Problem Sets

Jim Carlson
University of Utah
File = ProblemSets2004.tex

Draft of May 29, 2004

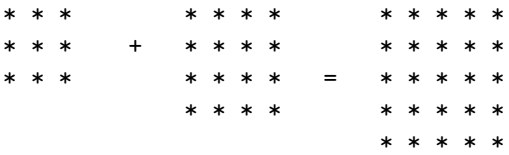
Contents

1 Puzzles

Many problems in number theory began as puzzles. Below are few of these. Try your wits against them! (*House rules: if you already know the answer, hold your fire and give your friends a chance to think about the problem.*)

1. Consider the two patterns of dots below. One pattern is square, the other triangular. Is it ever possible to rearrange a square pattern of dots into a triangular one?

2. Sometimes two square arrays of dots can be combined into a new square array of dots:



   Are there other examples like this?

3. Are there two cubical arrays of dots that can be merged to form another cubical array?

4. Consider a square array of dots, as in the figure below, but 100×100 rather than 5×5.

   How many dots are visible from the dot in the lower left corner?

5. (a) The robot R7L5 can only make two kinds of moves: seven units to the right or five units to the left. Is sequence of moves that take R7L5 one unit to the right of his current position? (b) The robot's friend, R6L4, want's to imitate him. Can R6L4 also move one unit the right by a clever choice of moves?

6. In the spring of the year 2004, just as Fred Dref graduated from high school, he observed a remarkable event. The seventeen year cicadas in his home town, which are green, and the eleven year cicadas, which are bright orange, emerged from the ground at the same time. Will Fred live to see this happen again? (b) Suppose that due to a mutation each kind of cicada has a period one year smaller. What are Fred's chances now? (c) Same question, but instead the mutation added a year.

7. Consider the puzzle in Figure 1 below. A legal move is to slide one "tile" horizontally or vertically into an empty square. Is there a sequence of moves that takes Figure 1 to Figure 2?

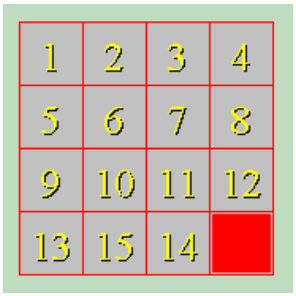


Figure 1: Start

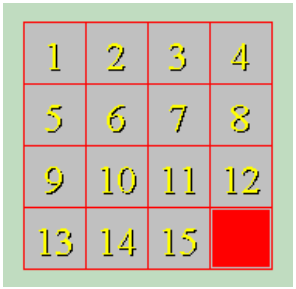


Figure 2: Finish

8. Consider a rectangular piece of paper R. Make one straight cut so that it falls into a square S and smaller rectangle R'. Is there a way of chossing the paper size so that R' is similar to R?

9. There are five regular solids: tetrahedron, cube, octahedron, icosahedron, dodecahedron. Make models of each. Are there any others?

10. Consider the figure below. Determine (quickly!) which points are inside and which are outside.

INSERT FIGURE

Try variations on the puzzles. For example, change the number of units of the (a) and (b) moves of the robot. Or change the number of units between the start and goal positions of the robot. Or change the geometry of the dot patterns. Etc. Try formulating your own problems.

2 Numbers and figures

Below are some problems about numbers and geometric figures. All are easy to state, but not all are easy to solve. Indeed, some are unsolved and others are unsolvable!

1. A number like 13 can be written as a sum of squares: $13 = 2^2 + 3^2$. Which of the following numbers can be represented as a sum of two squares? 125, 136, 177.

2. Three postive integers satisfying $x^2 + y^2 = z^2$ are called a *Pythagorean triple*. One example is 3, 4, 5. Find as many Pythagorean triples as you can, organize them into a table, and comment on any patterns you notice. Note: let's require that x, y, and z have no common factors. Such a triple is called *primitive*. Why is this a reasonable condition to impose?

3. Is there a right triangle with integer sides where the altitude has length 1?

4. Is there an equilateral triangle with integer sides? Is there an isosceles right triangle with integer sides?

5. Find some integer points (x, y) on the hyperbola $x^2 - 2y^2 = 1$. How many such points are there?

6. How many integer points lie on the related hyperbola $x^2 - y^2 = 1$?

7. What is the last digit of 7^{100}?

8. Find all prime numbers less than 50.

9. Consider the integer 200, 201, ... 219. Factor them into primes. Then try to factor the integers 12, 123, 1234, 12345, etc.

10. Is there a 100-digit prime number? If so, try to find one.

11. Can every even number bigger than 2 be expressed as a sum of two primes?

12. Prime numbers sometimes come in pairs, like 5 and 7 or 11 and 13. How many such "twin primes" are there?

13. Define $F_0 = 1$, $F_1 = 1$, $F_n = F_{n-1} + F_{n-2}$. Thus $F_2 = F_1 + F_0 = 2$. Find F_3, F_4 and F_5. Is there a formula for F_n in terms of n? About how big is F_{50}? This sequence of numbers is called the *Fibonacci* sequence. Do you notice anything about it? Any patterns? Are the patterns really true?

14. Select two positive integers at random. What is the probability that they are relatively prime? "Relatively prime" is math jargon for "have no factor in common."

15. What is the probability that a randomly chosen integer is not divisible by 2? What is the probability that it is not divisible by 3? What is the probability that it is not divisible by 2 and not divisible by 3?

One problem leads to an other. For example, problem 2 and the data we accumulate in studying it lead us to ask *which numbers are the the hypotenuse of a right triangle with integer sides*? It also leads to a fundamental question: how many primitive Pythagorean triplets are there?

We can also vary parameters. For example, in the problem about the hyperbola we can change the coefficients, considering equations like $x^2 - 2y^2 = 5$, $x^2 + y^2 = 5$, $x^2 - 13y^2 = 1$ or $x^2 - y^2 = 6$ or even $x^2 - 2y^2 = 0$. Formulate your own problems and investigate them.

An unsolved problem for which there is good evidence is called a *conjecture*. Would you call any of the above problems conjectures?

Library project. Find out about more about the Fibonacci series and report on it.

3 Even and odd

If a and b are both even or both odd, we say they have the same *parity*. Otherwise we say they have opposite parity.

1. Suppose a and b are even. What can you say about $a + b$, $a - b$, and ab? Same question for various combinations of even and odd. Organize your conclusions as a table.
2. Does the equation $12x + 23y = 1$ have an integer solution? What about $12x + 32y = 1$?
3. Suppose a^2 is even. What can you say about a?
4. Suppose a^2 is odd. What can you say about a?
5. Suppose $a^2 - b^2$ is even. What can you say about a and b?
6. Does the equation $x^2 = 2y^2$ have an integer solution?
7. Is the square root of two a rational number?

The parity of a number is determined by its *remainder mod 2*: the remainder left after long division of the number by 2. We can look at these remainders — also called *residues* — when dividing by another number. For now we'll concentrate on the number 4.

1. What are the possible residues mod 4 for positive integers?
2. What are the possible residues mod 4 of perfect squares?
3. Same question, but for sums of squares.
4. Is every number a sum of squares? What about the prime numbers?
5. Study the equations $x^2 - 7y^2 = 1$, $x^2 - 7y^3 = 3$. Do they have integer solutions? If so, how many?

Project. Study the family of equations $x^2 - 7y^2 = k$. For what k are they solvable in the integers? How many integer solutions do they have for fixed k?

