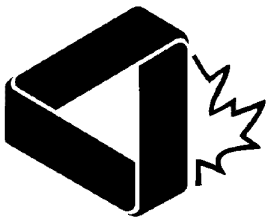
A Taste Of Mathematics



Aime–T–On les Mathématiques

Volume / Tome X
MODULAR ARITHMETIC

Naoki Sato

"Art of Problem Solving Inc."

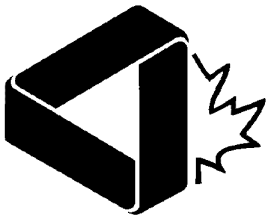
The ATOM series

The booklets in the series, **A Taste of Mathematics**, are published by the Canadian Mathematical Society (CMS). They are designed as enrichment materials for high school students with an interest in and aptitude for mathematics. Some booklets in the series will also cover the materials useful for mathematical competitions at national and international levels.

La collection ATOM

Publiés par la Société mathématique du Canada (SMC), les livrets de la collection Aime-t-on les mathématiques (ATOM) sont destinés au perfectionnement des étudiants du cycle secondaire qui manifestent un intérêt et des aptitudes pour les mathématiques. Certains livrets de la collection ATOM servent également de matériel de préparation aux concours de mathématiques sur l'échiquier national et international.

A Taste Of Mathematics



Aime–T–On les Mathématiques

Volume / Tome X
MODULAR ARITHMETIC

Naoki Sato

"Art of Problem Solving Inc."

Published by the Canadian Mathematical Society, Ottawa, Ontario
and produced by the CMS ATOM Office, St. John's, NL, Canada

Publié par la Société mathématique du Canada, Ottawa (Ontario)
et produit par le Bureau d'ATOM de la SMC, St. John's, NL, Canada

Printed in Canada by / imprimé au Canada par
Thistle Printing Limited

ISBN 978-0-919558-19-9

Table of Contents

About the author

Naoki Sato joined Art of Problem Solving Inc. in San Diego in 2005. He won first place in the 1993 Canadian Mathematical Olympiad, and represented Canada at the 1992 and 1993 International Mathematical Olympiads, winning a bronze and silver medal, respectively. He has also served as deputy leader for the Canadian IMO team in 1997, 2002, and 2006. Naoki earned a Bachelor's in mathematics at the University of Toronto, and a Master's in mathematics at Yale University. He is originally from Toronto, Canada.

"Art of Problem Solving Inc." is a WEB based resource for students looking for a greater challenge in mathematical problems.
See http://www.artofproblemsolving.com/

Preface

> "Mathematics is the queen of the sciences, and arithmetic the queen of mathematics." –Carl Friedrich Gauss

Number theory can be described as the study of the properties of integers. To give you an idea, here are some examples of the problems we will be looking at:

- When $n = 7^{1989}$ is expressed as an integer, what are the last two digits in n?
- Show that $n^5 - n$ is divisible by 5 for all integers n.
- Show that there are an infinite number of primes of the form $4k + 3$.
- What are all integer solutions to the equation $3x - 7y = 2$?
- A number is called **triangular** if it can be expressed as the sum $1+2+\cdots+n$ for some positive integer n. For example, 36 is triangular since $36 = 1 + 2 + \cdots + 8$, and it is also square since $36 = 6^2$. Prove that there are infinitely many numbers that are both triangular and square.

We assume that readers are already familiar with basic number theory concepts, such as divisibility and greatest common divisor, but this is not a strict prerequisite – the keen student can begin right away. Our main goal is to introduce readers to further concepts in number theory, and then show how they can be applied to solve problems. Thus, this booklet is meant to serve more as a problem-solving manual rather than a formal textbook, and proofs of theorems are sometimes replaced by well-chosen examples, which I hope will be more enlightening. However, all solutions are worked out in detail, as they would have to be on a written test. Readers who are interested in finding out more about number theory or problem solving are encouraged to consult the references at the back.

Like most pursuits, mathematics requires active participation, rather than passive spectating, to learn and appreciate the subject. What this means is that you must actually attempt to solve the problems given in this booklet, rather than go straight to the solutions.

For this purpose, problems are given at the end of each chapter, so set aside some time and try to solve them. If you get stuck, then move on to another problem, or come back to it later. A flash of inspiration may hit you when you least expect it, even if you're not consciously thinking about the problem. Only turn to the solutions when you think you've tried everything – otherwise, you deny yourself the pleasure and experience of having solved the problem yourself. Also note that many of the problems allow for different approaches, so you may find a solution that is different from ours which is still correct.

Above all else, we hope you enjoy reading and learning about number theory and the problem-solving process. Thanks to Shawn Godin for some helpful remarks. I welcome any suggestions, and especially corrections. Happy solving!

Naoki Sato
San Diego, California
June, 2009

1 Background

Before we begin, we go over some terminology, notation, and background material that you should be familiar with.

The **integers** refer to the set $\{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$, the **non-negative integers** refer to the set $\{0, 1, 2, 3, \ldots\}$, and the **positive integers** refer to the set $\{1, 2, 3, \ldots\}$. The term "number" will often refer to a positive integer, but the context should make this clear.

A positive integer $n > 1$ is called **prime** if the only factors of n are 1 and n; otherwise, n is called **composite**. If the prime p divides the product ab, then p must divide one of a or b, and only primes have this property. We sometimes write $a|b$ to express the fact that a divides b, so that we can also express the above as: if $p|ab$, then $p|a$ or $p|b$. The Fundamental Theorem of Arithmetic states that any positive integer n can be written in the form

$$n \;=\; p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k},$$

where the p_i are distinct primes and the e_i are positive integers. Furthermore, this form is unique, up to the order of primes.

The **greatest common divisor**, or gcd, of two integers a and b is the greatest integer that divides both a and b, so that, for example, $\gcd(18, 24) = 6$. The **least common multiple**, or lcm, of two integers a and b is the least positive integer that is a multiple of both a and b, so that $\mathrm{lcm}(18, 24) = 72$. If a has the prime factorization $p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$, and b has the prime factorization $p_1^{f_1} p_2^{f_2} \cdots p_k^{f_k}$, then

$$\begin{aligned} \gcd(a, b) &= p_1^{\min\{e_1, f_1\}} p_2^{\min\{e_2, f_2\}} \cdots p_k^{\min\{e_k, f_k\}}, \text{ and} \\ \mathrm{lcm}(a, b) &= p_1^{\max\{e_1, f_1\}} p_2^{\max\{e_2, f_2\}} \cdots p_k^{\max\{e_k, f_k\}}, \end{aligned}$$

thus, as before, $\mathrm{lcm}(24, 18) = \mathrm{lcm}(2^3 \cdot 3, 2 \cdot 3^2) = 2^3 \cdot 3^2 = 72$. Two integers a and b are called **relatively prime** if $\gcd(a, b) = 1$; that is, the only factor a and b have in common is 1.

For all a, b, $\gcd(a, b) \cdot \mathrm{lcm}(a, b) = ab$. The gcd has the following fundamental property: If $d|a$ and $d|b$, then $d|\gcd(a, b)$. Similarly, if $a|m$ and $b|m$, then $\mathrm{lcm}(a, b)|m$. For example, if we know that 18 divides n and 24 divides n, then we can conclude that $\mathrm{lcm}(18, 24) = 72$ divides n, but it is not necessarily true that $18 \cdot 24 = 432$ divides n.

For a positive integer n, $n!$ (read "n factorial") stands for the product $1 \cdot 2 \cdots (n-1) \cdot n$, and $0! = 1$.

Finally, "$\Rightarrow$" stands for "implies that", as in "$x = 2 \Rightarrow x^2 = 4$", and "$\Leftrightarrow$" stands for "if and only if", as in "$x^2 = 4 \Leftrightarrow x = -2$ or $x = 2$".

Problems

1. Find the following: (a) $\gcd(182, 390)$. (b) $\mathrm{lcm}(45, 60)$. (c) $\gcd(n, 7n)$.

2. Find all pairs of positive integers m and n such that $\gcd(m, n) = 3$ and $\text{lcm}(m, n) = 36$.

3. (a) Let n be a positive integer. Show that n and $n+1$ are relatively prime.
   (b) Prove or disprove: If m divides $n(n+1)$, then m divides n or $n+1$.

4. Let a and b be relatively prime integers. Show that if $a|n$ and $b|n$, then $ab|n$.

5. Let x and y be relatively prime integers, such that $x > y$. Find all possible values of $\gcd(x + y, x - y)$.

6. Show that if $a + b = \gcd(a, b) + \text{lcm}(a, b)$, then a divides b or b divides a.

2 A First Step

All mathematics grows and develops by trying to solve interesting and intriguing problems. In this spirit, let us consider the following problem:

Show that $3^{2000} + 4^{2000} + 5^{2000}$ is divisible by 13.

It is simply stated, and simple to understand – we know exactly what "is divisible by" means. However, it is quite another matter to attempt to actually solve the problem, and do what is being asked. Let

$$N \;=\; 3^{2000} + 4^{2000} + 5^{2000},$$

the number in question. The "obvious" approach is to take N and divide it by 13, but writing it out in full is out of the question; it has well over 1000 digits in decimal notation, so that even a calculator would not help. What can we do?

It turns out that there is a powerful tool for solving such problems, reducing them to a few simple calculations, called **modular arithmetic**. However, before we can get to this, we must first lay down some background.

Recall that an integer a is divisible by another integer b if there exists a third integer c such that $a = bc$. In such a case, we can also say that b divides a; in other words, there is no remainder when we divide b into a (or there is a remainder of 0). Division in general, however, does produce a remainder, and we state this fact formally as the division algorithm.

The Division Algorithm. Let a be an integer, and let b be a positive integer. Then there exist unique integers q and r (known as the quotient and remainder, respectively) such that

$$a \;=\; qb + r$$

and $0 \leq r < b$. Furthermore, b divides a if and only if $r = 0$.

For example, if we divide 3 into 20, then we obtain a quotient of 6 and a remainder of 2, because $20 = 6 \cdot 3 + 2$, and $0 \leq 2 < 3$. Thus, the division algorithm is merely a fancy way of saying that when you divide b into a, you always get

some quotient q and a remainder r, with r less than b. Also, as the last bit says, b divides a if and only if the remainder r is 0. Thus, analyzing remainders gives us a way of determining divisibility.

Going back to our original problem, we now have a way of looking at each piece of N, namely 3^{2000}, 4^{2000}, and 5^{2000}, separately. This is why we took our discussion through remainders: we know that 3^{2000} is not divisible by 13, but we can try to determine what remainder it leaves when divided by 13, and the same for 4^{2000} and 5^{2000}.

But we still seem to face the same problem – the number 3^{2000} is still too large to write out or punch into a calculator; the exponent of 2000 is what makes this number intractable. Perhaps we can find an answer by investigating what happens among smaller powers of 3. Thus, for $n \geq 0$, let $a(n)$ be the remainder of 3^n when it is divided by 13. We calculate $a(n)$ for the first few n:

n	0	1	2	3	4	5	6	7	8
3^n	1	3	9	27	81	243	729	2187	6561
$a(n)$	1	3	9	1	3	9	1	3	9

It is apparent that $a(n)$ seems to repeat every three numbers: 1, 3, 9, 1, 3, 9, and so on. Assume for now that this pattern continues indefinitely. Then we can find $a(2000)$ by determining where it lies in this cycle. We see that $a(0) = a(3) = a(6) = 1$, so that, in general, if n is a multiple of 3, then $a(n) = 1$. Since 1998 is a multiple of 3, $a(1998) = 1$. Then $a(1999) = 3$, and $a(2000) = 9$, the remainder we seek. We conclude that 3^{2000} is of the form $13x + 9$, or in other words, $3^{2000} = 13x + 9$ for some integer x.

If we do the same for 4^{2000} and 5^{2000}, then we find that 4^{2000} leaves a remainder of 3 and that 5^{2000} leaves a remainder of 1 upon division by 13, so that $4^{2000} = 13y + 3$ and $5^{2000} = 13z + 1$ for some integers y and z. Therefore,

$$\begin{aligned} N &= 3^{2000} + 4^{2000} + 5^{2000} \\ &= 13x + 9 + 13y + 3 + 13z + 1 \\ &= 13x + 13y + 13z + 13 \;=\; 13(x + y + z + 1), \end{aligned}$$

which shows that N is indeed divisible by 13. Notice that the values of x, y, and z themselves are irrelevant, because they are absorbed into multiples of 13 – it is the remainders that determine the divisibility of N.

This is the idea behind modular arithmetic: we can ignore the multiples, and work only with the remainders. Note that our solution is not really complete, because we assumed that $a(n)$ repeats every third number without proving it. Using modular arithmetic, we will see how we can calculate and prove this, and similar assertions, quickly and easily.

Problems

1. (a) Find all pairs of non-negative integers (x, y) such that $x^2 - y^2 = 84$.

(b) Show that for any non-negative integer a, the equation $x^2 - y^2 = a^3$ always has a solution in non-negative integers.

(c) For which n among 1, 2, ..., 20 does the equation $x^2 - y^2 = n$ have no solutions in non-negative integers x and y?

2. (a) Find the smallest positive integer n such that $360n$ is a perfect square.

(b) Find the smallest positive integer n such that $2n$ is a perfect square and $9n$ is a perfect cube.

3. Show that any odd perfect square can be written in the form $8k+1$, for some integer k. (1992 Euclid Waterloo Contest)

4. A man's age (less than 100) is a multiple of his grandson's age this year, and in fact, the same is true for the next five years. What are their ages?

3 Modular Arithmetic

Let us introduce some notation to make our lives easier, and agree to write $a \equiv b \pmod{m}$ (read "a is **congruent** to b **modulo** m") if a and b leave the same remainder when divided by m. (In such a relation, called a **congruence**, m is called the **modulus**.)

Note that this is the same as saying that a and b differ by a multiple of m, which turns out to be a better working definition. For example, $20-2 = 18 = 6\cdot 3$, so that $20 \equiv 2 \pmod{3}$. As further examples, $-2 \equiv 13 \equiv 3 \pmod{5}$.

In number theory parlance, taking the integers modulo m partitions them into m **congruence classes**, where two integers are in the same class if they are congruent to each other modulo m. For example, in modulo 3, the three classes are $\{\ldots, -6, -3, 0, 3, 6, \ldots\}$, $\{\ldots, -5, -2, 1, 4, 7, \ldots\}$, and $\{\ldots, -7, -4, -1, 2, 5, \ldots\}$, which are the set of integers of the form $3k$, $3k+1$, and $3k+2$, respectively.

However, all this is more than just handy notation: we can add, subtract, and multiply just as in ordinary arithmetic (but not divide – more on that later); hence, the name **modular arithmetic**.

For example, we may wish to find the remainder of a sum, say $115+287+541$, when divided by 5 (which will in turn indicate whether it is divisible by 5). We can calculate the sum first, then take the remainder: $115+287+541 = 943 = 5\cdot 188+3$, so that the remainder is 3. Or, we can take the remainders first, and then calculate the sum: $115 \equiv 0 \pmod{5}$, $287 \equiv 2 \pmod{5}$, and $541 \equiv 1 \pmod{5}$, so that

$$115 + 287 + 541 \;\equiv\; 0 + 2 + 1 \;\equiv\; 3 \pmod{5},$$

and we obtain the same remainder. The difference between the two methods will become more apparent as we tackle more complex problems. Now, for the record, let us state and prove the laws of this new arithmetic.

The Laws of Modular Arithmetic. Let $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$. Then:

(a) $a + c \equiv b + d \pmod{m}$ and $a - c \equiv b - d \pmod{m}$,

(b) $ac \equiv bd \pmod{m}$,

(c) $a^n \equiv b^n \pmod{m}$ for any positive integer n, and

(d) for any polynomial $p(x)$ in x with integer coefficients, $p(a) \equiv p(b) \pmod{m}$.

Proof. Since $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, there exist integers k and l such that $a - b = km$ and $c - d = lm$.

(a) First, $(a + c) - (b + d) = (k + l)m$, so that $(a + c) - (b + d)$ is divisible by m, and $a + c \equiv b + d \pmod{m}$. Similarly, $(a - c) - (b - d) = (k - l)m$, so that $a - c \equiv b - d \pmod{m}$.

(b) We have that $a = b + km$ and $c = d + lm$, so that

$$\begin{aligned} ac - bd &= (b + km)(d + lm) - bd \\ &= bd + blm + dkm + klm^2 - bd \\ &= blm + dkm + klm^2 \\ &= (bl + dk + klm)m, \end{aligned}$$

so that $ac - bd$ is divisible by m, and $ac \equiv bd \pmod{m}$.

(c) By using part (b) repeatedly, we get that $a^2 \equiv b^2 \pmod{m}$, $a^3 \equiv b^3 \pmod{m}$, ..., and eventually $a^n \equiv b^n \pmod{m}$.

(d) Let $p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$. By parts (b) and (c), $a_i a^i \equiv a_i b^i \pmod{m}$ for all i. Summing over all i, by repeatedly using part (a),

$$\begin{aligned} p(a) &= a_n a^n + a_{n-1} a^{n-1} + \cdots + a_1 a + a_0 \\ &\equiv a_n b^n + a_{n-1} b^{n-1} + \cdots + a_1 b + a_0 \\ &= p(b) \pmod{m}. \end{aligned}$$

■

Part (d) is the most important of these laws, because it encompasses all of the others, and has the most breadth of application. It states, essentially, that algebraic operations (that is, addition and multiplication) preserve congruence.

Now that those are out of the way, we can proceed to the business of using modular arithmetic to solve some problems.

Example 3.1. Let $N = 11 \cdot 12 + 13 \cdot 14 + 15 \cdot 16$.

(a) What is the units digit of N?

(b) What is the remainder when N is divided by 7?

Solution. (a) Intuitively, to find the units digits of N, we should be able to drop everything but the units digits in all of our calculations. Modular arithmetic justifies this intuition.

More precisely, finding the units digit of N is the same as finding N modulo 10: two positive integers have the same units digit precisely when they are congruent modulo 10. Hence, we need only compute N modulo 10:

$$\begin{aligned} N &= 11 \cdot 12 + 13 \cdot 14 + 15 \cdot 16 \\ &\equiv 1 \cdot 2 + 3 \cdot 4 + 5 \cdot 6 \\ &\equiv 2 + 12 + 30 \\ &\equiv 2 + 2 + 0 \\ &\equiv 4 \pmod{10}. \end{aligned}$$

Therefore, the units digit of N is 4. (If you just did this calculation in your head, then you are well on your way to understanding modular arithmetic. But do not worry if you did not, it should not take you long to pick it up.)

(b) Similarly, here we consider $N \pmod 7$:

$$\begin{aligned} N &= 11 \cdot 12 + 13 \cdot 14 + 15 \cdot 16 \\ &\equiv 4 \cdot 5 + 6 \cdot 0 + 1 \cdot 2 \\ &\equiv 20 + 0 + 2 \\ &\equiv 6 + 2 \\ &\equiv 8 \\ &\equiv 1 \pmod{7}. \end{aligned}$$

Therefore, N leaves a remainder of 1 when divided by 7.

Example 3.2. When $n = 7^{1989}$ is expressed as an integer, what are the last two digits in n?

(1989 Canadian Invitational Mathematics Challenge)

Solution. Finding the last two digits of n is the same as finding n modulo 100. Let us compute the first few powers of 7 modulo 100 to see if we can find a pattern:

$$\begin{aligned} 7^0 &\equiv 1, \\ 7^1 &\equiv 7, \\ 7^2 &\equiv 7 \cdot 7 \equiv 49, \\ 7^3 &\equiv 7 \cdot 49 \equiv 343 \equiv 43, \\ 7^4 &\equiv 7 \cdot 43 \equiv 301 \equiv 1, \\ 7^5 &\equiv 7 \pmod{100}, \end{aligned}$$

and so on. We see that the powers of 7 modulo 100 cycle, with period 4, because

$7^4 \equiv 1 \pmod{100}$. Therefore,

$$\begin{aligned} 7^{1989} &= 7^{4\cdot 497+1} \\ &= \underbrace{7^4 \cdot 7^4 \cdots 7^4}_{497} \cdot 7^1 \\ &\equiv 1 \cdot 1 \cdots 1 \cdot 7 \\ &\equiv 7 \pmod{100}, \end{aligned}$$

so that the last two digits of n are 07. Notice how a problem in modulo 100 at the base level becomes a problem in modulo 4 at the exponent level.

