Stanford University
Educational Program for Gifted Youth (EPGY)
Number Theory

Dana Paquin, Ph.D.
paquin@math.stanford.edu

Summer 2010

Note: These lecture notes are adapted from the following sources:

1. Ivan Niven, Herbert S. Zuckerman, and Hugh L. Montgomery, *An Introduction to Number Theory*, Fifth Edition, John Wiley & Sons, Inc., 1991.

2. Joseph H. Silverman, *A Friendly Introduction to Number Theory*, Third Edition, Prentice Hall, 2006.

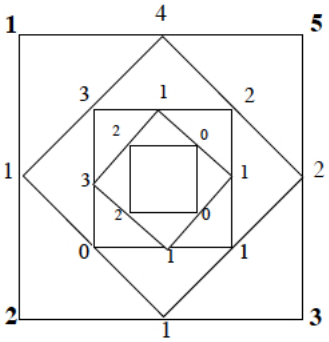
3. Harold M. Stark, *An Introduction to Number Theory*, The MIT Press, 1987.

Contents

Chapter 1

The Four Numbers Game

Choose 4 numbers and place them at the corners of a square. At the midpoint of each edge, write the *difference* of the two adjacent numbers, subtracting the smaller one from the larger. This produces a new list of 4 numbers, written on a smaller square. Now repeat this process. The game *ends* if/when a square with 0 at every vertex is achieved. Here's an example starting with the four numbers 1,5,3,2. We'll call this the $(1,5,3,2)$ game; note that the first number (1) is placed in the upper left-hand corner.



The $(1,5,3,2)$ game ends after 7 steps. We'll call this the *length* of the $(1,5,3,2)$ game. We'll be interested in determining whether or not all games must end in finitely many steps. Once it's clear how the game works, it's easier if we display the game more compactly as follows:

$$\begin{array}{cccc}
1 & 5 & 3 & 2 \\
4 & 2 & 1 & 1 \\
2 & 1 & 0 & 3 \\
1 & 1 & 3 & 1 \\
0 & 2 & 2 & 0 \\
2 & 0 & 2 & 0 \\
2 & 2 & 2 & 2 \\
0 & 0 & 0 & 0
\end{array}$$

Example 1.1 1. Find the length of the $(1, 3, 8, 17)$ game.

2. Find the length of the $(1, 2, 2, 5)$ game.
3. Find the length of the $(0, 1, 6, \pi)$ game.

Example 1.2 Is the length of the game affected by rotations and/or reflections of the square?

1. Find the length of the $(9, 7, 5, 1)$ game.
2. Find the length of the $(7, 5, 1, 9)$ game.
3. More generally, there are 4 total ways to "rotate" the $(9, 7, 5, 1)$ game. Find the length of each one.
4. Find the length of the $(5, 9, 7, 1)$ game (vertical reflection).
5. Find the length of the $(1, 7, 5, 9)$ game (horizontal reflection).
6. Find the length of the $(9, 1, 5, 7)$ game (major diagonal reflection).
7. Find the length of the $(7, 5, 9, 1)$ game (minor diagonal reflection).
8. There are 24 possible ways to arrange the numbers 9,7,5,1 on the vertices of a square–only 8 of them can be achieved by rotation and reflection. Find the length of the game for each configuration. Are the lengths all the same? Can you make any observations/conjectures?

Example 1.3 What is the greatest length of games using 4 integers between 0 and 9?

Example 1.4 Work out a few examples of the Four Numbers Game with rational numbers at the vertices. Does the game always end?

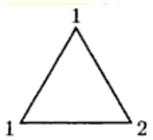
Observation 1.1 What happens if you multiply the 4 start numbers by a positive integer m? Is the length of the game changed? Once you've made and formally stated a conjecture, can you prove it?

Observation 1.2 Find several games with length at least 4. What do you observe about the numbers that appear after Step 4?

Theorem 1.1 Every Four Numbers Game played with nonnegative integers has finite length. More precisely, if we let A denote the largest of the 4 nonnegative integers and if k is the least integer such that $\dfrac{A}{2^k} < 1$, then the length of the game is at most $4k$.

Problem Set

1. Play the Three Numbers Game shown below using the same rules as the Four Numbers Game, and determine its length.



2. Experiment with examples of the k-Numbers Game for $k = 5, 6, 7, 8$. For each k, can you find examples of k-Numbers Games with finite length? Infinite length? Do you observe any patterns?
3. How does the length of the (a, b, c, d) game compare to the length of the $(ma + e, mb + e, mc + e, md + e)$ game?
4. Let a, b, c, d be nonnegative real numbers, and suppose that $a \geq c \geq b \geq d$. What is the maximum length of the Four Numbers Game (a, b, c, d) in this case?
5. Let a, b, c, d be nonnegative real numbers, and suppose that $a \geq b \geq d \geq c$. What is the maximum length of the Four Numbers Game (a, b, c, d) in this case?
6. Let a, b, c, d be nonnegative real numbers, and suppose that any 2 of the numbers a, b, c, d are equal. What is the maximum length of the Four Numbers Game (a, b, c, d) in this case?
7. The *Tribonacci numbers* are defined as follows:

$$t_0 = 0,\ t_1 = 1,\ t_2 = 1,\ t_3 = 2,\ t_4 = 4,\ t_5 = 7, \ldots.$$

In general,

$$t_n = t_{n-3} + t_{n-2} + t_{n-1}.$$

We'll define the n-th Tribonacci game as follows:

$$\begin{aligned} T_1 &= (t_2, t_1, t_0, 0) = (1, 1, 0, 0) \\ T_n &= (t_n, t_{n-1}, t_{n-2}, t_{n-3}) \end{aligned}$$

Can you find an equation for the length of T_n? Begin this problem by doing some experiments, and try to make a conjecture based on your observations. Then try to prove your conjecture.

8. Can you find a Four Numbers Game of length 20? Length 100? More generally, for a given integer N (possibly very large), can you find a Four Numbers Game of length N?

9. Numerous mathematical research papers have been written about the Four Numbers Game(and related games). The sequence of numbers that appear in the games are also called *Ducci sequences* after the Italian mathematician Enrico Ducci. Investigate Ducci sequences and their properties, extensions of the Four Numbers Game, the Four Real Numbers Game, k-Numbers Games, and/or other related topics. For example, if 4 nonnegative integers are picked at random, what's the probability that the game ends in 8 or fewer steps?

Chapter 2

Elementary Properties of Divisibility

One of the most fundamental ideas in elementary number theory is the notion of divisibility:

Definition 2.1 If a and b are integers, with $a \neq 0$, and if there is an integer c such that $ac = b$, then we say that a **divides** b, and we write $a \mid b$. If a does not divide b, then we write $a \nmid b$.

For example,

$$2 \mid 18, \quad 1 \mid 42, \quad 3 \mid (-6), \quad -7 \mid 49, \quad 9 \nmid 80, \quad -6 \nmid 31.$$

Theorem 2.1 Properties of Divisibility

1. If a, b, c, m, n are integers such that $c \mid a$ and $c \mid b$, then $c \mid (am + nb)$.
2. If x, y, z are integers such that $x \mid y$ and $y \mid z$, then $x|z$.

Proof. Since $c \mid a$ and $c \mid b$, there are integers s, t such that $sc = a, tc = b$. Thus

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

so $c \mid (am + bn)$. Similarly, since $x \mid y$ and $y \mid z$, there are integers u, v with $xu = y, yv = z$. Hence $xuv = z$, so $x \mid z$.

Theorem 2.2 If $a \mid b$ and $a \mid (b + c)$, then $a \mid c$.

Proof. Since $a \mid b$, there is an integer s such that $as = b$. Since $a \mid (b + c)$, there is an integer t such that $at = b + c$. Thus,

$$\begin{aligned} at - b &= c \\ at - as &= c \\ a(t - s) &= c. \end{aligned}$$

Since t and s are both integers, $t - s$ is also an integer, so $a \mid c$.

Example 2.1 Find all positive integers $n \geq 1$ for which

$$(n + 1) \mid (n^2 + 1).$$

Solution: $n^2 + 1 = n^2 - 1 + 2 = (n - 1)(n + 1) + 2$. Thus, if $(n + 1) \mid (n^2 + 1)$, we must have $(n + 1) \mid 2$ since $(n + 1) \mid (n - 1)(n + 1)$. Thus, $n + 1 = 1$ or $n + 1 = 2$. Now, $n + 1 \neq 1$ since $n \geq 1$. We conclude that $n + 1 = 2$, so the only n such that $(n + 1) \mid (n^2 + 1)$ is $n = 1$.

Example 2.2 If $7 \mid (3x + 2)$ prove that $7 \mid (15x^2 - 11x - 14.)$.

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

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

Thus, $7 \mid (15x^2 - 11x - 14)$.

Theorem 2.3 The **Division Algorithm:** If a and b are positive integers, then there are *unique* integers q and r such that

$$a = bq + r, \quad 0 \leq r < b.$$

We refer to this theorem as an *algorithm* because we can find the quotient q and the remainder r by using ordinary long division to divide a by b. We observe that $b \mid a$if and only if $r = 0$.

Problem Set

1. List all the divisors of the integer 12.
2. List all the numbers which divide both 24 and 36. Compare your answer with your answer to the previous problem.
3. Show that if $d \neq 0$ and $d \mid a$, then $d \mid (-a)$ and $-d \mid a$.
4. Show that if $a \mid b$ and $b \mid a$, then $a = b$ or $a = -b$.
5. Suppose that n is an integer such that $5|(n+2)$. Which of the following are divisible by 5?

   (a) $n^2 - 4$
   (b) $n^2 + 8n + 7$
   (c) $n^4 - 1$
   (d) $n^2 - 2n$

6. Find all integers $n \geq 1$ so that $n^3 - 1$ is prime. Hint: $n^3 - 1 = (n^2+n+1)(n-1)$.
7. Show that if $ac \mid bc$, then $a \mid b$.
8. (a) Prove that the product of three consecutive integers is divisible by 6.
   (b) Prove that the product of four consecutive integers is divisible by 24.
   (c) Prove that the product of n consecutive integers is divisible by $n!$.
9. Find all integers $n \geq 1$ so that $n^4 + 4$ is prime.
10. Find all integers $n \geq 1$ so that $n^4 + 4^n$ is prime.
11. Prove that the square of any integer of the form $5k + 1$ is of the same form.
12. Prove that 3 is not a divisor of $n^2 + 1$ for all integers $n \geq 1$.
13. A *prime triplet* is a triple of numbers of the form $(p, p+2, p+4)$, for which p, $p+2$, and $p+4$ are all prime. For example, $(3, 5, 7)$ is a prime triplet. Prove that $(3, 5, 7)$ is the only prime triplet.
14. Prove that if $3 \mid (a^2 + b^2)$, then $3 \mid a$ and $3 \mid b$. Hint: If $3 \nmid a$ and $3 \nmid b$, what are the possible remainders upon division by 3?
15. Let n be an integer greater than 1. Prove that if one of the numbers

$$2^n - 1, \ 2^n + 1$$

is prime, then the other is composite.

16. Suppose that p is an odd prime and that
$$\frac{a}{b} = 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p-1}.$$
Show that $p \mid a$.

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

18. Suppose that a is an integer greater than 1 and that n is a positive integer. Prove that if $a^n + 1$ is prime, then a is even and n is a power of 2. Primes of the form $2^{2^k} + 1$ are called *Fermat primes*.

19. Suppose that a is an integer greater than 1 and that n is a positive integer. Prove that if $a^n - 1$ is prime, then $a = 2$ and n is a prime. Primes of the form $2^n - 1$ are called *Mersenne primes*.

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

21. Can you find an integer $n > 1$ such that the sum
$$1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}$$
is an integer?

22. Show that every integer of the form
$$4 \cdot 14^k + 1, \quad k \geq 1$$
is composite. Hint: show that there is a factor of 3 when k is odd and a factor of 5 when k is even.

23. Show that every integer of the form
$$521 \cdot 12^k + 1, \quad k \geq 1$$
is composite. Hint: show that there is a factor of 13 when k is odd, a factor of 5 when $k \equiv 2 \mod 4$, and a factor of 29 when $4 \mid k$.

24. Show that for all integers a and b,
$$ab(a^2 - b^2)(a^2 + b^2)$$
is divisible by 30.

Chapter 3

Proof by Contradiction

In a **proof by contradiction** (or *reductio ad absurdum*), we assume, along with the hypotheses, the logical negation of the statement that we are trying to prove, and then reach some kind of contradiction. Upon reaching a contradiction, we conclude that the original assumption (i.e. the negation of the statement we are trying to prove) is false, and thus the statement that we are trying to prove must be true.

Example 3.1 Show, without using a calculator, that $6 - \sqrt{35} < \frac{1}{10}$.

Solution: Assume that $6 - \sqrt{35} \geq \frac{1}{10}$. Then

$$6 - \frac{1}{10} \geq \sqrt{35},$$

so

$$59 \geq 10\sqrt{35}.$$

Squaring both sides we obtain

$$3481 \geq 3500,$$

which is a contradiction. Thus our original assumption must be false, so we conclude that $6 - \sqrt{35} < \frac{1}{10}$.

Example 3.2 Let $a_1, a_2, \ldots, a_n$ be an arbitrary permutation of the numbers $1, 2, \ldots, n$, where n is an odd number. Prove that the product

$$(a_1 - 1)(a_2 - 2) \cdots (a_n - n)$$

is even.

Solution: It is enough to prove that some difference $a_k - k$ is even. Assume that all the differences $a_k - k$ are odd. Clearly

$$S = (a_1 - 1) + (a_2 - 2) + \cdots + (a_n - n) = 0,$$

since the a_k's are a reordering of $1, 2, \ldots, n$. S is an odd number of summands of odd integers adding to the even integer 0. This is a contradiction, so our initial assumption that all the $a_k - k$ are odd is thus false, so one of the terms $a_k - k$ is even, and hence the product is even.

Example 3.3 Prove that there are no positive integer solutions to the equation

$$x^2 - y^2 = 1.$$

Solution: Assume that there is a solution (x, y) where x and y are positive integers. Then we can factor the left-hand side of the equation to obtain

$$(x - y)(x + y) = 1.$$

Since x and y are both positive integers, $x - y$ and $x + y$ are integers. Thus, $x - y = 1$ and $x + y = 1$ or $x - y = -1$ and $x + y = -1$. In the first case, we add the two equations to obtain $x = 1$ and $y = 0$, which contradicts the assumption that x and y are both positive. In the second case, we add the two equations to obtain $x = -1$ and $y = 0$, which is again a contradiction. Thus, there are no positive integer solutions to the equation $x^2 - y^2 = 1$.

Example 3.4 If a, b, c are odd integers, prove that $ax^2 + bx + c = 0$ does not have a rational number solution.

Solution: Suppose $\dfrac{p}{q}$ is a rational solution to the equation. We may assume that p and q have no prime factors in common, so either p and q are both odd, or one is odd and the other even. Now

$$a\left(\frac{p}{q}\right)^2 + b\left(\frac{p}{q}\right) + c = 0 \implies ap^2 + bpq + cq^2 = 0.$$

If both p and p were odd, then $ap^2 + bpq + cq^2$ is also odd and hence $\neq 0$. Similarly if one of them is even and the other odd then either $ap^2 + bpq$ or $bpq + cq^2$ is even and $ap^2 + bpq + cq^2$ is odd. This contradiction proves that the equation cannot have a rational root.

Example 3.5 Show that $\sqrt{2}$ is irrational.

Solution: Proof by contradiction. Suppose that $\sqrt{2}$ is irrational, i.e.

$$\sqrt{2} = \frac{r}{s},$$

where r and s have no common factors (i.e. the fraction is in lowest terms). Then

$$2 = \frac{r^2}{s^2}, \text{ so } 2s^2 = r^2.$$

This means that r^2 must be even, so r must be even, say $r = 2c$. Then

$$2s^2 = (2c)^2 = 4c^2,$$

so

$$s^2 = 2c^2,$$

so s is also even. This is a contradiction since r and s have no common factors. Thus, $\sqrt{2}$ must be irrational.
We conclude with two important results.

Theorem 3.1 If n is an integer greater than 1, then n can be written as a finite product of primes.

Proof. Proof by contradiction. Assume that the theorem is false. Then there are composite numbers which cannot be represented as a finite product of primes. Let N be the smallest such number. Since N is the smallest such number, if $1 < n < N$, then the theorem is true for n. Let p be a prime divisor of N. Since N is composite,

$$1 < \frac{N}{p} < N,$$

so the theorem is true for $\frac{N}{p}$. Thus, there are primes $p_1, p_2 \cdots p_k$ such that

$$\frac{N}{p} = p_1 p_2 \cdots p_k.$$

Thus,

$$N = p p_1 p_2 \cdots p_k$$

is a finite product of primes. This is a contradiction, so we conclude that any integer greater than 1 can be written as a finite product of primes.

Theorem 3.2 There are infinitely many prime numbers.

Proof. Proof by contradiction. The following beautiful proof is attributed to Euclid. Assume that there are only finitely many (say, n) prime numbers. Then $\{p_1, p_2, \ldots, p_n\}$ is a list that exhausts all the primes. Consider the number

$$N = p_1 p_2 \cdots p_n + 1.$$

This is a positive integer, clearly greater than 1. Observe that none of the primes on the list $\{p_1, p_2, \ldots, p_n\}$ divides N, since division by any of these primes leaves a remainder of 1. Since N is larger than any of the primes on this list, it is either a prime or divisible by a prime outside this list. Thus we have shown that the assumption that any finite list of primes leads to the existence of a prime outside this list, so we have reached a contradiction. This implies that the number of primes is infinite.

Problem Set

1. The product of 34 integers is equal to 1. Show that their sum cannot be 0.

2. Prove that the sum of two odd squares cannot be a square.

3. Let $a_1, a_2, \ldots, a_{2000}$ be natural numbers such that

$$\frac{1}{a_1} + \frac{1}{a_2} + \cdots + \frac{1}{a_{2000}} = 1.$$

   Prove that at least one of the a_k's is even. Hint: clear the denominators.

4. A *palindrome* is an integer whose decimal expansion is symmetric, e.g. $1, 2, 11, 121$, 15677651 (but not $010, 0110$) are palindromes. Prove that there is no positive palindrome which is divisible by 10.

5. Let $0 < \alpha < 1$. Prove that $\sqrt{\alpha} > \alpha$.

6. In $\triangle ABC$, $\angle A > \angle B$. Prove that $BC > AC$.

7. Show that if a is rational and b is irrational, then $a + b$ is irrational.

8. Prove that there is no smallest positive real number.

9. Prove that there are no positive integer solutions to the equation

$$x^2 - y^2 = 10.$$

10. Given that a, b, c are odd integers, prove that the equation $ax^2 + bx + c = 0$ cannot have a rational root.

11. Prove that there do not exist positive integers a, b, c and n such that

$$a^2 + b^2 + c^2 = 2^n abc.$$

12. Show that the equation

$$b^2 + b + 1 = a^2$$

    has no positive integer solutions a, b.

13. Let a, b, c be integers satisfying $a^2 + b^2 = c^2$. Show that abc must be even.

Chapter 4

Mathematical Induction

Mathematical induction is a powerful method for proving statements that are "indexed" by the integers. For example, induction can be used to prove the following:

- The sum of the interior angles of any n-gon is $180(n-2)$ degrees.
- The inequality $n! > 2^n$ is true for all integers $n \geq 4$.
- $7^n - 1$ is divisible by 6 for all integers $n \geq 1$.

Each assertion can be put in the form:

$$P(n) \text{ is true for all integers } n \geq n_0,$$

where $P(n)$ is a statement involving the integer n, and n_0 is the starting point, or *base case*. For example, for the third assertion, $P(n)$ is the statement $7^n - 1$ is divisible by 6, and the base case is $n_0 = 1$. Here's how induction works:

1. Base case. First, prove that $P(n_0)$ is true.
2. Inductive step. Next, show that if $P(k)$ is true, then $P(k+1)$ must also be true.

Observe that these two steps are sufficient to prove that $P(n)$ is true for all integers $n \geq n_0$, as $P(n_0)$ is true by step (1), and step (2) then implies that $P(n_0+1)$ is true, which implies that $P(n_0+2)$ is true, etc.

You can think of induction in the following way. Suppose that you have arranged infinitely many dominos in a line, corresponding to statements $P(1)$, $P(2)$, $P(3)$, ... If you make the first domino fall, then you can be sure that all of the dominos will fall, provided that whenever one domino falls, it will knock down its neighbor. Knocking the first domino down is analogous to establishing the base case. Showing that each falling domino knocks down its neighbor is equivalent to showing that $P(n)$ implies $P(n+1)$.

Example 4.1 Prove that for any integer $n \geq 1$,

$$1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}.$$

Example 4.2 Prove that $n! > 2^n$ for all integers $n \geq 4$.

Solution: $P(n)$ is the statement $n! > 2^n$. The base case is $n_0 = 4$.

(i) Base case.

$$4! = 24 > 2^4 = 16,$$

so the base case $P(4)$ is true.

(ii) Inductive hypothesis. Assume that $n! > 2^n$. We must use this assumption to prove that $(n+1)! > 2^{n+1}$. The left-hand side of the inductive hypothesis is $n!$, and the left-hand side of the statement that we want to prove is $(n+1)! = (n+1)n!$. Thus, it seems natural to multiply both sides of the inductive hypothesis by $(n+1)$.

$$\begin{aligned} n! &> 2^n \\ (n+1)n! &> (n+1)2^n \\ (n+1)! &> (n+1)2^n. \end{aligned}$$

Finally, note that $(n+1) > 2$, so

$$(n+1)! > (n+1)2^n > 2 \cdot 2^n > 2^{n+1},$$

so we conclude that

$$(n+1)! > 2^{n+1},$$

as needed.

Thus, $n! > 2^n$ for all integers $n \geq 4$.

Example 4.3 Prove that the expression $3^{3n+3} - 26n - 27$ is a multiple of 169 for all natural numbers n.

Solution: $P(n)$ is the assertion $3^{3n+3} - 26n - 27$ is a multiple of 169, and the base case is $n_0 = 1$.

(i) Base case. Observe that $3^{3(1)+3} - 26(1) - 27 = 676 = 4(169)$ so $P(1)$ is true.

(ii) Inductive hypothesis. Assume that $P(n)$ is true, i.e. that is, that there is an integer M such that

$$3^{3n+3} - 26n - 27 = 169M.$$

We must prove that there is an integer K so that

$$3^{3(n+1)+3} - 26(n+1) - 27 = 169K.$$

We have:

$$\begin{aligned}
3^{3(n+1)+3} - 26(n+1) - 27 &= 3^{3n+3+3} - 26n - 26 - 27 \\
&= 27(3^{3n+3}) - 26n - 27 - 26 \\
&= 27(3^{3n+3}) - 26n - 26(26n) + 26(26n) \\
&\quad -27 - 26(27) + 26(27) - 26 \\
&= 27(3^{3n+3}) - 27(26n) - 27(27) + 26(26n) + 26(27) - 26 \\
&= 27(3^{3n+3} - 26n - 27) + 676n + 676 \\
&= 27(169M) + 169 \cdot 4n + 169 \cdot 4 \\
&= 169(27M + 4n + 4).
\end{aligned}$$

Thus, $3^{3n+3} - 26n - 27$ is a multiple of 169 for all natural numbers n.

Example 4.4 Prove that if k is odd, then 2^{n+2} divides

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

for all natural numbers n.

Solution: Let k be odd. $P(n)$ is the statement that 2^{n+2} is a divisor of $k^{2^n} - 1$, and the base case is $n_0 = 1$.

(i) Base case.

$$k^2 - 1 = (k-1)(k+1)$$

is divisible by $2^{1+2} = 8$ for any odd natural number k since $k-1$ and $k+1$ are consecutive even integers.

(ii) Inductive hypothesis. Assume that 2^{n+2} is a divisor of $k^{2^n} - 1$. Then there is an integer a such that $2^{n+2}a = k^{2^n} - 1$. Then

$$k^{2^{n+1}} - 1 = (k^{2^n} - 1)(k^{2^n} + 1) = 2^{n+2}a(k^{2^n} + 1).$$

Since k is odd, $k^{2^n} + 1$ is even and so $k^{2^n} + 1 = 2b$ for some integer b. This gives

$$k^{2^{n+1}} - 1 = 2^{n+2}a(k^{2^n} + 1) = 2^{n+3}ab,$$

and so the assertion follows by induction.

Example 4.5 The *Fibonacci Numbers* are given by

$$F_0 = 0, \; F_1 = 1, \; F_{n+1} = F_n + F_{n-1}, n \geq 1,$$

i.e. every number after the second one is the sum of the preceding two.
The first several terms of the Fibonacci sequence are

$$0, 1, 1, 2, 3, 5, 8, 13, 21, \ldots.$$

Prove that for all integers $n \geq 1$,

$$F_{n-1}F_{n+1} = F_n^2 + (-1)^{n+1}.$$

Solution: $P(n)$ is the statement that

$$F_{n-1}F_{n+1} = F_n^2 + (-1)^n$$

and the base case is $n_0 = 1$.

(i) Base case. If $n = 1$, then $0 = F_0F_2 = 1^2 + (-1)^1$.

(ii) Inductive hypothesis. Assume that $F_{n-1}F_{n+1} = F_n^2 + (-1)^n$. Then, using the fact that $F_{n+2} = F_n + F_{n+1}$, we have

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

which establishes the assertion by induction.

Example 4.6 Prove that

$$\frac{n^5}{5} + \frac{n^4}{2} + \frac{n^3}{3} - \frac{n}{30}$$

is an integer for all integers $n \geq 0$.

Solution: $P(n)$ is the statement that

$$\frac{n^5}{5} + \frac{n^4}{2} + \frac{n^3}{3} - \frac{n}{30}$$

is an integer and the base case is $n_0 = 0$.

(i) Base case. Since 0 is an integer, the statement is clearly true when $n = 0$.

(ii) Inductive hypothesis. Assume that

$$\frac{n^5}{5} + \frac{n^4}{2} + \frac{n^3}{3} - \frac{n}{30}$$

is an integer. We must show that

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

is also an integer. We have:

$$\begin{aligned}
&\frac{(n+1)^5}{5}+\frac{(n+1)^4}{2}+\frac{(n+1)^3}{3}-\frac{n+1}{30}\\
&=\frac{n^5+5n^4+10n^3+10n^2+5n+1}{5}+\frac{n^4+4n^3+6n^2+4n+1}{2}+\frac{n^3+3n^2+3n+1}{3}-\frac{n+1}{30}\\
&=\left[\frac{n^5}{5}+\frac{n^4}{2}+\frac{n^3}{3}-\frac{n}{30}\right]+\left[n^4+2n^3+2n^2+n+2n^3+3n^2+2n+n^2+n+1\right],
\end{aligned}$$

which is an integer by the inductive hypothesis and since the second grouping is a sum of integers.

Problem Set

1. Prove that for any integer $n \geq 1$,
$$2^0 + 2^1 + \cdots + 2^{n-1} = 2^n - 1.$$

2. Prove that for any integer $n \geq 1$, n^2 is the sum of the first n odd integers. (For example, $3^2 = 1 + 3 + 5$.)

3. Prove that $n^5 - 5n^3 + 4n$ is divisible by 120 for all integers $n \geq 1$.

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

5. Prove that
$$n^2 \mid ((n+1)^n - 1)$$
for all integers $n \geq 1$.

6. Show that
$$(x - y) \mid (x^n - y^n)$$
for all integers $n \geq 1$.

7. Use the result of the previous problem to show that
$$8767^{2345} - 8101^{2345}$$
is divisible by 666.

8. Show that
$$2903^n - 803^n - 464^n + 261^n$$
is divisible by 1897 for all integers $n \geq 1$.

9. Prove that if n is an even natural number, then the number $13^n + 6$ is divisible by 7.

10. Prove that $n! \geq 3^n$ for all integers $n \geq 7$.

11. Prove that $2^n \geq n^2$ for all integers $n \geq 4$.

12. Prove that for every integer $n \geq 2$, $n^3 - n$ is a multiple of 6.

13. Consider the sequence defined by $a_1 = 1$ and $a_n = \sqrt{2a_{n-1}}$. Prove that $a_n < 2$ for all integers $n \geq 1$.

14. Prove that the equation
$$x^2 + y^2 = z^n$$
has a solution in positive integers x, y, z for all integers $n \geq 1$.

15. Prove that $n^3 + (n+1)^3 + (n+2)^3$ is divisible by 9 for all integers $n \geq 1$.

16. Prove that
$$\frac{1}{n+1}+\frac{1}{n+2}+\cdots+\frac{1}{3n+1}>1$$
for all integers $n \geq 1$.

17. Prove that
$$\frac{4^n}{n+1} \leq \frac{(2n)!}{(n!)^2}$$
for all integers $n \geq 1$.

18. Show that $7^n - 1$ is divisible by 6 for all integers $n \geq 0$.

19. Consider the Fibonacci sequence $\{F_n\}$ defined by $F_0 = 0,\ F_1 = 1,\ F_{n+1} = F_n + F_{n-1}, n \geq 1$. Prove that each of the following statements is true for all integers $n \geq 1$.

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

   (b) $f_2 + F_4 + F_6 + \cdots + F_{2n} = F_{2n+1} - 1$

   (c) $F_n < 2^n$

   (d) $F_n = \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1+\sqrt{5}}{2}\right)^n\right]$

Chapter 5

The Greatest Common Divisor (GCD)

Definition 5.1 Let a and b be integers, not both zero. Let d be the largest number in the set of common divisors of a and b. We call d the **greatest common divisor** of a and b, and we write

$$d = \gcd(a, b),$$

or, more simply,

$$d = (a, b).$$

Example 5.1 We compute some simple gcd's.

- $(6, 4) = 2$
- $(3, 5) = 1$
- $(16, 24) = 8$
- $(4, 0) = 4$
- $(5, 5) = 5$
- $(3, 12) = 3$

Definition 5.2 If $(a, b) = 1$, we say that a and b are **relatively prime**.

In general, we'd like to be able to compute (a, b) without listing all of the factors of a and b. The **Euclidean Algorithm** is the most efficient method known for computing the greatest common divisor of two integers. We'll begin by illustrating the method with an example.

Example 5.2 Compute $(54, 21)$.

Solution: The first step is to divide 54 by 21, which gives a quotient of 2 and a remainder of 12. We write this as

$$54 = 2 \cdot 21 + 12.$$

Next, we divide 21 by 12, and obtain a quotient of 1 and a remainder of 9. We write this as

$$21 = 1 \cdot 12 + 9.$$

Next, we divide 12 by 9, and obtain a quotient of 1 and a remainder of 3. We write this as

$$12 = 1 \cdot 9 + 3.$$

Next, we divide 9 by 3 , and obtain a quotient of 3 and a remainder of 0. We write this as

$$9 = 3 \cdot 3 + 0.$$

The Euclidean algorithm says that we stop when we reach a remainder of 0, and that the remainder from the previous step is the greatest common divisor of the original two numbers. Thus,

$$(54, 21) = 3.$$

Now, why does this procedure work to give us the gcd? Working backwards through our string of equations, it's clear that $3 \mid 9$, so $3 \mid 12$, so $3 \mid 21$, so $3 \mid 54$. Thus, 3 is a common divisor of 21 and 54. But why is it the *greatest* common divisor? Let's suppose that d is some other common divisor of 21 and 54. We must show that $d \leq 3$. Observe that if $d \mid 21$ and $d \mid 54$, then $d \mid 12$, so $d \mid 9$, so $d \mid 3$. Thus, $d \leq 3$, so 3 is the gcd of 54 and 21.

Example 5.3 Compute $(36, 132)$, and use your computation to find integers x and y such that $(36, 132) = 36x + 132y$.

Solution:

$$\begin{aligned} 132 &= 3 \cdot 36 + 24 \\ 36 &= 1 \cdot 24 + 12 \\ 24 &= 2 \cdot 12 + 0. \end{aligned}$$

We conclude that

$$(36, 132) = 12.$$

Working backwards, we have:

$$\begin{aligned} 12 &= 36 - 1 \cdot 24 \\ &= 36 - 1 \cdot (132 - 3 \cdot 36) \\ &= 4 \cdot 36 - 1 \cdot 132. \end{aligned}$$

We conclude that

$$(36, 132) = 12 = 4 \cdot 36 - 1 \cdot 132.$$

Example 5.4 Compute $(53, 77)$, and use your computation to find integers x and y such that $(53, 77) = 53x + 77y$.

Solution:

$$\begin{aligned} 77 &= 1 \cdot 53 + 24 \\ 53 &= 2 \cdot 24 + 5 \\ 24 &= 4 \cdot 5 + 4 \\ 5 &= 1 \cdot 4 + 1 \\ 4 &= 4 \cdot 1 + 0. \end{aligned}$$

We conclude that $(53, 77) = 1$, so 53 and 77 are relatively prime.
Working backwards, we have:

$$\begin{aligned} 1 &= 5 - 1 \cdot 4 \\ &= 5 - 1 \cdot (24 - 4 \cdot 5) \\ &= 5 \cdot 5 - 1 \cdot 24 \\ &= 5 \cdot (53 - 2 \cdot 24) - 1 \cdot 24 \\ &= 5 \cdot 53 - 11 \cdot 24 \\ &= 5 \cdot 53 - 11 \cdot (77 - 1 \cdot 53) \\ &= 16 \cdot 53 - 11 \cdot 77. \end{aligned}$$

Thus,

$$(53, 77) = 1 = 16 \cdot 53 - 11 \cdot 77.$$

Theorem 5.1 Let a and b be integers, not both zero. Then (a, b) can be written as a *linear combination* of a and b, i.e. there exist integers x and y such that

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

and these integers can be found by the Euclidean algorithm method illustrated in the examples.

Note that since $(a,b) \mid a$ and $(a,b) \mid b$,

$$(a,b) \mid ax + by$$

for all integers x and y.

By Theorem 5.1, we can always find integers x and y so that $(a,b) = ax + by$. In general, let's consider the possible values that we can obtain from numbers of the form

$$ax + by$$

when we substitute all possible integers for x and y. For example, consider the case $a = 42$ and $b = 30$. Note that $(42,30) = 6$. Complete the table of values of $42x + 30y$ below for the given values of x and y.

	$x=-3$	$x=-2$	$x=-1$	$x=0$	$x=1$	$x=2$	$x=3$
$y=-3$							
$y=-2$							
$y=-1$							
$y=0$							
$y=1$							
$y=2$							
$y=3$							

Observe that $(42,30) = 6$ appears in the table, and is the smallest positive value of $ax + by$. In general, this is always true (and can be proven via the Euclidean algorithm).

Theorem 5.2 Let a and b be integers, not both zero. Then the smallest positive value of $ax + by$ (taken over all integers x and y) is (a,b).

Suppose that a, b, c are integers and that $a \mid bc$. When is it true that a is also a divisor of c? For example, $8 \mid 4 \cdot 10 = 40$, but $8 \nmid 4$ and $8 \nmid 10$. We can use Theorem 5.1 to answer this question.

Lemma 5.3 If $a \mid bc$ and if $(a,b) = 1$, then $a \mid c$.

Proof. Since $(a,b) = 1$, there are integers x and y such that

$$ax + by = 1,$$

and since $a \mid bc$, there is an integers k such that $ak = bc$. Then

$$\begin{aligned} c &= c \cdot 1 \\ &= c \cdot (ax + by) \\ &= (acx + bcy) \\ &= (acx + aky) \\ &= a(cx + ky). \end{aligned}$$

Thus, $a \mid c$.

Problem Set

1. Use the Euclidean algorithm to find each of the following.

   (a) $(77, 91)$

   (b) $(182, 442)$

   (c) $(2311, 3701)$

   (d) $(12345, 67890)$

2. Express $(17, 37)$ as a linear combination of 17 and 37.

3. Express $(399, 703)$ as a linear combination of 399 and 703.

4. Find integers r and s such that $547r + 632s = 1$.

5. Find integers r and s such that $398r + 600s = 2$.

6. Find integers r and s such that $922r + 2163s = 7$.

7. Use the Euclidean algorithm to find $(29, 11)$, and show that

$$\frac{29}{11} = 2 + \frac{1}{1 + \frac{1}{1+\frac{1}{1+\frac{1}{3}}}}.$$

8. Suppose that a, b, c are positive integers. Show that

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

9. Suppose that $(a, b) = d$. Show that

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

   Hint: use the theorem on linear combinations.

10. Show that if there is no prime p such that $p \mid a$ and $p \mid b$, then $(a, b) = 1$.

11. Show that if p is a prime and a is an integer, then either $(a, p) = 1$ or $(a, p) = p$.

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

13. Suppose that $(a, b) = 1$. Show that $(a + b, a^2 - ab + b^2) = 1$ or 3.

14. A number L is called a common multiple of m and n if both m and n divide L. The smallest such L is called the *least common multiple* of m and n and is denoted by $\text{lcm}(m, n)$. For example, $\text{lcm}(3, 7) = 21$ and $\text{lcm}(12, 66) = 132$.

   (a) Find each of the following.

      i. $\text{lcm}(8, 12)$

ii. $\mathrm{lcm}(20, 30)$
iii. $\mathrm{lcm}(51, 68)$
iv. $\mathrm{lcm}(23, 18)$

(b) For each of the lcm's that you computed in (a), compare the value of $\mathrm{lcm}(m, n)$ to the values of m, n and (m, n). Try to find a relationship.

(c) Prove that the relationship that you found in part (b) is true for all m and n.

(d) Suppose that $(m, n) = 18$ and $\mathrm{lcm}(m, n) = 720$. Find m and n. Is there more than one possibility? If so, find all of them.

(e) Suppose that $(a, b) = 1$. Show that for every integer c, the equation

$$ax + by = c$$

has a solution in integers x and y.

(f) Find integers x and y such that $37x + 47y = 103$.

15. Find two positive integers a and b such that $a^2+b^2 = 85113$ and $\mathrm{lcm}(a, b) = 1764$.

16. For all integers $n \geq 0$, define

$$F_n = 2^{2^n} + 1.$$

F_n is called the n-th *Fermat number*. Find (F_n, F_m).

17. Let a be an integer greater than or equal to 1. Find all integers $b \geq 1$ such that $(2^b - 1) \mid (2^a - 1)$.

18. Show that

$$(n^3 + 3n + 1, 7n^3 + 18n^2 - n - 2) = 1$$

for all integers $n \geq 1$.

19. Let the integers a_n and b_n be defined by the relationship

$$a_n + b_n\sqrt{2} = (1 + \sqrt{2})^n$$

for all integers $n \geq 1$. Prove that $(a_n, b_n) = 1$ for all integers $n \geq 1$.

20. Find integers x, y, z that satisfy the equation

$$6x + 15y + 20z = 1.$$

21. Under what conditions on a, b, c is it true that the equation

$$ax + by + cz = 1$$

has a solution? Describe a general method for finding a solution when one exists.

Chapter 6

Prime Factorization and the Fundamental Theorem of Arithmetic

Theorem 6.1 Let p be a prime number, and suppose that $p \mid ab$. Then either $p \mid a$ or $p \mid b$ (or p divides both a and b).

Proof. Suppose that p is a prime number that divides the product ab. If $p \mid a$, then we have nothing to prove, so let's assume that $p \nmid a$. Consider the greatest common divisor (a, p). We know that

$$(a, p) \mid p,$$

so $(a, p) = 1$ or $(a, p) = p$ since p is a prime. But, $(a, p) \neq p$, since $(a, p) \mid a$, and we are assuming that $p \nmid a$. Thus,

$$(a, p) = 1.$$

Thus, there exist integers x and y such that

$$ax + py = 1.$$

Multiplying both sides of this equation by b, we obtain

$$abx + pby = b.$$

Since $p \mid abx$ and $p \mid pby$, we conclude that

$$p \mid (abx + pby) = b.$$

Theorem 6.2 Let p be a prime number, and suppose that p divides the product $a_1 a_2 \cdots a_r$. Then p divides at least one of the factors $a_1, a_2, \ldots, a_r$.

Proof. If $p \mid a_1$, then we have nothing to prove, so let's assume that $p \nmid a_1$. Applying Theorem 6.1 to the product

$$a_1(a_2 a_3 \cdots a_r),$$

we conclude that

$$p \mid a_2 a_3 \cdots a_r.$$

Now, if $p \mid a_2$, then we are finished, so let's assume that $p \nmid a_2$. Applying Theorem 6.1 to the product

$$a_2(a_3 a_4 \cdots a_r),$$

we conclude that

$$p \mid a_3 a_4 \cdots a_r.$$

Continuing, we eventually find some a_k so that $p \mid a_k$.

Our goal now is to prove that *every* integer $n \geq 2$ can be factored *uniquely* into a product of primes $p_1 p_2 \cdots p_n$. Before we prove this result (which seems natural and, perhaps, obvious), let's look at an example that should illustrate that unique factorization into primes is, in fact, *not* obvious.

Example 6.1 Let

$$\mathbb{E} = \{\ldots, -8, -6, -4, -2, 0, 2, 4, 6, 8, \ldots\}$$

denote the set of *even* numbers. Consider the number 60 in $\mathbb{E}$.

- Observe that
$$60 = 2 \cdot 30 = 6 \cdot 10.$$
- Observe that 2, 6, 10, and 30 are all "primes" in $\mathbb{E}$ since they cannot be factored in $\mathbb{E}$.

Thus, 60 has two completely different prime factorizations in $\mathbb{E}$.

Although this example is somewhat contrived, it should convince you that there is real mathematical content to unique prime factorization. Certain number systems have unique factorization, and others do not. The set $\mathbb{Z}$ of integers has important properties that make the unique factorization theorem true.

Theorem 6.3 Fundamental Theorem of Arithmetic (FTA). Every integer $n \geq 2$ can be factored into a product of primes

$$n = p_1 p_2 \cdots p_n$$

in exactly one way.

Proof. Notice that the FTA actually contains two separate assertions that we must prove:

1. We must prove that every integer $n \geq 2$ can be factored into a product of primes.

2. We must prove that there is only one such factorization.

We'll begin by proving the first assertion. We'll construct a proof by contradiction. Suppose that there exist integers greater than 2 that cannot be written as a product of primes. There must be a smallest such integer. Call the smallest such integer N. Since N cannot be written as a product of primes, we can conclude that N is not prime. Thus, there exist integers b and c such that

$$N = bc,$$

with $b, c > 1$ and $b, c < N$. Since N is the smallest integer that cannot be written as a product of primes, b and c can both be written as products of primes:

$$b = p_1 p_2 \cdots p_k, \;\; c = q_1 q_2 \cdots q_l,$$

where all of the p_i and q_i are prime. Then

$$N = bc = p_1 p_2 \cdots p_k q_1 q_2 \cdots q_k$$

can also be written as a product of primes. This is a contradiction, so we conclude that no such integers exist. Thus, every integer $n \geq 2$ can be factored into a product of primes.

Next, we'll prove the second assertion. Suppose that there exists an integer n that we can factor as a product of primes in two ways, say

$$n = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_l.$$

We must show that these two factorizations are the same, possibly after rearranging the order of the factors. First, observe that

$$p_1 \mid n = q_1 q_2 \cdots q_l,$$

so by Theorem 6.2, p_1 must divide one of the q_i. We can rearrange the q_i's so that $p_1 \mid q_1$. But q_1 is also a prime number, so its only divisors are 1 and q_1. Thus, we conclude that

$$p_1 = q_1.$$

Now we cancel $p_1 = q_1$ from both sides of the equation to obtain

$$p_2 p_3 \cdots p_k = q_2 q_3 \cdots q_l.$$

Repeating the same argument as before, we note that

$$p_2 \mid q_1 q_2 \cdots q_l,$$

so by Theorem 6.2, p_2 must divide one of the q_i's, and after rearranging, we conclude that $p_2 \mid q_2$, so

$$p_2 = q_2$$

since q_2 is prime. Canceling $p_2 = q_2$ from both sides of the equation, we obtain

$$p_3p_4 \cdots p_k = q_3q_4 \cdots q_l.$$

We can continue this argument until either all of the p_i's or all of the q_i's are gone. But if all of the p_i's are gone, then the left-hand side of the equation is equal to 1, so there cannot be any q_i's left either. Similarly, if all of the q_i's are gone, then the right-hand side of the equation is equal to 1, so there cannot be any p_i's left either. Thus, the number of p_i's must be the same as the number of the q_i's, and after rearranging, we have

$$p_1 = q_1,\ p_2 = q_2,\ p_3 = q_3, \ldots, p_k = q_k.$$

Thus, there is only one way to write an integer $n \geq 2$ as a product of primes.

Applications of the Fundamental Theorem of Arithmetic.

Example 6.2 Show that $\sqrt{2}$ is irrational.

Solution: Proof by contradiction. Suppose that $\sqrt{2}$ is rational. Then there exist integers r, s such that

$$\sqrt{2} = \frac{r}{s}.$$

Then

$$2 = \frac{r^2}{s^2},$$

so

$$2s^2 = r^2.$$

Let n denote the number of prime factors in the prime factorization of s. Then there are $2n$ prime factors in the prime factorization of s^2, and since 2 is prime, there are $2n+1$ prime factors in the prime factorization of $2s^2$, so in particular, $2s^2$ has an odd number of prime factors. Next, let m denote the number of prime factors in the prime factorization of r. Then there are $2m$ prime factors in the prime factorization of r^2, so in particular, r^2 has an even number of prime factors. However, this contradicts the FTA since

$$2s^2 = r^2.$$

Thus, we conclude that $\sqrt{2}$ is irrational.

Example 6.3 Suppose that a and n are positive integers and that $\sqrt[n]{a}$ is rational. Prove that $\sqrt[n]{a}$ is an integer.