4 Sums and number shapes

Let $t_n = 1 + 2 + 3 + \cdots + n$. This is the n-th *triangular number*. The numbers t_1, t_2, t_3, t_4 count the dots in the figures below:

One can imagine other number shapes – square, pentagonal, hexagonal. One can also imagine three-dimensional shapes, e.g., tetrahedral and pyramidal. And one can even go to higher dimensions!

1. Find a formula for t_n
2. Let $s_n = n^2$ be the n-th square number (think dots). Show, without using the formula for t_n, that $t_{n-1} + t_n = s_n$.
3. Find a formula for $t'_n = 1 + 3 + 5 + \cdots + (2n - 1)$.
4. Study the tetrahedral numbers T_n.
5. Study the pyramidal numbers P_n.
6. Study the pentagonal and hexagonal numbers.

Approaches: geometric, algebraic, guess pattern – then use induction, finite differences, linear equation – then use induction.

5 Sequences, limits, and infinite sums

Here are some sequences of integers:

```
(a) 2 4 6 8 10 ...
(b) 1 4 9 16 25 ...
(c) 1 2 4 8 16 32 ...
(d) 1 1 2 3 5 8 13 ...
(e) 2 3 5 7 11 13 ...
(f) 1 7 10 5 9 11 12 6 ...
(g) 171 29241 5826 27638 4134 10727 ...
(h) 1 1 2 2 3 3 ...
```

About them we can ask various questions. (i) What is the next term? (ii) How is the sequence defined? (iii) Is there a formula for the n-th term of the sequence? (iv) How does the sequence grow?

Here are some sequences of real numbers:

```
(i) 1.0 1.15 1.3225 1.5208 1.7490 2.0114 ...
(j) 1.0 1.4 1.41 1.414 1.4142 1.41421 ...
(j) 1.0 1.5 1.41666.. 1.41421568627 1.41421356237 1.41421356237
(k) 0.414213562373 0.828427124746 0.242640687119 0.656854249492
    0.0710678118655 0.485281374239 0.899494936612 0.313708498985
    0.727922061358 0.142135623731 ...
(l) 1.0 1.5 1.8333 2.0833 2.2833 2.4500 2.5926 2.7179 ...
(m) 1.0 0.5 0.8333 0.5833 0.7833 0.6167 0.7595 0.6345 0.7456 ...
(n) 0.0 0.5 0.3333 0.5 0.4 0.5 0.4286 0.5 0.4444 0.5 ...
```

For some of these sequence there exists a *limit*. Informally, this is a number L such that the n-th term of the sequence gets closer and closer to L. A good example is the sequence

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

What is the limit of this sequence? Well, it is clearly 2. This gives meaning to the relation

$$1 + \frac{1}{2} + \frac{1}{2^2} + \frac{1}{2^3} + \cdots = 2$$

The sum of an *infinite series* is the limit of its *partial sums* S_n.

Definition. The sequence $\{a_n\}$ has the number L as a limit if for all $\epsilon > 0$ there exists an N such that $|a_n - L| < \epsilon$ for $n \geq N$. In that case we write $\lim_{n\to\infty} a_n = L$.

6 Pythagorean triplets

Before starting this section you should prepare a table of primitive Pythagorean triplets a, b, c. Then look for patterns.

1. Let a, b, c be a Pythagorean triple. If a and b have a common factor, what can you say about c?
2. Let a, b, c be a Pythagorean triple. If a and c have a common factor, what can you say about b?
3. Do you notice anything about the parity of a, b, c for primitive Pythagorean triples? Can you prove that what you notice is true in general?
4. Write $a^2 + b^2 = c^2$ as $c^2 - b^2 = a^2$. Then factor it: $(c + b)(c - b) = a^2$. Study the factors. Do you notice anything? Can you prove that what you notice is true?
5. Suppose that the product of two numbers U and V is a perfect square. What can you say about U and V? Does it help if U and V are relatively prime?
6. Is there a formula for (primitive) Pythagorean triplets?
7. How many primitive Pythagorean triplets are there?

7 Pell's equation I

Pell's equation is the Diophantine equation $x^2 - Ny^2 = 1$.

1. Find ten solutions of $x^2 - 2y^2 = 1$.
2. Find a solution of $x^2 - 2y^2 = 1$ with $x > 10,000$.
3. Find one positive solution for each of the following: $x^2 - 17y^2 = 1$, $x^2 - 19y^2 = 1$, $x^2 - 91y^2 = 1$, $x^2 - 277y^2 = 1$.
4. The equation $x^2 - 2y^2 = 1$ can be factored as $(x + \sqrt{2}y)(x - \sqrt{2}y) = 1$. Thus solutions like $x, y = 3, 2$ correspond to "factors of 1" like $u = 3+2\sqrt{2}$ and $\bar{u} = 3 - 2\sqrt{2}$. Consider the numbers u^2, u^3, etc. Do they factor Pell's equation? Do they give solutions of Pell's equation?
5. Reconsider problem 2.
6. Let x_n, y_n be the n-th positive solution of Pell's equation. How would you define this? What can you say about the size of x_n or y_n as a function of n?
7. How many solutions does the Diophantine equation $x^2 - 2y^2 = 1$ have? Answer this question for the related equations $x^2 - 3y^2 = 1$ and $x^2 - 4y^2 = 1$. Can you formulate a general theorem about solvability of Pell's equation?
8. The *fundamental solution* of Pell's equation is the positive integer solution x, y where x and y are as small as possible. What is the fundamental solution of $x^2 - 2y^2 = 1$? What are the fundamental solutions of $x^2 - 14y^2 = 1$?
9. Find a number $S > 10,000$ which is both square and triangular. How many numbers are there that are both square and triangular?
10. Library project: find out about Archimdes' Cattle Problem and report on it.

8 Elliptic curves

An *elliptic curve* E is given by the equation $y^2 = x^3 + ax + b$. We shall assume a and b are integers. The main task is to understand the set $E(\mathbb{Q})$ of solutions (points) with rational coordinates. No general procedure for finding such points given a and b is known. However, if two such points are known, there is a method that can produce more rational points.

1. Consider the elliptic curve $E : y^2 = x^3 - 17$. Show that $P = (-2, 3)$ and $Q = (-1, 4)$ lie on E.
2. Let L be the line joining P and Q. Does it meet E in another point?
3. Find other rational points of E.
4. What rational points can you find on the elliptic curve $y^2 = x^3 + x$.
5. Same question for $y^2 = x^3$.
6. Graph the set of real solutions $E(\mathbb{R})$ for the elliptic curves above. Comment.

The theory of elliptic curves played a crucial role in Wiles' proof of Fermat's last theorem. It also plays an important role in cryptography.

9 Primes I

An integer $n > 1$ is *prime* if it cannot be factored into smaller numbers. Otherwise, it is called *composite*. The first significant result is found in Euclid's *Elements*, written around 300 BC: there are infinitely many primes. While we have learned much about the primes, many mysteries remain.

1. If it takes one nanosecond to divide one number into another, how long does it take to factor a 20-digit number using trial division? Repeat the analysis for 40-digit and 100-digit numbers. Finally, how long does it take to factor an n-digit number? Express your answer in terms of the number of digits.

2. Prove that if n has a nontrivial factor, then it has a nontrivial factor $a \leq \sqrt{n}$. Consider the previous problem in the light of this result.

3. Use the sieve of Eratosthenes to make a list of primes $p \leq 100$. Do you notice any patterns? Comment on these, and seek more evidence for them.

4. Let $\pi(x)$ denote the number of primes less than or equal to x. Graph this function for $x \leq 100$. Is there a formula, perhaps an approximate one, for this graph?