Example 3.3. Show that $n^5 - n$ is divisible by 5 for all integers n.

Solution. Let $f(n) = n^5 - n$. Let us check the statement for n from 0 to 4:

n	$f(n)$	$f(n) \pmod 5$
0	0	0
1	0	0
2	30	0
3	240	0
4	1020	0

Thus, the statement holds for n from 0 to 4. It follows that $f(n) \equiv 0 \pmod 5$ for all integers n.

To see this, we use part (d) of the laws of modular arithmetic: Every integer is congruent to one of 0, 1, 2, 3, or 4 modulo 5. For example, if $n = 42$, then $n \equiv 2 \pmod 5$. By part (d), $f(42) \equiv f(2) \pmod 5$. But we have shown that $f(n) \equiv 0 \pmod 5$ for $n = 0$, 1, 2, 3, and 4, so that $f(n) \equiv 0$ for all integers n.

Remark. The polynomial

$$n(n-1)(n-2)(n-3)(n-4)$$

vanishes (becomes zero) for $n = 0$, 1, 2, 3, and 4. What do you get when you expand it, and reduce the coefficients modulo 5?

Example 3.4. Let n be an integer of the form $4k + 3$. Show that n cannot be written as the sum of two perfect squares.

Solution. To say that n is of the form $4k + 3$ is the same as saying that $n \equiv 3 \pmod 4$, so that this is an indication to work modulo 4. The first few perfect squares are 0, 1, 4, 9, 16, 25, etc. In modulo 4, these become 0, 1, 0, 1, 0, 1, etc. It seems that the even squares are always 0 modulo 4, and the odd squares are always 1 modulo 4. We can show this through a similar approach as in the previous problem:

n	0	1	2	3
n^2	0	1	4	9
$n^2 \pmod 4$	0	1	0	1

Hence, all squares are 0 or 1 modulo 4. This implies that the sum of two squares is either $0 + 0 \equiv 0$, $0 + 1 \equiv 1$, $1 + 0 \equiv 1$, or $1 + 1 \equiv 2$ modulo 4. Therefore, the sum of two squares can never be 3 modulo 4.

Example 3.5. Let x_1, x_2, ..., x_n be positive integers. Show that some subset of them adds up to an integer divisible by n.

Solution. Let

$$\begin{aligned} S_1 &= x_1, \\ S_2 &= x_1 + x_2, \\ &\cdots, \\ S_n &= x_1 + x_2 + \cdots + x_n. \end{aligned}$$

If $S_i \equiv 0 \pmod{n}$ for some i, then we can take the terms in S_i. Otherwise, each S_i must fall into the same congruence class as one of $1, 2, \ldots, n-1$ modulo n; in other words, all except the one with 0, for a total of $n-1$ classes. But there are n sums S_1, S_2, ..., S_n, so that, by the Pigeonhole Principle, some sums S_i and S_j, where $i < j$, are in the same congruence class, which means that $S_i \equiv S_j \pmod{n}$. The difference $S_j - S_i = x_{i+1} + x_{i+2} + \cdots + x_j \equiv 0 \pmod{n}$ gives a desired subset.

Example 3.6. Solve the equation $x^2 + y^2 = 3z^2$ in integers.

Solution. If $x = 0$, then $y^2 = 3z^2$, and $y = \pm z\sqrt{3}$. Since $\sqrt{3}$ is irrational, we must have $y = z = 0$.

Suppose now that $x > 0$. We have that $x^2 + y^2 = 3z^2 \equiv 0 \pmod{3}$. We can quickly verify that the only squares modulo 3 are 0 and 1, so that $x \equiv y \equiv 0 \pmod{3}$. Let $x = 3x_1$ and $y = 3y_1$, so that $x^2 + y^2 = 9x_1^2 + 9y_1^2 = 3z^2 \Rightarrow z^2 = 3(x_1^2 + y_1^2) \equiv 0 \pmod{3}$, so that $z \equiv 0 \pmod{3}$. Let $z = 3z_1$, so that $9z_1^2 = 3(x_1^2 + y_1^2) \Rightarrow x_1^2 + y_1^2 = 3z_1^2$, which is just our original equation $x^2 + y^2 = 3z^2$, only all variables have been divided by 3.

Using the same reasoning, we get that $x_1 = 3x_2$, $y_1 = 3y_2$, and $z_1 = 3z_2$, for some integers x_2, y_2, z_3, so that $x = 3^2 x_2$, and in general, $x = 3^n x_n$ for some integer x_n, for all positive integers n. However, this is a contradiction: The positive integer x has only a finite number of factors of 3. The same argument holds when $x < 0$. Therefore, $(x, y, z) = (0, 0, 0)$ is the only solution.

Remark. This solution uses Fermat's method of infinite descent.

Example 3.7. Show that there are an infinite number of primes of the form $4k + 3$.

Solution. We proceed using proof by contradiction. Suppose that there are only a finite number of primes of the form $4k + 3$, or 3 modulo 4, say p_1, p_2, ..., p_n. Let $N = 4p_1 p_2 \cdots p_n - 1$.

Since N is odd, the prime factors of N are all of the form $4k + 1$ or $4k + 3$. However, N cannot be divisible by any prime of the form $4k + 3$ – by assumption, p_1, p_2, ..., p_n are all the primes of the form $4k + 3$, and $N \equiv -1 \pmod{p_i}$ for all i.

Hence, N is the product of primes of the form $4k + 1$, which implies that $N \equiv 1 \pmod{4}$. However, $N \equiv -1 \pmod{4}$, contradiction. Therefore, there are

infinitely many primes of the form $4k + 3$.

Problems

1. Construct the addition and multiplication table for modulo 6.
2. Reduce the following numbers:
   (a) $2^{500} \pmod{11}$.
   (b) $6^{99} + 7^{99} \pmod{13}$.
   (c) $1 + 3 + 5 + \cdots + (2n - 1) \pmod{2}$.
3. Find all digits a and b such that $aabb$ is a four-digit perfect square.
4. Show that for every positive integer n, either $2^n - 1$ or $2^n + 1$ is divisible by 3.
5. Prove that for all positive integers n, $1^n + 8^n - 3^n - 6^n$ is divisible by 10.
6. Prove or disprove: $2^x \equiv 2^y \pmod{n}$ if $x \equiv y \pmod{n}$.
7. (a) Find all squares modulo 7.
   (b) Let a and b be positive integers. Show that if $a^2 + b^2 \equiv 0 \pmod{7}$, then $a \equiv b \equiv 0 \pmod{7}$.
8. Prove that
$$1 \cdot 3 \cdot 5 \cdots 1993 + 2 \cdot 4 \cdot 6 \cdots 1994$$
   is divisible by 1995.
9. Show that every prime greater than 3 can be expressed in the form $\sqrt{24n + 1}$ for some positive integer n.
10. Let a, b, and c be odd integers. Show that the quadratic equation $ax^2 + bx + c = 0$ cannot have rational roots.
11. The positive integers are listed in a table with six columns, as follows:

1	2	3	4	5	6
7	8	9	10	11	12
13	14	15	16	17	18
19	20	21	22	23	24
25	26	27	28	29	30
⋮	⋮	⋮	⋮	⋮	⋮

    (a) Prove that every prime greater than 3 appears in the first or fifth column.
    (b) Prove that there are infinitely many primes in the fifth column.
12. Find all positive integers n such that the equation $x^2 - y^2 = n$ has no solutions in non-negative integers x and y.

4 Linear Diophantine Equations and Congruences

A certain problem asks the following:

> A person wishes to mail a letter that will cost 29 cents. However, the only stamps he has are in 5 cent and 7 cent denominations. What combinations, if any, will work?

If we let x be the number of required 5 cent stamps, and y the number of required 7 cent stamps, then the problem becomes solving the equation $5x + 7y = 29$. Equations, such as this one, that demand integer solutions are known as **Diophantine** equations, named after the Greek mathematician Diophantus who studied such equations.

The linear equation $ax + by = c$

We first look at the linear diophantine equation $ax + by = c$, where a, b, and c are fixed integers, and x and y are integer variables. Let us determine just what values the expression $ax + by$ can attain.

For example, take $a = 4$ and $b = 10$. What values can $4x+10y$ attain? Since $4x + 10y = 2(2x + 5y)$, all values must be multiples of 2. Is 2 itself attainable? Yes, take $x = -2$ and $y = 1$: then $4x + 10y = -8 + 10 = 2$. We then realize that all multiples of 2 are attainable – just multiply the values of x and y by the same factor. For example, 12 is attainable because

$$\begin{aligned} 12 &= 6 \cdot 2 = 6 \cdot [4 \cdot (-2) + 10 \cdot 1] \\ &= 4 \cdot (-12) + 10 \cdot 6. \end{aligned}$$

In general, for the expression $ax + by$, $\gcd(a, b)$ divides both a and b, so that $\gcd(a, b)$ must divide $ax + by$, or in other words, $ax + by$ must be a multiple of $\gcd(a, b)$. We present a method that explicitly finds integers x and y such that $ax + by = \gcd(a, b)$.

The Euclidean Algorithm

Let a and b be positive integers, with $a > b$. By the division algorithm, there exist integers q and r such that $a = qb + r$, with $0 \leq r < b$, which can be found by dividing b into a.

Let $d = \gcd(a, b)$. Then d divides both a and b, so that d divides $a - qb = r$, which implies that d divides $\gcd(b, r)$. On the other hand, if we let $d' = \gcd(b, r)$, then d' divides both b and r, so that d' divides $qb + r = a$, which implies that d' divides $\gcd(a, b) = d$. Therefore, $d = d'$, or $\gcd(a, b) = \gcd(b, r)$.

The Euclidean algorithm is then the process of taking b and r, dividing r into b, and repeating. By what we have just said, the gcd is preserved. The numbers get smaller, so that eventually we will get a remainder of 0. At that point, the last dividend is the gcd. Let us illustrate the algorithm with an example.

Consider the pair 21 and 36. Dividing 21 into 36, we get a quotient of 1 and a remainder of 15. Then we take the numbers 21 and 15. Dividing 15 into 21, we get a quotient of 1 and a remainder of 6. We take 15 and 6, and dividing 6 into 15, we get a quotient of 2 and a remainder of 3, and finally 3 divides evenly into 6, so that $\gcd(36, 21) = 3$. These calculations can be nicely summarized as follows:

$$\begin{aligned} 36 &= 1 \cdot 21 + 15, \\ 21 &= 1 \cdot 15 + 6, \\ 15 &= 2 \cdot 6 + 3, \\ 6 &= 2 \cdot 3. \end{aligned}$$

To see why this works, consider the more general case:

$$\begin{aligned} a &= q_1 b + r_1, \\ b &= q_2 r_1 + r_2, \\ r_1 &= q_3 r_2 + r_3, \\ &\dots, \\ r_n &= q_{n+2} r_{n+1}. \end{aligned}$$

From $a = q_1 b + r_1$, we get $\gcd(a, b) = \gcd(b, r_1)$. From $b = q_2 r_1 + r_2$, we get $\gcd(b, r_1) = \gcd(r_1, r_2)$, and so on, until $\gcd(r_{n-1}, r_n) = \gcd(r_n, r_{n+1}) = r_{n+1}$, so that $\gcd(a, b) = r_{n+1}$.

Thus, the Euclidean algorithm calculates the gcd of two numbers, but we can extract more information from our calculations. Using some clever back-substituting, we can find x and y such that $36x + 21y = \gcd(36, 21) = 3$:

$$\begin{aligned} 3 &= 15 - 2 \cdot 6 \\ &= 15 - 2 \cdot (21 - 15) \\ &= 3 \cdot 15 - 2 \cdot 21 \\ &= 3 \cdot (36 - 21) - 2 \cdot 21 \\ &= 3 \cdot 36 - 5 \cdot 21. \end{aligned}$$

Thus, we can take $x = 3$ and $y = -5$.

In general, this method always gives an x and y such that $ax+by = \gcd(a, b)$. We can then multiply x and y by the appropriate factor to get every multiple of $\gcd(a, b)$. Since $ax + by$ can only attain multiples of $\gcd(a, b)$, these are exactly the values that it does attain.

Values of $ax + by$. Let a and b be positive integers. Then as x and y vary over all integers, $ax + by$ attains all multiples of $\gcd(a, b)$, and only multiples of $\gcd(a, b)$.

Corollary. The positive integers a and b are relatively prime if and only if there exist integers x and y such that $ax + by = 1$.

Example 4.1. Prove that the fraction

$$\frac{21n + 4}{14n + 3}$$

is irreducible for every positive integer n.

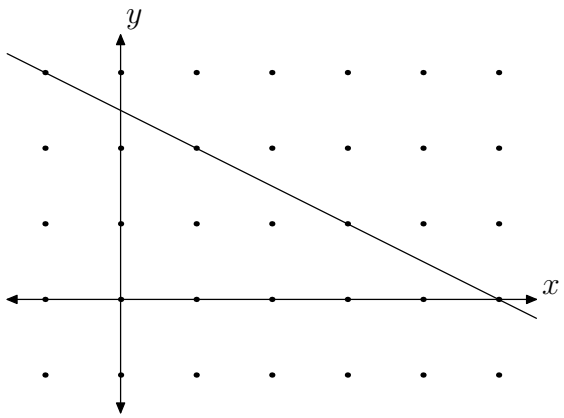
Solution. For all n, $3(14n+3)-2(21n+4)=1$, so that the numerator and denominator are relatively prime.

Interesting historical side note: Wilhelm Fliess, a physician and colleague of Sigmund Freud, created a theory centred around the numbers 23 and 28, based on his research into human biorhythms. Martin Gardner, in *Science: Good, Bad, and Bogus*, writes:

> Fliess's basic formula can be written $23x + 28y$, where x and y are positive or negative integers. On almost every page Fliess fits this formula to natural phenomena, ranging from the cell to the solar system. . . . He did not realize that if any two positive integers that have no common divisor are substituted for 23 and 28 in his basic formula, it is possible to express any positive integer whatever. Little wonder that the formula could be so readily fitted to natural phenomena!

We now turn our attention to the linear equation $ax+by=c$. By the result that we have just established, this equation has a solution in x and y if and only if c is a multiple of $\gcd(a,b)$. But given such a c, what do the solutions look like?

Let us take a look at an example, and graph the line $x+2y=5$:



As we can see, some solutions are $(-1,3)$, $(1,2)$, $(3,1)$, and $(5,0)$. If we let y be an arbitrary integer t, then $x=5-2t$ satisfies the equation, so that all solutions are of the form $(5-2t,t)$. In general, the solutions to the linear equation $ax+by=c$ always have this format.

Solutions to $ax+by=c$. Let a and b be positive integers, and let c be an integer. Then the equation $ax+by=c$ is solvable in integers if and only if c is a multiple of $\gcd(a,b)$. Furthermore, all solutions are of the form

$$(x,y) \;=\; \left(x_0 + t\cdot\frac{b}{d},\; y_0 - t\cdot\frac{a}{d}\right),$$

where $d=\gcd(a,b)$, (x_0,y_0) is a specific solution of $ax+by=c$, and t is an arbitrary integer.

Proof. We have already established that c must be a multiple of $\gcd(a, b)$. As stated, let $d = \gcd(a, b)$, and let (x_0, y_0) be a specific solution of $ax + by = c$, so that $ax_0 + by_0 = c$. If $ax + by = c$, then

$$\begin{aligned}(ax + by) - (ax_0 + by_0) = a(x - x_0) + b(y - y_0) = 0 \\ \Rightarrow \quad a(x - x_0) = b(y_0 - y) \\ \Rightarrow \quad \frac{a}{d} \cdot (x - x_0) = \frac{b}{d} \cdot (y_0 - y).\end{aligned}$$

Since b/d divides the right-hand side, b/d also divides the left-hand side. However, a/d and b/d are relatively prime, so that b/d divides $x - x_0$. Hence, let $x - x_0 = t \cdot b/d$, where t is an integer. Then $y_0 - y = t \cdot a/d$. This gives us the solutions as described. ■

The specific solution (x_0, y_0) can be found via the Euclidean algorithm, or trial and error.

Example 4.1. Find all integer solutions to the following equations:

(a) $3x + 4y = 0$.

(b) $3x - 7y = 2$.

(c) $2x + 8y = 3$.

(d) $36x + 21y = 6$.

Solution. (a) First, $\gcd(3, 4) = 1$, which divides 0, so that there are solutions. A specific solution is $(0, 0)$, so all solutions are given by $(x, y) = (4t, -3t)$.

(b) First, $\gcd(3, 7) = 1$, which divides 2, so that there are solutions. A specific solution is $(3, 1)$, so that all solutions are of the form $(x, y) = (3+7t, 1+3t)$.

(c) Since $\gcd(2, 8) = 2$ does not divide 3, there are no solutions.

(d) First, $\gcd(36, 21) = 3$, which divides 6, so that there are solutions. We derived earlier that $3 \cdot 36 - 5 \cdot 21 = 2$, so that a specific solution is $(6, -10)$, so that all solutions are given by $(x, y) = (6 + 7t, -10 - 12t)$.

The congruence $ax \equiv c \pmod{m}$

We now consider how to solve the congruence $ax \equiv c \pmod{m}$. We have in fact already solved it, when we solved the linear equation $ax + by = c$. But before we get ahead of ourselves, let us look at an example.

The linear equation $2x = 8$ is solved easily enough; just divide both sides by 2, and we get $x = 4$. But in modular arithmetic, things are not quite as straightforward. For example, take the congruence $2x \equiv 8 \pmod{10}$. If we try the same strategy and divide both sides by 2, we get $x \equiv 4 \pmod{10}$. But in doing this, we miss the solution $x = 9$, since $2 \cdot 9 = 18 \equiv 8 \pmod{10}$.

The reason this occurs is the existence of what are called **zero divisors** – numbers that are not zero, but when multiplied, become zero. For example,

neither 2 nor 5 are zero, but $2 \cdot 5 = 10 \equiv 0 \pmod{10}$. These zero divisors preclude division in modular arithmetic: For example, we cannot divide the congruence $2 \cdot 5 \equiv 0 \pmod{10}$ by 2, because then we would get $5 \equiv 0 \pmod{10}$, which is not true. We must go back to the basics; in this case, the definition itself.

The congruence $2x \equiv 8 \pmod{10}$ is equivalent to saying that $2x - 8 = 10k$ for some integer k. We can divide this equation by 2, and obtain $x - 4 = 5k$, which in turn is equivalent to saying that $x \equiv 4 \pmod{5}$. Note that this does include the solution $x = 9$.

For the general congruence $ax \equiv c \pmod{m}$, this is equivalent to saying that $ax - c = km$ for some integer k, or $ax - mk = c$. This is a linear equation in x and k, which we have already solved; only here, we are only interested in the values of x. We saw that there is a solution if and only if $\gcd(a, m)$ divides c, and in such a case, all solutions for x are given by

$$x \;=\; x_0 + t \cdot \frac{m}{d},$$

where x_0 is a specific solution, and $d = \gcd(a, m)$. Note that this is equivalent to saying that $x \equiv x_0 \pmod{m/d}$.

Example 4.3. Solve the following congruences:

(a) $7x \equiv 2 \pmod{11}$.

(b) $9x \equiv 6 \pmod{24}$.

(c) $2x \equiv 3 \pmod{12}$.

Solution. (a) In this example, $a = 7$, $c = 2$, and $m = 11$, so that $d = \gcd(a, m) = 1$, which divides c. We find that a specific solution to the congruence is $x_0 = 5$. Therefore, the solution is $x \equiv 5 \pmod{11}$.

(b) In this example, $a = 9$, $c = 6$, and $m = 24$, so that $d = \gcd(9, 24) = 3$, which divides c. We find that a specific solution to the congruence is $x_0 = 6$. Therefore, the solution is $x \equiv 6 \pmod{8}$.

(c) In this example, $a = 2$, $c = 3$, and $m = 12$, so that $d = \gcd(2, 12) = 2$, which does not divide c, so that there are no solutions.

Before we leave this chapter, we describe one more important concept in modular arithmetic. As we have indicated before, we do not have division in modular arithmetic. But, we do have the next best thing. Going back to our first example, we divided the equation $2x = 8$ by 2 to obtain the solution $x = 4$. We could have also multiplied both sides by $1/2$, because $1/2$ is the multiplicative inverse of 2. In modular arithmetic, we do not have division, but we have multiplicative inverses.