Solution: Since $\sqrt[n]{a}$ is rational and positive, there are positive integers r and s such that

$$\sqrt[n]{a} = \frac{r}{s},$$

so

$$as^n = r^n.$$

Without loss of generality, we may assume that $(r, s) = 1$ (otherwise, divide the numerator and denominator by (r, s) so that the fraction is in lowest terms). We will use proof by contradiction to show that $s = 1$. Suppose that $s > 1$. Then there is a prime p that divides s, so

$$p \mid as^n = r^n.$$

Thus, by Theorem 6.2,

$$p \mid r.$$

But this is a contradiction since $(r, s) = 1$. Thus, $s = 1$, so

$$\sqrt[n]{a} = r$$

is an integer. We can use this result, for example, to show that $\sqrt{2}$ is irrational. Since $1 < \sqrt{2} < 2$, $\sqrt{2}$ is not an integer, so it is not rational by the result of this example.

Example 6.4 Show that $\log_{10} 2$ is irrational.

Solution: Proof by contradiction. Suppose that $\log_{10} 2$ is rational. Then there exist integers r, s such that

$$\log_{10} 2 = \frac{r}{s}.$$

Then

$$10^{r/s} = 2,$$

so

$$10^r = 2^s,$$

or

$$5^r 2^r = 2^s,$$

which contradicts the FTA. Thus, $\log_{10} 2$ is irrational.

Example 6.5 Prove that if the polynomial

$$p(x) = a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n$$

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

Solution: Proof by contradiction. Assume that there is an integer m such that $p(m) = 14$. We know that $p(a_k) - 7 = 0$ for four distinct integers a_1, a_2, a_3, a_4. Then

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

for some polynomial $q(x)$ with integer coefficients. Then we have

$$14 - 7 = 7 = p(m) - 7 = (m - a_1)(m - a_2)(m - a_3)(m - a_4)q(m).$$

Since the factors $m - a_k$ are all distinct, we have decomposed the integer 7 into at least four different factors. However, by the FTA, the integer 7 can be written as a product of at most 3 different integers: $7 = (-7)(1)(-1)$. Thus, we have reached a contradiction, so we conclude that the polynomial cannot take the value 14 for any integral value of x.

Example 6.6 Prove that $m^5 + 3m^4n - 5m^3n^2 - 15m^2n^3 + 4mn^4 + 12n^5$ is never equal to 33.

Solution: Observe that

$$m^5 + 3m^4n - 5m^3n^2 - 15m^2n^3 + 4mn^4 + 12n^5$$

$$= (m - 2n)(m - n)(m + n)(m + 2n)(m + 3n).$$

Now, 33 can be decomposed as the product of at most four different integers: $33 = (-11)(3)(1)(-1)$ or $33 = (-3)(11)(1)(-1)$. If $n \neq 0$, the factors in the above product are all different. By the FTA, they cannot multiply to 33, since 33 is the product of at most 4 different factors and the expression above is the product of 5 different factors for $n \neq 0$.. If $n = 0$, the product of the factors is m^5, and 33 is clearly not a fifth power. Thus, $m^5 + 3m^4n - 5m^3n^2 - 15m^2n^3 + 4mn^4 + 12n^5$ is never equal to 33.

Example 6.7 Prove that there is exactly one natural number n such that $2^8+2^{11}+2^n$ is a perfect square.

Solution: Suppose that k is an integer such that

$$k^2 = 2^8 + 2^{11} + 2^n = 2304 + 2^n = 48^2 + 2^n.$$

Then

$$k^2 - 48^2 = (k - 48)(k + 48) = 2^n.$$

By the FTA,

$$k - 48 = 2^s \text{ and } k + 48 = 2^t,$$

where $s + t = n$. But then

$$2^t - 2^s = 48 - (-48) = 96 = 3 \cdot 2^5$$

, so

$$2^s(2^{t-s} - 1) = 3 \cdot 2^5.$$

By the FTA, $s = 5$ and $t - s = 2$, so $s + t = n = 12$. Thus, the only natural number n such that $2^8 + 2^{11} + 2^n$ is a perfect square is $n = 12$.

Problem Set

1. Give an example of four positive integers such that any three of them have a common divisor greater than 1, although only ± 1 divide all four of them.
2. Prove that $\sqrt{3}$ is irrational.
3. Prove that $\sqrt[3]{3}$ is irrational.
4. Prove that $\sqrt[5]{5}$ is irrational.
5. Prove that if $n \geq 2$, then $\sqrt[n]{n}$ is irrational. Hint: show that if $n > 2$, then $2^n > n$.
6. Prove that $\log_{10} 7$ is irrational.
7. Prove that $\dfrac{\log 3}{\log 2}$ is irrational.
8. Find the smallest positive integer such that $n/2$ is a square and $n/3$ is a cube.
9. In this exercise, you will continue your investigation of the set $\mathbb{E}$, the set of even numbers.
   (a) Classify all primes in $\mathbb{E}$. We will refer to such integers as $\mathbb{E}$-primes.
   (b) We have seen that 60 has two different factorizations as a product of $\mathbb{E}$-primes. Show that 180 has three different factorizations as a product of $\mathbb{E}$-primes.
   (c) Find the smallest number with four different factorizations in $\mathbb{E}$.
   (d) The number 12 has only one factorization as a product of primes in $\mathbb{E}$: $12 = 2 \cdot 6$. Describe all even numbers that have only one factorization as a product of $\mathbb{E}$-primes.
10. Let $\mathbb{M}$ denote the set of positive integers that leave a remainder of 1 when divided by 4, i.e.
$$\mathbb{M} = \{1, 5, 9, 13, 17, 21, \ldots\}.$$
Note that all numbers in $\mathbb{M}$ are numbers of the form $4k + 1$ for $k = 0, 1, 2, \ldots$.
    (a) Show that the product of two numbers in $\mathbb{M}$ is also in $\mathbb{M}$, i.e. if a and b both leave a remainder of 1 when divided by 4, then ab does as well.
    (b) Find the first six $\mathbb{M}$-primes in $\mathbb{M}$. An integer is an $\mathbb{M}$-prime if its only divisors in $\mathbb{M}$ are 1 and itself.
    (c) Find a number in $\mathbb{M}$ that has two different factorizations as a product of $\mathbb{M}$-primes. Conclude that $\mathbb{M}$ does not have unique factorization.
11. Consider the set
$$\mathbb{F} = \{a + b\sqrt{-6}\},$$
where a and b are integers.

(a) A prime in $\mathbb{F}$ is an element of $\mathbb{F}$ which has no factors in $\mathbb{F}$ other than 1 and itself. Show that 2 and 5 are $\mathbb{F}$-primes.

(b) Show that 7 and 31 are not $\mathbb{F}$-primes.

(c) Find two different factorizations of the number 10 in $\mathbb{F}$.

(d) Conclude that $\mathbb{F}$ does not have unique factorization.

12. Show that if p is a prime and $p \mid a^n$, then $p^n \mid a^n$.

13. How many zeros are there at the end of 100!?

14. Prove that the sum

$$1/3 + 1/5 + 1/7 + \cdots + 1/(2n+1)$$

is never an integer. Hint: Look at the largest power of $3 \leq n$.

15. Find the number of ways of factoring 1332 as the product of two positive relatively prime factors each greater than 1.

16. Let $p_1, p_2, \ldots, p_t$ be different primes and $a_1, a_2, \ldots a_t$ be natural numbers. Find the number of ways of factoring $p_1^{a_1} p_2^{a_2} \cdots p_t^{a_t}$ as the product of two positive relatively prime factors each greater than 1.

17. Show that the cube roots of three distinct prime numbers cannot be three terms (not necessarily consecutive) of an arithmetic progression.

18. Prove that there is no triplet of integers (a, b, c), except for $(a, b, c) = (0, 0, 0)$ for which

$$a + b\sqrt{2} + c\sqrt{3} = 0.$$

Chapter 7

Introduction to Congruences and Modular Arithmetic

Definition 7.1 We say that a **is congruent to** b **modulo** m, and write

$$a \equiv b \mod m,$$

if m divides $a - b$.

Equivalently, $a \equiv b \mod m$ if a and b leave the same remainder upon division by m. By the Division Algorithm, we observe that $a \equiv b \mod m$ if and only if there exists an integer k such that $a = b + km$.

Example 7.1 $7 \equiv 2 \mod 5$ since $5 \mid (7-2)$. Note that 7 and 2 both leave remainder 2 upon division by 5.

Example 7.2 $47 \equiv 35 \equiv 5 \mod 6$ since $6|(47-35)$ and $6|(35-5)$. Note that 47, 35, and 5 all leave remainder 5 upon division by 6.

Example 7.3 $9 \equiv 0 \mod 3$ since $3 \mid 9$. Note that 9 leaves a remainder of 0 upon division by 3.

Example 7.4 $15 \equiv 7 \equiv -1 \mod 8$ since $8 \mid (15-7)$ and $8 \mid (7 - -1)$.

Example 7.5 Construct an addition table and a multiplication table for arithmetic modulo 5.

Solution:

Addition modulo 5:

a, b	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Multiplication modulo 5:

a, b	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Note that if a is divided by m and leaves a remainder of r, then a is congruent to r modulo m. Recall (from the Division Algorithm) that the remainder r obtained upon dividing a by m satisfies

$$0 \leq r < m,$$

so every integer a is congruent, modulo m, to some integer between 0 and $m-1$. This is an important idea, and one that we will return to later. For now, we'll study some fundamental properties of congruences.

Theorem 7.1 Fundamental Properties of Congruences, Part 1. Let m be a positive integer. For all integers a, b, c, the following statements are true:

1. $a \equiv a \mod m$
2. If $a \equiv b \mod m$, then $b \equiv a \mod m$.
3. If $a \equiv b \mod m$, and $b \equiv c \mod m$, then $a \equiv c \mod m$.
4. For all integers $n \geq 1$, $a^n \equiv b^n \mod m$.

Proof.

1. Since $m \mid 0 = (a-a)$, $a \equiv a \mod m$.
2. Suppose that $a \equiv b \mod m$. Thus, $m \mid (a-b)$. Then there is an integer k such that $(a-b) = km$. Thus, $(b-a) = -km$, so $m \mid (b-a)$. Thus, $b \equiv a \mod m$.
3. Suppose that $a \equiv b \mod m$ and that $b \equiv c \mod m$. Thus, $m \mid (a-b)$ and $m \mid (b-c)$. Then there are integers k and l such that $(a-b) = km$ and $(b-c) = lm$. Thus,

$$(a-c) = (a-b) + (b-c) = km + lm = (k+l)m,$$

so $m \mid (a-c)$. Thus, $a \equiv c \mod m$.

Theorem 7.2 Fundamental Properties of Congruences, Part 2. Suppose that

$$a \equiv b \mod m \text{ and } c \equiv d \mod m.$$

Then:

1. $(a+c) \equiv (b+d) \mod m$,
2. $(a-c) \equiv (b-d) \mod m$,
3. $ac \equiv bd \mod m$, and
4. For all integers $n \geq 1$, $a^n \equiv b^n \mod m$.

Proof. Since $a \equiv b \mod m$, $m \mid (a-b)$, so there is an integer k such that $(a-b) = km$. Similarly, since $c \equiv d \mod m$, $m \mid (c-d)$, so there is an integer l such that $(c-d) = lm$.

1. To prove the first equivalence, we observe the following:

$$\begin{aligned}(a+c)-(b+d) &= (a-b)+(c-d)\\ &= km+lm\\ &= (k+l)m,\end{aligned}$$

so $m \mid (a+c)-(b+d)$. Thus, $(a+c) \equiv (b+d) \mod m$.

2. To prove the second equivalence, we observe the following:

$$\begin{aligned}(a-c)-(b-d) &= (a-b)+(d-c)\\ &= km-lm\\ &= (k-l)m,\end{aligned}$$

so $m \mid (a-c)-(b-d)$. Thus, $(a-c) \equiv (b-d) \mod m$.

3. Finally, to prove the third equivalence, we observe the following:

$$\begin{aligned}ac-bd &= c(a-b)+b(c-d)\\ &= ckm+blm\\ &= (ck+bl)m,\end{aligned}$$

so $m \mid (ac-bd)$. Thus, $ac \equiv bd \mod m$.

Theorem 7.3 If $a \equiv b \mod m$, then for any integer c,

$$(a \pm c) \equiv (b \pm c) \mod m, \text{ and } ac \equiv bc \mod m.$$

Proof. Since $m \mid (a-b)$, $m \mid (a-b)+(c-c) = (a+c)-(b+c)$ and $m \mid (a-b)-(c-c) = (a-c)-(b-c)$, so

$$(a \pm c) \equiv (b \pm c) \mod m.$$

Similarly, $m \mid (a-b)c = ac - bc$, so

$$ac \equiv bc \mod m.$$

Corollary 7.4 Suppose that $f(x)$ is a polynomial with integer coefficients. If $a \equiv b \mod m$, then

$$f(a) \equiv f(b) \mod m.$$

Proof. Let

$$f(x) = a_k x^k + a_{k-1}x^{k-1} + \cdots + a_1 x + a_0,$$

where $a_0, a_1, \ldots, a_k$ are integers. Then by Theorem 7.2,

$$a_k a^k + a_{k-1}a^{k-1} + \cdots + a_1 a + a_0 \equiv a_k b^k + a_{k-1}b^{k-1} + \cdots + a_1 b + a_0 \mod m.$$

Thus,

$$f(a) \equiv f(b) \mod m.$$

Note that in general, we are not allowed to "divide" in congruences. For example,

$$15 = 3 \cdot 5 \equiv 3 \cdot 1 \mod 6.$$

But

$$5 \not\equiv 1 \mod 6,$$

so we can't "cancel" the 3's. However, it is true that

$$3 \cdot 4 \equiv 3 \cdot 14 \mod 15$$

and

$$4 \equiv 14 \mod 5,$$

so in certain cases, we can cancel. Thus, it is a natural question to determine under which conditions we can cancel in congruences.

Theorem 7.5 Suppose that

$$ac \equiv bc \mod m$$

and that $(c, m) = 1$. Then

$$a \equiv b \mod m.$$

Proof. $m \mid (ac - bc) = (a - b)c$. Since $(m, c) = 1$, $m \mid (a - b)$.

Problem Set

1. Determine whether each of the following statements is true or false.

   (a) $17 \equiv 2 \mod 5$

   (b) $14 \equiv -6 \mod 10$

   (c) $97 \equiv 5 \mod 13$

2. Compute each of the following:

   (a) 30 modulo 4

   (b) 21 modulo 6

   (c) 100 modulo 9

   (d) 32 modulo 8

   (e) 29 modulo 5

   (f) 75 modulo 11

3. (a) Verify each of the following statements.

      i. $3 \cdot 5 \equiv 3 \cdot 13 \mod 4$

      ii. $7 \cdot 18 \equiv 7 \cdot (-2) \mod 10$

      iii. $3 \cdot 4 \equiv 3 \cdot 14 \mod 6$

   (b) Determine whether each of the following statements is true or false.

      i. $5 \equiv 13 \mod 4$

      ii. $18 \equiv -2 \mod 10$

      iii. $4 \equiv 14 \mod 6$

4. Can we add congruences? If $a \equiv b \mod m$ and $c \equiv d \mod m$, is it necessarily true that $a + c \equiv b + d \mod m$? If so, why? If not, provide an example that illustrates why not. To get started on this question, do some numerical examples.

5. Can we subtract congruences? If $a \equiv b \mod m$ and $c \equiv d \mod m$, is it necessarily true that $a - c \equiv b - d \mod m$? If so, why? If not, provide an example that illustrates why not. To get started on this question, do some numerical examples.

6. Can we multiply congruences? If $a \equiv b \mod m$ and $c \equiv d \mod m$, is it necessarily true that $ac \equiv bd \mod m$? If so, why? If not, provide an example that illustrates why not. To get started on this question, do some numerical examples.

7. Can we take powers of congruences? If $a \equiv b \mod m$ and $n \geq 1$ is a positive integer, is it necessarily true that $a^n \equiv b^n \mod m$? If so, why? If not, provide an example that illustrates why not. To get started on this question, do some numerical examples.

8. Can we cancel congruences? If $ab \equiv ac \mod m$, is it necessarily true that $b \equiv c \mod m$? If so, why? If not, provide an example that illustrates why not. To get started on this question, do some numerical examples.

9. Suppose that
$$ac \equiv bc \mod m$$
and that
$$\gcd(c, m) = 1.$$
Prove that
$$a \equiv b \mod m$$
in this case.

10. Find a if $a \equiv 97 \mod 7$ and $1 \leq a \leq 7$.

11. Find a if $a \equiv 32 \mod 19$ and $52 \leq a \leq 70$.

12. Construct the tables for addition and multiplication modulo 7.

Chapter 8

Applications of Congruences and Modular Arithmetic

Example 8.1 Find the remainder when 6^{1987} is divided by 37.

Solution: First, note that $6^2 \equiv -1 \mod 37$. Thus:

$$\begin{aligned} 6^{1987} &\equiv 6 \cdot 6^{1986} \mod 37 \\ &\equiv 6(6^2)^{993} \mod 37 \\ &\equiv 6(-1)^{993} \mod 37 \\ &\equiv -6 \mod 37 \\ &\equiv 31 \mod 37. \end{aligned}$$

Thus, the desired remainder is 31.

Example 8.2 Prove that 7 divides $3^{2n+1} + 2^{n+2}$ for all natural numbers n.

Solution: Observe that

$$3^{2n+1} \equiv 3 \cdot 9^n \equiv 3 \cdot 2^n \mod 7$$

and

$$2^{n+2} \equiv 4 \cdot 2^n \mod 7.$$

Thus,

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

for all natural numbers n.

Example 8.3 Prove that $641 \mid (2^{32} + 1)$.

Solution: First, observe that

$$641 = 2^7 \cdot 5 + 1 = 2^4 + 5^4.$$

Thus,

$$2^7 \cdot 5 \equiv -1 \mod 641$$

and

$$5^4 \equiv -2^4 \mod 641.$$

Thus,

$$\begin{aligned} 5^4 \cdot 2^{28} &= (5 \cdot 2^7)^4 \\ &\equiv (-1)^4 \mod 641 \\ &\equiv 1 \mod 641. \end{aligned}$$

Thus,

$$-2^4 \cdot 2^{28} = -2^{32} \equiv 1 \mod 641.$$

This implies that

$$-2^{32} - 1 \equiv 0 \mod 641,$$

so $641 \mid -(2^{32} + 1)$, which implies that

$$641 \mid (2^{32} + 1).$$

Example 8.4 Prove that there are no integers with $x^2 - 5y^2 = 2$. Hint: consider the equation modulo 5.

Solution: If $x^2 - 5y^2 = 2$, then $(x^2 - 5y^2) \equiv 2 \mod 5$. Since $5y^2 \equiv 0 \mod 5$, this implies that $x^2 \equiv 2 \mod 5$. Now, consider the possibilities for x and x^2 modulo 5.

x modulo 5	x^2 modulo 5
0	0
1	1
2	4
3	4
4	1

Thus, there is no x such that x^2 is congruent to 2 modulo 5, so there are no integers x and y such that $x^2 - 5y^2 = 2$.

Example 8.5 Find the units digit of 7^{100}.

Solution: To find the units digit of 7^{100}, we must find 7^{100} modulo 10.

$$\begin{aligned}
7^2 &\equiv -1 \mod 10 \\
7^3 &\equiv 7 \cdot 7^2 \mod 10 \\
&\equiv -7 \mod 10 \\
7^4 &\equiv (7^2)^2 \mod 10 \\
&\equiv (-1)^2 \mod 10 \\
&\equiv 1 \mod 10 \\
7^{100} &\equiv (7^4)^{25} \mod 10 \\
&\equiv 1^{25} \mod 10 \\
&\equiv 1 \mod 10.
\end{aligned}$$

Thus, the units digit of 7^{100} is 1.

Example 8.6 Find infinitely many integers n such that $2^n + 27$ is divisible by 7.

Solution: Observe that

$$\begin{aligned}
2^1 &\equiv 2 \mod 7 \\
2^2 &\equiv 4 \mod 7 \\
2^3 &\equiv 1 \mod 7 \\
2^4 &\equiv 2 \mod 7 \\
2^5 &\equiv 4 \mod 7 \\
2^6 &\equiv 1 \mod 7.
\end{aligned}$$

Thus,

$$2^{3k} \equiv (2^3)^k \equiv 1^k \mod 7$$

for all positive integers k. Thus,

$$2^{3k} + 27 \equiv 1 + 27 \equiv 28 \equiv 0 \mod 7$$

for all positive integers k. Thus, for all positive integers k,

$$7 \mid 2^{3k} + 27,$$

so $2^n + 27$ is divisible by 7 for all positive multiples of 3.

Example 8.7 Prove that $2^k - 5, k = 0, 1, 2, \ldots$ never leaves remainder 1 when divided by 7.

Solution: Observe that

$$2^1 \equiv 2 \mod 7,$$

$$2^2 \equiv 4 \mod 7,$$
$$2^3 \equiv 1 \mod 7,$$

and this cycle of three repeats, so for any k,

$$2^k \equiv 2,\ 4,\ \text{or } 1 \mod 7.$$

Thus

$$(2^k - 5) \equiv -3,\ -1,\ \text{or } -4 \mod 7,$$

so $2^k - 5$ can leave only remainders 3, 4, or 6 upon division by 7.

Example 8.8 Show that a positive integer n is divisible by 3 if and only if the sum of its digits is divisible by 3.

Solution: We show that n and the sum of its digits are congruent modulo 3. Suppose that the positive integer n is written in its standard decimal expansion as

$$n = a_k \cdot 10^k + a_{k-1}10^{k-1} + \cdots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0.$$

Observe that $10 \equiv 1 \mod 3$ and $10^m \equiv 1^m \equiv 1 \mod 3$ for any integer m. Thus,

$$\begin{aligned} n &\equiv a_k \cdot 10^k + a_{k-1}10^{k-1} + \cdots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0 \mod 3 \\ &\equiv a_k \cdot 1 + a_{k-1} \cdot 1 + \cdots + a_2 \cdot 1 + a_1 \cdot 1 + a_0 \mod 3 \\ &\equiv a_k + a_{k-1} + \cdots + a_2 + a_1 + a_0 \mod 3. \end{aligned}$$

Thus, the remainder obtained when n is divided by 3 is the same as the remainder obtained when the sum of the digits of n is divided by 3, so n is divisible by 3 if and only if the sum of its digits is divisible by 3.

Problem Set 1

1. Compute each of the following:

   (a) $51 \mod 13$

   (b) $342 \mod 85$

   (c) $62 \mod 15$

   (d) $10 \mod 15$

   (e) $(82 \cdot 73) \mod 7$

   (f) $(51 + 68) \mod 7$

   (g) $(35 \cdot 24) \mod 11$

   (h) $(47 + 68) \mod 11$

2. List all integers x in the range $1 \leq x \leq 100$ that satisfy $x \equiv 7 \mod 17$.

3. If an integer x is even, observe that it must satisfy the congruence $x \equiv 0 \mod 2$. If an integer y is odd, what congruence does it satisfy? What congruence does an integer z of the form $6k + 1$ satisfy?

4. Write a single congruence that is equivalent to the pair of congruences $x \equiv 1 \mod 4$, $x \equiv 2 \mod 3$.

5. Suppose that p is a prime number and that

   $$a^2 \equiv b^2 \mod p.$$

   Show that

   $$p \mid (a + b) \text{ or } p \mid (a - b).$$

6. Show that if $a \equiv b \mod n$ and $d \mid n$, then $a \equiv b \mod d$.

7. Show that a perfect square is congruent to either 0 or 1 modulo 4.

8. (a) Compute $5^2 \mod 3$.

   (b) Use (a) to compute $5^3 \mod 3$.

   (c) Use (a) and (b) to compute $5^{101} \mod 3$.

   (d) What is the remainder when 5^{101} is divided by 3?

9. (a) Compute $2^2 \mod 3$.

   (b) Compute $4^2 \mod 5$.

   (c) Compute $6^2 \mod 7$.

   (d) Compute $10^2 \mod 11$.

(e) Make a conjecture about the value of

$$(p-1)^2 \mod p,$$

where p is a prime number. Prove that your conjecture is true for all primes p.

10. (a) Compute $1 \cdot 2 \mod 3$.

(b) Compute $1 \cdot 2 \cdot 3 \cdot 4 \mod 5$.

(c) Compute $1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \mod 7$.

(d) Compute $1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10 \mod 11$.

(e) Make a conjecture about the value of

$$(p-1)! \mod p,$$

where p is a prime number. This result is known as Wilson's Theorem.

(f) Try to prove that your conjecture is correct for all primes p.

11. (a) Find (by trial and error or otherwise) all numbers x, $0 \leq x \leq 2$, such that $x^2 \equiv 1 \mod 3$.

(b) Find (by trial and error or otherwise) all numbers x, $0 \leq x \leq 4$, such that $x^2 \equiv 1 \mod 5$.

(c) Find (by trial and error or otherwise) all numbers x, $0 \leq x \leq 6$, such that $x^2 \equiv 1 \mod 7$.

(d) Find (by trial and error or otherwise) all numbers x, $0 \leq x \leq 10$, such that $x^2 \equiv 1 \mod 11$.

(e) Suppose that p is a prime. Make a conjecture about the numbers x, $0 \leq x \leq p-1$ such that $x^2 \equiv 1 \mod p$.

12. The **inverse** of a number x modulo m is the number y such that

$$xy \equiv 1 \mod m.$$

For example, since $3 \cdot 5 \equiv 1 \mod 7$, 5 is the inverse of 3 modulo 7 and 3 is the inverse of 5 modulo 7.

(a) Find the inverse of 1 modulo 7.

(b) Find the inverse of 2 modulo 7.

(c) Find the inverse of 4 modulo 7.

(d) Find the inverse of 6 modulo 7.

13. Let n be a positive integer greater than 3. Show that n, $n+2$, and $n+4$ cannot all be prime.

14. Let a, b, s, t be integers. If $a \equiv b \mod st$, show that $a \equiv b \mod s$ and $a \equiv b \mod t$.

15. A United States Postal Service money order has an identification number consisting of 10 digits together with an extra digit called a *check*. The check digit is the 10-digit number modulo 9. Thus, the number 3953988164 has the check digit 2 since

$$3953988164 \equiv 2 \mod 9.$$

If the number 39539881642 were incorrectly entered into a computer (programmed to calculate the check digit) as, say, 39559881642 (an error in the fourth position), the machine would calculate the check as 4, whereas the entered check digit would be 2. Thus, the error would be detected.

(a) Determine the check digit for a money order with identification number 7234541780.

(b) Suppose that in one of the noncheck positions of a money order number, the digit 0 is substituted for the digit 9, or vice versa. Prove that this error will not be detected by the check digit. Prove that all other errors involving a single position are detected.

(c) Suppose that a money order with identification number and check digit 21720421168 is erroneously copied as 27750421168. Will the check digit detect the error?

(d) A transposition error involving distinct adjacent digits is one of the form

$$...ab... \to ...ba...$$

with $a \neq b$. Prove that the money order check digit scheme will not detect such errors until the check digit itself is transposed.

16. As you have shown in the previous problem, the method used by the Postal Service does not detect all single-digit errors. One method that does detect all single-digit errors, as well as nearly all errors involving the transposition of two adjacent digits, is the Universal Product Code (UPC). A UPC identification number has 12 digits. The first 6 digits identify the manufacturer, the next 5 identify the product, and the last is a check. To explain how the check digit is calculated, we introduce the dot product notation for two k-tuples:

$$(a_1, a_2, \ldots, a_k) \cdot (b_1, b_2, \ldots, b_k) = a_1b_1 + a_2b_2 + \cdots + a_kb_k.$$

An item with UPC identification number $a_1a_2 \cdots a_{12}$ satisfies the condition

$$(a_1, a_2, \ldots, a_{12}) \cdot (3, 1, 3, 1, \ldots, 3, 1) \equiv 0 \mod 10.$$

Thus, the the UPC identification number 021000658978 has check digit 8 because

$$0{\cdot}3+2{\cdot}1+1{\cdot}3+0{\cdot}1+0{\cdot}3+0{\cdot}1+6{\cdot}3+5{\cdot}1+8{\cdot}3+9{\cdot}1+7{\cdot}3+8{\cdot}1 = 90 \equiv 0 \mod 10.$$

(a) Determine the UPC check digit for the number 07312400508.

(b) Explain why the UPC check digit scheme will identify all single-digit errors.

(c) Show that the only undetected transposition errors of adjacent digits a and b in the UPC scheme are those in which $|a-b|=5$.

17. Identification numbers printed on bank checks (on the bottom left between the two colons) consist of an eight-digit number $a_1a_2\cdots a_8$ and a check digit a_9 so that
$$(a_1,a_2,\ldots,a_9)\cdot(7,3,9,7,3,9,7,3,9)\equiv 0 \mod 10.$$
As in the case for the UPC scheme, this method detects all single-digit errors and all errors involving the transposition of adjacent digits a and b except when $|a-b|=5$. It also detects most errors of the form $\cdots abc\cdots \to \cdots cba\cdots$, whereas the UPC method detects no errors of this form. Use this method to determine the check digit for the number 09190204.

18. The International Standard Book Number (ISBN) $a_1a_2\cdots a_{10}$ has the property that
$$(a_1,a_2,\ldots,a_{10})\cdot(10,9,8,7,6,5,4,3,2,1)\equiv 0 \mod 11.$$
The digit a_{10} is the check digit. When a_{10} is required to be 10 to satisfy the congruence, the character X is used as the check digit.

(a) The ISBN assigned to one of my favorite number theory books (that you will receive a copy of at the end of the session!) is 0-13-186137-9. Verify that this ISBN satisfies the necessary congruence.

(b) Verify the check digit for the ISBN assigned to your favorite book (or any book that you have with you).

(c) The ISBN 0-669-03925-4 is the result of a transposition of two adjacent digits not involving the first or last digit. Determine the correct ISBN.

Problem Set 2

Applications of Congruences

1. Compute 5^{15} modulo 7 and 7^{13} modulo 11.
2. Find the number of integers n, $1 \leq n \leq 25$, such that $n^2+15n+122$ is divisible by 6. Hint: $n^2+15n+122 \equiv n^2+3n+2 \equiv (n+1)(n+2) \mod 6$.
3. Find the remainder when $6^{83}+8^{83}$ is divided by 49.
4. Prove that if $9 \mid (a^3+b^3+c^3)$, then $3 \mid abc$, for integers a, b, c.
5. Prove that there are no integers x, y that satisfy the equation $x^2 - 7y = 3$.
6. Prove that if $7 \mid (a^2+b^2)$ then $7 \mid a$ and $7 \mid b$.
7. Show that if $x^3+y^3=z^3$, then one of x, y, z must be a multiple of 7.
8. Prove that there are no integers x, y, z that satisfy the equation
$$800000007 = x^2+y^2+z^2.$$
9. Prove that the sum of the decimal digits of a perfect square cannot be equal to 1991.
10. Prove that
$$7 \mid 4^{2^n} + 2^{2^n} + 1$$
for all natural numbers n.
11. Find the last two digits of 3^{100}.
12. Show that a perfect square is congruent to either 0, 1, or 4 modulo 8.
13. Show that for all positive integers n, $n^3 \equiv n \mod 3$.
14. Show that if $5 \nmid n$, then $n^4 \equiv 1 \mod 5$.
15. Show that any odd prime number p is either congruent to 1 modulo 4 or congruent to 3 modulo 4.
16. Find all possible values of the sum of two squares modulo 4. Use your result to show that the number 2003 cannot be written as the sum of two squares.
17. Suppose that m is an integer greater than or equal to 0. Show that
$$49 \mid 5 \cdot 3^{4m+2} + 53 \cdot 2^{5m}.$$
18. Show that there are infinitely many integers n such that
$$43 \mid (n^2+n+41).$$

19. Show that if $n^2 - 2$ and $n^2 + 2$ are both primes, then $3 \mid n$.
20. Show that an integer n is divisible by 9 if and only if the sum of its digits is divisible by 9.
21. Show that an integer $n = (d_k d_{k-1} \dots d_1 d_0)$ is divisible by 11 if and only if $d_k - d_{k-1} + d_{k-2} - \dots \pm d_0$ is divisible by 11.
22. Show that an integer n is divisible by 4 if and only if its last two digits are divisible by 4.
23. Show that an integer n is divisible by 8 if and only if its last three digits are divisible by 8.
24. Find the least positive integer x such that $13 \mid (x^2 + 1)$.
25. Prove that 19 is not a divisor of $4n^2 + 4$ for any integer n.
26. Prove that any number that is a square must have one of the following for its units digit: 0, 1, 4, 5, 6, 9
27. Prove that $n^6 - 1$ is divisible by 7 if $\gcd(n, 7) = 1$.
28. Prove that $n^7 - n$ is divisible by 42 for any integer n.
29. Prove that $n^{13} - n$ is divisible by 2, 3, 5, 7, and 13 for any integer n.
30. Prove that the product of three consecutive integers is divisible by 504 if the middle one is a cube.
31. What is the last digit of 3^{400}?
32. Let N be a number with 9 distinct non-zero digits, such that, for each k from 1 to 9 inclusive, the first k digits of N form a number which is exactly divisible by k. Find N (there is only one such number).
33. Let $f(n)$ denote the sum of the digits of n.

    (a) For any integer n, prove that eventually the sequence

    $$f(n), f(f(n)), f(f(f(n))), \dots$$

    will become constant. This constant value is called the **digital sum** of n.

    (b) Prove that the digital sum of the product of any two twin primes, other than 3 and 5, is 8. *Twin primes* are primes that are consecutive odd numbers, such as 17 and 19.

    (c) Let $N = 4444^{4444}$. Find $f(f(f(N)))$.
34. The Fermat numbers are defined as

    $$F_n = 2^{2^n} + 1.$$

    Show that every F_n is either a prime or a pseudoprime. A pseudoprime is a composite integer n such that $n \mid (2^n - 2)$.

Chapter 9

Linear Congruence Equations

Definition 9.1 An equation of the form

$$a_1x_1 + a_2x_2 + \cdots + a_kx_k \equiv b \mod m,$$

with unknowns $x_1, x_2, \ldots, x_k$ is a **linear congruence equation** in k variables. A **solution** to this equation is a set of *integers* which satisfies the equation.

Example 9.1 $x = 1,\ y = 2,\ z = 3$ is a solution to the linear congruence equation

$$x + y + z \equiv 6 \mod 7.$$

Example 9.2 Solve the congruence

$$x + 12 \equiv 5 \mod 8.$$

Solution: The key step is to observe that we can subtract 12 from both sides of the equivalence (by Theorem 7.2).

$$\begin{aligned} x + 12 &\equiv 5 \mod 8 \\ x &\equiv (5 - 12) \mod 8 \\ x &\equiv -7 \mod 8 \\ x &\equiv 1 \mod 8 \end{aligned}$$

Thus, any integer x that is congruent to 1 modulo 8 will satisfy the congruence.

Example 9.3 Solve the congruence

$$4x \equiv 3 \mod 19.$$

Solution: First, observe that we *cannot* simply divide both sides by 4. However, by Theorem 7.3, we can multiply both sides of the equivalence by 5. Thus we obtain:

$$\begin{aligned} 4x &\equiv 3 \mod 19 \\ 20x &\equiv 15 \mod 19 \\ x &\equiv 15 \mod 19 \text{ since } 20 \equiv 1 \mod 19. \end{aligned}$$

Thus, any integer x that is congruent to 15 modulo 19 will satisfy the congruence. We can, of course, check our answer by substituting 15 into the original congruence:

$$4 \cdot 15 = 60 \equiv 3 \mod 19.$$

Example 9.4 Solve the congruence

$$x^2 + 2x - 1 \equiv 0 \mod 7.$$

Solution: This is *not* a linear congruence, but it illustrates an important principle. Since we're not really sure how to approach this congruence, we can just try $x = 0, x = 1, \ldots, x = 6$. In general, to solve a congruence modulo m, we can just try each value $0, 1, \ldots, m-1$ for each variable. For the congruence $x^2 + 2x - 1 \equiv 0 \mod 7$, we find the solutions

$$x \equiv 2 \mod 7 \text{ and } x \equiv 3 \mod 7.$$

Of course, there are other solutions, such as $x \equiv 9 \mod 7$, but we note that 9 and 2 are not really *different* solutions since they are congruent modulo 2. When we are asked to "find all solutions of a congruence," we mean that we wish to find all incongruent solutions, i.e. all solutions that are not congruent to one another.

Example 9.5 Solve the congruence

$$x^2 \equiv 3 \mod 4.$$

Solution:

x modulo 4	x^2 modulo 4
0	0
1	1
2	0
3	1

Thus, the congruence $x^2 \equiv 3 \mod 4$ has no solutions.

Consider the linear congruence equation

$$ax \equiv b \mod m.$$

We would like to determine when this congruence has a solution, and when the solution is unique. When there is only one solution modulo m, we say that this solution is unique. Before we begin the general theory, let's look at a few examples.

Example 9.6 Solve the congruence

$$6x \equiv 15 \mod 514.$$

Solution: If x is a solution of this congruence, then

$$514 \mid (6x - 15).$$

Note that 514 is even, and $6x$ is even and 15 is odd, so $6x - 15$ is odd. Thus, $6x - 15$ cannot be divisible by the number 514, so the congruence has no solutions. Observe (for future reference) that $\gcd(6, 514) = 2$ and $2 \nmid 15$.

Example 9.7 Solve the congruence

$$3x \equiv 5 \mod 7.$$

Solution: We try $x = 0, 1, 2, 3, 4, 5, 6$, and find that $x \equiv 4 \mod 7$ is the unique solution to this congruence. Observe (for future reference) that $\gcd(3, 7) = 1$ and $1 \nmid 5$.

Example 9.8 Solve the congruence

$$9x \equiv 15 \mod 21.$$

Solution: We try $x = 0, 1, 2, \ldots, 21$, and find that $x \equiv 4, 11, 18 \mod 21$ are three incongruent solutions to this congruence. Observe (for future reference) that $\gcd(9, 21) = 3$ and $3 \mid 15$.

Example 9.9 Suppose that we wish to solve an arbitrary linear congruence of the form

$$ax \equiv b \mod m.$$

Then we must find an integer x so that

$$m \mid (ax - b).$$

Equivalently, we must find an integer y so that

$$my = ax - b,$$

which we can rewrite as

$$ax - my = b.$$

Now, this type of equation should look familiar, as it is precisely the type of equation that we solved in Chapter 5.

Let $g = (a, m)$. We know that every number of the form

$$ax - my$$

is a multiple of g (since $g \mid a$ and $g \mid m$), so if $g \nmid b$, then $ax - my = b$ has no solutions. Thus, if $g = (a, m) \nmid b$, then the congruence $ax \equiv b \mod m$ has no solutions.

Next, suppose that $g \mid b$. By Theorem 5.1, we know that there exist integers u and v such that

$$au + mv = g.$$

Now, since $g \mid b$, we can multiply this equation by the integer b/g to obtain the equation

$$a\frac{bu}{g} + m\frac{bv}{g} = b.$$

This implies that

$$m \mid a\frac{bu}{g} - b,$$

so

$$a\frac{bu}{g} \equiv b \mod m.$$

Thus,

$$x_0 \equiv \frac{bu}{g} \mod m$$

is a solution to the congruence $ax \equiv b \mod m$. Thus, we have shown that if $g = (a, m) \mid b$, then $x_0 \equiv \frac{bu}{g} \mod m$ is a solution of the congruence.

At this point, it is natural to consider whether or not this x_0 is the *only* solution of the congruence. Suppose that x_1 is some other solution of the congruence $ax \equiv b \mod m$. Then

$$ax_1 \equiv ax_0 \mod m,$$

so

$$m \mid (ax_1 - ax_0) = a(x_1 - x_0).$$

This implies that

$$\frac{m}{g} \text{ divides } \frac{a(x_1 - x_0)}{g}.$$

Now, $(a, m) = g$, so $\left(\frac{a}{g}, \frac{m}{g}\right) = 1$. Thus, a/g and m/g have no common factors, so m/g must divide $x_1 - x_0$. So there is an integer k such that

$$k\frac{m}{g} = x_1 - x_0,$$

or

$$x_1 = x_0 + k\frac{m}{g}.$$

Finally, recall that any two solutions that differ by a multiple of m are considered to be the same, so there will be exactly g different solutions that are obtained by taking $k = 0, 1, \ldots, g-1$. Note that if $g = (a, m) = 1$, then there will be exactly one solution of the congruence $a \equiv b \mod m$.

We summarize these results in the following theorem.

Theorem 9.1 Solutions of Linear Congruences. Let a, b, and m be integers with $m \geq 1$. Let $g = (a, m)$.

(a) If $g \nmid b$, then the congruence $ax \equiv b \mod m$ has no solutions.

(b) If $g \mid b$, then the congruence $ax \equiv b \mod m$ has g incongruent solutions. To find the solutions, first find integers u and v that satisfy

$$au + mv = g.$$

As described in Chapter 5, the Euclidean algorithm can be used to find such integers u and v. Then

$$x_0 = \frac{bu}{g}$$

is one solution to $ax \equiv b \mod m$. A complete set of g incongruent solutions is given by

$$x \equiv x_0 + k\frac{m}{g} \mod m \text{ for } k = 0, 1, 2, \ldots, g-1.$$

Example 9.10 Find all solutions of the congruence

$$943x \equiv 381 \mod 2576.$$

Solution: $g = (943, 2576) = 23 \nmid 381$, so the congruence has no solutions.

Example 9.11 Find all solutions of the congruence

$$8x \equiv 7 \mod 13.$$

Solution: $g = (8, 13) = 1$, so there is $g = 1$ solution of the congruence. Notice that we are able to determine the number of solutions without having computed the solution! To find the solution, we first find integers u and v so that

$$8u + 13v = 1.$$

Using methods from Chapter 5, we find the solution $u = 5$ and $v = -3$. Thus,

$$x_0 = \frac{7 \cdot 5}{1} = 35 \equiv 9 \mod 13$$

is a solution of the congruence.

Example 9.12 Find all solutions of the congruence

$$6x \equiv 9 \mod 15.$$

Solution: $g = (6, 15) = 3 \mid 9$, so there are $g = 3$ incongruent solutions of the congruence. Notice that we are able to determine the number of solutions without having computed any of them! To find the solutions, we first find integers u and v so that

$$6u + 15v = 3.$$

Using methods from Chapter 5, we find the solution $u = -2$ and $v = 1$. Thus,

$$x_0 = \frac{9 \cdot -2}{3} = -6 \equiv 9 \mod 15.$$

is a solution of the congruence. To obtain all of the solutions, we start with $x_0 = 9$ and add multiples of the quantity $\frac{15}{3} = 5$. The 3 incongruent solutions are

$$9, 14, 4.$$

Finally, we consider the situation in which we have more than one congruence equation in one unknown.

Example 9.13 Solve the system of congruences

$$\begin{aligned} x \equiv\ & 2 \mod 4 \\ x \equiv\ & 1 \mod 6. \end{aligned}$$

Solution: There is no common solution to both congruences since the first congruence requires x to be odd and the second requires x to be even.

Example 9.14 Solve the system of congruences

$$\begin{aligned} x \equiv\ & 2 \mod 4 \\ x \equiv\ & 3 \mod 5. \end{aligned}$$

Solution: By inspection, we note that $x = 18$ is a common solution. To find all solutions of the system, we proceed as follows. The first congruence is satisfied by x if and only if

$$4 \mid (x - 2),$$

i.e. if and only if there exists an integer k such that

$$x = 2 + 4k.$$

Substituting this in the second congruence, we obtain

$$2 + 4k \equiv 3 \mod 5,$$

which we rewrite as

$$4k \equiv 1 \mod 5.$$

Next, we observe that $k \equiv 1 \mod 5$ is the only solution of this congruence. Thus, k is a solution of $2 + 4k \equiv 3 \mod 5$ if and only if k can be written in the form

$$k = 4 + 5j,$$

where j is an integer. Thus, x satisfies both congruences if and only if there is an integer j such that

$$x = 2 + 4(4 + 5j) = 20j + 18.$$

Thus, the unique solution of the system of congruences is

$$x \equiv 18 \mod 20.$$

The situation that we observed here is an example of a more general result, as described in the following theorem.

Theorem 9.2 If $(m, n) = 1$, then the congruences

$$\begin{aligned} x \equiv & \quad a \mod m \\ x \equiv & \quad b \mod n \end{aligned}$$

have a unique common solution modulo mn.

Proof. The first congruence has a solution x if and only if

$$m \mid (x - a),$$

i.e. if and only if there exists an integer k such that

$$x = a + mk.$$

Then the second congruence becomes

$$mk \equiv (b - a) \mod n.$$

Since $(m, n) = 1$, this congruence has a unique solution modulo n, say

$$k \equiv c \mod n.$$

Thus, k satisfies $mk \equiv (b-a) \mod n$ if and only if there exists an integer j such that

$$k = c + nj,$$

where j is an integer. Thus,

$$x = a + mk = a + m(c + nj) = a + mc + mnk \equiv a + mc \mod mn.$$

All solutions are congruent to $(a+mc) \mod mn$, so there is a unique solution modulo mn.

This result is actually a special case of a more general theorem. Sun Tzu (or Sun Zi) was a Chinese mathematician, and is known for authoring *Sun Tzu Suan Ching* (literally "Sun Tzu's Calculation Classic") in the third-fourth century AD, which contains the Chinese Remainder Theorem. The following problem was posed: How many soldiers are there in Han Xing's army? If you let them parade in groups of 3 soldiers, there are 2 left over. If they parade in rows of 5, there are 3 left over. If they parade in rows of 7, there are 2 left over.

