EXPLORING NUMBER THEORY

EXPLORING NUMBER THEORY

Hugh L. Montgomery

University of Michigan, Ann Arbor

2004

Copyright © 2004 by Hugh L. Montgomery. All rights reserved.

Typeset by $\mathcal{A}\mathcal{M}\mathcal{S}$-TEX

Reproduction or translation of any part of this work beyond that permitted by Sections 107 and 108 of the 1976 United States Copyright Act without the permission of the copyright owner is unlawful. Requests for permission or further information should be addressed to Hugh L. Montgomery, Department of Mathematics, University of Michigan, Ann Arbor, MI 48109–1109, or by internet email to hlm@umich.edu.

Preface

Many of the programs listed in Appendix P were written first to support instruction in a standard junior–senior level number theory lecture course. In 1993, Don Lewis suggested that such programs could also be used in a Freshman Seminar in which the students would discover the patterns and work out the theory for themselves. By developing their ability to conjecture and prove, students learn to think like mathematicians. At the same time, they acquire mathematical literacy, develop their problem-solving abilities, become comfortable using a computer as an exploratory tool, and learn to participate in group efforts. By having developed their skills of quantitative reasoning, such students are better able to make the most of subsequent mathematical activities. After an initial investment from the College of Literature, Science and the Arts, the course was offered first in 1993–1994, and has run every year since. Although officially billed as a Freshman Seminar, students at all levels have elected the course, and have reported positively on the experience. In the intervening years, the concept has been refined, this manual and accompanying programs have been expanded and improved, and finally the Instructor's Manual added.

The accompanying programs run under DOS on a PC. This may be done by obtaining a DOS prompt from within a windowing system, or by exiting the windowing system altogether. Some programs (such as **Factor** accept parameters on the command line, and of those, two of them (**EuAlgDem** and **R2D**) respond very differently depending on whether acceptable parameters are provided, or not. Some of the programs offer an opportunity to print some of the data being viewed. However, if printing is invoked and no printer is operational, then the computer may hang as it waits endlessly for the printer to respond. If printing fails when a program is run from within the DOS box of a windowing system, try exiting the window system before running the program.

The author is grateful to many people for their useful suggestions valuable contributions to this material, most especially to Harley Flanders, Sid Graham, Everett Howe, Don Lewis, John Rickert, Andrew Sterrett, and Ulrike Vorhauer. The author will be pleased to receive any comments or suggestions at the email address `hlm@umich.edu`.

Hugh L. Montgomery
6 September, 2004

Contents

Warning

The accompanying programs are intended for educational use only. We make no warranty, express or implied, that the programs are free of error, that they meet any particular standard of merchantability, or that the values they yield are accurate. Some of these programs have been put through strenuous tests, but many others have been checked only in the most casual manner. In order to extend the range of integers that may be dealt with, most of these programs use floating-point real arithmetic in their execution. Thus the accuracy of the results cannot be guaranteed, and consequently these programs should not be used for serious mathematical research. Any such use would be entirely at the user's own risk. The author disclaims all liability for direct, incidental, or consequential damages resulting from your use of these programs.

Chapter I
Basics

The *integers* are the numbers $\ldots, -2, -1, 0, 1, 2, \ldots$. The *rational numbers* are quotients of one integer by another, a/q where $q \neq 0$. *Number Theory* is the branch of mathematics devoted to the study and investigation of properties of integers and rational numbers. We can add, subtract, and multiply integers just as we do real numbers, but for division we encounter a major difference: We can divide any real number x by any other, y, provided only that $y \neq 0$, and we obtain a quotient, called x/y. Life in the integers is different, because x/y is not necessarily an integer. Before proceeding further, we review some of basic properties of the integers that we take for granted.

Algebraic identities. Under this heading we include such fundamental identities as

$a + (b + c) = (a + b) + c$	(addition is associative)
$a(bc) = (ab)c$	(multiplication is associative)
$a + b = b + a$	(addition is commutative)
$ab = ba$	(multiplication is commutative)
$a(b + c) = ab + ac$	(the distributive law)
$0 + a = a$ for all a	(0 is the additive identity)
$1 \cdot a = a$ for all a	(1 is the multiplicative identity)
For every a and b there is a	(subtraction)
unique x such that $a + x = b$	(this number x is denoted $b - a$)

This is not a complete list, as there are many more identities that follow from these. Some of these are still rather basic, such as $(-1) \cdot (-1) = 1$, while others are more advanced, such as $a^2 - b^2 = (a - b)(a + b)$. Of course, these same algebraic identities also hold for all real numbers, so it is not these identities that set the integers apart from the real numbers.

Ordering and inequalities. Some of these are fundamental,

$1 > 0$.	
Exactly one of $a < b$, $a = b$, $a > b$ is true.	(antisymmetry)
If $a < b$ and $b < c$ then $a < c$.	(transitivity)

while others are more advanced, such as the following:

$$\text{If } a > 0 \text{ and } b > 0 \text{ then } a + b > 0 \text{ and } ab > 0.$$
$$\text{If } a \geq b \text{ and } A \geq B \text{ then } a + A \geq b + B.$$
$$\text{If } a \geq b \text{ and } m \geq 0 \text{ then } ma \geq mb.$$

When talking about inequalities, we sometimes say, "a is positive," which means the same thing as "$a > 0$." Similarly, "a is negative," means the same as "$a < 0$." Of course, these inequalities also hold for all real numbers, so it is not these properties that set the integers apart from the real numbers.

Discreteness. The least positive integer is the number 1. That is, there is no integer x such that $0 < x < 1$. More generally, the least integer larger than n is $n + 1$; there are no integers in the open interval $(n, n + 1)$. Because the integers are spaced apart from each other in this way, we say that the integers are *discrete*. This is in sharp contrast with the real numbers, which run continuously with no gaps.

Mathematical Induction. This principle asserts that if $\mathcal{S}$ is a set of positive integers such that 1 is in $\mathcal{S}$ and also $n + 1$ is in $\mathcal{S}$ whenever n is in $\mathcal{S}$, then every positive integer is in $\mathcal{S}$. In symbols, we say that if $1 \in \mathcal{S}$ and $n \in \mathcal{S} \Longrightarrow n+1 \in \mathcal{S}$, then $\mathcal{S}$ contains all positive integers.

To appreciate the significance of this, suppose that we are trying to prove that a certain proposition concerning n is true for all positive integers n. Let $P(n)$ denote this assertion. Let $\mathcal{S}$ be the set of those n for which $P(n)$ is true. We verify that $P(1)$ is true—this is called the *basis* of the induction. Next we show that if $P(n)$ is true then $P(n + 1)$ is true—this is the *inductive step*. This approach is often useful, particularly when the assertions $P(n)$, $P(n + 1)$ are very similar. We now give two examples of assertions that can be proved by mathematical induction.

Theorem I.1. *For every positive integer n,*

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

This identity might have been surmised on the basis of numerical evidence. In general, we use numerical patterns to suggest properties of the integers. A proposed property is called a *conjecture*. When we are able to prove a conjecture, it becomes a *theorem*. When constructing a proof we can employ properties of the integers that were familiar to us when we began, but we can also appeal to any of the other theorems that we have already proved. In this way we enlarge our collection of known properties of the integers, one theorem at a time.

Proof. First we note that if $n = 1$ then the left hand side is $= 1$, and that the right hand side is

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

Thus the formula holds when $n = 1$. Now suppose that the formula holds for the integer n.

By adding $n+1$ to both sides of the identity we deduce that

$$\begin{aligned} 1+2+\cdots+n+(n+1) &= \frac{n(n+1)}{2}+(n+1) \\ &= \frac{n^2+n}{2}+\frac{2n+2}{2} \\ &= \frac{n^2+3n+2}{2} \\ &= \frac{(n+1)(n+2)}{2}. \end{aligned}$$

This is the correct formula for the integer $n+1$. Thus by the principle of mathematical induction we conclude that the formula holds for all positive integers n.

Theorem I.2. *Suppose that x is a real number, $x \neq 1$. Then for every positive integer n,*

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

This identity can be interpreted as an assertion concerning the factorization of polynomials, since we may write it as

$$x^{n+1}-1 = (x-1)(x^n+x^{n-1}+\cdots+x+1).$$

In this latter form, the identity holds also when $x=1$.

Proof. When $n=1$, the right hand side is

$$\frac{x^2-1}{x-1} = \frac{(x+1)(x-1)}{x-1} = x+1,$$

so the identity holds. Now suppose that the identity holds for n. Then

$$\begin{aligned} 1+x+\cdots+x^n+x^{n+1} &= \Big(1+x+\cdots+x^n\Big)+x^{n+1} \\ &= \frac{x^{n+1}-1}{x-1}+x^{n+1} \end{aligned}$$

by the inductive hypothesis. Here the right hand side is

$$\begin{aligned} &= \frac{x^{n+1}-1}{x-1}+\frac{x^{n+1}(x-1)}{x-1} \\ &= \frac{x^{n+1}-1}{x-1}+\frac{x^{n+2}-x^{n+1}}{x-1} \\ &= \frac{x^{n+1}-1+x^{n+2}-x^{n+1}}{x-1} \\ &= \frac{x^{n+2}-1}{x-1}, \end{aligned}$$

which is the proposed identity for $n+1$. Hence by mathematical induction, the proof is complete.

On several occasions above we have used '$\cdots$' to indicate terms of a series whose form is to be inferred by the reader. This practice becomes unsatisfactory in more complicated situations, since it may not be clear from the first few terms how the sequence is intended to continue. For greater precision, we write

$$\sum_{k=1}^{n} x_k$$

to denote the sum of the numbers x_k for k from 1 to n. Here Σ is a capital sigma, which is the Greek letter corresponding to the Roman letter S. (The lower case Greek sigma is written σ. When convenient Roman letters are not available in mathematics, for further symbols we frequently turn to the Greek alphabet, a copy of which is provided in Appendix G.) More generally, we may write $\sum_{k=a}^{b} x_k$ to denote the sum of x_k for $a \le k \le b$. If $b < a$ then there is no integer k satisfying $a \le k \le b$, and then we call the sum 'empty', and its value is 0. The symbol k is called the 'dummy variable'; its purpose is only to index the members of the sum. We can use any symbol we like for the dummy variable, as long as it is not currently in use for some other purpose. Thus there is no difference between writing $\sum_{k=a}^{b} x_k$ and $\sum_{i=a}^{b} x_i$.

For products of terms we have a similar device, so that instead of writing $x_1 x_2 \cdots x_n$ we write

$$\prod_{k=1}^{n} x_k.$$

Here Π is the capital Greek pi, which corresponds to the Roman letter P. For example, $n!$, called 'n factorial', is the product of the first n positive integers, $n! = 1 \cdot 2 \cdot 3 \cdots n$. In the pi notation, we would write $n! = \prod_{k=1}^{n} k$. If $b < a$ then the product $\prod_{k=a}^{b} x_k$ is empty, and its value is 1.

The reader is urged to start using the sigma and pi notations, so that in time it becomes comfortable and convenient.

Explorations

1. An *arithmetic progression* is a sequence of integers or real numbers in which each term u_n differs from the preceding term by a constant amount. (Note that the integers form an arithmetic progression with common difference 1.) Show by induction that if the sequence u_n forms an arithmetic progression then there exist numbers q and a such that $u_n = qn + a$ for all n.

2. Let u_n be defined by the formula $u_n = qn + a$. Show that these numbers form an arithmetic progression.

3. Use Theorem 1 to show that the sum of n consecutive members of an arithmetic progression is n times the average of the first and last terms taken.

4. A *geometric progression* is a sequence in which the ratio of u_n by the preceding term is constant. Show by induction that if the sequence u_n forms a geometric progression then there exist numbers a and r such that $u_n = ar^n$ for all n.

5. Show that if $u_n = ar^n$ for all n then the u_n form a geometric progression.

6. Use Theorem 2 to derive a formula for the sum of n consecutive members of a geometric progression. What if $r = 1$?

7. Express the identities of Theorems I.1 and I.2 using the sigma notation.

8. Show by induction that

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

Express this identity using the pi notation.

9. Use induction to show that

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

Express this identity using the sigma notation.

10. Use induction to show that

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

Express this using the sigma notation.

11. Show by induction that

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

Express this using the sigma notation.

12. Show by induction that

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

Express this using the sigma notation.

13. Note that

$$(u_1 - u_2) + (u_2 - u_3) + \cdots + (u_n - u_{n+1}) = u_1 - u_{n+1}.$$

Such a series is called 'telescoping'. Express the above using the sigma notation. Find a formula for u_k so that $u_k - u_{k+1} = \frac{1}{k(k+1)}$. Thus show that the sum in the preceding exercise can be interpreted as a telescoping sum.

14. Explain why

$$\prod_{i=1}^{n} \frac{i}{i+1} = \frac{1}{n+1}.$$

15. Find a formula for

$$1 \cdot n + 2 \cdot (n-1) + 3 \cdot (n-2) + \cdots + n \cdot 1,$$

and prove it.

16. The following is a proposed proof by induction that all horses have the same color. Can you find anything wrong with the proof?

Let $\mathcal{S}$ be a set of n horses. We show by induction on n that all horses in $\mathcal{S}$ have the same color. The basis of the induction, $n = 1$, is clear. Now suppose that the assertion holds for n. Let $\mathcal{S}$ be a set of $n+1$ horses. Suppose that one of these horses is called 'Silver'. Remove Silver from the set, so that a set $\mathcal{S}'$ of n horses remains. By the inductive hypothesis, all horses in $\mathcal{S}'$ have the same color. To see that Silver also has this same color, replace it and remove a different horse, say 'Trigger', so that we have a set $\mathcal{S}''$ of n horses. By the inductive hypothesis again all horses in $\mathcal{S}''$ have the same color. Since Silver is in this set, Silver also is the same color as the other horses.

17. Show that

$$\sum_{n=1}^{N} (ax_n + by_n) \;=\; a\Big(\sum_{n=1}^{N} x_n\Big) + b\Big(\sum_{n=1}^{N} y_n\Big).$$

18. Suppose that $\mathcal{S}$ is a nonempty set of positive integers. Show that $\mathcal{S}$ must contain a least element.

WILD PROBLEM

In an infinite checkerboard, each square has a positive integer written in it. The number in any square is the average of the four numbers in the adjacent squares. Prove that all squares have the same number written in them. (Two squares are considered to be adjacent if they share a common side.)

Chapter II
The Division Algorithm

Programs Used: Div, BasesTab, R2D, FacTab, GetNextP

When we divide one integer d (the *divisor*) into another, say D (the *dividend*), the quotient D/d is not necessarily an integer, but we can nevertheless obtain an integral *quotient* q and *remainder* r. We now formulate this precisely.

Theorem II.1. (The Division Algorithm) *Suppose that d is a positive integer, and that D is an integer. Then there exist unique integers q and r with $0 \le r < d$ such that $D = qd+r$.*

On dividing this last identity by d, we see that

$$\frac{D}{d} = q + \frac{r}{d},$$

which is to say that the rational number D/d can be written an an integer q plus a rational number lying between 0 (inclusive) and 1 (exclusive).

Proof. We partition the real line into intervals of length d,

$$\ldots, [-2d, -d), [-d, 0), [0, d), [d, 2d), \ldots$$

Thus each real number is a member of exactly one of these intervals. In particular, the integer D is a member of precisely one of these intervals, say $qd \le D < (q+1)d$. Thus if we set $r = D - qd$ then $D = qd + r$ and $0 \le r < d$. This completes the proof.

Suppose that d and D are integers with $d > 0$. We say that d *divides* D, and write $d \mid D$, if there is an integer q such that $dq = D$. This is equivalent to saying that D is a *multiple* of d. Otherwise we say that d does not divide D, and we write $d \nmid D$. The Division Algorithm allows us to determine when one integer divides another.

Theorem II.2. *Suppose that d and D are integers, with $d > 0$. Let q and r be defined as in the Division Algorithm, so that $D = qd + r$ and $0 \le r < d$. Then d divides D if and only if $r = 0$.*

Proof. If $r = 0$ then $D = qd$, so d divides D. Suppose that $0 < r < d$. We show that there does not exist an integer m such that $D = md$. We consider two cases. If $m \le q$ then $md \le qd < qd + r = D$, so that $md < D$ and hence $md \ne D$. Secondly, if $m > q$ then

$m \geq q+1$ and hence $md \geq (q+1)d = qd + d > qd + r = D$. Thus $md > D$, which implies that $md \neq D$. Hence the proof is complete.

We also use the Division Algorithm to compute the expansion of an integer in a prescribed base b. We say that $r_k r_{k-1} \ldots r_1 r_0$ is the base b expansion of a positive integer n if

$$n = r_0 + r_1 b + \cdots + r_k b^k \qquad \left(\text{i.e., } n = \sum_{i=0}^{k} r_i b^i\right)$$

with $0 \leq r_i < b$ for all i. The digits can be computed from the top down, or the bottom up. We begin with the latter. First divide n by b, to get a quotient n_1 and a remainder r_0. Thus

$$n = n_1 b + r_0.$$

Next divide n_1 by b to get a quotient n_2 and a remainder r_1. Thus $n_1 = n_2 b + r_1$, and hence the right hand side displayed above is

$$\begin{aligned} &= (n_2 b + r_1)b + r_0 \\ &= n_2 b^2 + r_1 b + r_0. \end{aligned}$$

Continuing, we use the Division Algorithm to write $n_2 = n_3 b + r_2$, so that the above is

$$\begin{aligned} &= (n_3 b + r_2)b^2 + r_1 b + r_0 \\ &= n_3 b^3 + r_2 b^2 + r_1 b + r_0. \end{aligned}$$

This process is repeated as long as n_i is positive. Since each n_i is smaller than the preceding one, the procedure eventually terminates.

Example 1. We compute the binary (i.e., base 2) expansion of 7196, trailing digits first.

$$\begin{aligned} 7196 &= 3598 \cdot 2 = 1799 \cdot 2^2 = (899 \cdot 2 + 1)2^2 = 899 \cdot 2^3 + 2^2 = (449 \cdot 2 + 1)2^3 + 2^2 \\ &= 449 \cdot 2^4 + 2^3 + 2^2 = (224 \cdot 2 + 1)2^4 + 2^3 + 2^2 = 224 \cdot 2^5 + 2^4 + 2^3 + 2^2 \\ &= 112 \cdot 2^6 + 2^4 + 2^3 + 2^2 = 56 \cdot 2^7 + +2^4 + 2^3 + 2^2 = 28 \cdot 2^8 + 2^4 + 2^3 + 2^2 \\ &= 14 \cdot 2^9 + 2^4 + 2^3 + 2^2 = 7 \cdot 2^{10} + 2^4 + 2^3 + 2^2 = (3 \cdot 2 + 1)2^{10} + 2^4 + 2^3 + 2^2 \\ &= 3 \cdot 2^{11} + 2^{10} + 2^4 + 2^3 + 2^2 = (1 \cdot 2 + 1)2^{11} + 2^{10} + 2^4 + 2^3 + 2^2 \\ &= 2^{12} + 2^{11} + 2^{10} + 2^4 + 2^3 + 2^2 \\ &= 1110000011100 \qquad \text{(in binary).} \end{aligned}$$

Suppose we wish to calculate the base b expansion of a positive integer m from the top down. We first construct a list of the powers of b, in order to find the integer k for which $b^k \leq m < b^{k+1}$. Then we divide b^k into m, and get a remainder: $m = q_k b^k + m_{k-1}$. Here

$q_k < b$ since $b^{k+1} > m$. Next we divide b^{k-1} into m_{k-1}, and so on. Finally we divide m_1 by b: $m_1 = q_1 b + m_0$. Put $q_0 = m_0$. Then the base b expansion of m is $q_k q_{k-1} \dots q_1 q_0$.

Example 2. We calculate the base 3 expansion of $m = 7196$, leading digits first. We begin by making a list of powers of 3:

k	1	2	3	4	5	6	7	8	9
3^k	3	9	27	81	243	729	2187	6561	19683

Thus we see that

$$\begin{aligned}7196 &= 3^8 + 635 = 3^8 + 2\cdot 3^5 + 149 = 3^8 + 2\cdot 3^5 + 3^4 + 68\\ &= 3^8 + 2\cdot 3^5 + 3^4 + 2\cdot 3^3 + 14 = 3^8 + 2\cdot 3^5 + 3^4 + 2\cdot 3^3 + 3^2 + 5\\ &= 3^8 + 2\cdot 3^5 + 3^4 + 2\cdot 3^3 + 3^2 + 3 + 2\\ &= 100212112 \qquad \text{(in base 3)}.\end{aligned}$$

Yet another application of the Division Algorithm arises when we attempt to distinguish between rational and irrational numbers by means of their decimal expansions.

Theorem II.3. *The decimal expansion of a real number x is eventually periodic if and only if x is rational.*

Proof. Suppose that the decimal expansion of x is eventually periodic with period k. Then the decimal expansion of $10^k x$ is identical with that of x from some point on. Hence when we subtract, we find that the decimal expansion of $10^k x - x$ terminates. That is, there is an integer h such that $(10^k x - x)10^h$ is an integer, say n. Then

$$x = \frac{n}{(10^k - 1)10^h},$$

so x is a rational number.

To prove the converse, suppose that x is rational, say $x = a/q$. We may suppose that both a and q are positive. If a is larger than q then we divide q into a and get a remainder: $a = nq + r$. Then $a/q = n + r/q$, and we see that the decimal expansion of the integer n is the part of the decimal expansion of a/q that appears before the decimal point, while the decimal expansion of r/q is the part that comes after. Thus we concentrate on r/q where $0 < r < q$. We recall the long division procedure: We divide q into $10r$ and get a remainder: $10r = d_1 q + r_1$. Since $r < q$ it follows that $d_1 q \le d_1 q + r_1 = 10r < 10q$, and hence that $d_1 < 10$. Hence d_1 is one of the numbers $0, 1, \dots, 9$. Thus

$$\frac{r}{q} = \frac{d_1}{10} + \frac{1}{10}\frac{r_1}{q}$$

with $0 \le r_1 < q$. Then we repeat this, dividing q into $10r_1$. After k steps we have

$$\frac{r}{q} = \frac{d_1}{10} + \frac{d_2}{10^2} + \cdots + \frac{d_k}{10^k} + \frac{r_k}{10^k q},$$

which, in the sigma notation, is

$$\frac{r}{q} = \sum_{i=1}^{k} \frac{d_i}{10^i} + \frac{r_k}{10^k q}.$$

Since each r_i is one of the numbers $0, 1, \ldots, q-1$, eventually we will encounter two remainders that have the same value: $r_h = r_k$ for some h and k with $0 < h < k$. But then when we divide q into $10r_h$ we obtain the same quotient d_h and remainder r_{h+1} as when we divide q into $10r_k$. That is, $d_h = d_k$ and $r_{h+1} = r_{k+1}$. By mathematical induction it follows that $d_{h+i} = d_{k+i}$ and that $r_{h+i} = r_{k+i}$ for all nonnegative integers i. Hence the decimal expansion of r/q is eventually periodic with a period $k - h$, so the proof is complete.

The Division Algorithm may be executed by hand calculation, but the work is error-prone and tedious. By assigning such mundane tasks to a computer, we are able to acquire data that is both more extensive and more reliable. Among the programs provided, several are useful in the present context. In particular, **Div** effects the Division Algorithm. You may type `div` `<Return>` and then provide the arguments, or the arguments may be entered on the command line. Try typing `div 9 101` `<Return>`. The program **BasesTab** provides a table of the expansions of numbers n to various bases b, for $2 \le b \le 16$ and $1 \le n \le 10^{18}$. When the base is larger than 10 we need new characters to denote the 'digits' $10, 11, \ldots, b-1$. For this purpose we set

$$A = 10, \quad B = 11, \quad C = 12, \quad D = 13, \quad E = 14, \quad F = 15.$$

This is standard in the hexadecimal system (i.e., base 16), which is used extensively in computer science. Type `basestab` `<Return>`. The commands available appear on the bottom line of the screen. Try typing `<PgDn>`. Type `n`, and then enter a large value. When you have finished fooling around, type `<Esc>`, and the program will terminate.

Explorations

1. Using at most a pocket calculator, compute the base 3 expansion of 1996, trailing digits first. Use **BasesTab** to confirm your answer.

2. Using at most a pocket calculator, compute the base 2 expansion of 1996, leading digits first. Use **BasesTab** to confirm your answer.

3. What can be said about the decimal expansion of n if $2 \mid n$? If $5 \mid n$? If $10 \mid n$? If n is of the form $5k + 2$?

4. What can you say about the units digit in the decimal expansion of the perfect squares, $1^2, 2^2, 3^2, \ldots$?

5. What can you say about the units digit in the decimal expansion of the powers of 3: $1, 3, 3^2, 3^3, 3^4, \ldots$?

6. Suppose that the decimal expansion of n is $d_k d_{k-1} \dots d_1 d_0$. Show that from a knowledge of the units digit d_0 alone, it is impossible to tell whether $4 \mid n$. Can you determine whether $4 \mid n$ if you know d_0 and d_1?

7. Let $s(n)$ denote the sum of the decimal digits of n. Construct a table of the values of $s(n)$, say for $1 \le n \le 20$, or so. Add to this table the remainder when n is divided by 9, and also the remainder when $s(n)$ is divided by 9. Note any pattern that emerges.

8. Let $s(n)$ be defined as in the preceding question. For several pairs m, n of positive integers, compute $s(m)$, $s(n)$, $s(m+n)$, and their remainders upon division by 9. Note any pattern that emerges.

9. Do the patterns found in the preceding two questions seem to generalize in some way to other bases? (The program **BasesTab** may be useful here.)

10. Suppose that n has decimal expansion $d_k d_{k-1} \dots d_1 d_0$. Let $a(n)$ denote the alternating sum of these digits, $a(n) = d_0 - d_1 + d_2 - \cdots + (-1)^k d_k$. (In the sigma notation, we would write $a(n) = \sum_{i=0}^{k} (-1)^i d_i$.) Construct a table of values of $a(n)$, and also the remainders when n and $a(n)$ are divided by 11. Note any pattern.

11. Let $a(n)$ be defined as in the preceding question. For several pairs m, n of positive integers, compute $a(m)$, $a(n)$, $a(m+n)$, and their remainders upon division by 11. Note any pattern that emerges.

12. Do the patterns found in the preceding two questions seem to generalize in some way to other bases? (The program **BasesTab** may be useful here.)

13. Careless Cary claimed that 100! is

9,332,621,543,944,152,681,699,238,856,266,700,490,715,968,264,381,
621,468,592,963,895,217,599,993,229,915,608,941,463,976,156,518,286,253,
697,920,827,223,758,251,185,210,916,864,000,000,000,000,000,000,000,000

Unfortunately, when he copied down the number, he skipped a digit. What is the value of the missing digit?

14. The program **R2D** (meaning 'rational to decimal') uses the Division Algorithm to compute the decimal expansion of any given rational number a/q with $0 \le a < q \le 10^9$. At the DOS prompt type `r2d 343 787 <Return>` to view a sceenful of the decimal expansion of 343/787. Note how hard it is to spot the periodicity in the digits. Next type `r2d <Return>`, then `a 343 <Return>`, and finally `q 787 <Return>`. The digits of 343/787 are now displayed in an environment that allows you to view further digits by paging down or by jumping to a specified place. The decimal expansion of a/q has a 'tail' (the aperiodic part) followed by 'cycles' (the periodic part). Let $t(a/q)$ and $c(a/q)$ denote the lengths of the tails and cycles for

a/q. Press c to reveal the cycles. Using a pocket calculator or **R2D**, construct a table of values of $t(1/q)$ and $c(1/q)$, at least for $1 \le q \le 20$. What is the smallest value of $t(1/q)$ that occurs? When is it this small? How large can $c(1/q)$ be? Can you show that it cannot be any larger? Is $c(1/q)$ often large?

15. Let $c(a/q)$ be defined as in the preceding question. Suppose that p is a prime number for which $c(1/p)$ is even. Divide the cycle into its first half and second half, and add the two numbers. What do you get? Formulate a conjecture. For example, when $p = 7$ we have $1/7 = 0.\overline{142857}$, and $142+857 = 999$. (The programs **GetNextP** and **FacTab** can be used to find primes.)

16. Note that each of the numbers

$$\begin{array}{l} 7 \\ 73 \\ 739 \\ 7393 \end{array}$$

is prime. Can this be extended? How far? Are there other such 'towers' of primes? What happens in other bases? The programs GetNextP and FacTab may be useful here.

17. Note that

$$\begin{aligned} 5^2 &= 25 & 6^2 &= 36 \\ 25^2 &= 625 & 76^2 &= 5776 \\ 625^2 &= 390625 & 376^2 &= 141376 \\ 0625^2 &= 390625 & 9376^2 &= 87909376 \\ 90625^2 &= 8212890625 & 09376^2 &= 87909376 \end{aligned}$$

Are there other examples of k digit numbers n such that the last k digits of n^2 form the number n? Do the two sequences above continue indefinitely?