We say that x is the **inverse** of a modulo m if $ax \equiv 1 \pmod{m}$, and write $x \equiv a^{-1} \pmod{m}$. We give a criterion for an integer to have an inverse.

Inverses. The inverse $a^{-1} \pmod{m}$ exists, and is unique modulo m, if and only if a is relatively prime to m.

Proof. Recall that the integers a and b are relatively prime if and only if there exist integers x and y such that $ax+by=1$. Consider the following sequence of statements:

(1) The inverse $a^{-1} \pmod{m}$ exists.

(2) There exists an integer x such that $ax \equiv 1 \pmod{m}$.

(3) There exist integers x and k such that $ax - km = 1$.

(4) The integers a and m are relatively prime.

Each statement is equivalent to the previous one, which shows that $a^{-1} \pmod{m}$ exists if and only if a and m are relatively prime. Now, let x and x' be two inverses of a, so that $ax \equiv ax' \equiv 1 \pmod{m}$. Then $xax \equiv xax'$, or $x \equiv x' \pmod{m}$, since $xa \equiv 1 \pmod{m}$, so that the inverse $a^{-1} \pmod{m}$ is unique. ■

As before, it is possible to compute inverses via the Euclidean algorithm or by trial and error. These inverses also give us another way of solving linear congruences.

Example 4.4.

(a) Compute $4^{-1} \pmod{17}$.

(b) Solve the congruence $4x \equiv 14 \pmod{17}$.

Solution. (a) We seek an x such that $4x \equiv 1 \pmod{17}$. Using the methods so far, we can find that the solution is $x \equiv 13 \pmod{17}$. Therefore, $4^{-1} \equiv 13 \pmod{17}$.

(b) Multiplying both sides by 13, we obtain $13 \cdot 4x = 52x \equiv x \equiv 13 \cdot 14 \equiv 182 \equiv 12 \pmod{17}$. Therefore, the solution is $x \equiv 12 \pmod{17}$.

In general, if $a^{-1} \pmod{m}$ exists, then the solution to the congruence $ax \equiv c \pmod{m}$ is $x \equiv a^{-1}c \pmod{m}$.

Finally, if we have a congruence of the form $ax \equiv ay \pmod{m}$, and a is relatively prime to m, then we can multiply both sides by a^{-1} to get $x \equiv y \pmod{m}$. This is sometimes called the cancellation law.

Problems

1. Find the following:
   (a) $\gcd(66, 147)$,
   (b) $\gcd(105, 273)$.
2. Find all integer solutions to the following equations:
   (a) $2x + 3y = 6$.
   (b) $44x + 28y = 80$.
3. Show that some multiple of 31 has 174 as its final three digits.

4. Let a, b, x, and y be integers. Show that if $ax + by = \gcd(a, b)$, then x and y are relatively prime.

5. Let S be the set of ordered pairs $(3i + 4j + 5k, 8i - j + 4k)$, where i, j, and k vary over all integers, and T be the set of ordered pairs $(m, 5m + 7n)$, where m and n vary over all integers. Show that $S = T$.

6. Let a, b, c, d be fixed integers with d not divisible by 5. Assume that m is an integer for which $am^3 + bm^2 + cm + d \equiv 0 \pmod 5$. Prove that there exists an integer n for which $dn^3 + cn^2 + bn + a \equiv 0 \pmod 5$.

7. Let a be a zero divisor modulo m; that is, a is non-zero, and there exists a non-zero b such that $ab \equiv 0 \pmod m$. Prove that a does not have an inverse modulo m.

5 Modular Arithmetic II

In this chapter we introduce the four pivotal theorems of modular arithmetic: Fermat's Little Theorem, Euler's Theorem, Wilson's Theorem, and the Chinese Remainder Theorem.

We saw earlier that computing powers of integers modulo a certain number was a key step in some of our problems. Fermat's Little Theorem and Euler's Theorem can make these calculations easier.

We must first recall some algebra. By the binomial theorem, for a positive integer n,

$$(x+y)^n = \binom{n}{0}x^n + \binom{n}{1}x^{n-1}y + \binom{n}{2}x^{n-2}y^2 + \cdots + \binom{n}{k}x^{n-k}y^k + \cdots + \binom{n}{n}y^n,$$

where

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

For all n,

$$\binom{n}{0} = \binom{n}{n} = 1.$$

Now suppose that n is a prime p, so that

$$(x+y)^p = \binom{p}{0}x^p + \binom{p}{1}x^{p-1}y + \binom{p}{2}x^{p-2}y^2 + \cdots + \binom{p}{k}x^{p-k}y^k + \cdots + \binom{p}{p}y^p.$$

Let $1 \le k \le p-1$. Then $p-k \le p-1$, so that both $k!$ and $(p-k)!$ do not contain any factors of p. However, $p!$ is divisible by p, so that

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

is also divisible by p. Therefore, reducing the coefficients modulo p, we get

$$\begin{aligned}(x+y)^p &= \binom{p}{0}x^p + \binom{p}{1}x^{p-1}y + \cdots + \binom{p}{k}x^{p-k}y^k + \cdots + \binom{p}{p}y^p \\ &\equiv x^p + y^p \pmod{p}.\end{aligned}$$

For example, with $p = 5$,

$$\begin{aligned}(x+y)^5 &= \frac{5!}{0!5!}x^5 + \frac{5!}{1!4!}x^4y + \frac{5!}{2!3!}x^3y^2 + \frac{5!}{3!2!}x^2y^3 + \frac{5!}{4!1!}xy^4 + \frac{5!}{5!0!}y^5 \\ &= x^5 + 5x^4y + 10x^3y^2 + 10x^2y^3 + 5xy^4 + y^5 \\ &\equiv x^5 + y^5.\end{aligned}$$

We now use this result to prove our first theorem.

Fermat's Little Theorem (FLT). If p is prime, then $n^p \equiv n \pmod{p}$.

Proof. We prove the result by induction on n. The result is clearly true for $n = 0$. Assume that it is true for some integer $n = k$, so that $k^p \equiv k \pmod{p}$. By the identity, $(k+1)^p \equiv k^p + 1^p \pmod{p}$, so that

$$\begin{aligned}(k+1)^p - (k+1) &\equiv k^p + 1 - k - 1 \\ &\equiv k^p - k \\ &\equiv 0 \pmod{p}.\end{aligned}$$

Thus, the theorem is true for $n = k + 1$, and by induction, it is true for all n. ■

You might also see this theorem stated as follows: If n is not divisible by p, then $n^{p-1} \equiv 1 \pmod{p}$.

Example 5.1. Show that $2^{74} + 3^{74}$ is divisible by 13.

Solution. We can simplify the expression by using the fact that by FLT, $2^{12} \equiv 3^{12} \equiv 1 \pmod{13}$. Hence,

$$\begin{aligned}2^{74} + 3^{74} &= 2^{6\cdot 12+2} + 3^{6\cdot 12+2} \\ &\equiv (2^{12})^6 \cdot 2^2 + (3^{12})^6 \cdot 3^2 \\ &\equiv 2^2 + 3^2 \\ &\equiv 0 \pmod{13}.\end{aligned}$$

Example 5.2. Show that $n^5 - n$ is divisible by 30 for all positive integers n.

Solution. In Example 3.3, we proved that $n^5 - n$ is divisible by 5 for all n, and we can use the same approach here, but FLT offers a different approach. First, 30 factors as $2 \cdot 3 \cdot 5$.

By FLT, $n^2 \equiv n \pmod{2}$ for all n. Multiplying both sides by n, we get $n^3 \equiv n^2 \pmod{2}$. Repeating, we get $n^4 \equiv n^3 \pmod{2}$ and $n^5 \equiv n^4 \pmod{2}$. Therefore, $n^5 \equiv n^4 \equiv n^3 \equiv n^2 \equiv n \pmod{2}$, which shows that $n^5 - n \equiv 0 \pmod{2}$ for all n.

Also by FLT, $n^3 \equiv n \pmod 3$ for all n. Multiplying both sides by n^2, we get $n^5 \equiv n^3 \pmod 3$, so that $n^5 \equiv n^3 \equiv n \pmod 3$, which shows that $n^5 - n \equiv 0 \pmod 3$ for all n.

Finally by FLT, $n^5 \equiv n \pmod 5$ for all n, or $n^5 - n \equiv 0 \pmod 5$. Therefore, $n^5 - n \equiv 0 \pmod{2 \cdot 3 \cdot 5}$ for all n.

Example 5.3. Prove that the expression

$$\frac{x^5}{5} + \frac{x^3}{3} + \frac{7x}{15}$$

is always an integer for all positive integral values of x.

(1968 Descartes Waterloo Contest)

Solution. Putting the expression over a common denominator, it becomes

$$\frac{3x^5 + 5x^3 + 7x}{15}.$$

Hence, we must show that $3x^5 + 5x^3 + 7x$ is divisible by 15 for all x.

Taking the expression modulo 3, $3x^5 + 5x^3 + 7x \equiv 2x^3 + x \pmod 3$. By FLT, $x^3 \equiv x \pmod 3$ for all x, so that $2x^3 + x \equiv 2x + x \equiv 3x \equiv 0 \pmod 3$. Hence, $3x^5 + 5x^3 + 7x$ is divisible by 3 for all x.

Taking the expression modulo 5, $3x^5 + 5x^3 + 7x \equiv 3x^5 + 2x \pmod 5$. By FLT, $x^5 \equiv x \pmod 5$ for all x, so that $3x^5 + 2x \equiv 3x + 2x \equiv 5x \equiv 0 \pmod 5$. Hence, $3x^5 + 5x^3 + 7x$ is divisible by 5 for all x.

Therefore, $3x^5 + 5x^3 + 7x$ is divisible by 15 for all x.

Example 5.4. Show that if p is a prime dividing $x^2 + 1$, then $p = 2$ or $p \equiv 1 \pmod 4$.

Solution. We must show that $p \not\equiv 3 \pmod 4$. Using proof by contradiction, suppose that $p \equiv 3 \pmod 4$, so $p = 4k + 3$ for some k. Since p divides $x^2 + 1$, $x^2 \equiv -1 \pmod p$, so that

$$x^{p-1} \;=\; x^{4k+2} \;=\; (x^2)^{2k+1} \equiv (-1)^{2k+1} \equiv -1 \pmod p.$$

However, p does not divide x, so that, by FLT, $x^{p-1} \equiv 1 \pmod p$, a contradiction. Therefore, $p \not\equiv 3 \pmod 4$.

It is natural to ask whether the converse of Fermat's Little Theorem is true; that is, if $a^n \equiv a \pmod n$ for some a and n, then is n a prime? The following problem shows that this is not necessarily the case. (See also problem 3 at the end of the chapter).

Example 5.5. A composite integer n is called a **pseudoprime** to base a if $a^n \equiv a \pmod n$. Show that 341 is a pseudoprime to base 2, but not to base 3.

Solution. We must show that $2^{341} \equiv 2 \pmod{341}$. First, 341 factors as $11 \cdot 31$.

By FLT, $2^{10} \equiv 1 \pmod{11}$, so that $2^{341} \equiv (2^{10})^{34} \cdot 2 \equiv 2 \pmod{11}$, and $2^{341} - 2 \equiv 0 \pmod{11}$. Also, $2^{30} \equiv 1 \pmod{31}$, so that $2^{341} \equiv (2^{30})^{11} \cdot 2^{11} \equiv 2048 \equiv 2 \pmod{31}$, so that $2^{341} - 2 \equiv 0 \pmod{31}$. Hence, $2^{341} - 2 \equiv 0 \pmod{341}$.

However, $3^{341} \equiv 3^{11} \equiv 3^2 \cdot (3^3)^3 \equiv 9 \cdot 27^3 \equiv 9 \cdot (-4)^3 \equiv 9 \cdot (-64) \equiv 9 \cdot (-2) \equiv -18 \equiv 13 \pmod{31}$, so that 3^{341} is not congruent to 3 modulo 341.

For our next result, we need to define some new terms. For a positive integer n, let $\phi(n)$ denote the number of positive integers less than n that are relatively prime to n. For example, the integers 1, 2, 3, 4, 5, and 6 are relatively prime to 7, so that $\phi(7) = 6$, and the integers 1, 3, 7, and 9 are relatively prime to 10, so that $\phi(10) = 4$.

By convention, $\phi(1) = 1$, and it can be shown that if the prime factorization of $n > 1$ is $p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$, then

$$\begin{aligned} \phi(n) &= p_1^{e_1 - 1} p_2^{e_2 - 1} \cdots p_k^{e_k - 1} (p_1 - 1)(p_2 - 1) \cdots (p_k - 1) \\ &= n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right). \end{aligned}$$

(See *An Introduction to the Theory of Numbers*, I. Niven, H. Zuckerman & H. Montgomery, for a proof.)

Call a set a **reduced residue system modulo** n if it contains a unique member belonging to each congruence class relatively prime to n. For example, $\{1, 3, 7, 9\}$ is a reduced residue system modulo 10, but so are $\{-9, 13, 17, 29\}$ and $\{11, -7, -23, 19\}$. A reduced residue system modulo n always contains $\phi(n)$ members.

Euler's Theorem. If a is relatively prime to n, then $a^{\phi(n)} \equiv 1 \pmod{n}$.

Proof. Let $S = \{r_1, r_2, \ldots, r_{\phi(n)}\}$ be a reduced residue system modulo n. We claim that the set $T = \{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ is also a reduced residue system modulo n.

First, since a is relatively prime to n, we have that ar_i is relatively prime to n for all i. Secondly, each element of T is in a distinct congruence class: if $ar_i \equiv ar_j \pmod{m}$, then by multiplying both sides by the inverse of a, we get $r_i \equiv r_j \pmod{m}$, and we know that the r_i are in distinct congruence classes. Finally, since T contains $\phi(n)$ elements, it must contains one in each congruence class relatively prime to n.

In other words, multiplying each element of S by a to get T simply permutes the elements, with respect to congruence classes modulo n. Then the products of the elements of S and T (and of any reduced residue system modulo n) are congruent modulo n:

$$\begin{aligned} r_1 r_2 \cdots r_{\phi(n)} &\equiv (ar_1)(ar_2) \cdots (ar_{\phi(n)}) \\ &= a^{\phi(n)} r_1 r_2 \cdots r_{\phi(n)} \\ \Rightarrow \quad a^{\phi(n)} &\equiv 1 \pmod{n}. \end{aligned}$$

■

Note that Euler's Theorem is a generalization of Fermat's Little Theorem, since $\phi(p) = p - 1$ for any prime p.

Example 5.6. Let a be relatively prime to n. Show that $a^{-1} \equiv a^{\phi(n)-1} \pmod{n}$.

Solution. By Euler's Theorem, $a^{\phi(n)} \equiv 1 \pmod{n}$. We then get the result by multiplying both sides by $a^{-1} \pmod{n}$.

Example 5.7. Let a and b be two relatively prime positive integers. Show that there exist positive integers m and n such that $a^m + b^n \equiv 1 \pmod{ab}$.

Solution. Let $S = a^m + b^n$, where $m = \phi(b)$ and $n = \phi(a)$. Then, by Euler's Theorem, $S = a^{\phi(b)} + b^{\phi(a)} \equiv 1 \pmod{a}$, or $S - 1 \equiv 0 \pmod{a}$, and similarly, $S \equiv 1 \pmod{b}$, or $S - 1 \equiv 0 \pmod{b}$. Therefore, $S - 1 \equiv 0 \pmod{ab}$, so that $S \equiv 1 \pmod{ab}$.

Our next result, Wilson's Theorem, is a pretty result concerning factorials.

Wilson's Theorem. If p is a prime, then $(p-1)! \equiv -1 \pmod{p}$.

Proof. The simple strategy is to pair inverses modulo p among the integers $1, 2, \ldots, p-1$. Let us take an example, and let $p = 13$. Then the inverse pairs modulo 13 are: 2 and 7, 3 and 9, 4 and 10, 5 and 8, and 6 and 11; note that the integers 1 and 12 are their own inverses. Hence,

$$\begin{aligned} 12! &\equiv 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10 \cdot 11 \cdot 12 \\ &\equiv 1 \cdot (2 \cdot 7) \cdot (3 \cdot 9) \cdot (4 \cdot 10) \cdot (5 \cdot 8) \cdot (6 \cdot 11) \cdot 12 \\ &\equiv 1 \cdot 1 \cdot 1 \cdot 1 \cdot 1 \cdot 1 \cdot 12 \\ &\equiv -1 \pmod{13}. \end{aligned}$$

Likewise, for any prime p, only 1 and $p-1$ are their own inverses, and the rest of the integers may be paired off by inverses. To see this, let x be an integer that is its own inverse. Then $x \cdot x \equiv x^2 \equiv 1 \pmod{p} \Rightarrow x^2 - 1 = (x-1)(x+1) \equiv 0 \pmod{p}$. Since p is a prime, p either divides $x - 1$ or $x + 1$, confirming that the only solutions are $x \equiv 1$ and $-1 \pmod{p}$. Hence,

$$\begin{aligned} (p-1)! &\equiv 1 \cdot 2 \cdots (p-1) \\ &\equiv 1 \cdot 1 \cdot 1 \cdots (p-1) \\ &\equiv -1 \pmod{p}. \end{aligned}$$

■

It turns out that an integer n is prime if and only if $(n-1)! \equiv -1 \pmod{n}$, but $(n-1)!$ grows so quickly as n does, for large n, that this is not an effective way of testing whether n is prime.

Example 5.8. Let $\{a_1, a_2, \ldots, a_{100}\}$ and $\{b_1, b_2, \ldots, b_{100}\}$ be reduced residue systems modulo 101. Can $\{a_1b_1, a_2b_2, \ldots, a_{100}b_{100}\}$ be a reduced residue systems modulo 101?

Solution. The answer is no. Since $\{a_1, a_2, \ldots, a_{100}\}$ is a reduced residue system modulo 101, its elements are a permutation of $1, 2, \ldots, 100$, with

respect to congruence classes. Hence, $a_1a_2 \cdots a_{100} \equiv 1 \cdot 2 \cdots 100 = 100! \equiv -1 \pmod{101}$, by Wilson's Theorem. Similarly, $b_1b_2 \cdots b_{100} \equiv -1 \pmod{101}$, so that $a_1a_2 \cdots a_{100}b_1b_2 \cdots b_{100} \equiv 1 \pmod{101}$.

But if $\{a_1b_1, a_2b_2, \ldots, a_{100}b_{100}\}$ is a reduced residue systems modulo 101, then $a_1b_1a_2b_2 \cdots a_{100}b_{100} \equiv -1 \pmod{101}$, a contradiction.

For our last result, consider the following problem:

> A teacher wishes to divide her students into groups. When she divides them into groups of four, there are three left over. When she divides them into groups of five, there are two left over. How many students are in her class, given that there are less than 40?

Setting n to be the number of students in the class, the problem translates into the following conditions:

$$n \equiv 3 \pmod{4}, \qquad n \equiv 2 \pmod{5},$$

and $1 \leq n < 40$. The following result guarantees that certain simultaneous systems of congruences always have a solution.

Chinese Remainder Theorem. Let $m_1, m_2, \ldots, m_k$ be integers that are pairwise relatively prime (that is, m_i and m_j are relatively prime for any distinct i, j), and let $a_1, a_2, \ldots, a_k$ be arbitrary integers. Then the system

$$\begin{aligned} x &\equiv a_1 \pmod{m_1}, \\ x &\equiv a_2 \pmod{m_2}, \\ &\cdots, \\ x &\equiv a_k \pmod{m_k}, \end{aligned}$$

has a unique solution modulo $m_1m_2 \cdots m_k$.

We omit a proof of this theorem, opting instead to go through a detailed example, which should illustrate the idea of the proof.