Theorem 9.3 Chinese Remainder Theorem. Let $m_1, m_2, \ldots, m_k$ be positive integers which are relatively prime in pairs. Then the k congruences

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

have a unique solution modulo $(m_1 m_2 \cdots m_k)$.

Example 9.15 Find a number n such that when divided by 4 leaves remainder 2, when divided by 5 leaves remainder 1, and when divided by 7 leaves remainder 1.

Solution: We want n such that

$$\begin{aligned} n \equiv & \quad 2 \quad \mod 4, \\ n \equiv & \quad 1 \quad \mod 5, \\ n \equiv & \quad 1 \quad \mod 7. \end{aligned}$$

This implies that

$$\begin{aligned} 35n \equiv & \quad 70 \quad \mod 140, \\ 28n \equiv & \quad 28 \quad \mod 140, \\ 20n \equiv & \quad 20 \quad \mod 140. \end{aligned}$$

We have $n \equiv 3(35n - 28n) - 20n \equiv 3(70 - 28) - 20 \equiv 106 \mod 140$. Thus all $n \equiv 106 \mod 140$ satisfy the given conditions.

Problem Set

1. Find all incongruent solutions to each of the following congruences.

   (a) $7x \equiv 3 \mod 15$

   (b) $6x \equiv 5 \mod 15$

   (c) $x^2 \equiv 1 \mod 8$

   (d) $x^2 \equiv 2 \mod 7$

   (e) $x^2 \equiv 3 \mod 7$

   (f) $8x \equiv 6 \mod 14$

   (g) $66x \equiv 100 \mod 121$

   (h) $21x \equiv 14 \mod 91$

2. Determine the number of incongruent solutions for each of the following congruences. You need not write down the actual solutions.

   (a) $893x \equiv 266 \mod 2432$

   (b) $72x \equiv 47 \mod 200$

   (c) $4183x \equiv 5781 \mod 15087$

   (d) $1537x \equiv 2863 \mod 6731$

3. Solve each of the following systems of congruences.

   (a)

$$\begin{aligned} x &\equiv 2 \mod 3 \\ x &\equiv 3 \mod 4 \end{aligned}$$

   (b)

$$\begin{aligned} x &\equiv 7 \mod 9 \\ x &\equiv 13 \mod 23 \\ x &\equiv 1 \mod 2 \end{aligned}$$

   (c)

$$\begin{aligned} 2x &\equiv 3 \mod 5 \\ 4x &\equiv 3 \mod 7 \end{aligned}$$

4. Find all incongruent solutions (or show that there are none) to

$$4x + y \equiv 6 \mod 12, \quad x + 4y \equiv 2 \mod 12.$$

5. Find all incongruent solutions to

$$3x + 4y \equiv 1 \mod 7.$$

6. Find all incongruent solutions to

$$3x + 7y \equiv 2 \mod 8.$$

7. Find all positive integers less than 1000 which leave remainder 1 when divided by 2, 3, 5, and 7.

8. A multiplication has been performed incorrectly, but the answer is correct mod 9, mod 10, and mod 11. What is the closest that the incorrect result can possibly be to the correct result?

9. The following multiplication was correct, but there is an x in place of a digit in the answer:

$$172195 \cdot 572167 = 985242x6565.$$

Find x without redoing the multiplication.

10. Show that an integer is divisible by 4 if and only if the number left when all digits other than the last two are eliminated is divisible by 4. Use this rule to find conditions for divisibility by 12.

11. Show that every integer satisfies at least one of the following six congruences: $x \equiv 0 \mod 2$, $x \equiv 0 \mod 3$, $x \equiv 1 \mod 4$, $x \equiv 1 \mod 6$, $x \equiv 3 \mod 8$, and $x \equiv 11 \mod 12$.

12. Prove the Chinese Remainder Theorem by induction.

13. Do there exist fourteen consecutive positive integers each of which is divisible by one or more primes $p, 2 \leq p \leq 11$?

14. Do there exist twenty-one consecutive integers each of which is divisible by one or more primes $p, 2 \leq p \leq 13$?

15. Let a, b, c be pairwise relatively prime integers. Show that $2abc - ab - bc - ca$ is the largest integer not of the form

$$bcx + acy + abz, \qquad x \geq 0, y \geq 0, z \geq 0.$$

16. What is the largest positive integer that is not the sum of a positive integral multiple of 42 and a positive composite integer?

Chapter 10

Fermat's Little Theorem

Let p be a prime number, and let a be any positive integer such that $a \not\equiv 0 \mod p$. In this section, we will consider powers of a (i.e. $a, a^2, a^3, \ldots$) modulo p.

Example 10.1 (a) Let $p = 3$. Compute a, a^2, a^3 modulo 3 for $a \equiv 0, 1, 2 \mod 3$.

a	a^2	a^3
0		
1		
2		

(b) Let $p = 5$. Compute a, a^2, a^3, a^4, a^5 modulo 5 for $a \equiv 0, 1, 2, 3, 4 \mod 5$.

a	a^2	a^3	a^4	a^5
0				
1				
2				
3				
4				

(c) Let $p = 7$. Compute $a, a^2, a^3, a^4, a^5, a^6, a^7$ modulo 7 for $a \equiv 0, 1, 2, 3, 4, 5, 6$ mod 7.

a	a^2	a^3	a^4	a^5	a^6	a^7
0						
1						
2						
3						
4						
5						
6						

(d) Based on the numerical evidence in these tables, we conjecture that

$$a^{p-1} \equiv 1 \mod p$$

and that

$$a^p \equiv a \mod p$$

for all $a \not\equiv 0 \mod p$. Create a similar table for $p = 11$ and observe that for $a = 1, 2, \ldots, 10$, we have $a^{10} \equiv 1 \mod 11$ and $a^{11} \equiv a \mod 11$.

Example 10.2 (a) Let $p = 5$ and $a = 2$. Compute the numbers

$$a, 2a, 3a, 4a \mod 5$$

and compare to the list of numbers $1, 2, 3, 4$. Repeat with $a = 3, 4$.

(b) Let$p = 7$ and $a = 2$. Compute the numbers

$$a, 2a, 3a, 4a, 5a, 6a \mod 7$$

and compare to the list of numbers $1, 2, 3, 4, 5, 6$. Repeat with $a = 3, 4, 5, 6$.

Theorem 10.1 Fermat's Little Theorem. Let p be a prime number, and let a be any number such that $a \not\equiv 0 \mod p$. Then

$$a^{p-1} \equiv 1 \mod p.$$

Proof. We will need the following result to prove Fermat's Little Theorem:

Lemma 10.2 Let p be a prime number, and let a be any number such that $a \not\equiv 0 \mod p$. Then the numbers

$$a, 2a, 3a, \ldots, (p-1)a \mod p$$

are the same as the numbers

$$1, 2, 3, \ldots, (p-1) \mod p,$$

although they may be in a different order.

Proof of the Lemma. First, observe that the list

$$a, 2a, 3a, \ldots, (p-1)a$$

contains $p-1$ numbers, and none of them are divisible by p. Next, suppose that two numbers, say ja and ka, in the list

$$a, 2a, 3a, \ldots, (p-1)a$$

are congruent modulo p. Then $ja \equiv ka \mod p$, so

$$p \mid (ja - ka) = (j-k)a.$$

Since $a \not\equiv 0 \mod p$, $p \nmid a$, so $p \mid (j-k)$ by Theorem 6.1. On the other hand, we know that $1 \leq j, k \leq p-1$, so $|j-k| < p-1$. However, there is only one number with absolute value less than $p-1$ that is divisible by p, and that number is zero. Thus, $j-k=0$, so $j=k$. We can conclude, therefore, that different multiples in the list

$$a, 2a, 3a, \ldots, (p-1)a$$

are distinct modulo p. Thus, the list

$$a, 2a, 3a, \ldots, (p-1)a$$

contains $p-1$ distinct non-zero values modulo p. However, there are only $p-1$ distinct nonzero values modulo p, namely

$$1, 2, 3, \ldots, (p-1).$$

We conclude that the list

$$a, 2a, 3a, \ldots, (p-1)a \mod p$$

must contain the same numbers as the list

$$1, 2, 3, \ldots, (p-1),$$

though the numbers may appear in a different order. This finishes the proof of Lemma 10.2.

We can now use Lemma 10.2 to prove Fermat's Little Theorem. Since the lists of numbers

$$a, 2a, 3a, \ldots, (p-1)a \mod p$$

and

$$1, 2, 3, \ldots, (p-1)$$

are the same, the product of the numbers in the first list is equal to the product of the numbers in the second list:

$$a \cdot 2a \cdot 3a \cdots (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdots (p-1) \mod p.$$

We can rewrite this equivalence as

$$a^{p-1}(p-1)! \equiv (p-1)! \mod p.$$

Finally, note that $\gcd((p-1)!, p) = 1$, so by Theorem 7.5, we can cancel the $(p-1)!$ from both sides to obtain Fermat's Little Theorem:

$$a^{p-1} \equiv 1 \mod p.$$

Note that we can multiply both sides by a to obtain

$$a^p \equiv a \mod p.$$

Example 10.3 Show that

$$23 \mid (6^{22} - 1).$$

Solution: By Fermat's Little Theorem,

$$6^{22} \equiv 1 \mod 23.$$

Example 10.4 Compute $2^{35} \mod 7$.

Solution: By Fermat's Little Theorem,

$$2^6 \equiv 1 \mod 7.$$

Thus we have:

$$\begin{aligned} 2^{35} &\equiv 2^{30}2^5 \mod 7 \\ &\equiv (2^6)^5 2^5 \mod 7 \\ &\equiv 2^5 \mod 7 \\ &\equiv 4 \mod 7. \end{aligned}$$

Example 10.5 Show that

$$341 \mid (2^{341} - 2).$$

Solution: Observe that $341 = 11 \cdot 31$. We'll show that both 11 and 31 are divisors of $2^{341} - 2$. By Fermat's Little Theorem,

$$2^{10} \equiv 1 \mod 11.$$

Thus,

$$2^{341} \equiv 2(2^{10})^{34} \equiv 2 \mod 11.$$

Thus,

$$11 \mid (2^{341} - 2).$$

Now,

$$2^5 \equiv 1 \mod 31.$$

Thus,

$$2^{341} \equiv 2(2^5)^{68} \equiv 2 \mod 31.$$

Thus,

$$31 \mid (2^{341} - 2).$$

Since $(11, 31) = 1$, their product also divides $2^{341} - 2$, i.e.

$$341 \mid (2^{341} - 2).$$

Example 10.6 Let

$$a_1 = 4, a_n = 4^{a_{n-1}}, n > 1.$$

Find the remainder when a_{100} is divided by 7.

Solution: By Fermat's Little Theorem, $4^6 \equiv 1 \mod 7$. Now, $4^n \equiv 4 \mod 6$ for all positive integers n, i.e., $4^n = 4 + 6t$ for some integer t. Thus

$$a_{100} \equiv 4^{a_{99}} \equiv 4^{4+6t} \equiv 4^4 \cdot (4^6)^t \equiv 4 \mod 7.$$

For the second equivalence above, we have used the fact that $a_{99} = 4^k$ for some integer k, so $a_{99} = 4 + 6t$ for some integer t.

Example 10.7 Fermat's Little Theorem can be used to show that a number is not prime without actually factoring it. For example, it can be shown that

$$2^{1234566} \equiv 899557 \not\equiv 1 \mod 1234567.$$

Thus, the number 1234567 cannot be a prime, since if it were, then Fermat's Little Theorem would tell us that $2^{1234566}$ must be congruent to 1 modulo 1234567.

Example 10.8 Solve the congruence

$$x^{103} \equiv 4 \mod 11.$$

Solution: By Fermat's Little Theorem,

$$x^{10} \equiv 1 \mod 11.$$

Thus,

$$x^{103} \equiv x^{100}x^3 \equiv x^3 \mod 11.$$

So, to solve the original congruence, we only need to solve $x^3 \equiv 4 \mod 11$. We can do this by trying successively $x = 0, 1, 2, \ldots, 10$. We find the solution

$$x \equiv 5 \mod 11.$$

Example 10.9 Does Fermat's Little Theorem apply to composite integers? Compute $2^8 \mod 9$, $3^7 \mod 8$, and $2^{14} \mod 15$.

Theorem 10.3 Existence and Uniqueness of Inverses. Suppose that $(a, m) = 1$. Then there exists a unique integer x such that $ax \equiv 1 \mod m$.

Proof. Observe that we must prove both existence and uniqueness. To prove existence, $(a, m) = 1$ implies that there exist integers x and y such that $ax + my = 1$. Thus,

$$my = 1 - ax \Rightarrow m \mid (1 - ax) \Rightarrow m \mid (ax - 1) \Rightarrow ax \equiv 1 \mod m.$$

To prove uniqueness, suppose that there exist two integers x_1 and x_2 such that

$$ax_1 \equiv ax_2 \equiv 1 \mod m.$$

Since $(a, m) = 1$, $x_1 \equiv x_2 \mod m$. Thus, a has a unique inverse mod m.

Example 10.10 Compute $(p-1)! \mod p$ for $p = 2, 3, 5, 7, 11, 13$. Make a conjecture about the value of $(p-1)! \mod p$.

Theorem 10.4 Wilson's Theorem. Suppose that p is a prime number. Then

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

Proof. Observe that

$$(p-1)! = (p-1)(p-2)(p-3)\cdots(2)(1).$$

By the previous theorem, each integer $1, 2, 3, \ldots, p-2, p-1$ has a unique inverse modulo p. Note that $1 \cdot 1 \equiv 1 \mod p$ and $(p-1)\cdot(p-1) \equiv 1 \mod p$, so 1 and $p-1$ are their own inverses. Moreover, we have seen that 1 and $p-1$ are the *only* x that satisfy $x^2 \equiv 1 \mod p$. Thus, each integer between 2 and $p-2$ has a unique inverse in the list $2, 3, \ldots, p-3, p-2$. Pairing each integer with its inverse modulo p, we obtain

$$\begin{aligned}(p-1)! &\equiv (p-1)(p-2)(p-3)\cdots(3)(2)(1) \mod p \\ &\equiv (p-1)\cdot 1 \cdot 1 \cdots 1 \mod p\end{aligned}$$

$$\equiv (p-1) \mod p.$$

Problem Set

1. Compute 9^{794} modulo 73.

2. Show that 91 is not prime by computing 2^{90} modulo 91.

3. Compute 2^7 modulo 7.

4. Compute 10^7 modulo 7.

5. Find all integers x such that $x^{86} \equiv 6 \mod 29$.

6. Find all integers x such that $x^{39} \equiv 3 \mod 13$.

7. If p is a prime number and if $a \not\equiv 0 \mod p$, then Fermat's Little Theorem tells us that $a^{p-1} \equiv 1 \mod p$.

   (a) The congruence $7^{1734250} \equiv 1660565 \mod 1734251$ is true. Can you conclude that 1734251 is composite?

   (b) The congruence $129^{64026} \equiv 15179 \mod 64027$ is true. Can you conclude that 64027 is composite?

   (c) The congruence $2^{52632} \equiv 1 \mod 52633$ is true. Can you conclude that 52633 is prime?

8. (a) Let p be a prime number. Show that

   $$p \mid (2^p - 2).$$

   (b) The ancient Chinese knew this result, and also believed that the converse was true. The converse states that if $n > 1$ and $n \mid (2^n - 2)$, then n is a prime number. It is probable that the Chinese observed this experimentally, but did not attempt to prove the conjecture. However, we know that the conjecture is wrong. For example, we have seen that

   $$341 \mid (2^{341} - 2),$$

   but $341 = 11 \cdot 31$ is not prime. We say that a composite integer n such that

   $$n \mid (2^n - 2)$$

   is a **pseudoprime**. There are infinitely many pseudoprimes. Show that $561 = 3 \cdot 11 \cdot 17$ is a pseudoprime.

9. Recall Wilson's Theorem: If p is a prime number, then

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

   Compute the value of $(m-1)! \mod m$ for some small values of m that are *not* prime. Do you observe any patterns? If you know the value of $(n-1)! \mod n$, how can you use this value to determine whether n is prime or composite?

10. Find all primes p such that $p \mid (2^p + 1)$.

11. If $(mn, 42) = 1$, prove that $168 \mid (m^6 - n^6)$.

12. If p is an odd prime prove that $n^p \equiv n \mod 2p$ for all integers n.

13. If p is an odd prime and $p \mid (m^p + n^p)$ prove that $p^2 \mid (m^p + n^p)$.

14. Prove that $19 \mid (2^{2^{6k+2}} + 3)$ for all integers $k \geq 0$.

15. Prove that if p is an odd prime

$$1^2 \cdot 3^2 \cdots (p-2)^2 \equiv 2^2 \cdot 4^2 \cdots (p-1)^2 \equiv (-1)^{(p+1)/2} \mod p.$$

16. Show that if p is a prime, a is an integer, and k is a nonnegative integer, then

$$a^{1+k(p-1)} \equiv a \mod p.$$

17. Show that if n is odd and a is an integer, then

$$a^n \equiv a \mod 3.$$

Chapter 11

Euler's Phi-Function and The Euler-Fermat Theorem

Definition 11.1 For $n \geq 1$, let $\phi(n)$ denote the number of positive integers that are less than or equal to n and relatively prime to n.

Example 11.1 $\phi(6) = 2$ since 1 and 5 are the only integers that are less than or equal to 6 and relatively prime to 6.

Example 11.2 Find the value of $\phi(m)$ for each m in the table below.

m	1	2	3	4	5	6	7	8	9	10
$\phi(m)$										

Theorem 11.1 For any prime p,

$$\phi(p) = p - 1$$

since every positive integer less than a prime p is relatively prime to p.

Example 11.3

1. Let $m = 6$. Compute $a^{\phi(m)} \mod m$ for $a = 1, 5$.
2. Let $m = 9$. Compute $a^{\phi(m)} \mod m$ for $a = 1, 2, 4, 5, 7, 8$.
3. Let $m = 10$. Compute $a^{\phi(m)} \mod m$ for $a = 1, 3, 7, 9$.

Based on the numerical evidence that we obtained in the previous example, we conjecture the following.

Theorem 11.2 Euler-Fermat Theorem. If $(a, m) = 1$, then

$$a^{\phi(m)} \equiv 1 \mod m.$$

Proof. The proof of the Euler-Fermat theorem is very similar to the proof of Fermat's Little Theorem, and will be left to you to complete as an exercise.

Note that Fermat's Little Theorem is actually a special case of the Euler-Fermat Theorem: If p is a prime number, then $\phi(p) = p - 1$.

To use the Euler-Fermat Theorem in problems and applications, we need an efficient method for computing $\phi(m)$ for arbitrary (i.e. not necessarily prime) integers m. If m is small, then it is fairly easy to find all the numbers less than or equal to m that are relatively prime to m. However, if m is large, then we do not want to have to write down all integers less than or equal to m and determine whether or not they are relatively prime to m. We'll begin by considering powers of primes.

Theorem 11.3 If p is a prime number, then

$$\phi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1) = p^k\left(1 - \frac{1}{p}\right).$$

Proof. By definition, $\phi(p^k)$ is the number of integers less than or equal to p^k that are relatively prime to p^k. There are p^k integers less than or equal to p^k. Thus,

$$\phi(p^k) = p^k - (\text{number of integers } \le p^k \text{ that are not relatively prime to } p^k.$$

The integers less than or equal to p^k that are not relatively prime to p^k are precisely those that are divisible by p. There are p^{k-1} such integers:

$$1 \cdot p, 2 \cdot p, 3 \cdot p, \ldots, p \cdot p^{k-1}.$$

Thus,

$$\phi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1) = p^k\left(1 - \frac{1}{p}\right).$$

Finally, we'll consider general composite numbers.

Example 11.4 1. Compute $\phi(6)$, $\phi(2)$, and $\phi(3)$. How do these values relate to one another?

2. Compute $\phi(10)$, $\phi(2)$, and $\phi(5)$. How do these values relate to one another?

3. Compute $\phi(30)$, $\phi(5)$, and $\phi(6)$. How do these values relate to one another?

4. Compute $\phi(72)$, $\phi(8)$, and $\phi(9)$. How do these values relate to one another?

Theorem 11.4 If $(a, b) = 1$, then $\phi(ab) = \phi(a)\phi(b)$.

Proof. Let n be a natural number with $n = ab, (a, b) = 1$. We arrange the ab integers $1, 2, \ldots, ab$ as follows.

$$\begin{array}{rrrlrll}
1 & 2 & 3 & \ldots & k & \ldots & a \\
a+1 & a+2 & a+3 & \ldots & a+k & \ldots & 2a \\
2a+1 & 2a+2 & 2a+3 & \ldots & 2a+k & \ldots & 3a \\
\ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\
(b-1)a+1 & (b-1)a+2 & (b-1)a+3 & \ldots & (b-1)a+k & \ldots & ba
\end{array}$$

Now, an integer r is relatively prime to m if and only if it is relatively prime to a and b. We shall determine first the number of integers in the above array that are relatively prime to a and find out how may of them are also relatively prime to b.

There are $\phi(a)$ integers relatively prime to a in the first row. Now consider the k-th column, $1 \leq k \leq a$. Each integer on this column is of the form $ma+k, 0 \leq m \leq b-1$. As $k \equiv ma + k \mod a$, k will have a common factor with a if and only if $ma + k$ does. This means that there are exactly $\phi(a)$ columns of integers that are relatively prime to a. We must determine how many of these integers are relatively prime to b.

We claim that no two integers $k, a+k, 2a+k, \ldots, (b-1)a+k$ on the k-th column are congruent modulo b. Suppose that $(ia+k) \equiv (ja+k) \mod b$. Then $a(i-j) \equiv 0 \mod b$. Thus, $b \mid a(i-j)$, so $b \mid a$ or $b \mid (i-j)$. Since $(a, b) = 1$, $b \nmid a$. Thus, $b \mid (i-j)$, so $(i-j) \equiv 0 \mod b$. Now $i, j \in [0, b-1]$ which implies that $|i-j| < b$. However, the only integer $(i-j)$ such that $|i-j| < b$ and $b \mid (i-j)$ is 0. This forces $i - j - 0$, so $i = j$. This means that the b integers in any of these $\phi(n)$ columns are, in some order, congruent to the integers $0, 1, \ldots, b-1$. But exactly $\phi(b)$ of these are relatively prime to b. This means that exactly $\phi(a)\phi(b)$ integers on the array are relatively prime to ab, so

$$\phi(n) = \phi(ab) = \phi(a)\phi(b).$$

Note. We say that a function $f : \mathbb{Z}^+ \to \mathbb{R}$ is **multiplicative** if

$$f(mn) = f(m)f(n)$$

for every pair of integers m, n such that

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

Thus, Theorem 11.4 says that Euler's phi-function is multiplicative.

Using Theorems 11.3 and 11.4, we can now obtain a general formula for $\phi(n)$.

Theorem 11.5 Let

$$n = p_1^{a_1} p_2^{a_2} \cdots p_m^{a_m}$$

be the prime factorization of n, where $p_1, p_2, \ldots, p_m$ are distinct primes and $a_1, a_2, \ldots, a_m$ are integers greater than or equal to 1. Then

$$\begin{aligned} \phi(n) &= \left(p_1^{a_1} - p_1^{a_1-1}\right)\left(p_2^{a_2} - p_2^{a_2-1}\right)\cdots\left(p_m^{a_m} - p_m^{a_m-1}\right) \\ &= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_m}\right). \end{aligned}$$

Example 11.5 Find $\phi(100)$.

Solution: We do *not* need to list the integers less than or equal to 100 and determine which are relatively prime to 100. Instead, we use Theorem 11.5. The prime factorization of 100 is

$$100 = 2^2 5^2.$$

Thus,

$$\begin{aligned} \phi(100) &= 100\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right) \\ &= 40. \end{aligned}$$

Example 11.6 Find infinitely many integers n such that $10 \mid \phi(n)$.

Solution: Take $n = 11^k$ for $k = 1, 2, \ldots$. Then $\phi(11^k) = 11^k - 11^{k-1} = 10 \cdot 11^{k-1}$, so

$$10 \mid \phi(11^k)$$

for all integers $k \geq 1$.

Example 11.7 Find the last two digits of 3^{1000}.

Solution: To find the last two digits of 3^{1000}, we need to compute

$$3^{1000} \text{ modulo } 100.$$

We know that

$$\phi(100) = \phi(2^2)\phi(5^2) = 40,$$

so by the Euler-Fermat Theorem,

$$3^{40} \equiv 1 \mod 100.$$

Thus,

$$3^{1000} = (3^{40})^{25} \equiv 1^{25} = 1 \mod 100,$$

so the last two digits are 01.

Example 11.8 Find the last 2 digits of $7^{7^{1000}}$.

Solution: Note that $7^{40} \equiv 1 \mod 100$. Now, $\phi(40) = 16$, so

$$\begin{aligned} 7^{16} &\equiv 1 \mod 40 \\ 7^{1000} &\equiv (7^{16})^{62} 7^8 \mod 40 \\ &\equiv 7^8 \equiv (7^4)^2 \equiv 1 \mod 40 \end{aligned}$$

Thus, $40 \mid 7^{1000} - 1$, so there exists an integer t such that $7^{1000} = 40t + 1$. Thus,

$$7^{7^{1000}} = 7^{40t+1} \equiv 7 \mod 100.$$

Problem Set

1. Find the value of $\phi(20)$.
2. Find the value of $\phi(60)$.
3. Find the value of $\phi(63)$.
4. Find the value of $\phi(97)$.
5. Find the value of $\phi(341)$.
6. Find the value of $\phi(561)$.
7. Find the value of $\phi(8800)$.
8. Show that if n is odd, then $\phi(2n) = \phi(n)$.
9. Show that if n is even, then $\phi(2n) = 2\phi(n)$.
10. Let x be the *smallest* positive integer such that

    $$2^x \equiv 1 \mod 63.$$

    Find x, and verify that $x \mid \phi(63)$.
11. Find the last three digits of 7^{9999}.
12. (a) The positive divisors of 6 are 1, 2, 3, and 6. Compute $\phi(1) + \phi(2) + \phi(3) + \phi(6)$.

    (b) The positive divisors of 8 are 1, 2, 4, and 8. Compute $\phi(1) + \phi(2) + \phi(4) + \phi(8)$.

    (c) The positive divisors of 9 are 1, 3, and 9. Compute $\phi(1) + \phi(3) + \phi(9)$.

    (d) Let $n \geq 1$. Make a conjecture about the value of

    $$\sum_{d|n} \phi(d),$$

    where the sum is taken over all of the divisors d of n. Try to prove that your conjecture is correct. To prove that your conjecture is correct, it may be useful to use the result of the next problem.
13. Recall that a function f is said to be *multiplicative* if $f(mn) = f(m)f(n)$ for all integers m and n such that $(m, n) = 1$. We know that Euler's ϕ-function is multiplicative. Suppose that f is a multiplicative function, and define a new function $g(n)$ as follows:

    $$g(n) = f(d_1) + f(d_2) + \cdots + f(d_r),$$

    where $d_1, d_2, \ldots, d_r$ are the divisors of n. Show that $g(n)$ is multiplicative.

14. What can you say about n if the value of $\phi(n)$ is a prime number? What if the value of $\phi(n)$ is the square of a prime number.

15. Find at least five different numbers n such that $\phi(n) = 160$.

16. Suppose that the integer n satisfies $\phi(n) = 1000$. Make a list of all the primes that might possibly divide n. Use this information to find all integers n that satisfy $\phi(n) = 1000$.

17. Find all values of n that satisfy each of the following equations:

    (a) $\phi(n) = n/2$
    (b) $\phi(n) = n/3$
    (c) $\phi(n) = n/6$

18. Find the remainder of
$$10^{10} + 10^{10^2} + \cdots + 10^{10^{10}}$$
upon division by 7.

19. (a) For each integer $2 \leq a \leq 10$, find the last four digits of a^{1000}.
    (b) Based on your experiments in (a), and further experiments if necessary, give a simple criterion that allows you to predict the last four digits of a^{1000} from the value of a.
    (c) Prove that your criterion in (b) is correct.

20. Show that for all natural numbers s, there is an integer n divisible by s such that the sum of the digits of n is equal to s.

21. Prove that $504 \mid (n^9 - n^3)$ for all integers $n \geq 1$.

22. Prove that for any odd integer $n > 0$, $n \mid (2^{n!} - 1)$.

23. Prove that for every natural number n there exists some power of 2 whose final n digits are all ones and twos.

24. Prove that there exists a positive integer k such that $k \cdot 2^n + 1$ is composite for every positive integer n.

25. Suppose that p and q are different odd primes and that a is an integer such that $(a, pq) = 1$. Show that
$$a^{\phi(pq)/2} \equiv 1 \mod pq.$$

26. Show that if $n > 2$, then $2 \mid \phi(n)$.

27. In this series of exercises, you will prove the Euler-Fermat Theorem. Let n be an integer greater than or equal to 1, and let a be an integer such that $(a, n) = 1$. Let
$$1 = b_1 < b_2 < \cdots < b_{\phi(n)} < n$$
be the $\phi(n)$ numbers between 0 and n that are relatively prime to n.

(a) Show that the numbers

$$b_1a, b_2a, \ldots, b_{\phi(n)}a \mod n$$

are the same as the numbers

$$b_1, b_2, \ldots, b_{\phi(n)} \mod n,$$

although they may be in a different order.

(b) Show that

$$(b_1a) \cdot (b_2a) \cdots (b_{\phi(n)}a) \equiv b_1 \cdot b_2 \cdots b_{\phi(n)} \mod n.$$

(c) Conclude that

$$a^{\phi(n)} \equiv 1 \mod n.$$

28. Liouville's lambda function $\lambda(n)$ is defined by factoring n into a product of primes,

$$n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$$

and then setting

$$\lambda(n) = (-1)^{k_1+k_2+\cdots k_r}.$$

We define $\lambda(1) = 1$. For example, to compute $\lambda(1728)$, we factor $1728 = 2^6 3^3$, and obtain

$$\lambda(1728) = (-1)^{6+3} = -1.$$

(a) Compute the following: $\lambda(30)$; $\lambda(504)$; $\lambda(60750)$.

(b) We use Liouville's lambda function to define a new function $G(n)$ by the formula

$$G(n) = \lambda(d_1) + \lambda(d_2) + \cdots + \lambda(d_r),$$

where $d_1, d_2, \ldots, d_r$ are the divisors of n. Compute the value of $G(n)$ for all $1 \leq n \leq 18$.

(c) Use your computations in (b), and additional computations if necessary, to make a conjecture for the value of $G(n)$. Prove that your conjecture is correct.

29. Recall that a function f is said to be *multiplicative* if $f(mn) = f(m)f(n)$ for all integers m and n such that $(m, n) = 1$. Show that Liouville's lambda function $\lambda(n)$ is multiplicative.

Chapter 12

Primitive Roots

We know by the Euler-Fermat Theorem that if $(a, n) = 1$, then

$$a^{\phi(n)} \equiv 1 \mod n,$$

and that if p is a prime number, then

$$a^{p-1} \equiv 1 \mod p$$

since $\phi(p) = p - 1$. However, $\phi(n)$ may not be the *smallest* integer b such that

$$a^b \equiv 1 \mod n.$$

For example, by Fermat's Little Theorem, we know that

$$2^6 \equiv 1 \mod 7.$$

However,

$$2^3 \equiv 1 \mod 7$$

is the smallest power of 2 that is congruent to 1 modulo 7. On the other hand, there may be some values of a that require the full $(p-1)$-st power. For example, the first power of 3 that is congruent to 1 modulo 7 is 3^6. Let's look at some more examples to try to deduce a pattern. For now, we'll consider the case

$$a^b \equiv 1 \mod p$$

where p is a prime.

Example 12.1 Complete the table below for $p = 5$. Let b denote the smallest integer such that $a^b \equiv 1 \mod p$. Recall that

$$\phi(5) = 5 - 1 = 4.$$

a	b such that $a^b \equiv 1 \mod 5$
1	
2	
3	
4	

Example 12.2 Complete the table below for $p = 7$. Let b denote the smallest integer such that $a^b \equiv 1 \mod p$. Recall that

$$\phi(7) = 7 - 1 = 6.$$

a	b such that $a^b \equiv 1 \mod 7$
1	
2	
3	
4	
5	
6	

Example 12.3 Complete the table below for $p = 11$. Let b denote the smallest integer such that $a^b \equiv 1 \mod p$. Recall that

$$\phi(11) = 11 - 1 = 10.$$

a	b such that $a^b \equiv 1 \mod 11$
1	
2	
3	
4	
5	
6	
7	
8	
9	
10	

Based on the numerical evidence in the tables above, we make the following observations:

1. The smallest exponent b so that $a^b \equiv 1 \mod p$ seems to divide $\phi(p) = p - 1$.
2. There are always some values of a that require the full $(p-1)$-st power.

Definition 12.1 Suppose that a is a positive integer such that $(a, p) = 1$. The **order** of a modulo p is the smallest positive integer b such that

$$a^b \equiv 1 \mod p,$$

and we write

$$b = \text{ord}_p(a).$$

By Fermat's Little Theorem, we know that

$$\mathrm{ord}_p(a) \leq \phi(p) = p - 1.$$

Theorem 12.1 Order Divisibility Property. Let a be an integer such that $(a, p) = 1$, and suppose that

$$a^n \equiv 1 \mod p.$$

Then

$$\mathrm{ord}_p(a) \mid n.$$

In particular,

$$\mathrm{ord}_p(a) \mid p - 1.$$

Proof. By definition,

$$a^{\mathrm{ord}_p(a)} \equiv 1 \mod p.$$

Suppose that

$$a^n \equiv 1 \mod p.$$

Let $g = \gcd(\mathrm{ord}_p(a), n)$. By Theorem 5.1, we know that there are integers u and v such that

$$\mathrm{ord}_p(a)u - nv = g.$$

Then, for any integer t, we have

$$g = \mathrm{ord}_p(a)(u + nt) - n(v + \mathrm{ord}_p(a)t),$$

and by choosing t to be sufficiently large, both $u+nt$ and $v+\mathrm{ord}_p(a)t$ will be positive. Thus, there are integers r and s such that

$$g = \mathrm{ord}_p(a)r - ns,$$

where r and s are both positive (you will see why we need them to be positive soon). Next, we compute the quantity

$$a^{\mathrm{ord}_p(a)r}$$

in two different ways:

$$\begin{aligned} a^{\mathrm{ord}_p(a)r} &= \left(a^{\mathrm{ord}_p(a)}\right)^r \equiv 1^r \equiv 1 \mod p \\ a^{\mathrm{ord}_p(a)r} &= a^{g+ns} = a^g \left(a^n\right)^s \equiv a^g \cdot 1^s \equiv a^g \mod p \end{aligned}$$

Thus, $a^g \equiv 1 \mod p$. Now, recall that $\mathrm{ord}_p(a)$ is the smallest power of a that is congruent to 1 modulo p. Thus,

$$\mathrm{ord}_p(a) \leq g.$$

On the other hand, $g = \gcd(\text{ord}_p(a), n)$, so

$$g \mid \text{ord}_p(a) \text{ and } g \mid n.$$

In particular,

$$g \leq \text{ord}_p(a).$$

We conclude that

$$g = \text{ord}_p(a),$$

so

$$\text{ord}_p(a) \mid n.$$

Finally, by Fermat's Little Theorem,

$$a^{p-1} \equiv 1 \mod p,$$

so

$$\text{ord}_p(a) \mid p - 1.$$

Definition 12.2 If

$$\text{ord}_p(a) = p - 1,$$

then a is called a **primitive root modulo** p.

Example 12.4 Using the tables that we created for $p = 5, 7, 11$, we observe that 2 and 3 are primitive roots modulo 5; 3 and 5 are primitive roots modulo 7; and 2, 6, 7, and 8 are primitive roots modulo 11.

Theorem 12.2 Primitive Root Theorem. Let p be a prime and suppose that $d \mid (p - 1)$. Then there are exactly $\phi(d)$ distinct integers a modulo p such that $\text{ord}_p(a) = d$. In particular, there are exactly $\phi(p - 1)$ primitive roots of p.

We will not give a proof of the Primitive Root Theorem here.

Example 12.5 The Primitive Root Theorem says that there are $\phi(10) = 4$ primitive roots modulo 11. We have found that there are indeed 4 primitive roots modulo 11–namely, 2, 6, 7, and 8. Similarly, there are $\phi(36) = 12$ primitive roots modulo 37 and $\phi(9906) = 3024$ primitive roots modulo 9907.

The following is an important property of primitive roots.

Theorem 12.3 Suppose that g is a primitive root modulo a prime p. Then every nonzero number modulo p can be expressed as a power of g. More precisely, for any number $1 \leq a < p$, we can pick out exactly one of the numbers

$$g, g^2, g^3, \ldots, g^{p-3}, g^{p-2}, g^{p-1}$$

as being congruent to a modulo p.

Proof. Since g is a primitive root modulo p,

$$g^{p-1} \equiv 1 \mod p,$$

and $p-1$ is the smallest integer b such that $g^b \equiv 1 \mod p$. Next, we claim that the numbers

$$g, g^2, g^3, \ldots, g^{p-3}, g^{p-2}, g^{p-1}$$

are all distinct modulo p. If not, then there would be exponents i and j such that $1 \leq i < j \leq p-1$ such that

$$g^j \equiv g^i \mod p.$$

Then

$$p \mid (g^j - g^i) = g^i(g^{j-i} - 1).$$

Thus,

$$p \mid g^i \text{ or } p \mid g^{j-i} - 1.$$

We know that $p \nmid g^i$ since $\gcd(g, p) = 1$. Thus,

$$p \mid g^{j-i} - 1,$$

so

$$g^{j-i} \equiv 1 \mod p,$$

and $j - i < p - 1$. This is a contradiction since $p-1$ is the smallest integer b such that $g^b \equiv 1 \mod p$. Thus, the numbers

$$g, g^2, g^3, \ldots, g^{p-3}, g^{p-2}, g^{p-1}$$

are distinct modulo p, so any number a such that $1 \leq a < p$ can be expressed as a power of g.

Note that the Primitive Root Theorem tells us that there are exactly $\phi(p-1)$ primitive roots modulo a given prime p. However, the theorem does not give us any information about how to find the primitive roots or about which specific numbers will be primitive roots modulo a given prime p. A natural question is the following: given a number a, for which primes p is a a primitive root? For example, we find that 2 is a primitive root for the primes

$$p = 3, 5, 11, 13, 19, 29, 37, 53, 59, 61, 67, 83.$$

Artin's Conjecture. There are infinitely many primes p such that 2 is a primitive root mod p.

Theorem 12.4 Let p be a prime. The congruence

$$x^2 + 1 \equiv 0 \mod p$$

has solutions if $p = 2$ or if $p \equiv 1 \mod 4$ but does not have any solutions if $p \equiv 3 \mod 4$.

Proof.

- When $p = 2$, $x = 1$ is a solution since
$$1^1 + 1 \equiv 0 \mod 2.$$

- Suppose that $p \equiv 1 \mod 4$. Then $4 \mid (p-1)$, so by the Primitive Root Theorem, there is an integer a such that
$$\mathrm{ord}_p(a) = 4.$$
Thus,
$$a^4 \equiv 1 \mod p,$$
so
$$a^4 - 1 \equiv (a^2-1)(a^2+1) \equiv 0 \mod p.$$
This implies that either
$$a^2 - 1 \equiv 0 \mod p$$
or
$$a^2 + 1 \equiv 0 \mod p.$$
Note that $a^2 - 1 \not\equiv 0 \mod p$ since $\mathrm{ord}_p(a) = 4$. Thus,
$$a^2 + 1 \equiv 0 \mod p,$$
so a is a solution of
$$x^2 + 1 \equiv 0 \mod p.$$

- Suppose that $p \equiv 3 \mod 4$. Then $4 \mid (p-3)$, so $4 \nmid (p-1)$. Since p is odd, $p-1$ is even, so $2 \mid (p-1)$. Thus, $(p-1, 4) = 2$. Now, suppose (by way of contradiction) that there is an integer a such that
$$a^2 + 1 \equiv 0 \mod p.$$
Then
$$a^4 \equiv (a^2)^2 \equiv (-1)^2 \equiv 1 \mod p.$$
By Fermat's Little Theorem, we also know that
$$a^{p-1} \equiv 1 \mod p.$$
Since $2 = (p-1, 4)$, there are integers u and v such that $2 = (p-1)s + 4t$. Thus, we have
$$a^2 \equiv a^{(p-1)s+4t} \equiv (a^{p-1})^s (a^4) t \equiv 1 \mod p.$$
Then
$$a^2 \equiv 1 \equiv -1 \mod p,$$

so

$$2 \equiv 0 \mod p.$$

This implies that

$$p \mid 2,$$

which is a contradiction since p is an odd prime. Thus, there is no integer a such that $a^2 + 1 \equiv 0 \mod p$, so the congruence

$$x^2 + 1 \equiv 0 \mod p$$

does not have any solutions in this case.

Finally, we note that the ideas of *order* and *primitive roots* can be extended to all (i.e. not necessarily prime) positive integers.

Definition 12.3 Suppose that $(a, n) = 1$. The **order** of a modulo n is the smallest positive integer b such that

$$a^b \equiv 1 \mod n.$$

By the Euler-Fermat Theorem, we know that

$$a^{\phi(n)} \equiv 1 \mod n.$$

Thus, $\text{ord}_n(a) \leq \phi(n)$. Using an argument similar to that given in the proof of Theorem 12.1, we can prove the following result.

Theorem 12.5 Suppose that $(a, n) = 1$ and that

$$a^b \equiv 1 \mod n.$$

Then

$$\text{ord}_n(a) \mid b,$$

and in particular,

$$\text{ord}_n(a) \mid \phi(n).$$

Definition 12.4 If $(a, n) = 1$ and $\text{ord}_n(a) = \phi(n)$, then we say that a is a **primitive root** modulo p.

Example 12.6 3 is a primitive root modulo 10 since $\phi(10) = 4$ and $3^1 \equiv 3 \mod 10$, $3^2 \equiv 9 \mod 10$, $3^3 \equiv 7 \mod 10$, $3^4 \equiv 1 \mod 10$.

Problem Set

1. Compute each of the following.

   (a) $\text{ord}_5(3)$

   (b) $\text{ord}_5(4)$

   (c) $\text{ord}_7(3)$

   (d) $\text{ord}_9(2)$

   (e) $\text{ord}_{15}(2)$

   (f) $\text{ord}_{16}(3)$

   (g) $\text{ord}_{10}(3)$

2. Find all primitive roots modulo 5.

3. Find all primitive roots modulo 7.

4. (a) Find all primitive roots modulo 13.

   (b) For each number d dividing 12, list the a's such that $1 \leq a < 13$ and $\text{ord}_{13}(1) = d$.

5. Find all primes less than 20 for which 3 is a primitive root.

6. In this exercise, you will investigate the value of $\text{ord}_n(2)$ for odd integers n.

   (a) Compute the value of $\text{ord}_n(2)$ for each odd number $3 \leq n \leq 19$.

   (b) In the table below, the value of $\text{ord}_n(2)$ is given for all odd numbers between 21 and 115.

$\text{ord}_{21}(2) = 6$	$\text{ord}_{23}(2) = 11$	$\text{ord}_{25}(2) = 20$	$\text{ord}_{27}(2) = 18$
$\text{ord}_{29}(2) = 28$	$\text{ord}_{31}(2) = 5$	$\text{ord}_{33}(2) = 10$	$\text{ord}_{35}(2) = 12$
$\text{ord}_{37}(2) = 36$	$\text{ord}_{39}(2) = 12$	$\text{ord}_{41}(2) = 20$	$\text{ord}_{43}(2) = 14$
$\text{ord}_{45}(2) = 12$	$\text{ord}_{47}(2) = 23$	$\text{ord}_{49}(2) = 21$	$\text{ord}_{51}(2) = 8$
$\text{ord}_{53}(2) = 52$	$\text{ord}_{55}(2) = 20$	$\text{ord}_{57}(2) = 18$	$\text{ord}_{59}(2) = 58$
$\text{ord}_{61}(2) = 60$	$\text{ord}_{63}(2) = 6$	$\text{ord}_{65}(2) = 12$	$\text{ord}_{67}(2) = 66$
$\text{ord}_{69}(2) = 22$	$\text{ord}_{71}(2) = 35$	$\text{ord}_{73}(2) = 9$	$\text{ord}_{75}(2) = 20$
$\text{ord}_{77}(2) = 30$	$\text{ord}_{79}(2) = 39$	$\text{ord}_{81}(2) = 54$	$\text{ord}_{83}(2) = 82$
$\text{ord}_{85}(2) = 8$	$\text{ord}_{87}(2) = 28$	$\text{ord}_{89}(2) = 11$	$\text{ord}_{91}(2) = 12$
$\text{ord}_{93}(2) = 10$	$\text{ord}_{95}(2) = 36$	$\text{ord}_{97}(2) = 48$	$\text{ord}_{99}(2) = 30$
$\text{ord}_{101}(2) = 100$	$\text{ord}_{103}(2) = 51$	$\text{ord}_{105}(2) = 12$	$\text{ord}_{107}(2) = 106$
$\text{ord}_{109}(2) = 36$	$\text{ord}_{111}(2) = 36$	$\text{ord}_{113}(2) = 28$	$\text{ord}_{115}(2) = 44$

   Using your result from (a) and this table, find a formula for $\text{ord}_{mn}(2)$ in terms of $\text{ord}_m(2)$ and $\text{ord}_n(2)$ when $(m, n) = 1$. Use your formula to find $\text{ord}_{11227}(2)$. Note that $11227 = 103 \cdot 109$.

(c) Use your results from (a) and the table to find a formula for $\text{ord}_{p^k}(2)$ in terms of $\text{ord}_p(2)$ and k, where p is a prime. Use your formula to find the value of $\text{ord}_{68921}(2)$. Note that $68921 = 41^3$.

