqrt{4n+2}\rfloor=\lfloor\sqrt{4n+3}\rfloor,$$

and the result follows.

371 Example Find a formula for the n-th non-square.

Solution: Let T_n be the n-th non-square. There is a natural number m such that $m^2<T_n<(m+1)^2$. As there are m squares less than T_n and n non-squares up to T_n, we see that $T_n=n+m$. We have then $m^2<n+m<(m+1)^2$ or $m^2-m<n<m^2+m+1$. Since n,m^2-m,m^2+m+1 are all integers, these inequalities imply $m^2-m+\frac{1}{4}<n<m^2+m+\frac{1}{4}$, that is to say, $(m-1/2)^2<n<(m+1/2)^2$. But then $m=\lfloor\sqrt{n}+\frac{1}{2}\rfloor$. Thus the n-th non-square is $T_n=n+\lfloor\sqrt{n}+1/2\rfloor$.

372 Example (Putnam 1983) Let $f(n)=n+\lfloor\sqrt{n}\rfloor$. Prove that for every positive integer m, the sequence

$$m,f(m),f(f(m)),f(f(f(m))),\ldots$$

contains at least one square of an integer.

Solution: Let $m=k^2+j, 0\leq j\leq 2k$. Split the m's into two sets, the set A of all the m with excess $j, 0\leq j\leq k$ and the set B with all those m's with excess $j, k<j<2k+1$.

Observe that $k^2\leq m<(k+1)^2=k^2+2k+1$. If $j=0$, we have nothing to prove. Assume that $m\in B$. As $\lfloor\sqrt{m}\rfloor=k$, $f(m)=k^2+j+k=(k+1)^2+j-k-1$, with $0\leq j-k-1\leq k-1<k+1$. This means that either $f(m)$ is a square or $f(m)\in A$. It is thus enough to consider the alternative $m\in A$, in which case $\lfloor\sqrt{m+k}\rfloor=k$ and

$$f(f(m))=f(m+k)=m+2k=(k+1)^2+j-1.$$

This means that $f(f(m))$ is either a square or $f(f(m))\in A$ with an excess $j-1$ smaller than the excess j of m. At each iteration the excess will reduce and eventually it will hit 0, whence we reach a square.

373 Example Solve the equation

$$\lfloor x^2-x-2\rfloor=\lfloor x\rfloor,$$

for $x\in\mathbb{R}$.

Solution: Observe that $\lfloor a\rfloor=\lfloor b\rfloor$ if and only if $\exists k\in\mathbb{Z}$ with $a,b\in[k,k+1)$ which happens if and only if $|a-b|<1$. Hence, the given equation has a solution if and only if $|x^2-2x-2|<1$. Solving these inequalities it is easy to see that the solution is thus

$$x\in(-1,\frac{1}{2}(1-\sqrt{5})]\cup[\frac{1}{2}(1+\sqrt{17}),\frac{1}{2}(1+\sqrt{21})).$$

374 Theorem If a,b are relatively prime natural numbers then

$$\sum_{k=1}^{a-1} \llbracket \frac{kb}{a} \rrbracket = \sum_{k=1}^{b-1} \llbracket \frac{ka}{b} \rrbracket = \frac{(a-1)(b-1)}{2}.$$

Proof: *Consider the rectangle with vertices at $(0,0),(0,b),(a,0),(a,b)$. This rectangle contains $(a-1)(b-1)$ lattice points, i.e., points with integer coordinates. This rectangle is split into two halves by the line $y = \frac{xb}{a}$. We claim that there are no lattice points on this line, except for the endpoints. For if there were a lattice point $(m,n), 0 < m < a, 0 < n < b$, then $\frac{n}{m} = \frac{b}{a}$. Thus n/m is a reduction for the irreducible fraction b/a, a contradiction. The points $L_k = (k, \frac{kb}{a}), 1 \leq k \leq a-1$ are each on this line. Now, $\llbracket \frac{kb}{a} \rrbracket$ equals the number of lattice points on the vertical line that goes from $(k,0)$ to $(k, \frac{kb}{a})$, i.e. $\sum_{k=1}^{a-1} \llbracket \frac{kb}{a} \rrbracket$ is the number of lattice points on the lower half of the rectangle. Similarly, $\sum_{k=1}^{b-1} \llbracket \frac{ka}{b} \rrbracket$ equals the number of lattice points on the upper half of the rectangle. Since there are $(a-1)(b-1)$ lattice points in total, and their number is shared equally by the halves, the assertion follows.* ❑

375 Example Find the integral part of

$$\sum_{k=1}^{10^6} \frac{1}{\sqrt{k}}.$$

Solution: The function $x \mapsto x^{-1/2}$ is decreasing. Thus for positive integer k,

$$\frac{1}{\sqrt{k+1}} < \int_k^{k+1} \frac{dx}{\sqrt{x}} < \frac{1}{\sqrt{k}}.$$

Summing from $k = 1$ to $k = 10^6 - 1$ we deduce

$$\sum_{k=2}^{10^6} \frac{1}{\sqrt{k}} < \int_1^{10^6} \frac{dx}{\sqrt{x}} < \sum_{k=1}^{10^6-1} \frac{1}{\sqrt{k}}.$$

The integral is easily seen to be 1998. Hence

$$1998 + 1/10^3 < \sum_{k=1}^{10^6} \frac{1}{\sqrt{k}} < 1999.$$

The integral part sought is thus 1998.

Practice

376 Problem Prove that for all real numbers x,y,

$$\llbracket x \rrbracket + \llbracket x+y \rrbracket + \llbracket y \rrbracket \leq \llbracket 2x \rrbracket + \llbracket 2y \rrbracket$$

holds.

377 Problem If x, y real numbers, when is it true that $\llbracket x \rrbracket \llbracket y \rrbracket \leq \llbracket xy \rrbracket$?

378 Problem If $n > 1$ is a natural number and $\alpha \geq 1$ is a real number, prove that

$$[\alpha] > \llbracket \frac{\alpha}{n} \rrbracket.$$

379 Problem If a, b, n are positive integers, prove that

$$\llbracket \frac{ab}{n} \rrbracket \geq a \llbracket \frac{b}{n} \rrbracket.$$

380 Problem Let α be a real number. Prove that $[\alpha]+[-\alpha]=-1$ or 0 and that $\lfloor\alpha\rfloor-2\lfloor\alpha/2\rfloor=0$ or 1.

381 Problem Prove that

$$\lfloor(2+\sqrt{3})^n\rfloor$$

is an odd integer.

382 Problem Show that the n-th element of the sequence

$$1,2,2,3,3,3,4,4,4,4,5,5,5,5,5,\ldots$$

where there are n occurrences of the integer n is $\lfloor\sqrt{2n}+1/2\rfloor$.

383 Problem Prove *Hermite's Identity*: if x is a real number and n is a natural number then

$$\lfloor nx\rfloor=\lfloor x\rfloor+\lfloor x+\frac{1}{n}\rfloor+\lfloor x+\frac{2}{n}\rfloor+\cdots+\lfloor x+\frac{n-1}{n}\rfloor.$$

384 Problem Prove that for all integers m, n, the equality

$$\lfloor\frac{m+n}{2}\rfloor+\lfloor\frac{n-m+1}{2}\rfloor=n$$

holds.

385 Problem If a, b, c, d are positive real numbers such that

$$\lfloor na\rfloor+\lfloor nb\rfloor=\lfloor nc\rfloor+\lfloor nd\rfloor$$

for all natural numbers n, prove that

$$a+b=c+d.$$

386 Problem If n is a natural number, prove that

$$\lfloor\frac{n+2-\lfloor n/25\rfloor}{3}\rfloor=\lfloor\frac{8n+24}{25}\rfloor.$$

387 Problem Solve the equation

$$\lfloor\frac{x}{1994}\rfloor=\lfloor\frac{x}{1995}\rfloor.$$

388 Problem Let $[\alpha,\beta]$ be an interval which contains no integers. Prove that there is a positive integer n such that $[n\alpha,n\beta]$ still contains no integers but has length at least $1/6$.

389 Problem (IMO 1968) For every natural number n, evaluate the sum

$$\sum_{k=0}^{\infty}\lfloor\frac{n+2^k}{2^{k+1}}\rfloor.$$

390 Problem (Putnam 1973) Prove that if $n\in\mathbb{N}$,

$$\min_{k\in\mathbb{N}}(k+\lfloor n/k\rfloor)=\lfloor\sqrt{4n+1}\rfloor.$$

391 Problem (Dirichlet's principle of the hyperbola) Let N be the number of integer solutions to $xy\leq n, x>0, y>0$. Prove that

$$N=\sum_{k=1}^{n}\lfloor\frac{n}{k}\rfloor=2\sum_{1\leq k\leq\sqrt{n}}\lfloor\frac{n}{k}\rfloor-\lfloor\sqrt{n}\rfloor^2.$$

392 Problem (Circle Problem) Let $r>0$ and let T denote the number of lattice points of the domain $x^2+y^2\leq r^2$. Prove that

$$T=1+4\lfloor r\rfloor+8\sum_{0<x\leq r\sqrt{2}}\lfloor\sqrt{r^2-x^2}\rfloor+4\lfloor\frac{r}{\sqrt{2}}\rfloor^2.$$

393 Problem Let $d=(a,b)$. Prove that

$$\sum_{1\leq n\leq b-1}\lfloor\frac{an}{b}\rfloor=\frac{(a-1)(b-1)}{2}+\frac{d-1}{2}.$$

394 Problem (Eisenstein) If $(a,b)=1$ and a,b are odd, then

$$\sum_{1\leq n\leq(b-1)/2}\lfloor\frac{an}{b}\rfloor+\sum_{1\leq n\leq(a-1)/2}\lfloor\frac{bn}{a}\rfloor=\frac{(a-1)(b-1)}{4}.$$

395 Problem Let $m\in\mathbb{N}$ with $m>1$ and let y be a positive real number. Prove that

$$\sum_{x}\lfloor\sqrt[m]{\frac{y}{x}}\rfloor=\lfloor y\rfloor,$$

where the summation runs through all positive integers x not divisible by the mth power of an integer exceeding 1.

396 Problem For which natural numbers n will 112 divide

$$4^n-\lfloor(2+\sqrt{2})^n\rfloor?$$

397 Problem A *triangular number* is a number of the form $1+2+\cdots+n, n\in\mathbb{N}$. Find a formula for the nth non-triangular number.

398 Problem (AIME 1985) How many of the first thousand positive integers can be expressed in the form

$$\lfloor 2x\rfloor+\lfloor 4x\rfloor+\lfloor 6x\rfloor+\lfloor 8x\rfloor?$$

399 Problem (AIME 1987) What is the largest positive integer n for which there is a unique integer k such that

$$\frac{8}{15}<\frac{n}{n+k}<\frac{7}{13}?$$

400 Problem Prove that if p is an odd prime, then

$$\lfloor (2+\sqrt{5})^p \rfloor - 2^{p+1}$$

is divisible by p.

401 Problem Prove that the n-th number not of the form $\lfloor e^k \rfloor, k = 1, 2, \ldots$ is

$$T_n = n + \lfloor \ln(n+1+\lfloor \ln(n+1) \rfloor) \rfloor.$$

402 Problem (Leningrad Olympiad) How many different integers are there in the sequence

$$\lfloor \frac{1^2}{1980} \rfloor, \lfloor \frac{2^2}{1980} \rfloor, \ldots, \lfloor \frac{1980^2}{1980} \rfloor?$$

403 Problem Let $k \geq 2$ be a natural number and x a positive real number. Prove that

$$\lfloor \sqrt[k]{x} \rfloor = \lfloor \sqrt[k]{\lfloor x \rfloor} \rfloor.$$

404 Problem

1. Find a real number $x \neq 0$ such that $x, 2x, \ldots, 34x$ have no 7's in their decimal expansions.
2. Prove that for any real number $x \neq 0$ at least one of $x, 2x, \ldots 79x$ has a 7 in its decimal expansion.
3. Can you improve the "gap" between 34 and 79?

405 Problem (AIME 1991) Suppose that r is a real number for which

$$\sum_{k=19}^{91} \lfloor r + \frac{k}{100} \rfloor = 546.$$

Find the value of $\lfloor 100r \rfloor$.

406 Problem (AIME 1995) Let $f(n)$ denote the integer closest to $n^{1/4}$, when n is a natural number. Find the exact numerical value of

$$\sum_{n=1}^{1995} \frac{1}{f(n)}.$$

407 Problem Prove that

$$\int_0^1 (-1)^{\lfloor 1994x \rfloor + \lfloor 1995x \rfloor} \binom{1993}{\lfloor 1994x \rfloor} \binom{1994}{\lfloor 1995x \rfloor} dx = 0.$$

408 Problem Prove that

$$\lfloor \sqrt{n} + \sqrt{n+1} \rfloor = \lfloor \sqrt{n} + \sqrt{n+2} \rfloor.$$

409 Problem (Putnam 1976) Prove that

$$\lim_{n\to\infty} \sum_{1 \leq k \leq n} \left(\lfloor \frac{2n}{k} \rfloor - 2 \lfloor \frac{n}{k} \rfloor \right) = \ln 4 - 1.$$

410 Problem (Putnam 1983) Prove that

$$\lim_{n\to\infty} \frac{1}{n} \int_1^n \left|\left| \frac{n}{x} \right|\right| dx = \log_3(4/\pi).$$

You may appeal to *Wallis Product Formula:*

$$\frac{2}{1} \cdot \frac{2}{3} \cdot \frac{4}{3} \cdot \frac{4}{5} \cdot \frac{6}{5} \cdot \frac{6}{7} \cdot \frac{8}{7} \cdot \frac{8}{9} \cdots = \frac{\pi}{2}.$$

6.2 De Polignac's Formula

We will consider now the following result due to De Polignac.

411 Theorem (De Polignac's Formula) The highest power of a prime p dividing $n!$ is given by

$$\sum_{k=1}^{\infty} \lfloor \frac{n}{p^k} \rfloor.$$

Proof: *The number of integers contributing a factor of p is $\lfloor n/p \rfloor$, the number of factors contributing a second factor of p is $\lfloor n/p^2 \rfloor$, etc..*❑

412 Example How many zeroes are at the end of 300!?

Solution: The number of zeroes is determined by how many times 10 divides into 300. Since there are more factors of 2 in 300! than factors of 5, the number of zeroes is thus determined by the highest power of 5 in 300!. By De Polignac's Formula this is $\sum_{k=1}^{\infty} \lfloor 300/5^k \rfloor = 60 + 12 + 2 = 74.$

413 Example Does

$$7 \Big| \binom{1000}{500}?$$

Solution: The highest power of 7 dividing into 1000! is $\lfloor 1000/7 \rfloor + \lfloor 1000/7^2 \rfloor + \lfloor 1000/7^3 \rfloor = 142+20+2 = 164$. Similarly, the highest power of 7 dividing into 500! is $71+10+1 = 82$. Since $\dbinom{1000}{500} = \dfrac{1000!}{(500!)^2}$, the highest power of 7 that divides $\dbinom{1000}{500}$ is $164-2\cdot 82 = 0$, and so 7 does not divide $\dbinom{1000}{500}$.