5. Find a 3-digit prime. Find primes with (a) 6 digits, (b) 10 digits, (c) 100 digits.

6. Study the values $f(1)$, $f(2)$, etc. for the polynomial function $f(n) = n^2 + n + 41$. What do you notice? What can you prove? What generalizations can you make?

7. Let $\pi(x)$ be the number of primes $p \leq x$. Is there an approximate formula for this function?

8. Let a positive integer be chosen at random. What can you say about the probability that it is prime?

9. Let p_n be the n-th prime. About how big is it as a function of n?

10. Write out from memory the proof that there are infinitely many primes.

11. Goldbach's Conjecture states that every even integer bigger than three can be written as sum of two primes. Is there evidence for this conjecture? Discuss.

12. Show that there are gaps in the primes that can be as large as you wish. More precisely, show that the numbers $n! + 2$, $n! + 3$, ..., $n! + n$ are composite.

13. Are there prime-free intervals of the form $[x, 1.1x]$? What about $[x, cx]$ for other values of $c > 1$?

14. Study the number of primes in the interval $[x, cx]$ for fixed $c > 1$.

The standard method for exchanging confidential information on the internet uses the RSA cryptosystem. Its ingredients are (a) the fact that it is easier to find very large prime numbers than it is to factor very large numbers into primes, (b) Fermat's little theorem about congruences modulo p.

10 Primes II

1. The *Prime Number Theorem* states that $\pi(x)$, the number of primes less than x, is approximately equal to $x/\log(x)$. Compare this approximation with $\pi(x)$ for $x = 100$, $x = 1000$, etc. How would you make the notion "approximately equal" precise?

2. The Prime Number Theorem was formulated by Gauss and finally proved (independently) by Hadamard and de la Valée Poussin. How did Gauss discover the formula $x/\log x$? The real answer is we don't know. However, we do know that from an early age Gauss was interested by the problem, and throughout his life he worked at tabulating more and more primes. Also, at an early age had a book which featured both a small table of primes and a table of logarithms. So he had two of the ingredients early on. It is natural when looking at data $\{(x, y)\}$ that span a great range to plot $\log y$ versus $\log x$. Below is data for $y = \pi(x)$. Make a log-log plot and think about the results. Can you "see" the Prime Number Theorem?

x	pi(x)
10	4
100	25
1000	168
10000	1229
100000	9592
1000000	78498

3. There is an even better version of the prime number theorem. It says that $\pi(x)$ is approximately the integral

$$\mathrm{li}(x) = \int_2^x \frac{dt}{\log t}$$

This integral is given by the asymptotic series

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

Use this series to computer $\pi(10^n)$ for various n. Comment on the accuracy of the approximation and on the number of terms used.

4. (Calculus) Derive the asymptotic formula.

5. (Calculus) Another way to compute $\mathrm{li}(x)$ is to use numerical integration, e.g., the trapezoidal rule or Simpson's rule. Explore these approaches. Use them to estimate the number of primes less than a billion.

6. The German mathematician Bernhard Riemann found even better approximations to the number of primes less than x. The first of these is the formula
$$\pi(x) \sim \mathrm{li}(x) - \frac{1}{2}\mathrm{li}(x^{1/2}).$$
The next is
$$\pi(x) \sim \mathrm{li}(x) - \frac{1}{2}\mathrm{li}(x^{1/2}) - \frac{1}{3}\mathrm{li}(x^{1/3})$$
What kind of results do these approximations give for the number of primes less than a billion? How do you think the pattern continues?

7. The Prime Number Theorem suggests that a randomly choose integer of magnitude n has about a $1/\log n$ chance of being prime. Suppose that for n odd you examine the sequence n, $n+2$, $n+4$, etc. How many terms do you need to inspect before having a 50-50 chance of finding a prime? To be precise, how many 100-digit odd integers do have to inspect to have an even chance of finding a prime?

8. The Twin Primes Conjecture states that there are infinitely many prime pairs p, $p+2$. Is there evidence for this conjecture? Discuss.

9. Twin primes have the form p, $p+2$. Can we extend this pattern to p, $p+2$, $p+4$? This is a short arithmetic progression of primes. How many such are there? What about arithmetic progressions with a different increment: p, $p+d$, $p+2d$? How long can such arithmetic progressions be?

11 Irrational numbers

A number is *rational* if it is a quotient of integers. Otherwise it is *irrational*. A number which satifisfies an algebraic equation with rational coefficients is called *algebraic*. Otherwise it is *transcendental*.

1. Express the following in decimal form: 1/7, 1/13, 712/321. Is the decimal expansion finite or eventually repeating?
2. Express the following as a fraction: $0.\overline{1213}$, $7.9\overline{1234}\cdots$. The part of the decimal expansion with a bar over it is repeated *ad infinitum*.
3. Prove that a number is rational if and only if its decimal expansion is either finite or eventually repeating.
4. Give an example of an irrational number.
5. Prove that the square root of two is irrational.
6. Prove that the square root of three is irrational.
7. Let $x_0 = 1$. Let x_{n+1} be the average of x_n and $3/x_n$. What happens to the terms of this sequence as n becomes large? Comment and generalize.
8. Prove that the cube root of two is irrational.
9. Show that the number $\sqrt{2} + \sqrt{3}$ is algebraic. Is it irrational?
10. What kind of number is the cube root of three?
11. Consider the polynomial $x^5 + x + 1$. Prove that it has a real root, which we shall call α. What kind of number is α?
12. Are there numbers which are not algebraic?
13. Study the sequence $x_n = \{n\sqrt{2}\}$. Here $\{x\}$ is the "remainder mod 1." For example, $\{3.1416\} = 0.1416$. In particular, examine the following question. Let y_n be the first digit of x_n to the right of the decimal point. Does it behave like a random sequence? You can study other sequences as well, e.g. the second digit or the first two digits. Look at the data in different ways, and other questions will come to mind. Is the behavior you see do to some special property of the number $\sqrt{2}$?

12 Divisibility

The *division algorithm* says that given positive integers a and b, there are integers q and r (the quotient and remainder) such that $b = aq + r$ where $0 \leq r < a$.

We say that a divides b if there is an integer q such that $b = aq$. In that case we write $a|b$, and we say that a is a divisor of b.

The *greatest common divisor* of a and b is the largest of the numbers that divide both a and b.

A positive integer p is prime if its only positive divisors are p and 1.

1. What are the quotient and remainder when we divide 112233 by 123?
2. How many divisors does $2 \cdot 3 \cdot 7 \cdot 11 = 693$ have? What about $2^2 \cdot 3^2 = 36$?
3. List all the divisors of 19481.
4. What is the greatest common divisor of 55 and 77? What is the greatest common divisor of 19481 and 286781?
5. List all the primes less than 100. Do you notice anything?
6. Factor the following numbers into primes: 12, 123, 1234, 12345, 123456, etc.
7. What are fast tests for divisiblity by 2, 3, 5, 9? Are there any other fast divisiblity tests? Why do they work?
8. Suppose a and b are divisible by three. What about $a + b$, $a - b$, and ab?
9. Suppose that ab is divisible by 3. What can you say about a and b?
10. Suppose that ab is divisible by 6. What can you say about a and b?

13 Euclidean algorithm

One way to find the greatest common divisor of two integers is to factor them into primes, then compare factors. However, there is a much better way, known to the Greeks at the time of Euclid (c. 350 BC).

> To find the greatest common divisor of a and b, first take away as many multiples of b as you can from a. If nothing remains, b is the greatest common divisor. Otherwise, let c be what remains. Then take away as many multiples of c as you can from b ... and so on.