7. Let p be a prime number.

   (a) What is the value of

$$(1 + 2 + 3 + \cdots + (p - 1)) \mod p?$$

   (b) What is the value of

$$(1^2 + 2^2 + 3^2 + \cdots + (p - 1)^2) \mod p?$$

   (c) For any positive integer k, find the value of

$$(1^k + 2^k + 3^k + \cdots + (p - 1)^k) \mod p.$$

8. Suppose that a and n are integers such that $(a, n) = 1$. Prove that

$$\text{ord}_n(a) \mid \phi(n).$$

   Hint: see the proof of the Order Divisibility Property.

9. (a) If g is a primitive root modulo 37, which of the numbers $g^2, g^3, \ldots, g^8$ are also primitive roots modulo 37?

   (b) If g is a primitive root modulo p, develop an easy-to-use rule for determining if g^k is a primitive root modulo p, and prove that your rule is correct.

   (c) Suppose that g is a primitive root modulo the prime $p = 21169$. Use your rule from (b) to determine which of the numbers $g^2, g^3, \ldots, g^{20}$ are primitive roots modulo 21169.

10. Suppose that p is a prime such that $p \equiv 3 \mod 4$ and that a and b are integers such that

$$a^2 + b^2 \equiv 0 \mod p.$$

   Show that

$$a \equiv b \equiv 0 \mod p.$$

11. Show that if $(a, 15) = 1$, then

$$a^{\phi(15)/2} \equiv 1 \mod 15,$$

   and conclude that 15 has no primitive roots. Hint: Consider the congruence modulo 3 and modulo 5.

12. Show that 21 has no primitive roots.

13. Show that 35 has no primitive roots.

14. Suppose that b and c are positive integers. Let $d = (b, c)$. Suppose that
$$a^b \equiv 1 \mod n \text{ and } a^c \equiv 1 \mod n.$$
Show that
$$a^d \equiv 1 \mod n.$$

15. If $a = b^2$ is a perfect square and p is an odd prime, explain why it is impossible for a to be a primitive root modulo p.

16. Suppose that $(a, m) = 1$, $(a, n) = 1$, and $(m, n) = 1$. Find a formula for $\mathrm{ord}_{mn}(a)$ in terms of $\mathrm{ord}_m(a)$ and $\mathrm{ord}_n(a)$.

17. Let $F_n = 2^{2^n} + 1$ and suppose that $p \mid F_n$, where p is a prime (possibly F_n itself). Show that
$$2^{2^n+1} \equiv 1 \mod p,$$
so that
$$\mathrm{ord}_p(2) \mid 2^{n+1}.$$
Use this to show that
$$\mathrm{ord}_p(2) = 2^{n+1}.$$
Since $\mathrm{ord}_p(2) \mid (p-1)$, show that there is an integer k such that $p = k \cdot 2^n + 1$. Recall that the order of a modulo p is the smallest positive integer b such that
$$a^b \equiv 1 \mod p,$$
and we write $b = \mathrm{ord}_p(a)$.

18. Show that if p is a prime and $\mathrm{ord}_p(a) = 3$, then
$$\left(\sum_{j=0}^{2} a^{j^2}\right)^2 \equiv -3 \mod p.$$

19. Show that if p is a prime and $\mathrm{ord}_p(a) = 4$, then
$$\left(\sum_{j=0}^{3} a^{j^2}\right)^2 \equiv 8a \mod p.$$

20. Show that if p is a prime and $\mathrm{ord}_p(a) = 6$, then
$$\sum_{j=0}^{5} a^{j^2} \equiv 0 \mod p.$$

Chapter 13

Squares Modulo p and Quadratic Residues

We have learned previously how to solve linear congruences of the form

$$ax \equiv c \mod p.$$

Next, we consider quadratic congruences modulo a prime p.

Example 13.1 Is 3 congruent to the square of some number modulo 7, i.e. can we find a number x such that

$$x^2 \equiv 3 \mod 7?$$

Solution:

$$\begin{aligned} 0^2 &\equiv 0 \mod 7 \\ 1^2 &\equiv 1 \mod 7 \\ 2^2 &\equiv 4 \mod 7 \\ 3^2 &\equiv 2 \mod 7 \\ 4^2 &\equiv 2 \mod 7 \\ 5^2 &\equiv 4 \mod 7 \\ 6^2 &\equiv 1 \mod 7 \end{aligned}$$

Thus, 3 is not congruent to a square modulo 7.

Example 13.2 Does the congruence

$$x^2 \equiv -1 \equiv 12 \mod 13$$

have a solution?

Solution: We compute $x^2 \mod 13$ for $x \equiv 0, 1, 2, \ldots, 12 \mod 13$ and find that the congruence has two solutions, $x \equiv 5 \mod 13$ and $x \equiv 8 \mod 13$.
To begin our study of squares modulo p, we compute the squares modulo p for $p = 3, 5, 7, 11$.

a	$a^2 \mod 3$
0	
1	
2	

a	$a^2 \mod 5$
0	
1	
2	
3	
4	

a	$a^2 \mod 7$
0	
1	
2	
3	
4	
5	
6	

a	$a^2 \mod 11$
0	
1	
2	
3	
4	
5	
6	
7	
8	
9	
10	

We make the following observations from this numerical data:

- Each number (other than 0) that appears as a square modulo p appears exactly twice.

- The square of the number b and the square of the number $p-b$ are the same.

Theorem 13.1 Suppose that p is a prime. Then

$$b^2 \equiv (p-b)^2 \mod p.$$

Proof.

$$(p-b)^2 = p^2 - 2pb + b^2 \equiv 0 - 0 + b^2 \equiv b^2 \mod p.$$

Thus, if we wish to find all of the numbers that are squares modulo p, we actually only need to compute half of them:

$$1^2 \mod p, 2^2 \mod p, \ldots, \left(\frac{p-1}{2}\right)^2 \mod p.$$

Our goal is to determine which numbers are squares modulo p, and which numbers are not squares modulo p. To begin, we need some terminology.

Definition 13.1 A nonzero number that is congruent to a square modulo p is called a **quadratic residue** modulo p.

Example 13.3 3 is a quadratic residue modulo 11 since

$$5^2 \equiv 3 \mod 11.$$

The set of quadratic residues modulo 11 is $\{1, 3, 4, 5, 9\}$. Notice that there are 5 quadratic residues modulo 11.

Definition 13.2 A nonzero number that is not congruent to a square modulo p is called a **quadratic nonresidue** modulo p.

Example 13.4 2 is a quadratic nonresidue modulo 11 since there is no integer x such that

$$x^2 \equiv 2 \mod 11.$$

The set of quadratic nonresidues modulo 11 is $\{2, 6, 7, 8, 10\}$. Notice that there are 5 quadratic nonresidues modulo 11.

Theorem 13.2 Let p be an odd prime. Then there are exactly $\left(\frac{p-1}{2}\right)$ quadratic residues modulo p and $\left(\frac{p-1}{2}\right)$ quadratic nonresidues modulo p.

Proof. The quadratic residues modulo p are precisely the squares modulo p. Thus, they are the numbers

$$1^2 \mod p, 2^2 \mod p, \ldots, (p-1)^2 \mod p.$$

However, since we have shown that

$$p^2 \equiv (p-b)^2 \mod p,$$

we only need to go halfway, i.e. the quadratic residues modulo p are the numbers

$$1^2 \mod p, 2^2 \mod p, \ldots, \left(\frac{p-1}{2}\right)^2 \mod p.$$

Note that the list above consists of $\left(\frac{p-1}{2}\right)$ numbers. Thus, to show that there are exactly $\left(\frac{p-1}{2}\right)$ quadratic residues modulo p, we just need to check that the numbers

$$1^2 \mod p, 2^2 \mod p, \ldots, \left(\frac{p-1}{2}\right)^2 \mod p$$

are all different modulo p. Suppose that b_1 and b_2 are two numbers between 1 and $\left(\frac{p-1}{2}\right)$ such that

$$b_1^2 \equiv b_2^2 \mod p.$$

Then

$$p \mid (b_1^2 - b_2^2) = (b_1+b_2)(b_1-b_2).$$

Now, $b_1 + b_2$ is between 2 and $p-1$, so it can't be divisible by p. Thus,

$$p \mid (b_1 - b_2).$$

However,

$$|b_1 - b_2| < \frac{p-1}{2},$$

so $b_1 - b_2 = 0$. Thus,

$$b_1 = b_2,$$

and we conclude that the numbers

$$1^2 \mod p, 2^2 \mod p, \ldots, \left(\frac{p-1}{2}\right)^2 \mod p$$

are all different modulo p, so there are exactly $\left(\frac{p-1}{2}\right)$ quadratic residues modulo p and $\left(\frac{p-1}{2}\right)$ quadratic nonresidues modulo p.

What happens when we multiply quadratic residues and nonresidues? Perform some experiments modulo 11 and make a conjecture. Recall that the quadratic residues modulo 11 are $\{1, 3, 4, 5, 9\}$ and the quadratic nonresidues are $\{2, 6, 7, 8, 10\}$.

- QR × QR = QR
- QNR × QNR = QR
- QR × QNR = QNR

To prove that the conjectures made above are correct, we must investigate the relationship between quadratic residues and primitive roots. Let g be a primitive root modulo p. By Theorem 12.3, we know that the powers of g,

$$g, g^2, g^3, \dots, g^{p-3}, g^{p-2}, g^{p-1},$$

give all the nonzero numbers modulo p. We know that half of the nonzero numbers modulo p are quadratic residues, and half are quadratic nonresidues. How do we know which are which?

We know that g^2 is a quadratic residue, since it is clearly a square. Similarly, $g^4 = (g^2)^2$ is also a quadratic residue. In general, any even power of g, say g^{2k} is a quadratic residue since $g^{2k} = (g^k)^2$. Since exactly $\left(\frac{p-1}{2}\right)$ of the exponents in the list

$$g, g^2, g^3, \dots, g^{p-3}, g^{p-2}, g^{p-1}$$

are even, and there are exactly $\left(\frac{p-1}{2}\right)$ quadratic residues modulo p, we conclude that the quadratic residues modulo p are precisely those numbers a that can be expressed as an even power of g, and the quadratic nonresidues modulo p are those numbers a that can be expressed as an odd power of g. Using this information, we can now prove the following.

Theorem 13.3 Quadratic Residue Multiplication Rule, Version 1. Let p be an odd prime. Suppose that a and b are any quadratic residues modulo p and that c and d are any quadratic nonresidues modulo p. Then:

- ab is a quadratic residue modulo p. The product of two quadratic residues modulo p is a quadratic residue modulo p.
- cd is a quadratic residue modulo p. The product of two quadratic nonresidues modulo p is a quadratic residue modulo p.
- ac is a quadratic nonresidue modulo p. The product of a quadratic residue modulo p and a quadratic nonresidue modulo p is a quadratic nonresidue modulo p.

Proof. Let g be a primitive root modulo p. Since a and b are quadratic residues modulo p, there exist integers j and k such that $1 \leq i, j \leq p-1$ and

$$a \equiv g^{2k} \mod p \text{ and } b \equiv g^{2j} \mod p.$$

Since c and d are quadratic nonresidues modulo p, there exist integers m and n such that $1 \leq m, n \leq p-1$ and

$$c \equiv g^{2m-1} \mod p \text{ and } d \equiv g^{2n-1} \mod p.$$

Then

$$ab \equiv g^{2(j+k)}$$

is an even power of g, so ab is a quadratic residue modulo p;

$$cd \equiv g^{2(m-n-1)}$$

is an even power of g, so cd is a quadratic residue modulo p; and

$$ac \equiv g^{2(k+m)-1} \mod p$$

is an odd power of g, so ac is a quadratic nonresidue modulo p.

We use the following notation for quadratic residues and nonresidues.

Definition 13.3 The **Legendre symbol** $\left(\dfrac{a}{p}\right)$ of a modulo p is defined by:

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue modulo } p \\ -1 & \text{if } a \text{ is a quadratic nonresidue modulo } p \end{cases}$$

Theorem 13.4 Quadratic Residue Multiplication Rule, Version 2. Let p be an odd prime. Then

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

Proof. This follows directly from Version 1 of the Quadratic Residue Mulitplication Rule.

Example 13.5 Is 75 a square modulo 97?

Solution: To determine whether or not 75 is a square modulo 97, we need to compute $\left(\dfrac{75}{97}\right)$. By the Quadratic Residue Multiplication Rule, we know that

$$\left(\frac{75}{97}\right) = \left(\frac{3\cdot 5\cdot 5}{97}\right) = \left(\frac{3}{97}\right)\left(\frac{5}{97}\right)\left(\frac{5}{97}\right).$$

Next, note that $\left(\frac{5}{97}\right) = \pm 1$, so

$$\left(\frac{5}{97}\right)\left(\frac{5}{97}\right) = 1.$$

Also,

$$10^2 \equiv 3 \mod 97,$$

so

$$\left(\frac{3}{97}\right) = 1.$$

Thus,

$$\left(\frac{75}{97}\right) = 1,$$

so 75 is a square modulo 97.

Note that the solution of the previous example was dependent on knowing that $\left(\frac{3}{97}\right) = 1$. It is thus important to be able to compute $\left(\frac{a}{p}\right)$ for arbitrary integers p. First, we need the following result.

Theorem 13.5 Suppose that p is an odd prime and that $a \not\equiv 0 \mod p$. Then

$$a^{(p-1)/2} \equiv \pm 1 \mod p.$$

Proof. Let $A = a^{(p-1)/2}$. By Fermat's Little Theorem,

$$A^2 = a^{p-1} \equiv 1 \mod p.$$

Thus,

$$p \mid (A^2 - 1) = (A-1)(A+1).$$

Thus,

$$p \mid (A-1)$$

or

$$p \mid (A+1).$$

If $p \mid (A-1)$, then

$$A \equiv 1 \mod p.$$

If $p \mid (A+1)$, then

$$A \equiv -1 \mod p.$$

Thus,

$$A = a^{(p-1)/2} \equiv \pm 1 \mod p.$$

We observe that the quantities

$$a^{(p-1)/2}$$

and

$$\left(\frac{a}{p}\right)$$

both take on the same values, namely ±1. We might consider whether these quantities are related to one another. You will explore this question in the problem set.

Problem Set

1. Make a list of all the quadratic residues and the quadratic nonresidues modulo the primes 7, 13, 17, and 19.

2. In this exercise, you will investigate the relationship between

$$a^{(p-1)/2} \mod p$$

and

$$\left(\frac{a}{p}\right).$$

Complete the following table. For example, in the second row, we have

$$2^{(5-1)/2} = 2^2 = 4 \equiv -1 \mod 5$$

AND

$$\left(\frac{2}{5}\right) = -1$$

since 2 is a quadratic nonresidue modulo 5 (the squares modulo 5 are 1 and 4).

p	a	$a^{(p-1)/2} \mod p$	$\left(\frac{a}{p}\right)$
5	1	1	1
5	2	-1	-1
5	3		
5	4		
7	1		
7	2		
7	3		
7	4		
7	5		
7	6		
11	1		
11	2		
11	3		
11	4		
11	5		
11	6		
11	7		
11	8		
11	9		
11	10		

Based on the numerical evidence in this table, make a conjecture about the relationship between $a^{(p-1)/2} \mod p$ and $\left(\frac{a}{p}\right)$.

3. In this exercise, you will consider primes p for which -1 is a quadratic residue. Recall that -1 is a quadratic residue modulo p if there is an integer x such that

$$x^2 \equiv -1 \equiv (p-1) \mod p.$$

(a) i. Is -1 a quadratic residue or nonresidue modulo 3?

Solution: -1 is a quadratic nonresidue modulo 3 since $1^2 \equiv 1 \not\equiv -1 \mod 3$ and $2^2 \equiv 1 \not\equiv -1 \mod 3$.

ii. Is -1 a quadratic residue or nonresidue modulo 5?

iii. Is -1 a quadratic residue or nonresidue modulo 7?

iv. Is -1 a quadratic residue or nonresidue modulo 11?

v. Is -1 a quadratic residue or nonresidue modulo 13?

vi. Is -1 a quadratic residue or nonresidue modulo 17?

vii. Is -1 a quadratic residue or nonresidue modulo 19?

(b) Note that any odd prime p is either congruent to 1 modulo 4 or congruent to 3 modulo 4. (If $p \equiv 0 \mod 4$, then $4 \mid p$, so p is not prime, and if $p \equiv 2 \mod 4$, then $(4-2) = 2 \mid p$, so p is not prime). For each prime p in part (a) such that -1 is a quadratic residue modulo p, compute p modulo 4. Do you observe any patterns?

(c) For each prime p in part (a) such that -1 is a quadratic nonresidue modulo p, compute p modulo 4. Do you observe any patterns?

(d) Make a conjecture describing which primes have -1 as a quadratic residue.

4. In this exercise, you will consider primes p for which 2 is a quadratic residue. Recall that 2 is a quadratic residue modulo p if there is an integer x such that

$$x^2 \equiv 2 \mod p.$$

(a) i. Is 2 a quadratic residue or nonresidue modulo 3?

ii. Is 2 a quadratic residue or nonresidue modulo 5?

iii. Is 2 a quadratic residue or nonresidue modulo 7?

iv. Is 2 a quadratic residue or nonresidue modulo 11?

v. Is 2 a quadratic residue or nonresidue modulo 13?

vi. Is 2 a quadratic residue or nonresidue modulo 17?

vii. Is 2 a quadratic residue or nonresidue modulo 19?

viii. Is 2 a quadratic residue or nonresidue modulo 23?

(b) Note that any odd prime p is either congruent to 1, 3, 5, or 7 modulo 8. (Otherwise, $2 \mid p$ so p is not prime). For each prime p in part (a) such that 2 is a quadratic residue modulo p, compute p modulo 8. Do you observe any patterns?

(c) For each prime p in part (a) such that 2 is a quadratic nonresidue modulo p, compute p modulo 8. Do you observe any patterns?

(d) Make a conjecture describing which primes have 2 as a quadratic residue.

5. Here are lists of the first few primes for which 3 is a quadratic residue and a quadratic nonresidue:

Quadratic residue:	11, 13, 23, 37, 47, 59, 61, 71, 73, 83, 97, 107, 109
Quadratic nonresidue:	5, 7, 17, 19, 29, 31, 41, 43, 53, 67, 79, 89, 101, 103, 113, 127

Try reducing these lists modulo m for various m's until you find a pattern, and make a conjecture describing which primes have 3 as a quadratic residue.

6. Suppose that p is a prime and that $(a, p) = 1$. Show that the equation

$$x^3 \equiv a \mod p$$

has solutions if

$$a^{(p-1)/2} \equiv 1 \mod p$$

and does not have solutions if

$$a^{(p-1)/2} \equiv -1 \mod p.$$

Chapter 14

Introduction to Quadratic Reciprocity

In this section, we'll consider which primes p have $a = -1$ as a quadratic residue and which primes p have $a = 2$ as a quadratic residue. That is, we wish to answer the following questions:

- For which primes p is there an integer x such that
$$x^2 \equiv -1 \mod p?$$
- For which primes p is there an integer x such that
$$x^2 \equiv 2 \mod p?$$

Theorem 14.1 Euler's Criterion. Let p be an odd prime. Then
$$a^{(p-1)/2} \equiv \left(\frac{a}{p}\right) \mod p.$$

Proof. We'll first consider the case when a is a quadratic residue modulo p and then when a is a nonresidue.

Suppose that a is a quadratic residue modulo p. Then $\left(\frac{a}{p}\right) = 1$. So we must show that $a^{(p-1)/2} \equiv 1 \mod p$ in this case. Let g be a primitive root modulo p. We know that a is an even power of g, i.e. a can be expressed in the form
$$a \equiv g^{2k} \mod p.$$
By Fermat's Little Theorem, we have:
$$a^{(p-1)/2} \equiv (g^{2k})^{(p-1)/2} \equiv (g^{p-1})^k \equiv 1^k \equiv 1 \mod p.$$
Thus, if a is a quadratic residue modulo p,
$$a^{(p-1)/2} \equiv \left(\frac{a}{p}\right) \mod p.$$

Next, suppose that a is a quadratic nonresidue modulo p. Then $\left(\frac{a}{p}\right) = -1$. So we must show that $a^{(p-1)/2} \equiv -1 \mod p$ in this case. Let g be a primitive root modulo p. We know that a is an odd power of g, i.e. a can be expressed in the form

$$a \equiv g^{2k+1} \mod p.$$

By Fermat's Little Theorem, we have:

$$a^{(p-1)/2} \equiv (g^{2k+1})^{(p-1)/2} \equiv (g^{p-1})^k g^{(p-1)/2} \equiv g^{(p-1)/2} \mod p.$$

Now,

$$g^{(p-1)} \equiv 1 \mod p,$$

so

$$g^{(p-1)/2} \equiv \pm 1 \mod p.$$

But g is a primitive root modulo p, so the smallest power of g that is congruent to 1 modulo p is the $(p-1)$-st power. Thus,

$$g^{(p-1)/2} \equiv -1 \mod p,$$

so we conclude that

$$a^{(p-1)/2} \equiv -1 \mod p$$

in this case. Thus, if a is a quadratic nonresidue modulo p,

$$a^{(p-1)/2} \equiv \left(\frac{a}{p}\right) \mod p.$$

Theorem 14.2 Quadratic Reciprocity, Part 1. Let p be an odd prime. Then

$$-1 \text{ is a quadratic residue modulo } p \text{ if } p \equiv 1 \mod 4,$$

and

$$-1 \text{ is a quadratic nonresidue modulo } p \text{ if } p \equiv 3 \mod 4.$$

Using the Legendre symbol,

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \mod 4, \\ -1 & \text{if } p \equiv 3 \mod 4. \end{cases}$$

Proof. Use Euler's Criterion:

$$(-1)^{(p-1)/2} \equiv \left(\frac{-1}{p}\right) \mod p.$$

First, suppose that $p \equiv 1 \mod 4$. Then $4 \mid (p-1)$, so there is an integer k such that

$$p = 4k + 1.$$

Then

$$(-1)^{(p-1)/2} = (-1)^{(4k+1-1)/2} = (-1)^{2k} = 1,$$

so

$$1 \equiv \left(\frac{-1}{p}\right) \mod p.$$

Thus, if $p \equiv 1 \mod 4$, -1 is a quadratic residue modulo 4.

Next, suppose that $p \equiv 3 \mod 4$. Then $4 \mid (p-3)$, so there is an integer k such that

$$p = 4k + 3.$$

Then

$$(-1)^{(p-1)/2} = (-1)^{(4k+3-1)/2} = (-1)^{2k+1} = -1,$$

so

$$-1 \equiv \left(\frac{-1}{p}\right) \mod p.$$

Thus, if $p \equiv 3 \mod 4$, -1 is a quadratic nonresidue modulo p.

Theorem 14.3 Quadratic Reciprocity, Part 2. Let p be an odd prime. Then

$$2 \text{ is a quadratic residue modulo } p \text{ if } p \equiv 1 \text{ or } 7 \mod 8,$$

and

$$2 \text{ is a quadratic nonresidue modulo } p \text{ if } p \equiv 3 \text{ or } 5 \mod 8.$$

Using the Legendre symbol,

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \text{ or } 7 \mod 8, \\ -1 & \text{if } p \equiv 3 \text{ or } 5 \mod 8. \end{cases}$$

Proof. Our first thought might be to use Euler's Criterion, as we did for the proof of Quadratic Reciprocity, Part 1. However, there is not an obvious way to compute $2^{(p-1)/2} \mod p$. Recall that when we proved Fermat's Little Theorem in Chapter 10, we first multiplied the numbers

$$1, 2, 3, \ldots, (p-1)$$

by a, and then multiplied them all together, which gave us a factor of a^{p-1} to pull out. To use Euler's Criterion, we want $\frac{1}{2}(p-1)$ factors of a to pull out, so instead of starting with all the numbers from 1 to p, we'll start with the numbers

$$1, 2, 3, \ldots, \frac{p-1}{2}$$

and multiply each by $a = 2$.

To illustrate the idea, we'll compute $\left(\frac{2}{13}\right)$. We begin with half the numbers from 1 to $13 - 1 = 12$:

$$1, 2, 3, 4, 5, 6.$$

Next, we multiply each by 2 and then multiply them together. We obtain:

$$(2 \cdot 1)(2 \cdot 2)(2 \cdot 3)(2 \cdot 4)(2 \cdot 5)(2 \cdot 6) = 2^6 \cdot 6!.$$

Notice the factor

$$2^6 = 2^{(13-1)/2},$$

which is what we are interested in computing. The main idea now is to reduce each of the numbers 2, 4, 6, 8, 10, 12 modulo 13 to obtain a number between 6 and -6. We have:

$$\begin{aligned} 2 &\equiv 2 \mod 13 \\ 4 &\equiv 4 \mod 13 \\ 6 &\equiv 6 \mod 13 \\ 8 &\equiv -5 \mod 13 \\ 10 &\equiv -3 \mod 13 \\ 12 &\equiv -1 \mod 13 \end{aligned}$$

Multiplying these numbers together, we have:

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

Thus

$$2^6 \cdot 6! \equiv -6! \mod 13,$$

which implies that

$$2^6 \equiv -1 \mod 13.$$

By Euler's Criterion, we conclude that 2 is a quadratic nonresidue modulo 13.

Next, let's think about the idea a little more generally. Let p be any odd prime. We wish to compute $2^{(p-1)/2}$. We start with the even numbers

$$1, 2, 3, \ldots, \frac{p-1}{2}$$

and multiply each by 2 to obtain the list

$$2 \cdot 1, 2 \cdot 2, 2 \cdot 3, \ldots, 2 \cdot \frac{p-1}{2}.$$

Next, we multiply the numbers together and factor out a 2 from each number to obtain

$$(2 \cdot 1) \cdot (2 \cdot 2)(2 \cdot 3) \cdots (2 \cdot \frac{p-1}{2}) = 2^{(p-1)/2} \left(\frac{p-1}{2}\right)!.$$

The next step is to reduce each number in the list

$$2, 4, 6, \ldots, p-1$$

modulo p so that it lies in the range $-\frac{p-1}{2}$ to $\frac{p-1}{2}$. The first few numbers won't change, but any number in the list larger than $(p-1)/2$ needs to have p subtracted from it (and thus becomes negative). The number of minus signs is exactly the number of integers in the list $2, 4, 6, \ldots, (p-1)$ that are larger than $(p-1)/2$. Thus, equating the two products, we have:

$$2^{(p-1)/2} \left(\frac{p-1}{2}\right)! = 2 \cdot 4 \cdot 6 \cdots (p-1) \equiv (-1)^{\text{number of minus signs}} \cdot \left(\frac{p-1}{2}\right)! \mod p.$$

We conclude that

$$2^{(p-1)/2} \equiv (-1)^{\text{number of minus signs}} \mod p.$$

Recall that the number of minus signs is exactly the number of integers in the list $2, 4, 6, \ldots, (p-1)$ that are larger than $(p-1)/2$.

Using this result, we can now prove the Theorem. Suppose that $p \equiv 3 \mod 8$. Then $8 \mid (p-3)$, so there is an integer k such that $p = 8k+3$. We need to list the numbers

$$2, 4, 6, \ldots, p-1$$

and determine how many of them are larger than $(p-1)/2$. In this case,

$$p - 1 = 8k + 2 \text{ and } \frac{p-1}{2} = \frac{8k+2}{2} = 4k + 1.$$

So the list is

$$2, 4, 6, \ldots, 4k \quad || \quad (4k+2), (4k+4), \ldots, 8k.$$

There are $2k+1$ even numbers between $4k+2$ and $8k+2$ (try it for a few values of k), so there are $2k+1$ numbers in the list larger than $(p-1)/2$. Thus, there are $2k+1$ minus signs, so

$$2^{(p-1)/2} \equiv (-1)^{2k+1} \equiv -1 \mod p.$$

We conclude that 2 is a quadratic nonresidue modulo p for any prime p that is congruent to 3 modulo 8.

The three remaining cases can be proved in a similar way, and are left to you as exercises.

Problem Set

1. Determine which of the following congruences has a solution. All of the moduli are primes.

   (a) $x^2 \equiv -1 \mod 5987$

   (b) $x^2 \equiv 6780 \mod 6781$

   (c) $x^2 \equiv 2 \mod 61$

   (d) $x^2 \equiv 2 \mod 59$

   (e) $x^2 + 14x - 35 \equiv 0 \mod 337$ (Hint: use the quadratic formula to figure out what number you need to take the square root of modulo 337.)

   (f) $x^2 - 64x + 943 \equiv 9 \mod 3011$

2. Suppose that p is an odd prime and that $a \equiv b \mod p$. Show that

$$\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right).$$

3. In this exercise, you will prove that there are infinitely many primes that are congruent to 1 modulo 4. Suppose that you are given a list

$$p_1, p_2, \ldots, p_r$$

   of primes that are congruent to 1 modulo 4. You can then find at least one new prime, not in the list, that is congruent to 1 modulo 4. Repeating this process indefinitely constructs a list of infinitely many primes that are congruent to 1 modulo 4.

   (a) Consider the number

$$A = (2p_1p_2 \cdots p_r)^2 + 1.$$

   Factor A into a product of primes, say

$$A = q_1q_2 \cdots q_s.$$

   (b) Show that

$$A \equiv 0 \mod q_i$$

   for each q_i.

   (c) Show that -1 is a quadratic residue modulo q_i for each q_i.

   (d) Conclude that each q_i is congruent to 1 modulo 4.

   (e) Explain why none of the q_i's could have been in the original list.

(f) Use the procedure described in this proof to produce a list of primes that are congruent to 1 modulo 4. Start with $p_1 = 5$. Then

$$A = (2p_1)^2 + 1 = 101,$$

so our second prime is

$$p_2 = 101 \equiv 1 \mod 4.$$

Repeat this procedure to find a few more primes that are congruent to 1 modulo 4 (you will probably want to use a calculator for the arithmetic).

4. Finish the proof of the Quadratic Reciprocity, Part 2 Theorem for the cases $p \equiv 7 \mod 8$, $p \equiv 1 \mod 8$, and $p \equiv 5 \mod 8$.

5. Suppose that q is a prime number that is congruent to 1 modulo 4, and suppose that the number $p = 2q+1$ is also a prime number. (For example, q could equal 5 and p would be 11). Show that 2 is a primitive root modulo p.

6. In this exercise, you will investigate the relationship between

$$\left(\frac{q}{p}\right) \text{ and } \left(\frac{p}{q}\right)$$

for various primes q and p. The following table gives the value of

$$\left(\frac{q}{p}\right)$$

for all odd primes $p, q \leq 37$.

q, p	$q = 3$	$q = 5$	$q = 7$	$q = 11$	$q = 13$	$q = 17$	$q = 19$	$q = 23$	$q = 29$
$p = 3$		-1	1	-1	1	-1	1	-1	-1
$p = 5$	-1		-1	1	-1	-1	1	-1	1
$p = 7$	-1	-1		1	-1	-1	-1	1	1
$p = 11$	1	1	-1		-1	-1	-1	1	-1
$p = 13$	1	-1	-1	-1		1	-1	1	1
$p = 17$	-1	-1	-1	-1	1		1	-1	-1
$p = 19$	-1	1	1	1	-1	1		1	-1
$p = 23$	1	-1	-1	-1	1	-1	-1		1
$p = 29$	-1	1	1	-1	1	-1	-1	1	

(a) Using the row with $p = 5$ and the column with $q = 5$, make a conjecture about the relationship between $\left(\frac{5}{p}\right)$ and $\left(\frac{p}{5}\right)$.

(b) What is the relationship between $\left(\frac{7}{3}\right)$ and $\left(\frac{3}{7}\right)$?

(c) In (a) and (b), you should have observed that sometimes $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)$ and sometimes $\left(\frac{q}{p}\right) = -\left(\frac{p}{q}\right)$. Make a list of the primes p whose rows and columns are exactly the same. For these primes, $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)$. Next, make a list of the primes p whose rows and columns are not exactly the same. For these primes, $\left(\frac{q}{p}\right) = -\left(\frac{p}{q}\right)$. Do you observe any patterns about your lists? Hint: consider the primes in your list modulo 4.

Chapter 15

The Law of Quadratic Reciprocity

The Law of Quadratic Reciprocity was first formulated by Euler and Lagrange, but Gauss gave the first proof in 1801. Gauss discovered the law for himself when he was 19, and during his lifetime he found seven different proofs. The Law of Quadratic Reciprocity is a beautiful and subtle theoretical result that also has important practical consequences.

Theorem 15.1 Law of Quadratic Reciprocity. Let p and q be distinct odd primes.

$$\begin{aligned}
\left(\frac{-1}{p}\right) &= \begin{cases} 1 & \text{if } p \equiv 1 \mod 4 \\ -1 & \text{if } p \equiv 3 \mod 4 \end{cases} \\
\left(\frac{2}{p}\right) &= \begin{cases} 1 & \text{if } p \equiv 1 \text{ or } 7 \mod 8 \\ -1 & \text{if } p \equiv 3 \text{ or } 5 \mod 8. \end{cases} \\
\left(\frac{q}{p}\right) &= \begin{cases} \left(\frac{p}{q}\right) & \text{if } p \equiv 1 \mod 4 \text{ or } q \equiv 1 \mod 4 \\ -\left(\frac{p}{q}\right) & \text{if } p \equiv 3 \mod 4 \text{ and } q \equiv 3 \mod 4 \end{cases}
\end{aligned}$$

We have already proved the result for $\left(\frac{-1}{p}\right)$ and $\left(\frac{2}{p}\right)$, and will not give the general proof for $\left(\frac{q}{p}\right)$ here.

Using the Law of Quadratic Reciprocity and the Quadratic Residue Multiplication Rule, we can compute $\left(\frac{a}{p}\right)$ for any number a and any prime p. The Law of Quadratic Reciprocity allows us to flip the Legendre symbol $\left(\frac{q}{p}\right)$ and replace it with $\pm\left(\frac{p}{q}\right)$. Then we can reduce p modulo q and repeat the process, at each stage obtaining a Legendre symbol with smaller and smaller entries, so that eventually we arrive at a Legendre symbol that we can compute.

Example 15.1 Determine whether the congruence

$$x^2 \equiv 5 \mod 3593$$

has a solution (3593 is prime).

Solution. We need to determine whether 5 is a quadratic residue modulo 3593, so we need to compute $\left(\frac{5}{3593}\right)$:

$$\begin{aligned}
\left(\frac{5}{3593}\right) &= \left(\frac{3593}{5}\right) \text{ since } 5 \equiv 1 \mod 4 \\
&= \left(\frac{3}{5}\right) \text{ since } 3593 \equiv 3 \mod 5 \\
&= -1 \text{ since 3 is a quadratic nonresidue modulo 5.}
\end{aligned}$$

Thus, 5 is a quadratic nonresidue modulo 3593, so the congruence does not have a solution.

Example 15.2 Determine whether the congruence

$$x^2 \equiv 14 \mod 137$$

has a solution (137 is prime).

Solution. We need to determine whether 14 is a quadratic residue modulo 137, so we need to compute $\left(\frac{14}{137}\right)$:

$$\begin{aligned}
\left(\frac{14}{137}\right) &= \left(\frac{2}{137}\right)\left(\frac{7}{137}\right) \text{ by the Quadratic Residue Multiplication Rule} \\
&= \left(\frac{7}{137}\right) \text{ since } 137 \equiv 1 \mod 8 \\
&= \left(\frac{137}{7}\right) \text{ since } 137 \equiv 1 \mod 4 \\
&= \left(\frac{4}{7}\right) \text{ since } 137 \equiv 4 \mod 7 \\
&= 1 \text{ since } 4 = 2^2 \text{ is a square modulo 7.}
\end{aligned}$$

Thus, 14 is a quadratic residue modulo 137, so the congruence does have a solution.

Example 15.3 Determine whether the congruence

$$x^2 \equiv 55 \mod 179$$

has a solution (179 is prime).

Solution: We need to determine whether 55 is a quadratic residue modulo 179, so we need to compute $\left(\dfrac{55}{179}\right)$:

$$\begin{aligned}
\left(\frac{55}{179}\right) &= \left(\frac{5}{179}\right)\left(\frac{11}{179}\right) \text{ by the Quadratic Residue Multiplication Rule} \\
&= \left(\frac{179}{5}\right)\cdot(-1)\cdot\left(\frac{179}{11}\right) \text{ since } 5 \equiv 1 \mod 4 \text{ and } 11 \equiv 179 \equiv 3 \mod 4 \\
&= \left(\frac{4}{5}\right)\cdot(-1)\left(\frac{3}{11}\right) \\
&= 1\cdot(-1)\cdot\left(\frac{3}{11}\right) \\
&= 1\cdot(-1)\cdot(-1)\cdot\left(\frac{11}{3}\right) \text{ since } 3 \equiv 11 \equiv 3 \mod 4 \\
&= 1\cdot(-1)\cdot(-1)\cdot\left(\frac{2}{3}\right) \\
&= 1\cdot(-1)\cdot(-1)\cdot(-1) \\
&= -1.
\end{aligned}$$

Thus, 55 is a quadratic nonresidue modulo 179, so the congruence does not have a solution.

Example 15.4 Find all odd primes p such that 3 is a quadratic residue modulo p.

Solution: We need to find all primes p such that $\left(\dfrac{3}{p}\right) = 1$. Since $3 \equiv 3 \mod 4$, we know that

$$\left(\frac{3}{p}\right) = \begin{cases} \left(\frac{p}{3}\right) & \text{if } p \equiv 1 \mod 4 \\ -\left(\frac{p}{3}\right) & \text{if } p \equiv 3 \mod 4. \end{cases}$$

Also,

$$\left(\frac{p}{3}\right) = \begin{cases} \left(\frac{1}{3}\right) = 1 & \text{if } p \equiv 1 \mod 3 \\ \left(\frac{2}{3}\right) = -1 & \text{if } p \equiv 2 \mod 3. \end{cases}$$

Thus, $\left(\frac{3}{p}\right) = 1$ if $p \equiv 1 \mod 3$ and $p \equiv 1 \mod 4$ or if $p \equiv 2 \mod 3$ and $p \equiv 3 \mod 4$.

Problem Set

1. Use the Law of Quadratic Reciprocity to compute each of the following Legendre symbols.

   (a) $\left(\dfrac{42}{61}\right)$

   (b) $\left(\dfrac{85}{101}\right)$

   (c) $\left(\dfrac{29}{541}\right)$

   (d) $\left(\dfrac{101}{1987}\right)$

   (e) $\left(\dfrac{31706}{43789}\right)$

2. Determine which of the following congruences are solvable. All of the moduli are prime.

   (a) $x^2 \equiv 10 \mod 89$

   (b) $x^2 \equiv 5 \mod 227$

   (c) $x^2 \equiv 5 \mod 229$

   (d) $x^2 \equiv 7 \mod 1009$

   (e) $x^2 \equiv 150 \mod 1009$

3. Find all primes q such that $\left(\dfrac{5}{q}\right) = -1$.

4. Find all primes p such that $x^2 \equiv 13 \mod p$ has a solution.

5. Prove that if a prime p is a quadratic residue of an odd prime q, and if p is of the form $4k+1$, then q is a quadratic residue of p.

6. Does the congruence

   $$x^2 - 3x - 1 \equiv 0 \mod 31957$$

   have any solutions? Hint: use the quadratic formula to find out what number you need to take the square root of modulo the prime 31957.

7. Let p be a prime number not equal to 2 or 5, and let A be any number. Suppose that p divides $A^2 - 5$. Show that p must be congruent to either 1 or 4 modulo 5.

8. Let p be a prime satisfying $p \equiv 3 \mod 4$. Suppose that a is a quadratic residue modulo p.

(a) Show that

$$x = a^{(p+1)/4}$$

is a solution to the congruence

$$x^2 \equiv a \mod p.$$

This gives an explicit way to find square roots modulo p for primes congruent to 3 modulo 4.

(b) Find a solution to the congruence

$$x^2 \equiv 7 \mod 787.$$

9. Let p be a prime satisfying $p \equiv 5 \mod 8$. Suppose that a is a quadratic residue modulo p.

(a) Show that one of the values

$$x = a^{(p+3)/8} \text{ or } x = 2a \cdot (4a)^{(p-5)/8}$$

is a solution to the congruence

$$x^2 \equiv a \mod p.$$

This gives an explicit way to find square roots modulo p for primes congruent to 5 modulo 8.

(b) Find a solution to the congruence

$$x^2 \equiv 5 \mod 541.$$

(c) Find a solution to the congruence

$$x^2 \equiv 13 \mod 653.$$

Chapter 16

Diophantine Equations

A **Diophantine equation** is a polynomial equation for which we seek integer solutions (or perhaps rational solutions). There is no universal method for determining whether a given Diophantine equation has a solution, or for finding all solutions if solutions do exist.

Example 16.1 Find all positive integer solutions of the equation $x^4 + 9 = y^2$.

Solution: We rewrite the equation in the form

$$\begin{aligned} y^2 - x^4 &= 9 \\ (y - x^2)(y + x^2) &= 9 \end{aligned}$$

Since we are interested in $y > 0, x > 0$, the factor $y + x^2$ is positive; thus, the other factor $y - x^2$ must also be positive. There are only two ways of factoring 9 as a product of positive integers: $9 = 1 \cdot 9$ and $9 = 3 \cdot 3$. Thus there are only three possibilities:

(a) $y + x^2 = 1$ and $y - x^2 = 9$

(b) $y + x^2 = 3$ and $y - x^2 = 3$

(c) $y + x^2 = 9$ and $y - x^2 = 1$

In each case, there are two equations and two unknowns. In case (a), we find $x = \pm\sqrt{-4}$, which is not an integer. In case (b), we find $x = 0$, which is not a positive integer. In case (c), we find $y = 5$, $x = \pm 2$. Thus, the only solution in positive integers is $x = 2$ and $y = 5$.

Theorem 16.1 Fermat's last theorem states that if $n \geq 3$, then there are no solutions to the equation

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

in nonzero integers. In 1637, Fermat wrote in the margin of his copy of *Arithmetica* of Diophantus that he had a "truly marvellous proof of this proposition which this margin is too narrow to contain." No correct proof of Fermat's Last Theorem was found for 357 years, until one was finally published by Andrew Wiles in 1995. Note that when $n = 2$, the equation $x^2 + y^2 = z^2$ has infinitely many solutions (which you will explore as an exercise).

Fermat also stated that the equation

$$x^2 + 2 = y^3$$

has only $x = 5, y = 3$ as a solution in positive integers and that the equation

$$x^2 + 4 = y^3$$

has only $x = 11, y = 5$ as a solution in positive integers. These statements have since been proven to be true using the ideas of quadratic field theory (developed 200 years after Fermat's announcement). It would be very interesting to know Fermat's proofs of these statements.

Congruences often provide an easy way of showing that certain Diophantine equations have no solutions.

Example 16.2 Find all integer solutions of the equation

$$x^2 - 7y^2 = -1.$$

Solution: Consider the equation modulo 7. If $x^2 - 7y^2 = -1$, then

$$\begin{aligned} x^2 - 7y^2 &\equiv -1 \mod 7 \\ x^2 &\equiv -1 \mod 7. \end{aligned}$$

However, $7 \equiv 3 \mod 4$, so -1 is a quadratic nonresidue modulo 7. Thus, there is no integer x such that $x^2 \equiv -1 \mod 7$. The squares modulo 7 are $1^2 \equiv 1 \mod 7, 2^2 \equiv 4 \mod 7, 3^2 \equiv 2 \mod 7, 4^2 \equiv 2 \mod 7, 5^2 \equiv 4 \mod 7, 6^2 \equiv 1 \mod 7$. We conclude that the equation has no integer solutions.

The main idea in using congruences to show that a Diophantine equation has no solutions is that if a Diophantine equation has no solutions modulo n, then it certainly has no solutions.

Theorem 16.2 Suppose that d is divisible by a prime $p \equiv 3 \mod 4$ or that d is divisible by 4. Then the equation

$$x^2 - dy^2 = -1$$

has no solutions.

Proof. Suppose that (x, y) is a solution to the equation. First, suppose that $p \equiv 3 \mod 4$ and $p \mid d$. Then $d \equiv 0 \mod p$. Then:

$$x^2 - dy^2 \equiv x^2 \equiv -1 \mod p.$$

But since $p \equiv 3 \mod 4$, -1 is a quadratic nonresidue modulo p, so no such integer x exists.

Next, suppose that $4 \mid d$. Then

$$x^2 - dy^2 \equiv x^2 \equiv -1 \mod 4.$$

But the squares modulo 4 are $1^2 \equiv 1 \mod 4, 2^2 \equiv 0 \mod 4, 3^2 \equiv 1 \mod 4$, so there is no integer x such that $x^2 \equiv -1 \equiv 3 \mod 4$. Thus the equation has no integer solutions.

Example 16.3 Find all integer solutions of the equation

$$x^2 - 5y^2 = 2.$$

Solution: Consider the equation modulo 5.

$$\begin{aligned} x^2 - 5y^2 &\equiv 2 \mod 5 \\ x^2 &\equiv 2 \mod 5 \end{aligned}$$

However, 2 is a quadratic nonresidue modulo 5, so no such integers x exists. The squares modulo 5 are $1^2 \equiv 1 \mod 5, 2^2 \equiv 4 \mod 5, 3^2 \equiv 4 \mod 5, 4^2 \equiv 1 \mod 5$. We conclude that the equation has no integer solutions.

Example 16.4 Are there integers x and y such that $x^2 - 5y^2 = 2$?

Hint: Consider the equation modulo 5.