414 Example Let $n = n_1+n_2+\cdots+n_k$ where the n_i are nonnegative integers. Prove that the quantity

$$\frac{n!}{n_1!n_2!\cdots n_k!}$$

is an integer.

Solution: From (3) in Theorem 365 we deduce by induction that

$$\lfloor a_1 \rfloor + \lfloor a_2 \rfloor + \cdots + \lfloor a_l \rfloor \le \lfloor a_1+a_2+\cdots+a_l \rfloor.$$

For any prime p, the power of p dividing $n!$ is

$$\sum_{j\ge 1} \lfloor n/p^j \rfloor = \sum_{j\ge 1} \lfloor (n_1+n_2+\cdots+n_k)/p^j \rfloor.$$

The power of p dividing $n_1!n_2!\cdots n_k!$ is

$$\sum_{j\ge 1} \lfloor n_1/p^j \rfloor + \lfloor n_2/p^j \rfloor + \cdots \lfloor n_k/p^j \rfloor.$$

Since

$$\lfloor n_1/p^j \rfloor + \lfloor n_2/p^j \rfloor + \cdots + \lfloor n_k/p^j \rfloor \le \lfloor (n_1+n_2+\cdots+n_k)/p^j \rfloor,$$

we see that the power of any prime dividing the numerator of

$$\frac{n!}{n_1!n_2!\cdots n_k!}$$

is at least the power of the same prime dividing the denominator, which establishes the assertion.

415 Example Given a positive integer $n > 3$, prove that the least common multiple of the products $x_1x_2\cdots x_k (k \ge 1)$, whose factors x_i are the positive integers with

$$x_1+x_2+\cdots x_k \le n,$$

is less than $n!$.

Solution: We claim that the least common multiple of the numbers in question is

$$\prod_{\substack{p \\ p \text{ prime}}} p^{\lfloor n/p \rfloor}.$$

Consider an arbitrary product $x_1x_2\cdots x_k$, and an arbitrary prime p. Suppose that $p^{\alpha_j}|x_j, p^{\alpha_j+1} \not| x_j$. Clearly $p^{\alpha_1}+\cdots+p\alpha_k \le n$ and since $p^{\alpha} \ge \alpha p$, we have

$$p(\alpha_1+\cdots\alpha_k) \le n \text{ or } \alpha_1+\cdots+\alpha_k \le \left\lfloor \frac{n}{p} \right\rfloor.$$

Hence it follows that the exponent of an arbitrary prime p is at most $\lfloor n/p \rfloor$. But on choosing $x_1 = \cdots = x_k = p, k = \lfloor n/p \rfloor$, we see that there is at least one product for which equality is achieved. This proves the claim.

The assertion of the problem now follows upon applying De Polignac's Formula and the claim.

Practice

416 Problem (AHSME 1977) Find the largest possible n such that 10^n divides $1005!$.

417 Problem Find the highest power of 17 that divides $(17^n - 2)!$ for a positive integer n.

418 Problem Find the exponent of the highest power of 24 that divides $300!$.

419 Problem Find the largest power of 7 in $300!$.

420 Problem (AIME 1983) What is the largest two-digit prime factor of the integer

$$\binom{200}{100}?$$

421 Problem (USAMO 1975)

1. Prove that

$$\llbracket 5x \rrbracket + \llbracket 5y \rrbracket \geq \llbracket 3x+y \rrbracket + \llbracket 3y+x \rrbracket.$$

2. Using the result of part 1 or otherwise, prove that

$$\frac{(5m)!(5n)!}{m!n!(3m+n)!(3n+m)!}$$

is an integer for all positive integers m, n.

422 Problem Prove that if $n > 1, (n,6) = 1$, then

$$\frac{(2n-4)!}{n!(n-2)!}$$

is an integer.

423 Problem (AIME 1992) Define a positive integer n to be a "factorial tail" if there is some positive integer m such that the base-ten representation of $m!$ ends with exactly n zeroes. How many positive integers less than 1992 are *not* factorial tails?

424 Problem Prove that if m and n are relatively prime positive integers then

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

is an integer.

425 Problem If p is a prime divisor of $\binom{2n}{n}$ with $p \geq \sqrt{2n}$ prove that the exponent of p in the factorisation of $\binom{2n}{n}$ equals 1.

426 Problem Prove that

$$\mathrm{lcm}\left(\binom{n}{1}, \binom{n}{2}, \ldots, \binom{n}{n}\right) = \frac{\mathrm{lcm}(1,2,\ldots,n+1)}{n+1}.$$

427 Problem Prove the following result of Catalan: $\binom{m+n}{n}$ divides $\binom{2m}{m}\binom{2n}{n}$.

6.3 Complementary Sequences

We define the *spectrum* of a real number α to be the infinite multiset of integers

$$Spec(\alpha) = \{\llbracket \alpha \rrbracket, \llbracket 2\alpha \rrbracket, \llbracket 3\alpha \rrbracket, \ldots\}.$$

Two sequences $Spec(\alpha)$ and $Spec(\beta)$ are said to be *complementary* if they partition the natural numbers, i.e. $Spec(\alpha) \cap Spec(\beta) = \varnothing$ and $Spec(\alpha) \cup Spec(\beta) = \mathbb{N}$.

For example, it appears that the two sequences

$$Spec(\sqrt{2}) = \{1,2,4,5,7,8,9,11,12,14,15,16,18,19,21,22,24,25,\ldots\},$$

and

$$Spec(2+\sqrt{2}) = \{3,6,10,13,17,20,23,27,30,34,37,40,44,47,51,\ldots\}$$

are complementary. The following theorem establishes a criterion for spectra to be complementary.

428 Theorem (Beatty's Theorem, 1926) If $\alpha > 1$ is irrational and

$$\frac{1}{\alpha}+\frac{1}{\beta}=1,$$

then the sequences

$$Spec(\alpha) \text{ and } Spec(\beta)$$

are complementary.

> **Proof:** *Since $\alpha > 1, \beta > 1, Spec(\alpha)$ and $Spec(\beta)$ are each sequences of distinct terms, and the total number of terms not exceeding N taken together in both sequences is $\llfloor N/\alpha \rrfloor + \llfloor N/\beta \rrfloor$. But $N/\alpha - 1 + N/\beta - 1 < \llfloor N/\alpha \rrfloor + [N/\beta] < N/\alpha + N/\beta$, the last inequality being strict because both α, β are irrational. As $1/\alpha + 1/\beta = 1$, we gather that $N-2 < \llfloor N/\alpha \rrfloor + \llfloor N/\beta \rrfloor < N$. Since the sandwiched quantity is an integer, we deduce $[N/\alpha]+[N/\beta] = N-1$. Thus the total number of terms not exceeding N in $Spec(\alpha)$ and $Spec(\beta)$ is $N-1$, as this is true for any $N \geq 1$ each interval $(n, n+1)$ contains exactly one such term. It follows that $Spec(\alpha) \cup Spec(\beta) = \mathbb{N}, Spec(\alpha) \cap Spec(\beta) = \varnothing$.* ❑

The converse of Beatty's Theorem is also true.

429 Theorem (Bang's Theorem, 1957) If the sequences

$$Spec(\alpha) \text{ and } Spec(\beta)$$

are complementary, then α, β are positive irrational numbers with

$$\frac{1}{\alpha}+\frac{1}{\beta}=1.$$

> **Proof:** *If both α, β are rational numbers, it is clear that $Spec(\alpha)$, $Spec(\beta)$ eventually contain the same integers, and so are not disjoint. Thus α and β must be irrational. If $0 < \alpha \leq 1$, given n there is an $\mathscr{M}$ for which $m\alpha - 1 < n \leq m\alpha$; hence $n = [m\alpha]$, which implies that $Spec(\alpha) = \mathbb{N}$, whence $\alpha > 1$ (and so $\beta > 1$ also). If $Spec(\alpha) \cap Spec(\beta)$ is finite, then*
>
> $$\lim_{n\to\infty} \frac{\llfloor n/\alpha \rrfloor + \llfloor n/\beta \rrfloor}{n} = 1,$$
>
> *but since $(\llfloor n/\alpha \rrfloor + \llfloor n/\beta \rrfloor)\dfrac{1}{n} \to 1/\alpha + 1/\beta$ as $n \to \infty$, it follows that $1/\alpha + 1/\beta = 1$.* ❑

430 Example Suppose we sieve the positive integers as follows: we choose $a_1 = 1$ and then delete $a_1 + 1 = 2$. The next term is 3, which we call a_2, and then we delete $a_2 + 2 = 5$. Thus the next available integer is $4 = a_3$, and we delete $a_3 + 3 = 7$, etc. Thereby we leave the integers $1, 3, 4, 6, 8, 9, 11, 12, 14, 16, 17, \ldots$. Find a formula for a_n.

Solution: What we are asking for is a sequence $\{S_n\}$ which is complementary to the sequence $\{S_n + n\}$. By Beatty's Theorem, $\llfloor n\tau \rrfloor$ and $\llfloor n\tau \rrfloor + n = \llfloor n(\tau+1) \rrfloor$ are complementary if $1/\tau + 1/(\tau+1) = 1$. But then $\tau = (1+\sqrt{5})/2$, the Golden ratio. The n-th term is thus $a_n = \llfloor n\tau \rrfloor$.

Practice

431 Problem (Skolem) Let $\tau = \dfrac{1+\sqrt{5}}{2}$ be the Golden Ratio. Prove that the three sequences $(n \geq 1)$ $\{\llfloor \tau \llfloor \tau n \rrfloor \rrfloor\}, \{\llfloor \tau \llfloor \tau^2 n \rrfloor \rrfloor\}, \{\llfloor \tau^2 n \rrfloor\}$ are complementary.

6.4 Arithmetic Functions

An *arithmetic* function f is a function whose domain is the set of positive integers and whose range is a subset of the complex numbers. The following functions are of considerable importance in Number Theory:

$d(n)$	*the number of positive divisors of the number n.*
$\sigma(n)$	*the sum of the positive divisors of n.*
$\phi(n)$	*the number of positive integers not exceeding n and relative prime to n.*
$\omega(n)$	*the number of distinct prime divisors of n.*
$\Omega(n)$	*the number of primes dividing n, counting multiplicity.*

In symbols the above functions are:

$$d(n)=\sum_{d|n}1,\ \sigma(n)=\sum_{d|n}d,\ \omega(n)=\sum_{p|n}1,\ \Omega(n)=\sum_{p^\alpha||n}\alpha,$$

and

$$\phi(n)=\sum_{\substack{1\leq k\leq n\\(k,n)=1}}1.$$

(The symbol $||$ in $p^\alpha||n$ is read *exactly divides* and it signifies that $p^\alpha|n$ but $p^{\alpha+1}\not|n$.)

For example, since 1, 2, 4, 5, 10 and 20 are the divisors of 20, we have $d(20)=6$, $\sigma(20)=42$, $\omega(20)=2$, $\Omega(20)=3$. Since the numbers $1,3,7,9,11,13,17,19$ are the positive integers not exceeding 20 and relatively prime to 20, we see that $\phi(20)=8$.

If f is an arithmetic function which is not identically 0 such that $f(mn)=f(m)f(n)$ for every pair of relatively prime natural numbers m,n, we say that f is then a *multiplicative function.* If $f(mn)=f(m)f(n)$ for every pair of natural numbers m,n we say then that f is *totally multiplicative*.

Let f be multiplicative and let n have the prime factorisation $n=p_1^{a_1}p_2^{a_2}\cdots p_r^{a_r}$. Then

$$f(n)=f(p_1^{a_1})f(p_2^{a_2})\cdots f(p_r^{a_r}).$$

A multiplicative function is thus determined by its values at prime powers. If f is multiplicative, then there is a positive integer a such that $f(a)\neq 0$. Hence $f(a)=f(1\cdot a)=f(1)f(a)$ which entails that $f(1)=1$.

We will now show that the functions d and σ are multiplicative. For this we need first the following result.

432 Theorem Let f be a multiplicative function and let $F(n)=\sum_{d|n}f(d)$. Then F is also multiplicative.

Proof: *Suppose that a,b are natural numbers with $(a,b)=1$. By the Fundamental Theorem of Arithmetic, every divisor d of ab has the form $d=d_1d_2$ where $d_1|a,d_2|b,(d_1,d_2)=1$. Thus there is a one-to-one correspondence between positive divisors d of ab and pairs d_1,d_2 of positive divisors of a and b. Hence, if $n=ab,(a,b)=1$ then*

$$F(n)=\sum_{d|n}f(d)=\sum_{d_1|a}\sum_{d_2|b}f(d_1d_2).$$

Since f is multiplicative the dextral side of the above equals

$$\sum_{d_1|a}\sum_{d_2|b}f(d_1)f(d_2)=\sum_{d_1|a}f(d_1)\sum_{d_2|b}f(d_2)=F(a)F(b).$$

This completes the proof. ❑

Since the function $f(n)=1$ for all natural numbers n is clearly multiplicative (indeed, totally multiplicative), the theorem above shows that $d(n)=\sum_{d|n} 1$ is a multiplicative function. If p is a prime, the divisors of p^a are $1, p, p^2, p^3, \ldots, p^a$ and so $d(p^a)=a+1$. This entails that if n has the prime factorisation $n=p_1^{a_1}p_2^{a_2}\cdots p_r^{a_r}$, then

$$d(n)=(1+a_1)(1+a_2)\cdots(1+a_r).$$

For example, $d(2904)=d(2^3\cdot 3\cdot 11^2)=d(2^3)d(3)d(11^2)=(1+3)(1+1)(1+2)=24$.

We give now some examples pertaining to the divisor function.

433 Example (AHSME 1993) For how many values of n will an n-sided polygon have interior angles with integral degree measures?

Solution: The measure of an interior angle of a regular n-sided polygon is $\frac{(n-2)180}{n}$. It follows that n must divide 180. Since there are 18 divisors of 180, the answer is 16, because $n\geq 3$ and so we must exclude the divisors 1 and 2.