Let us apply this algorithm, the *Euclidean algorithm*, to computing the gcd of 53 and 37, organizing our computations in the table below. In the table heading, `r` stands for remainder and `q` for quotient.

```
       a    b   r  q
       -------------
(1)   53  37  16  1
(2)   37  16   5  2
(3)   16   5   1  3
(4)    5   1   0  5
```

We stop when the remainder is 0. The gcd is the last nonzero remainder: it is 1.

1. Find the gcd of 321 and 123.
2. Find the gcd of 987654321 and 123456789.
3. Line (1) in the table above says that 37 goes into 53 once with a remainder of 16: $53 = 1 \cdot 37 + 16$. It can be rewritten as $16 = 53 - 1 \cdot 37$, which says *16 can be expressed in terms of 53 and 37*. Find similar interpretations for the other lines.
4. Can the gcd of 53 and 37 be expressed in terms of 53 and 37?
5. Solve the equation $53x - 37y = 1$.
6. Solve the equation $112x + 117y = 1$.
7. Solve the equation $2111x + 7111y = 1$.
8. Solve the equation $1122x + 1177y = 1$.
9. How does the number of steps needed to compute the gcd of a and b depend on a and b?

14 Congruences

We say that a and b are *congruent* modulo n if $a - b$ is divisible by n. In that case we write $a \equiv b \bmod n$

1. What are the numbers congruent to zero mod 2? What are the numbers congruent to one mod 2?
2. Describe the set of numbers $\{ x \mid x \equiv 2 \bmod 7\}$.
3. Find a positive number congruent to 23 mod 8 that is less than eight.
4. Find the smallest positive integer congruent to -11 mod 8.
5. Solve, where possible, the congruences $4x \equiv 3 \bmod 7$, $4x \equiv 3 \bmod 8$.
6. Solve the congruence $x + 4 \equiv 0 \bmod 7$. The solution is called a *additive inverse* mod 7. Do additive inverses always exist?
7. Solve the congrence $4x \equiv 1 \bmod 7$. The solution is called a *multiplicative inverse* of 4 mod 7. Do multiplicative inverses always exist?
8. Find the multiplicative inverse of 16 modulo 113.
9. Solve, where possible, the congruences $x^2 \equiv 3 \bmod 5$, $x^2 \equiv 4 \bmod 5$.
10. Is the following true? Explain. For all a, b, c, d, if $a \equiv b \bmod n$ and $c \equiv d \bmod n$ then $a + c \equiv b + d \bmod n$. Formulate similar statements for subtraction and multiplication. Are these statements true?
11. Suppose that $ax \equiv by \bmod n$. Is $x \equiv y \bmod n$?
12. Define a function $f(x) \equiv 59x \bmod 101$. Take for the result the *least positive residue*: the number congruent mod 101 to 59x that is nonnegative and less than 101. Define a sequence as follows: $x_1 = 1$; $x_{n+1} = f(x_n)$. Thus $x_2 = 50$, $x_3 = 76$, etc. What pattern do you see in this sequence?

15 Residues

The numbers 0, 1, 2, ..., $n-1$ form a *system of residues* modulo n. This means that very number is congruent mod n to exactly one of these residues. For example, mod 7 the system of residues is the set $\{ 0, 1, 2, \ldots, 6 \}$. The residue of 12345 is 4. We computed this by the division algorithm: 7 goes into 12345 a total of 1763 times leaving a remainder of 4. The residue, like the ring in the bathtub, is "what is left over."

Define addition of the residues a and b by forming the residue of the usual sum of a and b. Thus, mod 7, the sum of 4 and 5 is 2.

1. Construct the full addition table mod 7.
2. Does every residue mod 7 have an additive inverse? Make a table of additive inverses. Put "*" where one does not exist.
3. Explain how to define multiplication of residues. Find the multiplication table for the residues mod 7. Make a table of multiplicative inverses. Put "*" where one does not exist.
4. Does every residue have a multiplicative inverse?
5. Construct and study the arithmetic of residues for modulus 2, 3, 4, 5, 6. Can you form any general conclusions?
6. A residue is called *quadratic* if it is the square of another residue. Modulo 7, $3^2 \equiv 2$. Thus 2 is a quadratic residue. Find all quadratic residues mod 7. How many are there? Investigate the quadratic residues modulo other primes. Do you notice anything?
7. Which of these numbers are quadratic residues mod 13: 4, 5, 6?
8. Which of these numbers are quadratic residues mod 101: 50, 51, 52?
9. Define the "Legendre symbol" (a, n) to be 1 if a is a quadratic residue mod n, -1 otherwise. For a prime number p consider the sequence $(2, p)$, $(3, p)$, $(4, p)$, etc. It is a sequence of plus and minus ones. How does it compare to tossing a coin (plus one for heads, minus one for tails)? Does this question even make sense?

16 Cryptography I

A cryptosystem consists of a finite set $\mathbf{A}$ (the "alphabet"), and a pair of functions $f : \mathbf{A} \longrightarrow \mathbf{A}$, $g : \mathbf{A} \longrightarrow \mathbf{A}$. The functions f and g are inverses of eachother: for all x in $\mathbf{A}$, $g(f(x) = x$ and $f(g(x)) = x$. Example 1: Let $\mathbf{A} = \{ A, B, C, \ldots, Z \}$. Let

$$f(x) = \text{shift } x \text{ forward four places in the alphabet}$$

View the letters of the alphabet as arranged around a circle, so "shift forward" is really "shift clockwise." Thus $f(A) = E$ and $f(Z) = D$. Example 2: The alphabet is $\mathbf{A}' = \{ 0, 1, 2, \ldots, 25 \}$. We think of $\mathbf{A}'$ as being the same thing as $\mathbf{A}$, except that it is better suited to computation. The function $f(x) = x + 4 \bmod 26$ now plays the role of f.

Messages are encoded by applying f letter by letter. Thus $f(PAYNOW) = TECRSA$. Messages are decoded by applying the inverse function g. Turning to example 2, $PAYNOW$ corresponds to the sequence $15, 0, 24, 13, 14, 22$. The encoded version is $19, 4, 2, 17, 18, 0$.

1. Let the alphabet and the encoding function be as in example 1. What is the decoding function? Decode the message $SOFSWW$.

2. Let the alphabet and encoding function be as in example 2. What is the decoding function? Decode the message $17, 18, 0, 4, 2$.

3. Let the alphabet be as in example 2, but let the encryption function be $f(x) \equiv 7x \bmod 26$. Encrypt the message "MONDAY." Decrypt the message MUKYUN.

4. Encrypt the message $ATTACK$ using $f(x) = 5x \bmod 26$. What is the decryption function.

5. Bigger alphabets give somewhat better security, including better defense against statistical attacks. One way to make a bigger alphabet is to consider pairs from a given alphabet. Thus $ATTACK$ is broken up as AT, TA, CK. Its numerical counterpart is the sequence of vectors $(0, 19)$, $(19, 0)$, $(2, 10)$. We can encrypt using matrices, e.g.,

$$f(x_1, x_2) = (x_1, x_2) \begin{pmatrix} 4 & 1 \\ 3 & 3 \end{pmatrix}$$

   Encrypt the message $ATTACK$ using this matrix and comment on the result. Decrypt the message $QCRBNB$. Comment on the results.