Problem Set

1. Find all solutions in positive integers to the equation
$$x^2 + 12 = y^4.$$

2. Find all solutions in positive integers to the equation
$$x^3 + y^3 = 20.$$

3. Find all solutions in positive integers to the equation
$$x^3 - y^3 = 19.$$

4. Suppose that d is a perfect square. Find all integer solutions to the equation
$$x^2 - dy^2 = 1.$$

5. Show that 2 is the only prime which is the sum of 2 positive cubes. The word positive is necessary and hence must play a role in your proof; consider the examples $7 = 2^3 + (-1)^3, 61 = 5^3 + (-4)^3$.

6. In this exercise, you will investigate Pythagorean triples, i.e. positive integers (x, y, z) that satisfy the equation
$$x^2 + y^2 = z^2.$$

   (a) Suppose that (a, b, c) is a Pythagorean triple, and let d be a positive integer. Show that (da, db, dc) is also a Pythagorean triple. Thus, there are infinitely many Pythagorean triples.

   (b) A *primitive Pythagorean triple* is a triple of numbers (a, b, c) such that a, b, c have no common factors and satisfy $a^2 + b^2 = c^2$. Give 5 examples of primitive Pythagorean triples.

   (c) Suppose that (a, b, c) is a primitive Pythagorean triple. Show that c is odd.

   (d) Suppose that (a, b, c) is a primitive Pythagorean triple. Show that one of a and b is odd and the other is even.

   (e) Suppose that (a, b, c) is a primitive Pythagorean triple. Show that either a or b must be a multiple of c.

   (f) Suppose that (a, b, c) is a primitive Pythagorean triple. Show that one of a, b, c is divisible by 5.

7. In this exercise, you will find all primitive Pythagorean triples by following the steps outlined below. Suppose that (a, b, c) is a primitive Pythagorean triple. We can always switch a and b and still have a primitive Pythagorean triple, so let's suppose that a is odd and b is even.

(a) Show that $a^2 = (c - b)(c + b)$.

(b) Show that $\gcd(c - b, c + b) = 1$.

(c) Show that $c - b$ and $c + b$ are both squares. Then we can write

$$c + b = s^2 \text{ and } c - b = t^2,$$

where $s > t \geq 1$ are odd integers with no common factors.

(d) Solve these equations for b and c.

(e) Solve for a.

(f) Conclude that every primitive Pythagorean triple (a, b, c) with a odd and b even is given by the formulas

$$a = st, \ b = \frac{s^2 - t^2}{2}, \ c = \frac{s^2 + t^2}{2},$$

where $s > t \geq 1$ are chosen to be any odd integers with no common factors.

(g) Give all possible primitive Pythagorean triples with $s \leq 7$.

8. Suppose that p is an odd prime that can be written as the sum of two squares,

$$p = a^2 + b^2,$$

where a and b are positive integers. Show that $p \equiv 1 \mod 4$.

9. Show that the equation $x^2 + 7y^2 = 3$ has no integer solutions.

10. Show that the equation $x^2 - 3y^2 = 2$ has no integer solutions.

11. Show that the equation $x^2 - 11y^2 = 3$ has no integer solutions.

12. Show that the equation $11x^2 + 10x - y^2 + 2 = 0$ has no integer solutions.

13. Find all integer solutions of the equation $x^2 - 7y^2 = 3z^2$.

14. Show that the equation $x^2 + y^2 = 9z + 3$ has no integer solutions.

15. Show that the equation $x^2 + 2y^2 = 8z + 5$ has no integer solutions.

16. Show that the equation $(x^2 + y^2)^2 - 2(3x^2 - 5y^2)^2 = z^2$ has no integer solutions.

17. Show that the equation $x^2 = y^3 + 23$ has no integer solutions.

Chapter 17

Fibonacci Numbers and Linear Recurrences

Definition 17.1 The **Fibonacci numbers** F_n are defined as follows:

$$F_0 = 0, \quad F_1 = 1, \quad F_2 = 1, \quad F_n = F_{n-1} + F_{n-2} \text{ for } n \geq 3.$$

Notice that we don't have an explicit formula for F_n because we can't compute F_n directly. We have a rule that tells us how to compute F_n from the previous numbers. This is an example of a *recursion* or *recursive equation*.

Create a table of values of the first 20 Fibonacci numbers.

n	F_n	n	F_n
1	1	11	
2	1	12	
3	2	13	
4		14	
5		15	
6		16	
7		17	
8		18	
9		19	
10		20	

Notice that the Fibonacci numbers grow very rapidly. In fact, the 31st Fibonacci number is larger than 1 million,

$$F_{31} = 1,346,269$$

and the 45th Fibonacci number is larger than 1 billion,

$$F_{45} = 1,134,903,170.$$

We're interested in discovering number theoretic patterns that exist within the Fibonacci numbers, so one question that we should consider is how fast the Fibonacci numbers are growing. We can measure this by the ratio

$$\frac{F_n}{F_{n-1}}.$$

Create a table of values of F_n/F_{n-1} for $n \leq 20$.

n	F_n/F_{n-1}	n	F_n/F_{n-1}
2	1.00000	12	
3	2.00000	13	
4		14	
5		15	
6		16	
7		17	
8		18	
9		19	
10		20	
11			

Observe that the ratio F_n/F_{n-1} appears to be getting closer and closer to some number around 1.61803. Let's try to figure out exactly what this number is. The table suggests that F_n is approximately equal to αF_{n-1} for some number α:

$$\begin{aligned} F_n &\approx \alpha F_{n-1} \\ F_{n-1} &\approx \alpha F_{n-2} \\ F_n &\approx \alpha^2 F_{n-2} \end{aligned}$$

Using the recursive equation $F_n = F_{n-1} + F_{n-2}$, we have

$$\alpha^2 F_{n-2} \approx \alpha F_{n-2} + F_{n-2}.$$

Dividing by F_{n-2}, we obtain the equation

$$\alpha^2 - \alpha - 1 = 0,$$

which we solve to obtain

$$\alpha = \frac{1 \pm \sqrt{5}}{2}.$$

Note that

$$\frac{1+\sqrt{5}}{2} \approx 1.61803399.$$

We know that both values of α satisfy

$$\alpha^2 = \alpha + 1,$$

so for any number n, they both satisfy

$$\alpha^n = \alpha^{n-1} + \alpha^{n-2},$$

which looks a lot like the Fibonacci recursive equation $F_n = F_{n-1} + F_{n-2}$. We can formalize this observation as follows.

Let

$$\alpha_1 = \frac{1+\sqrt{5}}{2} \text{ and } \alpha_2 = \frac{1-\sqrt{5}}{2}.$$

Next, let

$$H_n = c_1\alpha_1^n + c_2\alpha_2^n,$$

where c_1 and c_2 are constants. Then

$$H_n = H_{n-1} + H_{n-2},$$

so H_n satisfies the same recursive formula as the Fibonacci sequence, and c_1 and c_2 can be any integers.

The idea now is to choose c_1 and c_2 so that H_n and the Fibonacci sequence F_n start with the same two values, i.e.

$$H_1 = F_1 = 1 \text{ and } H_2 = F_2 = 1.$$

Thus, we solve

$$c_1\alpha_1 + c_2\alpha_2 = 1 \text{ and } c_1\alpha_1^2 + c_2\alpha_2^2 = 1$$

to obtain

$$c_1 = \frac{1}{\sqrt{5}} \text{ and } c_2 = \frac{-1}{\sqrt{5}}.$$

We summarize our findings as follows. The formula for the n-th term of the Fibonacci sequence is named after Binet, who published it in 1843 (although it was known to Euler and Daniel Bernoulli at least 100 years earlier).

Theorem 17.1 Binet's Formula. Then Fibonacci sequence F_n is described by the recursion

$$F_1 = F_2 = 1 \text{ and } F_n = F_{n-1} + F_{n-2} \text{ for } n \geq 3.$$

Then the n-th term of the Fibonacci sequence is given by the formula

$$F_n = \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right].$$

Check the formula for the first few values of n to make sure that you believe the result.

Proof. For each positive integer $n \geq 1$, let

$$H_n = \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right].$$

We will prove that $H_n = F_n$ for all integers $n \geq 1$ by induction.

(i) Base case. First we check that $H_1 = F_1$ and $H_2 = F_2$.

$$\begin{aligned} H_1 &= \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^1 - \left(\frac{1-\sqrt{5}}{2}\right)^1\right] = \frac{1}{\sqrt{5}} \cdot \sqrt{5} = 1 = F_1 \\ H_2 &= \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^2 - \left(\frac{1-\sqrt{5}}{2}\right)^2\right] = \frac{1}{\sqrt{5}}\frac{4\sqrt{5}}{4} = 1 = F_2 \end{aligned}$$

(ii) Inductive hypothesis. Suppose that $H_k = F_k$ for all $k \leq n$. Then

$$\begin{aligned} H_{n+1} &= H_n + H_{n-1} \\ &= F_n + F_{n-1} \\ &= F_{n+1}. \end{aligned}$$

Thus, $H_n = F_n$ for every integer $n \geq 1$.

Definition 17.2 The number

$$\phi = \frac{1+\sqrt{5}}{2}$$

is known as the **golden ratio**. Binet's Formula states the following:

$$F_n = \frac{\phi^n - (1-\phi)^n}{\sqrt{5}}.$$

The golden ratio has fascinated Western intellectuals for at least 2400 years, and it has appeared in extremely diverse (and sometimes surprising areas):

- Architecture (Acropolis, Parthenon, Giza Pyramids, Great Mosque of Kairouan, Naqsh-e Jahan Square)
- Painting (Mona Lisa, De Divina Proportione, Dali's The Sacrament of the Last Supper)

- Book design
- Music
- Nature (Fibonacci spiral in plants, leaf arrangements, phyllotaxis, sunflower spirals, pinecone spirals)
- Human body

Theorem 17.2 Zeckendorf's Theorem. Every positive integer can be expressed in a unique way as the sum of one or more distinct Fibonacci numbers in such a way that the sum does not contain any 2 consecutive Fibonacci numbers.

Example 17.1 $100 = F_{11} + F_6 + F_4 = 89 + 8 + 3$ is the Zeckendorf representation of the integer 100. Observe that we can also express 100 as $100 = 89 + 8 + 2 + 1 = 55 + 34 + 8 + 3$, but these contain consecutive Fibonacci numbers.

For any given positive integer, we can find a representation that satisfies the conditions of Zeckendorf's Theorem by using a "greedy algorithm"–at each stage, choose the largest possible Fibonacci number.

Example 17.2 Find the Zeckendorf representation of each of the following:

1. 25
2. 34
3. 700

Problem Set

1. The golden ratio $\phi = \dfrac{1+\sqrt{5}}{2}$ satisfies some amazing identities. Prove (or investigate) the following:
   (a) $\dfrac{1}{\phi} = \phi - 1$
   (b) $\phi = \sqrt{1+\sqrt{1+\sqrt{1+\sqrt{1+\cdots}}}}$
   (c) $\phi = 5^{0.5} \cdot 0.5 + 0.5$
   (d) $\phi = 1 + \frac{1}{1+\frac{1}{\phi}}$
   (e) $\phi = 1 + \frac{1}{1+\frac{1}{1+\frac{1}{\phi}}}$
   (f) Can you continue the previous 2 identities?
   (g) $\phi^{\phi^{2+\phi}} = \phi^{\phi^{1+\phi^2}}$
   (h) $\phi = \frac{13}{8} + \sum\limits_{n=0}^{\infty} \frac{(-1)^{n+1}(2n+1)!}{(n+2)!n!4^{2n+3}}$
   (i) $\phi = 1 + 2\sin(\pi/10)$

2. Find the continued fraction expansion of the golden ratio $\phi = \frac{1+\sqrt{5}}{2}$. Then find the first 10 convergents in the continued fraction expansion of ϕ. What do you observe? See 25 for more information on continued fractions.

3. Find the Zeckendorf representation of each of the following:
   (a) 10
   (b) 500
   (c) 800

4. Compute the Zeckendorf representations for F_n^2 for $n = 1, 2, \ldots$. Try to figure out the pattern and prove that it holds in general.

5. (a) Show that F_{mn}/F_m is always an integer.
   (b) Compute the Zeckendorf representation of F_{mn}/F_n for different values of m and n. Can you find any patterns?

6. Make a list of the Fibonacci numbers that are prime. Make a conjecture of the form "If F_n is prime, then n is ...".

7. Find as many square Fibonacci numbers as you can. Do you think that there are finitely many or infinitely many square Fibonacci numbers?

8. Find all positive integer solutions of the Diophantine equation $89x + 55y = 1$. What do you observe?

9. The number
$$\phi = \frac{1+\sqrt{5}}{2} = 1.61803\ldots$$
is known as the *golden ratio.* We have observed that the ratio F_n/F_{n-1} gets closer and closer to the Golden Ratio as n increases. The golden ratio appears in many other places such as art, architecture, history, nature, and other branches of mathematics. Do some research online about the golden ratio, and write a short paper (with illustrations!) about places in which it appears.

10. The *Lucas sequence* is the sequence of numbers L_n given by the rules $L_1 = 1, L_2 = 3$, and $L_n = L_{n-1} + L_{n-2}$.

    (a) Write down the first 10 terms of the Lucas sequence.

    (b) Find a simple formula for L_n, similar to Binet's Formula for the Fibonacci number F_n.

    (c) Compare the value of $L_n^2 - 5F_n^2$ for each $1 \le n \le 10$. Make a conjecture about this value, and prove that your conjecture is correct.

    (d) Show that L_{3n} and F_{3n} are even for all n. Combining this fact with the formula that you discovered in (c), find an interesting equation satisfied by the pair of numbers
    $$\frac{1}{2}L_{3n}, \frac{1}{2}F_{3n}.$$

    (e) Compute the Zeckendorf representations for L_n and L_n^2 for $n = 1, 2, \ldots$. Do you observe any patterns?

11. Let P_n be the sequence defined by $P_1 = 1, P_2 = 9, P_3 = 1$, and $P_n = P_{n-1} + 4P_{n-2} - 4P_{n-3}$ for $n \ge 4$.

    (a) Write down the first 10 terms of P_n.

    (b) Does the sequence exhibit any strange behavior?

    (c) Find a formula for P_n, similar to Binet's Formula for the Fibonacci number F_n. Does the formula explain the behavior that you observed in (b)?

12. Consider the Fibonacci sequence reduced modulo m for various moduli m. For example,
$$\begin{aligned}
F_n \mod 2 &= 1,1,0,1,1,0,1,1,0,\ldots \\
F_n \mod 3 &= 1,1,2,0,2,2,1,0,1,1,2,0,2,2,1,0,\ldots \\
F_n \mod 4 &= 1,1,2,3,1,0,1,1,2,3,1,0,1,1,2,\ldots \\
F_n \mod 5 &= 1,1,2,3,0,3,3,1,4,0,4,4,3,2,0,2,2,4,1,0,1,1,2,\ldots
\end{aligned}$$

Observe that in each case, the Fibonacci sequence eventually starts to repeat. Thus there is an integer $N \geq 1$ such that

$$F_{n+N} \equiv F_n \mod m \text{ for all } n = 1, 2, \ldots.$$

The smallest such integer N is called the *period of the Fibonacci sequence* and is denoted by $N(m)$. Using the examples above, we have:

m	2	3	4	5
$N(m)$	3	8	6	20

(a) What is the value of $F_{N(m)}$ modulo m? What is the value of $F_{N(m)-1}$ modulo m?

(b) Write out the Fibonacci sequence modulo m in reverse direction:

$$F_{N(m)-1}, F_{N(m)-2}, \ldots, F_3, F_2, F_1 \mod m.$$

Do this for several values of m, and try to find a pattern.

(c) Prove that if $m \geq 3$, then the period $N(m)$ is even.

(d) Prove that if p is a prime such that $p \equiv 1 \mod 10$, then $N(p)$ divides $p-1$. Hint: one way to solve this problem is to use Binet's formula, but first you'll need to find a number modulo p to play the role of $\sqrt{5}$. You will also need to use Fermat's Little Theorem.

13. The Fibonacci numbers satisfy many amazing identities.

(a) Compute the quantity $F_{n+1}^2 - F_{n-1}^2$ for the first few integers $n = 2, 3, \ldots$. Make a conjecture for the value of $F_{n+1}^2 - F_{n-1}^2$, and prove that your conjecture is correct. Hint: it is equal to a Fibonacci number.

(b) Same question (and same hint) for the quantity $F_{n+1}^3 + F_n^3 - F_{n-1}^3$.

(c) Same question (but not the same hint) for the quantity $F_{n-1}F_{n+1} - F_n^2$.

(d) Same question for the quantity $4F_nF_{n-1} + F_{n-2}^2$. Hint: compare the value with the square of a Fibonacci number.

(e) Same question for the quantity $F_{n+4}^4 - 4F_{n+3}^4 - 19F_{n+2}^4 - 4F_{n+1}^4 + F_n^4$.

Fibonacci Nim

The game of **Fibonacci Nim** is played with two people and a pile containing n pennies (or sticks, or matches, or marbles, etc.). Person A removes j pennies from the pile, where $1 \leq j < n$. Player B then removes k pennies from the pile, where $1 \leq k \leq 2j$. The game continues in this way. Each player (after the first move) may take away as many pennies as he or she wishes with the restrictions that he or she must take at least one penny but no more than two times the number of pennies the previous player took. The player who takes the last penny wins the game.

Problems.

1. Find a winning strategy for Player 1 if $n = 4$.
2. Find a winning strategy for Player 1 if $n = 6$.
3. Find a winning strategy for Player 1 if $n = 7$.
4. Find a winning strategy for Player 1 if $n = 9$.
5. Find a winning strategy for Player 1 if $n = 10$.
6. Find a winning strategy for Player 1 if $n = 11$.
7. Find a winning strategy for Player 1 if $n = 12$.
8. Find a winning strategy for Player 1 if $n = 14$.
9. Find a winning strategy for Player 1 if $n = 25$.
10. Find a winning strategy for Player 1 if $n = 43$.
11. Show that Player 1 always has a winning strategy if n is not a Fibonacci number. Describe the winning strategy. Why doesn't Player 1 have a winning strategy if n is a Fibonacci number?

Unsolved Problems

1. Begin an array by writing the Fibonacci numbers: $0, 1, 1, 2, 3, 5, 8, 13, 21, \ldots$. Do not include the 0 or the first 1. Thus, the first row should be $1 \quad 2 \quad 3 \quad 5 \quad 8 \quad 13 \quad \cdots$ Start row 2 with the least unused positive integer, which is 4. Follow 4 by 6 (the rule for choosing the second term in each row will be described below), and finish the row using the Fibonacci recurrence, i.e. add the two most recent numbers to produce the next. Thus, the array should be the following: $\begin{array}{cccccc} 1 & 2 & 3 & 5 & 8 & 13 \quad \cdots \\ 4 & 6 & 10 & 16 & 26 & 42\cdots \end{array}$ Start row 3 with the least unused, which is 7, follow 7 by 12, and then use the Fibonacci recurrence to complete the row.

   To obtain the second number in each row, do the following. Let

   $$r = \frac{1+\sqrt{5}}{2}.$$

   Let x be the first number in the row. Then the second number is $\lfloor rx \rfloor$ if the row number is even and $\lfloor rx \rfloor + 1$ if the row number is odd. Here, $\lfloor a \rfloor$ means the greatest integer less than or equal to a. Thus, for example, row 3 starts with the least unused, which is 7, and is followed by $\lfloor 7r \rfloor = 11$.

   Find the first 8 rows of this array. What do you observe about the numbers in the second column?

2. Which numbers can be expressed as the sum of a Fibonacci number and a prime number? For example,

   $$122 = 13 + 109 = 21 + 101 = 55 + 67.$$

   The first number in each of the three summations is a Fibonacci number, while the second is a prime number.

   (a) Let $W(n)$ denote the number of ways that an integer n can be expressed as the sum of a Fibonacci number and a prime number. Find $W(n)$ for n from 1 to 25. (Remember that 0 is a Fibonacci number).

   (b) Find two numbers such that $W(n) = 0$.

   (c) **Unsolved question:** Are there any Fibonacci numbers greater than 1 that cannot be expressed as the sum of a Fibonacci number and a prime number? (i.e. is it possible to find a Fibonacci number n such that $W(n) = 0$?)

3. A number is said to be **squareful** if it contains at least one square in its prime factorization. The first six squareful numbers are 4,8,9,12,16,18.

   (a) Find the first six squareful Fibonacci numbers.

   (b) **Unsolved question:** Is it possible to find a Fibonacci number F_n (i.e. the n-th Fibonacci number, $F_0 = 0, F_1 = 1, F_2 = 1, F_3 = 2, F_4 = 3, F_5 = 5, F_6 = 8, \ldots$) such that n is prime and F_n is squareful?

4. Are there infinitely many prime Fibonacci numbers?
5. Which Fibonacci numbers can be written as half the difference or sum of two cubes?

Chapter 18

Mersenne Primes and Perfect Numbers

We begin this section by considering primes that can be written in the form $a^n - 1$ with $n \geq 2$. For example, 31 is such a prime, since $31 = 2^5 - 1$. The first step is to look at some data:

	$n = 2$	$n = 3$	$n = 4$	$n = 5$
$a = 2$	3	7	$15 = 3 \cdot 5$	31
$a = 3$				
$a = 4$				
$a = 5$				

We make the following observations:

1. If a is odd, then $a^n - 1$ is even, so it cannot be prime.
2. $a^n - 1$ is always divisible by $a - 1$.

   Proof. $a^n - 1 = (a-1)(a^{n-1} + a^{n-2} + \cdots + a^2 + a + 1)$. We refer to this formula as the **Geometric Series Formula**.

Thus, $a^n - 1$ will always be composite unless $a - 1 = 1$, i.e. $a = 2$. Next, let's look at a table of values of $2^n - 1$.

n	2	3	4	5	6	7	8	9	10
$2^n - 1$	3	7							

Theorem 18.1 If n is divisible by m, then $2^n - 1$ is divisible by $2^m - 1$.

Proof. Suppose that $m \mid n$. Then there is an integer k such that $n = mk$. Then

$$2^n = 2^{mk} = (2^m)^k,$$

and

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

Thus, if n is composite, then $2^n - 1$ is composite, and we can conclude the following result.

Theorem 18.2 If $a^n - 1$ is prime for some integers $a \geq 2$ and $n \geq 2$, then $a = 2$ and n is prime.

Definition 18.1 Primes of the form

$$2^p - 1$$

are called **Mersenne primes**.

The first few Mersenne primes are $2^2 - 1 = 3, 2^3 - 1 = 7, 2^5 - 1 = 31, 2^7 - 1 = 127, 2^{13} - 1 = 8191$. Note that not every number of the form $2^p - 1$ is prime. For example, $2^{11} - 1 = 2047 = 23 \cdot 89$ and $2^{29} = 233 \cdot 1103 \cdot 2089$.

It is currently not known whether or not there are infinitely many Mersenne primes. The largest known Mersenne prime is

$$2^{43,112,609} - 1,$$

discovered in 2008 at UCLA. This prime has 12,978,189 digits! You can participate in the search for such primes by downloading software from the Great Internet Mersenne Prime Search (GIMPS) website: `www.mersenne.org/prime.htm`. The following conjecture has been made (see *American Mathematical Monthly*, Volume 96, pages 125–128) about Mersenne primes, and it has been verified for all positive odd integers less than 20000000.

Conjecture 18.1 Mersenne Prime Conjecture Let p be any odd natural number. If two of the following conditions hold, then so does the third:

1. $p = 2^k \pm 1$ or $p = 4k \pm 3$.
2. $2^p - 1$ is a prime.
3. $\dfrac{2^p + 1}{3}$ is prime.

Complete the following table. Is the conjecture valid for the values of p considered below?

p	Is $p = 2^k \pm 1$ or $p = 4k \pm 3$?	Is $2^p - 1$ a prime?	Is $\frac{2^p+1}{3}$ prime?
3			
5			
7			
9			
11			
13			

The integer 6 has the property that the sum of the proper divisors of 6 (i.e. the divisors of 6 other than 6 itself) is equal to 6:

$$1 + 2 + 3 = 6.$$

Numbers with this property are called **perfect numbers**. Can you find another perfect number? The Greeks knew a method for finding perfect numbers that is closely related to Mersenne primes.

Theorem 18.3 Euclid's Perfect Number Formula. If $2^p - 1$ is a prime number, then

$$2^{p-1}(2^p - 1)$$

is a perfect number.

The first two Mersenne primes are $2^2 - 1 = 3$ and $2^3 - 1 = 7$. If we apply Euclid's Perfect Number Formula to these two Mersenne primes, we get the two perfect numbers 6 and 28. The next Mersenne prime is $2^5 - 1 = 31$. Euclid's formula gives us the perfect number 496. To check that 496 is a perfect number, we need to sum its proper divisors. We factor 496 as $496 = 2^4 \cdot 31$, so the proper divisors are

$$1, 2, 2^2, 2^3, 2^4, 31, 2 \cdot 31, 2^2 \cdot 31, 2^3 \cdot 31.$$

To illustrate the general method that we'll use to prove Euclid's Formula, we'll add the divisors in two stages. First,

$$1 + 2 + 2^2 + 2^3 + 2^4 = 31,$$

and second,

$$31 + 2 \cdot 31 + 2^2 \cdot 31 + 2^3 \cdot 31 = 31 \cdot 15.$$

Then

$$31 + 31 \cdot 15 = 496,$$

so 496 is indeed a perfect number. We can use a similar idea to prove Euclid's Formula.

Proof. Suppose that 2^p-1 is prime. Then the proper divisors of $2^{p-1}(2^p-1)$ are

$$1, 2, 2^2, 2^3, \ldots, 2^{p-1}$$

and

$$2^p-1, 2\cdot(2^p-1), 2^2\cdot(2^p-1), \ldots, 2^{p-2}(2^p-1).$$

We add the divisors together to obtain:

$$1+2+2^2+2^3+\cdots+2^{p-1} = \frac{2^p-1}{2-1} = 2^p-1$$

and

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

Then the sum of the proper divisors of $2^{p-1}(2^p-1)$ is

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

so $2^{p-1}(2^p-1)$ is indeed a perfect number.

A natural question to ask at this point is whether Euclid's Formula actually describes all perfect numbers. Does every perfect number have the form $2^{p-1}(2^p-1)$ with 2^p-1 prime, or are there other perfect numbers? Approximately 2000 years after Euclid's death, Euler showed that Euclid's Formula gives all *even* perfect numbers.

Theorem 18.4 Euler's Perfect Number Theorem. If n is an even perfect number, then n is of the form

$$n = 2^{p-1}(2^p-1),$$

where 2^p-1 is a Mersenne prime.

You will prove Euler's Perfect Number Theorem as a series of exercises. To prove Euler's Perfect Number Theorem, you will need to use the sigma function, which is defined as follows.

Definition 18.2 The sigma function $\sigma(n)$ is defined as

$$\sigma(n) = \text{sum of all divisors of } n \text{ including 1 and } n.$$

Example 18.1

$$\begin{aligned}\sigma(6) &= 1+2+3+6=12\\ \sigma(8) &= 1+2+4+8=15\\ \sigma(18) &= 1+2+3+6+9+18=39.\end{aligned}$$

Theorem 18.5 Sigma Function Formulas. Suppose that p is prime and $k \geq 1$.

1. $\sigma(p) = p+1$
2. $\sigma(p^k) = 1+p+p^2+\cdots+p^k = \dfrac{p^{k+1}-1}{p-1}$.
3. If $\gcd(m,n)=1$, then $\sigma(mn)=\sigma(m)\sigma(n)$.

The sigma function is related to perfect numbers in the following way. Recall that a number n is perfect if the sum of its divisors, other than n is equal to n. The sigma function is the sum of the divisors of n, including n. Thus, a number n is a perfect number exactly when $\sigma(n)=2n$.

Note that Euler's Formula describes all even perfect numbers, but says nothing about odd perfect numbers. It is not currently known whether or not any odd perfect numbers exist.

Problem Set

1. Show that if $a^n + 1$ is prime for some integers $a \geq 2$ and $n \geq 1$, then n must be a power of 2.

2. Let
$$F_k = 2^{2^k} + 1.$$
For example, $F_1 = 5, F_2 = 17, F_3 = 257, F_4 = 65537$. Fermat thought that all the F_k's might be prime, but Euler showed in 1732 that F_5 factors as
$$F_5 = 641 \cdot 6700417.$$
In 1880, Landry showed that F_6 is composite. Primes of the form $2^{2^k} + 1$ are called **Fermat primes**. Show that if $k \neq m$, then $\gcd(F_k, F_m) = 1$. Hint: if $k > m$, show that $F_m \mid (F_k - 2)$.

3. The numbers $3^n - 1$ are never prime if $n \geq 2$ since they are always even. However, it sometimes happens that $\dfrac{3^n - 1}{2}$ is prime. For example, $(3^3 - 1)/2 = 13$ is prime.

   (a) Find another prime of the form $(3^n - 1)/2$.

   (b) If n is even, show that $(3^n - 1)/2$ is divisible by 4, so it can never be prime.

   (c) Show that if n is a multiple of 5, then $(3^n - 1)/2$ is not prime.

   (d) Do you think that there are infinitely many primes of the form $(3^n - 1)/2$?

4. If m and n are integers with $\gcd(m, n) = 1$, prove that $\sigma(mn) = \sigma(m)\sigma(n)$. Hint: start by proving that $\sigma(pq) = \sigma(p)\sigma(q)$ for distinct primes p and q.

5. Compute the following values of the sigma function.

   (a) $\sigma(10)$ (b) $\sigma(20)$ (c) $\sigma(1728)$

6. (a) Show that a power of 3 can never be a perfect number.

   (b) More generally, if p is an odd prime, show that a power p^k can never be a perfect number.

   (c) Show that a number of the form $3^i \cdot 5^j$ can never be a perfect number.

   (d) More generally, if p is an odd prime number greater than 3, show that the product $3^i p^j$ can never be a perfect number.

   (e) Finally, show that if p and q are distinct odd prime numbers, then a number of the form $q^i p^j$ can never be a perfect number.

7. Show that a number of the form $3^m \cdot 5^n \cdot 7^k$ can never be a perfect number.

8. Take any even perfect number, except 6. Now sum the digits of the resulting number. Then sum the digits of the sum, and repeat this process until you obtain a single digit. What will this digit be? Can you prove that your conjecture is always true? For reference, the first several even perfect numbers (after 6) are 28, 496, 8128, and 33550336.

9. In this exercise, you will prove Euler's Perfect Number Theorem.

   (a) Suppose that $n = 2^k m$, where $k \geq 1$ and m is odd, is an even perfect number. Show that

   $$\sigma(n) = 2n = (2^{k+1} - 1)\sigma(m).$$

   (b) Show that there is some positive integer c so that

   $$\sigma(m) = 2^{k+1}c \text{ and } m = (2^{k+1} - 1)c.$$

   (c) Show that $c = 1$ by assuming that $c > 1$ and deriving a contradiction.

   (d) Conclude that $\sigma(m) = 2^{k+1} = m + 1$.

   (e) Conclude that m is prime, and that if n is an even perfect number, then n is of the form

   $$n = 2^k(2^{k+1} - 1),$$

   where $(2^{k+1} - 1)$ is prime.

10. If the product of the divisors of a number n (other than n itself) is equal to n, then we say that n is a *product perfect* number. For example, 6 is a product perfect number since $1 \cdot 2 \cdot 3 = 6$.

    (a) List all product perfect numbers between 2 and 50.

    (b) Describe all product perfect numbers. Your description should be precise enough to enable you to easily solve such problems as "Is 35710 product perfect?" and "Find a product perfect number larger than 10000.".

Chapter 19

Powers Modulo m and Successive Squaring

How would you compute

$$5^{100000000000000} \mod 12830603?$$

If 12830603 were prime, we might try using Fermat's Little Theorem, or the Euler-Fermat Theorem if it is not prime. However, we would like to be able to compute $5^{100000000000000} \mod 12830603$ without first having to factor 12830603. In fact, later we will want to be able to compute $a^k \mod m$ for numbers a, k, m that have hundreds of digits, so we certainly do not want to have to factor m first. These computations will be important when we study RSA Public Key Cryptography.

The method that we will use to compute $a^k \mod m$ is called the method of *successive squaring*. We will illustrate the idea with an example.

Example 19.1 Compute $7^{327} \mod 853$.

Solution: First, observe that

$$327 = 256 + 64 + 4 + 2 + 1.$$

Thus,

$$7^{327} \quad = \quad 7^{256} 7^{64} 7^4 7^2 7^1.$$

We can compute the 2^k-powers of 7 modulo 853 by successive squaring, as illustrated below.

$$\begin{aligned}
7^1 &\equiv 7 \mod 853\\
7^2 &\equiv 49 \mod 853\\
7^4 &\equiv (49)^2 \equiv 695 \mod 853\\
7^8 &\equiv (695)^2 \equiv 227 \mod 853\\
7^{16} &\equiv (227)^2 \equiv 349 \mod 853\\
7^{32} &\equiv (349)^2 \equiv 675 \mod 853\\
7^{64} &\equiv (675)^2 \equiv 123 \mod 853\\
7^{128} &\equiv (123)^2 \equiv 628 \mod 853\\
7^{256} &\equiv (628)^2 \equiv 298 \mod 853
\end{aligned}$$

Thus,

$$\begin{aligned}
7^{327} &= 7^{256}7^{64}7^{4}7^{2}7^{1}\\
&\equiv 298 \cdot 123 \cdot 695 \cdot 49 \cdot 7 \mod 853\\
&\equiv 828 \cdot 695 \cdot 49 \cdot 7 \mod 853\\
&\equiv 538 \cdot 49 \cdot 7 \mod 853\\
&\equiv 727 \cdot 7 \mod 853\\
&\equiv 286 \mod 853.
\end{aligned}$$

Example 19.2 Using successive squaring, show that

$$2^{283976710803262} \equiv 280196559097287 \mod 283976710803263.$$

Is the number 283976710803263 prime or composite?

Solution: If 283976710803263 were prime, then $2^{283976710803262}$ would be congruent to 1 modulo 2839767108032623. Thus, 2839767108032623 is composite. Note that we have determined that 2839767108032623 is composite without actually computing any factors.

Problem Set

1. Use the method of successive squaring to compute each of the following:
   (a) $5^{13} \mod 23$
   (b) $28^{749} \mod 1147$
   (c) $999^{179} \mod 1763$
2. (a) Compute $7^{7386} \mod 7387$. Is 7387 prime?
   (b) Compute $7^{7392} \mod 7393$. Is 7393 prime?
3. Show that 1763 is composite. Hint: compute $2^{1762} \mod 1763$.
4. Show that 1387 is composite.
5. (a) Show that 11111 is composite.
   (b) Show that 1111111 is composite.
   (c) Show that 1111111111111 is composite.

Chapter 20

Computing k-th Roots Modulo m

We have learned how to solve linear congruences of the form $ax \equiv b \mod m$ and quadratic congruences of the form $x^2 \equiv b \mod m$. In this section, we will develop techniques for solving congruences of the form

$$x^k \equiv b \mod m,$$

where $k \geq 3$. These methods will be important when we study RSA Public Key Cryptography.

Example 20.1 Solve the congruence

$$x^{131} \equiv 758 \mod 1073.$$

Solution: First, we compute $\phi(1073)$. Since $1073 = 29 \cdot 37$,

$$\phi(1073) = \phi(29)\phi(37) = 28 \cdot 36 = 1008.$$

Next, we observe that

$$\gcd(131, 1008) = 1,$$

so there are integers u and v such that

$$131u + 1008v = 1.$$

Using the method described in Chapter 5, we find $u = 731$ and $v = -95$. Thus,

$$131 \cdot 731 - 1008 \cdot 95 = 1.$$

Using this equation, we obtain the following:

$$\begin{aligned}(x^{131})^{731} &= x^{131\cdot 731} \\ &= x^{1+1008\cdot 95} \\ &= x \cdot (x^{1008})^{95}.\end{aligned}$$

By the Euler-Fermat Theorem,

$$x^{1008} \equiv 1 \mod 1073.$$

Thus,

$$(x^{131}) \equiv x \mod 1073,$$

so the original congruence becomes

$$x \equiv (x^{131})^{731} \equiv 758^{731} \mod 1073.$$

Thus, to find the solution of the original congruence, we must compute 758^{731} mod 1073. We can do this using the method of successive squaring. First, observe that

$$\begin{aligned} 731 &= 512 + 128 + 64 + 16 + 8 + 2 + 1 \\ 758^{731} &= 758^{512} \cdot 758^{128} \cdot 758^{64} \cdot 758^{16} \cdot 758^{8} \cdot 758^{2} \cdot 758. \end{aligned}$$

Computing powers of 758 modulo 1073, we obtain:

$$\begin{aligned} 758 &\equiv 758 \mod 1073 \\ 758^2 &\equiv 509 \mod 1073 \\ 758^4 &\equiv 488 \mod 1073 \\ 758^8 &\equiv 1011 \mod 1073 \\ 758^{16} &\equiv 625 \mod 1073 \\ 758^{32} &\equiv 53 \mod 1073 \\ 758^{64} &\equiv 663 \mod 1073 \\ 758^{128} &\equiv 712 \mod 1073 \\ 758^{256} &\equiv 488 \mod 1073 \\ 758^{512} &\equiv 1011 \mod 1073. \end{aligned}$$

Thus,

$$\begin{aligned} 758^{731} &= 758^{512} \cdot 758^{128} \cdot 758^{64} \cdot 758^{16} \cdot 758^{8} \cdot 758^{2} \cdot 758 \\ &\equiv 1011 \cdot 712 \cdot 663 \cdot 625 \cdot 1011 \cdot 509 \cdot 758 \mod 1073 \\ &\equiv 922 \cdot 197 \cdot 632 \cdot 758 \mod 1073 \\ &\equiv 297 \cdot 498 \mod 1073 \\ &\equiv 905 \mod 1073. \end{aligned}$$

Finally, note that we can use successive squaring to check that

$$905^{131} \equiv 758 \mod 1073.$$

The general method for computing k-th roots modulo m is described by the following algorithm.

Algorithm 20.1 Computing k-th Roots Modulo m. Let b, k, and m be integers such that

$$\gcd(b,m) = 1 \text{ and } \gcd(k, \phi(m)) = 1.$$

Then the following steps give a solution to the congruence

$$x^k \equiv b \mod m.$$

1. Compute $\phi(m)$.
2. Use the Euclidean Algorithm to find integers u and v that satisfy

$$ku + \phi(m)v = 1.$$

3. Compute $b^u \mod m$ by successive squaring. The value obtained gives the solution x.

Proof. We need to check that $x = b^u$ is a solution to the congruence $x^k \equiv b \mod m$.

$$\begin{aligned} x^k &= (b^u)^k \\ &= b^{uk} \\ &= b^{1-\phi(m)v} \\ &= b \cdot (b^{\phi(m)})^{-v} \\ &\equiv b \mod m. \end{aligned}$$

Problem Set

1. Solve the congruence $x^{329} \equiv 452 \mod 1147$.
2. Solve the congruence $x^{113} \equiv 347 \mod 463$.
3. Solve the congruence $x^{275} \equiv 139 \mod 588$.
4. (a) Try to use the method described in the Algorithm for Computing k-th Roots Modulo m to compute the square root of 23 modulo 1279 (note: the number 1279 is prime). What goes wrong?

   (b) More generally, if p is an odd prime, explain why the method described in the Algorithm cannot be used to find square roots modulo p.

   (c) Even more generally, explain why the Algorithm for Computing k-th Roots Modulo m does not work if $\gcd(k, \phi(m)) > 1$.

Chapter 21

RSA Public Key Cryptography

In this section, we describe a technique for encoding and decoding messages.

1. The first step in encoding a message is to convert it into a string of numbers. One simple method for doing this is to set

$$A = 11, B = 12, C = 13, \ldots, Z = 36.$$

   Here is a convenient table to use:

A	B	C	D	E	F	G	H	I	J	K	L	M
11	12	13	14	15	16	17	18	19	20	21	22	23

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
24	25	26	27	28	29	30	31	32	33	34	35	36

   Note that we have ignored spaces and other punctuation marks.

2. Next, we choose two large primes p and q and multiply them together to obtain a modulus m. We also compute

$$\phi(m) = \phi(pq) = (p-1)(q-1).$$

3. Next, we choose a number k such that

$$\gcd(k, \phi(m)) = 1.$$

4. Next, publish the numbers k and m for anyone to know, and keep the values of p and q secret.

5. Anyone who wants to **encode a message** to send to us can use the values of m and k to encode the message in the following way.

   (a) First, they convert their message into a string of digits as described above.

   (b) Next, they look at the number m and break their string of digits into numbers that are less than m so that their message is a list of numbers $a_1, a_2, \ldots, a_r$.

(c) Next, they use successive squaring to compute

$$a_1^k \mod m, a_2^k \mod m, \ldots, a_r^k \mod m.$$

These values form a new list of numbers $b_1, b_2, \ldots b_r$. This list is the encoded message.

6. To **decode the message** once we receive it, we use the following method.

(a) We have received the list of numbers $b_1, b_2, \ldots, b_r$, and we need to recover the numbers $a_1, a_2, \ldots, a_r$.

(b) Recall that each b_i is congruent to a_i^k modulo m, so to find each a_i, we must solve the congruence

$$x^k \equiv b_i \mod m.$$

Using the Algorithm for Computing k-th Roots Modulo m (described in Chapter 20), we can do this if we know $\phi(m)$.

(c) Since we know the values of p and q with $m = pq$, we know that

$$\phi(m) = \phi(pq) = (p-1)(q-1) = pq - p - q + 1 = m - p - q + 1.$$

(d) Finally, we apply the Algorithm for Computing k-th Roots Modulo m to solve each of the congruences $x^k \equiv b_i \mod m$. The solutions are the numbers $a_1, a_2, \ldots, a_r$. We then use this string of digits to recover the original message. For reference, here is the Algorithm for Computing k-th Roots Modulo m: Let b, k, and m be integers such that

$$\gcd(b, m) = 1 \text{ and } \gcd(k, \phi(m)) = 1.$$

Then the following steps give a solution to the congruence

$$x^k \equiv b \mod m.$$

i. Compute $\phi(m)$.

ii. Use the Euclidean Algorithm to find integers u and v that satisfy

$$ku + \phi(m)v = 1.$$

iii. Compute $b^u \mod m$ by successive squaring. The value obtained gives the solution x.

Example 21.1 Encode the message "STANFORD" using the public key $m = 143$ and $k = 23$.

Solution: First, we convert the text "STANFORD" to a string of numbers: 2930111416252814. The number m has three digits, so we break up the message 2930111416252814 as a string of numbers that are 2 digits each:

$$29, \quad 30, \quad 11, \quad 24, \quad 16, \quad 25, \quad 28, \quad 14.$$

Next, we use successive squaring to compute the 23-rd power of each number modulo 143. First, we compute $29^{23} \mod 143$. We have:

$$\begin{aligned} 29^{23} &= 29^{16}29^{4}29^{2}29^{1} \\ 29 &\equiv 29 \mod 143 \\ 29^{2} &\equiv 126 \mod 143 \\ 29^{4} &\equiv 3 \mod 143 \\ 29^{8} &\equiv 9 \mod 143 \\ 29^{16} &\equiv 81 \mod 143. \end{aligned}$$

Thus,

$$29^{23} \equiv 81 \cdot 3 \cdot 126 \cdot 29 \equiv 35 \mod 143.$$

Use successive squaring to compute the 23-rd power of each of the remaining numbers modulo 143:

$$\begin{aligned} 29^{23} &\equiv 35 \mod 143 \\ 30^{23} &\equiv \qquad \mod 143 \\ 11^{23} &\equiv \qquad \mod 143 \\ 24^{23} &\equiv \qquad \mod 143 \\ 16^{23} &\equiv \qquad \mod 143 \\ 25^{23} &\equiv \qquad \mod 143 \\ 28^{23} &\equiv \qquad \mod 143 \\ 14^{23} &\equiv \qquad \mod 143 \end{aligned}$$

Example 21.2 Decode the message

$$20, \quad 130, \quad 62, \quad 107$$

using the primes $p = 11$ and $q = 13$ and $k = 23$.

Solution: We must solve the congruences

$$\begin{aligned} a_1^{23} &\equiv 20 \mod 143 \\ a_2^{23} &\equiv 130 \mod 143 \\ a_3^{23} &\equiv 62 \mod 143 \\ a_4^{23} &\equiv 107 \mod 143 \end{aligned}$$

We can solve each of these using the Algorithm for Computing k-th Roots Modulo m. Since we know the primes $p = 11$ and $q = 13$, we can compute

$$\phi(m) = \phi(11)\phi(13) = 10 \cdot 12 = 120.$$

Next, we find integers u and v such that

$$23u + 120v = 1.$$

Using the Euclidean Algorithm, we obtain

$$u = 47 \text{ and } v = -9.$$

We are now able to solve each congruence. To solve the first congruence, we compute $20^u = 20^{47}$ modulo 143 by successive squaring. We obtain:

$$\begin{aligned}
20^{47} &= 20^{32}20^{8}20^{4}20^{2}20^{1} \\
20^{1} &\equiv 20 \mod 143 \\
20^{2} &\equiv 114 \mod 143 \\
20^{4} &\equiv 126 \mod 143 \\
20^{8} &\equiv 3 \mod 143 \\
20^{16} &\equiv 9 \mod 143 \\
20^{32} &\equiv 81 \mod 143
\end{aligned}$$

Thus,

$$20^{47} \equiv 20 \cdot 114 \cdot 126 \cdot 3 \cdot 81 \equiv 15 \mod 143,$$

so the first number in the message is 15, which corresponds to the letter E. Finish decoding the message by solving the remaining 3 congruences.