18. Let n be a four-digit number. Suppose that a is the largest of the four digits, b is the second largest, c the third largest, and d the smallest. Form two new four-digit numbers: $abcd$ and $dcba$. Let $f(n)$ be the difference between these. Describe the sequence $n, f(n), f(f(n)), f(f(f(n))), \ldots$. For example, if $n = 7196$, we find that

$$7196 \to 8082 \to 8532 \to 6174 \to 6174 \to 6174 \to \cdots$$

Experiment with other values of n, and form a conjecture. What happens in other bases, or with a different number of digits?

19. Let n be a positive integer, and let n' denote the integer obtained by reversing the digits of n. Put $f(n) = n + n'$. A number n is called a *palindrome* if $n = n'$. Does the sequence $n, f(n), f(f(n)), f(f(f(n))), \ldots$ always include a palindrome? For example, if $n = 69$, we find that

$$69 \to 165 \to 726 \to 1353 \to 4884,$$

a palindrome. Experiment, and form a conjecture. Suppose that every such sequence contains at least one palindrome. Would it be possible for the sequence to contain only finitely many palindromes?

In the two preceding problems, we have considered the sequence generated by repeatedly applying one fixed function f. In general, the function obtained by the k-fold iteration of f is denoted $f^k(n)$. In this notation, the sequences have the form $n, f(n), f^2(n), \ldots, f^k(n), \ldots$.

20. Let $f(n)$ be the sum of the squares of the decimal digits of f. For any given integer n, is the sequence $n, f(n), f^2(n), \ldots$ eventually periodic? For example, if $n = 3$ then we find that

$$3 \to 9 \to 81 \to 65 \to 61 \to 37 \to 58 \to 89 \to 145 \to 42 \to 20 \to 4 \to 16 \\ \to 37,$$

so we have a tail of length 5 and a cycle of length 8. Experiment, and form a conjecture.

21. Let

$$f(n) = \begin{cases} 3n+1 & \text{if } n \text{ is odd,} \\ n/2 & \text{if } n \text{ is even.} \end{cases}$$

Then $f(1) = 4$, $f(4) = 2$, and $f(2) = 1$, a cycle of length 3. What is the behavior of the sequence $n, f(n), f^2(n), \ldots, f^k(n), \ldots$ for other values of n? Experiment, and form a conjecture.

We sometimes define a sequence $u_1, u_2, \ldots$ by a formula, say $u_k = f(k)$. For example, the perfect squares are given by $u_k = k^2$. On other occasions (as above), we generate sequences by iteration of a function, so that $u_k = f(u_{k-1})$. Still more generally, we might define u_k in terms of several of the preceding terms in the sequence. This is called a *recurrence*. For example, the *Fibonacci numbers* F_k are defined by the recurrence $F_{k+1} = F_k + F_{k-1}$ together with the initial conditions $F_0 = 0$, $F_1 = 1$. Thus the first few Fibonacci numbers are

k	0	1	2	3	4	5	6	7	8	9	10	11	12
3^k	0	1	1	2	3	5	8	13	21	34	55	89	144

These numbers have many fascinating properties. For example, they form a *divisibility sequence* in the sense that if $d \mid n$ then $F_d \mid F_n$. In general we do not have a formula for the k^{th} term of a sequence generated by a recursion, but in the case of the Fibonacci numbers it can be shown that

$$F_k = \frac{1}{\sqrt{5}}\Big(\frac{1+\sqrt{5}}{2}\Big)^k - \frac{1}{\sqrt{5}}\Big(\frac{1-\sqrt{5}}{2}\Big)^k.$$

From this latter equation it is not so clear that F_k is always an integer, but from the defining recurrence we see by mathematical induction that F_k is an integer for all k. Similarly, recurrences that involve division will generate rational values, but in general not integers. However, it occasionally happens that such a recurrence unexpectedly seems to generate integers. We consider two examples of this sort.

22. Let $x_1 = 1$, and for $k \ge 1$ put

$$x_{k+1} = \frac{1 + x_1^2 + x_2^2 + \cdots + x_k^2}{k} \qquad \Big(\text{i.e., } x_{k+1} = \frac{1}{k}\Big(1 + \sum_{i=1}^{k} x_i^2\Big)\Big).$$

Calculate as many terms of this sequence as you can. Do you guess that the x_k are integers for all k?

23. Let $y_0 = 1$, $y_1 = 1$, $y_2 = 1$, $y_3 = 1$, and for $k \ge 2$ put

$$y_{k+2} = \frac{y_k^2 + y_{k-1}y_{k+1}}{y_{k-2}}.$$

Calculate as many terms of this sequence as you can. Do you guess that the y_k are integers for all k?

24. A standardized national exam taken by high school students recently posed the question, “Why is π irrational?” The official correct answer was “The number π is irrational because its decimal expansion is not periodic.” Comment on this, and propose how the question might be reformulated.

25. *The Towers of Hanoi.* You are given three vertical rods; on one of these are n rings. The rings are of different sizes, and are sorted by size with the largest at the bottom. The task is to transfer the entire stack, one ring at a time, to one of the other rods, subject to the rule that a larger ring never sits on top of a smaller ring. How many steps are required, and how should you proceed?

26. Suppose that you have a balance scale and a set of calibrated weights. How many of these weights do you need, and what should their values be, if you are to verify that an object has weight k, for any integer k from 1 to 40. Suppose (a) that the calibrated weights all go in one pan, and the unknown weight in the other; or (b) that the calibrated weights can be put in either or both pans.

WILD PROBLEMS

1. Show that the sum of the base 10 digits of 1996^n tends to infinity with n.

2. *The lonesome* 8. In dividing a certain three digit number into an eight digit number we obtain a five digit quotient and no remainder. The calculation has the following shape, but only one digit is known. Since there are 900 possible divisors and 90,000,000 potential dividends, one could say that there are 81×10^9 configurations to consider. Despite the apparent complexity of the situation, find the unique solution.

```
              X X 8 X X
X X X | X X X X X X X X
          X X X
        ---------
            X X X X
              X X X
           ---------
                X X X X
                X X X X
                -------
```

MANUFACTURER'S NOTICE

A defect has been found in certain examples of the associative law produced between 3 February, 1993 and 15 April, 1994. If you used the law during this period, please return the example to the manufacturer.

There is no cause for alarm.

Chapter III
Unique Factorization

Programs Used: **Factor**, **Div**, **DivTab**, **DivTest**,**ArFcnTab**,
GCD, **CoDivTab**, **CoMulTab**, **GCDTab**

A positive integer $p > 1$ is called a *prime number* if it has no divisor lying strictly between 1 and p. That is, the only positive divisors of p are the numbers 1 and p. Note that the integer 1 is not considered to be a prime number. The numbers 2, 3, 5, and 7 are prime numbers, but 4, 6, 8, and 9 are not, because $2 \mid 4$, $2 \mid 6$, $2 \mid 8$, and $3 \mid 9$. An integer $n > 1$ is said to be *composite* if it is not prime. Thus every positive integer is either prime or composite, except for the integer 1, which has a special status. We call an integer n a *unit* if $1/n$ is also an integer. Since $1/1 = 1$, an integer, we see that the number 1 is an example of a unit. Any integer $n > 1$ is either a prime or a product of primes. We call such a way writing n a *factorization* of n. We now show that such a factorization always exists and is unique.

Theorem III.1. (The Fundamental Theorem of Arithmetic) *If n is a positive integer then there exist prime numbers $p_1, p_2, \ldots, p_r$ such that*

$$n = p_1 p_2 \cdots p_r.$$

This representation is unique apart from the order of the factors.

Here we can allow n to be prime, since then $r = 1$, and we are simply asserting that $n = p_1$. When $n = 1$ the list of primes is empty ($r = 0$), and by convention we consider an empty product to have the value 1. The prime numbers $p_1, p_2, \ldots, p_r$ are not necessarily distinct. For example, $12 = 2 \cdot 2 \cdot 3$. When a prime factor is repeated, we can express the factorization more compactly by using powers, as in $12 = 2^2 \cdot 3$. By systematically using powers in this way, we can express an integer n as a product of primepowers, where the primes in question are distinct:

$$n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r} \qquad \left(\text{i.e., } n = \prod_{i=1}^{r} p_i^{a_i}\right).$$

These distinct primes p_i, and the associated exponents a_i, are uniquely determined by n, apart from the order of the factors. The subscript i used to index the primes has very little mathematical significance, and is a notational nuisance. We can express the factorization more tersely, but just as rigorously, by writing

$$n = \prod_p p^{a(p)}.$$

Here the primes form the index set over which the product is taken, and $a(p)$ is a function of prime number p; its values are non-negative integers, and $a(p) = 0$ for all sufficiently large primes. For example, when $n = 12$ we have $a(2) = 2$, $a(3) = 1$, and $a(p) = 0$ for all primes $p > 3$. Thus we may think of the Fundamental Theorem of Arithmetic as asserting that each positive integer n corresponds to a unique sequence of exponents $a(2), a(3), a(5), \ldots, a(p), \ldots$.

Although the existence and uniqueness of prime factorization might be accepted as a known that that does not require proof, we pause to consider how we might derive it from the more basic properties that we have already discussed. We consider the existence of a factorization first. If n is prime then we are done. If n is composite then n can be written $n = ab$ with $1 < a < n$ and $1 < b < n$. If a and b are prime then we are done, but if one or both of them is composite then we write them as products of smaller numbers. We continue in this way until all factors are prime. The process cannot continue indefinitely, since each new factor is smaller than the number it divides.

We now turn to the uniqueness of prime factorization. The main step is to establish the following important principle:

(1) If p is prime, and if $p \mid ab$, then $p \mid a$ or $p \mid b$.

By an easy induction it follows from this that

(2) If p is prime, and if $p \mid a_1 a_2 \cdots a_k$, then $p \mid a_i$ for some i, $1 \le i \le k$.

Now suppose that we have two factorizations of n, say

$$p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$$

where the p_i and the q_j are primes. From this identity we see that p_1 divides $q_1 q_2 \cdots q_s$. Hence by (2), $p_1 \mid q_j$ for some j. But q_j is prime, so it follows that $p_1 = q_j$. Cancel these to primes from the identity. This leaves a similar identity, but with fewer factors. By repeating this, we find that each p_i is paired with exactly one q_j, so that the factorizations are the same, apart possibly from the order of the factors.

To complete the proof of the uniqueness of prime factorization, it remains to establish (1). To this end we list all primes in increasing order, $p_1 = 2, p_2 = 3, \ldots$. Consider the proposition that

The assertion (1) holds if p is any one of the primes $p_1, p_2, \ldots, p_k$.

We prove this by induction on k. For the basis of the induction we consider first $p = 2$. If $2 \nmid a$ then a is an odd number, say $a = 2\alpha + 1$. Similarly, if $2 \nmid b$ then $b = 2\beta + 1$ for some β. Then

$$ab = (2\alpha + 1)(2\beta + 1) = 2(2\alpha\beta + \alpha + \beta) + 1.$$

That is, the product of two odd numbers is odd. Hence $2 \nmid ab$, and the basis is established. For the inductive step we suppose that the proposition holds for k and we take $p = p_{k+1}$. Suppose that $p \mid ab$, say $pm = ab$. We divide p into a and into b, using the Division Algorithm, so that $a = q_a p + r_a$ and $b = q_b p + r_b$ with $0 \le r_a < p$ and $0 \le r_b < p$. If $r_a = 0$ then $p \mid a$ and we are done. Similarly if $r_b = 0$. We show that the assumption that $r_a > 0$ and $r_b > 0$ leads to a contradiction. We know that

$$pm = ab = (q_a p + r_a)(q_b p + r_b) = p(q_a q_b p + q_a r_b + r_a q_b) + r_a r_b.$$

Thus if $n = m - q_a q_b p - q_a r_b - q_b r_a$ then

$$pn = r_a r_b.$$

Now decompose r_a as a product of primes. Since $r_a < p$, all the prime factors of r_a are less than p. Do the same for r_b. Thus we may write the above as

$$pn = q_1 q_2 \cdots q_t$$

where each q_j is one of the primes $p_1, p_2, \ldots, p_k$. Since q_1 is one of the primes for which (1) is known to hold, and since $q_1 \mid pn$, it follows that $q_1 \mid p$ or $q_1 \mid n$. But p is prime, so the first alternative is impossible, so $q_1 \mid n$, say $n = q_1 n_1$. On cancelling q_1 from both sides of the above identity, it follows that

$$pn_1 = q_2 q_3 \cdots q_t.$$

We repeat this, to see that $pn_2 = q_3 q_4 \cdots q_t$, and so forth, until finally $pn_t = 1$, a contradiction. This completes the inductive step, and hence (1) is proved.

As a first application of the Fundamental Theorem of Arithmetic, we note

Theorem III.2. *The number $\sqrt{2}$ is irrational.*

Proof. Suppose that there is a rational number m/n such that $(m/n)^2 = 2$. Then $m^2 = 2n^2$. Let 2^μ be the power of 2 in the canonical factorization of m, and 2^ν be the power of 2 in the factorization of n. Then the power of 2 in m^2 is 2μ, while the power of 2 in $2n^2$ is $2\nu + 1$. By the Fundamental Theorem of Arithmetic, it follows that $2\mu = 2\nu + 1$. But this implies that $2 \mid 1$. Thus we have a contradiction, and hence $\sqrt{2}$ is irrational.

Prime numbers have many interesting properties. One of the oldest theorems concerning primes is the following.

Theorem III.3. (Euclid) *There exist infinitely many prime numbers.*

Proof. We show that for any finite set $\mathcal{P}$ of primes, there is at least one prime number not in the set. Let $\mathcal{P}$ be a finite set of primes, and let P denote the product of all the primes in $\mathcal{P}$,

$$P = \prod_{p \in \mathcal{P}} p.$$

(Note that the symbol '$\in$' means 'is a member of'. Thus the product above is extended over all the primes in $\mathcal{P}$.) Put $n = P + 1$. Suppose that $p \in \mathcal{P}$, and write $n = (P/p)p + 1$. In the context of the Division Algorithm, this tells us that when we divide p into n we obtain a quotient $q = P/p$ and a remainder $r = 1$. (Note that P/p *is* an integer!) Since $r \neq 0$, by Theorem II.2 it follows that $p \nmid n$. That is, none of the primes in $\mathcal{P}$ divide n. But $n > 1$, so by the Fundamental Theorem of Arithmetic we know that either n is prime or is a product of two or more prime numbers. These prime factors of n divide n, and hence they are not members of the set $\mathcal{P}$. Thus there exists at least one prime number not in the set $\mathcal{P}$, and the proof is complete.

Euclid's construction provides the desired proof, but it gives us no feeling for the size of the n^{th} prime number, and it is not very useful for generating primes—the numbers become large very quickly, and it is not clear that every prime is eventually generated in this way.

$\mathcal{P}$	P	n
$\emptyset$	1	2
$\{2\}$	2	3
$\{2, 3\}$	6	7
$\{2, 3, 7\}$	42	43
$\{2, 3, 7, 43\}$	1806	$13 \cdot 139$
$\{2, 3, 7, 13, 43, 139\}$	3263442	3263443
$\{2, 3, 7, 13, 139, 3263443\}$	10650056950806	$547 \cdot 607 \cdot 1033 \cdot 31051$

Here the values of n are presented in factored form. For numbers up to 10^{18}, the computational burden of finding factorizations can be handled by the program **Factor**. For example, the last entry above can be found by typing `factor 10650056950807 <Return>`. Try it. The time required by **Factor** to complete its calculation depends on the size of the largest prime factors of n. In the example just considered, the performance is good because the prime factors are all reasonably small. This program handles all numbers up to 10^9 with ease, but for some larger numbers, particularly prime numbers, the response is sluggish. Apply **Factor** to 10650056950837. (You may have to wait several minutes for the answer, depending on the speed of your machine.) To treat a prime number of size near the upper limit 10^{18}, the time required will be more than 300 times greater. For more information on **Factor**, see the entry in Appendix P.

Although the computation of the factorization of n is time-consuming for some n, by Theorem II.2 it is always easy to determine whether one integer divides another: It suffices to perform just one long division.

Explorations

1. Make a list of the first several powers of 2, namely $1, 2, 4, 8, \ldots$. For each number $d = 2^i$ in the list, determine which of the other numbers in the list are divisible by d. The program **DivTest** is a useful aid.

2. Make a list of the first several powers of 3, namely $1, 3, 9, 27, \ldots$. For each number $d = 3^i$ in the list, determine which of the other numbers in the list are divisible by d. The program **DivTest** may be used as an aid.

3. Make a list of the first several numbers that can be written in the form $2^i 3^j$, $1, 2, 3, 6, 8, 9, 12, \ldots$. For each number $d = 2^i 3^j$ in the list, determine which other numbers in the list are divisible by d. It may be helpful here to arrange the numbers in a two-dimensional array:

$$\begin{array}{cc|ccccc}
 & & & & j & & \\
 & & 0 & 1 & 2 & 3 & \cdots \\
\hline
 & 0 & 1 & 3 & 9 & 27 & \cdots \\
 & 1 & 2 & 6 & 18 & 54 & \cdots \\
i & 2 & 4 & 12 & 36 & 108 & \cdots \\
 & 3 & 8 & 24 & 72 & 216 & \cdots \\
 & \vdots & \vdots & \vdots & \vdots & \vdots &
\end{array}$$

4. Let b and c be given positive integers, and suppose that any prime number that divides b or c (or both) is in the list $p_1, p_2, \ldots, p_r$. Thus by the Fundamental Theorem of Arithmetic we may write

$$b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_r^{\beta_r}, \qquad c = p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_r^{\gamma_r}.$$

What relationship exists between the exponents β_i and the γ_i if $b \mid c$? Use **DivTest** as an aid.

5. If $b \mid c$ and $c \mid d$, does it follow that $b \mid d$?

6. Using the program **DivTab**, or otherwise, find the positive divisors of 2; of 4; of 8, of 2^a. What are the positive divisors of 3, of 9, of 27, of 3^a?

For $n > 0$, let $d(n)$ be the number of positive divisors of n. This is called the *divisor function*. Since 1 and n are divisors of n, we have $d(1) = 1$, $d(p) = 2$ for all prime numbers p, and $d(n) > 2$ for all composite numbers. The program **ArFcnTab** creates a table of values of the divisor function (and several other functions). After typing `arfcntab` `<Return>`, on the bottom line of the screen you will find a menu of commands available to you.

7. Suppose that $n = \prod_p p^{a(p)}$. Can you find a formula for $d(n)$ in terms of the exponents $a(p)$?

8. If $d \mid n$ then the number n/d is called the *complementary divisor* of n, since $d \cdot n/d = n$. Show that if $d \mid n$ then $1 \le d \le \sqrt{n}$ if and only if $\sqrt{n} \le n/d \le n$. What if $d = \sqrt{n}$?

9. For what n is $d(n)$ odd? Data can be gathered using **ArFcnTab**.

10. What is the product of the smallest positive divisor of n and the largest? The second smallest and the second largest? Numerical evidence can be assembled using **DivTab**.

11. What numbers does 1 divide? What numbers does 0 divide? What numbers divide 1? What numbers divide 0?

Let b and c be integers. If $d \mid b$ and $d \mid c$ then d is called a *common divisor* of b and c. If $b = c = 0$ then every integer is a common divisor, and hence there is no largest such number. However, if at least one of b and c is non-zero, then there are only finitely many common divisors, and we let (b, c) denote the greatest common divisor. This notation is somewhat ambiguous, since (b, c) also denotes a point in the plane with coordinates b and c, or it might denote an interval $a < x < b$ of the real line. When such possibilities might cause confusion, we write $\gcd(b, c)$. This number is calculated by the program **GCD**. Try typing `gcd 34 119 <Return>`.

12. Suppose that b, c and their greatest common divisor (b, c) are written in the form

$$b = \prod_p p^{\beta(p)}, \qquad c = \prod_p p^{\gamma(p)}, \qquad (b, c) = \prod_p p^{\delta(p)}.$$

These are meant to be the canonic factorization of these numbers into prime powers, as provided by the Fundamental Theorem of Arithmetic. Use **CoDivTab** to view these numbers in several specific cases. Can you express the exponents $\delta(p)$ in terms of the $\beta(p)$ and $\gamma(p)$?

13. Which common divisors of b and c divide (b, c)?

14. If $b > 0$, what is $(b, 0)$?

15. Is it always true that $(b, c) = (c, b)$?

16. What is the relation between (b, c) and $(b, b + c)$?

17. How does (b, c) compare with (mb, mc)?

Let b and c be integers. If $b \mid m$ and $c \mid m$ then m is called a *common multiple* of b and c. Common multiples always exist, because bc is a common multiple of b and c. The least common multiple of b and c is denoted $[b, c]$, or $\operatorname{lcm}(b, c)$ to be unambiguous.

18. Use **CoMulTab** to examine the common multiples of given integers. If $b = \prod_p p^{\beta(p)}$ and $c = \prod_p p^{\gamma(p)}$, can you describe the factorization of $[b, c]$ in terms of the $\beta(p)$ and $\gamma(p)$?

19. How is $(b, c)[b, c]$ related to bc?

20. Does $[b, c]$ divide all common multiples of b and c?

21. The numbers b and c are said to be *relatively prime* if $(b, c) = 1$. If b and c are relatively prime, what can you say about the primes that divide b, and the primes that divide c?

22. If b and c are relatively prime, what is $[b, c]$?

23. How is $[mb, mc]$ related to $[b, c]$?

24. Suppose that $(m, n) = 1$. How are $d(m)$ and $d(n)$ related to $d(mn)$? Use the program **ArFcnTab** to explore.

25. Suppose that $(a, b) = 1$ and that $a \mid bc$. Does it follow that $a \mid c$?

26. The program **GCDTab** creates a 2-dimensional table of greatest common divisors (b, c). Move around in this table. When b and c are large, is (b, c) usually large? What values occur most often? Take $b = 111111111$. Five of the columns contain a variety of numbers, but two of the columns seem to contain only the number 1. Use the $\uparrow$ key to move up in the table. Does this phenomenon seem to persist? How long does it continue?

27. Explain why $k! + i$ is composite for $2 \le i \le k$. In this way, show that there exist arbitrarily long gaps between consecutive prime numbers. When $k! < 10^9$, find the gap constructed in the table generated by **FacTab**. How does the length of the guaranteed gap compare with other gaps between primes in that vicinity? In **FacTab**, type `n 2083133` to view the prime numbers between 20831330 and 20831530. Is there a long gap here? How long? Does this seem to be longer than the average, in this vicinity?

28. Let d be a fixed positive integer. Determine the logical relationship, if any, between the following two assertions:
(i) $a \mid b$;
(ii) $da \mid db$

29. A number n is called a *perfect square* (or sometimes just *square*) if there is an integer k such that $k^2 = n$. Using **Factor** as necessary, make a list of the factorizations of the first few perfect squares, $1^2, 2^2, 3^2, 4^2, \ldots$. Construct a criterion, in terms of the factorization of n, to determine whether n is a perfect square or not.

30. A number is said to be *squarefree* if it is not divisible by any perfect square larger than 1. Make a list of all perfect squares not exceeding 25. For each $n, 1 \le n \le 25$, use **DivTab** to construct a list of the divisors of n. By comparing the two lists, determine whether n is squarefree. List the squarefree n not exceeding 25, and their factorizations. Construct a criterion, in terms of the factorization of n, to determine whether or not n is squarefree.

31. Let n be a positive integer. Is it always possible to write $n = ab$ where a is a perfect square and b is squarefree? Is there ever more than one such representation?

32. Determine the logical connection, if any, between the following two assertions:
(i) $d(n)$ is a power of 2;
(ii) n is a perfect square.
The programs **Factor** and **ArFcnTab** may be helpful.

33. Show that $\sqrt{3}$ is irrational.

34. Show that if n is not a perfect square then $\sqrt{n}$ is irrational.

35. Show that $\sqrt[3]{2}$ is irrational.

36. Let a and b be rational. Show that $a + b\sqrt{2} \neq 0$ unless $a = b = 0$.

37. Suppose that a_1, a_2, b_1, b_2 are rational numbers. Show that if $a_1 + b_1\sqrt{2} = a_2 + b_2\sqrt{2}$ then $a_1 = a_2$ and $b_1 = b_2$.

38. Is $\sqrt{2} + \sqrt{3}$ irrational?

39. Let $\theta = \sqrt{2} + \sqrt{3}$. Note that $\frac{1}{2}\theta^2 - \frac{5}{2} = \sqrt{6}$. Can you find rational numbers a_1, a_1, a_2, a_3 so that $a_0 + a_1\theta + a_2\theta^2 + a_3\theta^3 = \sqrt{2}$? What about $\sqrt{3}$?

WILD PROBLEM

Suppose that you have a set of $n+1$ numbers taken from the numbers $1, 2, \ldots, 2n$. Show that there exist distinct numbers b and c in the set such that $b \mid c$.

Chapter IV
Linear Combinations of Integers

Programs Used: LnComTab, EuAlgDem, SlowGCD, FastGCD, GCD

Let b and c be two integers. An integer of the form $xb+yc$ is called a *linear combination* of b and c. Here x and y are arbitrary integers. As x and y run over all integral values, the quantity $xb+yc$ runs over a certain range of values. Our goal is to determine what that range of values is, and to describe how various values are taken on. For example, if $b = 12$ and $c = 15$ then for small values of x and y we obtain the linear combinations in the following table:

x

		-6	**-5**	**-4**	**-3**	**-2**	**-1**	**0**	**1**	**2**	**3**	**4**	**5**	**6**
	6	18	30	42	54	66	78	90	102	114	126	138	150	162
	5	3	15	27	39	51	63	75	87	99	111	123	135	147
	4	-12	0	12	24	36	48	60	72	84	96	108	120	132
	3	-27	-15	-3	9	21	33	45	57	69	81	93	105	117
	2	-42	-30	-18	-6	6	18	30	42	54	66	78	90	102
	1	-57	-45	-33	-21	-9	3	15	27	39	51	63	75	87
y	**0**	-72	-60	-48	-36	-24	-12	0	12	24	36	48	60	72
	-1	-87	-75	-63	-51	-39	-27	-15	-3	9	21	33	45	57
	-2	-102	-90	-78	-66	-54	-42	-30	-18	-6	6	18	30	42
	-3	-117	-105	-93	-81	-69	-57	-45	-33	-21	-9	3	15	27
	-4	-132	-120	-108	-96	-84	-72	-60	-48	-36	-24	-12	0	12
	-5	-147	-135	-123	-111	-99	-87	-75	-63	-51	-39	-27	-15	-3
	-6	-162	-150	-138	-126	-114	-102	-90	-78	-66	-54	-42	-30	-18

We let $\mathcal{S}(b,c)$ denote the set of all numbers that can be written in the form $xb + yc$ for some integral values of x and y. Thus $\mathcal{S}(12,15)$ is the set of all numbers appearing in the above table, if it were extended to infinity in all directions. The program **LnComTab** displays such tables of numbers $xb + yc$. This will serve to aid in answering the following questions.

Explorations

1. As x and y run over all integral values (both positive and negative), the quantity $12x + 15y$ takes on certain values. What values in the interval $[-50, 50]$ occur?

2. In the table created by **LnComTab**, is any value repeated? Is there any pattern to the repeated values? Are there any values that are not repeated? Can you find a subset of the table (possibly an infinite subset) within which every value occurs exactly once? (Every value that is found somewhere in the table, that is.)

3. Let b and c be integers, not both 0, and let $\mathcal{S}(b,c)$ denote the set of all integers that can be written in the form $xb + yc$. If $s_1 \in \mathcal{S}(b,c)$ and $s_2 \in \mathcal{S}(b,c)$, does it follow that $s_1 + s_2 \in \mathcal{S}(b,c)$? If $s \in \mathcal{S}(b,c)$ and m is an integer, does it follow that $ms \in \mathcal{S}(b,c)$?

4. Suppose that G and s are two members of $\mathcal{S}(b,c)$ with $G > 0$. Suppose that G is divided into s, using the Division Algorithm, to obtain a quotient q and a remainder r, so that $s = qG + r$. Does it follow that $r \in \mathcal{S}(b,c)$?

5. Let G be the least positive member of $\mathcal{S}(b,c)$. Does it follow that G divides every member of $\mathcal{S}(b,c)$?

6. Let G be the least positive member of $\mathcal{S}(b,c)$, and let $g = \gcd(b,c)$. Explain the relation between g and G.