17 Modular powers

Let us compute $71^{101} \bmod 107$. To this end, first write 100 as a sum of powers of two: $101 = 64 + 32 + 4 + 1$. Then compute the following powers:

$$71^2 = 5041 \equiv 12 \bmod 107$$
$$71^4 \equiv 12^2 \equiv 144 \equiv 37 \bmod 107$$
$$71^8 \equiv 37^2 \equiv 1369 \equiv 85 \bmod 107$$
$$71^{16} \equiv 85^2 \equiv 7225 \equiv 56 \bmod 107$$
$$71^{32} \equiv 56^2 \equiv 3136 \equiv 33 \bmod 107$$
$$71^{64} \equiv 33^2 \equiv 1089 \equiv 19 \bmod 107$$

Then

$$71^{101} \equiv 71^{64} \cdot 71^{32} \cdot 71^4 \cdot 71^1 \equiv 19 \cdot 33 \cdot 37 \cdot 71 \equiv 1647129 \equiv 78 \bmod 107$$

By repeated squaring and reducing mod N, we compute $71^{101} \bmod 107$ very efficiently using only small numbers. By contrast, 71^{101} is the 97 digit number below:

```
94862206168070821305954036946776446945298116937707818176786439552151797964934722932773425874270664687652004548893432210230582916384212908377589280798702736505275723857030629901600164520 71
```

Let's now put our new tools to use:

1. Compute $84^{123} \bmod 160$.
2. Compute $12345^{54321} \bmod 100003$. (Before you start: how many digits does the integer 12345^{54321} have?
3. Compute $2^{16} \bmod 17$ and $5^16 \bmod 17$. What do you notice?
4. Compute $6^{100} \bmod 101$ and $88^{100} \bmod 101$. What do you notice?
5. The *order* of a modulo N is the least positive integer k such that $a^k \equiv 1 \bmod N$. What is the order of 2 mod 23? What are the orders of the other elements mod 23? Do you notice anything?

18 Fermat's little theorem

Fermat's little theorem states that if p is a prime and p does not divide a, then

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

We explore why this theorem is true, what it is used for, and how it can be generalized.

1. Verify that $2^6 \equiv 1 \bmod 7$ and that $3^{100} \equiv 1 \bmod 101$.
2. Compute $2^{122} \bmod 123$. What does the result tell you about the number 123?
3. Compute $2^{126} \bmod 127$. What does this tell you about the number 127?
4. Compute $2^{1234566} \bmod 1234567$. What does the result tell you about 1234567?
5. Find a 100-digit number that is "probably prime."
6. Estimate the probablity that a number $n \leq N$ passes Fermat's test $2^{n-1} \equiv 1 \bmod n$ but is not prime. Do this for $N = 100, 1000, 10000, 100000$.
7. Can we improve Fermat's test to reduce (or eliminate) the possibility of accepting a number that is prime which is not really prime?
8. Suppose that we have an independent sequence of probabilistic primality tests: the probabilty that $T_n(x)$ accepts x as prime and x really is prime is 3/4. How many such tests must we apply to ensure that x is prime with probability 10^{-9}?
9. Solve the following congruences (a) $x^3 \equiv 8 \bmod 17$, (b) $x^5 \equiv 21 \bmod 823$
10. Consider the sequence of numbers $S = \{ 1, 2, 3, \ldots, 10 \}$. Compute the set of numbers $S' = \{ 2 \cdot 1, 2 \cdot 2, 2 \cdot 3, \ldots, 2 \cdot 10 \}$, where the products are taken mod 11. What do you notice about the numbers S'? Compute the product of all the numbers in S' in two different ways: first take the product then reduce mod 11. Then reduce mod 11 and take the product. Compare the two results. Do you find anything interesting?

Recall that if functions $f : S \longrightarrow S$ and $g : S \longrightarrow S$ satisfy $g(f(x)) = x$ and $f(g(x)) = x$ for all x, we say that f and g are *inverse* functions — one undoes what the other does.

1. What is the inverse function of $f(x) = x^3 \bmod 17$?
2. What is the inverse function of $f(x) = x^5 \bmod 823$?

Inverse functions are good for solving equations like $f(x) = a$. For then $x = g(a)$. However, does every function have an inverse? Discuss.

19 Euler's phi function

Let $\phi(n)$ be the number of integers k in the range $1 \leq k < n$ which are relatively prime to n. This is the *Euler phi function*.

1. Compute $\phi(5)$, $\phi(6)$, $\phi(7)$, and $\phi(8)$.
2. Let p be a prime. What is $\phi(p)$?
3. If p is a prime, what is $\phi(p^2)$? Can you generalize this?
4. If a and b have no common factors, then $\phi(ab) = \phi(a)\phi(b)$. (A function with this property is called *multiplicative*. Use this fact to compute $\phi(319)$.
5. Is the formula $\phi(ab) = \phi(a)\phi(b)$ true if a and b have a factor in common?
6. Euler generalized Fermat's little theorem as follows: if a and n have no factors in common, then $a^{\phi(n)} \equiv 1 \bmod n$. Explain why this is a generalization. Give a numerical example of the theorem.
7. Solve the congruence $x^3 \equiv 8 \bmod 187$. That is, find the cube root of 8 modulo 187.
8. Let $f(x) = x^3 \mod 187$. Find the inverse function of f.

Hint for proving that ϕ is multiplicative: arrange the numbers $1, 2, \ldots ab-1$ in a rectangle.

20 Cryptography II

The RSA cryptosystem uses an encryption function of the form $f(x) = x^a \bmod N$, where N is the product of two large primes p and q. The decryption function has the form $g(x) = x^b \bmod N$ for a suitable exponent b. The number b satisfies the congruence

$$ab \equiv 1 \bmod \phi(N).$$

If Alice wants to use RSA, she generates p, q, and a, where a is relatively prime to $p-1$ and $q-1$. Then she solves the above congruence to find b. Finally, she publicly announces the numbers N and a. That way Bob, or anyone else for that matter, can send secret messages to Alice. However, Alice is the only one who can read the messages, since only she knows b, which she has kept secret. Now Carla comes on the scene. She has intercepted a message from Bob, and she knows how to find b: just factor N to find p and q. Then she will know $\phi(N) = (p-1)(q-1)$ and so the equation for b. That equation is easy to solve. But why is Alice confident that Carla will fail?

In our first set of exercise, which are just warmups, Bob sends numbers to Alice. But he encrypts them first.

1. Let $p = 101$, $q = 103$, $a = 7$. Bob's plaintext is 61. What is the ciphertext that he sends to Alice?

2. Let p, q, a be as above. Alice received the ciphertext 99. What is the plaintext?

3. Why is the rule for computing b correct?

Now we will do something more realistic. First, text (capital letters, no spaces, nothing else) will be transformed into numbers using the dictionary below:

```
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
```

Consider, for example, the message THIS IS A TEST. Running all the letters together and then translating into numbers we find 3018192919291139152930. We'll then break this big number into eight digit chunks: 30181929 19291139 152930. Of course there is a small chunk left over, but this is OK. Alice has already generated two primes bigger than 36363636. These are $p = 38121509$ and $q = 88121507$. As her encryption exponent she has chosen $a = 7$. She gives Bob the information $(a, N) = (7, 3359324822194063)$. He uses this to encrypt THIS IS A TEST.

1. What ciphertext does Bob send to Alice for the plaintext THIS IS A TEST?

2. What decryption function does Alice use?

3. Alice has received the message 3108700497252621, 202239027630196, 2561624985828275, 1654717133283408. What is Bob trying to tell her?

4. Work in pairs: one will be Alice, one will be Bob. Then switch roles and repeat. Alice: construct two primes p and q at least eight digits long, and compute N. Select a suitable encryption exponent a. Tell Bob a and N. Bob will make encrypt a message and send it to Alice. Alice will decrypt. Later, she and Bob meet and compare notes to see if the encryption is correct.'