434 Example Prove that $d(n)\leq 2\sqrt{n}$.

Solution: Each positive divisor a of n can paired with its complementary divisor $\frac{n}{a}$. As $n=a\cdot\frac{n}{a}$, one of these divisors must be $\leq\sqrt{n}$. This gives at most $2\sqrt{n}$ divisors.

435 Example Find all positive integers n such that $d(n)=6$.

Solution: Since 6 can be factored as $2\cdot 3$ and $6\cdot 1$, the desired n must have only two distinct prime factors, p and q, say. Thus $n=p^\alpha q^\beta$ and either $1+\alpha=2, 1+\beta=3$ or $1+\alpha=6, 1+\beta=1$. Hence, n must be of one of the forms pq^2 or p^5, where p,q are distinct primes.

436 Example Prove that

$$\sum_{k=1}^{n} d(k)=\sum_{j=1}^{n}\left\lfloor\frac{n}{j}\right\rfloor$$

Solution: We have

$$\sum_{k=1}^{n} d(k)=\sum_{k=1}^{n}\sum_{j|k} 1.$$

Interchanging the order of summation

$$\sum_{j\leq n}\sum_{\substack{j\leq k\leq n\\ k\equiv 0 \mod j}} 1=\sum_{j\leq n}\left\lfloor\frac{n}{j}\right\rfloor,$$

which is what we wanted to prove.

437 Example (Putnam 1967) A certain locker room contains n lockers numbered $1,2,\ldots,n$ and are originally locked. An attendant performs a sequence of operations $T_1, T_2, \ldots, T_n$ whereby with the operation $T_k, 1\leq k\leq n$, the condition of being locked or unlocked is changed for all those lockers and only those lockers whose numbers are multiples of k. After all the n operations have been performed it is observed that all lockers whose numbers are perfect squares (and only those lockers) are now open or unlocked. Prove this mathematically.

Solution: Observe that locker $m, 1\leq m\leq n$, will be unlocked after n operations if and only if m has an odd number of divisors. Now, $d(m)$ is odd if and only if m is a perfect square. The assertion is proved.

Since the function $f(n) = n$ is multiplicative (indeed, totally multiplicative), the above theorem entails that σ is multiplicative. If p is a prime, then clearly $\sigma(p^a) = 1+p+p^2+\cdots+p^a$. This entails that if n has the prime factorisation $n = p_1^{a_1}p_2^{a_2}\cdots p_r^{a_r}$, then

$$\sigma(n) = (1+p_1+p_1^2+\cdots+p_1^{a_1})(1+p_2+p_2^2+\cdots+p_w^{a_2})\cdots(1+p_r+p_r^2+\cdots+p_r^{a_r}).$$

This last product also equals

$$\frac{p_1^{a_1+1}-1}{p_1-1}\cdot\frac{p_2^{a_2+1}-1}{p_2-1}\cdots\frac{p_r^{a_r+1}-1}{p_r-1}.$$

We present now some examples related to the function σ.

438 Example (Putnam 1969) Let n be a positive integer such that $24|n+1$. Prove that the sum of all divisors of n is also divisible by 24.

Solution: Since $24|n+1$, $n \equiv 1$ or $2 \mod 3$ and $d \equiv 1,3,5$ or $7 \mod 8$. As $d(\frac{n}{d}) \equiv -1 \mod 3$ or $\mod 8$, the only possibilities are

$$\begin{array}{llll} d\equiv 1, & n/d \equiv 2 & \mod 3 & \text{or vice versa,}\\ d\equiv 1, & n/d \equiv 7 & \mod 8 & \text{or vice versa,}\\ d\equiv 3, & n/d \equiv 5 & \mod 8 & \text{or vice versa.}\end{array}$$

In all cases $d + n/d \equiv 0 \mod 3$ and $\mod 8$, whence 24 divides $d + n/d$. As $d \not\equiv n/d$, no divisor is used twice in the pairing. This implies that $24|\sum_{d|n} d$.

We say that a natural number is *perfect* if it is the sum of its proper divisors. For example, 6 is perfect because $6 = \sum_{d|6, d\neq 6} d = 1+2+3$. It is easy to see that a natural number is perfect if and only if $2n = \sum_{d|n} d$. The following theorem is classical.

439 Theorem An even number is perfect if and only if it is of the form $2^{p-1}(2^p-1)$ where both p and 2^p-1 are primes.

> **Proof:** *Suppose that $p, 2^p-1$ are primes. Then $\sigma(2^p-1) = 1+2^p-1$. Since $(2^{p-1}, 2^p-1) = 1$, $\sigma(2^{p-1}(2^p-1)) = \sigma(2^{p-1})\sigma(2^p-1) = (1+2+2^2+\cdots+2^{p-1})(1+2^p-1) = (2^p-1)2(2^{p-1})$, and $2^{p-1}(2^p-1)$ is perfect.*
>
> *Conversely, let n be an even perfect number. Write $n = 2^s m, m$ odd. Then $\sigma(n) = \sigma(2^s)\sigma(m) = (2^{s+1}-1)\sigma(m)$. Also, since n perfect is, $\sigma(n) = 2n = 2^{s+1}m$. Hence $(2^{s+1}-1)\sigma(m) = 2^{s+1}m$. One deduces that $2^{s+1}|\sigma(m)$, and so $\sigma(m) = 2^{s+1}b$ for some natural number b. But then $(2^{s+1}-1)b = m$, and so $b|m, b \neq m$.*
>
> *We propose to show that $b = 1$. Observe that $b+m = (2^{s+1}-1)b + b = 2^{s+1}b = \sigma(m)$. If $b \neq 1$, then there are at least three divisors of m, namely $1, b$ and m, which yields $\sigma(m) \geq 1+b+m$, a contradiction. Thus $b = 1$, and so $m = (2^{s+1}-1)b = 2^{s+1}-1$ is a prime. This means that $2^{s+1}-1$ is a Mersenne prime and hence $s+1$ must be a prime.*❑

440 Example Prove that for every natural number n there exist natural numbers x and y such that $x-y \geq n$ and $\sigma(x^2) = \sigma(y^2)$.

Solution: Let $s \geq n, (s,10) = 1$. We take $x = 5s, y = 4s$. Then $\sigma(x^2) = \sigma(y^2) = 31\sigma(s^2)$.

Practice

441 Problem Find the numerical values of $d(1024), \sigma(1024), \phi(1024)$, $\Omega(1024)$ and $\phi(1024)$.

442 Problem Describe all natural numbers n such that $d(n) = 10$.

443 Problem Prove that

$$d(2^n - 1) \geq d(n).$$

444 Problem Prove that $d(n) \leq \sqrt{3n}$ with equality if and only if $n = 12$.

445 Problem Prove that the following *Lambert expansion* holds:

$$\sum_{n=1}^{\infty} d(n)t^n = \sum_{n=1}^{\infty} \frac{t^n}{1-t^n}.$$

446 Problem Let $d_1(n) = d(n), d_k(n) = d(d_{k-1}(n)), k = 2, 3, \ldots$. Describe $d_k(n)$ for sufficiently large k.

447 Problem Let $m \in \mathbb{N}$ be given. Prove that the set

$$\mathscr{A} = \{n \in \mathbb{N} : m|d(n)\}$$

contains an infinite arithmetic progression.

448 Problem Let n be a perfect number. Show that

$$\sum_{d|n} \frac{1}{d} = 2.$$

449 Problem Prove that

$$\prod_{d|n} d = n^{d(n)/2}.$$

450 Problem Prove that the power of a prime cannot be a perfect number.

451 Problem (AIME, 1995) Let $n = 2^{31}3^{19}$. How many positive integer divisors of n^2 are less than n but do not divide n?

452 Problem Prove that if n is composite, then $\sigma(n) > n + \sqrt{n}$.

453 Problem Prove that $\sigma(n) = n + k$, $k > 1$ a fixed natural number has only finitely many solutions.

454 Problem Characterise all n for which $\sigma(n)$ is odd.

455 Problem Prove that p is a prime if and only if $\sigma(p) = 1 + p$.

456 Problem Prove that

$$\frac{\sigma(n!)}{n!} \geq 1 + \frac{1}{2} + \cdots + \frac{1}{n}.$$

457 Problem Prove that an odd perfect number must have at least two distinct prime factors.

458 Problem Prove that in an odd perfect number, only one of its prime factors occurs to an odd power; all the others occur to an even power.

459 Problem Show that an odd perfect number must contain one prime factor p such that, if the highest power of p occurring in n is p^a, both p and a are congruent to 1 modulo 4; all other prime factors must occur to an even power.

460 Problem Prove that every odd perfect number having three distinct prime factors must have two of its prime factors 3 and 5.

461 Problem Prove that there do not exist odd perfect numbers having exactly three distinct prime factors.

462 Problem Prove that

$$\sum_{k=1}^{n} \sigma(k) = \sum_{j=1}^{n} j\llbracket\frac{n}{j}\rrbracket.$$

463 Problem Find the number of sets of positive integers $\{a, b, c\}$ such that $a \times b \times c = 462$.

6.5 Euler's Function. Reduced Residues

Recall that Euler's $\phi(n)$ function counts the number of positive integers $a \leq n$ that are relatively prime to n. We will prove now that ϕ is multiplicative. This requires more work than that done for d and σ.

First we need the following definitions.

464 Definition Let $n > 1$. The $\phi(n)$ integers $1 = a_1 < a_2 < \cdots < a_{\phi(n)} = n-1$ less than n and relatively prime to n are called the *canonical reduced residues* modulo n.

465 Definition A *reduced residue system* modulo n, $n > 1$ is a set of $\phi(n)$ incongruent integers modulo n that are relatively prime to n.

For example, the canonical reduced residues $\mod 12$ are $1,5,7,11$ and the set $\{-11,5,19,23\}$ forms a reduced residue system modulo 12.

We are now ready to prove the main result of this section.

466 Theorem The function ϕ is multiplicative.

Proof: *Let n be a natural number with $n = ab, (a,b) = 1$. We arrange the ab integers $1,2,\ldots,ab$ as follows.*

$$\begin{array}{rrrcrcr}
1 & 2 & 3 & \ldots & k & \ldots & a \\
a+1 & a+2 & a+3 & \ldots & a+k & \ldots & 2a \\
2a+1 & 2a+2 & 2a+3 & \ldots & 2a+k & \ldots & 3a \\
\ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\
(b-1)a+1 & (b-1)a+2 & (b-1)a+3 & \ldots & (b-1)a+k & \ldots & ba
\end{array}$$

Now, an integer r is relatively prime to m if and only if it is relatively prime to a and b. We shall determine first the number of integers in the above array that are relatively prime to a and find out how may of them are also relatively prime to b.

There are $\phi(a)$ integers relatively prime to a in the first row. Now consider the k-th column, $1 \leq k \leq a$. Each integer on this column is of the form $ma+k, 0 \leq m \leq b-1$. As $k \equiv ma+k \mod a$, k will have a common factor with a if and only if $ma+k$ does. This means that there are exactly $\phi(a)$ columns of integers that are relatively prime to a. We must determine how many of these integers are relatively prime to b.

We claim that no two integers $k, a+k, \ldots, (b-1)a+k$ on the k-th column are congruent modulo b. For if $ia+k \equiv ja+k \mod b$ then $a(i-j) \equiv 0 \mod b$. Since $(a,b) = 1$, we deduce that $i-j \equiv 0 \mod b$ thanks to Corollary 346. Now $i,j \in [0,b-1]$ which implies that $|i-j| < b$. This forces $i = j$. This means that the b integers in any of these $\phi(n)$ columns are, in some order, congruent to the integers $0,1,\ldots,b-1$. But exactly $\phi(b)$ of these are relatively prime to b. This means that exactly $\phi(a)\phi(b)$ integers on the array are relatively prime to ab, which is what we wanted to show.❑

If p is a prime and m a natural number, the integers

$$p, 2p, 3p, \ldots, p^{m-1}p$$

are the only positive integers $\leq p^m$ sharing any prime factors with p^m. Thus $\phi(p^m) = p^m - p^{m-1}$. Since ϕ is multiplicative, if $n = p_1^{a_1} \cdots p_k^{a_k}$ is the factorisation of n into distinct primes, then

$$\phi(n) = (p_1^{a_1} - p_1^{a_1-1}) \cdots (p_k^{a_k} - p_k^{a_k-1}).$$

For example, $\phi(48) = \phi(2^4 \cdot 3) = \phi(2^4)\phi(3) = (2^4 - 2^3)(3-1) = 16$, and $\phi(550) = \phi(2 \cdot 5^2 \cdot 11) = \phi(2) \cdot \phi(5^2) \cdot \phi(11) = (2-1)(5^2-5)(11-1) = 1 \cdot 20 \cdot 10 = 200$.

467 Example Let n be a natural number. How many of the fractions $1/n, 2/n, \ldots, (n-1)/n, n/n$ are irreducible?

Solution: This number is clearly $\displaystyle\sum_{k=1}^{n} \phi(k)$.

468 Example Prove that for $n > 1$,

$$\sum_{\substack{1\leq a\leq n\\(a,n)=1}} a = \frac{n\phi(n)}{2}.$$

Solution: Clearly if $1 \leq a \leq n$ and $(a,n) = 1$, $1 \leq n-a \leq n$ and $(n-a,n) = 1$. Thus

$$S = \sum_{\substack{1\leq a\leq n\\(a,n)=1}} a = \sum_{\substack{1\leq a\leq n\\(a,n)=1}} n-a,$$

whence

$$2S = \sum_{\substack{1\leq a\leq n\\(a,n)=1}} n = n\phi(n).$$

The assertion follows.

469 Theorem Let n be a positive integer. Then $\sum_{d|n} \phi(d) = n$.

> **Proof:** *For each divisor d of n, let $T_d(n)$ be the set of positive integers $\leq n$ whose gcd with n is d. As d varies over the divisors of n, the T_d partition the set $\{1,2,\ldots,n\}$ and so*
>
> $$\sum_{d|n} T_d(n) = n.$$
>
> *We claim that $T_d(n)$ has $\phi(n/d)$ elements. Note that the elements of $T_d(n)$ are found amongst the integers $d, 2d, \ldots \frac{n}{d}d$. If $k \in T_d(n)$, then $k = ad, 1 \leq a \leq n/d$ and $(k,n) = d$. But then $(\frac{k}{d}, \frac{n}{d}) = 1$. This implies that $(a, \frac{n}{d}) = 1$. Therefore counting the elements of $T_d(n)$ is the same as counting the integers a with $1 \leq a \leq n/d, (a, \frac{n}{d}) = 1$. But there are exactly $\phi(n/d)$ such a. We gather that*
>
> $$n = \sum_{d|n} \phi(n/d).$$
>
> *But as d runs through the divisors of n, n/d runs through the divisors of n in reverse order, whence $n = \sum_{d|n} \phi(n/d) = \sum_{d|n} \phi(d)$.*❑

470 Example If $p-1$ and $p+1$ are twin primes, and $p > 4$, prove that $3\phi(p) \leq p$.

Solution: Observe that $p > 4$ must be a multiple of 6, so

$$p = 2^a 3^b m,\ ab \geq 1,\ (m,6) = 1.$$

We then have $\phi(p) \leq 2^a 3^{b-1}\phi(m) \leq 2^a 3^{b-1} m = p/3$.