7. Still using the program **LnComTab**, compare the tables generated when $b = 12$, $c = 15$, with that for $b' = 27$, $c' = 15$. (Note that $27 = 12 + 15$.) How are the tables related? In general, how is $\mathcal{S}(b,c)$ related to $\mathcal{S}(b+c,c)$? How is it related to $\mathcal{S}(b+mc,c)$ where m is some given integer? Can you show that $\gcd(b,c) = \gcd(b+mc,c)$?

8. What happens to the table generated by **LnComTab** if $b = 12$, $c = 15$ is replaced by $b = 15$, $c = 12$?

9. Apply **LnComTab** with $b = 4$, $c = 5$. How does this compare with the table when $b = 12$, $c = 15$? In general, how is $\mathcal{S}(mb,mc)$ related to $\mathcal{S}(b,c)$?

10. Justify the following equalities:

$$\begin{aligned}(57,34) &= (1\cdot 34+23,34)\\ &= (23,34)\\ &= (34,23)\\ &= (1\cdot 23+11,23)\\ &= (11,23)\\ &= (23,11)\\ &= (2\cdot 11+1,11)\\ &= (1,11)\\ &= (11,1)\\ &= (11\cdot 1+0,1)\\ &= (0,1)\\ &= 1\end{aligned}$$

Apply a similar chain of identities to evaluate $(79,43)$. This method is known as the *Euclidean Algorithm*. Type `eualgdem 79 43 <Return>` to confirm your arithmetic.

11. The Euclidean Algorithm can be made slightly faster by introducing extra tricks. For example, when we apply the Division Algorithm, say $D = qd + r$, if $d - r$ is smaller than r we could instead write $D = (q+1)d - (q-r)$. Since $q+1$ is the nearest integer to D/d, this is called 'rounding to the nearest integer'. When we round up, the remainder is negative, but this does not matter, since $(-b,c) = (b,c)$. If we apply rounding to the nearest integer in the calculation of **10.**, we find that

$$\begin{aligned}(57,34) &= (2\cdot 34-11,34)\\ &= (-11,34)\\ &= (11,34)\\ &= (34,11)\\ &= (3\cdot 11+1,11)\\ &= (1,11)\\ &= (11,1)\\ &= (11\cdot 1+0,1)\\ &= (0,1)\\ &= 1\end{aligned}$$

Here we needed only 3 long divisions, whereas in **10.** we used 4 long divisions. How many long divisions are saved when you use rounding to the nearest integer in calculating $(79,43)$? The program **GCD** uses this improved version of the

Euclidean Algorithm. Try typing `gcd 79 43 <Return>`. If you type `eualgdem <Return>` without entering the arguments on the command line, then you are prompted for the values of b and c, and the results are displayed in a table. This presentation also allows you to switch between rounding down and rounding to the nearest integer.

12. Determine the value of $[113355, 224466]$. (Hint: First find their gcd.)

13. If we were to calculate (b, c) using only the definition of the greatest common divisor, then we would divide d into b, and if it divides evenly then we would divide d into c; all this for every $d \leq b$. That amounts to more than b long divisions. The program **SlowGCD** computes the gcd in this way. Apply **SlowGCD** to two 2-digit numbers, to two 3-digit numbers, etc., and note the time required in each case. The program **FastGCD** computes the gcd by using the Euclidean Algorithm. Apply **FastGCD** to the same pairs of numbers. How much faster is it?

14. A total of 270 contestants have registered for a bass fishing contest. As organizer, you must provide each contestant with one of *Harry's No-Fail* lures. At Al's Hardware, these lures are sold in boxes of 25 lures per box. At the Glennie Bait Shop across the street, they are sold in boxes of 12 lures per box. How many boxes should you buy at each place, in order to have a total of 270 lures. What if there were only 263 contestants? Is it always possible to buy exactly n lures, if n is large enough?

15. Suppose that b and c are positive integers, and that $g = (b, c)$. Show that if $g \mid n$ and if n is sufficiently large, then n can be written $n = bx + cy$ where x and y are non-negative integers. What is the largest n (in terms of b and c) for which this is impossible? Experiment, using **LnComTab**, and formulate a conjecture.

16. Thus far we have considered linear combinations of two integers. Suppose we now form linear combinations of three integers. Let a, b, c be given integers, and let $\mathcal{S}(a, b, c)$ denote the set of all linear combinations $ax + by + cz$ of these integers. Describe this set in terms of the greatest common divisor of a, b, c, denoted (a, b, c).

WILD PROBLEMS

1. There are N people at a party, $N \geq 2$. No one shakes hands with themselves, and no two people shake hands more than once. Prove that there are two people who shake hands with the same number of other people.

2. A couple invites four other couples to dinner, making ten people in all. At the end of the evening, the host asks each of the nine others, "How many people did you meet for the first time tonight?" The responses are nine different numbers. What did the hostess say? Assumptions: (i) The members of each couple had met previously; (ii) When one person meets another, the second also meets the first.

Chapter V
Farey Fractions

Programs Used: FareyTab, FracTab, D2R

The *Farey Fractions of order Q* are the rational numbers between 0 and 1 with denominator not exceeding Q, listed in increasing order, with each fraction expressed in reduced form. Thus the Farey Fractions of order 7 are:

$$\frac{0}{1}, \frac{1}{7}, \frac{1}{6}, \frac{1}{5}, \frac{1}{4}, \frac{2}{7}, \frac{1}{3}, \frac{2}{5}, \frac{3}{7}, \frac{1}{2}, \frac{4}{7}, \frac{3}{5}, \frac{2}{3}, \frac{5}{7}, \frac{3}{4}, \frac{4}{5}, \frac{5}{6}, \frac{6}{7}, \frac{1}{1}$$

The program **FareyTab** constructs a table of Farey Fractions, for orders up to 10^9. These fraction possess many curious properties. Before trying to prove anything, we first want to construct a large body of conjectures. The following questions should help you to formulate constructive guesses.

Explorations

1. For each pair of adjacent Farey Fractions in the table above, compute the difference between the fractions. Express the answer as a rational number, not as a decimal. Does a pattern emerge? Try other orders of fractions, until a pattern is evident.

2. Which pair of adjacent fractions above is closest together? Which pair is farthest apart?

3. If a/q and a'/q' are adjacent fractions, what is $\gcd(q, q')$?

4. If a/q and a'/q' are adjacent fractions among the Farey fractions of order Q, how does the size of $q + q'$ compare with Q?

5. Suppose that a/q and a'/q' are two rational numbers with $a/q < a'/q'$ and $q > 0$, $q' > 0$. (These fractions are not necessarily reduced, and they are not necessarily consecutive Farey Fractions of any order.) Where does the number

$$\frac{a + a'}{q + q'}$$

lie? Is it $< a/q$, between a/q and a'/q', or $> a'/q'$?

6. Suppose that a/q and a'/q' are consecutive Farey Fractions of order Q. When q is replaced by $Q+1$, by $Q+2$, $\ldots$, new fractions are inserted in the list. Eventually, a/q and a'/q' will no longer be adjacent. What is the least Q' for which they are not adjacent, and what is the first fraction to appear between them?

7. Let a/q and a'/q' be fixed fractions, and suppose that $a/q < a'/q'$. Think of (m, n) as representing a point in the plane given by Cartesian coordinates, and let θ denote the angle between the positive x-axis and the ray from the origin to (m, n). Thus $\tan\theta = n/m$. The program **FracTab** lists the fractions $(am + a'n)/(qm + q'n)$, sorted according to the size of the associated angle θ. For what pairs m, n is this new fraction less than a/q? Between a/q and a'/q'? Larger than a'/q'? Can you prove your conjecture?

8. Let a, q, a', q' be fixed, with $aq' - a'q = 1$. Describe the fractions that can be written in the form $(am + a'n)/(qm + q'n)$. Use **FracTab** to aid in formulating a conjecture, and then try to prove it.

9. Suppose that $aq' - a'q = 1$. Among all the fractions that lie between a/q and a'/q', which one has the smallest denominator? Experiment with **FracTab**, make a conjecture, and try to prove it.

10. Let a/q and a'/q' be given, with $a/q < a'/q'$. Is there any logical connection between the following two assertions?

(i) $fracy_1x_1 < \frac{y_2}{x_2}$;
(ii) $(ax_1 + a'y_1)/(qx_1 + q'y_1) < (ax_2 + a'y_2)/(qx_2 + q'y_2)$.

11. Suppose that a, q, a', q' are integers such that $aq' - a'q = 1$. Is there any logical connection between the following two assertions?

(i) $(xa + ya', xq + yq') = 1$;
(ii) $(x, y) = 1$.

12. Call two fractions a/q and a'/q' 'close' if $aq' - a'q = \pm 1$. (This is not a standard term—it is meant to be used only for this question.) If a/q and a'/q' are close, does it follow that a/q and $(a + a')/(q + q')$ are close? That $(a + a')/(q + q')$ and a'/q' are close?

13. Suppose that $1 \le q \le Q$, $1 \le q' \le Q$, and that $(q, q') = 1$. Among the Farey fractions of order Q, how many times is a fraction with denominator q adjacent to one with denominator q'? (Note: The answer is not the same for all pairs q, q'.)

14. Let Q be a positive integer. Explain why

$$\sum_{\substack{1\le q\le Q\\ 1\le q'\le Q\\ (q,q')=1\\ q+q'>Q}} \frac{1}{qq'} = 1.$$

15. Prove or disprove: For every real number θ, $0 \le \theta \le 1$, there is a rational number a/q such that

$$\left|\theta - \frac{a}{q}\right| < \frac{1}{q^2}.$$

16. Prove or disprove: For every real number θ, $0 \le \theta \le 1$, and every positive integer Q, there is a rational number a/q with $1 \le q \le Q$ such that

$$\left|\theta - \frac{a}{q}\right| < \frac{1}{qQ}.$$

17. Prove or disprove: For every real number θ, and every positive integer Q, there is a rational number a/q with $1 \le q \le Q$ such that

$$\left|\theta - \frac{a}{q}\right| < \frac{1}{qQ}.$$

18. Prove or disprove: For every real number θ there exist infinitely many pairs of integers a, q with $q > 0$ such that $|\theta - a/q| < 1/q^2$. (Here a and q are not necessarily relatively prime.)

19. Suppose that a and q are integers with $q \ne 0$. Explain why $|2q^2 - a^2| \ge 1$. Show that

$$\left(\sqrt{2} - \frac{a}{q}\right)\left(\sqrt{2} + \frac{a}{q}\right) = \frac{2q^2 - a^2}{q^2}.$$

Can you show that

$$\left|\sqrt{2} - \frac{a}{q}\right| > \frac{1}{4q^2}$$

for all rational numbers a/q?

20. Suppose that a/q and a'/q' are distinct rational numbers. Explain why

$$\left|\frac{a}{q} - \frac{a'}{q'}\right| \ge \frac{1}{qq'}.$$

21. Suppose that θ is a rational number. Show that there is a positive real number c (which may depend on θ) such that if $|q\theta - a| < c$ then $a/q = \theta$.

22. Prove or disprove: A real number θ is rational if and only if there is a real number $c > 0$ such that if a and q are integers with $q > 0$, and $\theta \neq a/q$, then $|\theta - a/q| \geq c/q$.

23. *Napier's number*, $e = 2.71828182845904523536\ldots$, can be defined by the infinite series

$$e = \frac{1}{0!} + \frac{1}{1!} + \frac{1}{2!} + \frac{1}{3!} + \cdots \qquad \left(\text{i.e., } e = \sum_{n=0}^{\infty} \frac{1}{n!}\right).$$

Here $0! = 1$ by convention. Since each term of this series is a rational number, any finite section of this series provides a rational approximation to e, say

$$\frac{a_N}{q_N} = \frac{1}{0!} + \frac{1}{1!} + \frac{1}{2!} + \frac{1}{3!} + \cdots + \frac{1}{N!}.$$

Construct a table, with rows indexed by N, and columns listing the values of a_N, q_N, and $q_N e - a_N$. Does it seem that there is a positive constant c as in the preceding question?

24. Let a_N and q_N be defined as above. Suppose that it has been shown that

$$\frac{a_N}{q_N} < e < \frac{a_N}{q_N} + \frac{2}{(N+1)!}$$

for all integers $N \geq 1$. (Given a rudimentary knowledge of infinite series, this can easily be done by appealing to the defining series above and to Theorem I.2.) Deduce that e is irrational.

25. The interval $[a/q, a'/q']$ between two consecutive Farey fractions of order Q is called a *Farey arc*. For any real number θ and any Q, there is always a Farey arc containing θ. For example, $\theta = (\sqrt{5} - 1)/2 = 0.61803398874989484820\ldots$, which is known as the *golden ratio*, lies in the following Farey arcs:

Q	a/q	a'/q'
1	$0/1$	$1/1$
2	$1/2$	$1/1$
$3, 4$	$1/2$	$2/3$
$5, 6, 7$	$3/5$	$2/3$

Extend this table, and note any patterns that emerge. Do you recognize the denominators that arise?

26. For the number $\sqrt{2} = 1.41421356237309504880\ldots$, construct a table similar to the one above, and note any patterns that arise.

27. For the number $e = 2.71828182845904523536\ldots$, construct a table similar to the one above, and note any patterns that arise.

28. Let $\|\theta\|$ denote the distance from θ to the nearest integer. Given the decimal expansion of e and a pocket calculator, we make a table of the values of $\|qe\|$ for $q = 1, 2, \ldots$.

q	$\|qe\|$
1	0.2817
2	0.4366
3	0.1548
4	0.1269
5	0.4086
6	0.3097
7	0.0280
8	0.2537
9	0.4645
10	0.1828

We let $q_1 = 1$, $q_2 = 3$, and $q_3 = 7$; these are the values of q for which $\|qe\|$ is smaller than any preceding value. Extend the table, say to $q = 40$, and note the record-breaking values of q. Does there seem to be any relation between these q_i and the findings in the preceding question?

29. Does the connection between the findings in the two preceding questions reflect a property that is special to the number e, or does it persist for other—or perhaps even all—real numbers. Choose a real number, and experiment.

30. The program **FareyTab** constructs tables of Farey fractions of order Q for $1 \le Q \le 10^9$. How long a bookshelf would be required to hold these tables, if they were all printed out in their entirety? Indicate any assumptions you make in your estimates.

31. How close can two rational numbers a/q and a'/q' be, without being equal? Of course two rational numbers can be quite close if their denominators are large, so the object is to determine how close these fractions can be, in terms of their denominators.

When we describe a real number by the first k digits of its decimal expansion, say $0.d_1d_2\cdots d_k$, we are not specifying a unique real number, but instead are describing an interval of real numbers whose decimal expansions have the same first k digits. Assuming that we are rounding to the nearest integer, this interval is $[0.d_1d_2\cdots d_k - \frac{1}{2\cdot 10^k}, 0.d_1d_2\cdots d_k + \frac{1}{2\cdot 10^k})$. The program **D2R** converts decimals to rationals in the sense that if some decimal digits are given, the program returns the rational number with least denominator that lies in the indicated interval.

32. Trailing 0's affect how **D2R** responds. Try typing d2r .31 <Return>, and then d2r .310 <Return>. Why is it to be expected that the response may be different?

33. Choose a rational number, and a pocket calculator (or **R2D**) to determine its first few decimal digits. Give **D2R** the first digit, then the first two digits, then the first three digits, until has enough digits to recover the original rational number. When we considered the decimal expansions of rational numbers we saw that the period of the expansion can be nearly as large as the denominator. How many decimal digits are needed in order for **D2R** to identify rational numbers reliably?

34. Choose a real number x. Let c_0 denote its integral part, $c_0 = [x]$, and r_0 the remainder, $r_0 = x - c_0$. Then put $x_1 = 1/r_0$, and repeat this, so that $c_1 = [x_1]$, $r_1 = x_1 - c_1$, and $x_2 = 1/r_1$. Calculate several more terms of these sequences, and note how easy the calculation is. Thus we have

$$x = c_0 + \frac{1}{x_1} = c_0 + \frac{1}{c_1 + \frac{1}{x_2}} = c_0 + \frac{1}{c_1 + \frac{1}{c_2 + \frac{1}{x_3}}} = \cdots .$$

These are initial segments of the *continued fraction expansion* of x. If the continued fraction process is truncated one obtains rational numbers,

$$\frac{h_0}{k_0} = c_0 + \frac{1}{c_1}, \quad \frac{h_1}{k_1} = c_0 + \frac{1}{c_1 + \frac{1}{c_2}}, \quad \frac{h_2}{k_2} = c_0 + \frac{1}{c_1 + \frac{1}{c_2 + \frac{1}{c_3}}}, \quad \cdots .$$

Use your values of c_i to calculate the approximations h_i/k_i. Are these numbers larger or smaller than x? How close are these numbers to x, in the sense of best rational approximations as considered in **26.** above? If x is rational, how do the h_i/k_i relate to Farey fractions? If x is a quadratic irrational, what do you note about the c_i?

WILD PROBLEM

Let c be a real number with the property that n^c is a positive integer whenever n is a positive integer. Show that c must be a non-negative integer.

Chapter VI
Parity and Permutations

Programs Used: BasesTab, **Merlin**, **PermCalc**

We call a number *even* if it is divisible by 2, and *odd* if it is not. Thus numbers of the form $2k$ are even, while numbers of the form $2k+1$ are odd. The *parity* of a number refers to its oddness or evenness. It is easy to see that the sum of two even numbers is even, since $2m + 2n = 2(m+n)$. Also, the sum of an even number and an odd number is odd, since $2m + (2n+1) = 2(m+n)+1$. Finally, the sum of two odd numbers is even: $(2m+1)+(2n+1) = 2(mn+1)$. As for multiplication, we note that the product of two even numbers is even: $(2m)(2n) = 2(2mn)$, the product of an even number and an odd number is even: $(2m)(2n+1) = 2(2mn+m)$, and the product of two odd numbers is odd: $(2m+1)(2n+1) = 2(2mn+m+n)+1$. These observations are summarized in the following tables.

$\oplus$	**0**	**1**
0	0	1
1	1	0

$\otimes$	**0**	**1**
0	0	0
1	0	1

Here '0' stands for any even number, and '1' stands for any odd number. This simple information can be put to good use.

1. Let $P(x) = a_k x^k + \cdots + a_1 x + a_0$ be a polynomial with integral coefficients. Is it true that all the numbers

$$\ldots, P(-4), P(-2), P(0), P(2), P(4), \ldots$$

have the same parity? Is it true that all the numbers

$$\ldots, P(-5), P(-3), P(-1), P(1), P(3), P(5), \ldots$$

have the same parity? Experiment with some simple polynomials.

2. Let $s(n)$ denote the sum of the base 3 digits of n. Using **BasesTab**, make a table of $s(n)$. Do n and $s(n)$ always have the same parity?

3. Describe the smallest set of points in the plane that have the following properties: The points $(0,0),(1,0),(0,1)$ are in the set; For any points **P** and **Q** in the set, the point **R** obtained by reflecting **P** about **Q** is also in the set. (That is, **Q** is the midpoint of the segment **PR**.)

4. Suppose that the two diagonally opposite corners of a checker board are removed. Show that it is not possible to cover the remaining region with dominos. (Each domino covers two adjacent squares.)

5. Each square of a 5×5 chess board has a knight on it. Show that it is not possible to move all 25 knights simultaneously so that afterwards each square again has exactly one knight on it. (The moves must be legal knight's moves: Two squares in one direction, and one square perpendicularly.)

6. Show that

$$\det \begin{bmatrix} 1985 & 8390 & 2382 & 7356 & 3678 \\ 5678 & 8765 & 1234 & 5432 & 5678 \\ 1092 & 2938 & 3847 & 4756 & 6574 \\ 1238 & 2346 & 3454 & 4561 & 5670 \\ 1122 & 3344 & 5566 & 1506 & 1961 \end{bmatrix} \neq 0.$$

7. Show that it is impossible to cover a 6×6 checker board by 18 dominos in such a way that every line running between columns or between rows crosses as least one domino. Show that such a construction is possible on an 8×8 checker board.

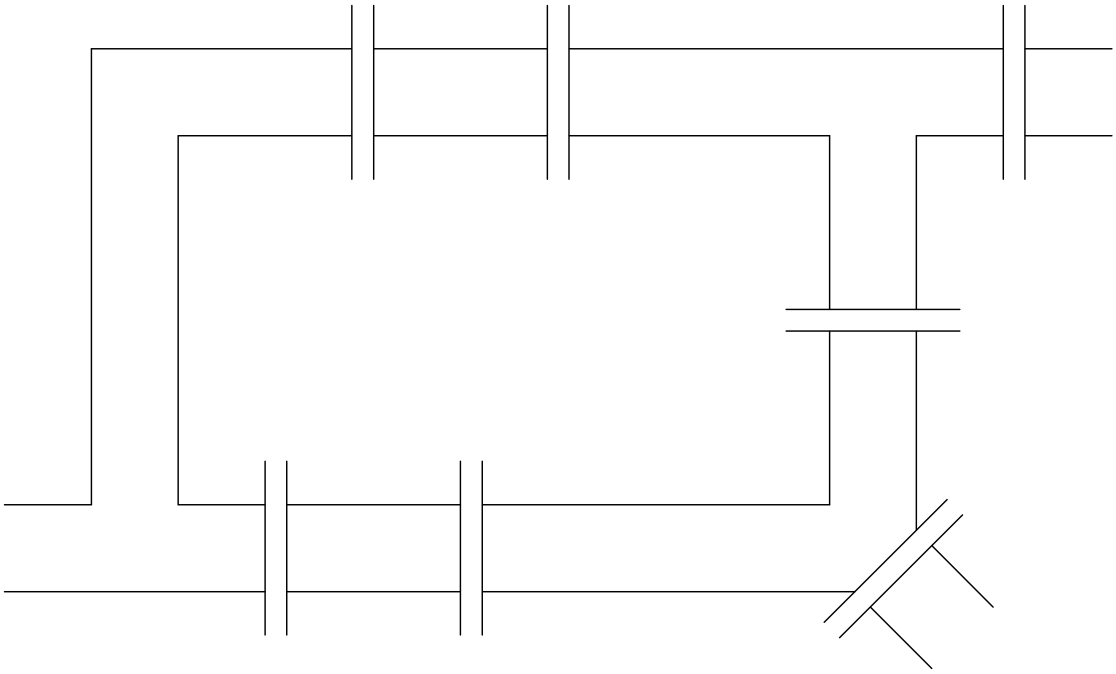
8. Suppose that $a_1, a_2, \dots, a_{2n+1}$ are integers such that whenever one member of the sequence is removed, the remaining members can be divided into two sets of n terms with equal sums. Show that $a_1 = a_2 = \cdots = a_{2n+1}$.

9. Suppose that $a_1, a_2, \dots, a_{2n}$ are integers such that whenever one member of the sequence is removed, the remaining numbers can be divided into two sets (one of them possibly empty) with equal sums. Show that $a_1 = a_2 = \cdots = a_{2n} = 0$.

10. Suppose that x, y, z, and w are integers such that $x^4 - 2y^4 + 4z^4 - 8w^4 = 0$. Show that $x = y = z = w = 0$.

11. There are n people in a room, and some pairs of them shake hands. Show that the number of people who shake hands an odd number of times is even. Does it matter if some pairs shake hands more than once?

12. Immanuel Kant lived in Königsberg, a town whose four parts were joined by seven bridges. Was it possible for Kant to take a walk in such a way that he crossed each bridged exactly once? The famous Swiss mathematician Leonard Euler (pronounced 'oiler'—he lived 1707–1783) found an elegant solution of this problem in 1736.



13. After White's 99^{th} move and Black's 98^{th} move, a chess game has reached the following (unlikely) situation. Prove that Black has a mate in four.

BR	**BKn**	**BB**	**BK**	**BQ**	**BB**	**BKn**	**BR**
WP	**WP**	**WP**	**WP**	**WP**	**WP**	**WP**	**WP**
WR	**WKn**	**WB**	**WQ**	**WK**	**WB**	**WKn**	**WR**

Permutations have a parity property that is important in mathematics and in the analysis of permutation puzzles. A *permutation* simply reorders a collection of objects. If we have n objects, we may call them $1, 2, \ldots, n$. The set of all permutations of n objects is denoted S_n, and is called the *symmetric group*. To specify a permutation, it is enough to describe where each object is to be placed. For example, suppose that

$$\pi_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 6 & 4 & 2 & 5 \end{pmatrix}, \qquad \pi_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 2 & 4 & 5 & 3 & 1 \end{pmatrix}.$$

Then the permutation π_1 takes the first element and places it in the third location, the second element in the first location, the third element in the sixth location, and so on. We can form the *composition* of two permutations by first performing one, and then the other. For example, if we perform π_1 first and then π_2, we obtain the permutation

$$\pi_2\pi_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 6 & 1 & 5 & 2 & 3 \end{pmatrix}.$$

Note that in this 'multiplication' of permutations, the one on the right is performed first.

14. With π_1 and π_2 defined as above, calculate $\pi_1\pi_2$. Is this the same as $\pi_2\pi_1$?

15. How many different permutations are there on n elements? That is, how big is S_n?

16. Let π_1, π_2, and π_3 be three permutations. Is it true in general that $\pi_3(\pi_2\pi_1) = (\pi_3\pi_2)\pi_1$?

The permutation π_1 displayed above is a particular kind of permutation called a *cycle* (or, more precisely, a 5-*cycle*) because it takes 1 to 3, 3 to 6, 6 to 5, 5 to 2, and 2 to 1 in a cycle, while all other numbers (in this case only one) remain fixed. For such permutations we have a more compact notation, namely $\pi_1 = (1\ 3\ 6\ 5\ 2)$. Alternatively, we could write $\pi_1 = (5\ 2\ 1\ 3\ 6)$, since it does not matter where in the cycle we begin. A *transposition* is a permutation in which two elements are exchanged but all the others are fixed. In other words, a transposition is the same thing as a 2-cycle.

17. Is the permutation π_2 displayed above a cycle? Can you write it as a product of disjoint cycles?

18. Suppose that $\pi_1 = (1\ 2\ 3)$ and that $\pi_2 = (4\ 5\ 6)$. Is it true that $\pi_1\pi_2 = \pi_2\pi_1$? Does this generalize to the product of any two disjoint cycles?

19. Suppose that π is a k-cycle. Is π^2 also a k-cycle? What about π^3? π^4? Is π^h a k-cycle for all h?

20. Suppose that π_1 is a k_1-cycle, and that π_2 is a k_2-cycle. Suppose that these cycles are disjoint, and put $\pi = \pi_1\pi_2$. Let the identity permutation (in which all elements are fixed) be denoted i. What is the least positive integer h such that $\pi^h = i$?

21. Given a permutation π, does there always exist an *inverse* permutation π^{-1} such that $\pi\pi^{-1} = \pi^{-1}\pi = i$? Experiment, say with the permutations π_1 and π_2 displayed above? If π is a k-cycle, is π^{-1} a k-cycle?

22. Can a k-cycle always be written as a product of transpositions? Is such a representation unique? What is the smallest number of transpositions that you can achieve?

23. Suppose that π is a permutation in S_n. We want to know whether there exist integers $a_1, a_2, \ldots, a_n$ with $1 \le a_1 \le n$, $2 \le a_2 \le n$, $3 \le a_3 \le n$, $\ldots$, $a_n = n$, such that

$$\pi = (1\ a_1)(2\ a_2)\cdots(n\ a_n).$$

Try to find such integers for the permutations π_1 and π_2 displayed above. Does it seem that such a representation always exists? Is it possible for a permutation to have more than one such representation?

It is tempting to call a permutation *even* if when it is expressed as a product of transpositions, the number of transpositions is even. This has the advantage that it makes it evident that the product of two even permutations is even, the product of an even permutation with an odd permutation is odd, and that the product of two odd permutations is even, but it ignores the possibility that a permutation might be both even and odd. Alternatively, we could say that if π is a product of disjoint cycles of lengths $k_1, k_2, \ldots, k_r$ then we call π odd or even according as whether $(k_1 - 1) + (k_2 - 1) + \cdots + (k_r - 1)$ is odd or even. This assigns a specific parity to each permutation, but it is no longer so clear that this product of two odd permutations is even, for example. The following question is intended to suggest a possible solution to these difficulties.

24. Let $\pi = (1\ 2\ 3\ 4\ 5\ 6\ 7)(8\ 9\ 10\ 11\ 12)$. What is the cycle structure of $(2\ 5)\pi$? Of $(9\ 11)\pi$? Of $(3\ 10)\pi$? In general, what is the cycle structure of $(i\ j)\pi$ for various values of i and j?

25. Sam Loyd's Fifteen Puzzle Suppose that you have a 4×4 frame that contains 15 numbered squares, and one blank space. Any square adjacent to the blank space can slide into that space, so that the positions of the square and the blank are exchanged. Explain why it is impossible to slide squares in such a way as to pass from the situation (a) below to (b).