Example 5.9. Solve the system

$$\begin{aligned} x &\equiv 2 \pmod{7}, \\ x &\equiv 4 \pmod{9}, \\ x &\equiv 8 \pmod{10}. \end{aligned}$$

Solution. First, consider the system

$$\begin{aligned} x &\equiv 1 \pmod{7}, \\ x &\equiv 0 \pmod{9}, \\ x &\equiv 0 \pmod{10}. \end{aligned}$$

The last two congruences say that $x \equiv 0 \pmod{90}$. Hence, we require multiples of 90 that are 1 modulo 7, leading to the equation $x = 90n = 7k + 1$. The

solutions to this are $(n, k) = (6 + 7t, 77 + 90t)$, so that all solutions are of the form $x = 90n = 540 + 630t$, or $x \equiv 540 \pmod{630}$. Call this solution e_1. Similarly, we find that the solutions to the systems

$$\begin{aligned} x &\equiv 0 \pmod 7, \\ x &\equiv 1 \pmod 9, \\ x &\equiv 0 \pmod{10}, \end{aligned}$$

and

$$\begin{aligned} x &\equiv 0 \pmod 7, \\ x &\equiv 0 \pmod 9, \\ x &\equiv 1 \pmod{10}, \end{aligned}$$

are $x \equiv 280 \pmod{630}$ and $x \equiv 441 \pmod{630}$, which we call e_2 and e_3, respectively. Let $x \equiv 2e_1 + 4e_2 + 8e_3 \pmod{630}$. Then $x \equiv 2 \cdot 1 + 4 \cdot 0 + 8 \cdot 0 \equiv 2 \pmod 7$. Similarly, $x \equiv 4 \pmod 9$ and $x \equiv 8 \pmod{10}$. Thus, $x \equiv 2 \cdot 540 + 4 \cdot 280 + 8 \cdot 441 \equiv 5728 \equiv 58 \pmod{630}$ is a solution to our original system.

But can there be other solutions? The original system can be expressed as

$$\begin{aligned} x &\equiv 58 \pmod 7, \\ x &\equiv 58 \pmod 9, \\ x &\equiv 58 \pmod{10}, \end{aligned}$$

so that 7, 9, and 10 divide $x - 58$, which implies that 630 divides $x - 58$, or $x \equiv 58 \pmod{630}$. Hence, this is the unique solution.

Example 5.10. Prove that for each positive integer n there exist n consecutive positive integers, none of which is an integral power of a prime number. (1989 International Mathematical Olympiad)

Solution. Let the n consecutive integers be $x, x+1, \ldots, x+n-1$. Observe that if an integer has at least two distinct prime factors, then it cannot be a perfect power of a single prime. Thus, let $p_1, p_2, \ldots, p_{2n}$ be $2n$ distinct primes. It suffices to find an x such that each term is divisible by at least two distinct primes, which is the case when x satisfies the system

$$\begin{aligned} x &\equiv 0 \pmod{p_1p_2}, \\ x + 1 &\equiv 0 \pmod{p_3p_4}, \\ &\ldots, \\ x + n - 1 &\equiv 0 \pmod{p_{2n-1}p_{2n}}, \end{aligned}$$

or

$$\begin{aligned} x &\equiv 0 \pmod{p_1p_2}, \\ x &\equiv -1 \pmod{p_3p_4}, \\ &\ldots, \\ x &\equiv -(n-1) \pmod{p_{2n-1}p_{2n}}. \end{aligned}$$

The Chinese Remainder Theorem guarantees that this system has a solution.

Problems

1. Reduce the following numbers:

   (a) $2^{1000} \pmod 7$.

   (b) $3^{421} \pmod{13}$.

   (c) $11^{777} \pmod{21}$.

2. (a) Let p be a prime, and let a be a positive integer such that $a \equiv 1 \pmod{p-1}$. Show that $n^a - n \equiv 0 \pmod p$ for all integers n.

   (b) Show that $n^{13} - n \equiv 0 \pmod{2730}$ for all integers n.

3. A number is called **Carmichael** (or an **absolute pseudoprime**) if it is a pseudoprime to all bases. Show that 561 is Carmichael.

4. Let p be an odd prime, and let a be relatively prime to p. Show that $a^{(p-1)/2} \equiv \pm 1 \pmod p$. Note: Euler's Criterion states that $a^{(p-1)/2} \equiv 1 \pmod p$ if and only if $a \equiv x^2 \pmod p$ for some x relatively prime to p; in other words, a is a **quadratic residue**.

5. The number $85^9 - 21^9 + 6^9$ is divisible by an integer between 2000 and 3000. Compute that integer. (No calculators allowed!)

   (1991 American Regions Mathematics League)

   Hint: Try testing the number modulo small primes. The largest prime factor turns out to be 7.

6. Let $p > 5$ be a prime, and let $N = 111...1$, with $p - 1$ 1s. Show that N is divisible by p.

7. Explain what the following table has to do with the Chinese Remainder Theorem:

	0	1	2	3	4	5	6
0	0	8	16	24	4	12	20
1	21	1	9	17	25	5	13
2	14	22	2	10	18	26	6
3	7	15	23	3	11	19	27

8. Let p be a prime of the form $4k + 1$, and let $n = (p-1)/2$. Prove that $(n!)^2 + 1 \equiv 0 \pmod p$.

9. Find the four smallest positive integers n, such that $n^8 - n^2$ is <u>not</u> divisible by 504.

6 Pythagorean Triples

A special Diophantine equation is $a^2 + b^2 = c^2$. The solutions (a, b, c) in integers to this equation, such as $(3, 4, 5)$ and $(5, 12, 13)$, are called **Pythagorean triples**, because Pythagoras's Theorem states that this is the equation satisfied by the sides of a right triangle. Here, we derive a formula that gives all Pythagorean triples.

First, if a, b, and c have any common factors greater than 1, then we divide them out. For example, from $(6, 8, 10)$, we divide by 2 to get $(3, 4, 5)$. Note that if d divides any two of a, b, or c, then it divides the third: For example, if $d|a$ and $d|b$, then $d^2|a^2$ and $d^2|b^2$, so $d^2|c^2$, which implies that $d|c$.

Let $d = \gcd(a, b, c)$, and let $(a_1, b_1, c_1) = (a/d, b/d, c/d)$. Then the integers a_1, b_1, c_1 are pairwise relatively prime; in other words, $\gcd(a_1, b_1) = \gcd(a_1, c_1) = \gcd(b_1, c_1) = 1$.

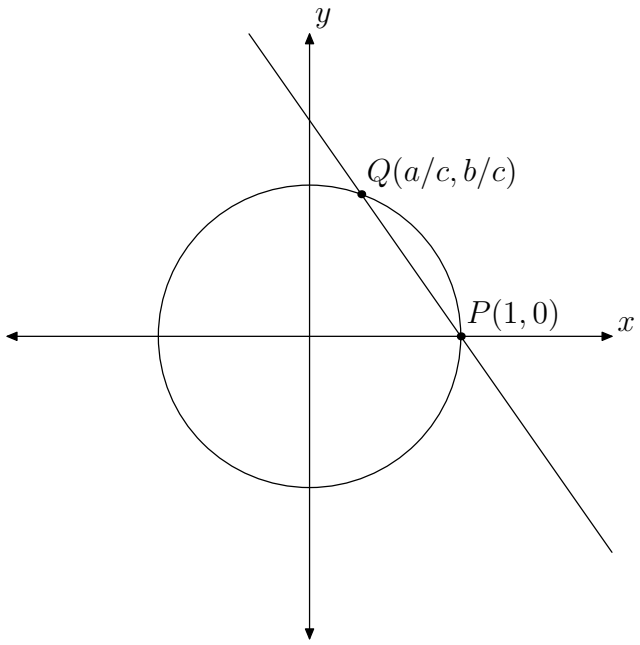
If both a and b are odd, then $c^2 = a^2 + b^2 \equiv 2 \pmod 4$, and 2 is not a square modulo 4, so that at least one of a or b must be even. Without loss of generality, assume that b is even. Then both a and c must be odd.

Since $a^2 + b^2 = c^2$, $c^2 - a^2 = (c + a)(c - a) = b^2$. By problem 5 of Chapter 1, $\gcd(c + a, c - a)$ is 1 or 2. Since $c + a$ and $c - a$ are both even, $\gcd(c + a, c - a) = 2$. Therefore, $(c + a)/2$ and $(c - a)/2$ are relatively prime. Their product is a perfect square, so that each is also a square, say $(c + a)/2 = m^2$ and $(c - a)/2 = n^2$, where m and n are relatively prime, which implies that $c = m^2 + n^2$ and $a = m^2 - n^2$. Finally, $b^2 = (c + a)(c - a) = 4m^2n^2$, so that $b = 2mn$.

Both m and n cannot be even; otherwise, a, b, and c would all be even, and we are assuming that they are relatively prime, and likewise if m and n are both odd. Hence, one of m and n must be even, and the other odd.

We began by factoring the gcd d out of the triple. Let us put this factor back in. Then the complete solution is given by $(a, b, c) = (d(m^2 - n^2), d(2mn), d(m^2 + n^2))$ and $(d(2mn), d(m^2 - n^2), d(m^2 + n^2))$, where $m \geq n$ are relatively prime positive integers, with one even and one odd, and d an arbitrary positive integer. We provide another solution, which uses geometry.

Again, assume that a, b, and c are relatively prime. We approach the problem using the coordinate plane. Let P be the point (1,0), and let Q be the point $(a/c, b/c)$. Assume that $Q \neq P$. Since $(a/c)^2 + (b/c)^2 = (a^2 + b^2)/c^2 = 1$, Q lies on the unit circle (the circle centred at $(0, 0)$ with radius 1).



Let m be the slope of the line PQ. Then the equation of the line PQ is $y = m(x-1)$. Furthermore, the point Q is in the first quadrant, so that the slope m is negative and is less than or equal to -1. Since the coordinates of P and Q are rational, so also is m. Let $m = -s/t$, where s and t are relatively prime positive integers, and $s \geq t$.

The point Q lies on the circle $x^2 + y^2 = 1$ and the line $y = m(x-1)$, and thus, is the solution to both equations:

$$\begin{aligned} x^2 + y^2 = x^2 + m^2(x-1)^2 = (m^2+1)x^2 - 2m^2x + m^2 = 1 \\ \Rightarrow \quad (m^2+1)x^2 - 2m^2x + m^2 - 1 = 0 \\ \Rightarrow \quad (x-1)[(m^2+1)x - (m^2-1)] = 0, \end{aligned}$$

so that $x = 1$ or $x = (m^2-1)/(m^2+1) = (s^2-t^2)/(s^2+t^2) = a/c$. The first solution corresponds to the point P, and the second to Q. For the second solution, $y = b/c = m(x-1) = (-s/t)[-2t^2/(s^2+t^2)] = 2st/(s^2+t^2)$. We conclude that $a = s^2 - t^2$, $b = 2st$, and $c = s^2 + t^2$. The solution then proceeds as before.

Problems

1. Show that $(3, 4, 5)$ is the only Pythagorean triple with three consecutive integers.

2. Let (a, b, c) be a Pythagorean triple. Show that $abc \equiv 0 \pmod{60}$.

3. Show that for any odd integer a, there exist integers b and c such that (a, b, c) is a Pythagorean triple.

4. Find a sequence of integers (u_n) for which

   (i) each u_n is a perfect square, and

   (ii) each partial sum $u_1 + u_2 + \cdots + u_n$ is a perfect square.

5. Show that if (a, b, c) is a Pythagorean triple, then for any positive integer n, there exist integers p and q such that (p, q, c^n) is also a Pythagorean triple.

6. Let (x, y, z) be a Pythagorean triple. Find t such that the following are also Pythagorean triples:

   (a) $(t - x, t - y, t + z)$.

   (b) $(t - x, t + y, t + z)$.

   (c) $(t + x, t - y, t + z)$.

7. Find all triples of positive integers (a, b, c) such that $a^2 + c^2 = 2b^2$. Hint: What is $(a + c)^2 + (a - c)^2$?

7 Pell's Equation

No perfect square can be exactly double another perfect square, since $\sqrt{2}$ is irrational, but there are some examples that come close, such as $17^2 = 289 = 2 \cdot 12^2 + 1$. This is a solution to an equation known as **Pell's Equation**, namely an equation of the form $x^2 - dy^2 = N$. Many problems reduce to an equation of this type, so that it will be helpful to know how to solve them.

If d is a perfect square, then $x^2 - dy^2$ factors. If d is negative, then there are a finite number of solutions. Thus, the most interesting cases are when d is positive and not a perfect square. Also, we limit our analysis to the cases $N = \pm 1$.

First, let us look at expressions of the form $a + b\sqrt{2}$, where a and b are integers. We will show that there is only one way to write down such a number; that is, if $a + b\sqrt{2} = c + d\sqrt{2}$, then $a = c$ and $b = d$. In other words, all the numbers of this form, such as $1 - \sqrt{2}$ and $2 + 3\sqrt{2}$, are different.

Assume that $a + b\sqrt{2} = c + d\sqrt{2}$, so that $a - c = (d - b)\sqrt{2}$. If $d \neq b$, then we can write

$$\sqrt{2} \;=\; \frac{a - c}{d - b}.$$

But $\sqrt{2}$ is irrational, a contradiction. Therefore, $b = d$, so that $a = c$. In particular, $a + b\sqrt{2} = c + d\sqrt{2}$ implies that $a - b\sqrt{2} = c - d\sqrt{2}$. This operation (of replacing $\sqrt{2}$ by $-\sqrt{2}$) is called **surd conjugation**. We implicitly perform this when we rationalize the denominator of a fraction; for example,

$$\frac{1}{5 + \sqrt{2}} \;=\; \frac{5 - \sqrt{2}}{(5 + \sqrt{2})(5 - \sqrt{2})} \;=\; \frac{5 - \sqrt{2}}{23}.$$

Now, let us look at an example of Pell's equation, the equation $x^2 - 2y^2 = 1$. Trying small numbers, we find that the two smallest solutions are $(1, 0)$ and $(3, 2)$.

There is a trick that generates all the solutions, and it is as follows. First, $3^2 - 2 \cdot 2^2 = 1$, which factors as $(3 + 2\sqrt{2})(3 - 2\sqrt{2}) = 1$.

Consider powers of $3 + 2\sqrt{2}$:

$$\begin{aligned}(3 + 2\sqrt{2})^2 &= (3 + 2\sqrt{2})(3 + 2\sqrt{2}) \\ &= 3 \cdot 3 + 3 \cdot 2\sqrt{2} + 2 \cdot 3\sqrt{2} + 2 \cdot 2 \cdot (\sqrt{2})^2 \\ &= 9 + 6\sqrt{2} + 6\sqrt{2} + 8 \\ &= 17 + 12\sqrt{2},\end{aligned}$$

and

$$\begin{aligned}(3 + 2\sqrt{2})^3 &= (3 + 2\sqrt{2})(17 + 12\sqrt{2}) \\ &= 51 + 36\sqrt{2} + 34\sqrt{2} + 48 \\ &= 99 + 70\sqrt{2}.\end{aligned}$$

Observe that $17^2 - 2 \cdot 12^2 = 1$ and $99^2 - 2 \cdot 70^2 = 1$. It turns out that all pairs generated this way are solutions, and we show why. Expanding,

$$\begin{aligned}&(3 + 2\sqrt{2})^n \\ &= 3^n + \binom{n}{1} 3^{n-1} \cdot 2\sqrt{2} + \binom{n}{2} 3^{n-2} \cdot (2\sqrt{2})^2 + \binom{n}{3} 3^{n-3} \cdot (2\sqrt{2})^3 + \cdots \\ &= 3^n + \binom{n}{2} 3^{n-2} \cdot 2^2 \cdot 2 + \cdots \\ &\quad + \left(\binom{n}{1} 3^{n-1} \cdot 2 + \binom{n}{3} 3^{n-3} \cdot 2^3 \cdot 2 + \cdots \right) \sqrt{2},\end{aligned}$$

so that, if

$$\begin{aligned}x_n &= 3^n + \binom{n}{2} 3^{n-2} \cdot 2^2 \cdot 2 + \cdots, \text{ and} \\ y_n &= \binom{n}{1} 3^{n-1} \cdot 2 + \binom{n}{3} 3^{n-3} \cdot 2^3 \cdot 2 + \cdots,\end{aligned}$$

then $x_n + y_n\sqrt{2} = (3 + 2\sqrt{2})^n$. But also

$$\begin{aligned}&x_n - y_n\sqrt{2} \\ &= 3^n + \binom{n}{2} 3^{n-2} \cdot 2^2 \cdot 2 + \cdots \\ &\quad - \left(\binom{n}{1} 3^{n-1} \cdot 2 + \binom{n}{3} 3^{n-3} \cdot 2^3 \cdot 2 + \cdots \right) \sqrt{2} \\ &= 3^n - \binom{n}{1} 3^{n-1} \cdot 2\sqrt{2} + \binom{n}{2} 3^{n-2} \cdot (2\sqrt{2})^2 - \binom{n}{3} 3^{n-3} \cdot (2\sqrt{2})^3 + \cdots \\ &= (3 - 2\sqrt{2})^n,\end{aligned}$$

which is really just another example of surd conjugation. Hence,

$$\begin{aligned}(x_n + y_n\sqrt{2})(x_n - y_n\sqrt{2}) &= x_n^2 - 2y_n^2 \\ &= (3+2\sqrt{2})^n(3-2\sqrt{2})^n \\ &= [(3+2\sqrt{2})(3-2\sqrt{2})]^n \\ &= 1^n = 1,\end{aligned}$$

so that (x_n, y_n) is also a solution to $x^2 - 2y^2 = 1$. Finally, we can solve for x_n and y_n from the simultaneous system of equations

$$\begin{aligned}x_n + y_n\sqrt{2} &= (3+2\sqrt{2})^n, \\ x_n - y_n\sqrt{2} &= (3-2\sqrt{2})^n.\end{aligned}$$

In general, it turns out that when $N = 1$, these are the only solutions, but we omit a proof here.

Solutions to $x^2 - dy^2 = 1$. If d is a non-negative, non-square integer, then the equation $x^2 - dy^2 = 1$ always has integer solutions. Letting (a, b) be the lowest positive integer solution to $x^2 - dy^2 = 1$, all positive integer solutions are of the form

$$(x_n, y_n) = \left(\frac{(a+b\sqrt{d})^n + (a-b\sqrt{d})^n}{2}, \frac{(a+b\sqrt{d})^n - (a-b\sqrt{d})^n}{2\sqrt{d}}\right). \qquad (*)$$

Furthermore, $x_n = 2ax_{n-1} - x_{n-2}$ and $y_n = 2ay_{n-1} - y_{n-2}$ for all $n \geq 2$.

For $N = -1$, the situation is similar. The equation $x^2 - dy^2 = -1$ might not have any solutions, but if it does, then let (a, b) be the lowest solution. Then taking (x_n, y_n) as in $(*)$, $x_n^2 - dy_n^2 = -1$ for n odd, and again these are all the solutions. It also turns out that $x_n^2 - dy_n^2 = 1$ for n even.

Example 6.1.

(a) Find all positive integers solutions to $x^2 - 2y^2 = 1$.

(b) Find all positive integers solutions to $x^2 - 2y^2 = -1$.

Solution. (a) The lowest solution is $(3, 2)$, so all solutions are given by

$$(x_n, y_n) = \left(\frac{(3+2\sqrt{2})^n + (3-2\sqrt{2})^n}{2}, \frac{(3+2\sqrt{2})^n - (3-2\sqrt{2})^n}{2\sqrt{2}}\right).$$

The first few solutions are $(3, 2)$, $(17, 12)$, and $(99, 70)$.

(b) The lowest solution is $(1, 1)$, so that all solutions are given by

$$(x_n, y_n) = \left(\frac{(1+\sqrt{2})^n + (1-\sqrt{2})^n}{2}, \frac{(1+\sqrt{2})^n - (1-\sqrt{2})^n}{2\sqrt{2}}\right),$$

where n is odd. The first few solutions are $(1,1)$, $(7,5)$, and $(41,29)$.

Example 6.2. A number is called **triangular** if it can be expressed as the sum $1+2+\cdots+n$ for some positive integer n. For example, 36 is triangular since $36 = 1+2+\cdots+8$, and it is also square since $36 = 6^2$. Prove that there are infinitely many numbers that are both triangular and square.

