Instructor's Guide to

Elementary Number Theory

Second Edition

by

Underwood Dudley

DePauw University

W. H. FREEMAN AND COMPANY
San Francisco

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

TABLE OF CONTENTS

INTRODUCTION

The first purpose of this booklet is to give answers, where appropriate, to even-numbered problems in the text and to give hints and comments on some even-numbered problems. Its second purpose is to give supplementary material and references which teachers may or may not want to use. Its third purpose is to let me comment on aspects of number theory and its teaching. This material, which can be easily recognized, may be passed over entirely.

Teaching mathematics is frustrating. One reason for this is that for all too many students, mathematics is a collection of formulas, and a course in mathematics consists in learning which formula solves which type of problem. Why the formula is what it is, how it connects with other formulas, or what the idea behind it is are of little concern to the average student. He mainly wants to get a good grade; besides, considering such things takes more mental effort than applying, robot-like, some meaningless formula to some artificial problem. We teachers know better, of course: we know that mathematics is a rich and beautiful structure, filled with bright ideas and satisfying consequences. We try to get students to see this glory, but most of them stubbornly refuse even to try; instead of beauty, give them a formula every time. It is frustrating.

No one is really to blame for this. In the early years of education, minds are not mature enough to grasp anything but formulas and it is inevitable that teachers and students should treat mathematics as more or less arbitrary rules. Even in high school, so many students lack the capacity for abstract thought that teachers must present formulas and nothing else; they would soon go crazy otherwise.

So, college students cannot be blamed for thinking that mathematics is nothing but formulas and equations, but we should try to get them to give up this error and see the truth. Unfortunately, it is easy for students to go through the usual calculus sequence without changing attitudes at all, and courses in statistics and differential equations only reinforce their faith in formulas. What students need is a course in which formulas and equations are not much use; a course that demands thought; a course where ideas must be understood. The ideal course is, as all teachers of number theory know, a course in number theory. It is better than a course in abstract algebra because the subject matter is familiar and concrete: positive integers are much less threatening than left semi-injective k-groupoids. All teachers of number theory deserve great praise for the hard work they do in introducing generations of students to the true nature of mathematics. However, we will not get it: virtue must be its own reward.

It is because number theory is different from almost all mathematics a student has seen before that it is so difficult to teach. The students do not know that the course will be different from any other: master a few formulas, plug some things into them on examinations, and forget them after the course is over. They will not believe you, at first, when you tell them that they must concentrate on mastering the ideas and understanding why things are true. Number theory may be the first course that students have had where it is no longer possible to solve a problem by leafing back in the text to find the example that is just like the problem and mindlessly imitating it. (There is a successful elementary functions text, published by a large and reputable firm, which says in its preface "Practically every kind of problem found in the problem sets was previously enunciated and solved in the various illustrations." How terrible! Encouraging students to become robots instead of thinking people--there ought to be a law!) The problems in this book often give no clue at all in their statements of how to go about solving them. Students can find this upsetting, but that is where mathematical development can take place: in trying this, that, or the other idea until one works. Students should be encouraged to do this. They should be told, with examples, that there is more than one way to solve some problems and they should not expect to have a solution spring fully before them. Some students have the idea that if they cannot see, all at once, how a problem is to be solved, then they cannot do it. They think that if they do not know the formula that works, they are helpless. They should be told that some problems cannot be solved with formulas and they should be persuaded to try something even if they do not know where it will lead and even though there is no guarantee of success. Their tolerance for frustration may be so low that they will refuse, but point out that it is through trial and error that knowledge advances. Think of Edison, trying all those things for the filament of his light bulb.

This text is for a course that emphasizes problems and their solution. There is not all that much material in the text that it would not be possible to devote half of the class time to the problems. One device that I have found useful, not unpopular with students, and that encourages them to do problems is to require that each student hand in a card on the day that a set of problems have been assigned, listing the numbers of the problems he thinks he has solved and the numbers of the ones he has not solved. By looking through the collection of cards, the teacher can see which problems gave difficulty, and then can call on students to write solutions on the board of the hard problems, selecting the "volunteers" from among the students whose cards say that they have solved the problem. Students like to see lots of problems solved and the teacher has time to go out for a drink of water.