Example 21.3 Encode the message "To be or not to be" using the primes $p = 12553$ and $q = 13007$.

Solution: First, we compute the modulus

$$m = pq = 163276871$$

and

$$\phi(m) = 163251312.$$

We also need to choose a k that is relatively prime to $\phi(m)$. We choose

$$k = 79921.$$

The message "TOBEORNOTTOBE" becomes the string of digits

$$30251215252824253030251215.$$

The modulus m is 9 digits long, so we break the message up into 8-digit numbers:

$$30251215, \quad 25282425, \quad 30302512, \quad 15.$$

Next, we use the method of successive squaring to raise each of these numbers to the k-th power modulo m:

$$\begin{aligned} 30251215^{79921} &\equiv 149419241 \mod 163276871 \\ 25282425^{79921} &\equiv 62721998 \mod 163276871 \\ 30302512^{79921} &\equiv 118084566 \mod 163276871 \\ 15^{79921} &\equiv 40481382 \mod 163276871 \end{aligned}$$

Thus, the encoded message is the list of numbers

$$149419241, \quad 62721998, \quad 118084566, \quad 40481382.$$

It is natural to consider how secure this cryptosystem is. Suppose that a message is intercepted by a third party. Since the modulus m and the exponent k are public, the third party can decode the message if they can find the value of $\phi(m) = \phi(p)\phi(q)$. So to decode the message, the third party must factor m to find the primes p and q. If m consists of 5 to 10 digits, then a computer will find the factors of m almost immediately. Using advanced methods from number theory, mathematicians have constructed techniques for factoring numbers with 50 to 100 digits. Thus, if the primes p and q have, say, 100 digits each, then there are no known techniques for the third party to determine p and q from the modulus $m = pq$. The idea underlying this coding technique is that although it is easy to multiply large numbers together, it is very difficult to factor a large number.

The cryptographic method described here is called a *public key cryptography system* because the encoding key consisting of the modulus m and the exponent k can be distributed to the public while the decoding method remains secure. This particular public key cryptosystem is called the *RSA public key cryptosystem* and is named after its inventors Ron Rivest, Adi Shamir, and Leonard Adleman, who invented the system in 1977.

Problem Set

1. Decode the following message, which was sent using the modulus $m = 7081$ and the exponent $k = 1789$:
$$5192, \quad 2604, \quad 4222.$$
Note that you will first need to factor m.

2. Research the history of public key cryptography and public key digital signatures. Discuss the political and social consequences of the availability of inexpensive unbreakable codes.

3. The problem of factoring large numbers has been much studied recently due to its importance in public key cryptography. Research each of the following factorization methods.

    (a) Pollard's ρ method

    (b) Pollard's $\rho - 1$ method

    (c) The quadratic sieve factorization method

    (d) Lenstra's elliptic curve factorization method

    (e) The number field sieve

Chapter 22

Pythagorean Triples

Definition. A **Pythagorean triple** is a triple (a, b, c) of integers such that

$$a^2 + b^2 = c^2.$$

The study of Pythagorean triples began long before the time of Pythagoras. In fact, there are Babylonian tablets, dating to around 1800 BC, that contain lists of such triples, including quite large ones, which indicates that the Babylonians probably had a systematic method for producing them.

(a) Find 4 examples of Pythagorean triples.

(b) Show that there are infinitely many Pythagorean triples by showing that if (a, b, c) is a Pythagorean triple, then (da, db, dc) is also a Pythagorean triple for any integer d.

(c) A **primitive Pythagorean triple** is a triple of numbers (a, b, c) that have no common factors and satisfy $a^2 + b^2 = c^2$. Find 4 examples of primitive Pythagorean triples.

(d) Prove that if (a, b, c) is a primitive Pythagorean triple, then either a is odd and b is even or a is even and b is odd. Also prove that c is always odd.

(e) Observe that if (a, b, c) is a primitive Pythagorean triple, then

$$a^2 = c^2 - b^2 = (c - b)(c + b).$$

For example,

$$3^2 = 5^2 - 4^2 = (5 - 4)(5 + 4) = 1 \cdot 9.$$

Write the Pythagorean triples

$$(15, 8, 17),\ (35, 12, 37),\ (33, 56, 65),\ (21, 20, 29),\ (63, 16, 65)$$

in this form (i.e. factor a^2 as a product of $(c - b)$ and $(c + b)$. In each case, what do you observe about $(c - b)$ and $(c + b)$? Prove that your observation is true for any primitive Pythagorean triple.

(f) Prove that any primitive Pythagorean triple (a, b, c) with a odd and b even can be obtained by using the formulas

$$a = st, \quad b = \frac{s^2 - t^2}{2}, \quad c = \frac{s^2 + t^2}{2},$$

where $s, t \geq 1$ are chosen to be any odd integers with no common factors.

(g) Show that if (a, b, c) is a primitive Pythagorean triple, then either a or b must be a multiple of 3.

(h) By examining the list of primitive Pythagorean triples in Problem 5, make a guess about whether a, b, or c is a multiple of 5. Try to show that your guess is correct.

(i) For each of the following questions, begin by compiling some data; next examine the data and formulate a conjecture. Finally, try to prove that your conjecture is correct.

i. Which odd numbers a can appear in a primitive Pythagorean triple (a, b, c)?

ii. Which even numbers b can appear in a primitive Pythagorean triple (a, b, c)?

iii. Which numbers c can appear in a primitive Pythagorean triple (a, b, c)?

(j) Observe that

$$33^2 + 56^2 = 65^2 \text{ and } 16^2 + 63^2 = 65^2$$

are 2 primitive Pythagorean triples with the same value of c. Can you find 3 primitive Pythagorean triples with the same value of c? Can you find more than 3?

(k) Observe that $(3, 4, 5)$, $(15, 8, 17)$, $(35, 12, 37)$, $(63, 16, 65)$ are all primitive Pythagorean triples that have $c = a + 2$.

i. Find two more primitive Pythagorean triples that have $c = a + 2$.

ii. Find a formula that describes all primitive Pythagorean triples (a, b, c) that have $c = a + 2$.

iii. For each primitive Pythagorean triple (a, b, c) that you've seen so far, compute the quantity $2c - 2a$. Do these values seem to have some special form? Try to prove that your observation is true for all primitive Pythagorean triples.

Chapter 23

Which Primes are Sums of Two Squares?

In this problem set, you will consider the following question: which prime numbers can be written as a sum of two squares? For example, the number 5 is a sum of two squares, since

$$5 = 1^2 + 2^2.$$

On the other hand, 19 cannot be written as a sum of two squares. To check this, note that none of the differences

$$19 - 1^2 = 18, \quad 19 - 2^2 = 15, \quad 19 - 3^2 = 10, \quad 19 - 4^2 = 3$$

is a square. In general, to check if a given number m is a sum of two squares, we check the numbers

$$m - 0^2, \quad m - 1^2, \quad m - 2^2, \ldots$$

until you obtain a square or until the numbers become negative.

(a) i. Make a list of the primes p, $5 \leq p \leq 229$ that can be written as a sum of two squares. (Ignore $p = 2$ for now.)

ii. Make a list of the primes p, $3 \leq p \leq 227$ that cannot be written as a sum of two squares.

iii. Do you observe any patterns? Consider the primes modulo 4. If $p \equiv 1 \mod 4$, is p always, sometimes, or never a sum of two squares? If $p \equiv 3 \mod 4$, is p always, sometimes, or never a sum of two squares?

(b) Prove that if the prime p can be written as a sum of two squares, then $p \equiv 1 \mod 4$.

(c) In the next problem, you will show that if p is a prime that is congruent to 1 modulo 4, then p can be written as a sum of two squares. In this problem, you will work through the method of proof known as Fermat's Descent Procedure for the specific example $p = 881$.

i. Verify that
$$387^2 + 1^2 = 170 \cdot 881.$$
Thus, you have written a multiple of p as a sum of two squares.

ii. Verify that $u = 47$ and $v = 1$ satisfy
$$u \equiv 387 \mod 170, \quad v \equiv 1 \mod 170, \quad -\frac{170}{2} \leq u, v \leq \frac{170}{2}.$$

iii. Verify that
$$47^2 + 1^2 \equiv 387^2 + 1^2 \equiv 0 \mod 170,$$
so $170 \mid (47^2 + 1^2)$ and $170 \mid (387^2 + 1^2)$.

iv. Verify that
$$47^2 + 1^2 = 170 \cdot 13$$
and
$$387^2 + 1^2 = 170 \cdot 881.$$

v. Multiply the equations in the previous step to show that
$$(47^2 + 1^2)(387^2 + 1^2) = 170^2 \cdot 13 \cdot 881.$$

vi. Use the identity $(u^2 + v^2)(A^2 + B^2) = (uA + vB)^2 + (vA - uB)^2$ to show that
$$18190^2 + 340^2 = 170^2 \cdot 13 \cdot 881.$$

vii. Divide by 170^2 to show that
$$107^2 + 2^2 = 13 \cdot 881.$$

viii. Observe that you have written a *smaller* multiple of 881 as a sum of two squares, and that you can repeat this process until p itself is written as a sum of two squares.

(d) In this problem, you will use Fermat's Descent Procedure to show that if $p \equiv 1 \mod 4$, then p can be written as a sum of two squares. So, suppose that p is a prime that is congruent to 1 modulo 4.

i. Show that there exists an integer A such that $p \mid (A^2 + 1)$. Hint: use quadratic reciprocity. If you haven't read the sections on quadratic reciprocity yet, just assume that there is an integer A such that $p \mid (A^2 + 1)$, and continue with the problem. It is always true that if $p \equiv 1 \mod 4$, then there is an integer A such that $p \mid (A^2 + 1)$.

ii. Show that there exist integers B $(B = 1)$ and M such that
$$A^2 + B^2 = Mp.$$
Show that $M < p$.

iii. Observe that if $M = 1$, then we're done, so suppose that $M \geq 2$. Choose numbers u and v satisfying

$$u \equiv A \mod M, \quad v \equiv B \mod M, \quad -\frac{1}{2}M \leq u, v \leq \frac{1}{2}M.$$

Show that there exists an integer r such that

$$u^2 + v^2 = Mr.$$

iv. Show that $(u^2 + v^2)(A^2 + B^2) = M^2 rp$.

v. Show that $r \geq 1$.

vi. Show that $r < M$.

vii. Show that $M \mid (uA + vB)$. Hint: use the identity $(u^2 + v^2)(A^2 + B^2) = (uA + vB)^2 + (vA - uB)^2$.

viii. Show that $M \mid (vA - uB)$. Hint: use the identity $(u^2 + v^2)(A^2 + B^2) = (uA + vB)^2 + (vA - uB)^2$.

ix. Conclude that

$$\left(\frac{uA + vB}{M}\right)^2 + \left(\frac{vA - uB}{M}\right)^2 = rp.$$

This means that you have written a *smaller* multiple of p as a sum of two squares.

x. Observe that you can repeat this process to write an even smaller multiple of p as a sum of two squares. Continuing repeatedly, observe that you must eventually end up with p itself written as a sum of two squares.

(e) Make a list of all primes $p < 50$ that can be written in the form

$$p = a^2 + ab + b^2.$$

For example, $p = 7$ has this form with $a = 2$ and $b = 1$, while $p = 11$ cannot be written in this form. Try to find a pattern and make a guess as to exactly which primes have this form, and try to prove at least part of your conjecture.

(f) Make a list of all primes $p < 50$ that can be written in the form

$$p = a^2 + 2b^2.$$

Try to find a pattern and make a guess as to exactly which primes have this form, and try to prove at least part of your conjecture.

(g) Suppose that p is a prime not equal to 5. If p can be written in the form $p = a + 5b^2$, show that

$$p \equiv 1 \text{ or } 9 \mod 20.$$

(h) Use the Descent Procedure twice, starting from the equation

$$557^2 + 55^2 = 26 \cdot 12049$$

to write the prime 12049 as a sum of two squares.

(i) Use the Descent Procedure, starting from the equation

$$259^2 + 1^2 = 34 \cdot 1973$$

to write the prime 1973 as a sum of two squares.

(j) Which primes $p < 100$ can be written as a sum of three squares,

$$p = a^2 + b^2 + c^2?$$

Based on the data that you collect, try to make a conjecture describing which primes can be written as a sum of three squares.

Chapter 24

Lagrange's Theorem

In this series of exercises, you will prove Lagrange's Theorem, which states that every positive integer can be expressed as the sum of four squares. For example,

$$5 = 2^2 + 1^2 + 0^2 + 0^2, \quad 21 = 4^2 + 2^2 + 1^2 + 0^2, \quad 127 = 11^2 + 2^2 + 1^2 + 1^2.$$

1. Show that 1 can be written as a sum of four squares.
2. Verify that

$$\begin{aligned}(x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2) &= (x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4)^2 \\ &\quad +(x_1y_2 - x_2y_1 + x_3y_4 - x_4y_3)^2 \\ &\quad +(x_1y_3 - x_3y_1 + x_4y_2 - x_2y_4)^2 \\ &\quad +(x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4)^2.\end{aligned}$$

   (This is known as Euler's identity). Conclude that the product of two numbers that are a sum of four squares is also a sum of four squares. Thus, since every positive integer greater than 1 can be expressed as a product of primes, it's enough to show that every prime can be expressed as a sum of four squares.

3. Show that 2 can be written as a sum of four squares.
4. Show that if p is an odd prime, then there are integers x, y, m such that

$$1 + x^2 + y^2 = mp.$$

5. Show that if p is an odd prime, then there exists an integer m such that $0 < m < p$ and integers x_1, x_2, x_3, x_4 such that

$$mp = x_1^2 + x_2^2 + x_3^2 + x_4^2.$$

6. Show that the least m with this property is $m = 1$, and conclude that every prime p can be written as a sum of four squares.

7. A related problem is to determine which positive integers can be expressed as a sum of three squares. Prove that any number of the form

$$4^t(8k+7),$$

where t and k are positive integers, can NOT be expressed as a sum of three squares.

8. Given a particular positive integer n, how can you (efficiently) write n as a sum of four squares? Try to determine an algorithm for writing a positive integer as a sum of four squares.

Chapter 25

Continued Fractions

Note: A calculator is required for this set of exercises, so if you don't have one, work with someone that does!

1. Observe that we can write the fraction $\dfrac{210}{47}$ as

$$4+\frac{1}{2+\frac{1}{7+\frac{1}{3}}}.$$

This is called the **continued fraction expansion** for the fraction $\dfrac{210}{47}$. Note that in the continued fraction expansion, all of the denominators are equal to 1. A more compact notation for this continued fraction expansion is $[4;2,7,3]$. Find the simple fraction corresponding to the continued fraction expansion $[1;2,3,4]$.

2. To find the continued fraction expansion of $\dfrac{8}{5}$, use the following procedure:

$$\begin{aligned} 8/5 &= 1+3/5 \\ &= 1+1/5/3 \\ &= 1+\frac{1}{1+\frac{2}{3}} \\ &= 1+\frac{1}{1+\frac{1}{1+\frac{1}{2}}} \end{aligned}$$

3. Consider the decimal expansion of π:

$$\pi = 3.14159265358979323846264 33\ldots$$

Observe that we can write this as

$$\pi = 3+\text{something},$$

where the “something” is a number between 0 and 1. Next, observe that we can rewrite this as:

$$\begin{aligned}
\pi &= 3 + 0.14159265358979323846264433\ldots \\
&= 3 + \frac{1}{\frac{1}{0.14159265358979323846264433\ldots}} \\
&= 3 + \frac{1}{7.06251330593104576930051\ldots} \\
&= 3 + \frac{1}{7 + 0.06251330593104576930051\ldots} \\
&= 3 + \frac{1}{7 + \text{a little bit more}}
\end{aligned}$$

The final equation above gives the fairly good approximation $\frac{22}{7}$ for π.

Now, if we repeat this process, we obtain:

$$\begin{aligned}
0.06251330593104576930051\ldots &= \frac{1}{\frac{1}{0.06251330593104576930051\ldots}} \\
&= 15.996594406685719888923060 \\
&= 15 + 0.996594406685719888923060
\end{aligned}$$

Thus, we have the following representation of π:

$$\pi = 3 + \frac{1}{7 + \frac{1}{15 + 0.996594406685719888923060}}$$

The bottom level of this fraction is 15.996594406685719888923060, which is very close to 16. If we replace it with 16, we get a rational number that is very close to π:

$$3 + \frac{1}{7 + \frac{1}{16}} = \frac{355}{113} = 3.14159292035398230088849557\ldots$$

The fraction $\frac{355}{113}$ agrees with π to six decimal places.

Continue this process, at each stage flipping the decimal that is left over and then separating off the whole integer part, to obtain a four-layer fraction representation of π. Use your final representation to get a rational number approximation for π, and compare with the known decimal approximation of π to see how accurate your approximation is.

4. An expression of the form

$$x = a_0 + \cfrac{1}{a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \frac{1}{\cdots}}}}$$

is called the **continued fraction** expansion of x. Use the procedure described above to compute the first 10 terms in the continued fraction of $\sqrt{2}$.

5. Find the continued fraction of 3.245.

6. Compute the first 10 terms in the continued fraction of $e = 2.7182818\ldots$.

7. (a) Compute the first 10 terms in the continued fractions of $\sqrt{3}$ and $\sqrt{5}$.

   (b) Do the terms in the continued fraction of $\sqrt{3}$ appear to follow a repetitive pattern? If so, prove that they really do repeat.

   (c) Do the terms in the continued fraction of $\sqrt{5}$ appear to follow a repetitive pattern? If so, prove that they really do repeat.

8. Compute the first 10 terms in the continued fraction expansion of the golden ratio $\phi = \dfrac{1+\sqrt{5}}{2}$.

9. Find the following remarkable continued fractions:

   (a) $\dfrac{4}{\pi}$

   (b) e

   (c) $\dfrac{e^{1/s}+1}{e^{1/s}-1}$

   (d) $\left(\sqrt{\phi+2}-\sqrt{\phi}\right)e^{2\pi/5}$, where $\phi = \frac{1+\sqrt{5}}{2}$ is the golden ratio.

10. Since all of the numerators in a continued fraction expansion are 1, we can express continued fraction expansions in a more convenient way by just listing the denominators. We write

$$[a_0, a_1, a_2, a_3, \ldots]$$

as shorthand for the continued fraction

$$a_0 + \cfrac{1}{a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \frac{1}{\cdots}}}}$$

Using this notation, our continued fraction expansion of π can be written as

$$\pi = [3, 7, 15, 1, 292, 1, 1, 1, 2, 1, 3, 1, 14, 2, 1, 1, 2, \ldots].$$

(a) The continued fraction expansion of π^2 is

$$[?,?,?,1,2,47,1,8,1,1,2,2,1,1,8,3,1,10,\ldots].$$

Fill in the three initial missing entries.

(b) Use the first five terms in the continued fraction of π^2 to find a rational number that is close to π^2. How close do you come?

11. We have seen that if a number α has a continued fraction expansion

$$\alpha = [a_0, a_1, a_2, \ldots],$$

then cutting off after a few terms gives a rational number that is close to α. The n**-th convergent to** α is the rational number

$$\frac{p_n}{q_n} = [a_0, a_1, a_2, \ldots, a_n] = a_0 + \cfrac{1}{a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \cdots + \frac{1}{a_n}}}}$$

obtained by using the terms up to a_n in the continued fraction expansion of α. For example, for the continued fraction expansion of

$$\pi = [3; 7, 15, 1, 292, 1, 1, 1, 2, 1, 3, 1, 14, 2, 1, 1, 2, \ldots],$$

the first few convergents are:

$$\begin{aligned}
\frac{p_0}{q_0} &= 3 \\
\frac{p_1}{q_1} &= 3 + \frac{1}{7} = \frac{22}{7} = 3.142857143 \\
\frac{p_2}{q_2} &= 1 + \frac{1}{7 + \frac{1}{15}} = \frac{333}{106} = 3.141509434
\end{aligned}$$

For the continued fraction expansion of $\sqrt{2} = [1, 2, 2, 2, 2, 2, 2, 2, \ldots]$, the first few convergents are:

$$\begin{aligned}
\frac{p_0}{q_0} &= 1 \\
\frac{p_1}{q_1} &= 1 + \frac{1}{2} = \frac{3}{2} = 1.5 \\
\frac{p_2}{q_2} &= 1 + \frac{1}{2 + \frac{1}{2}} = \frac{7}{5} = 1.4
\end{aligned}$$

For each $n = 1, 2, \ldots, 7$, compute the n-th convergent to $\sqrt{3}$.

12. Find the first 10 convergents in the continued fraction expansion of $\phi = \frac{1+\sqrt{5}}{2}$. What do you observe? Hint: Fibonacci numbers. See 17 for more information on Fibonacci numbers.

13. As in the previous problem, let

$$\frac{p_n}{q_n} = [a_0, a_1, a_2, \ldots, a_n] = a_0 + \cfrac{1}{a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \frac{1}{a_n}}}}$$

denote the n-th convergent to α.

(a) Show that $p_0 = a_0$ and $q_0 = 1$.

(b) Show that $p_1 = a_1 a_0 + 1$ and $q_1 = a_1$.

(c) Show that $p_2 = a_2 a_1 a_0 + a_2 + a_0$ and $q_2 = a_2 a_1 + 1$.

(d) Show that $p_3 = a_3 a_2 a_1 a_0 + a_3 a_2 + a_3 a_0 + a_1 a_0 + 1$ and $q_3 = a_3 a_2 a_1 + a_3 + a_1$.

(e) Show that, for all $n \geq 2$,

$$p_n = a_n p_{n-1} + p_{n-2}.$$

(f) Show that, for all $n \geq 2$,

$$q_n = a_n q_{n-1} + q_{n-2}.$$

14. Let the decimal expansion of α be

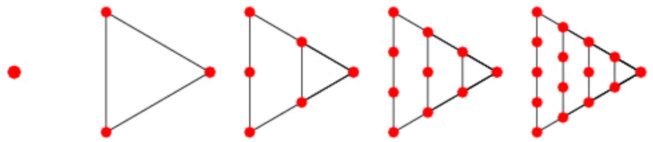
$$\alpha = b + \frac{b_1}{10} + \frac{b_2}{10^2} + \frac{b_3}{10^3} + \cdots,$$

where $0 \leq b_k \leq 9$ for all k. Suppose that for some convergent $\frac{p_n}{q_n}$, we have $q_n = 100$. Prove that either $b_3 = b_4 = 0$ or $b_3 = b_4 = 9$.

Chapter 26

Geometric Numbers

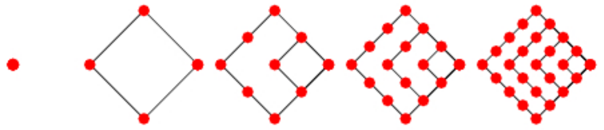
Triangular numbers are numbers that can be arranged in a triangular pattern. Visualize each triangle as sitting inside the next. The n-th triangular number T_n is formed using an outer triangle whose sides have n dots:



The first 5 triangular numbers are 1, 3, 6, 10, 15. Observe that the n-th triangular number, which we will denote T_n, is

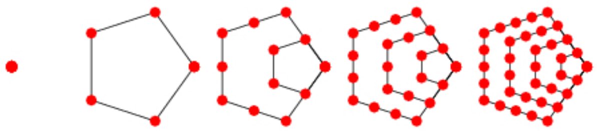
$$T_n = 1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}.$$

Square numbers are numbers that can be arranged in the shape of a square:



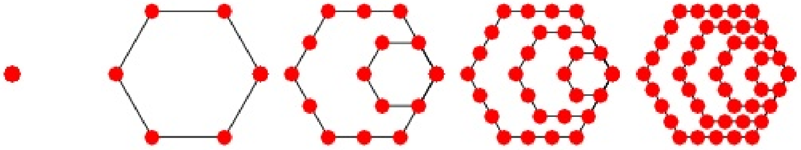
Visualize each square as sitting inside the next. The n-th square number is formed using an outer square whose sides have n dots. The n-th square number is $S_n = n^2$.

A **pentagonal number** is a number that can be arranged in the shape of a pentagon:



The first four pentagonal numbers are 1, 5, 12, 22. Visualize each pentagon as sitting inside the next one. The n-th pentagonal number is formed using an outer pentagon whose sides have n dots.

Hexagonal (and septagonal, r-gonal, etc.) numbers are defined similarly.



Problem Set

Note: Whenever possible, try to come up with *geometric* (rather than induction) proofs of the properties in the following problems.

1. Explain *geometrically* why $T_n = \dfrac{n(n+1)}{2}$ for all integers $n \geq 1$.
2. (a) Compute $T_1 + T_2$, $T_2 + T_3$, $T_3 + T_4$, and $T_4 + T_5$.

   (b) Computing more expressions of the form $T_n + T_{n+1}$ if necessary, make a conjecture about the sum of any two consecutive triangular numbers T_n and T_{n+1}, and prove that your conjecture is true for all integers $n \geq 1$.
3. (a) Compute $8T_1 + 1$, $8T_2 + 1$, $8T_3 + 1$, $8T_4 + 1$, and $8T_5 + 1$.

   (b) Computing more expressions of the form $8T_n + 1$ if necessary, make a conjecture about the expression $8T_n + 1$, and prove that your conjecture is correct for all integers $n \geq 1$.
4. Can you find any interesting equations that relate T_{a+b} To T_a and T_b? How about T_{ab}?
5. Show that if T is a triangular number, then $9T + 1$ is also a triangular number.
6. What are the possible digits that a triangular number can end in?
7. What are the possible digits that a square number can end in?
8. What are the possible last 2 digits that a square number can end in?
9. The **digital root** of a number is obtained in the following way. Start with your number, and sum its digits. Then sum the digits of the resulting number, and continue until only one digit remains. This is called the digital root. What are the possibilities for the digital root of a triangular number? What are the possibilities for the digital root of a square number?
10. How many four digit square numbers are composed of only even digits? What four digit square numbers can be reversed and become the square of another number?
11. (a) Compute 1^3, 1^3+2^3, $1^3+2^3+3^3$, $1^3+2^3+3^3+4^3$, and $1^3+2^3+3^3+4^3+5^3$.

    (b) Computing more expressions of the form

    $$1^3 + 2^3 + 3^3 + \cdots + n^3$$

    if necessary, make a conjecture about how the sum of the first n cubes is related to the n-th triangular number T_n. Prove that your conjecture is correct for all integers $n \geq 1$.
12. (a) Compute $3T_2 + T_1$, $3T_3 + T_2$, $3T_4 + T_3$, $3T_5 + T_4$, and $3T_6 + T_5$.

(b) Computing more expressions of the form $3T_n + T_{n-1}$ if necessary, make a conjecture about the expression $3T_n + T_{n-1}$, and prove that your conjecture is correct for all integers $n \geq 1$.

13. Can you find any triangular numbers whose square is also a triangular number?

14. Compile some data and try to make a conjecture about which numbers can be written as a sum of two triangular numbers. For example,

$$7 = 1 + 6 \text{ and } 25 = 10 + 15$$

are sums of two triangular numbers, while 19 cannot be written as the sum of two triangular numbers. Can you prove your conjecture?

15. There are 6 triangular numbers that can be expressed as the product of three consecutive integers. Can you find them?

16. Triangular numbers that can be expressed as a product of two primes are called **triangular semiprimes**. For example, 6 is a triangular semiprime because $6 = 2 \cdot 3$. Can you find other triangular semiprimes?

17. Are there 4 distinct triangular numbers in geometric progression?

18. Show that every even perfect number is triangular. Perfect numbers are numbers n with the property that the sum of the proper divisors of n (not including n) sum to n. For example, 6 is a perfect number because $1+2+3 = 6$. See Chapter 18 for more information on prefect numbers.

19. Show that every positive integer can be expressed as a sum of 3 or fewer triangular numbers.

20. Investigate the *minimum* number of squares needed to represent a given number. Do you see any patterns? For each number k, compare the minimum number of squares needed to represent k with the minimum number needed to represent k^2. What do you observe? (Note: it is known that every positive integer can be expressed as a sum of 4 or fewer square numbers.)

21. (a) What is the 5-th pentagonal number?

    (b) Find a general formula for the n-th pentagonal number P_n.

    (c) How do pentagonal numbers relate to triangular numbers? Find a number c such that the following is true: If P is a pentagonal number, then there is a triangular number T such that $P = cT$.

    (d) There are conjectured to be exactly 210 positive integers that cannot be expressed as the sum of 3 pentagonal numbers. Find 6 of them.

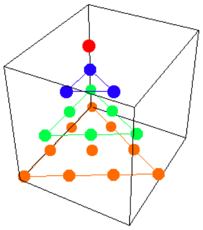
    (e) There are only 6 positive integers that cannot be expressed as the sum of 4 pentagonal numbers. Find them.

    (f) Show that every positive integer can be expressed as a sum of 5 or fewer pentagonal numbers.

22. (a) Find a general formula for the n-th hexagonal number.
    (b) Show that every hexagonal number is also a triangular number. Is every triangular number also a hexagonal number? If not, can you classify which ones are?
    (c) There are exactly 13 positive integers that cannot be expressed as a sum of 4 hexagonal numbers. Find 6 of them.
    (d) There are only 2 positive integers that cannot be expressed as a sum of 5 hexagonal numbers. Find them.
    (e) Show that every positive integer can be expressed as a sum of 6 hexagonal numbers.

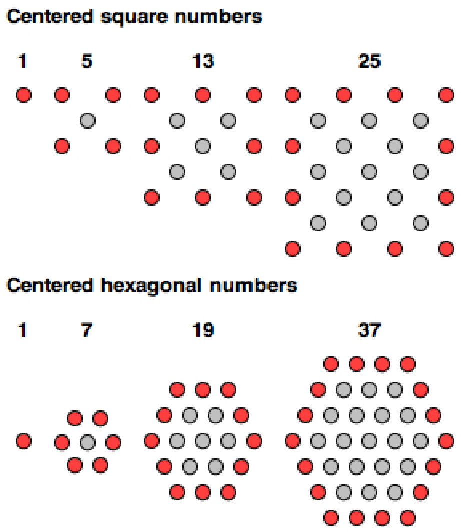
23. More generally, find a general formula for the n-th r-gonal number. Show that every positive integer can be expressed as a sum of r r-gonal numbers.

24. A **tetrahedral number** is a number corresponding to a configuration of points that form a pyramid with a triangular base:



    (a) What are the first 5 tetrahedral numbers?
    (b) Find a general formula for the n-th tetrahedral number. How does the n-th tetrahedral number relate to Pascal's triangle?
    (c) Can you classify which tetrahedral numbers are even and which are odd?
    (d) Are there any numbers that are both triangular and tetrahedral?
    (e) Are there any numbers that are both square and tetrahedral?
    (f) *Pollock's Conjecture* (1850) states that every number is the sum of at most 5 tetrahedral numbers; this conjecture has not yet been proven. It is also conjectured that there are exactly 241 numbers that cannot be written as the sum of 4 or fewer tetrahedral numbers. Can you find the first 5?
    (g) How would you define a square pyramidal number? A pentagonal pyramidal number? A hexagonal pyramidal number? Once you've defined a square pyramidal number, show that the sum of two consecutive tetrahedral numbers is a square pyramidal number. This is, of course, analogous to the 2-dimensional result (the sum of two consecutive triangular numbers is a square number).

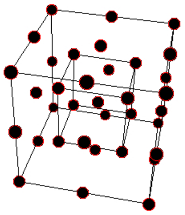
25. The **centered polygonal numbers** are numbers formed by a central dot, surrounded by polygonal numbers with a constant number of sides. Each side of a polygonal layer contains one dot more than a side in the previous layer.



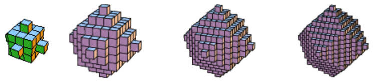
(a) Find the first 5 centered triangular, centered square, centered pentagonal, and centered hexagonal numbers.

(b) Find a general formula for the n-th centered k-gonal number. Can you explain your formula *geometrically*?

(c) How would you define a centered cube number? Can you find a general formula for the n-th centered cube number?



26. Investigate formulas for and properties of other geometric numbers. For example, a **rhombic dodecahedral number** is a number constructed as a centered cube with a square pyramid appended to each face.

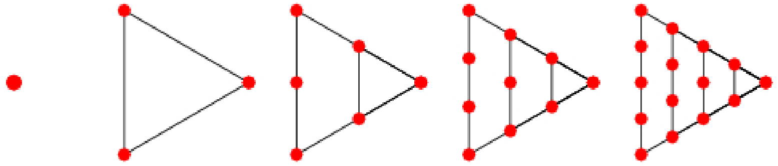


What is an octahedral number? How do octahedral numbers relate to pyramidal numbers? What is Pollock's conjecture for octahedral numbers?

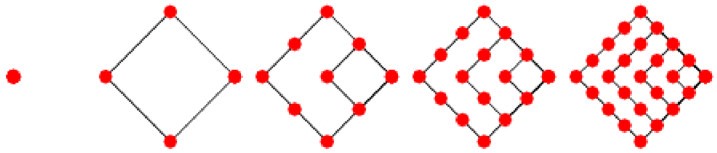
Chapter 27

Square-Triangular Numbers and Pell's Equation

Recall from Chapter 26 that triangular numbers are numbers of the form $T_m = \frac{m(m+1)}{2}$. Geometrically, they're numbers that can be arranged in the shape of a triangle:



The n-th triangular number is formed using an outer triangle whose sides have n dots. Similarly, *square* numbers are numbers that can be arranged in the shape of a square:



The n-th square number is formed using an outer square whose sides have n dots. The n-th square number is $S_n = n^2$.

Example 27.1 Make a list of the first 10 triangular and square numbers. Are there any numbers in both lists?

In this chapter, we'll develop a method for finding all *square-triangular numbers* (i.e. numbers which are both square and triangular numbers). One of the major questions we'll be interested in answering is whether or not there are infinitely many square-triangular numbers. Since triangular numbers are of the form

$$T_m = \frac{m(m+1)}{2}$$

and square numbers are of the form

$$S_n = n^2,$$

square-triangular numbers are integer solutions of the equation

$$n^2 = \frac{m(m+1)}{2}.$$

Next, multiply both sides by 8 and show that we can rewrite the previous equation as

$$8n^2 = 4m^2 + 4m = (2m+1)^2 - 1.$$

This suggests the substitution

$$x = 2m + 1 \text{ and } y = 2n.$$

Make this substitution, and rearrange to obtain the equation

$$x^2 - 2y^2 = 1.$$

Solutions to this equation produce square-triangular numbers with

$$m = \frac{x-1}{2} \text{ and } n = \frac{y}{2}.$$

In other words, if (x, y) is a solution of the equation $x^2 - 2y^2 = 1$, then $N = n^2 = \left(\frac{y}{2}\right)^2$ is a square-triangular number. Geometrically, the square has $y/2$ dots on a side and the triangle has $(x-1)/2$ dots on the bottom row.

Example 27.2 Show that $(x, y) = (3, 2)$ and $(x, y) = (17, 12)$ are both solutions of $x^2 - 2y^2 = 1$. Then find the corresponding values of (m, n) and the resulting square-triangular numbers. Can you find any other solutions (perhaps using a calculator or computer)?

To find all square-triangular numbers, we need to find all solutions of

$$x^2 - 2y^2 = 1.$$

Observe that we can factor this equation as

$$x^2 - 2y^2 = (x + y\sqrt{2})(x - y\sqrt{2}).$$

For example, we can write the solution $(x, y) = (3, 2)$ as

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

Next, observe what happens if we square both sides of this equation:

$$\begin{aligned}1 = 1^2 &= (3+2\sqrt{2})^2(3-2\sqrt{2})^2\\ &= (17+12\sqrt{2})(17-12\sqrt{2})\\ &= 17^2 - 2\cdot 12^2\end{aligned}$$

Thus, “squaring” the solution $(x, y) = (3, 2)$ produced the next solution $(x, y) = (17, 12)$!

Example 27.3 Cube the solution $(x, y) = (3, 2)$, and show that you obtain the solution $(x, y) = (99, 70)$. Which square-triangular number does this produce? What about taking the fourth power?

Example 27.4 What is the solution of Pell's equation corresponding to $(3+2\sqrt{2})^{16}$? What is the corresponding square-triangular number?

Theorem 27.1 There are infinitely many square-triangular numbers.

Proof. For every positive integer k,

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

By raising $(3+2\sqrt{2})$ to higher and higher powers, we continue to find more and more solutions to the equation $x^2 - 2y^2 = 1$, and each new solution gives us a new square-triangular number. (Note: the technique that we have used is interesting from a number-theoretic point of view. In attempting to solve a question about *integers*, we've used irrational numbers!)

Thus, there are infinitely square-triangular numbers, but it's natural to ask at this point whether or not our procedure actually produces all of them.

Theorem 27.2 Square-Triangular Number Theorem.

(a) Every solution (x_k, y_k) in positive integers to the equation

$$x^2 - 2y^2 = 1$$

is of the form

$$x_k + y_k\sqrt{2} = (3+2\sqrt{2})^k, \quad k = 1, 2, 3, \ldots.$$

(b) Every square-triangular number $n^2 = \frac{1}{2}m(m+1)$ is given by

$$m = \frac{x_k - 1}{2} \text{ and } n = \frac{y_k}{2}.$$

Proof. We've already checked (b). We just need to check that if (u, v) is *any* solution of $x^2 - 2y^2 = 1$, then it is of the form

$$u + v\sqrt{2} = (3 + 2\sqrt{2})^k$$

for some k. To do this, we'll use the method of descent. First, note that $u \geq 3$, and if $u = 3$, then $v = 2$, so there's nothing to check. Next, suppose that $u > 3$, and try to show that there must be another solution (s, t) in positive integers such that

$$u + v\sqrt{2} = (3 + 2\sqrt{2})(s + t\sqrt{2}) \text{ with } s < u.$$

If $(s, t) = (3, 2)$, then we're done (i.e. (u, v) is of the correct form). If not, then try to find another solution (q, r) such that

$$s + t\sqrt{2} = (3 + 2\sqrt{2})(q + r\sqrt{2}) \text{ with } q < s.$$

If we can do this, then we have

$$u + v\sqrt{2} = (3 + 2\sqrt{2})^2(q + r\sqrt{2}),$$

so if $(q, r) = (3, 2)$, then we're done. If not, we'll apply the procedure again. Observe that this process can't go on forever, since each time we get a new solution, the value of "x" is smaller (e.g. $q < s < u$. Since these values are all positive integers, they cannot get smaller forever, so the process must end in a finite number of steps. Thus, we eventually must reach $(3, 2)$ as a solution, so eventually we're able to write $u + v\sqrt{2}$ as a power of $3 + 2\sqrt{2}$.

Thus, it remains to show that if we start with a solution (u, v) with $u > 3$, then we can find a solution (s, t) with the property

$$u + v\sqrt{2} = (3 + 2\sqrt{2})(s + t\sqrt{2}) \text{ with } s < u.$$

To do this, multiply out the right-hand side to obtain

$$u + v\sqrt{2} = (3s + 4t) + (2s + 3t)\sqrt{2}.$$

Thus, we need to solve

$$u = 3s + 4t \text{ and } v = 2s + 3t.$$

Show that the solution is

$$s = 3u - 4v \text{ and } t = -2u + 3v$$

for s and t.

Now, there are three things left to check. We need to make sure that this (s, t) is really a solution of $x^2 - 2y^2 = 1$, that s and t are both positive, and that $s < u$. For the first, just check that $s^2 - 2t^2 = 1$ (remember that $u^2 - 2v^2 = 1$ since (u, v) is a solution). Once we know that s and t are both positive, we can check that $s < u$ as follows:

$$\begin{aligned}
s &= 3u - 4v \\
&= 3u - 4\left(\frac{1}{3}t + \frac{2}{3}u\right) \\
&= 3u - \frac{4}{3}t - \frac{8}{3}u \\
&= \frac{1}{3}u - \frac{4}{3}t
\end{aligned}$$

So it remains to make sure that s and t are both positive. First, we'll check that s is positive:

$$\begin{aligned}
u^2 &= 1 + 2v^2 > 2v^2 \\
u &> \sqrt{2}v \\
s &= 3u - 4v \\
&> 3\sqrt{2}v - 4v \\
&= (3\sqrt{2} - 4)v > 0
\end{aligned}$$

Finally, we'll check that t is positive:

$$\begin{aligned}
u &> 3 \\
u^2 &> 9 \\
9u^2 &> 9 + 8u^2 \\
9u^2 - 9 &> 8u^2 \\
u^2 - 1 &> \frac{8}{9}u^2 \\
2v^2 &> \frac{8}{9}u^2 \\
v &> \frac{2}{3}u \\
t &= -2u + 3v > -2u + 3\frac{2}{3}u = 0
\end{aligned}$$

This completes the descent proof.

More generally, any Diophantine equation of the form $x^2 - dy^2 = 1$, where d is a non-square positive integer is called a *Pell equation*. Pell's equation has an interesting history–its first recorded appearance is in the "Cattle problem of Archimedes" (287-212 BC), in a letter sent from Archimedes to Eratosthenes. In 1880, A. Amthor, a

German mathematician, showed that the total number of cattle had to be a number with 206,545 digits, beginning with 7766. Over the next 85 years, an additional 40 digits were found, but it was not until 1965 at the University of Waterloo that a complete solution was found–it took over 7.5 hours of computation on an IBM 7040 computer. However, they didn't print out the solution, and the problem was solved a second time using a Cray-1 computer in 1981.

So, we know that if we can find one solution of a Pell equation, then we can find infinitely many. But how do we find the smallest (i.e. fundamental solution)? To answer this question, we'll investigate the relationship between *continued fractions* and Pell equations.

Example 27.5 A **continued fraction** is an expression of the form

$$4+\frac{1}{2+\frac{1}{7+\frac{1}{3}}}.$$

This is called the **continued fraction expansion** for the fraction $\frac{210}{47}$. Note that in the continued fraction expansion, all of the denominators are equal to 1. A more compact notation for this continued fraction expansion is $[4; 2, 7, 3]$.

Example 27.6 Consider the decimal expansion of π:

$$\pi = 3.14159265358979323846264 33\ldots$$

Observe that we can write this as

$$\pi = 3 + \text{something},$$

where the "something" is a number between 0 and 1. Next, observe that we can rewrite this as:

$$\begin{aligned}
\pi &= 3 + 0.14159265358979323846264 33\ldots \\
&= 3 + \frac{1}{\frac{1}{0.14159265358979323846264 33\ldots}} \\
&= 3 + \frac{1}{7.0625133059310457693005 1\ldots} \\
&= 3 + \frac{1}{7 + 0.0625133059310457693005 1\ldots} \\
&= 3 + \frac{1}{7 + \text{a little bit more}}
\end{aligned}$$

The final equation above gives the fairly good approximation $\frac{22}{7}$ for π. Now, if we repeat this process, we obtain:

$$\begin{aligned}
0.06251330593104576930051\ldots &= \frac{1}{\frac{1}{0.06251330593104576930051\ldots}} \\
&= 15.996594406685719888923060 \\
&= 15 + 0.996594406685719888923060
\end{aligned}$$

Thus, we have the following representation of π:

$$\pi \quad = \quad 3 + \frac{1}{7 + \frac{1}{15 + 0.996594406685719888923060}}$$

The bottom level of this fraction is 15.996594406685719888923060, which is very close to 16. If we replace it with 16, we get a rational number that is very close to π:

$$3 + \frac{1}{7 + \frac{1}{16}} = \frac{355}{113} = 3.14159292035398230088495 57\ldots$$

The fraction $\dfrac{355}{113}$ agrees with π to six decimal places. Continue this process, at each stage flipping the decimal that is left over and then separating off the whole integer part, to obtain a four-layer fraction representation of π. Use your final representation to get a rational number approximation for π, and compare with the known decimal approximation of π to see how accurate your approximation is.
Using our more compact notation, we can express the continued fraction expansion of π as Using this notation, our continued fraction expansion of π can be written as

$$\pi = [3; 7, 15, 1, 292, 1, 1, 1, 2, 1, 3, 1, 14, 2, 1, 1, 2, \ldots].$$

Definition 27.1 The **n-th convergent to α** is the rational number

$$\frac{p_n}{q_n} = [a_0; a_1, a_2, \ldots, a_n] = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \cdots + \frac{1}{a_n}}}}$$

obtained by using the terms up to a_n in the continued fraction expansion of α.

Example 27.7 For the continued fraction expansion of

$$\pi = [3; 7, 15, 1, 292, 1, 1, 1, 2, 1, 3, 1, 14, 2, 1, 1, 2, \ldots],$$

the first few convergents are:

$$\begin{aligned}
\frac{p_0}{q_0} &= 3 \\
\frac{p_1}{q_1} &= 3 + \frac{1}{7} = \frac{22}{7} = 3.142857143 \\
\frac{p_2}{q_2} &= 1 + \frac{1}{7 + \frac{1}{15}} = \frac{333}{106} = 3.141509434
\end{aligned}$$

Consider again the Pell equation with $d = 2$:

$$x^2 - 2y^2 = 1.$$

Start by finding the continued fraction expansion of $\sqrt{2}$:

$$\sqrt{2} = [1; 2, 2, 2, 2, 2, 2, 2, \ldots].$$

The first few convergents are:

$$\begin{aligned} \frac{p_0}{q_0} &= 1 \\ \frac{p_1}{q_1} &= 1 + \frac{1}{2} = \frac{3}{2} \\ \frac{p_2}{q_2} &= 1 + \frac{1}{2 + \frac{1}{2}} = \frac{7}{5} \end{aligned}$$

What do you notice? The fundamental solution of $x^2 = 2y^2 = 1$ is $(3, 2)$, which is one of our convergents!