1	**2**	**3**	**4**
5	**6**	**7**	**8**
9	**10**	**11**	**12**
13	**15**	**14**	

(a)

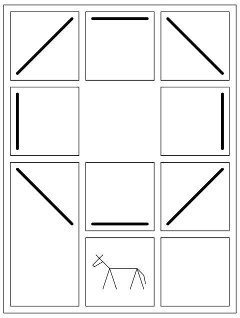
1	**2**	**3**	**4**
5	**6**	**7**	**8**
9	**10**	**11**	**12**
13	**14**	**15**	

(b)

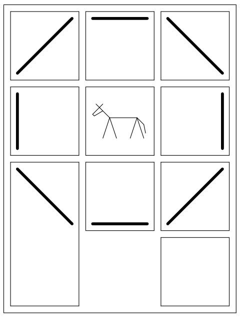
26. By sliding squares, one can move from the position below to one of (a) or (b) above. Which one?

3	9	15	2
13	5	11	14
12	1	8	4
6	10	7	

27. The object is to put the goat in his pen—that is, by sliding blocks, pass from (a) to (b) below. Explain why this appears at first sight to be impossible. What must be done in order to solve the problem?



(a)



(b)

28. Rubik's Cube (Bűvös Kocka) A $3 \times 3 \times 3$ cube is colored with six colors, so that each face has a solid color. The cubes are mechanically linked so that any face of 9 cubes can be rotated by $90°$. After a few moves the colors are wildly mixed. The object is to restore the cube to its initial condition.

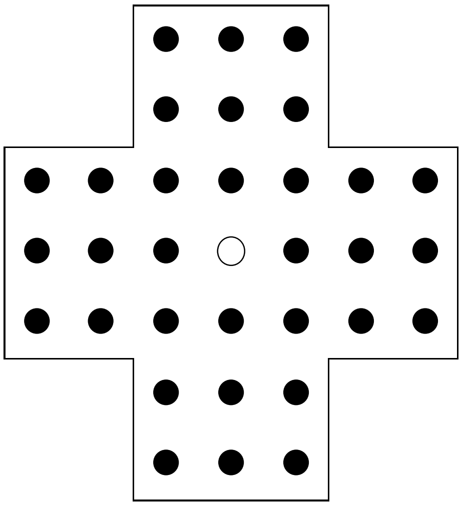
The center of a face rotates, but otherwise does not move. Hence the center of each face determines the eventual color of that face. If the corner and edge cubes could be arbitrarily permuted among themselves, how many configurations would there be? When a single move is made, what kind of permutation is performed on the corner cubes? On the edge cubes? Are these odd or even permutations?

29. Conway's Cubes Build a $3 \times 3 \times 3$ cube from the blocks described below, left. Similarly, build a $5 \times 5 \times 5$ cube from the blocks described below, right.

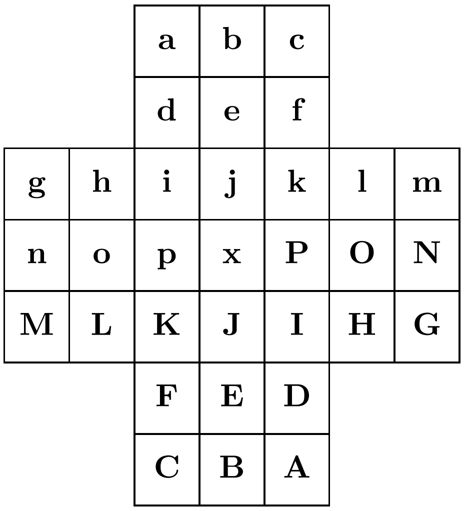
Dimensions	Quantity
$1 \times 1 \times 1$	3
$1 \times 2 \times 2$	6

Dimensions	Quantity
$1 \times 1 \times 3$	3
$1 \times 2 \times 2$	1
$2 \times 2 \times 2$	1
$1 \times 2 \times 4$	13

Peg Solitaire is played on a board in the shape of a Greek cross, as depicted below, on the left. A move is made by jumping a peg over an adjacent peg, into an empty hole just beyond. The peg that was jumped over is then removed. The most traditional problem is start with the board filled with pegs except for the central hole; the object is then to remove all pegs except one, which should be in the central hole. This is an example of a *reversal* problem. There are other interesting reversal problems, and still further problems that are entertaining. For future reference, we label the positions on the board as in the chart, below right.

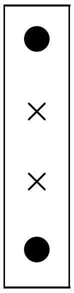


(a) The central one peg reversal problem

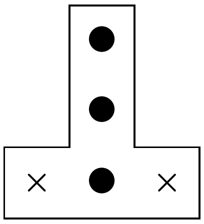


(b) The labeled board

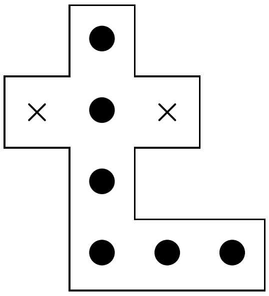
From a purely mechanical point of view, it is useful to note that sometimes a group of pegs can be removed from the board without disturbing the rest of the board. In such cases there is always one peg that must be present to start things going—we call it the *catalyst*. In the charts below, the catalyst is in one of the positions marked $\times$; the other such position must be empty. It is easy to verify that in either case the indicated pegs can be removed without jumping outside the indicated region.



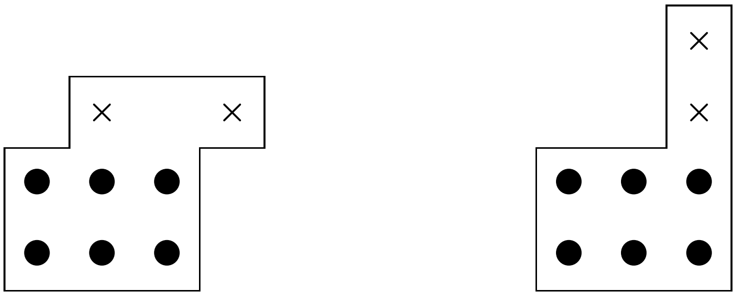
Catalyzed Pair



Catalyzed Triple



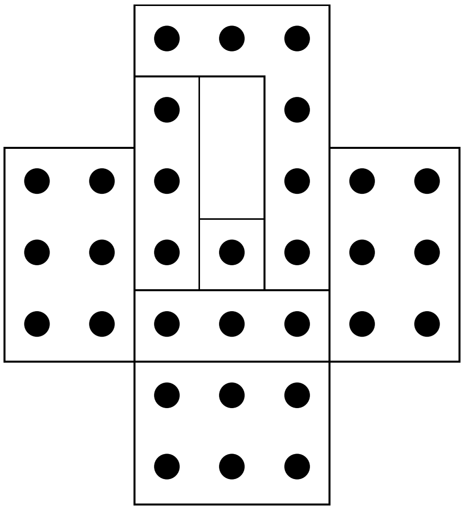
Catalyzed L



Two Catalyzed Sixes

In the catalyzed six on the left, the blank cell may be either filled or empty at the start—its condition will be restored. In both cases, all jumps leaving the six are in the up direction in the right hand column.

30. In the central one peg reversal problem, there are four possible first jumps, but because of symmetry we may suppose that it is downwards into the center hole. After this jump has been made, the remaining pegs on the board can be partitioned into shapes that we know how to remove—provided that they are catalyzed. Show that there is a way to order the regions below so that each one is catalyzed when its turn comes.



31. Of the other six one-peg reversal problems, five can be solved as easily as the one above, while the sixth one is harder (but still possible). Choose a one-peg reversal problem, and solve it.

While a complete analysis of Peg Solitaire seems beyond reach, we can treat a simpler game in which the rules are relaxed as follows: The number of pegs in a hole can be any integer (possibly negative), and in addition to jumps we are allowed unjumps. (An unjump has the effect of undoing a jump.) We call this the *Integral Game*. By making jumps (and unjumps) from the boundary toward the center of the board, it is possible to pass from any configuration to one in which each hole contains 0 pegs, except possibly for the four holes **i**, **j**, **p**, **x** on the board. Jumping back and forth across a hole reduces the number of pegs in the hole by 2 without affecting the rest of the board. Unjumps similarly may be used to increase the number of pegs in a hole by 2. By jumping (or unjumping) back and forth across our four holes we may arrange that the number of pegs in each of these holes is either 0 or 1. There are sixteen configurations of this kind, and we see that any configuration in the Integral Game is equivalent to one of these. It remains to show that these sixteen classes are genuinely distinct. To this end, let $S_{\mathbf{i}}$ be the sum of the number of pegs in the holes marked by 1 in the diagram (**i**) below. Note that when a jump is made, this sum is either unchanged or decreases by 2. Similarly, the sum is either unchanged or increases by 2 when an unjump is performed. Thus the parity of $S_{\mathbf{i}}$ is preserved. In our sixteen reduced configurations, this quantity is odd if and only if there is a peg in hole **i**. For holes **j**, **p**, and **x** we may form similar invariants, using the patterns in (**j**), (**p**), and (**x**) below. Thus we obtain a quadruple

		0	0	0		
		1	0	1		
0	1	1	0	1	1	0
0	0	0	0	0	0	0
0	1	1	0	1	1	0
		1	0	1		
		0	0	0		

(**i**)

		0	0	0		
		0	1	1		
1	1	0	1	1	0	1
0	0	0	0	0	0	0
1	1	0	1	1	0	1
		0	1	1		
		0	0	0		

(**j**)

		1	0	1		
		1	0	1		
0	0	0	0	0	0	0
0	1	1	0	1	1	0
0	1	1	0	1	1	0
		0	0	0		
		1	0	1		

(**p**)

		0	1	1		
		0	1	1		
0	0	0	0	0	0	0
1	1	0	1	1	0	1
1	1	0	1	1	0	1
		0	0	0		
		0	1	1		

(**x**)

of invariants—called the *Reiss invariants*. Since each of our sixteen reduced configurations has a different quadruple associated with it, we see that no one of them is equivalent to any other. In conclusion, we note that in the Integral Game we may pass from one configuration to another if and only if the two configurations have the same Reiss invariants.

31. Can the pattern in (**i**) be extended to arbitrarily large regions? Does it exhibit any periodicity?

32. Of the sixteen possible Reiss invariants, which ones can be attained by a single peg?

33. If we start with a full board except for an empty hole at the center, and end with a single peg, where can that peg be located?

34. If we have a single peg on the board, what other single pegs would have the same set of Reiss invariants?

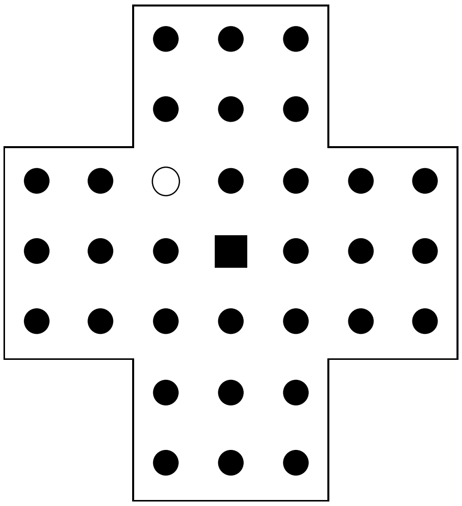
35. Does the Reiss theory apply to boards whose shape is different from the one we have adopted?

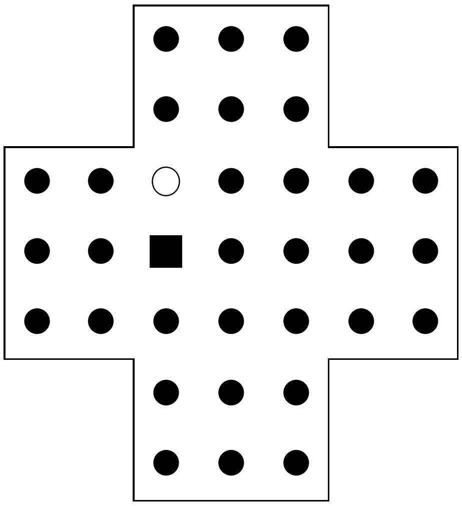
36. Suppose that we have a single peg in every hole of the board. What are the Reiss invariants of this configuration?

37. Suppose that we play solitaire not on the standard board, but on a different board, whose Reiss invariants are not $(0, 0, 0, 0)$. Show that all reversal problems are impossible.

38. To what locations can a given peg hop to, from its initial location?

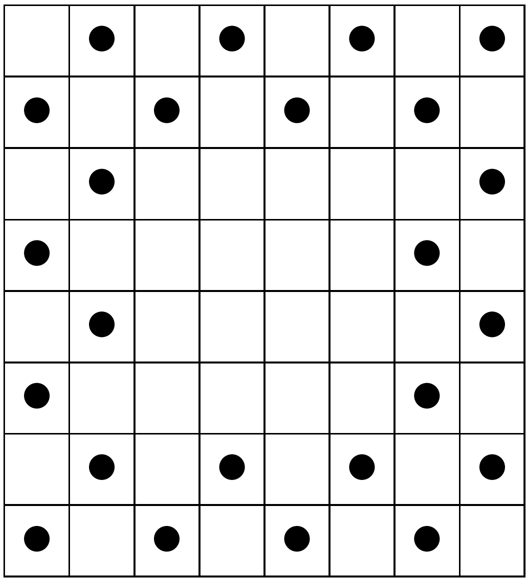
39. Suppose we start with an empty hole at position **i**, and a square peg in the central hole, **x**, as depicted below, left. Show that it is impossible to end up with only the square peg remaining.



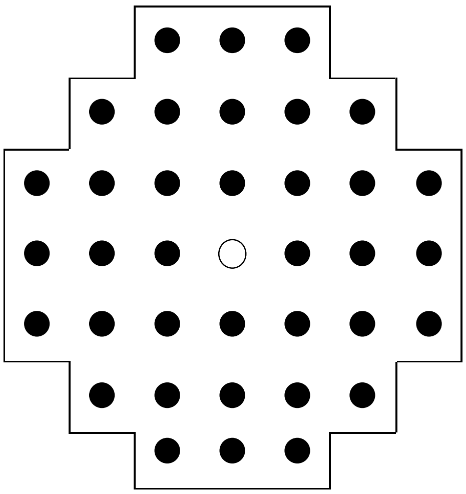


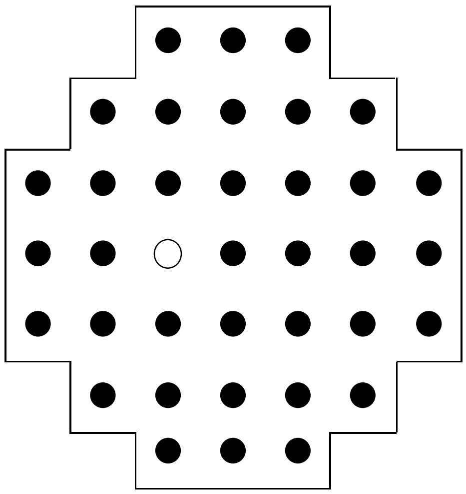
40. Suppose we start with an empty hole at position **i**, and a square peg in hole **p**, as depicted on the right, above. The object is to leave only this distinguished peg on the board. Determine where the square peg must end up, and solve the problem.

41. Suppose we put checker pieces on the black squares on the outer two ranks and files of a checker board, as below, left. We make jumps diagonally, as in checkers, removing the piece jumped over. Is it possible to end up with a single piece on the board?



42. Thus far we considered solitaire on the *English Board*. Below we have the *Continental Board*, which has four additional holes. Show that the situation on the left can not be reduced to a single peg.

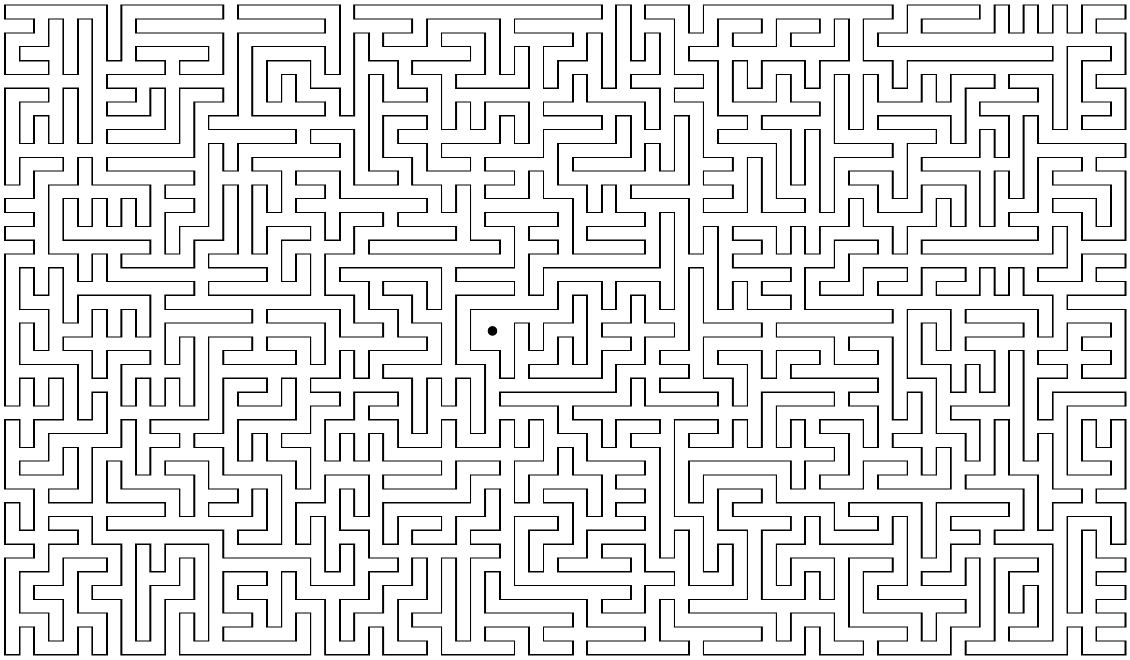




43. Reduce the situation on the right above to a single peg.

44. Show that all reversal problems on the Continental Board are impossible.

45. A simple closed curve in the plane separates points in its interior from those that are exterior. The interior is a bounded set, and has no hole in it. The exterior is unbounded, and has one hole. Describe a simple parity principle that allows one to determine quickly whether a given point not on a curve is in the interior or not. In the diagram below, is the indicated point interior?



46. Merlin was an electronic toy marketd by Parker Brothers (now part of HasBro) in 1978. Of the various puzzles it offered, the most memorable one involves pushing buttons on a 3×3 array until the outer ring of buttons is lit, and the central one is dark. When a button is pressed, the condition of certain buttons is reversed, in a predictable way. Thus, pushing a button twice has no effect, so the problem is one of parity. Set NUMLOCK on your computer, and use the program **MERLIN** to investigate. Can you reach the desired goal from an arbitrary initial position? Can you describe, from an initial position, which buttons must be pushed?

WILD PROBLEMS

1. Bulgarian Solitaire is played as follows: Choose a positive integer k, and put $n = k(k+1)/2$. Place n cards in several piles, not necessarily the same number of cards in every pile. Then repeatedly make the following move: Take one card from each pile, and put these cards together in a new pile. What eventually happens?

2. Suppose that a collection $\mathcal{R}$ of rational functions in two variables x, y is generated as follows: $x \in \mathcal{R}$; $y \in \mathcal{R}$; if $f \in \mathcal{R}$ and c is a real constant, then $cf \in \mathcal{R}$; if $f \in \mathcal{R}$ and $g \in \mathcal{R}$, then $f + g \in \mathcal{R}$ and $f - g \in \mathcal{R}$; if $f \in \mathcal{R}$ and f is not identically 0, then $1/f \in \mathcal{R}$. Does it follow that $xy \in \mathcal{R}$?

Chapter VII
Congruences

Programs Used: Div, GCD, CngArTab

In the preceding chapter we achieved a great deal by noting the remainders when numbers are divided by 2. We now extend this idea, and consider the behavior of remainders when numbers are divided by some particular number m. Suppose that b and c are given integers, and that we apply the division algorithm to both of them, so that

$$\begin{aligned} b &= q_1 m + r_1 \qquad (0 \le r_1 < m), \\ c &= q_2 m + r_2 \qquad (0 \le r_2 < m). \end{aligned} \tag{1}$$

For some purposes the two numbers b and c are interchangeable if the remainders r_1 and r_2 are the same.

Definition. *Suppose that $m > 1$, and that the equations* (1) *hold. We say that b and c are* congruent*, and write $b \equiv c \pmod m$, if $r_1 = r_2$.*

Since $b - c = (q_1 - q_2)m + (r_1 - r_2)$ and $-m < r_1 - r_2 < m$, we see that $m \mid (b - c)$ if and only if $r_1 = r_2$. That is, $b \equiv c \pmod m$ if and only if $c = b + km$ for some integer k. The set of integers congruent to $b \pmod m$ are precisely the numbers of the form $km + r_1$. These numbers form an arithmetic progression with common difference m. Such a set of numbers is called a *residue class* $\pmod m$.

Explorations

1. Choose a number $b \equiv 1 \pmod 4$, and a second number $c \equiv 2 \pmod 4$. What is $b + c$ congruent to, modulo 4 ? Do this several times with different values of b and c. Form a conjecture. Can you prove your conjecture?

2. Choose a number $b \equiv 2 \pmod 5$, and a second number $c \equiv 3 \pmod 5$. What is bc congruent to, modulo 5 ? Do this several times with different values of b and c. Form a conjecture. Can you prove your conjecture?

3. Suppose that $b \equiv c \pmod m$. How does (b, m) compare with (c, m) ? Experiment with several numbers, form a conjecture, and prove it.

4. Suppose that d and m are positive integers, and that $d \mid m$. Is there any logical relation between the two assertions (i) $b \equiv c \pmod{d}$ and (ii) $b \equiv c \pmod{m}$? How are the residue classes (mod d) related to the residue classes (mod m) ?

5. Let $P(x)$ be a polynomial with integral coefficients, say $P(x) = 3x^2 - x + 2$. If $b \equiv c \pmod{m}$ does it follow that $P(b) \equiv P(c) \pmod{m}$?

The numbers that give the remainder 0 when divided by 7 are the multiples of 7, namely the numbers

$$\ldots,\quad -28,\ -21,\ -14,\ -7,\quad 0,\quad 7,\quad 14,\quad 21,\quad 28,\quad \ldots$$

Let $\mathcal{R}_0$ denote the set of these numbers. Similarly, let $\mathcal{R}_1, \ldots, \mathcal{R}_6$ be the sets of numbers that give remainders $1, \ldots, 6$, respectively. Thus the members of $\mathcal{R}_1, \ldots, R_6$, are

$$\begin{array}{llllllllll}
\ldots, & -27, & -20, & -13, & -6, & 1, & 8, & 15, & 22, & 29, & \ldots \\
\ldots, & -26, & -19, & -12, & -5, & 2, & 9, & 16, & 23, & 30, & \ldots \\
\ldots, & -25, & -18, & -11, & -4, & 3, & 10, & 17, & 24, & 31, & \ldots \\
\ldots, & -24, & -17, & -10, & -3, & 4, & 11, & 18, & 25, & 32, & \ldots \\
\ldots, & -23, & -16, & -9, & -2, & 5, & 12, & 19, & 26, & 33, & \ldots \\
\ldots, & -22, & -15, & -8, & -1, & 6, & 13, & 20, & 27, & 34, & \ldots
\end{array}$$

respectively. These sets are the residue classes (mod 7). Drawing on our answer to the first question posed above, we see that if we add a number from $\mathcal{R}_i$, say $a \in \mathcal{R}_i$ to a number from $\mathcal{R}_j$, say $b \in \mathcal{R}_j$, then the sum $a+b$ lies in some one of these sets, say $\mathcal{R}_k$, and—this is the important part—the value of k depends only on i and j, not on the particular choices of a and b. Indeed, $k \equiv i + j \pmod{7}$. This allows us to define an addition on the residue classes themselves. The resulting addition table looks like this:

$\oplus$	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

TABLE 1. Addition modulo 7.

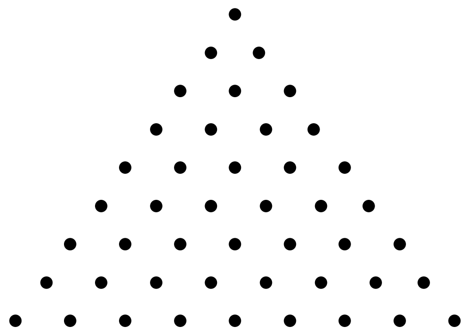
Note that in each row of the table, each of the numbers $0, 1, 2, 3, 4, 5, 6$ is an entry exactly once. For example, suppose we look for a b in row a. We find the b, say in column x. That is, $a + x \equiv b \pmod 7$.

6. Suppose that a and b are residue classes $\pmod m$. Show that there is a unique x such that $a + x \equiv b \pmod m$.

7. The identity $a(b + c) = ab + ac$ holds for all integers. It also holds for all rational numbers, for all real numbers, and even for all complex numbers. If a, b, c are residue classes $\pmod m$, does it follow that $a(b + c) \equiv ab + ac \pmod m$?

8. Let a and m be fixed, with $m > 1$. Let f be the function that takes each residue class $x \pmod m$ to the residue class $x+a \pmod m$. Is this function a permutation? If so, what is its cycle structure?

9. Suppose we have a triangular array of dots, with n dots on a side; the case $n = 9$ is depicted below. Suppose you have small equilateral triangles that are just large enough to cover three dots. For what values of n can these triangles cover all the dots, without overlapping? (It may be too much to expect a resolution of this for all values of n—just prove what you can.)



10. Suppose you have toothpicks that are just long enough to cover three consecutive dots in the pattern above. Show, for as many values of n as you can, that it is impossible to arrange the toothpicks so as to cover all the dots without overlapping.

11. For what values of m and n can an $m \times n$ rectangle be tiled by 1×2 blocks?

12. For what values of m and n can an $m \times n$ rectangle be tiled by 2×3 blocks?

13. For what values of m and n can an $m \times n$ rectangle be tiled by 2×4 blocks?

14. Suppose we have blocks that are 2×4, and also blocks that are 3×5. If m and n are sufficiently large, can we tile an $m \times n$ rectangle with these blocks?

15. A square array of numbers is called a *magic square* if the sum of the numbers in any row, or any column, is the same. Suppose we have an $n \times n$ magic square in which each of the numbers $1, 2, \dots, n^2$ occurs exactly once. What is the common value of the row and column sums?

16. Suppose you have an $n \times n$ square made of n^2 unit squares. Let a and b be given, with $0 \le a < n$ and $0 \le b < n$. Make a mark in one of the unit squares, and then move a places to the right and b places down. Any time you pass the right hand edge you start again on the left; any time you pass the bottom you start again at the top. Repeatedly make marks and move, until you land in a square that already has a mark in it. How many marks did you make? Did you land in the first square marked?

17. Proceed as above, but whenever you land in a marked square, make a further move α places to the right and β places down. Describe what happens, for various values of the parameters.

18. Proceed as above, but put a 1 in the first square, a 2 in the second square, and so on. Does this produce a magic square? Try this with $n = 3$, $a = b = \alpha = 1$, $\beta = 2$.

19. What is 365 (mod 7)? Given that July 4, 1998 was a Saturday, what day of the week was July 4, 1999? Assuming that n is not divisible by 100, the year n is a leap year if and only if $4 \mid n$. Assuming that the years n and $n + 12$ fall within the same century, what is the relationship between the calendar in year n and in year $n + 12$?

WILD PROBLEMS

1. *Magic Fifteens* is a game played as follows: There are 9 cards, each bearing one of the numbers $1, 2, \dots, 9$; they are face up. The two players alternately choose a card. The first player to possess three cards whose sum is 15 is the winner. Analyze this.

2. Alice and Bob have a pile of n sticks. They take turns removing sticks from the pile. On each turn a player must remove at least one stick, but never more that three sticks. The player who takes the last stick wins. Suppose that Alice moves first. Determine, for each n, which of them can force a win, and describe the winning strategy.

3. Suppose a rectangle is tiled by finitely many sub-rectangles, and that each of the sub-rectangles has the property that at least one of its side-lengths is an integer. Must the big rectangle also have this property?

Chapter VIII
Cancellation and Inverses modulo m

Programs Used: CngArTab, GCD, LinCon, LnCnDem

Just as we can add residue classes (mod m), we can multiply them. In the case of $m = 7$, the multiplication table is as follows:

$\otimes$	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

Except in the top row, where all entries are 0, we see in each row that the values $0, 1, 2, 3, 4, 5, 6$ each occur once, in some permuted order. However, the situation is not always so simple. Consider the case of $m = 6$:

$\otimes$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

In rows 1 and we see each of the possible values $0, 1, 2, 3, 4, 5$, each occurring once, in rows 1 and 5. However, in the other rows we see a fewer number of values, each repeated a larger number of times.