5. Let Eve and Fred be a second pair. They gain access to Bob's ciphertext and Alice's public code (a, N). Bad people that they are, they try to decrypt Bob's message to Alice.

6. Repeat the previous two exercises with much larger primes.

7. Must one take special care with the choice of primes, or can any old primes do, so long as they are big enough?

21 Primitive elements and discrete logarithms

The *order* of an element a modulo p is the least positive k such that $a^k \equiv 1 \bmod p$. We write $\mathrm{ord}(a)$ for this integer. For example, modulo 11, $ord(2) = 10$ and $ord(3) = 5$. (Check this).

A *primitive element* modulo p is an element of order $p - 1$. It is a theorem that a primitive element always exists. Finding them is another matter.

Consider the congruence $b^k \equiv a \bmod N$. The number k is called the *base b logarithm of a modulo N*, or sometimes just the *discrete logarithm* of a. For example, $\log_3 5 = 8 \bmod 11$. (Verify this).

1. Make a table of the orders of elements mod 11. What do you notice? Make similar tables for other moduli. What do you notice?
2. What are the primitive elements mod 11? How many of them are there? If an integer mod 11 is chosen at random, what is the probability that it is primitive?
3. If an element mod p is chosen at random, what is the probabiity that it is primitive.?
4. Find $\log_2 7 \bmod 23$.

Whereas there a fast algorithms to compute powers mod N, there a there are no fast algorithms to compute discete logarithms (unlike usual logarithms). This is the basis for the fact that discrete logarithms are used in cryptography. See [7].

22 Continued fractions

A continued fraction is an expression like

$$4 + \cfrac{1}{2 + \cfrac{1}{7 + \cfrac{1}{3}}}$$

Note that the numerators are all equal to 1. A more compact notation for the above continued fraction is [4; 2, 7, 3] or just [4,2,7,3].

It is obvious continued fraction can be converted into a simple fraction. The simple fraction of [4;2,7,3] is 210/47. Less obvious, but also true, is that a simple fraction can be converted into a continued fraction. Irrational numbers have infinite continued fraction expansions.

1. Find the simple fraction of $[1; 2, 3, 4]$.
2. Find the continued fraction of 103/99.
3. Write down the Euclidean algorithm table for the gcd of 103 and 99, as in the problem set on the Euclidean algorithm. Compare that table to the continued fraction expansion of 103/99. Do you see where the continued fraction comes from?
4. Compute the continued fraction expansion of 54322/12345.
5. The *convergents* of a continued fracton $[a_0; a_1, a_2, \ldots]$ are the continued fractions $[a_0]$, $[a_0; a_1]$, $[a_0; a_1, a_2]$, etc. Find the simple fractions of the convergents of $[1; 2, 3, 4]$.
6. The "next to the last convergent" of the continued fraction expansion of a/b gives a solution to the Diophantine Equation $ax - by = 1$. For example, the continued fraction of 210/47 is [4,2,7,3]. The next to the last convergent is [4,2,7]. Its simple fraction is 67/15. And $x, y = 15, 67$ solves $210x - 47y = 1$. Use this observation to solve $54322x - 12345y = 1$.
7. Find the continued fraction expansion of 1.4142135623730951.
8. Find the continued fraction expansion of $\sqrt{2}$. What are its first six convergents?
9. Investigate the continued fractions of square roots of integers.
10. Investigate the continued fractions of other numbers.

23 Pell's equation II

We will try to solve more challenging cases of Pell's equation, beginning with some warm-up problems.

1. Compare the convergents of $\sqrt{2}$ with the solutions of Pell's equation, $x^2 - 2y^2 = 1$.
2. Compare the convergents of $\sqrt{19}$ with solutions of $x^2 - 19y^2 = 1$. Can you formulate a general principle?
3. Compare the convergents of $\sqrt{29}$ with solutions of $x^2 - 29y^2 = 1$. Can you still formulate a general principle?
4. Find a fundamental solution of $x^2 - Ny^2 = 1$ for $N = 91$. Do the same for $N = 277$.

We define the *size* of a fundamental solution x, y of $x^2 - Ny^2 = 1$ to be the ratio of the number of digits of x to the number of digits of N.

CONTEST: *A prize of $10 plus one mathematics book* will be awarded to the person who finds the largest fundamental solution. To qualify, the solver must explain in both written and oral form how the solution was obtained.

24 Flipping coins

1. We will run a little experiment. A coin is tossed repeatedly. We record a the sequence of heads (H) and tails (T) that appear. Let H_n be the number of heads that have appeared in n trials. Let $F_n = H_n/n$ be the average number of heads per trial — the relative frequency of heads. Graph H_n and F_n for a sequence of 100 trials. What do you expect happens to the quantity F_n as n becomes larger and larger? Comment on the meaning of the statement "the probability of heads is 1/2." Examine your data. Does it look random? Any surprises? (It is a good idea to continue the experiment for much larger values of n).

2. Let us run our experiment again, but in a slightly different way. I begin with \$10. Each the coin is flipped, I gain or lose a dollar: gain for heads, lose for tails. If my balance becomes zero, The game stops. What is my expected fate?

3. We'll run the game in yet a different way. A random walker starts at the origin on the x axis. Each time the coin is flipped, he moves one unit to the left or right: right for heads, left for tails. After 100 random steps, where is our walker?

4. Let a coin be tossed four times. List the possible outcomes. What is the probability of each?

5. Let a coin be tossed 100 times. How many possible outcomes are there?

6. What is the probability that when a coin is tossed four times, heads appears each time? What is the probability that there are exactly 2 heads?

7. Let $P(k)$ be the probability that when a coin is tossed four times, k heads appear. Make a table of the function $P(k)$.

8. Repeat the preceding problem but with ten coin tosses. Can you compare with experiment?

9. We will run another little experiment. In each trial you will flip a coin 4 times, recording the total number of heads. Do this 20 times. Make a graph of the frequencies with which each outcome occurs. Repeat 20 more times and make the same graph. Then put the two data sets together and construct a new graph based on 40 trials. Comment on the results.

10. (a) Toss a coin twenty times. What is the probability that ten heads appear? (b) Toss a coin forty times. What is the probability that twenty heads appear? (c) Continue this theme, and comment.

Since $n!$ is very large even for modest values of n, Stirling's formula,

$$n! \sim \sqrt{2\pi} n^{n+1/2} e^{-n},$$

is often a useful approximation.

25 What is random?

Consider the following sequences of twenty 0's and 1's:

```
A: 0 0 0 1 0 1 1 1 1 1 1 0 1 0 0 0 0 1 1 0   (10 one's)
B: 1 0 1 0 1 0 0 0 0 1 0 1 0 1 0 1 1 1 1 1   (11 one's)
C: 0 1 1 0 1 1 1 1 0 1 0 1 0 1 1 0 0 1 0 1   (12 one's)
D: 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0   (10 one's)
E: 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0   (0  one's)
```

Which of them do you think were likely to have been generated by flipping a coin (1 for heads, 0 for tails)?

1. Can one formulate tests which should be passed by random sequences? In other words, how would one certify that a random number generator is operating properly?

2. Let $\{x\}$ denote the "remainder mod 1" of x. For example, $\{3.1416\} = 0.1416$. Let x_n be the digit to the right of the decimal point in $\{n\sqrt{2}\}$. Does this sequence behave like a random one?

3. Let $f(x) = 171x \bmod 30269$. Define a sequence of numbers by $x_0 = 1$, $x_{n+1} = f(x_n)$. Does this sequence behave like a random one (after a while, anyway)?