Solution. The sum $1+2+\cdots+n$ is equal to $n(n+1)/2$, so that we seek pairs (n,m) such that

$$\begin{aligned} n(n+1)/2 &= m^2 \\ \Rightarrow \quad n^2+n &= 2m^2 \\ \Rightarrow \quad 4n^2+4n &= 8m^2 \\ \Rightarrow \quad 4n^2+4n+1 &= (2n+1)^2 = 8m^2+1 \\ \Rightarrow \quad (2n+1)^2 - 8m^2 &= 1. \end{aligned}$$

We have used a technique called "completing the square", where we manipulate the expression to get a square in the variable n. Let $t = 2n+1$, so that $t^2 - 8m^2 = 1$, which is a Pell's equation. We find that the lowest solution is $(3,1)$, so that all solutions are given by

$$(t_k, m_k) \;=\; \left(\frac{(3+\sqrt{8})^k + (3-\sqrt{8})^k}{2}, \frac{(3+\sqrt{8})^k - (3-\sqrt{8})^k}{2\sqrt{8}} \right).$$

However, since $t = 2n+1$, we require t to be odd. We claim that t_k is odd for all k. First, $t_0 = 3$ and $t_1 = 17$. Also, $t_k = 6t_{k-1} - t_{k-2}$ for $k \geq 2$. Hence, $t_k \equiv t_{k-2} \pmod 2$. Since t_0 and t_1 are odd, t_k is odd for all k. Setting $n_k = (t_k - 1)/2$ gives an infinite number of values for n. The first few values of n are 1, 8, and 49.

Problems

1. Let x_n and y_n be as in $(*)$. Show that $x_n = 2ax_{n-1} - x_{n-2}$ and $y_n = 2ay_{n-1} - y_{n-2}$ for all $n \geq 2$.

2. Let n be a positive integer. Show that there exists a positive integer k such that
$$(\sqrt{2}-1)^n \;=\; \sqrt{k} - \sqrt{k-1}.$$

3. What is the smallest integer n, greater than one, 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, ..., a_n is defined to be
$$\left(\frac{a_1^2 + a_2^2 + \cdots + a_n^2}{n} \right)^{1/2}.$$

(1986 USAMO)

4. The area K of a triangle with sides a, b, and c is given by Heron's Formula:

$$K = \sqrt{s(s-a)(s-b)(s-c)},$$

where $s = (a+b+c)/2$, the semi-perimeter. Using this formula, it is easy to calculate that the area of the triangle with sides 3, 4, and 5 is 6, and the area of the triangle with sides 13, 14, and 15 is 84. Show that there are an infinite number of positive integers n such that the area of the triangle with sides $n-1$, n, and $n+1$ is also an integer.

8 Tips

Here are a few tips when it comes to solving problems in number theory. You may recognize a few from Chapter 1; they are good to remember.

- If a prime p divides the product ab, then p divides a or p divides b. More generally, if p divides the product $a_1 a_2 \cdots a_n$, then p must divide one of the factors a_i.
- For any integer n, n and $n+1$ are relatively prime. Hence, if a prime power p^k divides $n(n+1)$, then p^k divides either n or $n+1$. Also, if n divides m and $n+1$ divides m, then $n(n+1)$ divides m.
- More generally, if a and b are relatively prime integers, and a divides m and b divides m, then ab divides m. Even more generally, if a_1, a_2, ..., a_n are pairwise relatively prime integers, and a_i divides m for all i, then the product $a_1 a_2 \cdots a_n$ divides m. Hence, when trying to prove a congruence like $x \equiv 0 \pmod{n}$, it may help to split up the prime factors of n and deal with each individually. For example, to show that $x \equiv 0 \pmod{60}$, it suffices to show that $x \equiv 0 \pmod{4}$, $x \equiv 0 \pmod{3}$, and $x \equiv 0 \pmod{5}$.

  However, it is imperative that the a_i be pairwise relatively prime. For example, if $n \equiv 0 \pmod{4}$ and $n \equiv 0 \pmod{6}$, then we cannot conclude that $n \equiv 0 \pmod{24}$. (To see this, take $n = 12$).
- For many number theory problems, a key step can be finding the right modulus to work with. Sometimes it will be obvious, but other times it will not be, so do not be afraid to experiment. Always try small moduli such as 2, 3, and 4, and also ones that will simplify your expressions.
- For some problems, one must depart from modular theory and use basic principles. For example, you may have a congruence like $x \equiv 1 \pmod{2^n}$, but working within modular arithmetic limits you to working modulo 2^n. If this doesn't seem to be working, then try writing $x = 1 + k2^n$ and working with this equation. (A good example of this is selected problem 4.)
- If you are having trouble solving a problem, try solving a simpler problem; for example, look at a specific case, make an assumption, or change the numbers in the problem. Work with small numbers to develop a pattern.

9 Selected Problems

1. Show that, if n is a positive integer, $16^n + 10n - 1$ is divisible by 25.

   (1974 Descartes Waterloo Competition)

   Solution. By the binomial theorem,

   $$\begin{aligned} 16^n &= (1+15)^n \\ &= 1 + \binom{n}{1}15 + \binom{n}{2}15^2 + \cdots + \binom{n}{k}15^k + \cdots + 15^n \\ &\equiv 1 + 15n \pmod{25}, \end{aligned}$$

   since $\binom{n}{k}15^k = \binom{n}{k}3^k \cdot 5^k$ is divisible by 25 for $k \geq 2$. Hence,

   $$16^n + 10n - 1 \equiv 1 + 15n + 10n - 1 \equiv 25n \equiv 0 \pmod{25}.$$

   Induction will also work.

2. Determine the smallest integer k such that $60^n + k(71^n)$ is divisible by 1441 for all odd positive integers n.

   (1990 Descartes Waterloo Competition)

   Solution. The problem probably means "smallest positive integer k", because for any integer k that works, so does $k - 1441$.

   First, 1441 factors as $11 \cdot 131$. We consider these two prime factors separately. Since n is odd, $n = 2t + 1$ for some integer t. Then

   $$\begin{aligned} 60^n + k(71^n) &\equiv 5^{2t+1} + k \cdot 5^{2t+1} \\ &\equiv 5^{2t+1} \cdot (1+k) \pmod{11}, \end{aligned}$$

   so that $60^n + k(71^n)$ is divisible by 11 if and only if $k \equiv -1 \equiv 10 \pmod{11}$. Also,

   $$\begin{aligned} 60^n + k(71^n) &\equiv 60^{2t+1} + k \cdot (-60)^{2t+1} \\ &\equiv 60^{2t+1} + k \cdot (-1)^{2t+1} \cdot 60^{2t+1} \\ &\equiv 60^{2t+1} - k \cdot 60^{2t+1} \\ &\equiv 60^{2t+1} \cdot (1-k) \pmod{131}, \end{aligned}$$

   so that $60^n + k(71^n)$ is divisible by 131 if and only if $k \equiv 1 \pmod{131}$. Solving for k leads to $k \equiv 263 \pmod{1441}$. The smallest positive integer that satisfies this is clearly $k = 263$, which is the answer.

3. Call a number n **automorphic** if n^2 ends with the number n. For example, 76 is automorphic since $76^2 = 5776$. The following table lists automorphic numbers in four columns, such that, beginning with the second row, each is formed by appending a digit to the number above it on the left:

0	1	5	6
00	01	25	76
000	001	625	376
0000	0001	0625	9376
00000	00001	90625	09376
⋮	⋮	⋮	⋮

Show that the table can be extended indefinitely, and that these are the only automorphic numbers.

Solution. Let x_k be an automorphic number with k digits. Then we seek x_k such that $x_k^2 \equiv x_k \pmod{10^k}$, which becomes $x_k(x_k - 1) \equiv 0 \pmod{10^k}$.

If $k \geq 2$, then let x_{k-1} be the number formed by the last $k-1$ digits of x_k. Then $x_{k-1} \equiv x_k \pmod{10^{k-1}}$, so that $x_{k-1}^2 - x_{k-1} \equiv x_k^2 - x_k \equiv 0 \pmod{10^{k-1}}$. Hence, x_{k-1} is also automorphic. This says that any automorphic number with $k \geq 2$ digits must be formed by taking an automorphic number with $k-1$ digits, and appending another digit on the left.

Now, 10^k factors as $2^k \cdot 5^k$. Since x_k and $x_k - 1$ are relatively prime, 2^k must divide one of them, and the same goes for 5^k. This leads to four possible cases:

$$\begin{aligned}
&x \equiv 0 \pmod{2^k}, \quad x \equiv 0 \pmod{5^k}, \\
&x \equiv 1 \pmod{2^k}, \quad x \equiv 1 \pmod{5^k}, \\
&x \equiv 1 \pmod{2^k}, \quad x \equiv 0 \pmod{5^k}, \text{ and} \\
&x \equiv 0 \pmod{2^k}, \quad x \equiv 1 \pmod{5^k}.
\end{aligned}$$

By the Chinese Remainder Theorem, each of these four cases has a unique solution modulo 10^k. Therefore, for any k, there are exactly four automorphic numbers with k digits. (In fact, each of these four cases corresponds to a column above.) Hence, the table lists all automorphic numbers.

Additional Problem. Show that for any row, the sum of the numbers in the last two columns of the table is 1 greater than a power of 10.

4. Prove that if p is a prime and a and k are positive integers such that $p^k | (a-1)$, then $p^{n+k} | (a^{p^n} - 1)$.

Solution. We proceed by mathematical induction. The result is clear for $n = 0$. Assume that it is true for some integer $n = t$, so $p^{t+k} | (a^{p^t} - 1)$, so that $a^{p^t} = 1 + mp^{t+k}$ for some integer m. Then

$$\begin{aligned}
a^{p^{t+1}} &= (1 + mp^{t+k})^p \\
&= 1 + \binom{p}{1} mp^{t+k} + \binom{p}{2} (mp^{t+k})^2 + \cdots + (mp^{t+k})^p.
\end{aligned}$$

Recall that $\binom{p}{i} \equiv 0 \pmod{p}$ for $1 \leq i \leq p-1$, so in the sum above, all terms starting with the second are divisible by p^{t+k+1}. Therefore, $a^{p^{t+1}} \equiv 1 \pmod{p^{t+k+1}}$, and the result holds for $n = t+1$. By induction, the result holds for all n.

5. Find all positive integer solutions x, y, z of the equation $3^x + 4^y = 5^z$.

   (1991 International Mathematical Olympiad Short List)

   Solution. One evident solution is $(2, 2, 2)$. Taking both sides modulo 4, we obtain $(-1)^x \equiv 1 \pmod{4}$, so that x must be even. Taking both sides modulo 3, we obtain $1 \equiv (-1)^z \pmod{3}$, so that z must also be even. Thus, let $x = 2u$ and $z = 2v$, where u and v are positive integers, so that the equation becomes $3^{2u} + 2^{2y} = 5^{2v}$, which implies that $2^{2y} = 5^{2v} - 3^{2u} = (5^v + 3^u)(5^v - 3^u)$, so that both $5^v + 3^u$ and $5^v - 3^u$ are powers of 2.

   Thus, let $5^v + 3^u = 2^s$ and $5^v - 3^u = 2^t$, where s and t are non-negative integers, with $s > t$. Then $2 \cdot 5^v = 2^s + 2^t \Rightarrow 5^v = 2^{s-1} + 2^{t-1} = 2^{t-1}(2^{s-t}+1)$. The number 5^v cannot have any factors of 2, so that t must be equal to 1, and $5^v = 2^{s-t} + 1 = 2^{s-1} + 1$. This implies $5^v - 1 = 2^{s-1}$. If $s = 3$, then $v = 1$, which leads to $3^{2u} + 2^{2y} = 9^u + 4^y = 25$. The only solution to this is $u = 1$ and $y = 2$, which gives us $(x, y, z) = (2, 2, 2)$. Henceforth, assume that $s \geq 4$.

   Looking again at the equation $5^v - 1 = 2^{s-1}$, the left-hand side factors as

   $$5^v - 1 \;=\; (5-1)(5^{v-1} + 5^{v-2} + \cdots + 1) \;=\; 4 \cdot (5^{v-1} + 5^{v-2} + \cdots + 1),$$

   so that $5^{v-1} + 5^{v-2} + \cdots + 1 = 2^{s-3}$. The right-hand side is a power of 2 that is at least 2, so that it is even, giving that the left-hand side is even. Each term in the left-hand side is odd, and there are v of them, so that v must be even. Let $v = 2n$, where n is a positive integer. Then $5^{2n} - 1 = (5^n + 1)(5^n - 1) = 2^{s-1}$, so that both $5^n - 1$ and $5^n + 1$ are powers of 2. Note that $5^n + 1$ and $5^n - 1$ differ by 2, and the only powers of 2 that differ by 2 are 4 and 2, so that $5^n + 1 = 4$ and $5^n - 1 = 2$, which does not lead to any viable solutions. Therefore, the only solution is $(x, y, z) = (2, 2, 2)$.

6. Let n be an integer. Prove that if $2 + 2\sqrt{28n^2 + 1}$ is an integer then it is a square.

   (1969 Kürschák Competition)

   Solution. If $2 + 2\sqrt{28n^2 + 1}$ is an integer, then $28n^2 + 1$ must be a perfect square; moreover, it must be an odd perfect square. Thus, let $28n^2 + 1 = (2k+1)^2 = 4k^2 + 4k + 1 \Rightarrow 7n^2 = k(k+1)$. Since k and $k+1$ are relatively prime, any prime factor of $7n^2$ must divide either k or $k+1$, but not both. Hence, $k = 7a^2$ and $k + 1 = b^2$, or $k = a^2$ and $k + 1 = 7b^2$, for some integers a and b.

If $k = a^2$ and $k + 1 = 7b^2$, then $a^2 + 1 = 7b^2 \Rightarrow a^2 \equiv -1 \pmod 7$, which we can easily check is impossible. Therefore, $k = 7a^2$ and $k + 1 = b^2$. Then

$$2 + 2\sqrt{28n^2 + 1} \;=\; 2 + 2(2k + 1) \;=\; 4k + 4 \;=\; 4b^2 \;=\; (2b)^2.$$

7. Prove that the set of integers of the form $2^k - 3$ ($k = 2, 3, \ldots$) contains an infinite subset in which every two members are relatively prime.

   (1971 International Mathematical Olympiad)

   Solution. We construct the set inductively.

   Let $2 \le n_1 < n_2 < \cdots < n_k$ be k distinct positive integers such that any two members in the set $S = \{2^{n_1} - 3, 2^{n_2} - 3, \ldots, 2^{n_k} - 3\}$ are relatively prime.

   Let $p_1, p_2, \ldots, p_t$ be the primes that divide the members of this set, and let $n = (p_1 - 1)(p_2 - 1)\cdots(p_t - 1) + 1$. By Fermat's Little Theorem, for all $1 \le i \le t$,

$$\begin{aligned} 2^n - 3 &= 2 \cdot 2^{(p_1-1)(p_2-1)\cdots(p_t-1)} - 3 \\ &= 2 \cdot (2^{p_i-1})^{(p_1-1)\cdots(p_{i-1}-1)(p_{i+1}-1)\cdots(p_t-1)} - 3 \\ &\equiv 2 \cdot 1 - 3 \\ &\equiv -1 \pmod{p_i}. \end{aligned}$$

   Therefore, $2^n - 3$ is relatively prime to p_i for all i, so that $2^n - 3$ is relatively prime to every element in S. Add $2^n - 3$ to S. We repeat this construction to generate an infinite number of elements.

8. **Langford's Problem**. Let n be a positive integer. For certain n, it is possible to arrange two of each of the integers $1, 2, \ldots, n$, in some order, such that for each $1 \le i \le n$, there are i integers between the two appearances of the integer i. For example, for $n = 3$, the number 312132 is such an arrangement. Show that for $n \equiv 1$ or $n \equiv 2 \pmod 4$, there is no such arrangement.

   (Such arrangements exist for all other n, but this is very difficult to prove.)

   Solution. For $1 \le i \le n$, let a_i and b_i be the positions of the first and second appearances of i, respectively, so that, in our example 312132, $a_1 = 2$ and $b_1 = 4$. Then in general, $b_i - a_i = i + 1$, so that

$$\begin{aligned} \sum_{i=1}^{n} b_i - \sum_{i=1}^{n} a_i &= \sum_{i=1}^{n} (b_i - a_i) \\ &= \sum_{i=1}^{n} (i + 1) = \sum_{i=1}^{n} i + \sum_{i=1}^{n} 1 \\ &= \frac{n(n+1)}{2} + n \\ &= \frac{n^2 + 3n}{2}. \end{aligned}$$

Also, a_1, a_2, ..., a_n, b_1, b_2, ..., b_n, represent the integers 1, 2, ..., $2n$, so that

$$\sum_{i=1}^{n} a_i + \sum_{i=1}^{n} b_i \;=\; \sum_{i=1}^{2n} i \;=\; \frac{(2n)(2n+1)}{2} \;=\; 2n^2 + n.$$

Therefore,

$$\sum_{i=1}^{n} b_i \;=\; \frac{\frac{n^2+3n}{2} + 2n^2 + n}{2} \;=\; \frac{5n^2+5n}{4} \;=\; \frac{5n(n+1)}{4},$$

which is an integer if and only if $n \equiv 0$ or 3 (mod 4). This shows that n cannot be 1 or 2 modulo 4, but it alone does not prove that there is an arrangement if n is 0 or 3 modulo 4.

9. Let $p = 2m-1$, $q = 13m-1$, and $r = 15m-5$, where m is a positive integer. Note that if $m = 5$, p and q are perfect squares but r is not. If $m = 2$, q and r are perfect squares but p is not. Show that there is no single value of m for which each of p, q, and r is a perfect square.

   (1992 Euclid Waterloo Competition)

   Solution. It suffices to show that there is no value of m that makes both p and r perfect squares.

   Therefore, suppose that $p = 2m - 1 = x^2$ and $r = 15m - 5 = y^2$ for some integers m, x, and y. Then $m = (x^2+1)/2$, and substituting, $15 \cdot (x^2 + 1)/2 - 5 = y^2$, which becomes $15x^2 + 5 = 2y^2$. Taking both sides modulo 5, we get $0 \equiv 2y^2 \pmod 5$, which implies that $y^2 \equiv 0 \pmod 5$, which in turn implies that y is divisible by 5.

   Let $y = 5u$. Then $15x^2 + 5 = 2y^2 = 50u^2 \Rightarrow 3x^2 + 1 = 10u^2$. Again taking both sides modulo 5, we get $3x^2 + 1 \equiv 0 \Rightarrow 3x^2 \equiv -1 \equiv 4 \pmod 5$. Multiplying both sides by 2, which is the inverse of 3 modulo 5, we get $6x^2 \equiv x^2 \equiv 8 \equiv 3 \pmod 5$. However, it is easy to check that 3 is not a square modulo 5. Therefore, no such value of m can exist.

10. (a) For a positive integer n, let $s(n)$ denote the sum of the digits of n, as written in decimal notation. Show that $n \equiv s(n) \pmod 9$.

    (b) 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)

    (1975 International Mathematical Olympiad)

    Solution. (a) Let $a_k a_{k-1} \ldots a_1 a_0$ be the decimal digits of n, so that $n = 10^k a_k + 10^{k-1} a_{k-1} + \cdots + 10a_1 + a_0$. Then

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

(b) We seek $s(B)$. First, let us calculate $4444^{4444} \pmod 9$. We have that $4444 \equiv 7 \pmod 9$, so $4444^{4444} \equiv 7^{4444} \pmod 9$. Also, $4444 \equiv 4 \pmod 6$, so by Euler's Theorem, $7^{4444} \equiv 7^4 \pmod 9$. Hence,

$$4444^{4444} \equiv 7^4 \equiv 49^2 \equiv 4^2 \equiv 16 \equiv 7 \pmod 9.$$

By part (a), $s(B) \equiv 7 \pmod 9$. We should suspect that $s(B)$ is in fact 7; otherwise, $s(B)$ will be very difficult to calculate. We show that indeed $s(B) = 7$ by estimating A, then B, then $s(B)$.

First, $4444^{4444} < 10000^{4444} = (10^4)^{4444} = 10^{17776}$. Therefore, 4444^{4444} has at most 17776 digits, which means that A is at most $9 \cdot 17776 = 159984$.

Of the numbers among 1, 2, ..., 159984, the number with the greatest s-value is 99999, so that B is at most $9 \cdot 5 = 45$. Of the numbers among 1, 2, ..., 45, the number with the greatest s-value is 39, so that $s(B)$ is at most $3 + 9 = 12$. Since $s(B) \equiv 7 \pmod 9$, we conclude that $s(B)$ must be equal to 7.