471 Example Let $n \in \mathbb{N}$. Prove that the equation

$$\phi(x) = n!$$

is soluble.

Solution: We want to solve the equation $\phi(x) = n$ with the constraint that x has precisely the same prime factors as n. This restriction implies that $\phi(x)/x = \phi(n)/n$. It follows that $x = n^2/\phi(n)$.

Let $n = \prod_{p^\alpha || n} p^\alpha$. Then $x = \prod_{p^\alpha || n} \frac{p^\alpha}{p-1}$. The integer x will have the same prime factors as n provided that $\prod_{p|n}(p-1)|n$. It is clear then that a necessary and sufficient condition for $\phi(x) = n$ to be soluble under the restriction that x has precisely the same prime factors as n is $\prod_{p|n}(p-1)|n$. If $n = k!$, this last condition is clearly satisfied. An explicit solution to the problem is thus $x = (k!)^2/\phi(k!)$.

472 Example Let $\phi_k(n) = \phi(\phi_{k-1}(n)), k = 1, 2, \ldots,$ where $\phi_0(n) = \phi(n)$. Show that $\forall k \in \mathbb{N}, \phi_k(n) > 1$ for all sufficiently large n.

Solution: Let $p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$ be the prime factorisation of n. Clearly

$$p_1^{a_1/2} p_2^{a_2/2} \cdots p_r^{a_r/2} > 2^{r-1} \geq \frac{1}{2} \frac{p_1}{p_1 - 1} \cdots \frac{p_r}{p_r - 1}.$$

Hence

$$\phi(n) = \frac{p_1 - 1}{p_1} \frac{p_2 - 1}{p_2} \cdots \frac{p_r - 1}{p_r} p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r} \geq \frac{1}{2} \frac{p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}}{p_1^{a_1/2} p_2^{a_2/2} \cdots p_r^{a_r/2}}.$$

This last quantity equals $\sqrt{n}/2$. Therefore $\phi_1(n) > \frac{1}{2}\sqrt{\phi(n)} > \frac{1}{2}\sqrt{\frac{1}{4}\sqrt{n}} = \frac{1}{4}n^{1/4}$. In general we can show that $\phi_k(n) > \frac{1}{4}n^{2^{-k-1}}$. We conclude that $n \geq 2^{2^{k+2}}$ implies that $\phi_k(n) > 1$.

473 Example Find infinitely many integers n such that $10|\phi(n)$.

Solution: Take $n = 11^k, k = 1, 2, \ldots$. Then $\phi(11^k) = 11^k - 11^{k-1} = 10 \cdot 11^{k-1}$.

Practice

474 Problem Prove that

$$\phi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right).$$

475 Problem Prove that if n is composite then $\phi(n) \leq n - \sqrt{n}$. When is equality achieved?

476 Problem (AIME 1992) Find the sum of all positive rational numbers that are less than 10 and have denominator 30 when written in lowest terms.

Answer: 400

477 Problem Prove that $\phi(n) \geq n2^{-\omega(n)}$.

478 Problem Prove that $\phi(n) > \sqrt{n}$ for $n > 6$.

479 Problem If $\phi(n)|n$, then n must be of the form $2^a 3^b$ for nonnegative integers a, b.

480 Problem Prove that if $\phi(n)|n - 1$, then n must be square-free.

481 Problem (Mandelbrot 1994) Four hundred people are standing in a circle. You tag one person, then skip k people, then tag another, skip k, and so on, continuing until you tag someone for the second time. For how many positive values of k less than 400 will every person in the circle get tagged at least once?

482 Problem Prove that if $\phi(n)|n - 1$ and n is composite, then n has at least three distinct prime factors.

483 Problem Prove that if $\phi(n)|n - 1$ and n is composite, then n has at least four prime factors.

484 Problem For $n > 1$ let $1 = a_1 < a_2 < \cdots < a_{\phi(n)} = n-1$ be the positive integers less than n that are relatively prime to n. Define the Jacobsthal function

$$g(n) := \max_{1 \leq k \leq \phi(n)-1} a_{k+1} - a_k$$

to be the maximum gap between the a_k. Prove that $\omega(n) \leq g(n)$. (Hint: Use the Chinese Remainder Theorem).

485 Problem Prove that a necessary and sufficient condition for n to be a prime is that

$$\sigma(n) + \phi(n) = nd(n).$$

6.6 Multiplication in $\mathbb{Z}_n$

In section 3.5 we saw that $\mathbb{Z}_n$ endowed with the operation of addition $+_n$ becomes a group. We are now going to investigate the multiplicative structure of $\mathbb{Z}_n$.

How to define multiplication in $\mathbb{Z}_n$? If we want to multiply $\mathsf{a} \cdot_n \mathsf{b}$ we simply multiply $a \cdot b$ and reduce the result $\mod n$. As an example, let us consider Table 6.1. To obtain $4 \cdot_6 2$ we first multiplied $4 \cdot 2 = 8$ and then reduced $\mod 6$ obtaining $8 \equiv 2 \mod 6$. The answer is thus $4 \cdot_6 2 = 2$.

Another look at the table shows the interesting product $3 \cdot_6 2 = 0$. Why is it interesting? We have multiplied to non-zero entities and obtained a zero entity!

Does $\mathbb{Z}_6$ form a group under $\cdot_6$? What is the multiplicative identity? In analogy with the rational numbers, we would like 1 to be the multiplicative identity. We would then define the multiplicative inverse of **a** to be that **b** that has the property that $\mathsf{a} \cdot_6 \mathsf{b} = \mathsf{b} \cdot_6 \mathsf{a} = 1$. But then, we encounter some problems. For example, we see that $0, 2, 3$, and 4 do not have a multiplicative inverse. We need to be able to identify the invertible elements of $\mathbb{Z}_n$. For that we need the following.

$\cdot_6$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Table 6.1: Multiplication Table for $\mathbb{Z}_6$

486 Definition Let $n > 1$ be a natural number. An integer b is said to be the inverse of an integer a modulo n if $ab \equiv 1 \mod n$.

It is easy to see that inverses are unique $\mod n$. For if x, y are inverses to $a \mod n$ then $ax \equiv 1 \mod n$ and $ay \equiv 1 \mod n$. Multiplying by y the first of these congruences, $(ya)x \equiv y \mod n$. Hence $x \equiv y \mod n$.

487 Theorem Let $n > 1, a$ be integers. Then a possesses an inverse modulo n if and only if a is relatively prime to n.

> **Proof:** *Assume that b is the inverse of a* $\mod n$*. Then* $ab \equiv 1 \mod n$*, which entails the existence of an integer s such that* $ab - 1 = sn$*, i.e.* $ab - sn = 1$*. This is a linear combination of a and n and hence divisible by* (a, n)*. This implies that* $(a, n) = 1$*.*
>
> *Conversely if* $(a, n) = 1$*, by the Bachet-Bezout Theorem there are integers x, y such that* $ax + ny = 1$*. This immediately yields* $ax \equiv 1 \mod n$*, i.e., a has an inverse* $\mod n$*.*❑

488 Example Find the inverse of $5 \mod 7$.

Solution: We are looking for a solution to the congruence $5x \equiv 1 \mod 7$. By inspection we see that this is $x \equiv 3 \mod 7$.

According to the preceding theorem, a will have a multiplicative inverse if and only if $(a,n)=1$. We thus see that only the reduced residues $\mod n$ have an inverse. We let $\mathbb{Z}_n^\times = \{\mathtt{a}_1, \mathtt{a}_2, \ldots, \mathtt{a}_{\phi(n)}\}$. It is easy to see that the operation $\cdot_n$ is associative, since it inherits associativity from the integers. We conclude that $\mathbb{Z}_n^\times$ is a group under the operation $\cdot_n$.

We now give some assorted examples.

489 Example (IMO 1964) Prove that there is no positive integer n for which 2^n+1 is divisible by 7.

Solution: Observe that $2^1 \equiv 2, 2^2 \equiv 4$, $2^3 \equiv 1 \mod 7$, $2^4 \equiv 2 \mod 7$, $2^5 \equiv 4 \mod 7$, $2^6 \equiv 1 \mod 7$, etc. The pattern 2, 4, 1, repeats thus cyclically. This says that there is no power of 2 which is $\equiv -1 \equiv 6 \mod 7$.

490 Theorem If a is relatively prime to the positive integer n, there exists a positive integer $k \leq n$ such that $a^k \equiv 1 \mod n$.

> **Proof:** *Since $(a,n)=1$ we must have $(a^j,n)=1$ for all $j \geq 1$. Consider the sequence $a, a^2, a^3, \ldots, a^{n+1} \mod n$. As there are $n+1$ numbers and only n residues mod n, the Pigeonhole Principle two of these powers must have the same remainder $\mod n$. That is, we can find s,t with $1 \leq s < t \leq n+1$ such that $a^s \equiv a^t \mod n$. Now, $1 \leq t-s \leq n$. Hence $a^s \equiv a^t \mod n$ gives $a^{t-s}a^s \equiv a^{t-s}a^t \mod n$, which is to say $a^t \equiv a^{t-s}a^t \mod n$. Using Corollary 346 we gather that $a^{t-s} \equiv 1 \mod n$, which proves the result.*❏

If $(a,n)=1$, the preceding theorem tells us that there is a positive integer k with $a^k \equiv 1 \mod n$. By the Well-Ordering Principle, there must be a smallest positive integer with this property. This prompts the following definition.

491 Definition If m is the least positive integer with the property that $a^m \equiv 1 \mod n$, we say that a has order $m \mod n$.

For example, $3^1 \equiv 3, 3^2 \equiv 2, 3^3 \equiv 6, 3^4 \equiv 4, 3^5 \equiv 5, 3^6 \equiv 1 \mod 7$, and so the order of $3 \mod 7$ is 6. We write this fact as $\mathrm{ord}_7 3 = 6$.

Given n, not all integers a are going to have an order $\mod n$. This is clear if $n|a$, because then $a^m \equiv 0 \mod n$ for all positive integers m. The question as to which integers are going to have an order $\mod n$ is answered in the following theorem.

492 Theorem Let $n>1$ be a positive integer. Then $a \in \mathbb{Z}$ has an order $\mod n$ if and only if $(a,n)=1$.

> **Proof:** *If $(a,n)=1$, then a has an order in view of Theorem 490 and the Well-Ordering Principle. Hence assume that a has an order $\mod n$. Clearly $a \neq 0$. The existence of an order entails the existence of a positive integer m such that $a^m \equiv 1 \mod n$. Hence, there is an integer s with $a^m + sn = 1$ or $a \cdot a^{m-1} + sn = 1$. This is a linear combination of a and n and hence divisible by (a,n). This entails that $(a,n)=1$.* ❏

The following theorem is of utmost importance.

493 Theorem Let $(a,n)=1$ and let t be an integer. Then $a^t \equiv 1 \mod n$ if and only if $\mathrm{ord}_n a | t$.

> **Proof:** *Assume that $\mathrm{ord}_n a|t$. Then there is an integer s such that $s\mathrm{ord}_n a = t$. This gives*
>
> $$a^t \equiv a^{s\mathrm{ord}_n a} \equiv (a^{\mathrm{ord}_n a})^s \equiv 1^s \equiv 1 \mod n.$$
>
> *Conversely, assume that $a^t \equiv 1 \mod n$ and $t = x \cdot \mathrm{ord}_n a + y, 0 \leq y < \mathrm{ord}_n a$. Then*
>
> $$a^y \equiv a^{t - x\mathrm{ord}_n a} \equiv a^t \cdot (a^{\mathrm{ord}_n a})^{-x} \equiv 1 \cdot 1^{-x} \equiv 1 \mod n.$$
>
> *If $y>0$ we would have a positive integer smaller than $\mathrm{ord}_n a$ with the property $a^y \equiv 1 \mod n$. This contradicts the definition of $\mathrm{ord}_n a$ as the smallest positive integer with that property. Hence $y=0$ and thus $t = x \cdot \mathrm{ord}_n a$, i.e., $\mathrm{ord}_n a|t$.*❏

494 Example (IMO 1964) Find all positive integers n for which $2^n - 1$ is divisible by 7.

Solution: Observe that the order of $2 \mod 7$ is 3. We want $2^n \equiv 1 \mod 7$. It must then be the case that $3|n$. Thus $n = 3, 6, 9, 12, \ldots$.

The following result will be used repeatedly.

495 Theorem Let $n > 1, a \in \mathbb{Z}, (a,n) = 1$. If $r_1, r_2, \ldots, r_{\phi(n)}$ is a reduced set of residues modulo n, then $ar_1, ar_2, \ldots, ar_{\phi(n)}$ is also a reduced set of residues modulo n.

> **Proof:** *We just need to show that the $\phi(n)$ numbers $ar_1, ar_2, \ldots, ar_{\phi(n)}$ are mutually incongruent $\mod n$. Suppose that $ar_i \equiv ar_j \mod n$ for some $i \neq j$. Since $(a,n) = 1$, we deduce from Corollary 346 that $r_i \equiv r_j \mod n$. This contradicts the fact that the r's are incongruent, so the theorem follows.*❑

For example, as $1, 5, 7, 11$ is a reduced residue system modulo 12 and $(12, 5) = 1$, the set $5, 25, 35, 55$ is also a reduced residue system modulo 12. Again, the $1, 5, 7, 11$ are the $5, 25, 35, 55$ in some order and $1 \cdot 5 \cdot 7 \cdot 11 \equiv 5 \cdot 25 \cdot 35 \cdot 55 \mod 12$.

The following corollary to Theorem 495 should be immediate.

496 Corollary Let $n > 1, a, b \in \mathbb{Z}, (a,n) = 1$. If $r_1, r_2, \ldots, r_{\phi(n)}$ is a reduced set of residues modulo n, then $ar_1 + b, ar_2 + b, \ldots, ar_{\phi(n)} + b$ is also a reduced set of residues modulo n.