Explorations

1. Show that if $a \equiv \alpha \pmod{m}$ and $b \equiv \beta \pmod{m}$ then $ab \equiv \alpha\beta \pmod{m}$.

2. Suppose that $5x \equiv 2 \pmod{6}$. What possible values might x have, (mod 6)?

3. Suppose that $5x \equiv 5y \pmod{6}$. Does it follow that $x \equiv y \pmod{6}$?

4. Find the solutions of the congruence $4x \equiv 2 \pmod{6}$.

5. If $4x \equiv 4y \pmod{6}$, does it follow that $x \equiv y \pmod{6}$?

6. Suppose that a is one of the numbers $1, 2, 3, 4, 5, 6$, and that x_1 is found so that $ax_1 \equiv 1 \pmod{7}$. Suppose that x_2 is chosen so that $ax_2 \equiv 2 \pmod{7}$. What is the relation, if any, between x_1 and x_2?

7. Let m be given. Let $\mathcal{A}_1$ be the set of those $a \pmod{m}$ such that the congruence $ax \equiv 1 \pmod{m}$ has a solution. Let $\mathcal{A}_2$ be the set of those $a \pmod{m}$ such that the congruence $ax \equiv b \pmod{m}$ has a unique solution for every b. Let $\mathcal{A}_3$ be the set of those $a \pmod{m}$ such that the congruence $ax \equiv 0 \pmod{m}$ has a solution with $x \not\equiv 0 \pmod{m}$. Using the program **CngArTab**, determine these sets for various small values of m. Formulate a conjecture concerning the relationships between these sets.

8. Using **CngArTab** with $m = 15$, find the set $\mathcal{A}_1$ defined in question **7**. What is the relation between these numbers a and m? Try other m, if necessary, until a pattern emerges. Formulate a conjecture.

9. Solutions of the linear congruence $ax \equiv b \pmod{m}$ are provided by the program **LinCon**. Try typing `lincon 3 4 5 <Return>`. For small m, the solutions of the linear congruence may be found by inspecting row a of the multiplication table created by **CngArTab**. By experimenting with these programs, try to determine those triples a, b, m for which the congruence has a solution. When a solution exists, how many solutions are there?

10. Suppose that $ax \equiv 1 \pmod{m}$. If $au \equiv av \pmod{m}$ then by multiplying both sides by x we find that $u \equiv v \pmod{m}$. That is, if a has an inverse (namely x) (mod m), then we can cancel by a. Are there any other values of $a \pmod{m}$, other than those in $\mathcal{A}_1$, for which $au \equiv av \pmod{m}$ implies that $u \equiv v \pmod{m}$?

11. Suppose that $ax \equiv 1 \pmod{m}$, and that $ay \equiv 1 \pmod{m}$. Does it follow that $x \equiv y \pmod{m}$?

If $ax \equiv 1 \pmod{m}$ then we call x the *inverse* of a modulo m. We could write a^{-1} for this, to do so would cause confusion with the rational number $1/a$. Instead, we often let $\overline{a}$ denote a number such that $a\overline{a} \equiv 1 \pmod{m}$.

12. Solutions of linear congruences are calculated by applying the extended Euclidean algorithm. This procedure is demonstrated by the program **LnCnDem**. Try typing `lncndem 21 3 34 <Return>`. Try a triple a, b, m in which the congruence has no solution. Try a triple in which there is more than one solution.

13. Let a and m be given, and let f be the function that takes the residue class $x \pmod{m}$ to the residue class $ax \pmod{m}$. Under what circumstances is this function a permutation of the residue classes?

14. When the function described above is a permutation, describe its cycle structure.

15. A two digit number has the property that the product of its digits is 1/2 the number. What is the number?

WILD PROBLEMS

1. Each of n old ladies has a newsworthy item, and each such piece of gossip is distinct from the others. How many letters must they send before they all know all the gossip? The letters are sent sequentially, not simultaneously, and a lady can include in her letters all the information she knows.

2. Each of n talkative old men has a newsworthy item, and each such piece of gossip is distinct from the others. How many telephone calls must they make before they all know all the gossip? The calls are placed sequentially, not simultaneously, and two men can exchange all the information they know during a call.

ALCOHOL AND MATHEMATICS DON'T MIX:
DON'T DRINK AND DERIVE

Chapter IX
Factorials and Powers modulo m

Programs Used: FctrlTab, **PolySolv**, **PowerTab**, **Power**, **Order**, **OrderTab**, **Phi**, **Mult**, **R2D**

We now consider patterns that arise when the sequence of factorials 1!, 2!, 3!, ... is considered modulo m. Apart from one or two known properties, very little structure has been discovered in this sequence. Hence anything you observe might be a new discovery! We also investigate the sequence of powers of a number, 1, a, a^2, a^3, ... modulo m. Here many properties can be discovered. Some of these we can prove now, but others may remain as conjectures until later.

Explorations

1. Use the program **FctrlTab** to investigate the following question: What is $(p-1)!$ (mod p), when p is prime?

2. Using **FctrlTab** as above, what is $(p-2)!$ (mod p) ? What is $(p-3)!$ (mod p) ?

3. The program **PolySolv** allows you to define a polynomial $P(x)$, and choose a modulus m. With this information, it will then count the number of solutions of the congruence $P(x) \equiv 0 \pmod{m}$, and it will display up to 100 solutions. Using **PolySolv**, find the roots of the congruence $x^2 \equiv 1 \pmod{p}$ for various primes p. (That is, take $P(x) = x^2 - 1$.) Formulate a conjecture, and prove it.

4. As k tends to infinity with m fixed, the residue class $k!$ (mod m) is very easy to describe. What is this residue class, and why?

5. The program **PowerTab** displays the sequence $1, a, a^2, a^3, \ldots$ modulo m. By experimenting with various a and m, try to guess whether this sequence is always eventually periodic. Can you prove your conjecture?

6. Using **PowerTab** as above, try to describe the pairs a, m for which the sequence 1, a, a^2, a^3, ... (mod m) is purely periodic. Can you prove your conjecture?

7. For which a (mod m) is it true that $a^k \equiv 1 \pmod{m}$ for some positive integer k ?

Let a and m be given. If h is the least positive integer such that $a^h \equiv 1 \pmod{m}$, then h is called the *order* of a modulo m.

8. The only residue class a of order 1 modulo m is $a \equiv 1 \pmod{m}$. If p is prime, how many residue classes a have order 2 modulo p ?

9. If a has order h modulo m, and k is a positive integer such that $a^k \equiv 1 \pmod{m}$, then how is k related to h ?

10. Using **PowerTab**, determine the order of a modulo 7 for each a, $0 < a < 7$. Repeat this for several larger primes, noting the orders that occur. Formulate a conjecture.

The value of a^k modulo m can be determined by employing the program **PowerTab**, but for a single such value, the program **Power** is more convenient. For example, to determine the value of $2^{50} \pmod{101}$, type `power 2 50 101 [Enter]`. Similarly, the order of a modulo m is provided by the program **Order**. To determine the order of 2 modulo 101, type `order 2 101 <Return>`.

11. If r and s are positive integers such that $r \equiv s \pmod{7}$, does it follow that $2^r \equiv 2^s \pmod{7}$?

The residue classes a modulo m such that $(a, m) = 1$ are called the *reduced residue classes*. We let $\phi(m)$ denote the number of reduced residue classes. That is, $\phi(m)$ is the number of integers a, $1 \le a \le m$ such that $(a, m) = 1$. The function $\phi(m)$ is known as the *Euler phi function*. A table of values of $\phi(m)$ is provided by the program **ArFcnTab**; individual values may be obtained by typing `phi m <Return>`.

12. Using the programs **Order** and **Phi**, compare the order of a modulo m with $\phi(m)$ for various a and m. Formulate a conjecture relating these quantities.

13. Explain why $\phi(p) = p - 1$. Use **Phi** to evaluate $\phi(p^k)$ for various primes p, with $k > 1$. Can you guess a formula for this? Can you prove it?

14. The sequence $1,\ 2,\ 2^2,\ 2^3, \ldots \pmod{21}$ is purely periodic. With what period? What are the members of this sequence? Consider the sequence $5,\ 5 \cdot 2,\ 5 \cdot 2^2,\ 5 \cdot 2^3, \ldots \pmod{21}$. Is this purely periodic? With what period? What are the members of this sequence? Is there any overlap between these two sequences? List the reduced residue classes modulo 21. Note: The numbers $2^k \pmod{21}$ are provided by **PowerTab**, but there is no similar program that will give the numbers $5 \cdot 2^k \pmod{21}$. However, the program **Mult** makes it convenient to multiply residue classes. To find $11 \cdot 5 \pmod{21}$, for example, type `mult 11 5 21 <Return>`.

15. What are the powers of 12 modulo 19 ? Choose b so that $(b, 19) = 1$, with b not a power of 12 (mod 19). Compute the sequence $b,\ b \cdot 12,\ b \cdot 12^2,\ b \cdot 12^3, \ldots \pmod{19}$.

Is this sequence purely periodic? With what period? Is there any overlap with the powers of 12 ? Do these sequences, between them, exhaust the reduced residues modulo 19 ? If not, then choose a c that has not yet appeared, and compute the numbers $c,\ c \cdot 12,\ c \cdot 12^2,\ c \cdot 12^3, \ldots \pmod{19}$. Repeat this until the reduced residues are exhausted. Formulate a general conjecture, and try to prove it.

16. For various values of a and m, compare the order of a modulo m to the order of a^2 modulo m. Note the value of $\phi(m)$ in each instance. Formulate a conjecture.

17. For various values of a and m, compare the order of a modulo m to the order of a^3 modulo m. Note the value of $\phi(m)$ in each instance. Formulate a conjecture.

18. Formulate a general conjecture concerning the order of a^k modulo m in terms of the order of a modulo m and $\phi(m)$. Can you prove your conjecture?

19. Using **PolySolv**, determine the number of a of order 3 modulo p, for various primes p. Formulate a conjecture. Prove as much as you can.

20. Let p be an odd prime, and choose $k > 1$. Calculate the order of a modulo p^k for all reduced residues $a \pmod{p^k}$. What is the largest order that occurs? What happens if instead of p being an odd prime, the modulus is a power of 2 ? Formulate conjectures.

21. Using **PolySolv**, find all residue classes x such that $x^6 \equiv 1 \pmod{37}$. For each such x, use **Order** to determine the order of x modulo 37. In general, if x is a solution of $x^n \equiv 1 \pmod{m}$, what can you say about the order of x modulo m ?

22. What are the roots of the congruence $x^{p-1} \equiv 1 \pmod{p}$?

23. What are the roots of the congruence $x^p \equiv x \pmod{p}$?

24. What are the roots of the congruence $x^{\phi(m)} \equiv 1 \pmod{m}$?

Suppose that p is prime and that a is an integer with $p \nmid a$. The number a is called a *quadratic residue* of p if the congruence $x^2 \equiv a \pmod{p}$ has a solution; otherwise a is a *quadratic nonresidue* of p. To distinguish between the two possibilities we use the *Legendre symbol*, which is defined as follows:

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue of } p, \\ -1 & \text{if } a \text{ is a quadtratic nonresidue of } p, \\ 0 & \text{if } p \mid a. \end{cases}$$

25. Choose a prime number p, $p > 2$, and use **PowerTab** to compute the numbers $a^2 \pmod{p}$ for $0 \le a < p$. How many quadratic residues are there $\pmod{p}$? If a is a quadratic residue, how many x are there such that $x^2 \equiv a \pmod{p}$? How are these x related?

26. Explain why the numbers $1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2$ are all distinct (mod p). Determine the exact number of quadratic residues (mod p) for all primes p.

27. For all primes p, determine the value of the sum

$$\sum_{a=1}^{p} \left(\frac{a}{p}\right).$$

28. Let p be a prime number for which data was generated in question 25 above. Let $\mathcal{R}$ denote the set of quadratic residues that were found, and let $\mathcal{N}$ denote the quadratic nonresidues. Take two numbers from $\mathcal{R}$, and use **Mult** to determine their product (mod p). In which class does the product fall? Formulate a conjecture. Can you prove your conjecture?

29. Proceed as above, but now form the product of a member of $\mathcal{R}$ with a member of $\mathcal{N}$. Formulate a conjecture. Can you prove it?

30. Let p be a prime for which data was generated in question 25, and put $k = (p-1)/2$. Let $r_1, r_2, \ldots, r_k$ denote the quadratic residues that were formed. Choose a quadratic nonresidue of p, and call it n. Use **Mult** to compute the numbers $nr_1, nr_2, \ldots, nr_k \pmod{p}$. What are these numbers? Can you prove that this persists in general?

31. Proceed as in question **28** above, but now multiply two quadratic nonresidues. Formulate a conjecture. Try using your work on the preceding problem to prove your conjecture.

32. Let p be an odd prime. Explain why

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

for all integers a and b.

33. For several prime numbers p, apply **PolySolv** to locate roots of the congruence $x^2 + 1 \equiv 0 \pmod{p}$, and thus determine whether -1 is a quadratic residue or quadratic nonresidue of p. Can you find a simple way of predicting which it will be? There is a pattern in the data—can you spot it?

34. Let p be a prime for which you gathered data in question 25, and let $k = (p-1)/2$. For $0 \le a < p$, use the program **Power** to calculate $a^k \pmod{p}$. Formulate a conjecture relating this value to your findings in question 25.

35. Let p be an odd prime. By applying **Polysolv** to the congruence $x^2 - 2 \equiv 0 \pmod{p}$, determine the value of $\left(\frac{2}{p}\right)$. Repeat this for many primes, until a pattern emerges.

36. Let p and q be odd primes. By applying **Polysolv** to the congruence $x^2 - p \equiv 0 \pmod{q}$, determine the value of $\left(\frac{p}{q}\right)$. Similarly, find $\left(\frac{q}{p}\right)$. Repeat this for many pairs of primes, until a pattern emerges.

37. Suppose that $(10, m) = 1$. Is there any relation between the order of 10 modulo m and the period of the decimal expansion of $1/m$? Experiment, using **Order** and **R2D**, and formulate a conjecture. Can you prove your conjecture?

We conclude with some observations concerning algorithms that may be used in our calculations. The current status of factorials (mod m) and powers (mod m) is very different. In certain special circumstances we know the value of $k! \pmod{m}$, for example $(p-1)! \pmod{p}$, but in general the only way we have to calculate $k! \pmod{m}$ is to perform $k-1$ multiplications, reducing modulo m as we go. In contrast, it is very easy to calculate $a^k \pmod{m}$, even when k is large. To see why this is so, suppose that the binary expansion of k is $d_r d_{r-1} \cdots d_0$. That is, $k = \sum_{i=0}^{r} d_i 2^i$. Hence

$$a^k = a^{\sum d_i 2^i} = a^{d_0} a^{d_1 2} a^{d_2 2^2} \cdots a^{d_r 2^r} = a^{d_0} (a^2)^{d_1} \left(a^{2^2}\right)^{d_2} \cdots \left(a^{2^r}\right)^{d_r}.$$

It is easy to calculate the numbers $a, a^2, a^{2^2}, a^{2^3}, \cdots, a^{2^r} \pmod{m}$ by repeated squaring. With these values in hand, it remains to multiply together those values corresponding to i for which $d_i = 1$. For example, to calculate $a^{13} \pmod{m}$, we note that the binary expansion of 13 is 1101. Hence $a^{13} = a^{1+4+8} = a\, a^4\, a^8$. We calculate $a_1 \equiv a^2 \pmod{m}$, $a_2 \equiv a_1^2 \equiv a^4 \pmod{m}$, and $a_3 \equiv a_2^2 \equiv a^8 \pmod{m}$, and then $a^{13} \equiv a a_2 a_3 \pmod{m}$. In general, this requires $r-1$ multiplications of residue classes (to calculate $a^2, a^4, \ldots a^{2^r} \pmod{m}$), plus an additional $w(k)-1$ multiplications of residue classes, where $w(k)$, known as the *binary weight* of k, is the number of 1's in the binary expansion of k. The process of calculating the binary expansion of k (trailing digits first), and the repeated squaring, can be merged into one step, as follows: If k is even, say $k = 2k'$, then $a^k = (a^2)^{k'}$. We calculated $a^2 \pmod{m}$; this leaves us with another powering problem, but with an exponent that is half the size of the former one. If k is odd, say $k = 2k'+1$, then we write $a^k = a(a^2)^{k'}$. Again, we calculate $a^2 \pmod{m}$. In the example already considered, this would lead us to write

$$\begin{aligned} a^{13} &= a(a^{12}) = a(a^2)^6 \equiv a(a_1)^6 \pmod{m} \\ &= a(a_1^2)^3 \equiv a(a_2)^3 \pmod{m} \\ &= a a_2 (a_2^2) \equiv a a_2 a_3 \pmod{m}. \end{aligned}$$

38. Suppose you had a quick method for calculating $k! \pmod{m}$. Explain how this could be used to create a quick method for factoring m.

39. The program **PowerDem** demonstrates the powering algorithm described above. Apply this program to various numbers, until the procedure is clear to you. How many residue class multiplications are required to calculate $2^{50} \pmod{101}$?

40. Our efficient method for calculating powers can be used to prove compositeness of many numbers. For example, use **Power** to calculate $2^{580} \pmod{581}$, and explain how you can deduce that 581 is composite. In this example, 581 is so small that we could also prove its compositeness by calculating its prime factorization, but our method can be applied easily to numbers that are much too large to factor.

The method of proving compositeness employed above is not always successful. For example, 341 is composite, but $2^{340} \equiv 1 \pmod{341}$. In general, if $a^{m-1} \equiv 1 \pmod{m}$ then m is called a *base a probable prime*. If m is a base a probable prime but is nevertheless composite, then m is called a *base a pseudoprime*. Thus 341 is a base 2 pseudoprime. In the case of this number, its compositeness could be affirmed by changing to the base 3, since $3^{340} \not\equiv 1 \pmod{341}$. However, there do exist composite integers m that are base a pseudoprimes for all a relatively prime to m, the first example being $m = 561$. Such m are called *absolute pseudoprimes*, or *Carmichael numbers*. From the work of Carmichael early this century it seemed likely that there exist infinitely many Carmichael numbers, but the proof of this was only achieved in 1995. There is a more elaborate test, called the *strong pseudoprime test*, which still depends only on powering, and which does not suffer from the defect of the simple pseudoprime test. Thus, in practice, we are able to prove that m is composite, even when m is extremely large, although the proof is indirect, and generally does not reveal anything about the factors of m.

WILD PROBLEMS

1. What is the sum of the digits of the sum of the digits of the sum of the digits of 4444^{4444} ?

2. During a lecture with an audience of 5 people, each member of the audience fell asleep exactly twice. For each pair of members of the audience, there was a moment when they were both asleep. Prove that there was a time when at least three members of the audience were asleep.

3. Show that a product of four consecutive positive integers cannot be a perfect square or a perfect cube.

Chapter X
The Chinese Remainder Theorem

Programs Used: **ResComp**, **IntAPTab**, **CRT**, **ArFcnTab**, **Phi**, **DivTab**, **CRTDem**, **Mult**, **LinCon**, **LnCnDem**

Let m be a fixed positive integer. For any integer a, let $\mathcal{A}_a$ be the set of all integers x such that $x \equiv a \pmod{m}$. Thus $\mathcal{A}_a$ is an arithmetic progression,

$$\mathcal{A}_a = \{\dots, -3m+a, -2m+a, -m+a, a, m+a, 2m+a, 3m+a, \dots\}.$$

If a and b are two integers, then $\mathcal{A}_a = \mathcal{A}_b$ if $a \equiv b \pmod{m}$, and $\mathcal{A}_a$ is disjoint from $\mathcal{A}_b$ if $a \not\equiv b \pmod{m}$. Moreover, every integer is contained in one of the sets $\mathcal{A}_0, \mathcal{A}_1, \dots, \mathcal{A}_{m-1}$. That is,

(1) If $0 \le a < b < m$ then $\mathcal{A}_a \cap \mathcal{A}_b = \emptyset$;
(2) $\mathbb{Z} = \bigcup_{a=0}^{m-1} \mathcal{A}_a$.

When a family of subsets has these two properties, we say that they *partition* the set. In this case, the residue classes modulo m partition the integers.

In the above discussion we had only one modulus. Suppose now that we have two moduli, m and n. For given integers a and b, we want to find all integers x such that

$$\begin{aligned} x &\equiv a \pmod{m}, \\ x &\equiv b \pmod{n}. \end{aligned} \tag{1}$$

That is, we seek to determine the intersection of two arithmetic progressions.

Explorations

1. The program **ResComp** allows you to COMPare the RESidue class of $x \pmod{m}$ with the residue class $x \pmod{n}$. Take $m = 3$, $n = 5$, and look for integers x such that $x \equiv 2 \pmod{3}$, $x \equiv 3 \pmod{5}$. Using `PgUp` and `PgDn`, find all such x in the range $-50 \le x \le 50$. Repeat this with another pair (a, b), where a is determined (mod 3) and b is determined (mod 5). For each x the program displays a pair (a, b). Is this sequence of pairs periodic? If so, with what period?

2. Using **ResComp** as above, find all x such that $x \equiv 7 \pmod{10}$ and $x \equiv 2 \pmod{12}$. More generally, which pairs (a, b) occur? Here a is determined (mod 10), and b is determined (mod 12). Of the pairs that occur, how often do they occur?

For each integer x, the program **ResComp** provides a pair (a, b). The program **IntAPTab** does the opposite—it generates a TABle of the INTersections of two Arithmetic Progressions. That is, for a given pair (a, b), this program specifies the set of solutions to the simultaneous congruences (1). In each case, the set of solutions is either empty, or else is an arithmetic progression. Note that the rows of the table are indexed by $a \pmod{m}$, while the columns are indexed by $b \pmod{n}$.

3. In the program **IntAPTab**, take $m = 3$, $n = 5$, and note the table that is generated. Next take $m = 10$, $n = 12$. What happens if $m = n$? For what pairs (m, n) is it true that the congruences (1) have a solution for all choices of a and b? Formulate a conjecture. Can you prove your conjecture?

The description of the intersection of two arithmetic progressions was known to the Chinese in the first century A.D., and the central theorem on this topic is known today as the Chinese Remainder Theorem. The program **CRT** provides the intersection of two arithmetic progressions, from the DOS command line. Try typing `crt 2 3 3 5` `<Return>`.

4. When $(m, n) = 1$ we have a one-to-one correspondence $x \leftrightarrow (a, b)$ between residue classes $x \pmod{mn}$ and pairs (a, b) where a is a residue class $\pmod{m}$ and b is a residue class $\pmod{n}$. In the table generated by **IntAPTab**, the value of a is indicated at the left; it is printed in white if $(a, m) = 1$, otherwise it is printed in yellow. Similarly, the column heading b is printed in white if $(b, n) = 1$, otherwise in yellow. Finally, the corresponding value $x \pmod{mn}$ is printed in white if $(x, mn) = 1$; otherwise it is printed in yellow. By experimenting with **IntAPTab**, try to formulate a guess as to which pairs (a, b) give rise to x such that $(x, mn) = 1$. Can you prove your conjecture?

5. How is $\phi(mn)$ related to $\phi(m)$ and $\phi(n)$ when $(m, n) = 1$? Use the program **ArFcnTab** and/or **Phi** to investigate. Can you prove your conjecture, using the result of the preceding problem?

6. Devise a formula for $\phi(m)$ in terms of the prime factorization of m. (Recall that a formula for $\phi(p^k)$ has already been established.)

7. How is $\phi(mn)$ related to $\phi(m)\phi(n)$ when $(m, n) > 1$? Experiment, and form a conjecture. Can you prove it?

8. Using **ArFcnTab**, or otherwise, find all integers m such that $\phi(m)$ is odd. Can you prove that there are no further such numbers?

9. For each integer k, $1 \le k \le 20$, find the number of solutions x of the equation $\phi(x) = k$. Do you find any k for which the number of solutions is exactly 1?

10. The expression $\sum_{d|n} \phi(d)$ denotes the sum of $\phi(d)$ over all positive divisors d of n. Thus

$$\sum_{d|6} \phi(d) = \phi(1) + \phi(2) + \phi(3) + \phi(6) = 1 + 1 + 2 + 2 = 6.$$

For several values of n, use **DivTab** to generate a list of the positive divisors of n. Then use **Phi** to evaluate the Euler phi-function of the divisors. In this way, compute $\sum_{d|n} \phi(d)$. Formulate a conjecture concerning the value of this sum. Can you prove your conjecture?

11. The program **CRT** determines the solution of (1) by reducing the problem to solving a linear congruence. Try typing `crtdem 2 3 3 5 <Return>` for an explanation of the reasoning involved. Apply **CRTDem** to several situations, until you understand the approach. Without using any programs, find the solutions of the simultaneous congruences

$$\begin{aligned} x &\equiv 7 \pmod{37}, \\ x &\equiv 11 \pmod{73}. \end{aligned}$$

Use appropriate programs (**Mult**, **LinCon**, **LnCnDem**, **CRT**, **CRTDem**, etc.) to verify your calculations.

12. What would you do if you had to find the intersection of three or more arithmetic progressions? Using whatever programs are suitable, find those x such that

$$\begin{aligned} x &\equiv 2 \pmod{3}, \\ x &\equiv 3 \pmod{5}, \\ x &\equiv 5 \pmod{7}, \\ x &\equiv 7 \pmod{11}, \\ x &\equiv 11 \pmod{13}. \end{aligned}$$

13. Suppose that I choose n cards from a pack of 52. I find that I can deal my cards to 5 people, and they come out evenly. However, when I deal my cards to 11 people, I have 2 cards left over. What is n?

14. Suppose that $(m, n) = 1$, and that you have an $m \times m$ magic square employing the numbers $1, 2, \ldots, m^2$ and an $n \times n$ magic square using the numbers $1, 2, \ldots, n^2$. Can you use them to construct an $mn \times mn$ magic square containing the numbers $1, 2, \ldots, (mn)^2$?

WILD PROBLEMS

1. Suppose that you have a balance scale, and eight coins. Either they are all the same weight, or else seven of them have the same weight and one of them is lighter. By making at most two weighings, determine whether there is a lighter coin, and identify which one it is, if it exists.

2. Suppose that you have a balance scale, and twelve coins. Eleven of them have the same weight, but one of them has a different weight. In at most three weighings, find the false coin.

Chapter XI
Public Key Cryptography

Programs Used: Factor, Phi, LinCon, Power, RSAPars, RSA

For centuries, one of the hazards of cryptography was that a copy of your code book might fall into enemy hands, so that all your encrypted transmissions could then be intercepted and decoded. Worse yet, you might have no way of knowing whether one of your communications stations had been taken over by the enemy: The enemy might be masquerading as one of your own troops. All this changed in 1976 when Whitfield Diffie and Martin Hellman proposed a form of encryption that should be easy to perform but would be difficult to break, even if the encryption procedure were made public. The scheme works like this: Suppose that Bob wants to receive a message from Alice without observers being able to read the message. Bob chooses a very large integer m, say $m \approx 10^{200}$, and defines a permutation π of the numbers $1, 2, \ldots, m$. The algorithm for computing π is made public, and in particular is given to Alice. The characters of Alice's message can be associated with digits in a standard way, and the digits can be broken into blocks of length not exceeding 200, so that Alice's message is equivalent to one or more integers t, each one in the interval $[1, m]$. Thus t is the *plaintext*. Alice computes $c = \pi(t)$; this is the *cryptotext*; it is also an integer in the interval $[1, m]$. Alice sends c to Bob. Since an observer may also gain access to c, for the security of the communication it is essential that there be no quick algorithm for computing the inverse permutation π^{-1}, since $t = \pi^{-1}(c)$. However, Bob possesses some secret information concerning π that allows him to compute π^{-1} quickly, and hence read Alice's message. A permutation with the peculiar property that π is easy to compute while π^{-1} is difficult (i.e., would take centuries on the fastest computers) is called a *trap door function*.

The success of the Diffie-Hellman scheme depends on being able to find trap door functions. This was achieved in 1977 by Ron Rivest, Adi Shamir, and Len Adleman. Their *RSA method* depends on the number theory that we have been investigating: Bob secretly chooses two 100-digit primes p_1, p_2, and sets $m = p_1 p_2$. Bob also chooses a large positive integer k with the property that $(k, \phi(m)) = 1$. Among the reduced residue classes $\pmod{m}$, the map $\pi(x) \equiv x^k \pmod{m}$ is a permutation. Bob makes m and k public, and Alice sends him $c \equiv t^k \pmod{m}$. (Recall that we have a powering algorithm that makes this easy.) Since Bob knows how to factor m, Bob knows the value of $\phi(m)$. Hence Bob can find a positive integer k' such that $kk' \equiv 1 \pmod{\phi(m)}$. (We use the extended Euclidean algorithm to solve linear congruences, so this is also fast.) We now show that the map $x \mapsto x^{k'} \pmod{m}$ is the inverse permutation that we need. To this end, choose q so that

$kk' = 1 + q\phi(m)$, and recall Euler's congruence, which asserts that if $(x, m) = 1$ then $x^{\phi(m)} \equiv 1 \pmod{m}$. Hence

$$(x^k)^{k'} = x^{kk'} = x^{1+q\phi(m)} = x(x^{\phi(m)})^q \equiv x(1)^q = x \pmod{m}.$$

Thus the decryption process for Bob is similar to Alice's encryption, but with the parameter k replaced by k'. Note that only Bob can calculate k'. Even Alice can't read her own message, once she's encoded it!