11. Prove that if n is a non-negative integer, then $19 \times 8^n + 17$ is not a prime number

(1976 British Mathematical Olympiad)

Solution. Let $f(n) = 19 \cdot 8^n + 17$. Our strategy is to find integers that divide $f(n)$ for certain values of n.

For example, taking $f(n)$ modulo 3, we find that $f(n) = 19 \cdot 8^n + 17 \equiv (-1)^n + 2 \pmod 3$. This is 0 when n is even, so that we may assume that n is odd, say $n = 2t + 1$.

Then $f(n) = f(2t+1) = 19 \cdot 8^{2t+1} + 17 = 152 \cdot 64^t + 17$. Taking this modulo 5, it becomes $f(n) \equiv 2 \cdot (-1)^t + 2 \pmod 5$. This is 0 when t is odd, so that we may assume that t is even, say $t = 2u$.

Then $f(n) = f(4u+1) = 19 \cdot 8^{4u+1} + 17 = 152 \cdot 4096^u + 17$. Since $4096 \equiv 1 \pmod{13}$, $f(4u+1) \equiv 152 + 17 \equiv 169 \equiv 0 \pmod{13}$. To summarize,

if n is even, then $f(n) \equiv 0 \pmod 3$ (and $f(n) > 3$),

if n is of the form $4t + 3$, or $n \equiv 3 \pmod 4$, then $f(n) \equiv 0 \pmod 5$ (and $f(n) > 5$),

and if n is of the form $4t + 1$, or $n \equiv 1 \pmod 4$, then $f(n) \equiv 0 \pmod{13}$ (and $f(n) > 13$).

Therefore, $f(n)$ can never be a prime.

10 Solutions to Chapter Problems

Chapter 1

1. (a) 26. (b) 180. (c) Since $n|7n$, $\gcd(n, 7n) = n$.

2. Since $\gcd(m, n) = 3$, both m and n are multiples of 3. Let $a = m/3$ and $b = n/3$, so that $\gcd(a, b) = \gcd(m/3, n/3) = \gcd(m, n)/3 = 1$, and $\operatorname{lcm}(a, b) = \operatorname{lcm}(m/3, n/3) = \operatorname{lcm}(m, n)/3 = 12$. In other words, a and b are relatively prime numbers whose product is 12. The only possibilities for (a, b) are $(1, 12)$, $(3, 4)$, $(4, 3)$, and $(12, 1)$. (The pair $(2, 6)$ is not a solution since $\gcd(2, 6) = 2$.) The corresponding solutions for (m, n) are $(3, 36)$, $(9, 12)$, $(12, 9)$, and $(36, 3)$.

3. (a) Let $d = \gcd(n, n+1)$, so that d divides both n and $n+1$. Then d divides their difference $(n + 1) - n = 1$. Hence, $d = 1$.

   (b) The statement is false. For example, 6 divides $8 \cdot 9 = 72$, but 6 does not divide 8 nor 9.

4. If $a|n$ and $b|n$, then $\operatorname{lcm}(a, b)|n$. But $\operatorname{lcm}(a, b) = ab/\gcd(a, b) = ab$. Therefore, $ab|n$.

5. Let $d = \gcd(x + y, x - y)$, so that $d|(x + y)$ and $d|(x - y)$. Then d divides $(x+y)+(x-y) = 2x$, and d divides $(x+y)-(x-y) = 2y$, so that d divides $\gcd(2x, 2y) = 2\gcd(x, y) = 2$. Hence, $d = 1$ or 2. We leave it to the reader to check that both values are possible.

6. Multiplying both sides by $\gcd(a, b)$, the equation becomes

$$\begin{aligned} a\gcd(a,b) + b\gcd(a,b) &= \gcd(a,b)^2 + \gcd(a,b)\cdot\operatorname{lcm}(a,b) \\ &= \gcd(a,b)^2 + ab \\ \Rightarrow \quad \gcd(a,b)^2 - a\gcd(a,b) - b\gcd(a,b) + ab &= 0 \\ \Rightarrow \quad (\gcd(a,b) - a)(\gcd(a,b) - b) &= 0. \end{aligned}$$

   Therefore, $\gcd(a, b) = a$ or $\gcd(a, b) = b$. If $\gcd(a, b) = a$, then a divides b, and if $\gcd(a, b) = b$, then b divides a.

Chapter 2

1. (a) First, observe that $x^2 - y^2$ factors as $(x + y)(x - y)$. Hence, both $x + y$ and $x - y$ must be factors of 84, whose product is 84, with $x + y \geq x - y$. We list all the possibilities:

$x+y$	$x-y$	x	y
84	1	–	–
42	2	22	20
28	3	–	–
21	4	–	–
14	6	10	4
12	7	–	–

Note that we only get a valid solution when $x+y$ and $x-y$ are both even or both odd. Thus, the only solutions for (x, y) are $(22, 20)$ and $(10, 4)$.

(b) We have that $x^2 - y^2 = (x+y)(x-y) = a^3$. If we take $x+y = a^2$ and $x-y = a$, then $2x = a^2 + a = a(a+1)$. Since either a or $a+1$ must be even, $a(a+1)$ is even, so that $x = a(a+1)/2$ is an integer. Similarly, $y = a(a-1)/2$ is an integer. Thus, the equation $x^2 - y^2 = a^3$ always has a solution, namely $(x, y) = (a(a+1)/2, a(a-1)/2)$.

(c) The values of n are 2, 6, 10, 14, and 18.

2. (a) For $360n$ to be a perfect square, each prime must appear an even number of times in the prime factorization. The integer 360 factors as $2^3 \cdot 3^2 \cdot 5$, so that n must have at least one factor of 2 and one factor of 5. Hence, the smallest value of n is $2 \cdot 5 = 10$.

   (b) For $2n$ to be a perfect square, each prime must appear an even number of times in the prime factorization of $2n$, and for $9n$ to be a perfect cube, each prime must appear in multiples of 3 in the prime factorization of $9n$. We can assume that the only prime factors of n are 2 and 3.

   The number of factors of 2 in n must be odd and a multiple of 3. It is easy to check that the smallest such number is 3. The number of factors of 3 in n must be even and two less (or one more) than a multiple of 3. It is similarly found that the lowest such number is 4. Hence, the value of n we seek is $2^3 \cdot 3^4 = 648$.

3. Let n^2 be an odd perfect square. If n is even, then n^2 is as well, so that n must be odd, meaning that $n = 2m+1$ for some integer m. Then

$$n^2 \;=\; 4m^2 + 4m + 1 \;=\; 8 \cdot \frac{m(m+1)}{2} + 1.$$

   Since either m or $m+1$ must be even, $m(m+1)/2$ must be an integer. Setting $k = m(m+1)/2$, we see that n^2 is of the form $8k+1$.

4. Let a and b be the man's and grandson's age this year, respectively. Then we seek a and b such that $b|a$, $(b+1)|(a+1)$, $(b+2)|(a+2)$, $(b+3)|(a+3)$, $(b+4)|(a+4)$, and $(b+5)|(a+5)$.

   Let us consider the following problem: Given a positive integer n, which values of m satisfy $n|m$ and $(n+1)|(m+1)$? Clearly $m = n$ is one value. Let m' be another value, so that $n|m'$ and $(n+1)|(m'+1)$. Since $n|m$ and $n|m'$, n divides their difference $m'-m$. Similarly, $(n+1)|(m+1)$ and $(n+1)|(m'+1)$, so that $n+1$ divides their difference $(m'+1)-(m+1) = m'-m$, so that both n and $n+1$ divide $m'-m$.

   But n and $n+1$ are relatively prime, so that $n(n+1)$ divides $m'-m$, or $m'-m$ is a multiple of $n(n+1)$. Thus, for example, for $n = 4$, $m = 4$ is one solution, and the next solutions are $4 + 4 \cdot 5 = 24$, $24 + 4 \cdot 5 = 64$, etc. We

list all such values of n and m below, where $n < m < 100$:

n	m
1	$3, 5, 7, 9, \ldots$
2	$8, 14, 20, 26, \ldots$
3	$15, 27, 39, 51, \ldots$
4	$24, 64, 84$
5	$35, 65, 95$
6	$48, 90$
7	63
8	80
9	99

Going back to our original problem, we seek a value of a that is in the m column in one row, such that $a + 1$ is in the next row, $a + 2$ is in the row under that, and so on, until $a + 4$. Looking at the rows for $n = 4$, 5, and 6, we see that $a + 4$ must be equal to 65, which gives us $a = 61$ and $b = 1$. We check that these values work.

Chapter 3

1.

$+$	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

$\cdot$	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

2. (a) Looking at the first few powers of 2 modulo 11, we find that $2^{10} = 1024 \equiv 1 \pmod{11}$. Therefore, $2^{500} = (2^{10})^{50} \equiv 1^{50} \equiv 1 \pmod{11}$.

   (b) Since $7 \equiv -6 \pmod{13}$, $6^{99} + 7^{99} \equiv 6^{99} + (-6)^{99} \equiv 6^{99} + (-1)^{99} \cdot 6^{99} \equiv 6^{99} - 6^{99} \equiv 0 \pmod{13}$.

   (c) Each of the terms is odd, and there are n terms, so that the sum is congruent to $1 + 1 + \cdots + 1 = n \pmod{2}$. Hence, $1 + 3 + 5 + \cdots + (2n - 1)$ is 0 modulo 2 if n is even, and 1 modulo 2 if n is odd.

3. Algebraically, *aabb* equals

$$1000a + 100a + 10b + b \;=\; 1100a + 11b \;\equiv\; 0 \pmod{11},$$

   so that the square is divisible by 11. Since 11 is prime, the square is divisible by $11^2 = 121$. Checking all square multiples of 121 up to 10000, we find that the only one that fits the pattern is $121 \cdot 8^2 = 88^2 = 7744$. Therefore, the only solution is $a = 7$ and $b = 4$.

4. The product of 2^n-1 and 2^n+1 is $(2^n)^2-1 = 4^n-1$, and $4^n-1 \equiv 1^n-1 \equiv 0 \pmod 3$. Since 3 is prime, 3 must divide one of 2^n-1 and 2^n+1.

   You may have noticed that 2^n-1 is divisible by 3 when n is even, and 2^n+1 is divisible by 3 when n is odd. Prove this.

5. Since $10 = 2 \cdot 5$, we consider modulo 2 and 5 separately.

   For all $n \geq 1$,

   $$1^n + 8^n - 3^n - 6^n \equiv 1^n + 0 - 1^n - 0 \equiv 0 \pmod 2,$$

   so that the expression is divisible by 2. Similarly,

   $$1^n + 8^n - 3^n - 6^n \equiv 1^n + 3^n - 3^n - 1^n \equiv 0 \pmod 5,$$

   so that the expression is divisible by 5. Hence, it is divisible by 10.

6. There are many counter-examples. For example, $1 \equiv 4 \pmod 3$, but $2^1 \equiv 2 \pmod 3$ and $2^4 \equiv 1 \pmod 3$. This shows that exponentiation does not necessarily preserve congruence.

7. (a) We check the squares modulo 7:

n	0	1	2	3	4	5	6
n^2	0	1	4	9	16	25	36
$n^2 \pmod 7$	0	1	4	2	2	4	1

   Thus, the squares in modulo 7 are 0, 1, 2, and 4.

   (b) Checking all possible sums of two squares modulo 7, as derived in part (a), we find that the only sum that gives 0 is $0 + 0$. Hence, both squares must be divisible by 7.

8. Each summand contains 997 factors, so that

   $$\begin{aligned}
   &1 \cdot 3 \cdot 5 \cdots 1993 + 2 \cdot 4 \cdot 6 \cdots 1994 \\
   &\equiv 1 \cdot 3 \cdot 5 \cdots 1993 + (-1993) \cdot (-1991) \cdot (-1989) \cdots (-1) \\
   &\equiv 1 \cdot 3 \cdot 5 \cdots 1993 + (-1)^{997} \cdot 1 \cdot 3 \cdot 5 \cdots 1993 \\
   &\equiv 1 \cdot 3 \cdot 5 \cdots 1993 - 1 \cdot 3 \cdot 5 \cdots 1993 \\
   &\equiv 0 \pmod{1995}.
   \end{aligned}$$

9. We must show that for any prime $p > 3$, there exists an integer n such that $p = \sqrt{24n+1}$. Squaring both sides, this becomes $p^2 = 24n + 1$. Thus, the problem becomes showing that $p^2 \equiv 1 \pmod{24}$, or $p^2 - 1 \equiv 0 \pmod{24}$. The number 24 factors as $3 \cdot 8$, so that we consider these factors separately.

   Since $p > 3$, p is congruent to 1 or 2 modulo 3. In either case, $p^2 \equiv 1 \pmod 3$, so that $p^2 - 1 \equiv 0 \pmod 3$.

Also, since p^2 is an odd perfect square, by problem 3 at the end of Chapter 2, $p^2 \equiv 1 \pmod 8$, or $p^2 - 1 \equiv 0 \pmod 8$. Hence, $p^2 - 1 \equiv 0 \pmod{24}$.

Here is another solution: In Problem 11, it is shown that every prime $p \geq 5$ is of the form $6k \pm 1$, where k is a positive integer. Then

$$p^2 \;=\; 36k^2 \pm 12k + 1 \;=\; 12k(3k \pm 1) + 1.$$

If k is even, then $12k$ is a multiple of 24, and if k is odd, then $3k \pm 1$ is even, so that $12(3k \pm 1)$ is a multiple of 24. Hence, in either case, $p^2 \equiv 1 \pmod{24}$.

10. The roots of the quadratic are given by the quadratic formula:

$$\frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

For these roots to be rational, $b^2 - 4ac$ must be a perfect square. We claim that $b^2 - 4ac$ cannot be a perfect square, thus showing that the roots cannot be rational.

Suppose that $b^2 - 4ac$ is a perfect square, say d^2.
First, note that $b^2 - 4ac \equiv b^2 \equiv 1 \pmod 2$, since b is odd. By problem 3 of Chapter 2, odd squares are congruent to 1 modulo 8, so that

$$d^2 \;\equiv\; b^2 \;\equiv\; 1 \pmod 8 \Rightarrow b^2 - d^2 \;=\; 4ac \;\equiv\; 0 \pmod 8.$$

This implies that $4ac = 8n$ for some integer n, from which we get $ac = 2n$. But a and c are odd, so that their product ac is odd as well, a contradiction. Therefore, $b^2 - 4ac$ cannot be a perfect square.

11. (a) The numbers in the columns are of the form $6k+1$, $6k+2$, $6k+3$, $6k+4$, $6k+5$, and $6k+6$ (or $6k$), respectively.

All numbers of the form $6k$, $6k+2$, and $6k+4$ are divisible by 2, and thus, cannot be primes greater than 2. Also, all numbers of the form $6k+3$ are divisible by 3, and thus, cannot be primes greater than 3. This leaves only the forms $6k+1$ and $6k+5$, which represent the first and fifth columns, respectively.

(b) We follow Example 3.7. Suppose that there are a finite number of primes of the form $6k+5$, say $p_1, p_2, \ldots, p_n$. Let $N = 6p_1p_2 \cdots p_n - 1$.

Now, N is divisible neither by 2 nor 3, since $N \equiv -1 \pmod 6$. Therefore, by part (a), N is only divisible by primes of the form $6k+1$ or $6k+5$. However, N cannot be divisible by any prime of the form $6k+5$ either, since $N \equiv -1 \pmod p$ for any such prime p.

Hence, N is divisible only by primes of the form $6k+1$, which implies that $N \equiv 1 \pmod 6$. But $N \equiv -1 \pmod 6$, a contradiction. Therefore, there are an infinite number of primes of the form $6k+5$.

12. If n is odd, then $n = 2m + 1$ for some non-negative integer m. Then we can take $x = m + 1$ and $y = m$.

    If n is divisible by 4, so that $n = 4m$ for some integer m, then we can take $x = m + 1$ and $y = m - 1$.

    This leaves the case that n is twice an odd number. Then $n = 2(2m + 1) = 4m + 2$ for some m, so that $n \equiv 2 \pmod 4$. But x^2 is 0 or 1 modulo 4, so that the only possible values of $x^2 - y^2$ are -1, 0, or 1 modulo 4, and the equation $x^2 - y^2 = n$ cannot have any solutions.
    Therefore, the equation $x^2 - y^2 = n$ has no solutions in non-negative integers exactly when $n \equiv 2 \pmod 4$, which agrees with our answer to problem 1(c) of Chapter 2.

Chapter 4

1. (a) 3. (b) 21.

2. (a) $(-6 + 3t, 6 - 2t)$. (b) $(40 + 7t, -60 - 11t)$.

3. The problem is equivalent to showing that the congruence $31x \equiv 174 \pmod{1000}$ has a solution. Since $\gcd(31, 174) = 1$, the congruence does have a solution. (We are only asked to show that there is such a multiple, not find it explicitly.)

4. Let $u = a/\gcd(a, b)$ and $v = b/\gcd(a, b)$. Then $a/\gcd(a, b) \cdot x + b/\gcd(a, b) \cdot y = ux + vy = 1$. Hence, x and y are relatively prime.

5. We show that $S = T$ by showing that every ordered pair in S is also in T, and vice-versa.

   Let $(3i + 4j + 5k, 8i - j + 4k)$ be an ordered pair in S, where i, j, and k are integers. To show that this ordered pair lies in T, we must find integers m and n such that $m = 3i + 4j + 5k$ and $5m + 7n = 8i - j + 4k$. We can simply solve for n, to get

$$\begin{aligned} n &= \frac{8i - j + 4k - 5m}{7} \\ &= \frac{8i - j + 4k - 5(3i + 4j + 5k)}{7} \\ &= \frac{-7i - 21j - 21k}{7} \\ &= -i - 3j - 3k, \end{aligned}$$

   which is an integer.

   Now, let $(m, 5m + 7n)$ be an ordered pair in T, where m and n are integers. To show that this ordered pair lies in S, we must find integers i, j, and k such that $3i + 4j + 5k = m$ and $8i - j + 4k = 5m + 7n$. Multiplying the second equation by 4, we get $32i - 4j + 16k = 20m + 28n$. Adding this to

the first equation, we get $35i + 21k = 21m + 28n$. Dividing by 7, we get $5i + 3k = 3m + 4n$.

Since $4 = 2 \cdot 5 - 2 \cdot 3$, we can take $i = 2n$ and $k = m - 2n$. Thus,

$$5i + 3k \;=\; 5(2n) + 3(m - 2n) \;=\; 3m + 4n.$$

Then, solving for j in the equation $8i - j + 4k = 5m + 7n$, we get

$$j \;=\; 8i + 4k - 5m - 7n = 8(2n) + 4(m - 2n) - 5m - 7n \;=\; n - m.$$

6. Assume that $am^3 + bm^2 + cm + d \equiv 0 \pmod 5$. If $m \equiv 0 \pmod 5$, then $d \equiv 0 \pmod 5$, but we are given that d is not divisible by 5, so that m is relatively prime to 5, and $m^{-1} \pmod 5$ exists. Let $n \equiv m^{-1} \pmod 5$, so that $am^3n^3 + bm^2n^3 + cmn^3 + dn^3 \equiv a + bn + cn^2 + dn^3 \equiv 0 \pmod 5$.

7. Suppose that $a^{-1} \pmod m$ exists. Multiply the congruence $ab \equiv 0 \pmod m$ by a^{-1} to get $b \equiv 0 \pmod m$, but b is non-zero modulo m, a contradiction.

Chapter 5

1. (a) By FLT, $2^6 \equiv 1 \pmod 7$, so that

$$2^{1000} = 2^{6 \cdot 166 + 4} = (2^6)^{166} \cdot 2^4 \equiv 1 \cdot 16 \equiv 2 \pmod 7.$$

(b) By FLT, $3^{12} \equiv 1 \pmod{13}$.
Since $421 \equiv 1 \pmod{12}$, $3^{421} \equiv 3^1 \equiv 3 \pmod{13}$.