Practice

497 Problem Find the order of 5 modulo 12.

6.7 Möbius Function

498 Definition The *Möbius function* is defined for positive integer n as follows:

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1, \\ (-1)^{\omega(n)} & \text{if } \omega(n) = \Omega(n), \\ 0 & \text{if } \omega(n) < \Omega(n). \end{cases}$$

Thus μ is 1 for $n = 1$ and square free integers with an even number of prime factors, -1 for square free integers with an odd number of prime factors, and 0 for non-square free integers. Thus for example $\mu(6) = 1, \mu(30) = -1$ and $\mu(18) = 0$.

499 Theorem The Möbius Function μ is multiplicative.

> **Proof:** *Assume $(m,n) = 1$. If both $\mathscr{M}$ and n are square-free then*
>
> $$\mu(m)\mu(n) = (-1)^{\omega(m)}(-1)^{\omega(n)} = (-1)^{\omega(m)+\omega(n)} = \mu(mn).$$
>
> *If one of m, n is not square-free then*
>
> $$\mu(m)\mu(n) = 0 = \mu(mn).$$
>
> *This proves the theorem.* ❑

500 Theorem

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{if } n = 1, \\ 0 & \text{if } n > 1. \end{cases}$$

Proof: *There are* $\binom{\omega(n)}{k}$ *square-free divisors* d *of* n *with exactly* k *prime factors. For all such* $d, \mu(d) = (-1)^k$. *The sum in question is thus*

$$\sum_{d|n} \mu(d) = \sum_{k=0}^{\omega(n)} \binom{\omega(n)}{k} (-1)^k.$$

By the Binomial Theorem this last sum is $(1-1)^{\omega(n)} = 0$.❑

501 Theorem (Möbius Inversion Formula) Let f be an arithmetical function and $F(n) = \sum_{d|n} f(d)$. Then

$$f(n) = \sum_{d|n} \mu(d) F(n/d) = \sum_{d|n} \mu(n/d) F(d).$$

Proof: *We have*

$$\begin{aligned} \sum_{d|n} \mu(d) F(n/d) &= \sum_{d|n} \sum_{d|n} \sum_{s|\frac{n}{d}} f(s) \\ &= \sum_{ds|n} \mu(d) f(s) \\ &= \sum_{s|n} f(s) \sum_{d|\frac{n}{s}} \mu(d). \end{aligned}$$

In view of theorem 500, *the inner sum is different from* 0 *only when* $\frac{n}{s} = 1$. *Hence only the term* $s = n$ *in the outer sum survives, which means that the above sums simplify to* $f(n)$.❑

We now show the converse to Theorem 501.

502 Theorem Let f, F be arithmetic functions with $f(n) = \sum_{d|n} \mu(d) F(n/d)$ for all natural numbers n. Then $F(n) = \sum_{d|n} f(d)$.

Proof: *We have*

$$\begin{aligned} \sum_{d|n} f(d) &= \sum_{d|n} \sum_{s|d} \mu(s) F(d/s) \\ &= \sum_{d|n} \sum_{s|d} \mu(d/s) F(s) \\ &= \sum_{s|n} \sum_{r|\frac{n}{s}} \mu(r) F(s). \end{aligned}$$

Using Theorem 500, *the inner sum will be* 0 *unless* $s = n$, *in which case the entire sum reduces to* $F(n)$.❑

Practice

503 Problem Prove that

$$\phi(n) = n \sum_{d|n} \frac{\mu(d)}{d}.$$

504 Problem If f is an arithmetical function and $F(n) =$

$\sum_{k=1}^{n} f([n/k])$, then

$$f(n) = \sum_{j=1}^{n} \mu(j)F([n/j]).$$

505 Problem If F is an arithmetical function such that $f(n) = \sum_{k=1}^{n} \mu(k)F([n/k])$, prove that $F(n) = \sum_{j=1}^{n} f(j)$.

506 Problem Prove that $\sum_{d|n} |\mu(d)| = 2^{\omega(n)}$.

507 Problem Prove that $\sum_{d|n} \mu(d)d(d) = (-1)^{\omega(n)}$.

508 Problem Given any positive integer k, prove that there exist infinitely many integers n with

$$\mu(n+1) = \mu(n+2) = \cdots = \mu(n+k).$$

Chapter 7

More on Congruences

7.1 Theorems of Fermat and Wilson

509 Theorem (Fermat's Little Theorem) Let p be a prime and let $p \not| a$. Then

$$a^{p-1} \equiv 1 \mod p.$$

Proof: *Since $(a,p)=1$, the set $a\cdot 1, a\cdot 2, \ldots, a\cdot(p-1)$ is also a reduced set of residues* $\mod p$ *in view of Theorem 495. Hence*

$$(a\cdot 1)(a\cdot 2)\cdots(a\cdot(p-1)) \equiv 1\cdot 2\cdots(p-1) \mod p,$$

or

$$a^{p-1}(p-1)! \equiv (p-1)! \mod p.$$

As $((p-1)!,p)=1$ we may cancel out the $(p-1)!$'s in view of Corollary 346. This proves the theorem.❑

As an obvious corollary, we obtain the following.

510 Corollary For every prime p and for every integer a,

$$a^p \equiv a \mod p.$$

Proof: *Either $p|a$ or $p \not| a$. If $p|a, a \equiv 0 \equiv a^p$* $\mod p$ *and there is nothing to prove. If $p \not| a$, Fermat's Little Theorem yields $p|a^{p-1}-1$. Hence $p|a(a^{p-1}-1) = a^p - a$, which again gives the result.*❑

The following corollary will also be useful.

511 Corollary Let p be a prime and a an integer. Assume that $p \not| a$. Then $\mathrm{ord}_p a | p-1$.

Proof: *This follows immediately from Theorem 493 and Fermat's Little Theorem.*❑

512 Example Find the order of $8 \mod 11$.

Solution: By Corollary 511 $\mathrm{ord}_{11} 8$ is either $1,2,5$ or 10. Now $8^2 \equiv -2 \mod 11, 8^4 \equiv 4 \mod 11$ and $8^5 \equiv -1 \mod 11$. The order is thus $\mathrm{ord}_{11} 8 = 10$.

513 Example Let $a_1 = 4, a_n = 4^{a_{n-1}}, n > 1$. Find the remainder when a_{100} is divided by 7.

Solution: By Fermat's Little Theorem, $4^6 \equiv 1 \mod 7$. Now, $4^n \equiv 4 \mod 6$ for all positive integers n, i.e., $4^n = 4+6t$ for some integer t. Thus

$$a_{100} \equiv 4^{a_{99}} \equiv 4^{4+6t} \equiv 4^4 \cdot (4^6)^t \equiv 4 \mod 7.$$

514 Example Prove that for $m,n \in \mathbb{Z}$, $mn(m^{60}-n^{60})$ is always divisible by 56786730.

Solution: Let $a = 56786730 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 31 \cdot 61$. Let $Q(x,y) = xy(x^{60}-y^{60})$. Observe that $(x-y)|Q(x,y)$, $(x^2-y^2)|Q(x,y)$, $(x^3-y^3)|Q(x,y)$, $(x^4-y^4)|Q(x,y)$, $(x^6-y^6)|Q(x,y)$, $(x^{10}-y^{10})|Q(x,y)$, $(x^{12}-y^{12})|Q(x,y)$, and $(x^{30}-y^{30})|Q(x,y)$.

If p is any one of the primes dividing a, the Corollary to Fermat's Little Theorem yields $m^p - m \equiv 0 \mod p$ and $n^p - n \equiv 0 \mod p$. Thus $n(m^p-m)-m(n^p-n) \equiv 0 \mod p$, i.e., $mn(m^{p-1}-n^{p-1}) \equiv 0 \mod p$. Hence, we have $2|mn(m-n)|Q(m,n), 3|mn(m^2-n^2)|Q(m,n), 5|mn(m^4-n^4)|Q(m,n), 7|mn(m^6-n^6)|Q(m,n), 11|mn(m^{10}-n^{10})|Q(m,n), 13|mn(m^{12}-n^{12})|Q(m,n), 31|$ $n^{30})|Q(m,n)$ and $61|mn(m^{60}-n^{60})|Q(m,n)$. Since these are all distinct primes, we gather that $a|mnQ(m,n)$, which is what we wanted.

515 Example (Putnam 1972) Show that given an odd prime p, there are always infinitely many integers n for which $p|n2^n+1$.

Answer: For any odd prime p, take $n = (p-1)^{2k+1}, k = 0,1,2,\ldots$. Then

$$n2^n+1 \equiv (p-1)^{2k+1}(2^{p-1})^{(p-1)^{2k}}+1 \equiv (-1)^{2k+1}1^{2k}+1 \equiv 0 \mod p.$$

516 Example Prove that there are no integers $n > 1$ with $n|2^n-1$.

Solution: If $n|2^n-1$ for some $n>1$, then n must be odd and have a smallest odd prime p as a divisor. By Fermat's Little Theorem, $2^{p-1} \equiv 1 \mod p$. By Corollary 511 , $\text{ord}_p 2$ has a prime factor in common with $p-1$. Now, $p|n|2^n-1$ and so $2^n \equiv 1 \mod p$. Again, by Corollary 511, $\text{ord}_p 2$ must have a common prime factor with n (clearly $\text{ord}_p 2 > 1$). This means that n has a smaller prime factor than p, a contradiction.

517 Example Let p be a prime. Prove that

1. $$\binom{p-1}{n} \equiv (-1)^n \mod p,\ 1 \le n \le p-1.$$
2. $$\binom{p+1}{n} \equiv 0 \mod p,\ 2 \le n \le p-1.$$
3. If $p \neq 5$ is an odd prime, prove that either f_{p-1} or f_{p+1} is divisible by p.

Solution: (1) $(p-1)(p-2)\cdots(p-n) \equiv (-1)(-2)\cdots(-n) \equiv (-1)^n n! \mod p$. The assertion follows from this.
(2) $(p+1)(p)(p-1)\cdots(p-n+2) \equiv (1)(0)(-1)\cdots(-n+2) \equiv 0 \mod p$. The assertion follows from this.
(3) Using the Binomial Theorem and Binet's Formula

$$f_n = \frac{1}{2^{n-1}}\left(\binom{n}{1}+5\binom{n}{3}+5^2\binom{n}{5}+\cdots\right).$$

From this and (1),

$$2^{p-2}f_{p-1} \equiv p-1-(5+5^2+\cdots+5^{(p-3)/2}) \equiv -\frac{5^{(p-1)/2}-1}{4} \mod p.$$

Using (2),

$$2^p f_{p+1} \equiv p+1+5^{(p-1)/2} \equiv 5^{(p-1)/2}+1 \mod p.$$

Thus

$$2^p f_{p-1} f_{p+1} \equiv 5^{p-1} - 1 \mod p.$$

But by Fermat's Little Theorem, $5^{p-1} \equiv 1 \mod p$ for $p \neq 5$. The assertion follows.

518 Lemma If $a^2 \equiv 1 \mod p$, then either $a \equiv 1 \mod p$ or $a \equiv -1 \mod p$.

> **Proof:** *We have $p|a^2 - 1 = (a-1)(a+1)$. Since p is a prime, it must divide at least one of the factors. This proves the lemma.*❑

519 Theorem (Wilson's Theorem) If p is a prime, then $(p-1)! \equiv -1 \mod p$.

> **Proof:** *If $p = 2$ or $p = 3$, the result follows by direct verification. So assume that $p > 3$. Consider $a, 2 \leq a \leq p-2$. To each such a we associate its unique inverse $\overline{a} \mod p$, i.e. $a\overline{a} \equiv 1 \mod p$. Observe that $a \neq \overline{a}$ since then we would have $a^2 \equiv 1 \mod p$ which violates the preceding lemma as $a \neq 1, a \neq p-1$. Thus in multiplying all a in the range $2 \leq a \leq p-2$, we pair them of with their inverses, and the net contribution of this product is therefore 1. In symbols,*
>
> $$2 \cdot 3 \cdots (p-2) \equiv 1 \mod p.$$
>
> *In other words,*
>
> $$(p-1)! \equiv 1 \cdot \left(\prod_{2 \leq a \leq p-2} j \right) \cdot (p-1) \equiv 1 \cdot 1 \cdot (p-1) \equiv -1 \mod p.$$
>
> *This gives the result.* ❑

520 Example If $p \equiv 1 \mod 4$, prove that

$$\left(\frac{p-1}{2}\right)! \equiv -1 \mod p.$$

Solution: In the product $(p-1)!$ we pair off $j, 1 \leq j \leq (p-1)/2$ with $p-j$. Observe that $j(p-j) \equiv -j^2 \mod p$. Hence

$$-1 \equiv (p-1)! \equiv \prod_{1 \leq j \leq (p-1)/2} -j^2 \equiv (-1)^{(p-1)/2} \left(\frac{p-1}{2}\right)! \mod p.$$

As $(-1)^{(p-1)/2} = 1$, we obtain the result.

521 Example (IMO 1970) Find the set of all positive integers n with the property that the set

$$\{n, n+1, n+2, n+3, n+4, n+5\}$$

can be partitioned into two sets such that the product of the numbers in one set equals the product of the numbers in the other set.

Solution: We will show that no such partition exists. Suppose that we can have such a partition, with one of the subsets having product of its members equal to A and the other having product of its members equal to B. We might have two possibilities. The first possibility is that exactly one of the numbers in the set $\{n, n+1, n+2, n+3, n+4, n+5\}$ is divisible by 7, in which case exactly one of A or B is divisible by 7, and so $A \cdot B$ is not divisible by 7^2, and so $A \cdot B$ is not a square. The second possibility is that all of the members of the set are relatively prime to 7. In this last case we have

$$n(n+1) \cdots (n+6) \equiv 1 \cdot 2 \cdots 6 \equiv A \cdot B \equiv -1 \mod 7.$$

But if $A = B$ then we are saying that there is an integer A such that $A^2 \equiv -1 \mod 7$, which is an impossibility, as -1 is not a square $\mod 7$. This finishes the proof.

Practice

522 Problem Find all the natural numbers n for which $3|(n2^n+1)$.

523 Problem Prove that there are infinitely many integers n with $n|2^n+2$.

524 Problem Find all primes p such that $p|2^p+1$.

Answer: $p=3$ only.

525 Problem If p and q are distinct primes prove that

$$pq|(a^{pq}-a^p-a^q-a)$$

for all integers a.