In the RSA method, the permutation being employed constitutes a trap door function only to the extent that large composite integers are difficult to factor. In the present state of knowledge one can factor a number of size 10^{150}, but there is no guarantee that there does not exist some factoring method yet to be discovered by which even much larger numbers could be factored quickly. One could imagine that such a method might be taken as a State Secret. Indeed, when Rivest, Shamir, and Adleman published their work in 1978, the Director of the National Security Agency (General Odum) gave serious consideration to going to Congress asking for legislation that would make all research in number theory "born classified" as is the case with atomic research. He was dissuaded from this, but in any case any lingering impression that number theory is the purest of the pure, totally devoid of practical application, has been forever dispelled.

Rivest, Shamir and Adleman patented their method, and formed the company RSA Data Systems to market RSA–based products. To emphasize the security of their system, they offered a prize of \$100 for the first decryption of the message

$$c = 96869613754622061477140922254355882905759991124574319874695120930816298225145708356931476622883989628013391990551829945157815154,$$

which was encrypted using the 129-digit modulus

$$m = 114381625757888867669235779976146612010218296721242362562561842935706935245733897830597123563958705058989075147599290026879543541$$

and the public exponent

$$k = 9007.$$

The estimate at that time was that it would take 40 trillion years to factor this m. However, on 29 April, 1994, Derek Atkins, Michael Graff, Arjen Lenstra, and Paul Leyland announced that $m = p_1 p_2$ where

$$p_1 = 3490529510847650949147849619903898133417764638493387843990820577,$$

$$p_2 = 32769132993266709549961988190834461413177642967992942539798288533.$$

This enabled them to determine the secret exponent,

$$k' = 106698614368578024442868771328920154780709906633937862801226224496631063125911774470873340168597462306553968544513277109053606095,$$

and consequently the plaintext

$$t = 200805001301070903002315180419000118050019172105011309190800151919090618010705.$$

After conversion[1] back to alphabetic characters, this reads

[1]Their protocol for converting is different from the one we propose in Table 1. See question 7 below.

THE MAGIC WORDS ARE SQUEAMISH OSSIFRAGE

Lenstra (at Bellcore) and his team used the double large prime variation of the multiple polynomial quadratic sieve factoring method. The calculation took more than 5000 mips years, and was executed over a period of 8 months on over 600 different computers that were made available for the purpose by volunteers in more than 20 countries, on all continents except Antarctica. The final stage of the computation took 45 hours on a 16K MasPar MP-1 massively parallel computer. The relatively short time that it took to factor RSA-129 is partly due to increased speed and power of computer hardware, but it is mainly due to progress that has been made in developing faster factoring algorithms.

The RSA-129 modulus was factored by combining the latest factoring algorithms with enormous computing resources. With larger moduli, the RSA method is considered to be secure, and is widely used. In the spring of 1996, Rivest (a mathematician at MIT) sold his interest in the company to a venture capital firm for $50,000,000. So being a mathematician is not only fun, but occasionally also profitable!

The program **RSA** automates the arithmetic operations that arise when executing the RSA algorithm. To use this program you will need a public modulus, a public exponent, and a secret exponent. Since typing such data from the keyboard is tedious and prone to error, it is best to keep the public parameters in a computer file. The program **RSAPars** will assist you in this. It is best to choose your private exponent k' first, since then you can take it to be something memorable, such as your parents' home phone number. Do not use your Social Security Number or something really sensitive, since you will be using a modulus $m < 10^{18}$, and hence any energetic person could use m and k to reconstruct k'. Since $(k', \phi(m)) = 1$, and since $\phi(m)$ is even when $m > 2$, your private exponent k' must be odd. Once you have chosen k', the program assists you in choosing a public modulus m, by selecting the prime factors of m. There is no need to enter a prime exactly. Simply enter an approximate size x, and the computer will find the least prime $p > x$ such that $(p - 1, k') = 1$. The program will not allow you to use the same prime twice, since it is advantageous for m to be squarefree (see question 4 below). Once you have entered two or more primes, and you are satisfied with the value attained, you can indicate that you are done, and the computer will find the complementary public exponent k. You may now save m and k to a file, so that others can use these values to send you a message. Choose a filename that identifies you, and add a tag number (Alice might take `alice1`), so that if you ever want to establish a second set of RSA parameters you will have a way of distinguishing them. The program takes '.pub' as the default extension of the file. After exiting, Alice can view the file that has been created by typing `type alice1.pub` `<Return>` at the DOS prompt, or by using Notepad.

Once Bob has the file `alice1.pub`, he can send her an encrypted message by using the **RSA** program. This program has no word-processing capabilities, so Bob must first compose a text file. This he can do by by opening Notepad. (In the Windows menuing system, open Start, choose Programs, then Accessories). After typing his plaintext, and saving saving his message to a file, say bob2alic.txt, he invokes **RSA**, where he can `Load` the `Plain` text file, and set the `Variables` by `Reading` them from `alice1.pub`. Each letter of the text needs to be converted to a two-digit `Code`; the codes are then concatenated to form a sequence of `Residues`. Each residue is taken to the power k modulo m to form a new sequence of residues. This is the Encryption. This new sequence of residues can be Saved to a file, whose name by default is `bob2alic.rsa`. In turn, Alice can Load the Cipher text and her Variables, including her secret Decrypting exponent k'. She can then Decrypt to

CODE	CHAR	ASCII	CODE	CHAR	ASCII	CODE	CHAR	ASCII	CODE	CHAR	ASCII
00		32	25	9	57	50	R	82	75	k	107
01	!	33	26	:	58	51	S	83	76	l	108
02	"	34	27	;	59	52	T	84	77	m	109
03	#	35	28	<	60	53	U	85	78	n	110
04	$	36	29	=	61	54	V	86	79	o	111
05	%	37	30	>	62	55	W	87	80	p	112
06	&	38	31	?	63	56	X	88	81	q	113
07	'	39	32	@	64	57	Y	89	82	r	114
08	(	40	33	A	65	58	Z	90	83	s	115
09	)	41	34	B	66	59	[	91	84	t	116
10	*	42	35	C	67	60	\	92	85	u	117
11	+	43	36	D	68	61	]	93	86	v	118
12	,	44	37	E	69	62	^	94	87	w	119
13	-	45	38	F	70	63	_	95	88	x	120
14	.	46	39	G	71	64	`	96	89	y	121
15	/	47	40	H	72	65	a	97	90	z	122
16	0	48	41	I	73	66	b	98	91	{	123
17	1	49	42	J	74	67	c	99	92	|	124
18	2	50	43	K	75	68	d	100	93	}	125
19	3	51	44	L	76	69	e	101	94	~	126
20	4	52	45	M	77	70	f	102	95	EoL	13
21	5	53	46	N	78	71	g	103	96	—	
22	6	54	47	O	79	72	h	104	97	—	
23	7	55	48	P	80	73	i	105	98	—	
24	8	56	49	Q	81	74	j	106	99	—	

Table 1. Character to Code Correspondence

recover the original plaintext sequence of residues. These can be separated to form `Codes`, and finally `Text`, which can be `Saved`. When dealing with encrypted files it is sometimes handy to have some indication as to what is in the file. When the **RSA** program reads a file, it looks for lines that begin with the symbol '%'. Such lines are passed to the destination without change. Hence Bob might put at the top of his message the line

```
% This is a message from Bob to Alice.
```

The **RSA** program also places the encryption history in such comment lines, so that the recipient will know what parameters have been used.

Before proceeding further we consider how to convert characters into numbers. This can be done in many ways. For example, we could let A correspond to 1, B to 2, ..., and Z to 26. Alternatively, computers store alphanumeric characters by their ASCII codes. (ASCII is an abbreviation for American Standard Code for Information Interchange.) The first of these methods makes no provision for punctuation, numerals, or lower case letters. The second provides all printable characters, but is inefficient because each character requires three digits (in base 10). The characters that can be typed in the standard keyboard have ASCII codes between 32 (to denote a space ' ') and 126 (for '~'). As a compromise between the two systems described above, we subtract 32 from each ASCII code to obtain a 2–digit number. These numbers run from 00 to 94. In order to preserve the line breaks in a file we need an end-of-line marker; we assign the code 95 for this purpose. Thus we have the codes in Table 1.

Explorations

1. Suppose that Bob took the (ridiculously small) modulus $m = 91$, and proposed the public exponent $k = 17$. Suppose that Alice sent him the encrypted message $c = 51$. Use the programs **Factor**, **Phi**, **LinCon**, and **Power** appropriately to recover her plaintext t.

2. The proof above that $x^{kk'} \equiv x \pmod{m}$ assumed that $(x, m) = 1$. If $m = p_1p_2$ where p_1 and p_2 are distinct primes, what is the probability that $(x, m) > 1$ when x is randomly chosen?

3. Show that if m is squarefree then the restriction to $(x, m) = 1$ is unnecessary. That is, if m is squarefree and $kk' \equiv 1 \pmod{\phi(m)}$, then $x^{kk'} \equiv x \pmod{m}$ for all integers x.

4. The encrypted message

355456249 475197422 636832086 601788838

was created using the modulus $m = 670726081$ and the public exponent $k = 663599161$. The program **RSA** will assist in decrypting this, but first you must determine the value of $\phi(m)$, and then solve the congruence $kk' \equiv 1 \pmod{\phi(m)}$. (Use **Factor** and/or **Phi**, and then **LinCon**.) Next use a text editor to create a file, say `prob4.rsa`, that consists of the line displayed above. Then type `rsa` `<Return>`, Load the `Cipher text` `prob4.rsa`, and enter the `Variables`. Type `Esc` to return to the main menu, and then `Decrypt`. The resulting residues can be separated into 2–digit `Codes`, which may be read as `Text`. What was the message?

5. Although Bob is the only person who can decrypt a message encrypted with his parameters, he has no way of knowing that the message actually came from Alice, since anyone can use his parameters. To overcome this defect, suppose that Bob has a trap door function π_B and that Alice also has a trap door function π_A. Suppose that Alice sends $c = \pi_B(\pi_A^{-1}(t))$ to Bob. What should Bob do, to decrypt this? Can anyone else decrypt it? Can Bob now be sure that the message came from Alice?

6. In the preceding problem there was a tacit assumption that the trap door functions π_A and π_B act on the same set of numbers. Suppose now that π_A permutes the residue classes modulo m_A, and that π_B permutes the residue classes modulo m_B. If $m_A \le m_B$ then we may still proceed as above, since we may consider $\pi_A^{-1}(t)$ as lying in the interval $[0, m_A)$, which defines a unique residue class m_B. How would you modify the above procedure if $m_A > m_B$?

7. In formulating their challenge, Rivest, Shamir and Adleman did not use the system in Table 1 to convert from alphanumeric characters to a residue class t. By comparing t with the stated text can you infer the system that they used instead?

8. Let $m = 854937209155735099$, and suppose that you are given the information that m has at most two prime factors, and that $\phi(m) = 854937207303842520$. Can you find the primes?

9. Suppose that $m = 1247 = 29 \cdot 43$, so that $\phi(m) = 1176$. In order that $x^{kk'} \equiv x \pmod{m}$ for all x, it is sufficient that $kk' \equiv 1 \pmod{\phi(m)}$, but is it necessary? Suppose that $k = 5$. How many k' are there, $0 \le k' < \phi(m)$, such that $x^{kk'} \equiv x \pmod{m}$ for all x? What if you take instead $k = 11$? Why is the number of admissible k' so large? To achieve security, the acceptable k' should be very rare. How should the prime factors of m be chosen, to achieve this?

WILD PROBLEMS

1. What integers can be written in the form $a^2 - b^2$?

2. Let $P(n)$ denote the number of (base 10) palindromes not exceeding n. Show that there are infinitely many n for which both n and $P(n)$ are palindromes.

Chapter XII
Sums of Two Squares

Programs Used: SumsPwrs, **WrngTab**, **FctrlTab**, **Mult**, **DivTab**, **Power**

The program **SumsPwrs** displays the representations of n as a sum of s k-th powers, and counts the number of representations in various ways. For sums of two squares we take $s = k = 2$. Try typing `sumspwrs 65 2 2 [Enter]`.

Explorations

1. The program **WrngTab** generates a table of the number of representations of n as a sum of s k-th powers. Type `wrngtab` <`Return`>, and then set $s = 2$, $k = 2$. By examining the values displayed on the initial screen, determine which primes p, $2 \le p < 200$, can be expressed as a sum of two squares. Can you find a pattern in your data?

2. When p is a prime that is represented as a sum of two squares, how many representations does it have? Formulate a conjecture.

3. For what n is $r(n)$ odd? If $2 \mid r(n)$, does it follow that $4 \mid r(n)$? Formulate conjectures.

4. Find n such that $8 \nmid r(n)$. Can you find a pattern in these n? Formulate a conjecture.

5. Choose a point (x, y) in the plane with $x \ge 0$, $y > 0$. Plot the points (x, y), $(-y, x)$, $(-x, -y)$, $(y, -x)$. Describe the geometric relation between these points. Explain why they are all distinct. Prove that if $n > 0$ then $4 \mid r(n)$.

6. Let $f(n) = r(n)/4$. If $(m, n) = 1$, how is $f(mn)$ related to $f(m)$ and $f(n)$? Experiment and form a conjecture.

7. Suppose that $m = x^2 + y^2$, and that $n = v^2 + w^2$. Show that $mn = (xv - yw)^2 + (xw + yv)^2$. Let $\mathcal{S}_2$ denote the set of numbers that can be expressed as a sum of two squares. Show that if $m \in \mathcal{S}_2$ and $n \in \mathcal{S}_2$ then $mn \in \mathcal{S}_2$. (Thus we say, "The set $\mathcal{S}$ is closed under multiplication.")

8. Suppose that $p = x^2 + y^2$. Choose $\overline{y}$ so that $0 < \overline{y} < p$ and $y\overline{y} \equiv 1 \pmod{p}$. Put $u = x\overline{y}$. Show that $u^2 \equiv -1 \pmod{p}$. Deduce that $u^{p-1} \equiv (-1)^{(p-1)/2} \pmod{p}$. Deduce that $p \equiv 1 \pmod{4}$.

9. Using the program **FctrlTab**, determine the value of $u = ((p-1)/2)! \pmod{p}$ for several primes p. Using **Mult**, find the value of $u^2 \pmod{p}$ for these same p. Formulate a conjecture. Use Wilson's congruence to prove it.

10. Let $d_1(n)$ denote the number of positive divisors d of n such that $d \equiv 1 \pmod{4}$, and similarly let $d_3(n)$ denote the number of positive divisors d of n such that $d \equiv 3 \pmod{4}$. Use **DivTab** to evaluate $d_1(n)$ and $d_3(n)$ for several n. How is $d_1(n) - d_3(n)$ related to $r(n)$? Formulate a conjecture.

11. Let

$$\chi(n) = \begin{cases} 1 & \text{if } n \equiv 1 \pmod{4}, \\ -1 & \text{if } n \equiv 3 \pmod{4}, \\ 0 & \text{otherwise.} \end{cases}$$

Note that $d_1(n) - d_3(n) = \sum_{d|n} \chi(d)$. Show that $\chi(mn) = \chi(m)\chi(n)$ for *all* pairs of integers m, n.

12. Suppose that $p \equiv 1 \pmod{4}$, and that u has been found so that $u^2 \equiv -1 \pmod{p}$. We wish to find x and y so that $x^2 + y^2 = p$. Explain why there exist integers a and x with $0 < x < \sqrt{p}$ such that

$$\left| \frac{u}{p} - \frac{a}{x} \right| < \frac{1}{x\sqrt{p}}.$$

(Recall question 10 of Chapter V.) Put $y = ux - ap$. Explain why $|y| < \sqrt{p}$. Show that $x^2 + y^2 \equiv 0 \pmod{p}$ and that $0 < x^2 + y^2 < 2p$. Deduce that $x^2 + y^2 = p$.

13. Suppose that $p = x_1^2 + y_1^2 = x_2^2 + y_2^2$ with all variables positive. Suppose that u has been determined so that $u^2 \equiv -1 \pmod{p}$, that $y_1 \equiv ux_1 \pmod{p}$, and $y_2 \equiv ux_2 \pmod{p}$. Explain why $x_1y_2 \equiv x_2y_1 \pmod{p}$. Explain why $0 < y_2x_1 < p$ and $0 < y_1x_2 < p$. Deduce that $y_2x_1 = y_1x_2$. Explain why $(x_1, y_1) = 1$. Deduce that $x_1 = x_2$, $y_1 = y_2$. That is, each residue class u such that $u^2 \equiv -1 \pmod{p}$ is associated with at most one representation of p with positive variables. Conclude that if $p > 2$ then the equation $p = x^2 + y^2$ has exactly 2 solutions in positive variables. That is, $r(p) = 8$ for all odd p.

14. In order to construct representations of p as a sum of two squares, it is useful to have a number u such that $u^2 \equiv -1 \pmod{p}$. We may take $u = ((p-1)/2)!$, but this is not very useful in practice, since the calculation involves $\approx p$ multiplications. Choose x at random, $0 < x < p$, and form the number $u \equiv x^{(p-1)/4} \pmod{p}$, using the program **Power**. Then use **Mult** to compute $u^2 \pmod{p}$. For one fixed $p \equiv 1 \pmod{4}$, do this for several x. What values of u^2 arise? With what relative frequency? Is this a fast (probabilistic) method for finding u so that $u^2 \equiv -1 \pmod{p}$?

Chapter XIII
Binomial Coefficients

Program Used: PascalsT

Pascal's Triangle is the familiar pattern of binomial coefficients

$$\begin{array}{ccccccccccccccc} &&&&&&& 1 &&&&&&& \\ &&&&&& 1 && 1 &&&&&& \\ &&&&& 1 && 2 && 1 &&&&& \\ &&&& 1 && 3 && 3 && 1 &&&& \\ &&& 1 && 4 && 6 && 4 && 1 &&& \\ && 1 && 5 && 10 && 10 && 5 && 1 && \\ & 1 && 6 && 15 && 20 && 15 && 6 && 1 & \\ 1 && 7 && 21 && 35 && 35 && 21 && 7 && 1 \\ &&&&&&& \vdots &&&&&&& \end{array}$$

Before considering what number-theoretic properties these numbers might have, we first establish some basic formulas and notation.

Let $\mathcal{S}$ be a set containing exactly n elements. The *binomial coefficient* $\binom{n}{k}$ is the number of subsets of $\mathcal{S}$ that contain exactly k elements. In conversation, we refer to the binomial coefficient as "n choose k". Since the emptyset $\emptyset$ is a subset of any set, we have $\binom{n}{0} = 1$ for all non-negative integers n. Similarly, since there is only one subset of $\mathcal{S}$ containing n elements, namely $\mathcal{S}$ itself, we have $\binom{n}{n} = 1$ for all non-negative integers n. Clearly $\binom{n}{k} = 0$ if $k < 0$ or if $k > n$. We now derive a formula for $\binom{n}{k}$ when $0 < k < n$. Suppose we list the elements of $\mathcal{S}$ in some order, say $e_1, e_2, \ldots, e_n$. We could take our subset to be the first k of these, $\mathcal{T} = \{e_1, e_2, \ldots, e_k\}$. There are $n!$ ways of forming the initial list of n elements, since any one of n of them can come first, any one of $n-1$ of them can come second, and so on. However, we must consider how many times a particular subset $\mathcal{T}$ arises in this way. There are $k!$ orders in which the elements of $\mathcal{T}$ can be listed, and there are $(n-k)!$ orders in which the remaining $n-k$ elements can be listed. Thus there are $k!(n-k)!$ ways of listing the elements of $\mathcal{S}$ so that the same k elements lie in the first k positions. That is, when we list the elements of $\mathcal{S}$ in the $n!$ different ways, each subset of size k occurs in the first k positions exactly $k!(n-k)!$ times. Hence

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} \tag{1}$$

for $0 \le k \le n$.

The familiar rule for forming a row of Pascal's Triangle from the row immediately above it depends on the formula

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}. \tag{2}$$

This is easy to prove using the formula (1), since the right hand side above is

$$\begin{aligned}\frac{(n-1)!}{(k-1)!(n-k)!} + \frac{(n-1)!}{k!(n-1-k)!} &= \frac{(n-1)!}{(k-1)!(n-1-k)!} \cdot \Big(\frac{1}{n-k} + \frac{1}{k}\Big)\\ &= \frac{(n-1)!}{(k-1)!(n-1-k)!} \cdot \frac{n}{(n-k)k}\\ &= \frac{n!}{k!(n-k)!}.\end{aligned}$$

This gives (2). It is instructive to note that we can prove (2) by combinatorial reasoning, without using (1). To do this, note first that of subsets $\mathcal{T}$ of $\mathcal{S}$ containing exactly k elements can be divided into two classes, according as to whether $e_n \in \mathcal{T}$ or not. Suppose that $e_n \in \mathcal{T}$. To determine the remaining elements of $\mathcal{T}$ we must choose $k-1$ elements from among $\{e_1, e_2, \dots, e_{n-1}\}$. There are $\binom{n-1}{k-1}$ ways of doing this. Now consider those subsets $\mathcal{T}$ for which $e_n \notin \mathcal{T}$. To determine the elements of $\mathcal{T}$, we must choose k elements from $\{e_1, e_2, \dots, e_{n-1}\}$. There are $\binom{n-1}{k}$ ways of doing this. On combining these two counts, we obtain (2) again.

The *Binomial Theorem* asserts that

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}. \tag{3}$$

To see why this should be so, think of the left hand side as a product of n factors,

$$(x+y)(x+y)\cdots(x+y).$$

When we expand this into monomials, we choose from each factor either an x or a y. Since there are n factors, the monomials we obtain are all of the form $x^k y^{n-k}$ for some k. Suppose we fix k. Choose k locations above in which the x is to be taken. In the remaining locations take the y. There are $\binom{n}{k}$ ways of choosing these k locations. Hence the monomial $x^k y^{n-k}$ arises exactly $\binom{n}{k}$ times. That is, we have (3).

If the above reasoning seems unconvincing, we could alternatively proceed by induction. Certainly (3) holds when $n = 1$; this is the basis of the induction. Suppose that (3) holds for n. Then

$$(x+y)^{n+1} = (x+y)(x+y)^n.$$

By the inductive hypothesis this is

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

$$= x\sum_{k=0}^{n}\binom{n}{k}x^k y^{n-k} \quad + \quad y\sum_{k=0}^{n}\binom{n}{k}x^k y^{n-k}$$
$$= \sum_{k=0}^{n}\binom{n}{k}x^{k+1} y^{n-k} \quad + \quad \sum_{k=0}^{n}\binom{n}{k}x^k y^{n+1-k}.$$

In the first sum, put $j = k+1$. As k runs from 0 to n, j runs from 1 to $n+1$. We now use j as our index, and replace k at each occurence by $j-1$. Thus the above is

$$= \sum_{j=1}^{n+1}\binom{n}{j-1}x^j y^{n+1-j} \quad + \quad \sum_{k=0}^{n}\binom{n}{k}x^k y^{n+1-k}.$$

In the first sum we can allow j to take the value 0, since $\binom{n}{-1} = 0$. Similarly, in the second sum we can allow k to take the value $n+1$, since $\binom{n}{n+1} = 0$. Also, j is just a dummy variable used to index the terms, so we can call it anything we want. Let's call it k instead of j. Then the above is

$$= \sum_{k=0}^{n+1}\binom{n}{k-1}x^k y^{n+1-k} \quad + \quad \sum_{k=0}^{n}\binom{n}{k}x^k y^{n+1-k}$$
$$= \sum_{k=0}^{n+1}\left(\binom{n}{k-1} + \binom{n}{k}\right)x^k y^{n+1-k}.$$

By (2) we see that this is

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

This is (3) for $n+1$. This completes the inductive step, so the proof is complete.

By taking $x = y = 1$ in (3) we obtain the interesting identity

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

That is, the sum of the entries in the nth row of Pascal's Triangle is 2^n. This is obvious also for combinatorial reasons: When forming a subset $\mathcal{T}$ of $\mathcal{S}$, there are two possibilities for e_1. Either $e_1 \in \mathcal{T}$ or $e_1 \notin \mathcal{T}$. Similarly there are two possibilities for e_2, for e_3, etc. This gives altogether 2^n possibilities. That is, $\mathcal{S}$ has 2^n subsets (including both the emptyset and $\mathcal{S}$).

With these basic formulas concerning binomial coefficients in hand, we can consider their number-theoretic properties. In some cases you will find it easy to provide a proof that an observed pattern continues indefinitely, but in other cases proofs may be hard to achieve. As an aid, you may want to use the program **PascalsT**. This program does not display the binomial coefficients, but only their values modulo m. Thus by taking $m = 2$, we find a 1 in the table when the binomial coefficient is odd, and a 0 when it is even.

Explorations

1. What is the highest power of 2 dividing $(2n)!/n!$?

2. Let p be a prime number. What is the least positive number n such that $p \mid \binom{n}{k}$ for all k in the range $0 < k < n$? What is the second such n? The third? (Take $m = p$ in **PascalsT**.)

3. Take $m = 2$ in **PascalsT**. The pattern created by rows 0–3 is repeated twice in rows 4–7, with an inverted triangle of 0's between. Does this generalize? How would you express this in terms of equations?

4. For $0 \le n \le 15$, count the number of odd entries in the nth row of Pascal's Triangle. (Take $m = 2$ in **PascalsT**.)

5. For $0 \le n \le 15$, write n in binary (i.e., base 2), and note the number of 1's that occur. This number is called $w(n)$, the *binary weight of* n.

6. By comparing the binary expansion of k with the binary expansion of n, can you guess whether $\binom{n}{k}$ is odd or even?

7. Describe the pattern formed by Pascal's Triangle when all entries are divided by 7.

8. Describe the pattern formed by Pascal's Triangle when all entries are divided by 8.

9. Apply **PascalsT** with $m = 15$, and examine the row $n = 15$. List the elements that are not divisible by 3. List the elements that are not divisible by 5. Does this suggest something?

10. Choose an n, say $n \le 15$. Can you find j and k with $0 < j < n$, $0 < k < n$, so that $\binom{n}{j}$ and $\binom{n}{k}$ are relatively prime?

11. Each interior member of Pascal's triangle is surrounded by six adjacent members. Form two products, each one by multiplying every other one of the surrounding numbers. How do these products compare? Formulate a conjecture, and prove it.

12. For each positive integer n form a sum $\binom{n}{0} + \binom{n-1}{1} + \binom{n-2}{2} + \cdots$ in which the terms continue as long as it falls in Pascal's triangle. Do you recognize the numbers generated? Formulate a conjecture, and prove it.

Chapter XIV
Primitive Roots

Programs Used: **Factor**, **Ind**, **IndTab**, **Order**, **OrderTab**, **PolySolv**, **PowerTab**, **PrimRoot**

Suppose that a is a reduced residue class modulo m. That is, $(a, m) = 1$. As in Chapter 9, we let the *order* of $a \pmod m$ be the least positive integer h such that $a^h \equiv 1 \pmod m$. In that chapter we found that $h \mid \phi(m)$. We say that a is a *primitive root* of m if the order of a modulo m is $\phi(m)$, which is the largest possible value. Not all moduli have primitive roots, but by developing further properties of orders we are able to show that for each prime p there is at least one primitive root. If g is a primitive root modulo p then the numbers $1, g, g^2, \dots, g^{p-2}$ form a reduced residue system modulo p. Hence if $(a, p) = 1$ then there is a number μ such that $a \equiv g^\mu \pmod p$. This number μ is known as the *index* of a, and we write $\mu = \operatorname{ind} a$. This is quite analogous to taking the logarithm of a positive real number, and offers many of the same advantages.

Explorations

1. Use the program **PowerTab** to find integers k such that $a^k \equiv 1 \pmod m$ for various a and m. How is the least such k related to the others? Formulate a conjecture, and prove it.

2. Suppose that a has order h modulo m. Describe the order of a^k as a function of h and k. Formulate a conjecture, and prove it. The program **OrderTab** is useful for experimentation here.

3. Suppose that a has order h modulo m and that b has order k modulo m. If $(h, k) = 1$, then what is the order of ab modulo m? Use **OrderTab** to experiment. Formulate a conjecture, and prove it.