Theorem 27.3 Continued Fractions and Fundamental Solutions of Pell Equations. Consider the Pell equation $x^2 - dy^2 = 1$. Let $\frac{h_i}{k_i}$, $i = 0, 1, \ldots$ denote the sequence of convergents to the continued fraction expansion for $\sqrt{d}$. Then the fundamental solution (x_1, y_1) of the Pell equation satisfies $x_1 = h_i$ and $y_1 = k_i$ for some i.

Example 27.8 Consider the Pell equation $x^2 - 3y^2 = 1$. Find the continued fraction expansion of $\sqrt{3} = 1.7320508075688...$, and use it to find the fundamental solution of the Pell equation.

$$\begin{aligned} \sqrt{3} &= [1; 1, 2, 1, 2, 1, 2, 1, 2, \ldots] \\ \frac{p_0}{q_0} &= 1 \\ \frac{p_1}{q_1} &= 1 + \frac{1}{1} = \frac{2}{1} \\ \frac{p_2}{q_2} &= 1 + \frac{1}{1 + \frac{1}{2}} = \frac{5}{3} = 1.6666... \end{aligned}$$

Example 27.9 Consider the Pell equation $x^2 - 7y^2 = 1$. Find the continued fraction expansion of $\sqrt{7} = 2.6457513110645907...$, and use it to find the fundamental solution of the Pell equation.

$$\begin{aligned}
\sqrt{7} &= [2;1,1,1,4,1,1,1,4,1,1,1,4,\ldots] \\
\frac{p_0}{q_0} &= 2 \\
\frac{p_1}{q_1} &= 2+\frac{1}{1}=\frac{3}{1} \\
\frac{p_2}{q_2} &= 2+\frac{1}{1+\frac{1}{1}}=\frac{5}{2}=2.5 \\
\frac{p_3}{q_3} &= 2+\frac{1}{1+\frac{1}{1+\frac{1}{1}}}=\frac{8}{3}=2.6666...
\end{aligned}$$

Problem Set

1. Use the continued fraction technique to find the smallest solution of $x^2 - 61y^2 = 1$.

2. Use the continued fraction technique to find the smallest solution of $x^2 - 63y^2 = 1$.

3. How many positive integer solutions are there to the equation $x^2 - y^2 = 1$?

4. Find four solutions in positive integers to the equation
$$x^2 - 5y^2 = 1.$$

5. Let (x_k, y_k) be the solutions to $x^2 - 2y^2 = 1$, as described in Theorem 27.2.

   (a) Find a, b, c, d such that
   $$x_{k+1} = ax_k + by_k \text{ and } y_{k+1} = cx_k + dy_k.$$

   (b) Find e, f, g, h such that if (m, n) satisfies $n^2 = \dfrac{m(m+1)}{2}$, then
   $$(1 + em + fn, 1 + gm + hn)$$
   also produces a square-triangular number.

   (c) If L is a square-triangular number, show that
   $$1 + 17L + 6\sqrt{L + 8L^2}$$
   is the next largest square-triangular number.

6. Let ST_n denote the n-th square-triangular number. Show that
$$ST_n = 34ST_{n-1} - ST_{n-2} + 2.$$

7. What can you say about the size of the n-th square-triangular number as a function of n?

8. Study the ratio $r_n = x_n/y_n$ as n becomes large. Can you explain your observation?

9. Recall from Chapter 26 that the general formula for the n-th pentagonal number is $P_n = \frac{n(3n-1)}{2}$.

   (a) Are there any pentagonal numbers (other than 1) that are also triangular numbers? Are there infinitely many? What is the Diophantine equation that produces pentagonal-triangular numbers?

(b) Are there any pentagonal numbers (other than 1) that are also square numbers? Are there infinitely many? What is the Diophantine equation that produces pentagonal-square numbers?

(c) Are there any numbers (other than 1) that are simultaneously triangular, square, and pentagonal numbers? Are there infinitely many? What is the Diophantine equation that produces pentagonal-square-triangular numbers?

(d) Are there any numbers (other than 1) that are both pentagonal and hexagonal? Are there infinitely many? What is the Diophantine equation that produces pentagonal-hexagonal numbers?

10. **Solutions of Pell Equations.**

(a) Suppose that (x_1, y_1) is a solution of the Pell equation $x^2 - dy^2 = 1$. Square both sides of

$$1 = x_1^2 - dy_1^2 = (x_1 + y_1\sqrt{d})(x_1 - y_1\sqrt{d})$$

to show that $(x_1^2 + y_1^2 d, 2x_1y_1)$ is also a solution. Thus, if we find one solution of $x^2 - dy^2 = 1$, then we can find infinitely many solutions.

(b) The smallest solution of $x^2 - 15y^2 = 1$ is $(4, 1)$. Find two more solutions of this Pell equation.

(c) The smallest solution of $x^2 - 22y^2 = 1$ is $(197, 42)$. Find a solution of this Pell equation whose x is larger than 10^6.

(d) Prove, using the technique that we used for the Pell equation $x^2 - 2y^2 = 1$, that every solution of the Pell equation $x^2 - 11y^2 = 1$ is of the form

$$x_k + y_k\sqrt{11} = (10 + 3\sqrt{11})^k, \quad k = 1, 2, 3, \ldots.$$

Note: Although we know that once we find one solution of Pell's equation we can find infinitely many solutions, it can often be difficult to find the smallest solution. In addition, there's currently no known pattern for the size of the smallest solution to $x^2 - dy^2 = 1$. For example, the smallest solution of $x^2 - 61y^2 = 1$ is $(1766319049, 226153980)$, while the smallest solution of $x^2 - 63y^2 = 1$ is $(8, 1)$, and the smallest solution of $x^2 - 65y^2 = 1$ is $(129, 16)$. The smallest solution of $x^2 - 73y^2 = 1$ is $(2281249, 267000)$, while the smallest solution of $x^2 - 75y^2 = 1$ is $(26, 3)$.

11. Investigate the Archimedes cattle problem, which Archimedes (287-212 BC) communicated to students at Alexandria in a letter to Eratosthenes. Can you determine the size of the 8 unknowns, and thus the size of the herd?

If thou art diligent and wise, O stranger, compute the number of cattle of the Sun, who once upon a time grazed on the fields of the Thrinacian isle of Sicily, divided into four herds of different colours, one milk white, another a glossy black, a third yellow and the last dappled. In each herd were bulls, mighty in number according to these proportions: Understand, stranger, that the white bulls were equal to a half and a third of the black together with the whole of the yellow, while the black were equal to the fourth part of the dappled and a fifth, together with, once more, the whole of the yellow. Observe further that the remaining bulls, the dappled, were equal to a sixth part of the white and a seventh, together with all of the yellow. These were the proportions of the cows: The white were precisely equal to the third part and a fourth of the whole herd of the black; while the black were equal to the fourth part once more of the dappled and with it a fifth part, when all, including the bulls, went to pasture together. Now the dappled in four parts were equal in number to a fifth part and a sixth of the yellow herd. Finally the yellow were in number equal to a sixth part and a seventh of the white herd. If thou canst accurately tell, O stranger, the number of cattle of the Sun, giving separately the number of well-fed bulls and again the number of females according to each colour, thou wouldst not be called unskilled or ignorant of numbers, but not yet shalt thou be numbered among the wise.

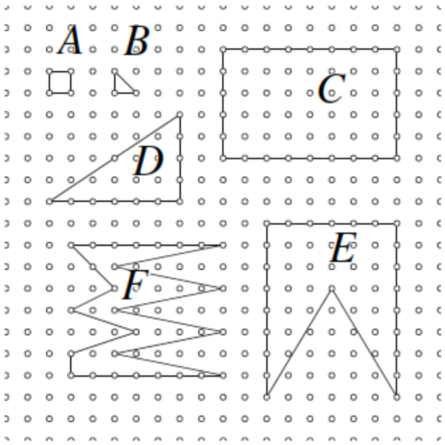
But come, understand also all these conditions regarding the cattle of the Sun. When the white bulls mingled their number with the black, they stood firm, equal in depth and breadth, and the plains of Thrinacia, stretching far in all ways, were filled with their multitude. Again, when the yellow and the dappled bulls were gathered into one herd they stood in such a manner that their number, beginning from one, grew slowly greater till it completed a triangular figure, there being no bulls of other colours in their midst nor none of them lacking. If thou art able, O stranger, to find out all these things and gather them together in your mind, giving all the relations, thou shalt depart crowned with glory and knowing that thou hast been adjudged perfect in this species of wisdom.

Chapter 28

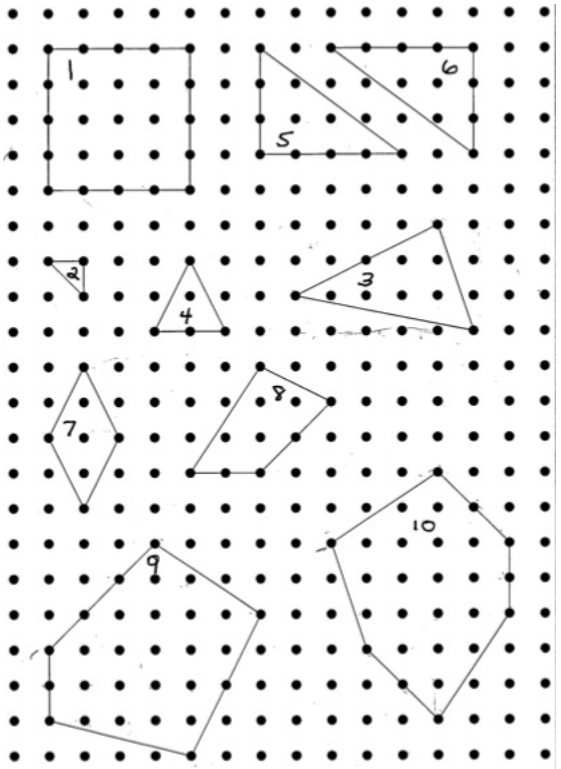
Pick's Theorem

Pick's Theorem is a beautiful result that establishes a connection between the area of a lattice polygon and the number of lattice points inside and on the boundary of the polygon. The polygon may be convex or concave–the only requirement for Pick's Theorem is that the edges of the polygon do not intersect. *Lattice points* are points with integer coordinates in the x, y-plane. A *lattice line segment* is a line segment that has 2 distinct lattice points as endpoints, and a *lattice polygon* is a polygon whose sides are lattice line segments–this just means that the *vertices* of the polygon are lattice points.

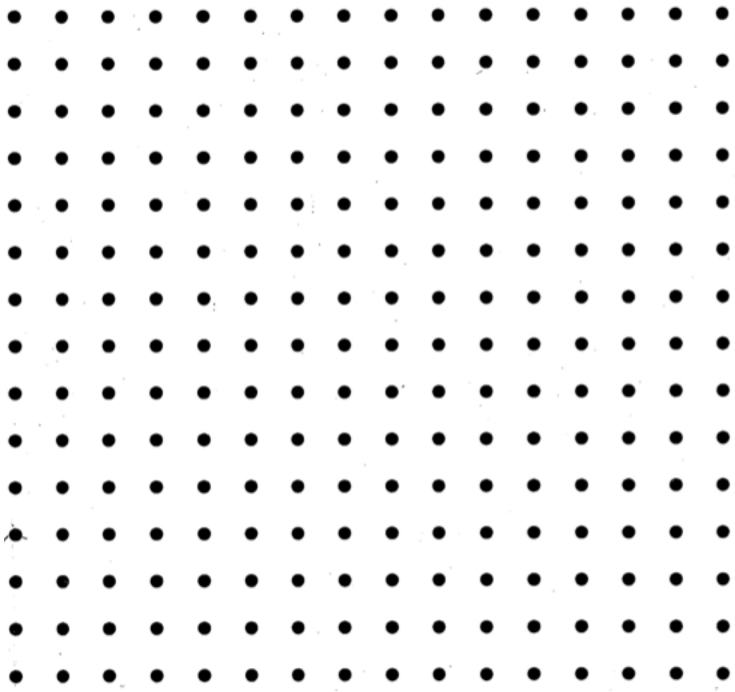
Example 28.1 Find the area of each of the following lattice polygons. Make a table that contains the following information for each polygon: the area of the polygon, the number of lattice points inside the polygon, and the number of lattice points on the boundary of the polygon. Can you make any observations or conjectures?



Example 28.2 Repeat the previous problem for each of the following polygons. Add the information from these polygons to the table that you created in the previous problem.



Example 28.3 Construct at least 5 different polygons that contain 4 boundary lattice points and 6 interior lattice points. Keep in mind that the polygons do not need to be convex! What is the area of each polygon?



Example 28.4 Let P be the triangle with vertices $(0, 0)$, $(3, 1)$, and $(1, 4)$. Find the area of P, the number of lattice points inside the polygon, and the number of lattice points on the boundary of the polygon.

Based on your work on these examples (do more examples if necessary), you should be able to make a conjecture about the statement of Pick's Theorem.

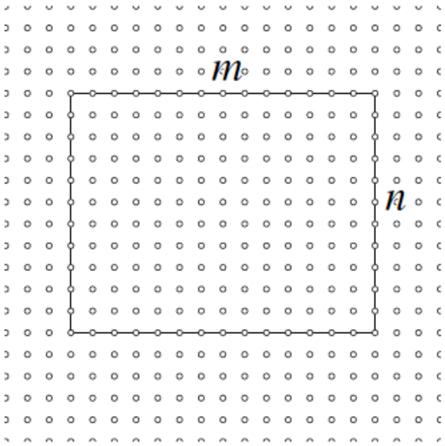
Theorem 28.1 Pick's Theorem. Let P be a simple lattice polygon, and let $A(P)$ denote the area of P. Let B denote the number of lattice points on the boundary of P, and let I denote the number of lattice points in the interior of P. Then

$$A(P) =$$

Problem Set

1. **A Proof of Pick's Theorem using Induction.**
(Reference: `http://www.geometer.org/mathcircles/pick.pdf`).
In this series of exercises, you will prove Pick's Theorem.

(a) Consider an $m \times n$ lattice-aligned rectangle:



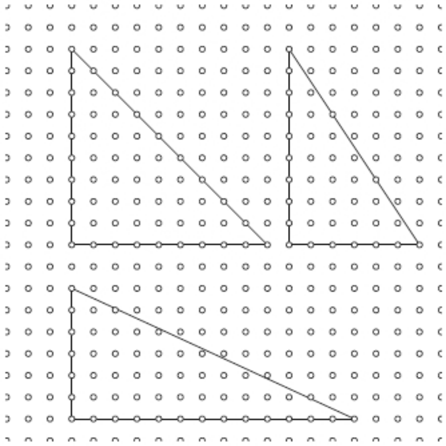
Show that for such a rectangle,

$$I = (m-1)(n-1) \text{ and } B = 2m + 2n.$$

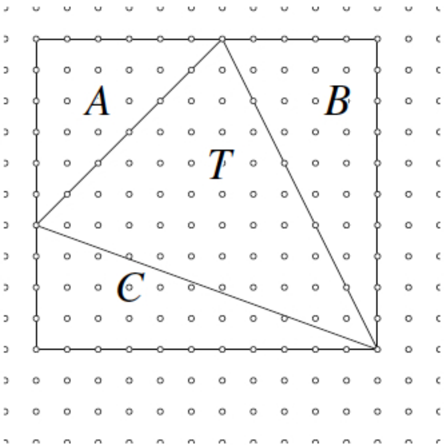
Conclude that

$$A = I + \frac{B}{2} - 1.$$

(b) Next, find I and B for a lattice-aligned right triangle with legs m and n. Prove that Pick's Theorem holds for such a triangle.



(c) The next step is to show that Pick's Theorem holds for arbitrary triangles. If T is an arbitrary triangle, draw right triangles A, B, C to form a rectangle R, as shown below.



Suppose that triangle A has I_a interior points and B_a boundary points. Use similar notation for triangles B and C. Let I_r and B_r denote the number of interior and boundary points of the rectangle, respectively. We already know that Pick's Theorem holds for A, B, C, R, so we know that

$$\begin{aligned} A(A) &= I_a + \frac{B_a}{2} - 1 \\ A(B) &= I_b + \frac{B_b}{2} - 1 \\ A(C) &= I_c + \frac{B_c}{2} - 1 \\ A(R) &= I_r + \frac{B_r}{2} - 1 \end{aligned}$$

We want to show that

$$A(T) = I_t + \frac{B_t}{2} - 1.$$

We know that

$$A(T) = A(R) - A(A) - A(B) - A(C).$$

Explain why

$$B_r = B_a + B_b + B_c - B_t$$

and

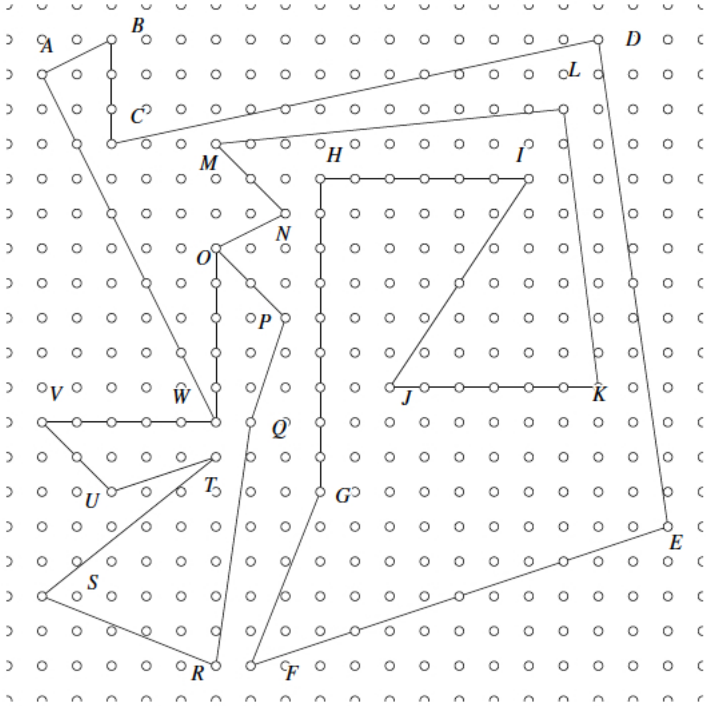
$$I_r = I_a + I_b + I_c + I_t + (B_a + B_b + B_c - B_r) - 3.$$

Use these equations to show that

$$A(T) = I_t + \frac{B_t}{2} - 1.$$

(d) So far, we've shown that Pick's Theorem is true for every polygon with 3 sides. To complete the proof that Pick's Theorem is true for any polygon, we'll use induction on the number of sides of the polygon. The base case is $n = 3$ sides, and we've already shown that Pick's Theorem holds for $n = 3$. For the inductive step, assume that Pick's Theorem holds for $n = 3, 4, \dots, k - 1$ sides. We must now prove that Pick's Theorem holds for $n = k$ sides to complete the induction.

Suppose that P is a polygon with k sides ($k > 3$). Show that P must have an *interior diagonal* that will split P into 2 smaller polygons. Here's an example. OW is the interior diagonal for this example.



Once we have shown that we can always split a polygon P with k sides into 2 smaller polygons P_1 and P_2 (each with fewer than k sides), the final step is to show that if 2 polygons satisfy Pick's Theorem, then the polygon formed by *attaching* the 2 will also satisfy Pick's Theorem. Since the smaller polygons satisfy Pick's Theorem by the inductive hypothesis, we have

$$A(P) = A(P_1) + A(P_2) = I_1 + \frac{B_1}{2} - 1 + I_2 + \frac{B_2}{2} - 1.$$

Finally, find a relationship between I and I_1, I_2 and between B and B_1, B_2 to conclude that

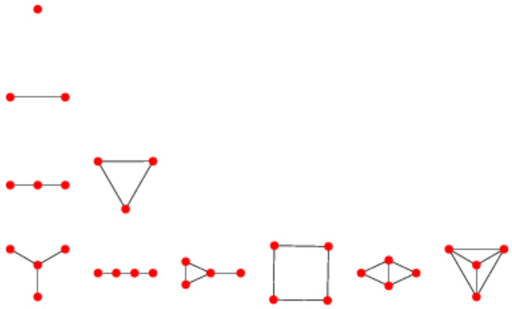
$$A(P) = I + \frac{B}{2} - 1.$$

2. **A Proof of Pick's Theorem using Euler's Formula.** A **graph** $G = (V, E)$ consists of a V, a nonempty, finite set of *vertices*, and E, a finite set of unordered

pairs of distinct elements of V called *edges*. If $\{u, v\}$ is an edge e of G, the edge e is said to connect u and v, and the vertices u and v are the *endpoints of the edge* e. Some examples of graphs are shown below. These graphs are both *planar* (can be drawn in such a way that no 2 edges cross) and connected (there is a path between every pair of distinct vertices of G). Euler's Formula states that if G is a connected, planar graph with n vertices, e edges, and f regions, then

$$v - e + f = 2.$$

(A planar graph splits the plane into *regions*, including one unbounded region "outside" the graph. For example, the graph on the far right in the fourth row below contains 4 regions.)



Can you prove this result?

(a) To prove Pick's Theorem from Euler's Formula, start with a simple lattice polygon P, and show that you can always dissect the polygon into *primitive lattice triangles*. A *primitive lattice triangle* is a triangle that has no lattice points in its interior, and no lattice points other than vertices on its sides.

(b) Next, show that the area of a primitive lattice triangle is equal to $\frac{1}{2}$. (Of course, you can't use Pick's Theorem since that's what we're trying to prove! You must use geometry to prove this result.)

(c) Once you've proved these results, it's relatively easy to obtain Pick's Theorem. Begin by observing that the vertices of the graph of P are the lattice points in the interior and on the sides of P, and the edges of the graph P are the sides of P and of the primitive triangles in the dissection of P. The f regions of the graph of P are the $f - 1$ primitive triangles and the complement of P in the plane. Since each primitive triangle has area 1/2, we have

$$A(P) = \frac{1}{2}f - 1.$$

Let e_i denote the number of interior edges of primitive triangles, and let e_s denote the number of edges of primitive triangles on the sides of P. Explain why

$$3(f - 1) = 2e_i + e_s = 2e - e_s.$$

Use Euler's Formula to rewrite this equation as

$$f - 1 = 2(v - 2) - e_s + 2.$$

Finally, use

$$A(P) = \frac{1}{2}(f - 1)$$

and

$$v = B(P) + I(P)$$

to obtain Pick's Theorem.

3. Among all of the lattice points on a lattice line L through the origin $(0, 0)$, there are exactly 2 that have minimum positive distance from the origin. Such lattice points are called *visible lattice points*. Show that a lattice point (a, b) is visible if and only if a and b are relatively prime.

4. Show that if (a, b) is a visible lattice point, then the lattice points on the line through (a, b) are all of the form $t(a, b)$, where t is an integer.

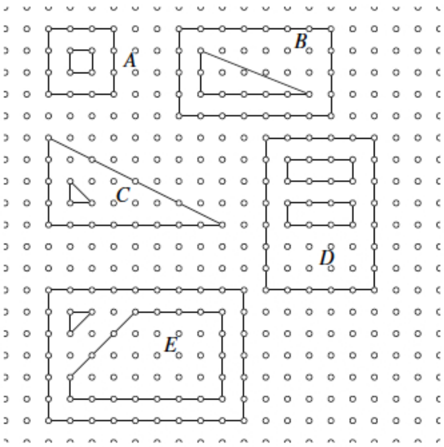
5. Consider the lattice line segment from $(0, 0)$ to the point (a, b), where a and b are any nonnegative integers. How many lattice points are there between $(0, 0)$ and (a, b) (excluding the endpoints)?

6. Let P be a lattice n-gon, with vertices $p_1 = (a_1, b_1),\ p_2 = (a_2, b_2), \ldots, p_n = (a_n, b_n)$. Let
$$d_i = \gcd(a_{i+1} - a_i, b_{i+1} - b_i).$$
Show that the number of lattice points on the boundary of P is
$$B(P) = \sum_{i=1}^{n} d_i.$$

7. Let L be a line in the plane, and suppose that the slope of L is irrational. Show that there is at most one lattice point on L. Give an example of a line with irrational slope containing one lattice point. Give an example of a line with irrational slope containing no lattice points.

8. Let L be a line with rational slope in the plane. Show that if there is a lattice point on L, then the y-intercept of L is rational. Show that if there is one lattice point on L, then there are infinitely many lattice points on L. Give an example of 2 lines with rational slope, one containing no lattice points, and the other containing infinitely many.

9. **Polygons with Holes.** In the following figure, there are 5 examples of polygons with holes. Polygons A, B, C have one hole, and polygons D and E have 2 holes. Find the area of each of these polygons. Make a table that contains the following information for each polygon: I, B, area, number of holes. Doing more examples if necessary, modify Pick's Theorem to derive a formula that works for polygons with holes. Then derive a proof of your conjecture.



10. Find the equation of the line connecting 2 points $A(n, 0)$ and $B(0, n)$, and show that this line contains all points of the form $(i, n-i)$, where i is an integer. There are $n-1$ such points between A and B. Connect each one of them with the origin $O(0, 0)$. The lines divide $\triangle OAB$ into n small triangles. Show that the 2 triangles next to the axes (i.e. the triangle adjacent to the x-axis and the triangle adjacent to the y-axis) contain no lattice points in their interior. Next, prove that if n is prime, then each of the remaining triangles contains exactly the same number of lattice points.

11. An $n \times n$ square is randomly tossed onto the plane. Prove that it may never contain more than $(n+1)^2$ lattice points.

12. Is it possible to construct an equilateral lattice triangle? A lattice square? A regular lattice hexagon? For which n is it possible to construct a regular lattice n-gon (i.e. a convex polygon that is equilateral and equiangular)?

13. For which positive integers n is it possible to construct a lattice square with area n?

14. For each integer $n > 2$, construct a lattice triangle with $I(T) = 0$ and $B(T) = n$.

15. If T is a lattice triangle with $I(T) = 1$, show that $B(T)$ must be equal to 3, 4, 6, 8, or 9. For each of these possible values, construct an example of such a lattice triangle.

16. This problem is an introduction to how Pick's Theorem generalizes in higher dimensions. First, we'll rewrite Pick's Theorem as follows. Let P be a lattice polygon, and let $L(P)$ denote the total number of lattice points in the interior and on the sides of P, so

$$L(P) = B(P) + I(P).$$

Then Pick's Theorem can be restated as follows:

$$L(P) = A(P) + \frac{1}{2}B(P) + 1.$$

The generalization of Pick's Theorem that we'll prove in this exercise describes how $L(P)$ changes as the polygon undergoes dilation by a positive integer. For each positive integer n, we define the lattice polygon nP as

$$nP = \{nx \mid x \in P\}.$$

Prove that

$$L(nP) = A(P)n^2 + \frac{1}{2}B(P)n + 1.$$

17. Let M be a bounded set in the plane with area greater than 1. Show that M must contain two distinct points (x_1, y_1) and (x_2, y_2) such that the point $(x_2 - x_1, y_2 - y_1)$ is an integer point (not necessarily in M).

18. Use the previous result to show that if S is a bounded, convex region in the plane that is symmetric about the origin and has area greater than 4, then S must contain an integer point other than $(0, 0)$.

19. Construct an example of a circle with exactly n lattice points in its interior (for $n = 1, 2, \ldots$).

20. Let $C(\sqrt{n})$ denote the circle with center $(0, 0)$ and radius $\sqrt{n}$.

    (a) Find the number of lattice points on the boundary of $C(\sqrt{18})$, $C(\sqrt{19})$, $C(\sqrt{20})$, and $C(\sqrt{21})$.

    (b) Find the number of lattice points in the interior and on the boundary of the circles $C(\sqrt{5})$, $C(\sqrt{7})$, and $C(\sqrt{10})$.

    (c) Can you find a general formula (or a rule for determining a formula, or any observations that might lead to a rule) for the number of lattice points on the boundary of $C(\sqrt{n})$?

    (d) ($\star$) Let $L(n)$ be the number of lattice points in the interior and on the boundary of the circle $C(\sqrt{n})$. Show that

$$\lim_{n\to\infty} \frac{L(n)}{n} = \pi.$$

21. ($\star$) Use the previous result to show that

$$\frac{\pi}{4} = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \cdots .$$

Hint:

$$L(n) = 1 + 4 \sum_{0<m\leq n} (d_1(m) - d_3(m)),$$

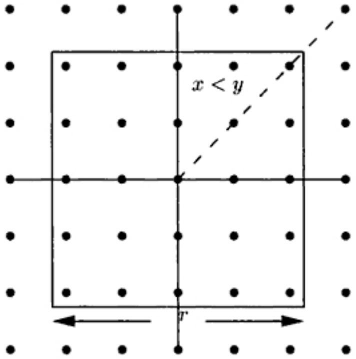
where $d_1(k)$ denotes the number of divisors of k congruent to $1 \mod 4$, and $d_3(k)$ denotes the number of divisors of k congruent to $3 \mod 4$.

22. ($\star$) Consider the square region $S(t)$ in the plane defined by the inequalities

$$|x| \leq t \text{ and } |y| \leq t,$$

where t is a positive real number. Let $N(t)$ denote the number of lattice points in this square, and let $V(t)$ denote the number of lattice points in the square that are *visible* from the origin. (Among all the lattice points on a lattice line L through th origin, there are exactly 2 that have minimum positive distance to the origin. Such lattice points are called *visible*. It may be useful to prove that a lattice point (a, b) is visible if and only if a and b are relatively prime.) Show that

$$\lim_{t\to\infty} \frac{V(t)}{N(t)} = \frac{6}{\pi^2}.$$



23. Do some research on Ehrhart's Theorem and the extension of Pick's Theorem to higher dimensions.

Chapter 29

Farey Sequences and Ford Circles

Definition 29.1 Farey Sequence. The **Farey sequence of order** n, denoted F_n is the sequence of completely reduced fractions between 0 and 1 which, in lowest terms, have denominators less than or equal to n, arranged in order of increasing size.

Example 29.1

$$\begin{aligned}
F_1 &= \{0/1, 1/1\} \\
F_2 &= \{0/1, 1/2, 1/1\} \\
F_3 &= \{0/1, 1/3, 1/2, 2/3, 1/1\} \\
F_4 &= \{0/1, 1/4, 1/3, 1/2, 2/3, 3/4, 1/1\} \\
F_5 &= \{0/1, 1/5, 1/4, 1/3, 2/5, 1/2, 3/5, 2/3, 3/4, 4/5, 1/1\} \\
F_6 &= \{0/1, 1/6, 1/5, 1/4, 1/3, 2/5, 1/2, 3/5, 2/3, 3/4, 4/5, 5/6, 1/1\} \\
F_7 &= \{0/1, 1/7, 1/6, 1/5, 1/4, 2/7, 1/3, 2/5, 3/7, 1/2, 4/7, 3/5, 2/3, 5/7, 3/4, 4/5, 5/6, 6/7, 1/1\}
\end{aligned}$$

Properties of Farey Sequences.

1. F_n contains F_k for all $k \leq n$.

2. F_n is equal to F_{n-1} plus an additional fraction for each number that is less than n and coprime to n. For example, F_6 consists of F_5 together with 1/6 and 5/6.

3. Let $|F_n|$ denote the number of fractions in F_n. For $n > 1$, $|F_n|$ is odd and the middle term of F_n is equal to 1/2.

4. $|F_n| = |F_{n-1}| + \phi(n)$

5. Since $|F_1| = 2$, we obtain

$$|F_n| = 1 + \sum_{k=1}^{n} \phi(k),$$

where $\phi(k)$ is Euler's totient function ($\phi(k)$ is equal to the number of positive integers less than or equal to k that are relatively prime to k).

6. **The mediant property.** Unfortunately, addition of fractions is not as easy as we would like it to be. For example,
$$\frac{1}{5}+\frac{1}{3}\neq\frac{1+1}{5+3}=\frac{1}{4}.$$
But, looking at the Farey sequences F_4 and F_5, how does 1/4 relate to 1/5 and 1/3? Can you find other Farey sequences in which you observe this phenomena? In particular, choose 3 consecutive terms of F_n, say $p_1/q_1, p_2/q_2, p_3/q_3$. Compute
$$\frac{p_1+p_3}{q_1+q_3}.$$
What do you observe?

7. **The mediant property and how to compute F_n.** How do we go from the $(n-1)$-st row to the n-th row?

Lemma 29.1 If $0<\frac{a}{b}<\frac{c}{d}<1$, then
$$\frac{a}{b}<\frac{a+c}{b+d}<\frac{c}{d}.$$

Proof.

$$\begin{aligned}\frac{a}{b} &< \frac{c}{d}\\ ad &< bc\\ ad+ab &< bc+ab\\ a(b+d) &< b(a+c)\\ \frac{a}{b} &< \frac{a+c}{b+d}\end{aligned}$$

Similarly,

$$\begin{aligned}\frac{a}{b} &< \frac{c}{d}\\ ad &< bc\\ ad+cd &< bc+cd\\ d(a+c) &< c(b+d)\\ \frac{a+c}{b+d} &< \frac{c}{d}\end{aligned}$$

This completes the proof of the Lemma, and we thus have the following algorithm for computing F_n:

Algorithm 29.1 How to Compute F_n.

(a) Copy F_{n-1} in order.

(b) Insert the **mediant fraction** $\dfrac{a+c}{b+d}$ between $\dfrac{a}{b}$ and $\dfrac{c}{d}$ if $b+d \leq n$. (If $b+d > n$, the mediant $\dfrac{a+c}{b+d}$ will appear in a later sequence).

Use this algorithm to find F_4 from F_3. Then find F_5. Check your results with the sequences given at the beginning of this chapter.

8. Suppose that p_1/q_1 and p_2/q_2 are two successive terms of F_n. Prove that $p_2q_1 - p_1q_2 = 1$. Note that it is equivalent to prove that if p_1/q_1 and p_2/q_2 are two successive terms of F_n with p_1/q_1 less than p_2/q_2, then

$$\frac{p_2}{q_2} - \frac{p_1}{q_1} = \frac{1}{q_1q_2}.$$

Note: there's a beautiful proof of this result using Pick's Theorem!

Proof. We'll use induction on n and the mediant property to prove this result. First, we need to look at the base case, $n = 1$. We have:

$$\begin{aligned} F_1 &= \left\{\frac{0}{1}, \frac{1}{1}\right\} \\ 1 \cdot 0 - 0 \cdot 1 &= 1 \end{aligned}$$

Thus, we have verified the best case. For the inductive hypothesis, we'll suppose that the statement is true for $n = k$, and we'll consider $n = k + 1$. This means that in the Farey sequence F_k, we have

$$F_k = \left\{\ldots, \frac{p_1}{q_1}, \frac{p_2}{q_2}, \ldots\right\}$$

and

$$p_2q_1 - p_1q_2 = 1.$$

Now, recall how we obtain F_{k+1} from F_k. We first copy F_k in order. Then, we insert the mediant fraction $\dfrac{a+c}{b+d}$ between $\dfrac{a}{b}$ and $\dfrac{c}{d}$ if $b+d \leq k+1$. If $b+d > k+1$, the mediant $\dfrac{a+c}{b+d}$ will appear in a later sequence. So, let's look at the mediant fraction

$$\frac{p_1+p_2}{q_1+q_2}.$$

If $q_1 + q_2 \leq k+1$, then

$$F_{k+1} = \left\{ \dots, \frac{p_1}{q_1}, \frac{p_1+p_2}{q_1+q_2}, \frac{p_2}{q_2}, \dots \right\}.$$

Then

$$\begin{aligned} (p_1+p_2)q_1 - p_1(q_1+q_2) &= p_2q_1 - p_1q_2 \\ &= 1 \\ p_2(q_1+q_2) - q_2(p_1+p_2) &= p_2q_1 - p_1q_2 \\ &= 1 \end{aligned}$$

On the other hand, if $q_1 + q_2 > k+1$, then

$$F_{k+1} = \left\{ \dots, \frac{p_1}{q_1}, \frac{p_2}{q_2}, \dots \right\},$$

so it's clear from the inductive hypothesis that the property holds. This completes the induction proof.

9. If p_1/q_1, p_2/q_2, and p_3/q_3 are three successive terms of F_n, then

$$\frac{p_2}{q_2} = \frac{p_1+p_3}{q_1+q_3}.$$

Proof.

$$\begin{aligned} p_2q_1 - p_1q_2 &= 1 \\ p_3q_2 - p_2q_3 &= 1 \\ p_2q_1 - p_1q_2 &= p_3q_2 - p_2q_3 \\ p_2q_1 + p_2q_3 &= p_1q_2 + p_3q_2 \\ \frac{p_2}{q_2} &= \frac{p_1+p_3}{q_1+q_3} \end{aligned}$$

Next, we'll investigate the remarkable connection between Farey sequences and Ford circles.

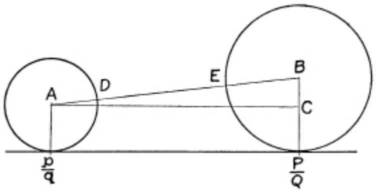
Definition 29.2 Ford Circle. For every rational number p/q in lowest terms, the **Ford circle** $C(p,q)$ is the circle with center $(\frac{p}{q}, \frac{1}{2q^2})$ and radius $\frac{1}{2q^2}$. This means that $C(p,q)$ is the circle tangent to the x-axis at $x = p/q$ with radius $\frac{1}{2q^2}$. Observe that every small interval of the x-axis contains points of tangency of infinitely many Ford circles.

Example 29.2 Sketch $C(0,1)$, $C(1,1)$, $C(1,2)$, $C(1,3)$, $C(2,3)$. Several Ford circles are illustrated in Figure 29.1.

Example 29.3 Consider three adjacent terms of F_n. What do you observe about the corresponding Ford circles?

Theorem 29.2 No Ford circles intersect. The representative circles of two distinct fractions are either tangent at one point or wholly external to one another.

Proof.
Let p/q and P/Q be distinct fractions in lowest terms. Without loss of generality, we'll assume that $\frac{p}{q} < \frac{P}{Q}$. Consider the distance between the centers of their representative Ford circles $C(p,q)$ and $C(P,Q)$.



The coordinates of point A are $\left(\frac{p}{q}, \frac{1}{2q^2}\right)$ and the coordinates of point B are $\left(\frac{P}{Q}, \frac{1}{2Q^2}\right)$. Thus we have:

$$\begin{aligned} AB^2 &= \left(\frac{P}{Q} - \frac{p}{q}\right)^2 + \left(\frac{1}{2Q^2} - \frac{1}{2q^2}\right)^2 \\ &= \left(\frac{1}{2Q^2} + \frac{1}{2q^2}\right)^2 + \frac{(Pq - pQ)^2 - 1}{Q^2q^2} \\ &= (AD + EB)^2 + \frac{(Pq - pQ)^2 - 1}{Q^2q^2}. \end{aligned}$$

There are three cases to consider:

1. Case 1. If $|Pq - pQ| > 1$, then $AB > AD + EB$, and the circles are wholly external to one another.
2. Case 2. If $|Pq - pQ| = 1$, then $AB = AD + EB$, and the circles are tangent. Observe that this happens exactly when p/q and P/Q are adjacent terms in a Farey sequence!
3. Case 3. If $|Pq - pQ| < 1$, then, since $Pq - pQ$ is an integer, we must have $Pp - pQ = 0$. Thus, $\dfrac{P}{Q} = \dfrac{p}{q}$, which is impossible since we assumed that the fractions are distinct.

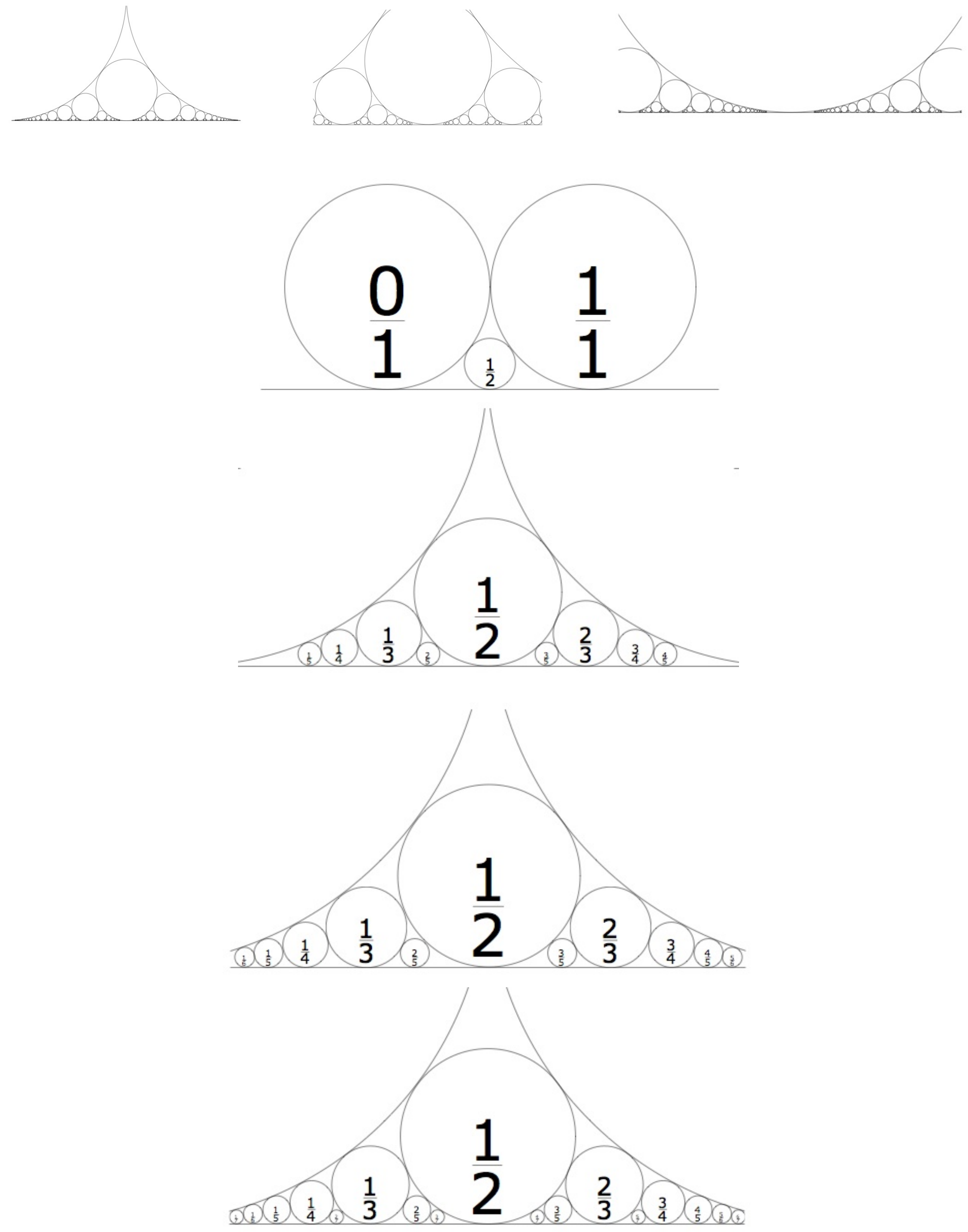


Figure 29.1: Ford circles.

Thus, we conclude that the representative Ford circles of two distinct fractions are either tangent at one point or wholly external. Moreover, the circles are tangent at one point precisely when the fractions are adjacent in some Farey sequence F_n.

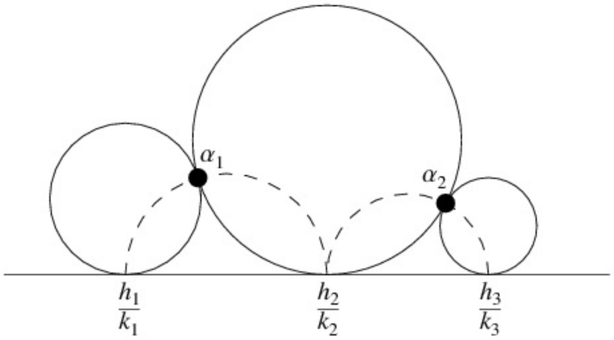
Theorem 29.3 Ford circles and the Farey sequence. Suppose that h_1/k_1, h_2/k_2, and h_3/k_3 are three consecutive terms in some Farey sequence F_n. Then the circles $C(h_1, k_1)$ and $C(h_2, k_2)$ are tangent at

$$\alpha_1 = \left(\frac{h_2}{k_2} - \frac{k_1}{k_2(k_2^2 + k_1^2)}, \frac{1}{k_2^2 + k_1^2}\right),$$

and the circles $C(h_2, k_2)$ and $C(h_3, k_3)$ are tangent at

$$\alpha_2 = \left(\frac{h_2}{k_2} + \frac{k_3}{k_2(k_2^2 + k_3^2)}, \frac{1}{k_2^2 + k_3^2}\right).$$

Moreover, α_1 lies on the semicircle with diameter $h2/k2 - h1/k1$, and α_2 lies on the semicircle with diameter $h3/k3 - h2/k2$.



Theorem 29.4 Largest Ford circle between tangent Ford circles. Suppose that $C(a, b)$ and $C(c, d)$ are tangent Ford circles. Then the largest Ford circle between them is $C(a + c, b + d)$, the Ford circle associated with the mediant fraction.

Problem Set.

1. Find F_8 by using F_7 and the algorithm that we developed.

2. Suppose that p_1/q_1 and p_2/q_2 are two successive terms of F_n. In this problem, we will use Pick's Theorem to prove that $p_2q_1 - p_1q_2 = 1$. See Chapter 28 for more information on Pick's Theorem. Let T be the triangle with vertices $(0,0)$, (p_1, q_1), and (p_2, q_2).

   (a) Show that T has no lattice points in its interior, i.e. $I(T) = 0$.

   (b) Show that the only boundary points of T are the vertices of the triangle, i.e. $B(T) = 3$.