526 Problem If p is a prime prove that $p|a^p+(p-1)!a$ for all integers a.

527 Problem If $(mn,42)=1$ prove that $168|m^6-n^6$.

528 Problem Let p and q be distinct primes. Prove that

$$q^{p-1}+p^{q-1}\equiv 1 \mod pq.$$

529 Problem If p is an odd prime prove that $n^p\equiv n \mod 2p$ for all integers n.

530 Problem If p is an odd prime and $p|m^p+n^p$ prove that $p^2|m^p+n^p$.

531 Problem Prove that $n>1$ is a prime if and only if $(n-1)!\equiv -1 \mod n$.

532 Problem Prove that if p is an odd prime

$$1^2\cdot 3^2\cdots(p-2)^2\equiv 2^2\cdot 4^2\cdots(p-1)^2\equiv(-1)^{(p-1)/2} \mod p$$

533 Problem Prove that $19|(2^{2^{6k+2}}+3)$ for all nonnegative integers k.

7.2 Euler’s Theorem

In this section we obtain a generalisation of Fermat’s Little Theorem, due to Euler. The proof is analogous to that of Fermat’s Little Theorem.

534 Theorem (Euler’s Theorem) Let $(a,n)=1$. Then $a^{\phi(n)}\equiv 1 \mod n$.

Proof: *Let $a_1,a_2,\ldots,a_{\phi(n)}$ be the canonical reduced residues $\mod n$. As $(a,n)=1$, $aa_1,aa_2,\ldots,aa_{\phi(n)}$ also forms a set of incongruent reduced residues. Thus*

$$aa_1\cdot aa_2\cdots aa_{\phi(n)}\equiv a_1a_2\cdots a_{\phi(n)} \mod n,$$

or

$$a^{\phi(n)}a_1a_2\cdots a_{\phi(n)}\equiv a_1a_2\cdots a_{\phi(n)} \mod n.$$

As $(a_1a_2\cdots a_{\phi(n)},n)=1$, we may cancel the product $a_1a_2\cdots a_{\phi(n)}$ from both sides of the congruence to obtain Euler’s Theorem.❑

Using Theorem 534 we obtain the following corollary.

535 Corollary Let $(a,n)=1$. Then $\text{ord}_n a|\phi(n)$.

536 Example Find the last two digits of 3^{1000}.

Solution: As $\phi(100)=40$, by Euler’s Theorem, $3^{40}\equiv 1 \mod 100$. Thus

$$3^{1000}=(3^{40})^{25}\equiv 1^{25}=1 \mod 100,$$

and so the last two digits are 01.

537 Example Find the last two digits of $7^{7^{1000}}$.

Solution: First observe that $\phi(100) = \phi(2^2)\phi(5^2) = (2^2-2)(5^2-5) = 40$. Hence, by Euler's Theorem, $7^{40} \equiv 1 \mod 100$. Now, $\phi(40) = \phi(2^3)\phi(5) = 4\cdot 4 = 16$, hence $7^{16} \equiv 1 \mod 40$. Finally, $1000 = 16\cdot 62+8$. This means that $7^{1000} \equiv (7^{16})^{62}7^8 \equiv 1^{62}7^8 \equiv (7^4)^2 \equiv 1^2 \equiv 1 \mod 40$. This means that $7^{1000} = 1+40t$ for some integer t. Upon assembling all this

$$7^{7^{1000}} \equiv 7^{1+40t} \equiv 7\cdot(7^{40})^t \equiv 7 \mod 100.$$

This means that the last two digits are 07.

538 Example (IMO 1978) m,n are natural numbers with $1 \leq m < n$. In their decimal representations, the last three digits of 1978^m are equal, respectively, to the last three digits of 1978^n. Find m,n such that $m+n$ has its least value.

Solution: As $m+n = n-m+2m$, we minimise $n-m$. We are given that

$$1978^n - 1978^m = 1978^m(1978^{n-m}-1)$$

is divisible by $1000 = 2^35^3$. Since the second factor is odd, 2^3 must divide the first and so $m \geq 3$. Now, $\text{ord}_{125}1978$ is the smallest positive integer s with

$$1978^s \equiv 1 \mod 125.$$

By Euler's Theorem

$$1978^{100} \equiv 1 \mod 125$$

and so by Corollary 7.3 $s|100$. Since $125|(1978^s-1)$ we have $5|(1978^s-1)$, i.e., $1978^s \equiv 3^s \equiv 1 \mod 5$. Since $s|100$, this last congruence implies that $s = 4, 20$, or 100. We now rule out the first two possibilities.

Observe that

$$1978^4 \equiv (-22)^4 \equiv 2^4\cdot 11^4 \equiv (4\cdot 121)^2 \equiv (-16)^2 \equiv 6 \mod 125.$$

This means that $s \neq 4$. Similarly

$$1978^{20} \equiv 1978^4\cdot(1978^4)^4 \equiv 6\cdot 6^4 \equiv 6\cdot 46 \equiv 26 \mod 125.$$

This means that $s \neq 20$ and so $s = 100$. Since s is the smallest positive integer with $1978^s \equiv 1 \mod 125$, we take $n-m = s = 100$ and $m = 3$, i.e., $n = 103, m = 3$, and finally, $m+n = 106$.

539 Example (IMO 1984) Find one pair of positive integers a,b such that:
(i) $ab(a+b)$ is not divisible by 7.
(ii) $(a+b)^7 - a^7 - b^7$ is divisible by 7^7. Justify your answer.

Solution: We first factorise $(a+b)^7 - a^7 - b^7$ as $ab(a+b)(a^2+ab+b^2)^2$. Using the Binomial Theorem we have

$$\begin{aligned}
(a+b)^7 - a^7 - b^7 &= 7(a^6b+ab^6+3(a^5b^2+a^2b^5)+5(a^4b^3+a^3b^4)) \\
&= 7ab(a^5+b^5+3ab(a^3+b^3)+5(a^2b^2)(a+b)) \\
&= 7ab(a+b)(a^4+b^4-a^3b-ab^3+a^2b^2 \\
&\qquad +3ab(a^2-ab+b^2)+5ab) \\
&= 7ab(a+b)(a^4+b^4+2(a^3b+ab^3)+3a^2b^2) \\
&= 7ab(a+b)(a^2+ab+b^2)^2.
\end{aligned}$$

The given hypotheses can be thus simplified to

$$(\text{i})' \ ab(a+b) \text{ is not divisible by } 7,$$

$$(\text{ii})' \ a^2+ab+b^2 \text{ is divisible by } 7^3.$$

As $(a+b)^2 > a^2+ab+b^2 \geq 7^3$, we obtain $a+b \geq 19$. Using trial and error, we find that $a = 1, b = 18$ give an answer, as $1^2+1\cdot 18+18^2 = 343 = 7^3$.

Let us look for more solutions by means of Euler's Theorem. As $a^3-b^3=(a-b)(a^2+ab+b^2)$, (ii)' is implied by

$$(\mathrm{ii})'' \left\{ \begin{array}{ll} a^3 \equiv b^3 & \mod 7^3 \\ a \not\equiv b & \mod 7. \end{array} \right.$$

Now $\phi(7^3)=(7-1)7^2=3\cdot 98$, and so if x is not divisible by 7 we have $(x^{98})^3 \equiv 1 \mod 7^3$, which gives the first part of (ii)'. We must verify now the conditions of non-divisibility. For example, letting $x=2$ we see that $2^{98} \equiv 4 \mod 7$. Thus letting $a=2^{98}, b=1$. Letting $x=3$ we find that $3^{98} \equiv 324 \mod 7^3$. We leave to the reader to verify that $a=324, b=1$ is another solution.

Practice

540 Problem Show that for all natural numbers s, there is an integer n divisible by s, such that the sum of the digits of n equals s.

541 Problem Prove that $504|n^9-n^3$.

542 Problem Prove that for odd integer $n>0$, $n|(2^{n!}-1)$.

543 Problem Let $p \not| 10$ be a prime. Prove that p divides infinitely many numbers of the form

$$11\ldots 11.$$

544 Problem Find all natural numbers n that divide

$$1^n+2^n+\cdots+(n-1)^n.$$

545 Problem Let $(m,n)=1$. Prove that

$$m^{\phi(n)}+n^{\phi(n)} \equiv 1 \mod mn.$$

546 Problem Find the last two digits of a_{1001} if $a_1=7, a_n=7^{a_{n-1}}$.

547 Problem Find the remainder of

$$10^{10}+10^{10^2}+\cdots+10^{10^{10}}$$

upon division by 7.

548 Problem Prove that for every natural number n there exists some power of 2 whose final n digits are all ones and twos.

549 Problem (USAMO 1982) Prove that there exists a positive integer k such that $k\cdot 2^n+1$ is composite for every positive integer n.

550 Problem (Putnam 1985) Describe the sequence $a_1=3, a_n=3^{a_{n-1}} \mod 100$ for large n.

Chapter 8

Scales of Notation

8.1 The Decimal Scale

As we all know, any natural number n can be written in the form

$$n = a_0 10^k + a_1 10^{k-1} + \cdots + a_{k-1} 10 + a_k,$$

where $1 \leq a_0 \leq 9, 0 \leq a_j \leq 9, j \geq 1$. For example, $65789 = 6 \cdot 10^4 + 5 \cdot 10^3 + 7 \cdot 10^2 + 8 \cdot 10 + 9$.

551 Example Find all whole numbers which begin with the digit 6 and decrease 25 times when this digit is deleted.

Solution: Let the number sought have $n+1$ digits. Then this number can be written as $6 \cdot 10^n + y$, where y is a number with n digits (it may begin with one or several zeroes). The condition of the problem stipulates that

$$6 \cdot 10^n + y = 25 \cdot y$$

whence

$$y = \frac{6 \cdot 10^n}{24}.$$

From this we gather that $n \geq 2$ (otherwise, $6 \cdot 10^n$ would not be divisible by 24). For $n \geq 2, y = 25 \cdot 10^{k-2}$, that is, y has the form $250 \cdots 0 (n-2 \text{ zeroes})$. We conclude that all the numbers sought have the form $625 \underbrace{0 \ldots 0}_{n-2 \text{ zeroes}}$.

552 Example (IMO 1968) Find all natural numbers x such that the product of their digits (in decimal notation) equals $x^2 - 10x - 22$.

Solution: Let x have the form

$$x = a_0 + a_1 10 + a_2 10^2 + \cdots + a_{n-1} 10^{n-1}, \quad a_k \leq 9, a_{n-1} \neq 0.$$

Let $P(x)$ be the product of the digits of x, $P(x) = x^2 - 10x - 22$. Now, $P(x) = a_0 a_1 \cdots a_{n-1} \leq 9^{n-1} a_{n-1} < 10^{n-1} a_{n-1} \leq x$ (strict inequality occurs when x has more than one digit). So $x^2 - 10x - 22 < x$, and we deduce that $x < 13$, whence x has either one digit or $x = 10, 11, 13$. If x had one digit, then $a_0 = x^2 - 10x - 22$, but this equation has no integral solutions. If $x = 10, P(x) = 0$, but $x^2 - 10x - 22 \neq 0$. If $x = 11, P(x) = 1$, but $x^2 - 10x - 22 \neq 1$. If $x = 12, P(x) = 2$ and $x^2 - 10x - 22 = 2$. Therefore, $x = 12$ is the only solution.

553 Example A whole number decreases an integral number of times when its last digit is deleted. Find all such numbers.

Solution: Let $0 \leq y \leq 9$, and $10x + y = mx, m$ and x natural numbers. This requires $10 + y/x = m$, an integer. We must have $x|y$. If $y = 0$, any natural number x will do, and we obtain the multiples of 10. If $y = 1, x = 1$, and we obtain 11. If $y = 2, x = 1$ or $x = 2$ and we obtain 12 and 22. Continuing in this fashion, the sought numbers are: the multiples of $10, 11$, $12, 13$, $14, 15$, $16, 17$, $18, 19$, $22, 24$, $26, 28$, $33, 36$, $39, 44$, $48, 55$, $66, 77, 88$, and 99.

554 Example Let A be a positive integer, and A' be a number written with the aid of the same digits with are arranged in some other order. Prove that if $A + A' = 10^{10}$, then A is divisible by 10.

Solution: Clearly A and A' must have ten digits. Let $A = a_{10}a_9 \ldots a_1$ be the consecutive digits of A and $A' = a'_{10}a'_9 \ldots a'_1$. Now, $A + A' = 10^{10}$ if and only if there is a $j, 0 \leq j \leq 9$ for which $a_1 + a'_1 = a_2 + a'_2 = \cdots = a_j + a'_j = 0, a_{j+1} + a'_{j+1} = 10, a_{j+2} + a'_{j+2} = a_{j+3} + a'_{j+3} = \cdots = a_{10} + a'_{10} = 9$. Notice that $j = 0$ implies that there are no sums of the form $a_{j+k} + a'_{j+k}, k \geq 2$, and $j = 9$ implies that there are no sums of the form $a_l + a'_l, 1 \leq l \leq j$. On adding all these sums, we gather

$$a_1 + a'_1 + a_2 + a'_2 + \cdots + a_{10} + a'_{10} = 10 + 9(9 - j).$$

Since the a'_s are a permutation of the a_s, we see that the sinistral side of the above equality is the even number $2(a_1 + a_2 + \cdots + a_{10})$. This implies that j must be odd. But this implies that $a_1 + a'_1 = 0$, which gives the result.

555 Example (AIME 1994) Given a positive integer n, let $p(n)$ be the product of the non-zero digits of n. (If n has only one digit, then $p(n)$ is equal to that digit.) Let

$$S = p(1) + p(2) + \cdots + p(999).$$

What is the largest prime factor of S?

Solution: Observe that *non-zero* digits are the ones that matter. So, for example, the numbers 180, 108, 118, 810, 800, and 811 have the same value $p(n)$.

We obtain all the three digit numbers from 001 to 999 by expanding the product

$$(0 + 1 + 2 + \cdots + 9)^3 - 0,$$

where we subtracted a 0 in order to eliminate 000. Thus

$$(0 + 1 + 2 \cdots + 9)^3 - 0 = 001 + 002 + \cdots + 999.$$

In order to obtain $p(n)$ for a particular number, we just have to substitute the (possible) zeroes in the decimal representation, by 1's, and so

$$p(1) + p(2) + \cdots + p(n) = 111 + 112 + \cdots + 999 = (1 + 1 + 2 + \cdots + 9)^3 - 1,$$

which equals $46^3 - 1$. (In the last sum, 111 is repeated various times, once for 001, once for 011, once for 100, once for 101, once for 110, etc.) As $46^3 - 1 = 3^3 \cdot 5 \cdot 7 \cdot 103$, the number required is 103.