4. Suppose that a has order h modulo m and order k modulo n. Assuming that $(m, n) = 1$, determine the order of a modulo mn, as a function of h and k. The order of a modulo m can be found from **OrderTab** or by typing `order a m <Return>`. Formulate a conjecture and prove it.

5. Use **PolySolv** with the polynomial $f(x) = x^3+x+1$. For each prime $p < 100$, note how many solutions the congruence $f(x) \equiv 0 \pmod p$ has. What is the maximum number of roots encountered? Repeat this with $g(x) = x^4 + x^3 + x^2 + x + 1$. For which primes are there roots? When there is a root, how many roots are there? Formulate a conjecture concerning the maxiumum number of roots modulo p of a polynomial of degree d.

6. Let $f(x)$ be a polynomial with integral coefficients, and suppose that a is an integer. Divide $x - a$ into $f(x)$ to obtain a quotient polynomial $g(x)$ and a remainder r. Thus $f(x) = (x - a)g(x) + r$. What is the connection between the following two assertions: (i) $f(a) \equiv 0 \pmod p$; (ii) $r \equiv 0 \pmod p$. Show that if $f(a) \equiv 0 \pmod p$ and if the conjecture formulated in question **5** above is true for $g(x)$ then it is also true for $f(x)$. Hence prove this conjecture by induction on the degree d of the polynomial.

7. How many roots modulo p does the polynomial $x^{p-1} - 1$ have? Use **PolySolv** to experiment, formulate a conjecture, and prove it.

8. Suppose that $f(x)$ and $g(x)$ are polynomials such that $f(x)g(x) = x^{p-1} - 1$ then the number of roots of $f(x)$ modulo p is $\deg f$.

9. Suppose that $d \mid p - 1$. Use **PolySolv** to determine the number of roots of $x^d \equiv 1 \pmod p$. Formulate a conjecture, and prove it. (Hint: Try dividing $x^d - 1$ into $x^{p-1} - 1$.)

10. Let p be a given prime number, and suppose that q is a prime with $q^\alpha \| p-1$. That is, $q^\alpha \mid p - 1$ but $q^{\alpha+1} \nmid p - 1$. How many residue classes modulo p have order exactly q^α? Use **Factor** to factor $p - 1$, and then use **OrderTab**. Formulate a conjecture, and prove it.

11. Combine your findings related to questions **3** and **10** above to show that every prime number has at least one primitive root g.

12. Use **OrderTab**, and try to guess a formula for the number of different primitive roots modulo p. Use your findings from questions **2** and **11** above to prove your conjecture.

13. Suppose that g is a primitive root modulo p. Under what conditions on μ and ν is it true that $g^\mu \equiv g^\nu \pmod p$? Use **PowerTab**

14. Suppose that $(a, p) = 1$, and that $d \mid p - 1$. How is the value of $a^{(p-1)/d} \pmod p$ related to the number of roots of the congruence $x^d \equiv a \pmod p$? Use **PowerTab** and **PolySolv** to experiment, and formulate a conjecture. To prove the conjecture, suppose that g is a primitive root modulo p, and write $a \equiv g^\alpha \pmod p$, $x \equiv g^\mu \pmod p$.

Suppose we want to find all solutions to the congruence $x^5 \equiv 41 \pmod{101}$. We first find a primitive root of the prime number 101. This can be done by typing `primroot 101 <Return>`. In general, by typing `primroot p a <Return>` one obtains the least primitive root of p greater than a. But the use of **PrimRoot** can be omitted here, since the next step is to invoke **IndTab**, which automatically starts with the least positive primitive root as the base, namely 2 when $p = 101$. From this program we find that $\operatorname{ind} 41 = 45$ when $p = 101$ and $g = 2$. If we write $x \equiv 2^\mu \pmod{101}$, then the congruence in question becomes $2^{5\mu} \equiv 2^{45} \pmod{101}$. Since 2 is a primitive root of 101, this is equivalent to the congruence $5\mu \equiv 45 \pmod{100}$. That is, $\mu \equiv 9 \pmod{20}$, which has solutions 9, 29, 49, 69, 89 modulo 100. The program **IndTab** starts with a table of indices, sometimes called the *discrete logarithm*, but by typing `E` it switches to exponentials, which is to say powers of 2 (mod 101). From this program, or from **PowerTab**, we find that

$$2^9 \equiv 7, \quad 2^{29} \equiv 59, \quad 2^{49} \equiv 50, \quad 2^{69} \equiv 3, \quad 2^{89} \equiv 83 \pmod{101}$$

are the desired solutions. One can use **PolySolv** with $f(x) = x^5 - 41$ to confirm this finding.

15. Use **IndTab** as above to find all solutions of the following congruences:
(a) $x^2 \equiv 11 \pmod{97}$;
(b) $x^3 \equiv 21 \pmod{107}$.
(c) $x^4 \equiv 5 \pmod{31}$;
(d) $x^5 \equiv 2 \pmod{61}$;
(e) $x^6 \equiv 11 \pmod{113}$;

16. Use **OrderTab** to find moduli that have primitive roots. Formulate a conjecture concerning which moduli have primitive roots. Suppose that $m = m_1 m_2$ with $(m_1, m_2) = 1$. Suppose that $(\phi(m_1), \phi(m_2)) > 1$. Explain why m does not have a primitive root. (Hint: Recall your findings from question **4** above.)

WILD PROBLEM

The numbers m and n are integers between 3 and 97. Pam has been told the product of these two numbers, while Sam has been told their sum. They carry on the following truthful conversation:

Pam:	I don't know the values of m and n.
Sam:	I knew you didn't; neither do I.
Pam:	Now I know the values!
Sam:	Oh, then so do I!

What are m and n?

Number theorists are never past their prime:

2,	**3,**	**5,**	**7,**	**11,**	**13,**	**17,**	**19,**	**23,**
29,	**31,**	**37,**	**41,**	**43,**	**47,**	**53,**	**59,**	**61,**
67,	**71,**	**73,**	**79,**	**83,**	**89,**	**97,**	**101,**	**103,**
107,	**109,**	**113,**	**127,**	**131,**	**137,**	**139,**	**149,**	**151,**
157,	**163,**	**167,**	**173,**	**179,**	**181,**	**191,**	**193,**	**. . .**

Appendix E
Equivalence Relations and Partitionings

If $\mathcal{S}$ and $\mathcal{T}$ are two sets, then their *Cartesian product*, written $\mathcal{S} \times \mathcal{T}$, is the set of all ordered pairs (s,t) such that $s \in \mathcal{S}$ and $t \in \mathcal{T}$. This concept originates in René Descartes' description of points in the plane by means of rectangular coordinates. Thus the Euclidean plane is presented as the Cartesian product $\mathbf{R} \times \mathbf{R}$. A *relation* (or *binary relation*) on a set $\mathcal{S}$ is simply a subset of $\mathcal{S} \times \mathcal{S}$. For example, if $\mathcal{R} = \{(x,y) \in \mathbf{R} \times \mathbf{R} : x \le y\}$, then $\mathcal{R}$ is a relation, and saying that $(x,y) \in \mathcal{R}$ is the same thing as saying that $x \le y$. This is typical of relations that we use: Instead of expressing that x is related to y by writing $(x,y) \in \mathcal{R}$, we write $x \,\mathcal{R}\, y$.

In our study of congruences we develop properties of the relation $a \equiv b \pmod{m}$. Thus for each positive integer m we a relation

$$\mathcal{R}_m = \{(a,b) \in \mathbf{Z} \times \mathbf{Z} : m|(a-b)\}.$$

This relation has three important properties that are particularly worth noting:

$$\begin{aligned} a \equiv a \pmod{m} & \qquad \text{(Reflexive)} \\ a \equiv b \pmod{m} \Longrightarrow b \equiv a \pmod{m} & \qquad \text{(Symmetric)} \\ a \equiv b \pmod{m}, b \equiv c \pmod{m} \Longrightarrow a \equiv c \pmod{m} & \qquad \text{(Transitive)} \end{aligned}$$

A relation with these three properties is called an *equivalence relation*. For $0 \le i < m$ let $\mathcal{C}_i$ denote the set of all numbers that are congruent to $i \pmod{m}$. Thus

$$\begin{aligned} \mathcal{C}_0 &= \{\cdots, -2m, -m, 0, m, 2m, \cdots\}, \\ \mathcal{C}_1 &= \{\cdots, -2m+1, -m+1, 1, m+1, 2m+1, \cdots\}, \\ \mathcal{C}_2 &= \{\cdots, -2m+2, -m+2, 2, m+2, 2m+2, \cdots\}, \\ &\vdots \\ \mathcal{C}_{m-1} &= \{\cdots, -m-1, -1, m-1, 2m-1, 3m-1, \cdots\}. \end{aligned}$$

Here we see that every number in $\mathcal{C}_i$ is congruent (mod m) to every other number in $\mathcal{C}_i$, but to no number outside $\mathcal{C}_i$. That is, if $a \in \mathcal{C}_i$ and $b \in \mathcal{C}_j$, then $a \equiv b \pmod{m}$ if and only if $i = j$. We note that each set $\mathcal{C}_i$ is an arithmetic progression; we call these sets *residue classes*. In general, we could let $\mathcal{C}_a$ denote the arithmetic progression with common difference m that contains the number a,

$$\mathcal{C}_a = \{\cdots, -2m + a, -m + a, a, m + a, 2m + a, \cdots\}.$$

Thus $a \equiv b \pmod{m}$ if and only if $\mathcal{C}_a = \mathcal{C}_b$.

It is particularly noteworthy that every integer a is in exactly one of the sets $\mathcal{C}_i$. Such a configuration of subsets is called a *partitioning*. Thus congruences modulo m define an equivalence relation on one hand, and a partitioning of the integers on the other. It is no accident that congruences do both of these things. Indeed, it is not hard to show that if $\mathcal{R}$ is an equivalence relation on a set $\mathcal{S}$ then the equivalence classes $\mathcal{C}_a = \{b \in \mathcal{S} : a\mathcal{R}b\}$ define a partitioning of $\mathcal{S}$. (See Problem 4. below.) Conversely, suppose we start with a partitioning of $\mathcal{S}$ into disjoint subsets $\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3, \ldots$. Suppose that $a \in \mathcal{C}_i$ and that $b \in \mathcal{C}_j$. Then we can define a relation $\mathcal{R}$ by saying that $a\,\mathcal{R}\,b$ if and only if $i = j$. It is not hard to show that this relation is an equivalence relation. (See Problem 5. below.) Thus equivalence relations and partitionings are interchangeable, and it is immaterial whether we use the language of one or of the other.

Explorations

1. For each of the following relations, determine which of the three properties (Reflexive, Symmetric, Transitive) hold, and hence determine which of these relations are equivalence relations.

(a) $a \le b$;	(d) similarity of triangles;
(b) $a \mid b$;	(e) congruence of triangles;
(c) $\ell_1 \| \ell_2$ (parallel lines);	(f) $a > b$.

2. For $r = 0, 1, 2, \ldots$, let $\mathcal{P}_r$ denote the set of positive integers that have exactly r prime factors (counting multiplicity). Thus for example, $12 \in \mathcal{P}_3$ since $12 = 2 \cdot 2 \cdot 3$ has 3 prime factors.
(a) Explain why the sets $\mathcal{P}_r$ partition the positive integers.
(b) Describe the members of $\mathcal{P}_0$.
(c) Describe the members of $\mathcal{P}_1$.
(d) Describe the associated equivalence relation.
(e) If $a \in \mathcal{P}_i$ and $b \in \mathcal{P}_j$, can you predict which class $\mathcal{P}_k$ that $a + b$ falls in?
(f) If $a \in \mathcal{P}_i$ and $b \in \mathcal{P}_j$, can you predict which class $\mathcal{P}_k$ that ab falls in?

3. We have shown that any positive integer n can be written uniquely in the form $n = ab^2$ where a is squarefree. Call the number a the "squarefree part" of n. Suppose we define a relation by saying that $m \approx n$ if they have the same squarefree part.
(a) Show that $\approx$ is an equivalence relation.
(b) Describe the numbers n such that $n \approx 1$.
(c) Describe the associated partitioning of the positive integers.

4. Suppose that $\mathcal{R}$ is an equivalence relation defined on a set $\mathcal{S}$. For $s \in \mathcal{S}$, let

$$\mathcal{C}_s = \{t \in \mathcal{S} : s\,\mathcal{R}\,t\}.$$

(a) Show that for $s \in \mathcal{C}_s$ for every $s \in \mathcal{S}$.
(b) Show that if $\mathcal{C}_s$ and $\mathcal{C}_t$ have an element in common, then $\mathcal{C}_s = \mathcal{C}_t$.
(c) Show that the sets $\mathcal{C}_s$ form a partitioning of $\mathcal{S}$.

5. Suppose that a family of sets $\mathcal{C}_i$ form a partitioning of a given set $\mathcal{S}$. Define the relation $\mathcal{R}$ by saying that $a\,\mathcal{R}\,b$ if there is an i such that $a \in \mathcal{C}_i$ and $b \in \mathcal{C}_i$.
(a) Show that the relation $\mathcal{R}$ is reflexive.
(b) Show that the relation $\mathcal{R}$ is symmetric.
(c) Show that the relation $\mathcal{R}$ is transitive.
(d) Deduce that $\mathcal{R}$ is an equivalence relation.

I KNOW YOU BELIEVE YOU UNDERSTAND WHAT YOU THINK I SAID, BUT I AM NOT SURE YOU REALIZE THAT WHAT YOU HEARD IS NOT WHAT I MEANT.

Appendix G
The Greek Alphabet

Name	Upper	Lower	Sound
alpha	A	α	a
beta	B	β	b
gamma	Γ	γ	g
delta	Δ	δ	d
epsilon	E	ϵ, ε	e
zeta	Z	ζ	z
eta	H	η	ē
theta	Θ	θ, ϑ	th
iota	I	ι	i
kappa	K	κ, $\varkappa$	k
lambda	Λ	λ	l
mu	M	μ	m
nu	N	ν	n
xi	Ξ	ξ	x
omicron	O	o	o
pi	Π	π, ϖ	p
rho	P	ρ, ϱ	r
sigma	Σ	σ, ς	s
tau	T	τ	t
upsilon	Υ	υ	y, u
phi	Φ	ϕ, φ	f
chi	X	χ	ch
psi	Ψ	ψ	ps
omega	Ω	ω	ō

NOTES

Greek letters that are indistinguishable from their Roman counterparts are not used in mathematics.

The variant lower case sigma, ς, is not used in mathematics—it occurs in Greek words ending in s.

The variant ϖ of pi and ϱ of rho were common in mathematics as recently as the nineteenth century, but are rare today.

Both forms of epsilon, theta, kappa, and phi are in common use in mathematics, but one should not use both forms of the same letter in the same paper.

One should be careful not to confuse the lower case epsilon (in either form) with the mathematical symbol $\in$, which means 'is an element of'.

**THERE ARE THREE KINDS
OF MATHEMATICIANS:
THOSE WHO CAN COUNT,
AND THOSE WHO CAN'T.**

Appendix L
Logic

Statements have truth values, which may be True (abbreviated T) or False (abbreviated F). If A is a statement, then "not A" is a statement whose truth value is the opposite of A. We can diagram this in a truth table:

A	not A
T	F
F	T

We also have various ways of combining statements. For example, we may take two statements A and B, and combine them to form a single statement "A and B". The truth value of "A and B" is determined by the truth values of A and of B. In the truth table below we give the rule that defines the values of "A and B", "A or B", "A xor B", "A $\implies$ B", and "A $\iff$ B". Here "xor" is the exclusive or; it may be spoken as "A x-or B", or "either A or B." Similarly, the symbol "$\implies$" stands for an implication; it may be read "A implies B," or "if A then B". Finally, "$\iff$" denotes an implication in both directions, which can be expressed in words in various ways, such as "A implies and is implied by B," or "A if and only if B," or "A is equivalent to B."

A	B	A and B	A or B	A xor B	A $\implies$ B	A $\iff$ B
T	T	T	T	F	T	T
T	F	F	T	T	F	F
F	T	F	T	T	T	F
F	F	F	F	F	T	T

By using these basic rules, we can determine the truth values of various combinations of statements. For example, in the table below we compute the values of "not A", and hence the values of "B or (not A)." We also reproduce, in the last column, the values of "A $\implies$ B."

A	B	not A	B or not A	A $\Longrightarrow$ B
T	T	F	T	T
T	F	F	F	F
F	T	T	T	T
F	F	T	T	T

Since the entries in the last two columns are the same, we are able to deduce from the above that

$$\text{B or not A} \qquad \Longleftrightarrow \qquad \text{A} \Longrightarrow \text{B}$$

That is, "B or not A" and "A $\Longrightarrow$ B" are logically equivalent. By computing truth tables, we are able to establish further useful identities among combinations of statements.

When combining statements in a complicated way, it is important to introduce parentheses so that the order that operations are to be performed is made clear. For example, the relation displayed above is ambiguous; it was intended to mean

$$(\text{B or not A}) \qquad \Longleftrightarrow \qquad (\text{A} \Longrightarrow \text{B}),$$

although it could equally well be interpreted as

$$((\text{B or not A}) \Longleftrightarrow \text{A}) \qquad \Longrightarrow \qquad \text{B},$$

which is a quite different statement.

Explorations

1. Supply the missing entries in the following truth table:

A	not A	not (not A)
T	F	
F	T	

In this way, establish that "not (not A)" and "A" are logically equivalent. That is,

$$\text{not (not A)} \qquad \Longleftrightarrow \qquad \text{A}.$$

2. Supply the values in the following table:

A	B	C	B or C	A and B	A and C	A and (B or C)	(A and B) or (A and C)
T	T	T					
T	T	F					
T	F	T					
T	F	F					
F	T	T					
F	T	F					
F	F	T					
F	F	F					

On comparing the last two columns, we conclude that

$$\text{A and (B or C)} \qquad \Longleftrightarrow \qquad \text{(A and B) or (A and C)}$$

That is, "and" is distributive over "or" in the same way that multiplication is distributive over addition: $a(b+c) = ab + ac$.

3. Supply the values in the following table:

A	B	C	B and C	A or B	A or C	A or (B and C)	(A or B) and (A or C)
T	T	T					
T	T	F					
T	F	T					
T	F	F					
F	T	T					
F	T	F					
F	F	T					
F	F	F					

On comparing the last two columns, we conclude that

$$\text{A or (B and C)} \qquad \Longleftrightarrow \qquad \text{(A or B) and (A or C)}$$

That is, "or" is distributive over "and". On combining this with the preceding result, we find that each of "and" and "or" is distributive over the other. This is different from ordinary arithmetic, where multiplication is distributive over addition, but addition is not distributive over multiplication. That is, the equation $a + bc = (a+b)(a+c)$ does not hold identically.

4. Complete the entries in the following truth table:

A	B	A $\implies$ B	B $\implies$ A	(not A) $\implies$ (not B)	(not B) $\implies$ (not A)
T	T				
T	F				
F	T				
F	F				

The implication "B $\implies$ A" is called the *converse* of the implication "A $\implies$ B." On comparing the third and fourth columns above, we see that an implication is not equivalent to its converse: One may be true while the other is false. For example, suppose that a and b are positive integers. Then

$$\text{If } a|b \text{ then } a \leq b$$

is a true implication, but its converse

$$\text{If } a \leq b \text{ then } a|b$$

is false. On the other hand, on comparing the third and sixth columns above, we discover that

$$\text{A} \implies \text{B} \qquad \iff \qquad (\text{not B}) \implies (\text{not A}).$$

That is, the implication "A $\implies$ B" is logically equivalent to its *contrapositive*, "(not B) $\implies$ (not A)." When proving a theorem, we often find it more convenient to prove the contrapositive. This is permissible, since there is no logical distinction between the two. For example, suppose that $p > 2$. Rather than prove that if p is prime then p is odd, it might seem more natural to prove that if p is even (i.e., not odd) then p is composite (i.e., not prime).

5. Complete the entries in the following truth table:

A	B	A $\implies$ B	A and (A $\implies$ B)	(A and (A $\implies$ B)) $\implies$ B
T	T			
T	F			
F	T			
F	F			

We see that the statement "(A and (A $\implies$ B)) $\implies$ B" is always true. Such a statement is called a *tautology*. This particular tautology is the principle that we use to make deductions. For example, we know that 37 is a prime number > 2, and we know that if p is a prime number > 2 then p is odd. Hence we can deduce that 37 is odd.

6. Another important principle that we use in reasoning can be certified by completing the entries in the following table:

A	B	C	$A \Rightarrow B$	$B \Rightarrow C$	$(A \Rightarrow B)$ and $(B \Rightarrow C)$	$A \Rightarrow C$	$((A \Rightarrow B)$ and $(B \Rightarrow C)) \Longrightarrow (A \Rightarrow C)$
T	T	T					
T	T	F					
T	F	T					
T	F	F					
F	T	T					
F	T	F					
F	F	T					
F	F	F					

That is,

If A implies B and B implies C then A implies C.

This is known as the *law of the syllogism*.

7. Complete the entries in the following truth table:

A	B	A xor B	(A xor B) xor B
T	T		
T	F		
F	T		
F	F		

By comparing the first and last columns, deduce that

$$(\text{A xor B}) \text{ xor B} \qquad \Longleftrightarrow \qquad \text{A}.$$

If we let the number 1 correspond to True, and 0 correspond to False, then "A xor B" corresponds to adding A and B (mod 2). Thus the identity above corresponds to the congruence $(x + y) + y \equiv x \pmod 2$. More generally, $x_1 + x_2 + \cdots + x_n \equiv 1 \pmod 2$ if and only if an odd number of the numbers x_i is odd. Similarly, A_1 xor A_2 xor ... xor A_n is true if and only if an odd number of the statements A_i is true. This statement can be rendered using only "and" and "or", but the expressions are rather bulky. For $n = 2$ we write "(A_1 and (not A_2)) or ((not A_1) and A_2)."

For $n = 3$ we write

$$\begin{aligned}
&(\mathrm{A}_1 \text{ and } \mathrm{A}_2 \text{ and } \mathrm{A}_3) \\
\text{or } &(\mathrm{A}_1 \text{ and } (\text{not } \mathrm{A}_2) \text{ and } (\text{not } \mathrm{A}_3)) \\
\text{or } &((\text{not } \mathrm{A}_1) \text{ and } \mathrm{A}_2 \text{ and } (\text{not } \mathrm{A}_3)) \\
\text{or } &((\text{not } \mathrm{A}_1) \text{ and } (\text{not } \mathrm{A}_2) \text{ and } \mathrm{A}_3).
\end{aligned}$$

Here we have 4 blocks with elements linked by "and" in each block. How many such blocks are needed when $n = 4$? For general n?

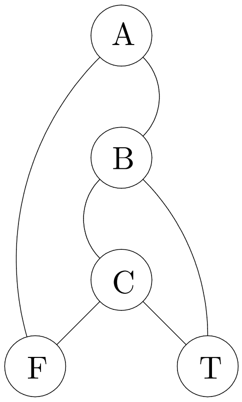
In our initial discussion, we saw that "A $\Longrightarrow$ B" can be expressed equivalently as "B or not A". In the problem above we saw that "A xor B" can also be expressed using "and", "or" and "not." Indeed, any desired function of basic statements A_1, A_2, $\ldots$, A_n can be expressed using only conjunction (i.e., "and"), disjunction (i.e., "or"), and negation (i.e., "not"). If two such expressions are logically equivalent then the equivalence can be established by manipulating the expressions according to the following fundamental rules.

The laws of logic

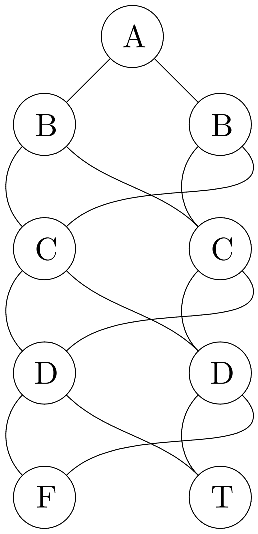
1. Law of double negation	not (not A) $\iff$ A
2. DeMorgan's laws	not (A and B) $\iff$ (not A) or (not B) not (A or B) $\iff$ (not A) and (not B)
3. Commutative laws	A and B $\iff$ B and A A or B $\iff$ B or A
4. Associative laws	A and (B and C) $\iff$ (A and B) and C A or (B or C) $\iff$ (A or B) or C
5. Distributive laws	A and (B or C) $\iff$ (A and B) or (A and C) A or (B and C) $\iff$ (A or B) and (A or C)
6. Idempotent laws	A and A $\iff$ A A or A $\iff$ A
7. Identity laws	A or F $\iff$ A A and T $\iff$ A
8. Inverse laws	A and (not A) $\iff$ F A or (not A) $\iff$ T
9, Domination laws	A and T $\iff$ T A or F $\iff$ F
10. Absorption laws	A and (A or B) $\iff$ A A or (A and B) $\iff$ A

In Problems 1–3 above some of these laws were verified; the rest may be verified similarly. Note that, apart from the first law, the laws are in dual pairs; the dual is obtained by interchanging "and" with "or" and "T" with "F." Since the laws have this duality, and since any logical equivalence can be derived from these laws, it follows that each logical equivalence has a dual equivalence.

As we saw in Problem 7 above, simple statements may lead to cumbersome expressions. In some cases a statement can be expressed more compactly by means of a *decision diagram* in which the truth values of the variables determine a path through the diagram. All paths terminate at T or F. For example, the statement "A and (B or C)" is expressed by the diagram



Note that from each circled node, the left branch is taken if the variable is false, while the right branch is taken if it is true. In each level of the diagram only one variable appears, although it may appear several times. For example, the statement "A xor B xor C xor D" is depicted as follows:



8. Use the laws of logic to simplify the expression "not (A $\Longrightarrow$ B)."

9. Use the laws of logic to verify that

$$(A \Longrightarrow B) \text{ and not } B) \qquad \Longrightarrow \qquad \text{not } A$$

is a tautology. (That this is a tautology could also be established by means of a truth table, or by using the results of Problems 4 and 5: First, by Problem 4, we know that the implication "A $\Longrightarrow$ B" is equivalent to its contrapositive, "(not B) $\Longrightarrow$ (not A)." Then apply the principle of Problem 5 to the contrapositive.)

10. The first step in the preceding problem is to replace implications "P $\Longrightarrow$ Q" by the more basic "Q or not P." Form the dual of the expression that was obtained. What is this dual equivalent to?

11. Suppose that three statements A, B, and C are combined by majority vote, so that the result is T if two or more of A, B, C are true, and otherwise the result is F. Construct a decision design to describe this combination.

12. Suppose that five statements A, B, C, D, and E are combined by majority vote, so that the result is T if three or more of A, B, C, D, E are true, and otherwise the result is F. Construct a decision design to describe this combination.

The statement below is true.

The statement above is false.

Appendix P
Reference Guide to the Programs

ArFcnTab

Function Constructs a TABle of values of the six ARithmetic FunCtioNs $\omega(n) = \sum_{p|n} 1$, $\Omega(n) = \sum_{p^a \| n} a$, $\mu(n)$, $d(n) = \sum_{d|n} 1$, $\phi(n)$, and $\sigma(n) = \sum_{d|n} d$.

Syntax `arfcntab`

Commands

`PgUp`	Display the next 20 values
`PgDn`	Display the preceding 20 values
`J`	Jump to a new point in the table
`P`	Print 500 values, starting at the top of the displayed screen
`Esc`	Escape from the environment

Restrictions $1 \le n < 10^9$

Algorithm When the program begins execution, it first constructs a list of the primes not exceeding $10^{9/2}$, by sieving. These primes are used for trial division. The factorizations are determined simultaneously for all 20 numbers (or all 500 numbers, in the case of printing).

See also Pi

BasesTab

Function Constructs a TABle of the expansions of integers n in various BASES b.

Syntax `basestab`

Commands

`PgUp`	Display the preceding 20 values
`PgDn`	Display the next 20 values
$\leftarrow$	Shift to smaller bases
$\rightarrow$	Shift to larger bases
`J`	Jump to a new point in the table
`Esc`	Escape from the environment

Restrictions $2 \le b \le 16$, $1 \le n \le 10^{18}$

Algorithm The division algorithm is used to calculate base b digits, trailing digits first.

CngArTab

Function Displays the addition and multiplication TABles for CoNGruence ARithmetic (mod m).

Syntax `cngartab`

Commands

$\uparrow$	Move up
$\downarrow$	Move down
$\leftarrow$	Move left
$\rightarrow$	Move right
`a`	Start at column a
`b`	Start at row b
`m`	Set modulus m
`s`	Switch between addition and multiplication
`r`	Display only reduced residues (in multiplication table)
`p`	Print the table (if $m \le 24$)
`Esc`	Escape from the environment

Restrictions $1 \le m < 10^9$

See also PowerTab

CoDivTab

Function Constructs a TABle of the COmmon DIVisors of two given numbers b and c.