Knowing that problems may have to be exhibited to the whole class also encourages some students to take some care in their preparation. Most students do not realize that when they are writing the solution to a problem in mathematics they are writing in English. Most have the idea that the point of a problem is its answer (which is usually put in a box) and that what led up to it is unimportant. Of course, this is just backward. The answer to a problem is its least important part: the point of a problem is communicating its solution. One can point out that the practice in communication that students get in writing solutions will be valuable in life after school: they will most likely never have to solve a diophantine equation, but they will have to get ideas out of their heads and into the heads of others. Solving a problem has two parts: the first is getting the problem solved to the satisfaction of the solver and the second is putting the solution in a form so that someone else can understand it. This is a new idea to many students; they believe that once the answer is written down, nothing else is needed. Some students will not give up easily: if I had a dollar for every student who has said, in an aggrieved tone, "But there's the right answer--why did you take points off?" I would have--many dollars. Some students refuse to try to produce solutions written in English, others try and succeed only indifferently, but now and then a student will get the idea and produce mathematical prose that is almost indistinguishable from the prose in an average textbook. They are the students who master the mathematics too: does clear writing come from clear thinking, or can trying to write clearly force clear thinking?

All of the above may be of no particular use because teaching styles differ and they all work when done by the right person. My first number theory course was taught by an instructor whose style was to, in effect, copy the textbook on the blackboard for the class. That was probably bad style, and it is a tribute to the power of number theory that it can be transmitted to a receptive mind through many different agents.

SECTION 1

Some people think that a course in number theory ought to start with the development of the number system. There is something to be said for that idea, and students certainly ought to see the number system developed somewhere, but I have chosen to omit that material.

The purpose of mathematics is to deal with quantities in the world of physical reality so as to enable us to understand and control it. This is the reason mathematics is studied; if it were only symbol manipulation there would be no reason for preferring mathematics to chess as a topic of study. Both develop the mind in the same way, but we study mathematics because it is useful. I think that numbers are part of physical reality just as atoms are. That 17 is a prime is independent of the human nervous system; water is made up of hydrogen and oxygen throughout the universe; the square root of 2 has been and always will be irrational, even when the human race has disappeared. Number theory deals directly with physical things, and a course in number theory is thus a course in applied mathematics. Number theorists want to know why numbers do what they do and they will apply any area of mathematics--algebra, complex variables, anything useful--to find out.

In courses in applied mathematics, you want to get right to the real problems. In statics there is no time spent on the theory of n-dimensional vector spaces; in statistics there is no development of measure theory; we want to get our hands on the objects of study right away. Numbers are things to be investigated, even though ingenious man has shown that they can be constructed from other things.

Problems

2. 1 and 73.
4. The equation is $7x + 13y = 1$ and all solutions are $x = 2 - 13t$, $y = -1 + 7t$, t an integer.
6. All solutions are $x = 5 + 19t$, $y = -6 - 23t$, t an integer.
10. (a) If $p \mid n$ and $p \mid (n + 1)$, then $p \mid (n + 1) - n$. Or, note that $1 \cdot (n + 1) + (-1) \cdot n = 1$.

(b) 1 or 2 depending on whether n is odd or even.

14. There are integers x and y such that $cx + ay = d$, so $bcx + aby = db$. Each of the terms on the left is divisible by b.

SECTION 2

Identifying prime numbers has always been an important problem. Gauss sounded a little annoyed at the intractability of the primes when he wrote (Disquisitiones Arithmeticae, translated by A. A. Clarke, Yale University Press, New Haven, 1966, p. 396)

> The problem of distinguishing prime numbers from composite numbers and of resolving the latter into their prime factors is known to be one of the most important and useful in arithmetic. It has engaged the industry and wisdom of ancient and modern geometers to such an extent that it would be superfluous to discuss the problem at length. Nevertheless we must confess that all methods that have been proposed thus far are either restricted to very special cases or are so laborious and prolix that even for numbers that do not exceed the limits of tables constructed by estimable men, i. e., for numbers that do not yield to artificial methods, they try the patience of even the practiced calculator.