556 Example (AIME 1992) Let S be the set of all rational numbers $r, 0 < r < 1$, that have a repeating decimal expansion of the form

$$0.abcabcabc\ldots = 0.\overline{abc},$$

where the digits a, b, c are not necessarily distinct. To write the elements of S as fractions in lowest terms, how many different numerators are required?

Solution: Observe that $0.abcabcabc\ldots = \dfrac{abc}{999}$, and $999 = 3^3 \cdot 37$. If abc is neither divisible by 3 nor 37, the fraction is already in lowest terms. By the Inclusion-Exclusion Principle, there are

$$999 - (999/3 + 999/37) + 999/3 \cdot 37 = 648$$

such numbers. Also, fractions of the form $s/37$, where $3|s, 37 \not| s$ are in S. There are 12 fractions of this kind. (Observe that we do not consider fractions of the form $l/3^t, 37|s, 3 \not| l$, because fractions of this form are greater than 1, and thus not in S.)

The total number of distinct numerators in the set of reduced fractions is thus $640 + 12 = 660$.

557 Example (Putnam 1956) Prove that every positive integer has a multiple whose decimal representation involves all 10 digits.

Solution: Let n be an arbitrary positive integer with k digits. Let $m = 123456780 \cdot 10^{k+1}$. Then all of the n consecutive integers $m+1, m+2, \ldots m+n$ begin with 1234567890 and one of them is divisible by n.

558 Example (Putnam 1987) The sequence of digits

$$123456789101112131415161718192021 22 \ldots$$

is obtained by writing the positive integers in order. If the 10^n digit of this sequence occurs in the part in which the m-digit numbers are placed, define $f(n)$ to be m. For example $f(2) = 2$, because the hundredth digit enters the sequence in the placement of the two-digit integer 55. Find, with proof, $f(1987)$.

Solution: There are $9 \cdot 10^{j-1}$ j-digit positive integers. The total number of digits in numbers with at most r digits is $g(r) = \sum_{j=1}^{r} j \cdot 9 \cdot 10^{r-1} = r10^r - \frac{10^r - 1}{9}$. As $0 < \frac{10^r - 1}{9} < 10^r$, we get $(r-1)10^r < g(r) < r10^r$. Thus $g(1983) < 1983 \cdot 10^{1983} < 10^4 \cdot 10^{1983} = 10^{1987}$ and $g(1984) > 1983 \cdot 10^{1984} > 10^3 \cdot 10^{1984}$. Therefore $f(1987) = 1984$.

Practice

559 Problem Prove that there is no whole number which decreases 35 times when its initial digit is deleted.

560 Problem A whole number is equal to the arithmetic mean of all the numbers obtained from the given number with the aid of all possible permutations of its digits. Find all whole numbers with that property.

561 Problem (AIME 1989) Suppose that n is a positive integer and d is a single digit in base-ten. Find n if

$$\frac{n}{810} = 0.d25d25d25d25\ldots.$$

562 Problem (AIME 1992) For how many pairs of consecutive integers in

$$\{1000, 1001, \ldots, 2000\}$$

is no carrying required when the two integers are added?

563 Problem Let m be a seventeen-digit positive integer and let N be number obtained from m by writing the same digits in reversed order. Prove that at least one digit in the decimal representation of the number $M+N$ is even.

564 Problem Given that

$$e = 2 + \frac{1}{2!} + \frac{1}{3!} + \frac{1}{4!} + \cdots,$$

prove that e is irrational.

565 Problem Let t be a positive real number. Prove that there is a positive integer n such that the decimal expansion of nt contains a 7.

566 Problem (AIME 1988) Find the smallest positive integer whose cube ends in 888.

567 Problem (AIME 1987) An ordered pair (m, n) of nonnegative integers is called *simple* if the addition $m+n$ requires no carrying. Find the number of simple ordered pairs of nonnegative integers that sum 1492.

568 Problem (AIME 1986) In the parlor game, the “magician” asks one of the participants to think of a three-digit number abc, where a, b, c represent the digits of the number in the order indicated. The magician asks his victim to form the numbers acb, bac, cab and cba, to add the number and to reveal their sum N. If told the value of N, the magician can identity abc. Play the magician and determine abc if $N = 319$.

569 Problem The integer n is the smallest multiple of 15 such that every digit of n is either 0 or 8. Compute $n/15$.

570 Problem (AIME 1988) For any positive integer k, let $f_1(k)$ denote the square of the sums of the digits of k. For $n \geq 2$, let $f_n(k) = f_1(f_{n-1}(k))$. Find $f_{1988}(11)$.

571 Problem (IMO 1969) Determine all three-digit numbers N that are divisible by 11 and such that $N/11$ equals the sum of the squares of the digits of N.

572 Problem (IMO 1962) Find the smallest natural number having last digit is 6 and if this 6 is erased and put in front of the other digits, the resulting number is four times as large as the original number.

573 Problem

1. Show that *Champernowne's number*

   $$\chi = 0.123456789101112131415161718192021\ldots$$

   is irrational.

2. Let $r \in \mathbb{Q}$ and let $\varepsilon > 0$ be given. Prove that there exists a positive integer n such that

   $$|10^n\chi - r| < \varepsilon.$$

574 Problem A *Liouville number* is a real number x such that for every positive k there exist integers a and $b \geq 2$, such that

$$|x - a/b| < b^{-k}.$$

Prove or disprove that π is the sum of two Liouville numbers.

575 Problem Given that

$$1/49 = 0.020408163265306122448979591836734693877551,$$

find the last thousand digits of

$$1 + 50 + 50^2 + \cdots + 50^{999}.$$

8.2 Non-decimal Scales

The fact that most people have ten fingers has fixed our scale of notation to the decimal. Given any positive integer $r > 1$, we can, however, express any number in base r.

576 Example Express the decimal number 5213 in base-seven.

Solution: Observe that $5213 < 7^5$. We thus want to find $0 \leq a_0, \ldots, a_4 \leq 6, a_4 \neq 0$, such that

$$5213 = a_4 7^4 + a_3 7^3 + a_2 7^2 + a_1 7 + a_0.$$

Now, divide by 7^4 to obtain

$$2 + \text{proper fraction} = a_4 + \text{proper fraction}.$$

Since a_4 is an integer, it must be the case that $a_4 = 2$. Thus $5213 - 2 \cdot 7^4 = 411 = a_3 7^3 + a_2 7^2 + a_1 7 + a_0$. Dividing 411 by 7^3 we obtain

$$1 + \text{proper fraction} = a_3 + \text{proper fraction}.$$

Thus $a_3 = 1$. Continuing in this way we deduce that $5213 = 21125_7$.

577 Example Express the decimal number $13/16$ in base-six.

Solution: Write

$$\frac{13}{16} = \frac{a_1}{6} + \frac{a_2}{6^2} + \frac{a_3}{6^3} + \ldots.$$

Multiply by 6 to obtain

$$4 + \text{proper fraction} = a_1 + \text{proper fraction}.$$

Thus $a_1 = 4$. Hence $13/16 - 4/6 = 7/48 = \frac{a_2}{6^2} + \frac{a_3}{6^3} + \ldots$. Multiply by 6^2 to obtain

$$5 + \text{proper fraction} = a_2 + \text{proper fraction}.$$

We gather that $a_2 = 5$. Continuing in this fashion, we deduce that $13/16 = .4513_6$.

578 Example Prove that 4.41 is a perfect square in any scale of notation.

Solution: If 4.41 is in scale r, then

$$4.41 = 4 + \frac{4}{r} + \frac{1}{r^2} = \left(2 + \frac{1}{r}\right)^2.$$

579 Example Let $\lfloor\lfloor x\rfloor\rfloor$ denote the greatest integer less than or equal to x. Does the equation

$$\lfloor\lfloor x\rfloor\rfloor+\lfloor\lfloor 2x\rfloor\rfloor+\lfloor\lfloor 4x\rfloor\rfloor+\lfloor\lfloor 8x\rfloor\rfloor+\lfloor\lfloor 16x\rfloor\rfloor+\lfloor\lfloor 32x\rfloor\rfloor=12345$$

have a solution?

Solution: We show that there is no such x. Recall that $\lfloor\lfloor x\rfloor\rfloor$ satisfies the inequalities $x-1<\lfloor\lfloor x\rfloor\rfloor\leq x$. Thus

$$\begin{aligned}x-1+2x-1+4x-1+\cdots+32x-1 &< \lfloor\lfloor x\rfloor\rfloor+\lfloor\lfloor 2x\rfloor\rfloor+\lfloor\lfloor 4x\rfloor\rfloor+\lfloor\lfloor 8x\rfloor\rfloor\\ &\quad +\lfloor\lfloor 16x\rfloor\rfloor+\lfloor\lfloor 32x\rfloor\rfloor\\ &\leq x+2x+4x+\cdots+32x.\end{aligned}$$

From this we see that $63x-6<12345\leq 63x$. Hence $195<x<196$.

Write then x in base-two:

$$x=195+\frac{a_1}{2}+\frac{a_2}{2^2}+\frac{a_3}{2^3}+\ldots,$$

with $a_k=0$ or 1. Then

$$\begin{aligned}\lfloor\lfloor 2x\rfloor\rfloor &= 2\cdot 195+a_1,\\ \lfloor\lfloor 4x\rfloor\rfloor &= 4\cdot 195+2a_1+a_2,\\ \lfloor\lfloor 8x\rfloor\rfloor &= 8\cdot 195+4a_1+2a_2+a_3,\\ \lfloor\lfloor 16x\rfloor\rfloor &= 16\cdot 195+8a_1+4a_2+2a_3+a_4,\\ \lfloor\lfloor 32x\rfloor\rfloor &= 32\cdot 195+16a_1+8a_2+4a_3+2a_4+a_5.\end{aligned}$$

Adding we find that $\lfloor\lfloor x\rfloor\rfloor+\lfloor\lfloor 2x\rfloor\rfloor+\lfloor\lfloor 4x\rfloor\rfloor+\lfloor\lfloor 8x\rfloor\rfloor+\lfloor\lfloor 16x\rfloor\rfloor+\lfloor\lfloor 32x\rfloor\rfloor=63\cdot 195+31a_1+15a_2+7a_3+3a_4+a_5$, i.e. $31a_1+15a_2+7a_3+3a_4+a_5=60$. This cannot be because $31a_1+15a_2+7a_3+3a_4+a_5\leq 31+15+7+3+1=57<60$.

580 Example (AHSME 1993) 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 $x_0=x_5$?

Solution: Write x_0 in base-two,

$$x_0=\sum_{k=1}^{\infty}\frac{a_n}{2^n}\quad a_n=0\text{ or }1.$$

The algorithm given just moves the binary point one unit to the right. For x_0 to equal x_5 we need $0.a_1a_2a_3a_4a_5a_6a_7\ldots=0.a_6a_7a_8a_9a_{10}a_{11}a_{12}\ldots$. This will happen if and only if x_0 has a repeating expansion with $a_1a_2a_3a_4a_5$ as the repeating block . There are $2^5=32$ such blocks. But if $a_1=a_2=\cdots=a_5=1$, then $x_0=1$, which is outside $[0,1)$. The total number of values for which $x_0=x_5$ is thus $32-1=31$.

581 Example (AIME 1986) The increasing sequence

$$1,3,4,9,10,12,13,\ldots$$

consists of all those positive integers which are powers of 3 or sums distinct powers of 3. Find the hundredth term of the sequence.

Solution: If the terms of the sequence are written in base-3, they comprise the positive integers which do not contain the digit 2. Thus, the terms of the sequence in ascending order are thus

$$1,10,11,100,101,110,111,\ldots.$$

In the *binary* scale, these numbers are, of course, 1, 2, 3, ... To obtain the 100-th term of the sequence we just write 100 in binary $100=1100100_2$ and translate this into ternary: $1100100_3=3^6+3^5+3^2=981$.

Practice

582 Problem (Putnam, 1987) For each positive integer n, let $\alpha(n)$ be the number of zeroes in the base-three representation of n. For which positive real numbers x does the series

$$\sum_{n=1}^{\infty} \frac{x^{\alpha(n)}}{n^3}$$

converge?

583 Problem Prove that for $x \in \mathbb{R}, x \geq 0$, one has

$$\sum_{n=1}^{\infty} \frac{(-1)^{\llbracket 2^n x \rrbracket}}{2^n} = 1 - 2(x - \llbracket x \rrbracket).$$

584 Problem (Putnam, 1981) Let $E(n)$ denote the largest k such that 5^k is an integral divisor of $1^1 2^2 3^3 \cdots n^n$. Calculate

$$\lim_{n \to \infty} \frac{E(n)}{n^2}.$$

585 Problem (AHSME, 1982) The base-eight representation of a perfect square is $ab3c$ with $a \neq 0$. Find the value of c.

586 Problem (Putnam, 1977) An ordered triple of (x_1, x_2, x_3) of positive irrational numbers with $x_1 + x_2 + x_3 = 1$ is called balanced if $x_n < 1/2$ for all $1 \leq n \leq 3$. If a triple is not balanced, say $x_j > 1/2$, one performs the following "balancing act":

$$B(x_1, x_2, x_3) = (x_1', x_2', x_3'),$$

where $x_i' = 2x_i$ if $x_i \neq x_j$ and $x_j' = 2x_j - 1$. If the new triple is not balanced, one performs the balancing act on it. Does continuation of this process always lead to a balanced triple after a finite number of performances of the balancing act?

587 Problem Let C denote the class of positive integers which, when written in base-three, do not require the digit 2. Show that no three integers in C are in arithmetic progression.

588 Problem Let $B(n)$ be the number of 1's in the base-two expansion of n. For example, $B(6) = B(110_2) = 2, B(15) = B(1111_2) = 4$.

1. (PUTNAM 1981) Is

$$\exp\left(\sum_{n=1}^{\infty} \frac{B(n)}{n^2 + n}\right)$$

a rational number?

2. (PUTNAM 1984) Express

$$\sum_{n=0}^{2^m - 1} (-1)^{B(n)} n^m$$

in the form $(-1)^m a^{f(m)} (g(m))!$ where a is an integer and f, g are polynomials.

589 Problem What is the largest integer that I should be permitted to choose so that you may determine my number in twenty "yes" or "no" questions?

8.3 A theorem of Kummer

We first establish the following theorem.