4. Define a sequence of numbers as follows. First, set $x, y, z = a, b, c$ for some seed values a, b, c. Let

   $$w = \{x/30269.0 + y/30307.0 + z/30323.0\}$$

   where $\{x\}$ is x modulo 1, as above. Repeatedly apply the substitutions

   $$x \leftarrow 171x \bmod 30269, \quad y \leftarrow 172y \bmod 30307, \quad z \leftarrow 170z \bmod 30323$$

   and compute w as above. Does the sequence of w's behave like a random one?

5. A pseudorandom number generator based on repeatedly applying a function $f(x) = ax \bmod n$ is called a *linear congruential generator*. What number-theoretic properties must a and n satisfy for it to be a good generator?

Pseudorandom numbers have many applications, including computer games and the computations of areas, volumes, and high-dimensional integrals. We describe one such computation, a computation of π by the Monte Carlo method:

Generate a sequence of random numbers $P_k = (x_k, y_k)$ where $|x_k| \leq 1$ and $|y_k| \leq 1$. Let H_n denote the number of points P_k for $k \leq n$ that lie in the unit circle: $x_k^2 + y_k^2 \leq 1$. (Think of throwing darts at the unit circle, which sits inside a 2×2 square. The number H_n is the number of "hits" in n throws.) Study the sequence of numbers $F_n = H_n/4$ as n gets larger and larger.

26 The Fibonacci sequence

Mathematics abounds in fascinating sequences, e.g.

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, \ldots\ldots \quad (1)$$

and

$$1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, \ldots \quad (2)$$

We will study a few of the second of these sequence, the *Fibonacci sequence*.

1. What is the next term in the sequence? What is the general rule for constructing the Fibonacci sequence?
2. Solve the Diophantine equation $89x + 55y = 1$. What do you notice? Is this part of a pattern? Can you prove that the pattern holds in general?
3. Do you notice anything interesting about successive pairs of Fibonacci numbers F_n, F_{n+1}? Can you prove that your observation is correct?
4. Study the ratio F_{n+1}/F_n as n becomes large.
5. What can you say about the rate at which the terms in the Fibonacci sequence grow?
6. About how big is F_{100}?
7. Consider the much simpler sequence defined by $x_0 = u$, $x_{n+1} = ax_n$. Can you find a general formula for x_n? Is there any way of taking this as a hint for a general formula for the Fibonacci series?

Library project. Learn more about the history and applicability of the Fibonacci sequence. Who was Fibonacci? When did he live? What did he do?

27 Eight classics

Why prove a theorem? First, to be certain that it is true. A proved theorem is an enduring truth and a solid foundation on which to build new knowledge. Consider the durability and influence of the mathematics in Euclid's *Elements*, written around 300 BC in Alexandria. Second, and just as important, a proof gives insight. We want to know not only that a given result is true, but *why* it is true. That is reason enough. But understanding is also a tool to make further progress.

Below are seven theorems, each a milestone in the progress of mathematical knowledge, each part of our shared intellectual heritage. Learn them thoroughly: learn the statement, go over the proof until it becomes second nature. Each is a model of tight and elegant mathematical reasoning.

Theorem 1 *For a right triangle, the square of the hypotenuse is equal to the sum of the squares of the opposite sides.*

Theorem 2 *A triangle inscribed in a circle is a right triangle.*

Theorem 3 *There are infinitely many prime numbers.*

Theorem 4 *The square root of two is irrational.*

Theorem 5 *The series* $1 + 1/2 + 1/3 + 1/4 + \cdots$ *diverges.*

Theorem 6 *The set of rational numbers is countable.*

Theorem 7 *The set of real numbers is uncountable.*

Theorem 8

$$1 + \frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{4^2} + \cdots = \frac{\pi^2}{6}$$

Exercise. Thoroughly learn and understand these theorems and their proofs.

28 Areas

Let $f(x)$ be a function which is positive on the interval $[a, b]$. The *integral* of f on this interval, is the area under the graph, as in the figure below:

INSERT FIGURE

We write this as

$$Area = \int_a^b f(x)dx.$$

If the graph of f is a straight line, then the figure is a triangle or trapezoid, and so the integral can be computed via elementary geometry. One has

$$\int_a^b f(x)dx \sim (f(a) + f(b))\frac{b-a}{2}.$$

(What is $\int_1^2 xdx$?) If the graph is more complicated, we can break the interval $[a, b]$ up into n subintervals and add up the areas of the n trapezoids.

INSERT FIGURE

This gives an approximate value of the integral. To get a better approximation, use more and smaller subintervals.

1. Compute $\int_1^2 x^2 dx$.
2. Compute $\int_1^2 \frac{dx}{x}$. By definition this integral is $\log 2$, where the logarithm is the natural one.
3. Compute $\int_2^{100} \frac{dx}{\log x}$ Recall that this integral is by definition $li(100)$. By the prime number theorem it is an approximation to the number of primes less than 100.

Still better approximate computations of integrals are given by *Simpson's rule*. The idea is that if $a < b < c$ are equally spaced points, then the formula

$$\int_a^c f(x)dx \sim (f(a) + 4f(b) + f(c))\frac{c-a}{6}$$

is a good approximation.

Projects. (1) Redo the above problems using the new approximation. (2) Estimate the number of primes less than 1000 and compare with the actual value. (3) Estimate the number of primes less than a billion. It will help to break the integral up into subintervals [2,4], [4, 8], [8, 16], etc. On intervals of this form the function $1/\log(x)$ varies slowly and so few subintervals are needed in Simpson's rule are needed to get accurate results. (4) An even better approximation to the number of primes $\pi(x)$ less than or equal to x is given by

$$\pi(x) = \text{li}(x) - \frac{1}{2}\text{li}(x^{1/2}) - \frac{1}{3}\text{li}(x^{1/3})$$

Revise your computation of the number of primes less than a billion using this approximation. The improved formula is due to the German mathematician Bernhard Riemann.

29 Finding roots

Consider the problem of finding a real root of a polynomial $f(x)$ with real coefficients, e.g., $f(x) = x^3 + x - 27$. One approach is to use the *bisection method*. Choose two numbers $a < b$ where $f(a)$ and $f(b)$ have different signs. Then there is a root between a and b. (Why?) Now let $m = (a + b)/2$ be the midpoint of the interval $[a, b]$. Compare the signs of $f(a)$, $f(m)$ and $f(b)$ to determine on which of the two subintervals $[a, m]$, $[m, b]$ there is a sign change. Replace $[a, b]$ by the subinterval on which the sign changes. Repeat this process until the endpoints are close enough together. You have now located a root somewhere between a and b.

In the problems below you are asked to find roots of various equations and congruences.

1. Use the bisection method to find the square root of two. Compare with other methods you know.

2. Find a root of $x^3 + x - 27$ accurate to within 0.01. How does this root compare with the real root of $x^3 - 27$. Comment. Is the real root of $x^3 + x - 27$ rational or irrational?

3. Find a positive solution to the equation $2 \sin x = x$.

4. Explain why a polynomial of odd degree has at least one real root. Is the same true of polynomials of even degree?

5. Is the following number the square root of 13 modulo $10^{100} + 267$?

   ```
   3016889423070531962876260796686126874 8
   1091985115020756088100025381819333883 9
   2661711612351469494342 06
   ```

6. Solve the following congruences (a) $x^2 \equiv 11 \mod 127$, (b) $x^2 \equiv 3 \mod 325343$, (c) $x^2 \equiv 7 \mod 10^{100} + 267$.