   (c) Conclude, using Pick's Theorem, that
   $$A(T) = \frac{1}{2}.$$

   (d) Use geometry to show that
   $$A(T) = \frac{1}{2}\left(p_2q_1 - p_1q_2\right).$$

   (e) Conclude that
   $$p_2q_1 - p_1q_2 = 1.$$

3. Let a/b and a'/b' be the fractions immediately to the left and the right of the fraction $1/2$ in the Farey sequence of order n. Prove that b is the greatest odd integer less than or equal to n. Next, by experimenting with various choices of n, make and prove a conjecture about the value of $a + a'$.

4. Prove that the sum of the fractions in the Farey sequence F_n is equal to $\frac{1}{2}\left[1 + \sum_{j=1}^{n} \phi(j)\right]$.

5. Let a/b and a'/b' run through all pairs of adjacent fractions in the Farey sequence of order $n > 1$. Make and prove a conjecture about the values of
   $$\min\left(\frac{a'}{b'} - \frac{a}{b}\right) \text{ and } \max\left(\frac{a'}{b'} - \frac{a}{b}\right).$$

6. Consider the fractions from $0/1$ to $1/1$ inclusive in the Farey sequence of order n. Reading from left to right, let the denominators of these fractions be $b_1, b_2, \ldots, b_k$ so that $b_1 = b_k = 1$. By experimenting with various values of n, make and prove a conjecture about the value of $\sum_{j=1}^{k-1} \frac{1}{b_j b_{j+1}}$.

7. Suppose that $C(a, b)$ and $C(c, d)$ are tangent Ford circles. Prove that the largest Ford circle between them is $C(a + c, b + d)$, the Ford circle associated with the mediant fraction.

8. Suppose that a/b and c/d are adjacent terms in F_n (so that $C(a, b)$ and $C(c, d)$ are tangent Ford circles). Find a formula for all fractions that are adjacent to a/b in some Farey sequence.

9. Suppose that h_1/k_1, h_2/k_2, and h_3/k_3 are three consecutive terms in some Farey sequence F_n. Find the point of tangency of the circles $C(h_1, k_1)$ and $C(h_2, k_2)$, and the point of tangency of the circles $C(h_2, k_2)$ and $C(h_3, k_3)$

10. It can be shown that

$$|F_n| = 1 + \sum_{k=1}^{n} \phi(k) \approx \frac{3n^2}{\pi^2}.$$

Complete the following table to investigate the accuracy of this approximation as n increases.

n	$\lvert F_n\rvert = 1 + \sum_{k=1}^{n} \phi(k)$	$\frac{3n^2}{\pi^2}$	n	$\lvert F_n\rvert = 1 + \sum_{k=1}^{n} \phi(k)$	$\frac{3n^2}{\pi^2}$
1			15		
2			25		
3			100		
4			200		
5			500		
6			700		
7			1000		
8			2000		
9			5000		
10			10000		

11. Investigate the relationship between the total area of Ford circles and the Riemann Hypothesis.

Chapter 30

The Card Game SET

The Mathematical Framework. Each card has four characteristics (symbol, color, number, and filling), each of which has three possible values. Thus, we can associate each card in the SET deck with a 4-tuple of numbers

$$(x_1, x_2, x_3, x_4),$$

where each x_i is 0, 1, or 2. We will use the following labeling scheme:

Symbol	Label
diamond	0
oval	1
squiggle	2

Color	Label
purple	0
red	1
green	2

Number	Label
three	0
one	1
two	2

Filling	Label
striped	0
solid	1
unfilled	2

Finally, we will label the four characteristics symbol, color, number, and filling *in that order*. Since there are 4 characteristics, each of which has 3 possible values, we can associate each card in the SET deck with an element in the set $D = \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$. Some examples of the labeling scheme are as follows:

- A card with one red unfilled squiggle would have label $(2, 1, 1, 2)$.
- A card with two purple solid ovals would have label $(1, 0, 2, 1)$.
- A card with two green solid diamonds would have label $(0, 2, 2, 1)$.
- A card with three purple striped squiggles would have label $(2, 0, 0, 0)$.

Note that every possible combination of the four characteristics does appear in the SET deck, so there are a total of

$$3 \cdot 3 \cdot 3 \cdot 3 = 3^4 = 81$$

cards in the deck. We will call the set of all 81 4-tuples the set D.

Multiplication on D. Next, we define a multiplication operation on the set $D = \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$ which reflects how we obtain a SET from two given cards. Suppose that two cards have labels

$$x = (x_1, x_2, x_3, x_4) \text{ and } y = (y_1, y_2, y_3, y_4).$$

Then we define the product xy as follows:

$$xy = (2(x_1+y_1) \mod 3,\ 2(x_2+y_2) \mod 3,\ 2(x_3+y_3) \mod 3,\ 2(x_4+y_4) \mod 3).$$

Problems.

1. Choose any 2 cards from your deck of SET cards, and call them x and y.
   (a) Find the 4-tuple labels for x and y and compute the product xy. Find the card in the deck that corresponds to xy. What do you notice about x, y, and xy?
   (b) Multiply x and xy. Which card does this produce?
   (c) Multiply y and xy. Which card does this produce?
   (d) Does order matter? Is xy the same card as yx? Prove your answer using the definition of multiplication of cards and by interpreting the question in terms of SETs.
   (e) Repeat parts (a)-(d) for 3 more pairs of cards.

2. Suppose that

$$\begin{aligned} x &= (1, 1, 1, 1) \\ y &= (0, 0, 0, 0) \\ z &= (1, 2, 2, 0) \\ w &= (2, 2, 1, 1). \end{aligned}$$

Compute each of the products xy, xz, and xw, and zw. Then sketch in the appropriate symbols to see how this multiplication translates into cards. You will need purple, green, and red pens to complete this exercise. Describe what you discover.

3. (a) Based on what you discovered in the previous exercise, explain why you would expect the following properties to be true. Hint: think about what these properties say in terms of the cards.

   Property 1: $x(xy) = y$
   Property 2: $(xy)y = x$

   (b) Prove that these properties are indeed true.

4. Choose any card from your deck of SET cards. How many SETs are there that contain this card?

5. Choose any 2 cards from your deck of SET cards. How many SETs are there that contain both of these cards?

6. Choose any 3 cards from your deck of SET cards, and call them x, y, and z. Compute the products zx, zy, and xy. Next, compute $(zx)(zy)$ and $z(xy)$. What do you observe? Repeat with a different choice of 3 cards.

7. A SET magic square is a square array of cards such that any horizontal row, vertical column, or main diagonal forms a SET.

   (a) Construct a 3×3 magic square.

   (b) Consider the following method for constructing a 3×3 SET magic square. Start with any three cards that do not form a set, and place them in the 1, 3, and 5 positions in the square (counting left to right and top to bottom). Show that it is always possible to create a 3×3 SET magic square when we start with this configuration.

8. What is the maximum number of red cards that contain no sets? More generally, what is the maximum number of cards that all share a particular feature (number, color, shape, or filling) that contains no sets?

9. Is it possible for the game to end with three cards left?

10. Prove that 5 cards that have two common features must include a SET. For example, consider only the red cards with solid filling, and prove that any collection of 5 such cards must contain a SET.

11. Prove that among 7 cards there cannot be exactly 4 SETs.

12. If 12 randomly selected cards don't contain a SET and 3 additional cards are added, what is the probability of a SET being present?

13. What is the probability of having 2 disjoint SET among 12 randomly selected cards?

14. How does the game change, and how do the answers to some of these questions change, if you combine 2 or 3 decks of cards together?

15. A **cap** is a collection of cards which have no SET but the addition of *any* card to the collection will produce a SET.

    (a) Suppose that we are playing SET with only the red ovals. What is the maximum size of a cap?

    (b) Suppose that we are playing SET with all of the red cards. What is the maximum size of a cap?

16. Does cancellation hold in D? That is, if x, y, z are elements of D such that $xy = xz$, must $y = z$? Provide a proof to support your claim.

17. Prove that $(zx)(zy) = z(xy)$.

18. A ***D*-set** is defined to be a subset $S \subseteq D$ of the form

$$S = \{x, y, xy\},$$

where $x, y \in D$. D-sets correspond to SETs in the card game. Prove that there are a total of 1080 possible D-sets in D (and thus there are a total of 1080 possible sets in the card game). How many D-sets can a given element $x \in S$ be a member of?

19. Suppose that $U \subseteq D$. We say that U is **product-free** if $xy \notin U$ whenever $x, y \in U$. Note that product-free subsets of D translate into collections of cards that fail to contain a SET. Prove that if U is product-free, then xU is also product-free. For any set $S \subseteq D$, and $x \in D$, the set xS is defined to be the set

$$xS = \{xs \text{ such that } s \in S\}.$$

20. Prove that if $S \subseteq D$ is a product-free set and $x \in S$, then $S \cap xS = \{x\}$. Conclude that any product-free set can contain at most 41 elements, and that any collection of 42 cards must contain a SET.

21. The largest known collection of cards containing no SET is given below. Its cardinality is 20. If we let $\alpha(D)$ denote the cardinality of the largest product-free subset of D, then this fact together with the result of the previous exercise yields $20 \leq \alpha(D) \leq 41$. Can you tighten the upper bound on $\alpha(D)$? That is, can you find an upper bound that is less than 41, or optimally, can you prove that $\alpha(D) = 20$? Here is a product-free set of 20 elements in D:

$$(0,1,0,0),\ (0,2,0,1),\ (1,2,0,0),\ (1,1,0,1),\ (2,1,0,1),\ (2,2,0,0),\ (0,0,2,0)$$

$$(0,1,1,0),\ (0,2,1,1),\ (1,2,1,0),\ (1,1,1,1),\ (2,1,1,1),\ (2,2,1,0),\ (0,0,2,1)$$

$$(0,1,2,2),\ (0,2,2,2),\ (1,2,2,1),\ (1,1,2,0),\ (2,1,2,0),\ (2,2,2,1)$$

22. What is the largest number of SETs that can be present among a layout of 9 cards?

23. What is the largest number of SETs that can be present among a layout of 12 cards?

Chapter 31

Magic Squares

A **magic square** of order n is an $n \times n$ array (or square) containing n^2 different entries such that the sum of the n numbers in any horizontal, vertical, or main diagonal line is always the same magic constant. If the rows and columns sum to the magic constant (but the main diagonals do not), the resulting array is called a **semi-magic square**. For example, the following is an example of a 5×5 semi-magic square:

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

The numbers in any row or column sum to 65, but the main diagonals do not both sum to 65.

Example 31.1 Construct a 3×3 magic square.

The De la Loubère Method. In 1693, De la Loubère gave a rule for inserting the numbers

$$1, 2, 3, \ldots, n^2$$

into an $n \times n$ square (where n is an **ODD** integer) so that a magic square is formed. The procedure is outlined as follows.

1. Start with an empty $n \times n$ square, where n is odd. We'll begin with $n = 5$:

2. The basic rule is to count diagonally upwards to the right. For example, if we have written a 12 in the 2nd position of the 4th row,

	12			

then the numbers 13, 14, 15 should be placed as follows:

				15
			14	
		13		
	12			

3. To construct a magic square, begin in the middle of the top row with a 1. (Here we for the first time use the assumption that n is odd, which guarantees that there is a middle square in the top row). If we don't start there, the row and column sums will be ok, but the diagonals won't add to the magic sum, so we will create a semi-magic square instead of a magic square.

		1		

4. Now, the first thing we observe is that it is impossible to move diagonally upwards from this position, since we are already at the top of the square. This is an example of what can go wrong with the basic method of moving diagonally upwards to the right. There are actually three things that can go wrong:

   (a) We could be at the top edge of the square, so we can't go up.

   (b) We could be at the right edge of the square so we can't move right.

   (c) The square we would like to put the next number in may already be occupied.

   Here is what to do in these cases:

   (a) If we are at the top edge, pretend that the top edge is pasted to the bottom edge and come up through the bottom. In other words, we pretend that the bottom row is the row above the top row. Moving diagonally upwards to the right means moving up one row and over one column to the right. So the 2 goes in the bottom row one column to the right of the column containing the 1. Thus, after 1, we place 2 as follows:

		1		
			2	

   (b) If you are at the right edge, pretend that the right edge is pasted to the left edge and that the left edge is immediately to the right of the right edge. We are in this situation after counting to 3, since we have:

		1		
				3
			2	

   Then moving diagonally upwards to the right is the same as moving right one column and up one row. Moving right one column from the rightmost column puts us in the leftmost column, so 4 must be in the leftmost column, and moving up one row we put the 4 in the row above the row containing the 3. So we get

		1		
4				
				3
			2	

(c) If there is a number already occupying the square we would like to move into, abandon the plan of moving diagonally upwards to the right and instead just drop down one square from the square one is in presently. We are in this situation after we place the number 5. Indeed, continuing from the previous diagram, we place the 5 diagonally upwards, so the 6 will be placed directly below the 5.

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

5. Continuing, we obtain the following 5×5 magic square with magic constant 65.

Problems.

1. Starting with 1 in the lower-left hand corner, construct the 3×3 and 4×4 squares given by the Loubère method. Verify that the 3×3 square is a semi-magic square with magic constant 15 and that the 4×4 square is neither a magic square nor a semi-magic square.
2. Construct a 7×7 magic square using the Loubère method.
3. Construct examples of several $n \times n$ squares for **even** n using the Loubère method. Compute the row and column sums for your examples, and make a conjecture about the Loubère method for even n using your results.
4. Can the numbers 0 through 5 be inserted in a 2×3 rectangle in such a way that the sums of the entries of the two rows are equal?
5. The numbers 0 through $n^2 - 1$ are placed in an $n \times n$ square in such a way as to make it semi-magic. (The process used is not necessarily the Loubère method). What is the magic sum? Hint: consider the sum of every number in the square and how this total is related to the magic sum.
6. Is there a 2×2 magic square?

7. A 9×9 square may be split up naturally into nine 3×3 squares. Using the numbers from 0 to 80, construct a semi-magic square such that each of the nine 3×3 squares is also semi-magic.

8. Complete the following 5×5 magic square.

1		19	23	
18			5	9
	4	8		
7			14	3
	13	2	6	

9. Research the *pyramid method* for constructing magic squares. Construct a 5×5 magic square using the pyramid method.

10. Research *Greco-Latin squares*, and construct an example of a 5×5 Greco-Latin square.

Chapter 32

Mathematical Games

Reference: Tatiana Shubin, Department of Mathematics, San Jose State University, San Jose, CA, shubin@math.sjsu.edu.

In all of the games described below there are two players, Alice and Bob, and Alice always plays first. The problem is to decide which one of the two players has a winning strategy (and, of course, to describe this strategy). An answer to the question Which player has a winning strategy? must include a detailed description of such strategy, i.e., you have to explain what the winning player should do so that this player wins REGARDLESS of his opponents moves. To solve a game means to find a winning or a non-losing strategy for one of the players. In particular, to solve a game, you must provide an algorithm that secures a win for one player, or a tie, against any possible moves from the opponent, from the beginning of the game.

1. (a) There are 25 matches on a table. During each turn, a player can take any number of matches between 1 and 4. The player that takes the last match wins.

   (b) Same game as above but it starts with 24 matches.

   (c) Same game again, only the initial number of matches is N.

2. (a) Now there are two piles of matches, one pile with 10 matches and another one with 7. During each turn, a player can take any number of matches from either one of the two piles. The player who takes the last match wins.

   (b) What will happen if the numbers of matches in the piles are m and n?

3. (a) Alice and Bob want to produce a 20-digit number, writing one digit at a time from left to right. Alice wins if the number they get is not divisible by 7; Bob wins if the number is divisible by 7.

   (b) What will happen if 7 is replaced by 13 in the previous game?

4. Given a convex n-gon, the players take turns drawing diagonals that do not intersect those diagonals that have already been drawn. The player unable to draw a diagonal loses.

5. There are 25 matches in a pile. A player can take 1, 2, or 4 matches during each turn. The player who cannot continue (no more matches left) loses.

6. On one square of an 8 by 8 chessboard there is a lame tower that can move either to the left or down through any number of squares. Alice and Bob take turns moving the tower. The player unable to move the tower loses. (Consider various initial positions of the tower.)

7. There are two piles of matches; one pile contains 10 matches while the other contains 7. A player can take one match from the first pile, or one match from the second pile, or one match from each of the two piles. The player unable to move loses.

8. At the start of the game, there is a number 60 written on the board. During each turn, a player can reduce the number that is currently on the board by any of its positive divisors. If the resulting number is a 0, the player loses.

9. Alice calls out any integer between 2 and 9, Bob multiplies it by any integer between 2 and 9, then Alice multiplies the new number by any integer between 2 and 9, and so on. The player who first gets a number bigger than 1000 wins.

10. (a) There are several minuses written along a line. A player replaces either one minus by a plus or two adjacent minuses by two pluses. The player who replaces the last minus wins.

    (b) Same game as above, only the minuses are written around a circle.

11. There are nine cards on a table labeled by numbers 1 trough 9. Alice and Bob take turns choosing one card. The player that has collected a set of cards with the property that the sum of numbers on three cards out of their total set is 15 wins. Theres a tie if none of the players has a set of cards with this property at the end of the game. Does any of the players have a winning strategy? A non-losing strategy?

12. Players start with one pile of pebbles. During each move, a player must split one pile into two nonempty piles in such a way that all resulting piles have different number of pebbles. The player unable to make a move loses.

    (a) After the first move, the piles contain 5 and 11 pebbles. Find a winning strategy for Bob.

    (b) After the first move, the piles contain 5 and 11 pebbles. Give an example of a bad move after which Bob will necessarily lose.

    (c) Which player has a winning strategy if they start with 11 pebbles?

    (d) Which player has a winning strategy if they start with 22 pebbles?

    (e) Can you solve the game in general?

13. In a box, there are

(a) 57 candies

(b) 50 candies

(c) 1000 candies

(d) $N > 1$ candies

During each turn, a player can take any amount of candy subject to the following two conditions.

- The first player cannot take all the candy.
- A player cannot take more candy than his opponent has just taken.

The player who takes the last candy wins. Which of the players has a winning strategy?

14. Suppose we start with N integers: $1, 2, 3, \ldots, N$. During each turn, a player circles one of the numbers in such a way that all circled numbers are pairwise relatively prime. No number can be circled twice. The player unable to complete a turn loses. Which player has a winning strategy if:

    (a) $N = 10$

    (b) $N = 12$

    (c) $N = 15$

    (d) $N = 30$

    (e) N is any positive integer

15. Players start with one pile of pebbles. During each move, a player must split one pile into two nonempty piles in such a way that all resulting piles have different number of pebbles. The player unable to make a move loses.

    (a) After the first move, the piles contain 5 and 11 pebbles. Find a winning strategy for Bob.

    (b) After the first move, the piles contain 5 and 11 pebbles. Give an example of a bad move after which Bob will necessarily lose.

    (c) Which player has a winning strategy if they start with 11 pebbles?

    (d) Which player has a winning strategy if they start with 22 pebbles?

    (e) Can you solve the game in general?

Chapter 33

The 5 Card Trick of Fitch Cheney

The trick. Take an ordinary deck of 52 cards, and draw a hand of 5 cards from it. Choose them deliberately or randomly, but do not show them to the magician. Instead, give them to the magician's assistant, who will then give 4 of them, 1 at a time, to the magician. The magician can then name the hidden card.

The mathematics. Suppose that 5 cards are drawn from a standard deck of 52 cards. Note that among these 5 cards, there must be 2 of the same suit (by the Pigeonhole Principle, since there are 4 suits). We will label these two cards the *base card* and the *hidden card* in such a way that it is possible to go from the base card to the hidden card by adding at most 6, modulo 13, to the base card. Assume that we have labeled the cards as follows:

Card rank	Value
Ace	1
2	2
3	3
4	4
5	5
6	6
7	7
8	8
9	9
10	10
Jack	11
Queen	12
King	13

So, for example, if both the 3 of diamonds and the queen of diamonds are among the four cards, we will choose the queen to be the base card and the ace to be the hidden card since $12 + 4 \equiv 3 \mod 13$.

The assistant always hands the base card first to the magician. This reveals the suit of the hidden card to the magician, and also sets the base point at which the magician should add up to 6, modulo 13, to obtain the value of the hidden card.

The order in which the 3 remaining cards are presented can be used to reveal what number should be added to the base card, as there are 6 possible permutations of the 3 remaining cards. Use the ordering above to put the 3 remaining cards in order. If there are two cards with the same value, use the suit to break the tie. For example, order the suits alphabetically–clubs, diamonds, hearts, spades. Use the following code to determine the number which the magician adds to the base card, where H stands for high, M for middle, and L for low:

Order	Number to add to the base card
LMH	1
LHM	2
MLH	3
MHL	4
HLM	5
HML	6

Example. Suppose that the five cards drawn are the queen of hearts, the 3 of diamonds, the king of spades, the 8 of clubs, and the 7 of spades. Since there are two cards in the spade suit, and the king has value 13, the assistant will choose the 7 of spades to be the base card and the king of spades to be the hidden card. Thus, the assistant will first give the 7 of spades to the magician. Next, the assistant needs to use the remaining three cards to tell the magician to add 6 to the 7 of spades to obtain 13, the king of spades. Using our ordering above, the code HML corresponds to the number 6, so the assistant should give the magician the three remaining cards in the order highest, middle, lowest. Thus, the assistant gives the magician the cards in the order queen of hearts, 8 of clubs, and 3 of diamonds. The magician recognizes the code for the number 6, adds 6 to the 7 of spades, and concludes that the hidden card must be the king of spades.

Reference: Michael Klever, *The Best Card Trick*, **The Mathematical Intelligencer**, Volume 24, Number 1, Winter 2002.

This trick is credited to Dr. William Fitch Cheney, Jr. (1894-1974).

Chapter 34

Conway's Rational Tangles

Summary of the rational tangles operations:

- Let x denote the number associated with the current tangle.
- Twist: $T \ : \ x \to x+1$.
- Rotate: $R \ : \ x \to -\dfrac{1}{x}$.

1. Given a tangle number $\dfrac{m}{n}$, where m and n are integers and the fraction is in lowest terms, is it always possible to use the TWIST and ROTATE operations to obtain the tangle number 0 (i.e the untangled configuration)? If so, how do you do it? How do you know that you'll always be able to reach the tangle number 0?
2. Is it possible to start from 0 and get to any positive or negative fraction using TWISTs and ROTATEs? Given relatively prime integers i and j, is it always possible to obtain the tangle number $\dfrac{i}{j}$? If so, how do you do it? If not, what numbers are not possible to obtain?
3. In this problem, you will discover and prove formulas for various combinations of TWIST and ROTATE (starting in each case with the tangle number 0). The letter T denotes the twist operation and the letter R denotes the rotate operation. So, for example, $T(TRT)^n$ means first do 1 TWIST, then do TWIST-ROTATE-TWIST n times.
   (a) Show that $T^n \ : \ 0 \to n$.
   (b) Show that $T(TRT)^n \ : \ 0 \to \frac{1}{n+1}$. To get started, work out the fraction produced by $T(TRT)^n$ for a few small values of n. Then try to prove the general formula.
   (c) Discover and prove a formula for T^2RT^n.

(d) Discover and prove a formula for $T^2(TRT)^n$.

(e) Discover and prove a formula for $T(TRT)^nR$.

(f) Discover and prove a formula for $T^{n+1}RT^n$.

(g) Can you find other patterns?

4. How does infinity relate to tangle numbers? For example, try starting with zero and do a single ROTATE. What happens? What happens if you do another ROTATE? What happens if you do a ROTATE, then a TWIST? How do these examples relate to the number infinity?

5. In this problem, you'll investigate the relationship between rational tangles and the Euclidean algorithm for computing the gcd.

(a) Describe the order of the TWIST and ROTATE operations that you would use to obtain the tangle number 0 starting from a tangle number of $-5/17$.

(b) Next, use the Euclidean algorithm *with subtraction* instead of addition to find the gcd of 5 and 17:

$$\begin{aligned} 5 &= 17 \times 1 - 12 \\ 17 &= 12 \times 1 + 5 = 12 \times 2 - 7 \\ 12 &= 7 \times 1 + 5 = 7 \times 2 - 2 \\ 7 &= 2 \times 1 + 5 = 2 \times 2 + 3 = 2 \times 3 + 1 = 2 \times 4 - 1 \\ 2 &= 1 \times 1 + 1 = 1 \times 2 + 0 \end{aligned}$$

What do you observe? How does the calculation above compare with the calculation that you did in part (a)?

(c) Repeat parts (a) and (b) for a different tangle number. Discuss your observations.

Chapter 35

Invariants and Monovariants

Example 35.1 Write 11 numbers on a sheet of paper–six zeros and five ones. Perform the following operation 10 times: cross out any two numbers, and if they were equal, write another zero on the board. If they were not equal, write a one. Show that no matter which numbers are chosen at each step, the final number on the board will be a one.

Solution. The sum of the numbers at the start is 5. After each operation, the sum can only increase by 0 or 2. Thus, the parity of the sum remains the same. Since the original sum was odd, the final remaining number must be odd as well. In this example, the parity of the sum of the numbers is an *invariant*.

Example 35.2 The numbers $1, 2, \ldots, 20$ are written on a blackboard. It is permitted to erase any two numbers a and b and write the new number $a+b-1$. What number can be on the blackboard after 19 such operations?

Solution. For any collection of n numbers on the board, let X denote the sum of all of the numbers decreased by n. How does X change when we erase a and b and write the new number $a + b - 1$? If the sum of all the numbers except a and b is equal to S, then before the transformation, we have

$$X = S + a + b - n,$$

and after the transformation, we have

$$X = S + (a + b - 1) - (n - 1) = S + a + b - n.$$

Thus, X is invariant. Initially, we have

$$X = (1 + 2 + \cdots + 20) - 20 = \frac{19 \cdot 20}{2} = 190.$$

When there is only one number left, we must have $X = 190$, so the last number must be 191.

Example 35.3 A circle is divided into 6 sectors. The numbers $1, 0, 1, 0, 0, 0$ are written into the sectors in the counterclockwise direction. You may increase any two neighboring numbers by 1. Is it possible to make all of the numbers equal?

Solution. Consider the quantity $I = a_1 - a_2 + a_3 - a_4 + a_5 - a_6$. This quantity is invariant, and $I = 2$ initially. Thus, $I = 0$ cannot be obtained.

Example 35.4 A dragon has 100 heads. A knight can cut off 15, 17, 20, or 5 heads with one blow of his sword. In each of these respective cases, 24, 2, 12, or 14 new heads grow back. If all heads are cut off, the dragon dies. Is it possible for the knight to kill the dragon?

Solution. Note that

$$(24-15) \equiv (2-17) \equiv (14-20) \equiv (17-5) \equiv 0 \mod 3.$$

Thus, the total number of heads never changes modulo 3. Since the original sum is $100 \equiv 1 \mod 3$, the total number of heads will always be congruent to 1 modulo 3, so it's not possible for the knight to kill the dragon.

Example 35.5 (IMO 1986) To each vertex of a pentagon, assign an integer x_i such that the sum $S = \sum_{i=1}^{5} x_i > 0$. If x, y, z are the numbers assigned to three successive vertices and if $y < 0$, then we replace (x, y, z) by $(x + y, -y, y + z)$. This step is repeated as long as there exists a vertex labeled with a negative integer. Determine whether or not this algorithm always stops.

Solution. The algorithm always stops. Consider the function

$$f(x_1, x_2, x_3, x_4, x_5) = \sum_{i=1}^{5}(x_i - x_{i+2})2, \ x_6 = x_1, \ x_7 = x_2.$$

Clearly $f > 0$ always and f is integer-valued. Suppose, without loss of generality, that $y = x_4 < 0$. Then $f_{\text{new}} - f_{\text{old}} = 2Sx_4 < 0$ since $S > 0$. Thus, if the algorithm does not stop, then we can find an infinite decreasing sequence of nonnegative integers $f_0 > f_1 > f_2 > \cdots$. This is impossible, so the algorithm must stop.

The function f used in this example is an example of a *monovariant*, a generalization of the idea of invariance. Even if we cannot identify some function that never changes, we may be able to identify a function that *always changes in the same direction*. If there is some nonnegative, integer-valued function that decreases at each step of a process, that process must eventually terminate.

Problem Set.

1. Suppose that the positive integer n is odd. Write the numbers $1, 2, \ldots, 2n$ on the board. Choose any 2 numbers a and b, erase them, and write $|a - b|$. Prove that an odd number will remain at the end.

2. Start with the set $\{3, 4, 12\}$. In each step, you may choose two of the numbers a and b and replace them by $0.6a - 0.8b$ and $0.8a + 0.6b$. Can you reach (a) or (b) in finitely many steps?

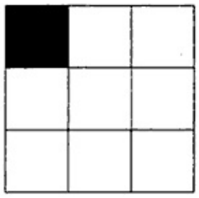
   (a) $\{4, 6, 12\}$

   (b) $\{x, y, z\}$, where each of $|x - 4$, $|y - 6|$, $|z - 12|$ are less than $\dfrac{1}{\sqrt{3}}$

3. The numbers $1, 2, \ldots, 20$ are written on a blackboard. It is permitted to erase any two numbers a and b and write the new number $ab + a + b$. What number can be on the blackboard after 19 such operations? Hint: consider the quantity obtained by increasing each number by 1 and multiplying the result.

4. Consider an 8×8 array of squares in which one of the squares is colored black and all of the others are colored white. You may recolor all of the squares in a row or column. Is it possible to make all of the boxes white?

5. Consider a 3×3 array in which only the upper left corner is colored black and all other squares are colored white. You may recolor all of the squares in a row or column. Is it possible to make all of the boxes white?



6. Consider an 8×8 array of squares in which all four corner squares are colored black and all other squares are colored white. You may recolor all of the squares in a row or column. Is it possible to make all of the boxes white?

7. There are green, yellow, and red chameleons. Whenever 2 chameleons of different colors meet, they change to the third color.

   (a) Given 4 green, 5 yellow, and 5 red chameleons, is it possible to have all chameleons change to the same color?

   (b) Given 4 green, 5 yellow, and 6 red chameleons, is it possible to have all chameleons change to the same color?

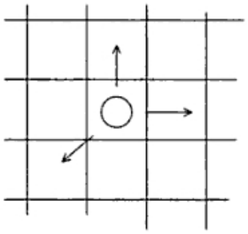
   (c) Given 13 green, 15 yellow, and 17 red chameleons, is it possible to have all chameleons change to the same color?

(d) Can you find a condition which is necessary and sufficient for a given starting configuration to be solvable? (Here, solvable means that it is possible to obtain a configuration in which all chameleons have the same color).

8. The number 8^n is written on the board. The sum of its digits is calculated, then the sum of the digits of the result is calculated, and so on, until a single digit is reached. What is this digit if $n = 1989$?

9. Consider an 8×8 chessboard with the usual coloring. You may recolor *all* squares (a) of a row or column or (b) of a 2×2 square. Can you reach just one black square?

10. A pawn moves across an $n \times n$ chessboard so that in one move it can shift one square to the right, one square upward, or along a diagonal down and left.



Can the pawn move through all of the squares on the board, visiting each square exactly once, and finish its trip on the square immediately to the right of the initial one?

11. The boxes of an $m \times n$ table are filled with numbers so that the sum of the numbers in each row and in each column is equal to 1. Prove that $m = n$.

12. The integers $1, 2, \ldots, n$ are arranged in any order. In one step, you may switch any 2 neighboring integers. Prove that you can never obtain the initial order after an odd number of steps.

13. (2008 Putnam) Start with a finite sequence $a_1, a_2, \ldots, a_n$ of positive integers. If possible, choose 2 indices $j < k$ such that a_j does not divide a_k, and replace a_j and a_k by $\gcd(a_j, a_k)$ and $\text{lcm}(a_j, a_k)$ respectively. Prove that this process must eventually stop. Hint: can you find a monovariant?

Chapter 36

Number Theory Problems from AMC, AHSME, AIME, USAMO, and IMO Mathematics Contests

1. (1998 AHSME #13) Walter rolls four standard six-sided dice and finds that the product of the numbers on the upper faces is 144. Which of the following could **not** be the sum of the upper four faces?

   (A) 14 (B) 15 (C) 16 (D) 17 (E) 18

2. (2000 AMC 10 #1) Let I, M, and O be distinct positive integers such that the product $I \cdot M \cdot O = 2001$. What is the largest possible value of the sum $I + M + O$?

   (A) 23 (B) 55 (C) 99 (D) 111 (E) 671

3. (1999 AMC 10 #7) Find the sum of all prime numbers between 1 and 100 that are simultaneously one greater than a multiple of 5 and one less than a multiple of 6.

   (A) 52 (B) 82 (C) 123 (D) 143 (E) 214

4. (1995 AHSME #29) For how many three-element sets of positive integers $\{a, b, c\}$ is it true that $a \times b \times c = 2310$?

   (A) 32 (B) 36 (C) 40 (D) 43 (E) 45

5. (1999 AMC 10 #14) All even numbers from 2 to 98 inclusive, except those ending in 0, are multiplied together. What is the rightmost digit (the units digit) of the product?

(A) 0 (B) 2 (C) 4 (D) 6 (E) 8

6. (1999 AMC 10 #15) How many three-element subsets of the set

$$\{88, 95, 99, 132, 166, 173\}$$

have the property that the sum of the three elements is even?

(A) 6 (B) 8 (C) 10 (D) 12 (E) 24

7. (1998 AHSME #30) For each positive integer n, let

$$a_n = \frac{(n+9)!}{(n-1)!}.$$

Let k denote the smallest positive integer for which the rightmost nonzero digit of a_k is odd. The rightmost nonzero digit of a_k is

(A) 1 (B) 3 (C) 5 (D) 7 (E) 9

8. (1992 AHSME #17) The two-digit integers from 19 to 92 are written consecutively to form the large integer

$$N = 192021 \cdots 909192.$$

Suppose that 3^k is the highest power of 3 that is a factor of N. What is k?

(A) 0 (B) 1 (C) 2 (D) 3 (E) 4

9. (1997 AHSME #20) Which one of the following integers can be expressed as the sum of 100 consecutive positive integers?

(A) 1,627,384,950 (C) 3,579,111,300 (E) 5,815,937,260
(B) 2,345,678,910 (D) 4,692,581,470

10. (2000 AMC 10 #17) Boris has an incredible coin changing machine. When he puts in a quarter, it returns five nickels; when he puts in a nickel, it returns five pennies; and when he puts in a penny, it returns five quarters. Boris starts with just one penny. Which of the following amounts could Boris have after using the machine repeatedly?

(A) \$3.63 (B) \$5.13 (C) \$6.30 (D) \$7.45 (E) \$9.07

11. (2000 AMC 10 #25) In year N, the 300th day of the year is a Tuesday. In year $N+1$, the 200th day is also a Tuesday. On what day of the week did the 100th day of year $N-1$ occur?

(A) Thursday (B) Friday (C) Saturday (D) Sunday (E) Monday

12. (1991 AHSME #15) A circular table has 60 chairs around it. There are N people seated at this table in such a way that the next person to be seated must sit next to someone. What is the smallest possible value for N?

    (A) 15 (B) 20 (C) 30 (D) 40 (E) 58

13. (1992 AHSME #23) Let S be a subset of $\{1, 2, 3, \ldots, 50\}$ such that no pair of distinct elements in S has a sum divisible by 7. What is the maximum number of elements in S?

    (A) 6 (B) 7 (C) 14 (D) 21 (E) 23

14. (1974 AHSME #8) What is the smallest prime number dividing the sum $3^{11} + 5^{13}$?

    (A) 2 (B) 3 (C) 5 (D) $3^{11} + 5^{13}$ (E) none of these

15. (1983 AIME) Let $a_n = 6^n + 8^n$. Determine the remainder when a_{83} is divided by 49.

16. (2004 AMC 10B #4) A standard six-sided die is rolled and P is the product of the five numbers that are visible. What is the largest number that is certain to divide P?

    (A) 6 (B) 12 (C) 24 (D) 144 (E) 720

17. (1999 AHSME #6) What is the sum of the digits of the decimal form of the product $2^{2004} \cdot 5^{2006}$?

    (A) 2 (B) 4 (C) 5 (D) 7 (E) 10

18. (2002 AMC 10B #14) The number $25^{64} \cdot 64^{25}$ is the square of a positive integer N. What is the sum of the digits of N?

    (A) 7 (B) 14 (C) 21 (D) 28 (E) 35

19. (2002 AMC 10A #14 and 12A #12) Both roots of the quadratic equation

    $$x^2 - 63x + k = 0$$

    are prime numbers. What is the number of possible values of k?

(A) 0 (B) 1 (C) 2 (D) 4 (E) 6

20. (1986 AHSME #23) Let

$$N = 69^5 + 5 \cdot 69^4 + 10 \cdot 69^3 + 10 \cdot 69^2 + 5 \cdot 69 + 1.$$

How many positive integers are factors of N?

(A) 3 (B) 5 (C) 69 (D) 125 (E) 216

21. (2003 AMC 12A #23) How many perfect squares are divisors of the product

$$1! \cdot 2! \cdot 3! \cdot 9!?$$

(A) 504 (B) 672 (C) 864 (D) 936 (E) 1008

22. (1990 AHSME #11) How many positive integers less than 50 have an odd number of positive integer divisors?

(A) 3 (B) 5 (C) 7 (D) 9 (E) 11

23. (1993 AHSME #15) For how many values of n will an n-sided regular polygon have interior angles with integer degree measures?

(A) 16 (B) 18 (C) 20 (D) 22 (E) 24

24. (2002 AMC 12 #20) Suppose that a and b are digits, not both nine and not both zero, and the repeating decimal

$$0.abababab\cdots$$

is expressed as a fraction in lowest terms. How many different denominators are possible?

(A) 3 (B) 4 (C) 5 (D) 8 (E) 9

25. (1996 AHSME #29) Suppose that n is a positive integer such that $2n$ has 28 positive divisors and $3n$ has 30 positive divisors. How many positive divisors does $6n$ have?

(A) 32 (B) 34 (C) 35 (D) 36 (E) 38

26. (1998 AHSME #28) How many ordered triples of integers (a, b, c) satisfy

$$|a + b| + c = 19 \text{ and } ab + |c| = 97?$$

(A) 0 (B) 4 (C) 6 (D) 10 (E) 12

27. (2008 USAMO) Prove that for each positive integer n, there are pairwise relatively prime integers $k_0, k_1, \ldots, k_n$, all strictly greater than 1, such that

$$k_0 k_1 \cdots k_n - 1$$

is the product of two consecutive integers.

28. (2007 USAMO) Let n be a positive integer. Define a sequence by setting $a_1 = n$ and, for each $k > 1$, let a_k be the unique integer in the range $0 \leq a_k \leq k - 1$ for which $a_1 + a_2 + \cdots + a_k$ is divisible by k. For example, when $n = 9$, the sequence is $9, 1, 2, 0, 3, 3, 3, \ldots$. Prove that for any n, the sequence $a_1, a_2, \ldots$ eventually becomes constant.

29. (1979 IMO) If a, b are natural numbers such that

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

prove that $1979|a$.

30. (2007 IMO) Let a and b be positive integers. Show that if $4ab - 1$ divides $(4a^2 - 1)$, then $a = b$.

Chapter 37

Challenge Contest Problems

For each of these problems, experiment numerically with the given problem, and try to come up with conjectures. Then, try to prove that your conjectures are correct. To get started with each problem, try small cases and look for patterns.

1. (Putnam 1990) Let
$$T_0 = 2,\ T_1 = 3,\ T_2 = 6,$$
and for $n \geq 3$,
$$T_n = (n+4)T_{n-1} - 4nT_{n-2} + (4n-8)T_{n-3}.$$
The first few terms are
$$2, 3, 6, 14, 40, 152, 784, 5158, 40576, 363392.$$
Find a formula for T_n of the form
$$T_n = A_n + B_n,$$
where (A_n) and (B_n) are well-known sequences.

2. For each integer $n > 1$, find *distinct* positive integers x and y such that
$$\frac{1}{x} + \frac{1}{y} = \frac{1}{n}.$$

3. For each positive integer n, find positive integer solutions $x_1, \ldots, x_n$ of the equation
$$\frac{1}{x_1} + \frac{1}{x_2} + \cdots + \frac{1}{x_n} + \frac{1}{x_1 x_2 \cdots x_n} = 1.$$

4. Define $s(n)$ to be the number of ways that the positive integer n can be written as an ordered sum of at least one positive integer. For example,
$$4 = 1+3 = 3+1 = 2+2 = 1+1+2 = 1+2+1 = 2+1+1 = 1+1+1+1,$$
so $s(4) = 8$. Conjecture a general formula for $s(n)$.

5. Let $g(n)$ be the number of odd terms in the row of Pascal's Triangle which starts with $1, n, \ldots$. For example, $g(6) = 4$ since the row

$$1, 6, 15, 20, 15, 6, 1$$

contains 4 odd numbers. Conjecture a formula for (or an easy way of computing) $g(n)$.

6. A group of n people are standing in a circle, numbered consecutively clockwise from 1 to n. Starting with person #2, we remove every other person, proceeding clockwise. For example, if $n = 6$, the people are removed in the order 2,4,6,3,1, and the last person remaining is #5. Let $j(n)$ denote the last person remaining (e.g. $j(6) = 5$).

   (a) Compute $j(n)$ for $n = 2, 3, \ldots, 25$.

   (b) Conjecture an easy way of computing $j(n)$. You may not get a nice formula, but try to find an algorithm which is easy to implement.

7. Observe that

$$6 = 1^2 - 2^2 + 3^2$$

and

$$7 = -1^2 + 2^2 + 3^2 - 4^2 - 5^2 + 6^2.$$

Investigate this pattern, and make a conjecture about a more general result..

8. (Putnam 1983) Let $f(n) = n + \lfloor \sqrt{n} \rfloor$, where $\lfloor n \rfloor$ is the greatest integer less than or equal to n. Prove that, for every positive integer m, the sequence

$$m, f(m), f(f(m)), f(f(f(m))), \ldots$$

contains the square of an integer. You should begin this problem by experimenting with some numerical values. Make tables of the sequence

$$m, f(m), f(f(m)), f(f(f(m))), \ldots$$

for various positive integers m.

9. Lockers in a row are numbered $1, 2, 3 \ldots, 1000$. At first, all of the lockers are closed. A person walks by, and opens every other locker, starting with locker #2. Thus, lockers $2, 4, 6, \ldots, 998$ are open. Another person walks by, and changes the "state" (i.e., closes a locker if it is open, opens a locker if it is closed) of every third locker, starting with #3. Then another person changes the state of every fourth locker, starting with #4. This process continues until no more lockers can be altered. Which lockers will be closed? Hint: Start doing some experimentation with a smaller number of lockers.

10. (1985 AIME) The numbers in the sequence

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

are of the form

$$a_n = 100 + n^2,$$

where $n = 1, 2, 3, \ldots$. For each n, let d_n be the greatest common divisor of a_n and a_{n+1}. Find the maximum value of d_n as n ranges through the positive integers.

11. (Russia, 1995) The sequence $a_0, a_1, a_2, \ldots$ satisfies

$$a_{m+n} + a_{m-n} = \frac{1}{2}(a_{2m} + a_{2n})$$

for all integers $m, n \geq 0$ with $m \geq n$. If $a_1 = 1$, find a_{1995}.

12. Into how many regions is the plane divided by n lines in **general position** (no two lines parallel; no three lines meet in a point)?

13. A **great circle** is a circle drawn on a sphere that is an "equator," i.e. its center is also the center of the sphere. Suppose that there are n great circles on a sphere, no three of which meet at any point. Into how many regions do they divide the sphere?

14. What is the first time after 12:00 at which the hour and minute hands meet?

15. Let $\mathbb{N}$ denote the natural numbers $\{1, 2, 3, 4, \ldots\}$. Consider a function $f : \mathbb{N} \to \mathbb{N}$ which satisfies

$$f(1) = 1,\ f(2n) = f(n),\ f(2n+1) = f(2n) + 1$$

for all $n \in \mathbb{N}$. Find a nice simple algorithm for $f(n)$. Your algorithm should be a single sentence long, at most.

16. Define the function $f(x)$ by

$$f(x) = \frac{1}{1-x}$$

and denote r iterations of the function f by f^r, i.e.

$$\begin{aligned} f^2(x) &= f(f(x)) \\ f^3(x) &= f(f(f(x))) \\ f^4(x) &= f(f(f(f(x)))). \end{aligned}$$

Compute $f^{1999}(2000)$.

17. (1997 IMO) An $n \times n$ square matrix (square array) whose entries come from the set $S = \{1, 2, \ldots, 2n-1\}$ is called a *silver* matrix if, for each $i = 1, \ldots, n$, the i-th row and the i-th column together contain all elements of S. Show that there is no silver matrix for $n = 1997$.

18. (Taiwan, 1995) Consider the operation which transforms the 8-term sequence $x_1, x_2, \ldots, x_8$ into the new 8-term sequence

$$|x_2 - x_1|, |x_3 - x_2|, \ldots, |x_8 - x_7|, |x_1 - x_8|.$$

Find all 8-term sequences of integers which have the property that after finitely many applications of this operation, one is left with a sequence, all of whose terms are equal.

19. There are 25 people sitting around a table, and each person has two cards. One of the numbers $1, 2, 3 \ldots, 25$ is written on each card, and each number occurs on exactly two cards. At a signal, each person passes one of her cards–the one with the smaller number–to her right-hand neighbor. Prove that, sooner or later, one of the players will have two cards with the same number.

20. For positive integers n, define S_n to be the minimum value of the sum

$$\sum_{k=1}^{n} \sqrt{(2k-1)^2 + a_k^2},$$

as the $a_1, a_2, \ldots, a_n$ range through all positive values such that

$$a_1 + a_2 + \cdots + a_n = 17.$$

Find S_{10}.