590 Theorem (Legendre) Let p be a prime and let $n = a_0 p^k + a_1 p^{k-1} + \cdots + a_{k-1} p + a_k$ be the base-p expansion of n. The exact power m of a prime p dividing $n!$ is given by

$$m = \frac{n - (a_0 + a_1 + \cdots + a_k)}{p - 1}.$$

Proof: *By De Polignac's Formula*

$$m = \sum_{k=1}^{\infty} \llbracket \frac{n}{p^k} \rrbracket.$$

Now, $\llbracket n/p \rrbracket = a_0p^{k-1} + a_1p^{k-2} + \cdots a_{k-2}p + a_{k-1}, \llbracket n/p^2 \rrbracket = a_0p^{k-2} + a_1p^{k-3} + \cdots + a_{k-2}, \ldots, \llbracket n/p^k \rrbracket = a_0.$ *Thus*

$$\begin{aligned}\sum_{k=1}^{\infty} \llbracket n/p^k \rrbracket &= a_0(1+p+p^2+\cdots+p^{k-1}) + a_1(1+p+p^2+\cdots+p^{k-2}) + \\ &\quad \cdots + a_{k-1}(1+p) + a_k \\ &= a_0\frac{p^k-1}{p-1} + a_1\frac{p^{k-1}-1}{p-1} + \cdots + a_{k-1}\frac{p^2-1}{p-1} + a_k\frac{p-1}{p-1} \\ &= \frac{a_0p^k + a_1p^{k-1} + \cdots + a_k - (a_0+a_1+\cdots+a_k)}{p-1} \\ &= \frac{n-(a_0+a_1+\cdots+a_k)}{p-1},\end{aligned}$$

as wanted.❑

591 Theorem (Kummer's Theorem) The exact power of a prime p dividing the binomial coefficient $\binom{a+b}{a}$ is equal to the number of "carry-overs" when performing the addition of a, b written in base p.

Proof: *Let* $a = a_0 + a_1p + \cdots + a_kp^k, b = b_0 + b_1p + \cdots + b_kp^k, 0 \leq a_j, b_j \leq p-1,$ *and* $a_k + b_k > 0$. *Let* $S_a = \sum_{j=0}^{k} a_j, S_b = \sum_{j=0}^{k} b_j$. *Let* $c_j, 0 \leq c_j \leq p-1,$ *and* $\varepsilon_j = 0$ *or 1, be defined as follows:*

$$\begin{aligned}&a_0 + b_0 = \varepsilon_0 p + c_0, \\ &\varepsilon_0 + a_1 + b_1 = \varepsilon_1 p + c_1, \\ &\varepsilon_1 + a_2 + b_2 = \varepsilon_2 p + c_2, \\ &\vdots \\ &\varepsilon_{k-1} + a_k + b_k = \varepsilon_k p + c_k.\end{aligned}$$

Multiplying all these equalities successively by $1, p, p^2, \ldots$ *and adding them:*

$$\begin{aligned}a + b + \varepsilon_0 p + \varepsilon_1 p^2 + \ldots + \varepsilon_{k-1}p^k &= \varepsilon_0 p + \varepsilon_1 p^2 + \ldots + \varepsilon_{k-1}p^k + \varepsilon_k p^{k+1} \\ &\quad + c_0 + c_1 p + \cdots + c_k p^k\end{aligned}.$$

We deduce that $a + b = c_0 + c_1p + \cdots + c_kp^k + \varepsilon_kp^{k+1}$. *By adding all the equalities above, we obtain similarly:*

$$S_a + S_b + (\varepsilon_0 + \varepsilon_1 + \cdots + \varepsilon_{k-1}) = (\varepsilon_0 + \varepsilon_1 + \cdots + \varepsilon_k)p + S_{a+b} - \varepsilon_k.$$

Upon using Legendre's result from above,

$$(p-1)m = (a+b) - S_{a+b} - a + S_a - b + S_b = (p-1)(\varepsilon_0 + \varepsilon_1 + \cdots + \varepsilon_k),$$

which gives the result.❑

Chapter 9

Miscellaneous Problems

592 Example Prove that

$$\sum_{\substack{p\\ p\ \text{prime}}} \frac{1}{p}$$

diverges.

Solution: Let $\mathscr{F}_x$ denote the family consisting of the integer 1 and the positive integers n all whose prime factors are less than or equal to x. By the Unique Factorisation Theorem

$$\prod_{\substack{p\leq x\\ p\ \text{prime}}} \left(1+\frac{1}{p}+\frac{1}{p^2}+\cdots\right) = \sum_{n\in\mathscr{F}_x} \frac{1}{n}. \tag{9.1}$$

Now,

$$\sum_{n\in\mathscr{F}_x} \frac{1}{n} > \sum_{n\leq x} \frac{1}{n}.$$

As the harmonic series diverges, the product on the sinistral side of 2.3.3 diverges as $x \to \infty$. But

$$\prod_{\substack{p\leq x\\ p\ \text{prime}}} \left(1+\frac{1}{p}+\frac{1}{p^2}+\cdots\right) = \sum_{\substack{p\leq x\\ p\ \text{prime}}} \frac{1}{p} + O(1).$$

This finishes the proof.

593 Example Prove that for each positive integer k there exist infinitely many even positive integers which can be written in more than k ways as the sum of two odd primes.

Solution: Let a_k denote the number of ways in which $2k$ can be written as the sum of two odd primes. Assume that $a_k \leq C\ \forall k$ for some positive constant C. Then

$$\left(\sum_{\substack{p>2\\ p\ \text{prime}}} x^p\right)^2 = \sum_{k=2}^{\infty} a_k x^{2k} \leq C\frac{x^4}{1-x^2}.$$

This yields

$$\sum_{\substack{p>2\\ p\ \text{prime}}} x^{p-1} \leq \sqrt{C}\frac{x}{\sqrt{1-x^2}}.$$

Integrating term by term,

$$\sum_{\substack{p>2\\ p \text{ prime}}} \frac{1}{p} \leq \sqrt{C}\int_0^1 \frac{x}{\sqrt{1-x^2}}\,dx = \sqrt{C}.$$

But the leftmost series is divergent, and we obtain a contradiction.

594 Example (IMO 1976) Determine, with proof, the largest number which is the product of positive integers whose sum is 1976.

Solution: Suppose that

$$a_1 + a_2 + \cdots + a_n = 1976;$$

we want to maximise $\prod_{k=1}^{n} a_k$. We shall replace some of the a_k so that the product is enlarged, but the sum remains the same. By the arithmetic mean-geometric mean inequality

$$\left(\prod_{k=1}^{n} a_k\right)^{1/n} \leq \frac{a_1 + a_2 + \cdots + a_n}{n},$$

with equality if and only if $a_1 = a_2 = \cdots = a_n$. Thus we want to make the a_k as equal as possible.

If we have an $a_k \geq 4$, we replace it by two numbers $2, a_k - 2$. Then the sum is not affected, but $2(a_k - 2) \geq a_k$, since we are assuming $a_k \geq 4$. Therefore, in order to maximise the product, we must take $a_k = 2$ or $a_k = 3$. We must take as many 2's and 3's as possible.

Now, $2+2+2 = 3+3$, but $2^3 < 3^2$, thus we should take no more than two 2's. Since $1976 = 3 \cdot 658 + 2$, the largest possible product is $2 \cdot 3^{658}$.

595 Example (USAMO 1983) Consider an *open* interval of length $1/n$ on the real line, where n is a positive integer. Prove that the number of irreducible fractions $a/b, 1 \leq b \leq n$, contained in the given interval is at most $(n+1)/2$.

Solution: Divide the rational numbers in $(x, x+1/n)$ into two sets: $\{\frac{s_k}{t_k}\}, k = 1, 2, \ldots, r$, with denominators $1 \leq t_k \leq n/2$ and those $u_k/v_k, k = 1, 2, \ldots, s$ with denominators $n/2 < v_k \leq n$, where all these fractions are in reduced form. Now, for every t_k there are integers c_k such that $n/2 \leq c_k t_k \leq n$. Define $u_{s+k} = c_k s_k, v_{s+k} = c_k t_k, y_{k+r} = u_{k+r}/v_{k+r}$. No two of the $y_l, 1 \leq l \leq r+s$ are equal, for otherwise $y_j = y_k$ would yield

$$|u_k/v_k - u_i/v_i| \geq 1/v_i \geq 1/n,$$

which contradicts that the open interval is of length $1/n$. Hence the number of distinct rationals is $r + s \leq n - \lfloor\!\lfloor n/2 \rfloor\!\rfloor \leq (n+1)/2$.

Aliter: Suppose to the contrary that we have at least $\lfloor\!\lfloor (n+1)/2 \rfloor\!\rfloor + 1 = a$ fractions. Let $s_k, t_k, 1 \leq k \leq a$ be the set of numerators and denominators. The set of denominators is a subset of

$$\{1, 2, \ldots, 2(a-1)\}.$$

By the Pigeonhole Principle, $t_i | t_k$ for some i, k, say $t_k = m t_i$. But then

$$|s_k/t_k - s_i/t_i| = |m s_i - s_k|/t_k \geq 1/n,$$

contradicting the hypothesis that the open interval is of length $1/n$.

596 Example Let

$$Q_{r,s} = \frac{(rs)!}{r!s!}.$$

Show that $Q_{r,ps} \equiv Q_{r,s} \mod p$, where p is a prime

Solution: As

$$Q_{r,s} = \prod_{j=1}^{r} \binom{js-1}{s-1}$$

and

$$Q_{r,ps} = \prod_{j=1}^{r} \binom{jps-1}{ps-1},$$

it follows from

$$(1+x)^{jps-1} \equiv (1+x^p)^{js-1}(1+x)^{p-1} \mod p$$

that

$$\binom{jps-1}{ps-1} \equiv \binom{js-1}{s-1} \mod p,$$

whence the result.

Practice

597 Problem Find a four-digit number which is a perfect square such that its first two digits are equal to each other and its last two digits are equal to each other.

598 Problem Find all integral solutions of the equation

$$\sum_{k=1}^{x} k! = y^2.$$

599 Problem Find all integral solutions of the equation

$$\sum_{k=1}^{x} k! = y^z.$$

600 Problem (USAMO 1985) Determine whether there are any positive integral solutions to the simultaneous equations

$$x_1^2 + x_2^2 + \cdots + x_{1985}^2 = y^3,$$

$$x_1^3 + x_2^3 + \cdots + x_{1985}^3 = z^2$$

with distinct integers $x_1, x_2, \ldots, x_{1985}$.

601 Problem Show that the Diophantine equation

$$\frac{1}{a_1} + \frac{1}{a_2} + \ldots + \frac{1}{a_{n-1}} + \frac{1}{a_n} + \frac{1}{a_1 a_2 \cdots a_n}$$

has at least one solution for every $n \in \mathbb{N}$.

602 Problem (AIME 1987) Find the largest possible value of k for which 3^{11} is expressible as the sum of k consecutive positive integers.

603 Problem (AIME 1987) Let $\mathscr{M}$ be the smallest positive integer whose cube is of the form $n+r$, where $n \in \mathbb{N}, 0 < r < 1/1000$. Find n.

604 Problem Determine two-parameter solutions for the "almost" Fermat Diophantine equations

$$x^{n-1} + y^{n-1} = z^n,$$

$$x^{n+1} + y^{n+1} = z^n,$$

$$x^{n+1} + y^{n-1} = z^n.$$

605 Problem (AIME 1984) What is the largest even integer which cannot be written as the sum of two odd composite numbers?

606 Problem Prove that are infinitely many nonnegative integers n which cannot be written as $n = x^2 + y^3 + z^6$ for nonnegative integers x, y, z.

607 Problem Find the integral solutions of

$$x^2 + x = y^4 + y^3 + y^2 + y.$$

608 Problem Show that there are infinitely many integers x, y such that

$$3x^2 - 7y^2 = -1.$$

609 Problem Prove that

1. $$a^3 + b^3 + c^3 - 3abc = (a+b+c)(a^2 + b^2 + c^2 - ab - bc - ca).$$

2. Find integers a, b, c such that $1987 = a^3 + b^3 + c^3 - 3abc$.

3. Find polynomials P,Q,R in x,y,z such that

$$P^3+Q^3+R^3-3PQR=(x^3+y^3+z^3-3xyz)^2$$

4. Can you find integers a,b,c with $1987^2=a^3+b^3+c^3-3abc$?

610 Problem Find all integers n such that n^4+n+7 is a perfect square.

611 Problem Prove that 1991^{1991} is not the sum of two perfect squares.

612 Problem Find infinitely many integers $x>1, y>1, z>1$ such that

$$x!y!=z!.$$

613 Problem Find all positive integers with

$$m^n-n^m=1.$$

614 Problem Find all integers with

$$x^4-2y^2=1.$$

615 Problem Prove that for every positive integer k there exists a sequence of k consecutive positive integers none of which can be represented as the sum of two squares.

616 Problem (IMO 1977) In a finite sequence of real numbers, the sum of any seven successive terms is negative, and the sum of any eleven successive terms is positive. Determine the maximum number of terms in the sequence.

617 Problem Determine an infinite series of terms such that each term of the series is a perfect square and the sum of the series at any point is also a perfect square.

618 Problem Prove that any positive rational integer can be expressed as a finite sum of distinct terms of the harmonic series, $1, 1/2, 1/3, \ldots$.

619 Problem (Wostenholme's Theorem) Let $p>3$ be a prime. If

$$\frac{a}{b}=1+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{p-1},$$

then $p^2|a$.

620 Problem Prove that the number of odd binomial coefficients in any row of Pascal's Triangle is a power of 2.

621 Problem Prove that the coefficients of a binomial expansion are odd if and only if n is of the form 2^k-1.

622 Problem Let the numbers c_i be defined by the power series identity

$$(1+x+x^2+\cdots+x^{p-1})/(1-x)^{p-1}:=1+c_1x+c_2x^2+\cdots.$$

Show that $c_i \equiv 0 \mod p$ for all $i \geq 1$.

623 Problem Let p be a prime. Show that

$$\binom{p-1}{k} \equiv (-1)^k \mod p$$

for all $0 \leq k \leq p-1$.

624 Problem (Putnam 1977) Let p be a prime and let $a \geq b > 0$ be integers. Prove that

$$\binom{pa}{pb} \equiv \binom{a}{b} \mod p.$$

625 Problem Demonstrate that for a prime p and $k \in \mathbb{N}$,

$$\binom{p^k}{a} \equiv 0 \mod p,$$

for $0<a<p^k$.

626 Problem Let p be a prime and let $k, a \in \mathbb{N}, 0 \leq a \leq p^k-1$. Demonstrate that

$$\binom{p^k-1}{a} \equiv (-1)^a \mod p.$$