(c) By Euler's Theorem, $11^{\phi(21)} = 11^{12} \equiv 1 \pmod{21}$.
Since $777 \equiv 9 \pmod{12}$,

$$\begin{aligned} 11^{777} &\equiv 11^9 \equiv (11^2)^4 \cdot 11 \\ &\equiv 121^4 \cdot 11 \equiv 16^4 \cdot 11 \\ &\equiv 256^2 \cdot 11 \equiv 4^2 \cdot 11 \\ &\equiv 176 \equiv 8 \pmod{21}. \end{aligned}$$

2. (a) Since $a \equiv 1 \pmod{p-1}$, $a = 1 + k(p-1)$ for some integer k.
If $n \equiv 0 \pmod p$, then $n^a - n \equiv 0 \pmod p$. Otherwise, n is relatively prime to p, so that, by FLT, $n^{p-1} \equiv 1 \pmod p$, and

$$\begin{aligned} n^a &= n^{1+k(p-1)} = n \cdot (n^{p-1})^k \\ &\equiv n \cdot 1 \equiv n \pmod p. \end{aligned}$$

Therefore, $n^a - n \equiv 0 \pmod p$ for all n.

(b) First, 2730 factors as $2 \cdot 3 \cdot 5 \cdot 7 \cdot 13$. Note that for each of the values $p = 2$, 3, 5, 7, and 13, p is prime, and $p - 1$ divides $12 = 13 - 1$, so that, by part (a), $n^{13} \equiv n \pmod p$ for all n. Hence, $n^{13} \equiv n \pmod{2 \cdot 3 \cdot 5 \cdot 7 \cdot 13}$.

3. First, 561 factors as $3 \cdot 11 \cdot 17$. Hence, it suffices to show that for each of the values $p = 3$, 11, and 17, $n^{561} \equiv n \pmod{p}$ for all n.

   We find that for each value of p, $p - 1$ divides $560 = 561 - 1$, so that, by part (a) of problem 2, $n^{561} - n \equiv 0 \pmod{3 \cdot 11 \cdot 17}$ for all n.

4. Let $x = a^{(p-1)/2}$. Then by FLT, $x^2 = a^{p-1} \equiv 1 \pmod{p}$, which implies that $x^2 - 1 = (x-1)(x+1) \equiv 0 \pmod{p}$. Therefore, $x \equiv 1$ or $-1 \pmod{p}$.

5. Let $N = 85^9 - 21^9 + 6^9$. Note that $85 \equiv 21 \pmod{64}$,
   and $6^9 = 2^9 \cdot 3^9 \equiv 0 \pmod{64}$, so that $N \equiv 21^9 - 21^9 + 0 \equiv 0 \pmod{64}$.

   Also, $N \equiv 0^9 - 1^9 + 1^9 \equiv 0 \pmod{5}$, and $N \equiv 1 - 0 + (-1)^9 \equiv 0 \pmod{7}$, and $64 \cdot 5 \cdot 7 = 2240$, so that this is the factor we seek.

6. The number $9N$ is a number with $p - 1$ 9s, so that $9N = 10^{p-1} - 1$. The prime p is greater than 5, so that p is relatively prime to 10. By FLT, $10^{p-1} - 1 \equiv 0 \pmod{p}$, so that $9N \equiv 0 \pmod{p}$. Since $p > 3$, 9 is relatively prime to p, which implies that $N \equiv 0 \pmod{p}$.

7. The table acts as a look-up table. Let a be an integer between 0 and 3, and b an integer between 0 and 6. Then the solution to the system

$$\begin{aligned} x &\equiv a \pmod{4}, \\ x &\equiv b \pmod{7}, \end{aligned}$$

   is the entry in the row headed by a and column headed by b.

8. Writing it out,

$$\begin{aligned} (n!)^2 &= 1 \cdot 2 \cdots n \cdot n \cdot (n-1) \cdots 1 \\ &\equiv 1 \cdot 2 \cdots n \cdot (n-p) \cdot (n-p-1) \cdots (1-p) \\ &\equiv 1 \cdot 2 \cdots n \cdot (-1) \cdot (p-n) \cdot (-1) \cdot (p-n+1) \cdots (-1) \cdot (p-1) \\ &\equiv (-1)^n \cdot 1 \cdot 2 \cdots n \cdot (n+1) \cdot (n+2) \cdots (2n) \pmod{p}, \end{aligned}$$

   since $p = 2n + 1$. Also, $p = 4k + 1$ for some integer k, so that $2n + 1 = 4k+1 \Rightarrow n = 2k$, so that n is even, and the expression becomes $1 \cdot (p-1)! \equiv -1 \pmod{p}$, by Wilson's Theorem. Hence, $(n!)^2 \equiv -1 \pmod{p}$.

9. First, 504 factors as $2^3 \cdot 3^2 \cdot 7$.

   If $n \equiv 0 \pmod{3}$, then $3|n$, so that $9|(n^8 - n^2)$. Otherwise, n is relatively prime to 3, and thus, relatively prime to 9.
   By Euler's Theorem, $n^{\phi(9)} = n^6 \equiv 1 \pmod{9}$, so that $n^8 \equiv n^2 \pmod{9}$. Therefore, $n^8 - n^2 \equiv 0 \pmod{9}$ for all n.

   By FLT, $n^7 \equiv n \pmod{7}$ for all n, so that $n^8 - n^2 \equiv 0 \pmod{7}$ for all n.

   Finally, let us list $n^8 - n^2 \pmod{8}$:

n	0	1	2	3	4	5	6	7
$n^8 - n^2 \pmod{8}$	0	0	4	0	0	0	4	0

Hence, $n^8 - n^2$ is not divisible by 8, and by extension 504, yielding if $n \equiv 2$ or 6 (mod 8), or equivalently, $n \equiv 2 \pmod 4$. The first four such numbers are 2, 6, 10, and 14.

Chapter 6

1. Let the triple be $(n-1, n, n+1)$, so that $(n-1)^2 + n^2 = (n+1)^2$, or $n^2 - 2n + 1 + n^2 = n^2 + 2n + 1 \Rightarrow n^2 = 4n \Rightarrow n = 0$ or $n = 4$. We reject $n = 0$, so that the only solution is indeed (3,4,5).

2. Since (a, b, c) is Pythagorean triple, we have

$$abc = k(m^2 - n^2) \cdot 2kmn \cdot k(m^2 + n^2) = k^3 \cdot 2mn(m^4 - n^4)$$

for some integers k, m, and n. It suffices to show that

$$2mn(m^4 - n^4) \equiv 0 \pmod{60},$$

or equivalently, that $mn(m^4 - n^4) \equiv 0 \pmod{30}$.

By Example 3.3, $m^5 \equiv m \pmod{30}$ and $n^5 \equiv n \pmod{30}$. Hence,

$$mn(m^4 - n^4) \equiv m^5 n - mn^5 \equiv mn - mn \equiv 0 \pmod{30}.$$

3. Take $b = (a^2 - 1)/2$ and $c = (a^2 + 1)/2$.
Then $a^2 + b^2 = a^2 + (a^4 - 2a^2 + 1)/4 = (a^4 + 2a^2 + 1)/4 = c^2$.

4. We construct the sequence inductively. First, let $a_1 = 3$ and $a_2 = 4$, so that $a_1^2 + a_2^2 = 25$, which is a perfect square. By problem 3, if we take $a_3 = (25 - 1)/2 = 12$, then $a_1^2 + a_2^2 + a_3^2 = 169 = 13^2$ is a perfect square. In general, assume that we have constructed the values a_1, a_2, ..., a_{n-1}, and $a_1^2 + a_2^2 + \cdots + a_{n-1}^2$ is an odd perfect square, say x^2. Taking our cue from problem 3, let $a_n = (x^2 - 1)/2$. Since x^2 is an odd square, $x^2 \equiv 1 \pmod 8$, so that a_n is even. Also,

$$\begin{aligned} a_1^2 + a_2^2 + \cdots + a_{n-1}^2 + a_n^2 &= x^2 + \left(\frac{x^2 - 1}{2}\right)^2 = x^2 + \frac{x^4 - 2x^2 + 1}{4} \\ &= \frac{x^4 + 2x^2 + 1}{4} = \left(\frac{x^2 + 1}{2}\right)^2 \\ &= (a_n + 1)^2, \end{aligned}$$

which is also an odd perfect square. Thus, $a_1^2 + a_2^2 + \cdots + a_n^2$ is a perfect square for all n. Finally, we can set $u_n = a_n^2$ for all n.

5. Let S be the set of integers that can be expressed as the sum of two perfect squares. Since $c^2 = a^2 + b^2$, c is in S. Two general elements in S are $x^2 + y^2$ and $z^2 + w^2$. Their product is

$$\begin{aligned} (x^2 + y^2)(z^2 + w^2) &= x^2 z^2 + y^2 w^2 + x^2 w^2 + y^2 z^2 \\ &= x^2 z^2 + 2xzyw + y^2 w^2 + x^2 w^2 - 2xwyz + y^2 z^2 \\ &= (xz - yw)^2 + (xw - yz)^2, \end{aligned}$$

so that the product of any two elements in S is also in S. Hence, $c \cdot c = c^2$ is in S, $c \cdot c^2$ is in S, and so on, producing all powers of c.

6. (a) For $(t-x, t-y, t+z)$ to be a Pythagorean triple, we must have

$$\begin{aligned} & (t-x)^2 + (t-y)^2 = (t+z)^2 \\ \Rightarrow \quad & t^2 - 2tx + x^2 + t^2 - 2ty + y^2 = t^2 + 2tz + z^2 \\ \Rightarrow \quad & t^2 - 2xt - 2yt - 2zt = z^2 - x^2 - y^2 = 0 \\ \Rightarrow \quad & t(t - 2x - 2y - 2z) = 0. \end{aligned}$$

The only values are then $t = 0$, which we reject, and $t = 2x + 2y + 2z$.

(b) Proceeding as in part (a), we get $t = 2x + 2z - 2y$.

(c) Proceeding as in part (a), we get $t = 2y + 2z - 2x$.

We can use these formulas to derive new triples from previous ones. For example, applying (a), (b), and (c) to the triple $(3, 4, 5)$, we get $(21, 20, 29)$, $(5, 12, 13)$, and $(15, 8, 17)$.

7. Assume that $c < a$. Let $p = (a + c)/2$ and $q = (a - c)/2$.
Then $p^2 + q^2 = b^2$, so that $(p, q, b) = (k(m^2 - n^2), k(2mn), k(m^2 + n^2))$, or $(p, q, b) = (k(2mn), k(m^2 - n^2), k(m^2 + n^2))$, for some integers k, m, and n, such that one of m, n is odd and the other even, and $m \geq n$.

Then we have $a = p + q = k(m^2 + 2mn - n^2)$, and
$c = q - p = \pm k(m^2 - 2mn - n^2)$. Thus, the complete solution is

$$(a, b, c) \;=\; (k(m^2 + 2mn - n^2), k(m^2 + n^2), \pm k(m^2 - 2mn - n^2)).$$

Chapter 7

1. Let $u = a + b\sqrt{d}$ and $v = a - b\sqrt{d}$, so that,
from $(*)$, $x_n = (u^n + v^n)/2$ and $y_n = (u^n - v^n)/(2\sqrt{d})$.

Then $u + v = 2a$ and $uv = a^2 - db^2 = 1$, so that u and v are the roots of the quadratic

$$(t - u)(t - v) = t^2 - (u + v)t + uv = t^2 - 2at + 1,$$

which means that $u^2 - 2au + 1 = v^2 - 2av + 1 = 0$, so that
$u^n - 2au^{n-1} + u^{n-2} = v^n - 2av^{n-1} + v^{n-2} = 0$. Adding these, we get

$$\begin{aligned} & u^n + v^n - 2a(u^{n-1} + v^{n-1}) + (u^{n-2} + v^{n-2}) = 0 \\ \Rightarrow \quad & \frac{u^n + v^n}{2} - 2a \cdot \frac{u^{n-1} + v^{n-1}}{2} + \frac{u^{n-2} + v^{n-2}}{2} = 0 \\ & \Rightarrow \quad x_n - 2ax_{n-1} + x_{n-2} = 0, \end{aligned}$$

which shows that $x_n = 2ax_{n-1} - x_{n-2}$. The relation for y_n is similarly proven.

2. Let x_n and y_n be integers defined by $(\sqrt{2}-1)^n = x_n\sqrt{2} - y_n$.
Then $(\sqrt{2}+1)^n = x_n\sqrt{2} + y_n$, so that

$$\begin{aligned} 2x_n^2 - y_n^2 &= (x_n\sqrt{2} - y_n)(x_n\sqrt{2} + y_n) \\ &= (\sqrt{2}-1)^n(\sqrt{2}+1)^n \\ &= [(\sqrt{2}-1)(\sqrt{2}+1)]^n \\ &= 1^n = 1. \end{aligned}$$

Now $(\sqrt{2}-1)^n = x_n\sqrt{2} - y_n = \sqrt{2x_n^2} - \sqrt{y_n^2} = \sqrt{2x_n^2} - \sqrt{2x_n^2 - 1}$, showing that we can take $k = 2x_n^2$.

3. The sum of the first n perfect squares is

$$\frac{n(n+1)(2n+1)}{6}.$$

Hence, we seek pairs (n, m) such that

$$\begin{aligned} \frac{(n+1)(2n+1)}{6} &= m^2 \\ \Rightarrow \quad 2n^2 + 3n + 1 &= 6m^2 \\ \Rightarrow \quad 16n^2 + 24n + 8 &= 48m^2 \\ \Rightarrow \quad 16n^2 + 24n + 9 = (4n+3)^2 &= 48m^2 + 1 \\ \Rightarrow \quad (4n+3)^2 - 48m^2 &= 1. \end{aligned}$$

Let $t = 4n + 3$, so that our equation becomes $t^2 - 48m^2 = 1$. The smallest solution to this is $(7, 1)$, so that all solutions are given by

$$(t_k, m_k) \;=\; \left(\frac{(7+\sqrt{48})^k + (7-\sqrt{48})^k}{2}, \frac{(7+\sqrt{48})^k - (7-\sqrt{48})^k}{2\sqrt{48}} \right).$$

The first few solutions are $(7, 1)$, $(97, 14)$, and $(1351, 195)$. For n to be an integer, we require $t \equiv 3 \pmod 4$, which we have for $t_3 = 1351$. Hence, the smallest n is $(1351 - 3)/4 = 337$. (We ignore $t_1 = 7$ since n must be greater than 1.)

4. If $a = n - 1$, $b = n$, and $c = n + 1$, then $s = 3n/2$, so that

$$\begin{aligned} K &= \sqrt{\frac{3n}{2} \cdot \frac{n+2}{2} \cdot \frac{n}{2} \cdot \frac{n-2}{2}} \\ &= \sqrt{\frac{3n^2(n^2-4)}{16}} \\ &= \frac{n}{4} \cdot \sqrt{3(n^2-4)}. \end{aligned}$$

If n is odd, then $3n^2(n^2-4)$ is also odd, and K cannot be an integer, so that n must be even. Let $n = 2x$, so that

$$K \;=\; \frac{2x}{4} \cdot \sqrt{3(4x^2-4)} \;=\; x\sqrt{3(x^2-1)}.$$

We require $3(x^2-1)$ to be a perfect square, say y^2. Then y must be divisible by 3; let $y = 3m$. Then $3(x^2-1) = y^2 = 9m^2$, so that $x^2 - 1 = 3m^2$, or $x^2 - 3m^2 = 1$. The smallest solution to this is $(2, 1)$, so that all solutions are given by

$$(x_t, m_t) \;=\; \left(\frac{(2+\sqrt{3})^t + (2-\sqrt{3})^t}{2}, \frac{(2+\sqrt{3})^t - (2-\sqrt{3})^t}{2\sqrt{3}} \right).$$

Taking $n_t = 2x_t$ gives an infinite number of values for n.

11 Practice Problems

1. If 332, 520, and 755 are each divided by d (an integer greater than one), the remainder r is the same. Determine the value of $d + r$.

   (1992 Euclid Waterloo Competition)

2. A table consists of eleven columns. Reading across the first row of the table we find the numbers 1991, 1992, 1993, ..., 2000, 2001. In the other rows, each entry in the table is 13 greater than the entry above it, and the table continues indefinitely. If a vertical column is chosen at random, then what is the probability of that column containing a perfect square?

   (1991 Fermat Waterloo Competition)

3. Let abc be a three-digit integer. Show that $abc + bca + cab$ is divisible by 37.

4. Let n be an odd positive integer. Show that $5^n + 11^n + 17^n$ is divisible by 33.

5. Prove that there are no integers solutions to the equation $x^2 - 17y^2 = 11$.

6. Let S_1 be the sequence of positive integers 1, 2, 3, 4, ... For all $n \geq 1$, we obtain the sequence S_{n+1} from S_n by adding 1 to every term that is divisible by n (and leaving the other terms unchanged), so that S_2 is the sequence 2, 3, 4, 5, ..., and S_3 is 3, 3, 5, 5, ... Find all n for which the first $n-1$ terms of S_n are equal to n.

7. Show that for all positive integers n, $6^{2n+1} + 5^{n+2}$ is divisible by 31.

8. Find the greatest common divisor of all numbers in the sequence $\{13^n + 6 : n = 2, 4, 6, \ldots\}$.

9. Show that for any seven positive integers, there exists a pair whose sum or difference is divisible by 10.

10. A school orders 99 textbooks. When the bill comes, the first and last digits are obscured, and reads $\$-,112.7-$. What are the missing digits?

11. A point is called a **lattice point** if both of its coordinates are integers. Find the shortest distance between two lattice points on the line $2x + 3y = 10$.

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

13. Prove that $p^{p-1} + 1989$ is composite for every prime p.

    (Mathematical Mayhem J26)

14. Show that $n^{22} \equiv n^2 \pmod{100}$ for all integers n.

    (Mathematical Mayhem H89)

15. Let S be the set of all positive integers that are of the form $2^a 3^b$; that is, all positive integers that only have factors of two and three (and 1 is in S; $a = b = 0$). Calculate the sum of the reciprocals of the elements of S:

$$\frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \frac{1}{6} + \frac{1}{9} + \frac{1}{12} + \cdots .$$

    (Mathematical Mayhem H116)

16. Let $x > y$, where x and y are positive integers. Show that if x and y satisfy the equation $x^2 - y^2 = 1995$, then neither x nor y can be a multiple of 3.

    (Mathematical Mayhem H163)

17. The system of equations $(a + 1)(b - 5) = N$ and $(a - 1)(b + 5) = N$ has integer solutions for $N = 1995$. Determine the next smallest positive integer greater than 1995 that also yields integer solutions (a, b).

    (Mathematical Mayhem H189)

18. Let n be a positive integer, and let $a_1, a_2, \ldots, a_n$ be an arithmetic sequence, such that the common difference is relatively prime to n. Show that exactly one of the terms of the sequence is divisible by n.

19. Find a set of four consecutive integers such that the smallest is a multiple of 5, the next smallest is a multiple of 7, the third is a multiple of 9 and the largest is a multiple of 11.

    (1978 Euclid Waterloo Competition)

20. Let $a_1, a_2, \ldots, a_{15}$ be a permutation of the integers $1, 2, \ldots, 15$. Show that

$$(a_1 - 1)(a_2 - 2) \cdots (a_{15} - 15)$$

    must be even.

21. Determine all positive integer solutions $(x_0, x_1, \ldots, x_n)$ of the system

$$\begin{aligned} 4x_1 &= 5x_0 + 1, \\ 4x_2 &= 5x_1 + 1, \\ &\ldots, \\ 4x_n &= 5x_{n-1} + 1. \end{aligned}$$

22. (a) Show that n^4 is congruent to 0 or 1 modulo 16 for all integers n.

    (b) Determine all non-negative integral solutions $(n_1, n_2, \ldots, n_{14})$, if any, apart from permutations, of the Diophantine equation

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

    (1979 USAMO)

23. The tens digit of a perfect square is 7. What is the units digit?

24. Show that there do not exist integers x, y, and z, such that $x^2 + y^2 + z^2 = 1991$.

25. (a) A sequence has n^{th} term $a_n = 2^n k + 1$, where k is a fixed integer. Show that there is no prime, p, such that every term of the sequence is divisible by p.

    (b) For the sequence defined in part (a), show that there are no two primes, p and q, such that every term of the sequence is divisible by either p or q.

    (1991 Euclid Waterloo Competition)

26. A palindromic number is a number that reads the same forwards and back, such as 14541 and 2882. Show that a palindromic number with an even number of digits is divisible by 11.