Syntax `codivtab`

Restrictions $1 \le b < 10^9$, $1 \le c < 10^9$

Algorithm Tests every d in the range $1 \le d \le \min(b, c)$.

See also CoMulTab, DivTab

CoMulTab

Function Constructs a TABle of the COmmon MULtiples of two given numbers b and c.

Syntax `comultab`

Restrictions $|b| < 10^9$, $|c| < 10^9$

Algorithm The Euclidean Algorithm is used the calculate (b, c), and hence $[b, c]$. Then multiples of this latter number are listed.

See also CoDivTab

CRT

Function Determines the intersection of two arithmetic progressions. Let $g = (m_1, m_2)$. The set of x such that $x \equiv a_1 \pmod{m_1}$, $x \equiv a_2 \pmod{m_2}$ is empty if $a_1 \not\equiv a_2 \pmod{g}$. Otherwise the intersection is an arithmetic progression $a \pmod{m}$. In the Chinese Remainder Theorem it is required that $g = 1$, and then $m = m_1 m_2$. In general, $m = m_1 m_2/g$.

Syntax `crt` [$\texttt{a}_1$ $\texttt{m}_1$ $\texttt{a}_2$ $\texttt{m}_2$]

Restrictions $|a_i| < 10^{18}$, $1 \le m_i < 10^{18}$

Algorithm First the linear congruence $m_1 y \equiv a_2 - a_1 \pmod{m_2}$ is solved. If $a_1 \not\equiv a_2 \pmod{g}$, then this congruence has no solution, and the intersection of the two given arithmetic progressions is empty. Otherwise, let y denote the unique solution of this congruence in the interval $0 \le y < m_2/g$. Then the intersection of the two given arithmetic progressions is the set of integers $x \equiv a \pmod{m}$ where $a = ym_1 + a_1$ and $m = m_1 m_2/g$.

See also CRTDem, IntAPTab, LinCon, LnCnDem, ResComp

CRTDem

Function Demonstrates the method employed to determine the intersection of two given arithmetic progressions.

Syntax `crtdem` [$\texttt{a}_1$ $\texttt{m}_1$ $\texttt{a}_2$ $\texttt{m}_2$]

Restrictions $|a_i| < 10^{18}$, $1 \le m_i < 10^{18}$

Algorithm See the description given for the program CRT.

See also CRT, LnCnDem, ResComp

D2R

Function Converts a Decimal TO Rational. That is, the program returns the rational number a/q with least q such that the initial decimal digits of a/q coincide with the decimal digits given.

Syntax `d2r` [x]

Restrictions $|a| < 10^{18}$, $1 \le q < 10^{18}$

Algorithm Suppose that k decimal digits of x are given after the decimal point. Put $\delta = 0.5 \cdot 10^{-k}$. We want to find a/q with q minimal such that $|x - a/q| \le \delta$. By the continued fraction algorithm the least i is found such that $|x - h_i/k_i| \le \delta$. Then the desired rational number is given by $a = ch_{i-1} + h_{i-2}$, $q = ck_{i-1} + k_{i-2}$ where c is the least positive integer such that a/q lies in the specified interval. Since this inequality holds when $c = a_i$, it suffices to search the interval $[1, a_i]$.

See also R2D

Div

Function Applies the division algorithm. Given a divisor $d \neq 0$ and a dividend D, a quotient q and remainder r are found so that $D = dq + r$ with $0 \leq r < |d|$.

Syntax `div [d D]`

Restrictions $0 < |d| < 10^{18}$, $|D| < 10^{18}$

Algorithm Long division, to find the integer part of the quotient.

See also CoDivTab, CoMulTab, DivTab, DivTest

DivTab

Function Constructs a TABle of the DIVisors of a given number n.

Syntax `divtab`

Restrictions $1 \leq n < 10^9$

Algorithm The number n is factored, and a list of divisors is created with the exponents of primes in lexicographic order. This is sorted to numerical order by the heapsort algorithm.

See also CoDivTab, CoMulTab, Div, DivTest

DivTest

Function Tests whether b divides c, and presents the canonical factorization of both numbers.

Syntax `divtest [b c]`

Restrictions $|b| < 10^{18}$, $|c| < 10^{18}$

Algorithm By the Division Algorithm, $c = qb + r$. Then $b \mid c$ if and only if $r = 0$. The canonical factorizations are determined by trial division.

See also CoDivTab, CoMulTab, Div, DivTab

EuAlgDem

Function DEMonstrates the EUclidean ALGorithm. If the parameters b and c are specified on the command line, then (b, c) is calculated by using the identities $(b,c) = (c,b)$, $(b,c) = (b+mc,c)$, $(b,0) = |b|$, and then the program terminates. Otherwise an environment is provided in which each remainder is expressed as a linear combination of b and c. In this case one can also toggle between rounding down and rounding to the nearest integer quotient.

Syntax `eualgdem [b c]`

Commands

`PgUp`	Display the top portion of the table
`PgDn`	Display the bottom portion of the table
`b`	Enter a new value of b
`c`	Enter a new value of c
`d`	Round down
`n`	Round to the nearest quotient
`P`	Print the table
`Esc`	Escape from the environment

Restrictions $|b| < 10^{18}$, $|c| < 10^{18}$

Algorithm The Euclidean Algorithm or Extended Euclidean Algorithm.

See also FastGCD, GCD, SlowGCD

FacTab

Function Constructs a TABle of the least prime FACtor of odd integers from $10N + 1$ to $10N + 199$.

Syntax `factab`

Commands

`PgUp`	Display the next 100 values
`PgDn`	Display the preceding 100 values
`N`	New N; view table starting at $10N + 1$
`Esc`	Escape from the environment

Restrictions Integers not exceeding $10^9 + 189$ (i.e. $0 \le N \le 99999999$).

Algorithm When the program begins execution, it first constructs a list of the odd primes not exceeding $\sqrt{10^9 + 200}$, by sieving. We call these the "small primes." There are 15803 such primes, the last one being 31607. The next prime after this is 31621. When N is specified, the odd integers in the interval $[10N, 10N + 200]$ are sieved by those small primes not exceeding $\sqrt{10N + 200}$; least prime factors are noted as they are found.

See also Factor, GetNextP

Factor

Function FACTORs a given integer n.

Syntax `factor [n]`

Restrictions $|n| < 10^{18}$

Algorithm Trial division. After powers of 2, 3, and 5 are removed, the trial divisors are reduced residues modulo 30.

Comments Factors are reported as they are found. The program can be interrupted by touching a key. This program provides a user interface for the procedure Canonic found in the NoThy unit. To view the source code, examine the file `nothy.pas`.

FareyTab

Function Constructs a TABle of FAREY fractions of order Q. Fractions are displayed in both rational and decimal form, up to 20 of them at a time.

Syntax `fareytab`

Commands

`PgUp`	View the next 19 smaller entries
`PgDn`	View the next 19 larger entries
`D`	Center the display at a decimal x
`R`	Center the display at a rational number a/q
`P`	Print the table (allowed for $Q \le 46$)
`Esc`	Escape from the environment

Restrictions $1 \le Q < 10^9$

Algorithm If a/q and a'/q' are neighboring Farey fractions of some order Q, say $a/q < a'/q'$, then $a'q - q'a = 1$. By the extended Euclidean algorithm, for given relatively prime a and q we find x and y such that $xq - ya = 1$. Then $q' = y + kq$, $a' = x + ka$ where k is the largest integer such that $y + kq \le Q$. With a/q given, the next smaller Farey fraction a''/q'' is found similarly. The Farey fractions surrounding a given decimal number x are found by the continued fraction algorithm. Fractions are computed only as needed by the screen or the printer.

See also FracTab

FastGCD

Function Times the execution of the Euclidean algorithm in calculating the Greatest Common Divisor of two given integers.

Syntax `fastgcd`

Restrictions $|b| < 10^{18}$, $|c| < 10^{18}$

Algorithm Euclidean algorithm, rounding down.

See also GCD, SlowGCD

FctrlTab

Function Provides a table of $n!$ (mod m). Each screen displays 100 values.

Syntax `fctrltab`

Commands

`PgUp`	View the preceding 100 entries
`PgDn`	View the next 100 entries
`J`	Jump to a new position in the table
`M`	Enter a new modulus
`P`	Print the first 60 lines of the table
`Esc`	Escape from the environment

Restrictions $0 \le n \le 10089$, $0 < m < 10^6$

Algorithm All 10089 values are calculated as soon as m is specified, unless $m < 10089$, in which case only m values are calculated.

FracTab

Function Lists FRACtions $(xa + ya')/(xq + yq')$ in a TABle with entries sorted according to the value of $\arctan y/x$, for $|x| \le Q$, $|y| \le Q$.

Syntax `fractab`

Remarks The data generated reflects some of the properties of Farey fractions.

Restrictions $1 \le a \le q < 10^3$, $1 \le a' \le q' < 10^3$, $Q < 10^3/q$, $Q < 10^3/q'$

See also FareyTab

GCD

Function Calculates the Greatest Common Divisors of two given integers.

Syntax `gcd [b c]`

Restrictions $|b| < 10^{18}$, $|c| < 10^{18}$

Algorithm Euclidean algorithm with rounding to the nearest integer.

See also EuAlgDem, FastGCD, SlowGCD

GCDTab

Function Constructs a TABle of the Greatest Common Divisors of pairs of numbers b, c.

Syntax `gcdtab`

Restrictions $|b| < 10^{18}$, $|c| < 10^{18}$

Algorithm Entries in the table are calculated by the Euclidean Algorithm.

See also GCD, EuAlgDem

GetNextP

Function Finds the least Prime larger than a given integer x, if $x \le 10^9$. If $10^9 < x \le 10^{18}$, it finds an integer n, $n > x$, such that the interval (x, n) contains no prime but n is a strong probable prime to bases 2, 3, 5, 7, and 11. A rigorous proof of the primality of n can be obtained by using the program PrimRoot.

Syntax `getnextp` [x]

Restrictions $0 \le x < 10^{18}$

Algorithm If $0 \le x \le 10^9$ then the least prime larger than x is found by sieving. If $10^9 < x \le 10^{18}$ then strong probable primality tests are performed.

See also FacTab, PrimRoot

IndTab

Function Generates a TABle of INDices of reduced residue classes modulo a prime number p, with respect to a specified primitive root. Also generates a table of powers of the primitive root, modulo p. Up to 200 values are displayed a one time.

Syntax `indtab`

Commands

`PgUp`	View the preceding 200 entries
`PgDn`	View the next 200 entries
`J`	Jump to a new position in the table
`E`	Switch from indices to exponentials
`I`	Switch from exponentials to indices
`M`	Enter a new prime modulus
`B`	Choose a new primitive root as the base
`P`	Print table(s)
`Esc`	Escape from the environment

Restrictions $p < 10^4$

Algorithm The least positive primitive root g of p is found using the program PrimRoot. The powers of g modulo p and the indices with respect to g are generated in two arrays.

See also PowerTab, PrimRoot

IntAPTab

Function Creates a TABle with rows indexed by $a \pmod{m}$ and columns indexed by $b \pmod{n}$. The INTersection of these two Arithmetic Progressions is displayed (if it is nonempty) as a residue class (mod $[m, n]$).

Syntax `intaptab`

Commands

↑	Move up
↓	Move down
←	Move left
→	Move right
`a`	Start at row a
`b`	Start at column b
`m`	Set modulus m
`n`	Set modulus n
`P`	Print (when table is small enough)
`Esc`	Escape from the environment

Restrictions $m < 10^4$, $n < 10^4$

Algorithm Chinese Remainder Theorem

See also CRT, CRTDem, ResComp

Comments Reduced residues are written in white, the others in yellow.

LinCon

Function Finds all solutions of the LINear CONgruence $ax \equiv b \pmod{m}$.

Syntax `lincon` [`a b m`]

Restrictions $|a| < 10^{18}$, $|b| < 10^{18}$, $0 < m < 10^{18}$

Algorithm The extended Euclidean algorithm is used to find both the number $g = (a, m)$ and a number u such that $au \equiv g \pmod{m}$. If $g \nmid b$ then there is no solution. Otherwise, the solutions are precisely those x such that $x \equiv c \pmod{m/g}$ where $c = ub/g$.

See also LnCnDem

LnCnDem

Function DEMonstrates the method used to find all solutions to the LiNear CoNgruence $ax \equiv b \pmod{m}$.

Syntax `lncndem` [`a b m`]

Restrictions $|a| < 10^{18}$, $|b| < 10^{18}$, $0 < m < 10^{18}$

See also LinCon

LnComTab

Function Constructs a TABle of the LiNear COMbinations of two given integers b and c.

Syntax `lncomtab`

Restrictions $|b| < 10^9$, $|c| < 10^9$

Merlin

Function Provides emulation of an electronic toy marketed in 1978 by Parker Brothers, now part of Hasbro; see `www.hasbro.com`.

Syntax `merlin`

Commands

`1`	reverse squares 1, 2, 4, 5
`2`	reverse squares 1, 2, 3
`3`	reverse squares 2, 3, 5, 6
`4`	reverse squares 1, 4, 7
`5`	reverse squares 2, 4, 5, 6, 8
`6`	reverse squares 3, 6, 9
`7`	reverse squares 4, 5, 7, 8
`8`	reverse squares 7, 8, 9
`9`	reverse squares 5, 6, 8, 9
`R`	Restart at a new random position
`Esc`	Escape from the environment

Comments The elapsed time, number of moves, and least possible number of moves is reported when the goal is attained.

Mult

Function MULTiplies residue classes. If a, b, and m are given with $m > 0$, then c is found so that $c \equiv ab \pmod{m}$ and $0 \le c < m$.

Syntax `mult` [`a b m`]

Restrictions $|a| < 10^{18}$, $|b| < 10^{18}$, $0 < m < 10^{18}$

Algorithm If $m \le 10^9$ then ab is reduced modulo m. If $10^9 < m \le 10^{12}$ then we write $a = a_1 10^6 + a_0$, and compute $a_1 b 10^6 + a_0 b$ modulo m, with reductions modulo m after each multiplication. Thus all numbers encountered have absolute value at most 10^{18}. If $10^{12} < m \le 10^{18}$ then we write $a = a_1 10^9 + a_0$, $b = b_1 10^9 + b_0$; we compute ab/m in floating-point real arithmetic and let q be the integer nearest this quantity; we write $q = q_1 10^9 + q_0$; $m = m_1 10^9 + m_0$. Then

$$ab - qm = ((a_1 b_1 - q_1 m_1)10^9 + a_1 b_0 + a_0 b_1 - q_1 m_0 - q_0 m_1)10^9 \\ + a_0 b_0 - q_0 m_0.$$

The right hand side can be reliably evaluated, and this quantity has absolute value less than m. If it is negative we add m to it to obtain the final result. The assumption is that the machine will perform integer arithmetic accurately for integers up to $4 \cdot 10^{18}$ in size. The object is to perform congruence arithmetic with a modulus up to 10^{18} without introducing a full multiprecision package.

Nim

Function

Syntax `nim`

Remarks

Restrictions

Algorithm

See also

Order

Function Calculates the ORDER of a reduced residue class $a \pmod m$. That is, it finds the least positive integer h such that $a^h \equiv 1 \pmod m$.

Syntax `order` [`a m` [`c`]]

Restrictions $|a| < 10^{18}$, $0 < m < 10^{18}$, $0 < c < 10^{18}$

Algorithm The parameter c should be any known positive number such that $a^c \equiv 1 \pmod m$. For example, if m is prime then one may take $c = m - 1$. If a value of c is not provided by the user, or if the value provided is incorrect, then the program assigns $c = \text{Carmichael}\,(m)$. (This involves factoring m by trial division.) Once c is determined, then c is factored by trial division. Prime divisors of c are removed, one at a time, to locate the smallest divisor d of c for which $a^d \equiv 1 \pmod m$. This number is the order of a modulo m.

See also OrderDem, OrderTab

OrderDem

Function DEMonstrates the method used to calculate the ORDER of a reduced residue class $a \pmod{m}$.

Syntax `order [a m [c]]`

Restrictions $|a| < 10^{18}$, $0 < m < 10^{18}$, $0 < c < 10^{18}$

Algorithm See the description given for the program Order.

See also Order, OrderTab

OrderTab

Function Constructs a TABle of the ORDER of a modulo m.

Syntax `ordertab`

Commands

$\rightarrow$	Display the next columns
$\downarrow$	Display the next 20 rows
$\leftarrow$	Display the preceding columns
$\uparrow$	Display the preceding 20 rows
`a`	Display column a
`m`	Display row m
`P`	Print a portion of the table
`Esc`	Escape from the environment

Restrictions $-9999 \le a \le 9985$, $1 \le m \le 9999$

See also Order, OrderDem

PascalsT

Function Constructs a table of PASCAL'S Triangle $\binom{n}{k} \pmod{m}$. Rows are indexed by n, columns by k. Up to 20 rows and 18 columns are displayed at one time.

Syntax `pascalst`

Commands

$\uparrow$	Display the preceding 20 rows
$\downarrow$	Display the next 20 rows
$\leftarrow$	Display the preceding 20 columns
$\rightarrow$	Display the next 20 columns
`T`	Move to the top of the triangle
`M`	Choose a new modulus
`Esc`	Escape from the environment

Restrictions $0 \le k \le n < 10^4$, $0 < m < 10^3$

Algorithm The rows are calculated inductively by the recurrence $\binom{n}{k-1} + \binom{n}{k} = \binom{n+1}{k}$. The entire nth row is calculated, where n is the top row on the current screen. Other entries in the screen are calculated from the top row.

PermCalc

Function Acts as a pocket calculator, for permutations.

Syntax `permcalc`

Commands

$\uparrow$	Display the preceding 20 rows
$\downarrow$	Display the next 20 rows
$\leftarrow$	Display the preceding 20 columns
$\rightarrow$	Display the next 20 columns
`T`	Move to the top of the triangle
`M`	Choose a new modulus
`Esc`	Escape from the environment

Remarks

Restrictions

Algorithm

See also

Phi

Function Calculates the Euler PHI function of n.

Syntax `phi` [`n`]

Restrictions $1 \le n < 10^{18}$

Algorithm The canonical factorization of n is found by trial division, and then $\phi(n)$ is found by means of the formula $\phi(n) = \prod_{p^\alpha \| n} p^{\alpha-1}(p-1)$.

Pi

Function Determines the number $\pi(x)$ of primes not exceeding an integer x.

Syntax `pi` [`x`]

Restrictions $2 \le x < 10^9$

Algorithm Primes up to 31607 are constructed, by sieving. These primes are used as trial divisors, to sieve intervals of length 10^4 until x is reached.

Comments The running time is roughly linear in x. For faster methods of computing $\pi(x)$, see the following papers.

J. C. Lagarias, V. S. Miller, and A. M. Odlyzko, "Computing $\pi(x)$: The Meissel-Lehmer method," *Math. Comp.* **44** (1985), 537–560.
J. C. Lagarias and A. M. Odlyzko, "New algorithms for computing $\pi(x)$," *Number Theory: New York 1982* (D. V. Chudnovsky, G. V. Chudnovsky, H. Cohn and M. B. Nathanson, eds.), pp. 176–193; Lecture Notes in Mathematics 1052, Springer-Verlag (Berlin), 1984.
J. C. Lagarias and A. M. Odlyzko, "Computing $\pi(x)$: an analytic method," *J. Algorithms* **8** (1987), 173–191.

PolySolv

Function Finds all solutions of a given polynomial congruence $P(x) \equiv 0 \pmod{m}$.

Syntax `polysolv`

Commands

`C`	Count the zeros
`D`	Define the polynomial
`M`	Choose the modulus
`Esc`	Escape from the environment

Restrictions $1 \le m < 10^4$, $P(x)$ must be the sum of at most 20 monomials, only the first 100 zeros found are displayed on the screen

Algorithm The polynomial is evaluated at every residue class modulo m.

Comments The running time here is roughly linear in m. When m is large there is a much faster method available, using more sophisticated techniques.

Power

Function Computes $a^k \pmod{m}$ in the sense that it returns a number c such that $0 \le c < m$ and $c \equiv a^k \pmod{m}$.

Syntax `power` [`a k m`]

Restrictions $|a| < 10^{18}$, $0 \le k < 10^{18}$, $0 < m < 10^{18}$

Algorithm If k is even, say $k = 2k'$, then $a^k \equiv (a^2)^{k'} \pmod{m}$. If k is odd, say $k = 2k' + 1$, then $a^k \equiv a(a^2)^{k'} \pmod{m}$. These identities are used repeatedly, until the exponent is reduced to 0.

See also PowerDem, PowerTab

PowerDem

Function DEMonstrates the POWERing algorithm used to compute $a^k \pmod{m}$.

Syntax `powerdem` [`a k m`]

Restrictions $|a| \le 10^{18}$, $0 \le k \le 10^{18}$, $0 < m \le 10^{18}$

See also Power, PowerTab

PowerTab

Function Constructs a TABle of POWERs $a^k \pmod{m}$.

Syntax `powertab`

Commands

$\uparrow$	Display the preceding 20 rows
$\downarrow$	Display the next 20 rows
$\leftarrow$	Display the preceding rows
$\rightarrow$	Display the next rows
`B`	Change the base
`E`	Move to a new exponent
`M`	Change the modulus
`P`	Print the first 54 lines of the table
`Esc`	Escape from the environment

Restrictions $|a| < 10^9$, $1 \le k < 10^9$, $1 \le m < 10^9$

Algorithm The first entry in each row is computed by the powering algorithm. Then the remaining entries on the screen are determined inductively.

See also Power, PowerDem

PrimRoot

Function Finds the least primitive root g of a prime number p, such that $g > a$.

Syntax `primroot` [`p` [`a`]] If p is specified on the command line but not a, then by default $a = 0$.

Restrictions $2 \le p < 10^{18}$, $|a| < 10^{18}$

Algorithm The prime factors $q_1, q_2, \ldots, q_r$ of $p-1$ are found by trial division. Then g is a primitive root of p if and only if both $g^{p-1} \equiv 1 \pmod{p}$ and $g^{(p-1)/q_i} \not\equiv 1 \pmod{p}$ for all i, $1 \le i \le r$. When a g is found that satisfies these conditions, not only is g a primitive root of p, but also the primality of p is rigorously established.

See also Order, OrderDem, OrderTab

ResComp

Function Compares residues $x \pmod{m}$ with $x \pmod{n}$.

Syntax `rescomp`

Restrictions $|x| < 10^9$, $1 \le m < 10^9$, $1 \le n < 10^9$

Algorithm Division algorithm to find remainders.

See also CRT, CRTDem, IntAPTab

RSA

Function Demonstrates RSA encryption. Plaintext is taken from an ASCII file with the default extension .txt. The ASCII code of a printable keyboard character lies between 32 and 126. By subtracting 32 we obtain a number between 0 and 94. In this way each character is associated with a 2-digit code. The code 95 is used as an end-of-line marker. The codes are concatenated k at a time to represent residues modulo m where $10^{2k} \le m < 10^{2k+2}$. Ciphertext can be saved as a sequence of residues to a file with the default extension .rsa. Public RSA parameters can be entered from the keyboard or read from a file with the default extension .pub. A line in the source file that begins with the symbol '%' is treated as a comment, and is passed to the destination file without alteration. When saving, the encryption history is included as a comment. This implementation is not secure because numbers $m < 10^{18}$ are easily factored. The RSA method is the patented property of RSA Data Systems. For information concerning licensing send email to patents@rsa.com. For information concerning RSA-based products, connect on the World Wide Web to http://www.rsa.com/.

Syntax `rsa`

Commands

↑	Move the window up one screenful
↓	Move the window down one screenful
`V`	set the Variables
`L`	Load plain or cipher text
`E`	Encipher
`D`	Decipher
`C`	convert from text or residues to Codes
`T`	convert from codes to Text
`R`	convert from codes to Residues
`S`	Save
`P`	Print
`Esc`	Escape from the environment

Restrictions $100 \le m < 10^{18}$, $0 < k < 10^{18}$, $0 < k' < 10^{18}$

Algorithm Each residue class $a \pmod m$ is replaced by $b \equiv a^k \pmod m$. To decipher, replace b by $b^{k'} \pmod m$ where $kk' \equiv 1 \pmod{\phi(m)}$.

See also RSAPars

RSAPars

Function Aids in forming RSA PARameterS. The private exponent k' is chosen first, and then m is constructed by choosing primes p such that $(p-1, k') = 1$. When m has been determined, the public exponent is derived. The public parameters m and k can be saved to a file, with the default extension .pub.

Syntax `rsapars`

Restrictions $1 < k' < 10^{18}$, k' odd, $100 \le m < 10^{18}$, m squarefree.

Algorithm Primes $p < 10^9$ are found (rigorously) by sieving. Primes $10^9 < p < 10^{18}$ are found (unrigorously) by applying strong pseudoprime tests to bases 2, 3, 5, 7, and 11. Once k' and the prime factors of m have been chosen, the public exponent k is determined by solving the linear congruence $kk' \equiv 1 \pmod{\phi(m)}$.

See also RSA, LinCon

R2D

Function Converts a Rational number a/q TO Decimal form, or in base b. If a and q (and optionally b) are entered on the command line then a screenful of digits is given and the program terminates. Otherwise the first 10^9 digits may be viewed, 1000 at a time. The base b can be changed; the default is $b = 10$. When $b > 10$ the 'digit' 10 is represented by A, ..., 15 by F. (When $b = 16$ this is the standard hexadecimal convention.) The digits are initially displayed in yellow, but the periodicity of the expansion can be highlighted, in which case alternate cycles are displayed in green and red. In this latter mode the length $T(a/q)$ of the aperiodic 'tail' and the length $C(a/q)$ of the 'cycle' are also displayed. (These values also depend on b.)

Commands

`PgUp`	Move the window up one screenful
`PgDn`	Move the window down one screenful
`J`	Jump to a new position in the table of digits
`a`	enter a numerator a
`q`	enter a denominator q
`B`	enter a base b
`C`	highlight or Conceal the Cycles
`P`	Print the first 2997 digits (1 page)
`Esc`	Escape from the environment

Syntax `r2d [a q [b]]`

Restrictions $1 \le a < q \le 10^9$, $2 \le b \le 16$

Algorithm Remainders r_i are uniquely determined by the relations $0 \le r_i < q$, $r_i \equiv ab^i \pmod{q}$. Digits d_i are found from the identity $br_i = d_i q + r_{i+1}$. Assume that $(a, q) = 1$. If there is an integer k such that $q \mid b^k$ then let k be the least such integer; the expansion terminates after exactly k digits. Otherwise, the length $T(a/q)$ of the aperiodic tail is the least non-negative integer t such that the denominator q' of ab^t/q is relatively prime to b. The length $C(a/q)$ of the cycle is the order of b modulo q'.

See also D2R, Order

SlowGCD

Function Times the calculation of the greatest common divisor of two numbers b and c, when only the definition is used. The only purpose in this is to provide a comparison with FastGCD.

Syntax `slowgcd`

Restrictions $|b| < 10^9$, $|c| < 10^9$

Algorithm For each d, $1 \le d \le \min(|b|, |c|)$, trial divisions are made to determine whether $d \mid b$ and $d \mid c$. A record is kept of the largest such d found. Since the running time is essentially linear in $\min(|b|, |c|)$, only small arguments should be used.

See also FastGCD, GCD

SumsPwrs

Function Finds all representations of n as a sum of s k-th powers, and counts them in various ways.

Syntax `sumspwrs [n s k]`

Restrictions $1 \le n < 10^{11}$, $2 \le s \le 75$, $2 \le k \le 10$

Algorithm After $s - 1$ summands have been chosen, a test is made as to whether the remainder is a k-th power. Summands are kept in monotonic order; the multiplicity is recovered by computing the appropriate multinomial coefficient. In some cases, such as sums of two squares, much faster methods exist for finding all representations.

See also Wrg1Tab, Wrg2Tab, WrgCnTab

WrngTab

Function Creates a TABle of the number $r(n)$ of representations of $n = \sum_{i=1}^{s} x_i^s$ as a sum of s k-th powers, as in WaRiNG's problem. If $k > 2$ then the x_i are non-negative, but for $k = 2$ the x_i are arbitrary integers.

Syntax `wrngtab`

Commands

`PgUp`	Move up
`PgDn`	Move down
`s`	Set s, the number of summands
`k`	Set k, the exponent
`N`	Start the table at $10n$
`P`	Print the table
`Esc`	Escape from the environment

Restrictions $1 \le s \le 75$, $2 \le k \le 10$, $1 \le n \le 10^{11}$

Algorithm Search for representations, with summands in monotonic order. The multiplicity of a representation is recovered by multiplying by the appropriate multinomial coefficient.

See also SumsPwrs