30 A beautiful identity

Leonhard Euler (1707-1783) proved many beautiful formulas. Here is one of them:

$$\frac{\pi^2}{6} = 1 + \frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{4^2} + \cdots \tag{3}$$

How did Euler discover this amazing formula? His starting point was the infinite series for the sine:

$$\sin x = x - \frac{x^3}{3!} + \frac{x^5}{5!} \pm \cdots \tag{4}$$

The sine function of course, cannot be represented by a polynomial (why?) but it can be represented by a polynomial of infinite degree:

$$g(x) = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \cdots \tag{5}$$

To find the zeroth coefficient, set $f(x) = \sin x$ and compare $f(0) = 0$ with $g(0) = a_0$. Thus $a_0 = 0$. To find the first coefficient, compare $f'(0) = 1$ with $g'(0) = a_1$ Thus $a_1 = 1$. To compute the n-th coefficient, we compare the n-th derivatives of f and g evaluated at the origin.

Now a polynomial $p(x)$ of degree d can also be written as a product

$$p(x) = C(x - r_1)(x - r_2) \cdots (x - r_d), \tag{6}$$

where the r_i are the roots. Proceeding by analogy, used the fact that the sine function has roots at $n\pi$ for all integers n to write the factorization:

$$\sin x = Cx \left(1 - \frac{x^2}{\pi^2}\right) \left(1 - \frac{x^2}{4\pi^2}\right) \left(1 - \frac{x^2}{9\pi^2}\right) \left(1 - \frac{x^2}{16\pi^2}\right) \cdots \tag{7}$$

He also argued that $C = 1$ — we will leave this part to you.

Finally, Euler compared the coefficient of x^3 in the infinite sum for the sine with the coefficient of x^3 in the multiplied-out infinite product. We will also leave this part to you.

Problem. What formula do you get when you compare the coefficients of x^5 in the sum and product? What other formulas can you find?

Note. Here are some other formulas relating π to infinite series:

$$\frac{\pi^2}{8} = 1 + \frac{1}{3^2} + \frac{1}{5^2} + \frac{1}{7^2} + \cdots$$

$$\frac{\pi}{4} = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} \pm \cdots$$

One way to prove/discover these is to use Fourier series.

31 History of Mathematics

The history of mathematics — mathematics as known from written documents — begins around 3000 BC in Sumeria (present-day Iraq). From that period we have accounting records written on clay tablets in a base 60 system. By 1800 BC in Babylon techniques of calculation had already reached a high level of sophistication. One tablet from that period shows a square with in inscribed diagonal, the square root of two written out to three base-sixty (sexagesimal) places. (What is the equivalent decimal accuracy?) See Neugebauer [5].

A completely different kind of mathematics, with geometry as its focus, arose in Greece beginning perhaps as early as 600 BC. By 300 BC Greek geometry was codified by Euclid in his *Elements* [3]. This founding document was written in Alexandria, in present-day Egypt. At that time Alexandria was the center of scholarship and research. The Greek school introduced the world to the notion of logical proof. Among the specific methods of proof was *contradiction*, used, for example, to show that the square root of two is irrational and that there are infinitely many primes. The Greeks also introduced the idea systematically organizing a body of mathematical knowledge via definitions, axioms, and theorems.

Another milestone in mathematics is the work of Ptolemy, also in Alexandria, around 150 BC. His book the *Almagest* is a work of mathematical astronomy based on the idea that the motion of celestial bodies can be described by a a nested system of uniformly rotating circles. Though not a correct representation of the reality of these motions, Ptolemy's methods were sufficient to make some rather accurate predictions of astronomical phenomena, e.g., when Jupiter would appear at the zenith at midnight (opposition). As part of his work, which required spherical trigonometry, Ptolemy compiled very accurate trig tables. Of course Ptolemy regarded the Earth as a sphere, and even compiled a work, the *Geography* in which cities known to him were listed with latitudes and longitudes. The latitudes, which can be easily measured by measuring the angle between the horizon and the pole star, were rather accurate. The longitudes, which require accurate measurement of time, were very poor. This one reason why Columbus, who owned a copy of the *Geography*, thought that India was much closer to Europe as one sails west than it actually is.

In a short space one can say little about the long history history of mathematics. Thus we will conclude with a list of names, topics, and references for those who wish to learn more. In many cases we will just give a name. The reader can begin his or her research by using that names as a search key for Google or the web site

www-gap.dcs.st-and.ac.uk/~history/BiogIndex.html.

However, to go into any significant depth, one will have to read books. Consult your local library!

Names

1. 600 BC – 300 AD. Appolonius, Archimedes, Eratosthenes, Euclid, Ptolemy, Pythagoras, Thales, Zeno.

   Who was he? When did he live? What language did he speak, and in what language did he write? For what is he best known? Other questions ... these will come to you as you read.

2. 300 AD – 1000 AD. al-Battani, al-Kindi, al-Khwarizmi, Bhaskara I

3. 11th Century. Khayyam

4. 12th Century. Bhaskara II, Fibonacci

5. 13th Century. Al-Tusi, al-Maghribi, Li Zhi

6. 14th Century: Oresme

7. 15th Century. Copernicus, Regiomantus, Scipio del Ferro,

8. 17th Century. Barrow, Fermat, Newton, Wallis

9. 18th Century. Euler, Gauss, Lagrange, Laplace

10. 19th Century. Cantor, Chebyshev, Dirichlet, Fourier, Hilbert, Klein, Noether, Poincaré, Riemann.

11. 20th Centry. Gödel, Noether, Turing .

32 Unsolved problems

1. Does the function $f(n) = n^2 + n + 41$ take infinitely many prime values? Same for $g(n) = n^2 + 1$.

33 Notes

Stuff to do

Prob, stat: fairness tests

Sequences

Special primes

Density

Python's random number generator

```
# Wichman-Hill random number generator.
#
# Wichmann, B. A. & Hill, I. D. (1982)
# Algorithm AS 183:
# An efficient and portable pseudo-random number generator
# Applied Statistics 31 (1982) 188-190
#
# see also:
#        Correction to Algorithm AS 183
#        Applied Statistics 33 (1984) 123
#
#        McLeod, A. I. (1985)
#        A remark on Algorithm AS 183
#        Applied Statistics 34 (1985),198-200

# This part is thread-unsafe:
# BEGIN CRITICAL SECTION
x, y, z = self._seed
x = (171 * x) % 30269
y = (172 * y) % 30307
z = (170 * z) % 30323
self._seed = x, y, z
# END CRITICAL SECTION

return (x/30269.0 + y/30307.0 + z/30323.0) % 1.0
```

References

[1] Davenport, the Higher Arithmetic.

[2] G.J.O. Jameson, The Prime Number Theorem, London Mathematical Society Student Texts 53, Cambridge University Press 2003, pp 252.

[3] *Euclid's Elements*, Sir Thomas Heath, Dover, three volumes.

[4] Lenstra's article on Pell's equation in the *Notices*.

[5] The Exact Sciences in Antiquity.

[6] R.L. Rivest, A. Shamir, and L. Adelman, A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. 1977

[7] Joseph Silverman, A Friendly Introduction to Number Theory, 2nd Edition, Prentice-Hall (2001), pp. 386.

[8] Stopple, XX

[9] . A. Wichmann, B. A. and I.D. Hill, Algorithm AS 183: An efficient and portable pseudo-random number generator Applied Statistics 31 (1982) 188-190. see also: Correction to Algorithm AS 183, Applied Statistics 33 (1984) 123, and A. I. McLeod, A remark on Algorithm AS 183 Applied Statistics 34 (1985),198-200