27. Prove that no positive integer ending in the two digits 99 can be a perfect square.

28. Find three positive integers m, n, and p such that $5^m + 9^n = 7p^2$, or show that no such integers exist.

29. Determine the least value of c such that the equation $7x + 11y = c$ has exactly 13 solutions (x, y) in positive integers.

30. (a) Show that among any 5 numbers, it is possible to choose 3 whose sum is divisible by 3.

    (b) Show that among any 17 numbers, it is possible to choose 5 whose sum is divisible by 5.

31. Solve the congruence $x^3 \equiv 53 \pmod{60}$.

32. Let p be a prime. Prove that p is the smallest prime dividing $(p-1)!+1$.

33. Determine all integer solutions (x, y) to the Diophantine equation

$$x^3 - y^3 \;=\; 2xy + 8.$$

(International Mathematical Olympiad Proposal)

34. Let a_1, a_2, a_3, $\ldots$, a_n be the numbers 1, 2, 3, $\ldots$, n written in any order. Prove that $\sum_{i=1}^{n} |a_i - i|$ is always even.

(1988 Descartes Waterloo Competition)

35. Let n be a positive integer. Let b be the last digit of 2^n, and a the remaining digits, so that $2^n = 10a + b$. Show that the product $ab \equiv 0 \pmod 3$.

36. Prove that there are no prime numbers in the infinite sequence 10001, 100010001, 1000100010001, ...

37. Prove that if $pn+1$ is the square of an integer, where n is an integer and p is a prime, then $n+1$ can be written as the sum of p squares.

(Mathematical Mayhem H135)

38. Let n be a positive integer, such that both $2n+1$ and $3n+1$ are squares. Show that 40 divides n.

39. For which digits a, b is $ababab1$ a perfect cube?

(Mathematical Mayhem A28)

40. Define a sequence (a_n) by $a_1 = 7$ and $a_n = 7^{a_{n-1}}$ for $n \geq 2$. Find the units digit of a_n for all n.

41. Find the integer n such that $133^5 + 110^5 + 84^5 + 27^5 = n^5$.

(1991 Japanese Mathematics Olympiad)

42. Let $f(x)$ be a polynomial in x with integer coefficients, such that $f(-3) = f(4) = 2$. Show that there is no integer a such that $f(a) = 5$.

43. Let N be a positive integer whose units digit is k. If the k is moved to the front of the number, the new number is k times the original number.
    (a) Prove that N can be found for every k, $0 < k < 10$.
    (b) Show that if $k = 4$, then all solutions are given by

$$\left\lfloor \frac{102564 \cdot 10^{6n}}{999999} \right\rfloor,$$

where $\lfloor x \rfloor$ is the greatest integer function, and n is a positive integer.

(Mathematical Mayhem S39)

44. Let $u_1, u_2, u_3, \ldots$, be a sequence of integers satisfying the recurrence relation $u_{n+2} = u_{n+1}^2 - u_n$. Suppose $u_1 = 39$ and $u_2 = 45$. Prove that 1986 divides infinitely many terms of the sequence.

    (1986 CMO)

45. The sequence (p_n) is defined as follows: $p_1 = 2$, and for $n \geq 2$, p_n is the greatest prime factor of $p_1 p_2 \cdots p_{n-1} + 1$. Prove that 5 is not a term in this sequence.

46. Let p be a prime and a and b be positive integers. Show that

$$\binom{pa}{pb} \equiv \binom{a}{b} \pmod{p}.$$

47. Let a be an integer, such that $\gcd(a, 3) = 1$ and $x^2 \equiv a \pmod 3$ has a solution in x. Prove that $x^2 \equiv a \pmod{3^k}$ has a solution for all positive integers k.

48. In Camelot, there are 45 chameleons; 13 are grey, 15 are brown, and 17 are crimson. When two of different colours meet, they both change to the third colour. Can all the chameleons eventually turn the same colour?

    (Tournament of Towns)

49. An $a \times b$ rectangle can be tiled with $n \times 1$ rectangular tiles. Show that a or b is divisible by n.

50. Each of the numbers $x_1, x_2, \ldots, x_n$ is equal to 1 or -1, such that

$$x_1x_2x_3x_4 + x_2x_3x_4x_5 + \cdots + x_nx_1x_2x_3 = 0.$$

    Show that n is divisible by 4.

51. Show that $n^4 + 3n^2 + 1$ is not a perfect square for any positive integer n.

    (1982 International Mathematical Olympiad Proposal)

52. Let p be a prime such that $p \equiv 3 \pmod 4$. Show that if x and y are positive integers such that $x^2 + y^2 \equiv 0 \pmod p$, then $x \equiv y \equiv 0 \pmod p$.

53. Show that if p and q are positive integers such that

$$\frac{p}{q} = 1 + \frac{1}{2} - \frac{2}{3} + \frac{1}{4} + \frac{1}{5} - \frac{2}{6} + \frac{1}{7} + \frac{1}{8} - \frac{2}{9} + \cdots + \frac{1}{478} + \frac{1}{479} - \frac{2}{480},$$

    then p is divisible by 641.

    (1989 Descartes Waterloo Competition)

54. Let n be a positive integer. Show that $2^{2^n} + 2^{2^{n-1}} + 1$ has at least n prime factors.

55. Show that if x and y are positive integers such that $x^2 + y^2 - x$ is divisible by $2xy$, then x is a perfect square.

    (1991 British Mathematical Olympiad)

56. Let F_n denote the n^{th} Fibonacci number.
    Show that $F_{n+p} \equiv F_n + F_{n-p} \pmod{p}$ for all primes p.

57. Find all triples of positive integers (x, y, z) such that $8^x + 15^y = 17^z$.

    (1991 International Mathematical Olympiad Correspondence Course)

58. Let m and n be positive integers, such that for every positive integer k, $\gcd(11k - 1, m) = \gcd(11k - 1, n)$. Prove that for some integer l, $m = 11^l n$.

59. A sequence of primes (a_n) satisfies $a_n = 2a_{n-1} \pm 1$. Show that the sequence must be finite.

60. Let $a_1, a_2, \ldots, a_n$ be a permutation of the numbers $1, 2, \ldots, n$. Can the n numbers $b_i = a_1 + a_2 + \cdots + a_i$ for $i = 1, 2, \ldots, n$ ever be a complete residue system modulo n? (By this we mean can these numbers have all possible remainders represented when divided by n).

    (Mathematical Mayhem H192)

61. Show that there do not exist rationals x and y such that $x^2 + xy + y^2 = 2$.

62. Find all pairs of rational numbers (x, y) such that $(x + y\sqrt{3})^2 = 4 + 3\sqrt{3}$.

63. Let $n > 1$ be an odd integer. Show that the equation

$$\frac{1}{x} + \frac{1}{y} = \frac{4}{n}$$

    has solutions in positive integers x and y if and only if n has a prime factor of the form $4k - 1$.

12 Hints to Practice Problems

1. The given implies $332 \equiv 520 \equiv 755 \pmod{d}$. Use this to find d, and then r.
2. Work modulo 13.
3. Express the numbers algebraically. For example, $abc = 100a + 10b + c$.
4. Work modulo 3 and 11.
5. Work modulo 17.
6. Write down the sequences S_n for the first few n, say 10 of them, and list which n satisfy the condition. Guess and prove your answer.
7. Work modulo 31.

8. Guess what the gcd is from the first few terms, and then prove your guess.

9. Work modulo 10. Play with congruence classes, and use the Pigeonhole Principle.

10. Work modulo 9 and 11.

11. Find all solutions, or simply draw a graph.

12. Work modulo 8, 3, and 5.

13. Work modulo 2.

14. Work modulo 4 and 25.

15. Show that S is equal to the product of the geometric series

$$\frac{1}{1}+\frac{1}{2}+\frac{1}{2^2}+\cdots, \text{ and } \frac{1}{1}+\frac{1}{3}+\frac{1}{3^2}+\cdots.$$

16. Factor the equation, and see what solutions are possible.

17. Expand both equations, and get a relationship between a and b. The answer is 2200.

18. Let a be the first term and d the common difference. Then the k^{th} term is $a+kd$, $1 \le k \le n$. We wish to solve $a+kd \equiv 0 \pmod{n}$ in k.

19. First, write out the congruences. Then follow Example 5.9.

20. Suppose that the product is odd. Then every factor of the product must be odd. Take their sum modulo 2.

21. Add 4 to each side of each equation.

22. (a) Work modulo 16, or divide into the cases where n is even and n is odd.

    (b) Use part (a).

23. Let n be such that the tens digit of n^2 is 7. We can assume that n has only two digits (since these are the only ones we are interested in). Let $n = 10a+b$. Then $n^2 = 100a^2+20ab+b^2 \equiv 20ab+b^2 \pmod{100}$. The tens digit of n^2 is then the last digit of $2ab$, plus any carry-over of b^2, which is the tens digit of b^2, so this carry-over must be odd. Find b.

24. Work modulo 8.

25. (a) If there exists such a prime p, then in particular it divides a_1 and a_2. Show that this implies $k \equiv 0 \pmod{p}$, which implies $a_1 \equiv 1 \pmod{p}$, a contradiction.

    (b) By your argument in part (a), no prime can divide both a_1 and a_2. Reason similarly that no prime can divide both a_1 and a_2. Hence, if such primes p and q exist, then letting p divide a_1, q must divide a_2, and p must divide a_3. Use the fact that p divides both a_1 and a_3 to arrive at a contradiction.

26. Express the number algebraically.
For example, $2882 = 2 \cdot 10^3 + 8 \cdot 10^2 + 8 \cdot 10 + 2$.

27. Suppose that $n^2 \equiv 99 \pmod{100}$. Work with the units digit of n, and then the tens digit.

28. Work modulo 4.

29. Estimate what the value of c must be, and then refine your estimate.
Draw a graph.

30. Use the Pigeonhole Principle.

31. Solve the congruence in modulo 4, 3, and 5 first, and then combine into modulo 60.

32. By Wilson's Theorem, p divides $(p-1)! + 1$. Let q be a prime less than p. Show that $(p-1)! \equiv 0 \pmod{q}$.

33. Let $t = x - y$, and substitute (for x or y).

34. You can remove the absolute value signs by showing that $|x| \equiv x \pmod{2}$ for any integer x.

35. Check the values of a and b modulo 3 for small values of n, and find and prove a pattern.

36. Find an explicit formula for the n^{th} term.

37. Let $pn + 1 = x^2$. This implies that $x^2 \equiv 1 \pmod{p}$, which, further, implies that $x \equiv 1$ or $-1 \pmod{p}$. If $x \equiv 1 \pmod{p}$, then let $x = 1 + pk$, so that $pn + 1 = (1 + pk)^2 = 1 + 2pk + p^2k^2 \Rightarrow n + 1 = 1 + 2k + pk^2$. Massage this expression to get a sum of p squares, and consider the case $x \equiv -1 \pmod{p}$ similarly.

38. Work modulo 8 and 5.

39. Let $n^3 = ababab1$. Show that $n \equiv 1 \pmod{30}$. Find bounds on n.

40. As seen in Example 3.2, the units digit of 7^a is governed by a modulo 4.

41. By Example 5.2, $n^5 \equiv n \pmod{30}$ for all n.
Hence, $n \equiv 133 + 110 + 84 + 27 \equiv 24 \pmod{30}$. Find bounds on n.

42. Let $g(x) = f(x) - 2$. Then $g(-3) = g(4) = 0$, so $g(x) = (x+3)(x-4)q(x)$ for some polynomial $q(x)$, also with integer coefficients. If $f(a) = 5$, then $g(5) = 3 = (a+3)(a-4)q(a)$. What can these factors on the right be, numerically?

43. (b) Let M be the number N without the units digit 4. Then the relation looks like $M4 \cdot 4 = 4M$. This implies that the last digit of M is the last digit of $4 \cdot 4$, which is 6. Then the last two digits of M are the last two digits of $64 \cdot 4$, which are 56. Continue this process to derive all digits of M. Use the same process to find the answers to part (a).

44. First, $u_3 = 1986 \equiv 0 \pmod{1986}$. Next, consider the sequence of pairs $(u_n, u_{n-1}) \pmod{1986}$. Show that by the Pigeonhole Principle, if some pair of congruence classes appears, then it must eventually appear again.
Then consider the first repetition: the smallest p and q, such that $p < q$, $u_p \equiv u_q \pmod{1986}$, and $u_{p-1} \equiv u_{q-1} \pmod{1986}$.

45. Suppose that $p_n = 5$ for some n. Then $p_1 p_2 \cdots p_{n-1} + 1 = 2^a 3^b 5^c$ for some integers a, b, and c.

46. The symbol $\binom{pa}{pb}$ stands the coefficient of x^{pb} in $(1+x)^{pa}$.
Also, $(1+x)^{pa} \equiv (1+x^p)^a \pmod{p}$.

47. Use induction. More explicitly, use the solution for k to construct a solution for $k+1$.

48. Let g and b be the number of grey and brown chameleons, respectively. Consider what happens to $g - b \pmod 3$ during any meeting.

49. You may have seen the problem about tiling a modified chessboard with dominoes. The trick is to realize that every domino covers one white square and one black square.

    Therefore, for this problem, colour every square one of n colours, so that every $n \times 1$ tile covers a square of each colour, and show that if neither a nor b is divisible by n, then not all colours have the same number of squares.

50. Work modulo 2 to show that n is even, so $n = 2k$ for some n. Then consider the product of the terms to show that k is even.

51. Observe that $n^4 + 3n^2 + 1 = (n^2+1)^2 + n^2$.

52. Use Example 5.4.

53. Replace each fraction of the form $-\frac{2}{3k}$ by $\frac{1-3}{3k} = \frac{1}{3k} - \frac{1}{k}$. Simplify, and then combine appropriately. Remember that 641 is a prime number.

54. Let $f(n) = 2^{2^n} + 2^{2^{n-1}} + 1$. Show that $f(n-1)$ divides $f(n)$, and then use induction.

55. Show that if p^{2n+1} divides x, then p^{2n+2} divides x.

56. Using the Fibonacci relation, show that

$$\begin{aligned} F_{n+p} &= F_{n+p-1} + F_{n+p-2} \\ &= F_{n+p-2} + 2F_{n+p-3} + F_{n+p-4} \\ &\cdots \\ &= F_n + \binom{p}{1} F_{n-1} + \binom{p}{2} F_{n-2} + \cdots + F_{n-p}. \end{aligned}$$

57. Follow selected problem 6.

58. It suffices to show that if $p^e|m$, where p is a prime not equal to 11, then $p^e|n$. Find a k such that $11k - 1 \equiv 0 \pmod{p^e}$.

59. Show that if the plus sign holds for one n, then it holds for all n. Similarly for the minus sign. Then find a formula for a_n.

60. Try small values of n. Rule out the case n odd. Some experimentation is required.

61. Work modulo 3.

62. Try surd conjugation.

63. Rearrange the equation to get $(4x - n)(4y - n) = n^2$, and work modulo 4.

13 Problems for Investigation

Here is a selection of interesting problems that you may explore on your own.

- For Pell's equation $x^2 - dy^2 = 1$, we described everything except how to find the lowest solution (a, b). There is a systematic way using **continued fractions**. Find out how.

  Also, what are the solutions to other Pellian equations, such as $x^2 - 3y^2 = 2$? What about $3x^2 - 2y^2 = 1$?

- **Pascal's Triangle** is the triangular array formed by writing a 1, and then in each new row, writing the sum of the two numbers above it:

$$\begin{array}{ccccccccccc}
 & & & & & 1 & & & & & \\
 & & & & 1 & & 1 & & & & \\
 & & & 1 & & 2 & & 1 & & & \\
 & & 1 & & 3 & & 3 & & 1 & & \\
 & 1 & & 4 & & 6 & & 4 & & 1 & \\
1 & & 5 & & 10 & & 10 & & 5 & & 1 \\
 & & & & & \vdots & & & & &
\end{array}$$

  The k^{th} entry in the n^{th} row is $\binom{n}{k}$, as in Chapter 5. Let us reduce all entries modulo 2:

$$\begin{array}{ccccccccccc}
 & & & & & 1 & & & & & \\
 & & & & 1 & & 1 & & & & \\
 & & & 1 & & 0 & & 1 & & & \\
 & & 1 & & 1 & & 1 & & 1 & & \\
 & 1 & & 0 & & 0 & & 0 & & 1 & \\
1 & & 1 & & 0 & & 0 & & 1 & & 1 \\
 & & & & & \vdots & & & & &
\end{array}$$

You may notice a pattern already. What do you get if you extend this table, say another 10 rows? 20? What happens if you replace 2 by other numbers? (While you're at it, you may wish to look up a fractal called a "Sierpiński gasket".)

- The number 142857 exhibits the following remarkable property:

$$\begin{aligned} 1 \cdot 142857 &= 142857, \\ 2 \cdot 142857 &= 285714, \\ 3 \cdot 142857 &= 428571, \\ 4 \cdot 142857 &= 571428, \\ 5 \cdot 142857 &= 714285, \\ 6 \cdot 142857 &= 857142. \end{aligned}$$

Each of these multiples is a cyclic permutation of the original number. What other numbers exhibit this property? (Hint: What is $7 \cdot 142857$?) Also, note that $142 + 857 = 999$ and $14 + 28 + 57 = 99$.

- Some primes can be written as the sum of two perfect squares, such as $13 = 2^2 + 3^2$ and $29 = 2^2 + 5^2$. Which primes can be written as the sum of two squares? Which numbers can be written as the sum of two squares?

14 References

If you are interested in reading more about number theory or problem solving, we recommend the following books:

Number Theory

- A. Adler & J. Coury, *The Theory of Numbers*, Jones and Bartlett.
- E. Barbeau, *Pell's Equation*, Springer-Verlag.
- E. Barbeau, *Power Play*, Mathematical Association of America.
- G. E. Andrews, *Number Theory*, Dover Publications.
- I. Niven, H. Zuckerman & H. Montgomery, *An Introduction to the Theory of Numbers*, John Wiley & Sons.
- J. Roberts, *The Lure of the Integers*, Mathematical Association of America.

Problem Solving

- E. Barbeau, W.O. Moser, M.S. Klamkim, *Five Hundred Mathematical Challenges*, Mathematical Association of America.
- A. Engel, *Problem-Solving Strategies*, Springer-Verlag.
- L. Larson, *Problem-Solving Through Problems*, Springer-Verlag.
- E. Lozansky, C. Rousseau, *Winning Solutions*, Springer-Verlag.

ATOM

A Taste Of Mathematics / Aime-T-On les Mathématiques

1. Edward J. Barbeau
   Mathematical Olympiads' Correspondence Program (*1995-1996*)
2. Bruce L.R. Shawyer
   Algebra — Intermediate Methods
3. Peter I. Booth, John Grant McLoughlin, and Bruce L.R. Shawyer
   Problems for Mathematics Leagues
4. Edward J. Barbeau, and Bruce L.R. Shawyer
   Inequalities
5. Richard Hoshino, and John Grant McLoughlin
   Combinatorial Explorations
6. Peter I. Booth, John Grant McLoughlin, and Bruce L.R. Shawyer
   Problems for Mathematics Leagues — II
7. Jim Totten
   Problems of the Week
8. Peter I. Booth, John Grant McLoughlin, and Bruce L.R. Shawyer
   Problems for Mathematics Leagues — III
9. Edward J. Barbeau
   The CAUT Problems

Cost per volume (including shipping and handling charges):
Regular Rate $15.00 — CMS Member's Rate $12.00 (excluding taxes).
For non-Canadian shipping addresses the rates quoted must be paid in US funds.

Coût par volume (frais y compris d'expédition et de manutention) :
Taux régulier 15,00 $ — Tarif d'membre de la SMC 12,00 $ (avant taxes).
Pour une adresse à l'étranger, paiement requis en devises américaines.

For more information and to order:
Pour plus d'informations et pour compléter une commande :

www.cms.math.ca/Publications/books

or contact: ou contacter :

CMS/SMC Publications
1785 Alta Vista Drive, Suite 105, Ottawa (Ontario) CANADA K1G 3Y6

Email: publications@cms.math.ca
Courriel : publications@smc.math.ca

Canadian Mathematical Society / Société mathématique du Canada
1785 Alta Vista Drive, Suite 105, Ottawa (Ontario) CANADA K1G 3Y6
www.cms.math.ca