Gauss was nothing if not a practiced calculator. Students might be set to factoring numbers by hand--5-digit numbers would probably be as large as they could handle--or by pocket calculator, which would add two or three more digits. It would make them appreciate what labor factor tables and computers save, since even a mediocre factoring program can factor eight-digit numbers with ease and no one's patience is tried.

Students should be aware that number theory is not a dead subject and that the problem of distinguishing prime numbers is getting as much attention now as it did in the time of Gauss. The sieve of Eratosthenes, which takes about $n^{\frac{1}{2}}$ steps to verify that an integer of size n is prime, is not the last word in finding primes since there exist methods using only $n^{1/3}$ or $n^{1/4}$ steps. But even they take too long when they are used on integers of 60 or so digits. Very recently a new method has been devised which takes only about $\log_2 n$ steps, and 60-digit integers cause computers no difficulties at all.

Such an astonishing improvement is not made without some loss, and the loss is that the new method is probabilistic so it does not identify primes with absolute certainty. The idea is to test an integer, using a test based on Fermat's Theorem. The test says either "the integer is composite" or "the probability the integer is prime is 1/2." The test can be repeated, independently, so by doing it enough times, we can find that the integer being tested is either composite or that it prime with probability as close to 1 as we please. If the test does not say that the integer is composite 60 times in a row, then the probability that the integer is prime is $1/2^{60} = 8.67\cdot10^{-19}$ and that is close enough to zero to conclude that the integer is prime. We cannot be absolutely sure, and if we test 1,000,000,000,000,000,000 integers we will most likely make at least one mistake, but we can take that risk.

M. O. Rabin in "A probabilistic algorithm for testing primality" (to appear) reports that all of the Mersenne primes $2^p - 1$ with $p \leq 500$ were found by a computer in 10 minutes without error. Also, with probability $1 - 10^{-18}$, the largest primes less than 2^{300} and 2^{400} are $2^{300} - 153$ and $2^{400} - 593$, respectively. With the same probability, the largest pair of twin primes known--they have about 123 digits--are $\left(\prod_{p<300} p\right) 338 + 821$ and that number plus 2.

This new method has an application outside of mathematics. A method for sending messages in cipher, unreadable to those who do not know how to decipher them, is based on finding large numbers with exactly two large prime factors. If we have two 60-digit primes and multiply them together, even if our enemy captures the 120-digit product he will be helpless because he will not be able to factor it. (The probabilistic method tells only if an integer is prime or composite. It is of no help in finding the factors of integers known to be composite.) But we know the factorization and can decipher the message. The probabilistic method makes it easy to find 60-digit primes, something that was not easy before. Details on this application of number theory to national security can be found in Martin Gardner's Mathematical Games column in Scientific American 237 (August 1977) 120-124.

Problems

2. $5\cdot7\cdot67$, $2\cdot5\cdot4567$, $3^3\cdot7\cdot11\cdot13\cdot37\cdot101\cdot9901$. One way of getting the last factorization is to note that $10^{12} - 1 = (10^6 - 1)(10^6 + 1) = (10^3 - 1)(10^3 + 1)(10^6 + 1) = 999\cdot1001\cdot1000001$.

4. (a) The first counterexample occurs at $n = 20$: $119 = 7\cdot17$ and $121 = 11^2$. There are others at $n = 24$, 31, and 36.
(b) Each counterexample generates infinitely many others. For example, if $n = 20 + 77k$, $k = 0, 1, \ldots$, then $7 | (6n - 1)$ and $11 | (6n + 1)$ for all n.

8. No: $6 | 4\cdot3$.

10. One way is to note that $n^2 < n(n + 1) < (n + 1)^2$ if $n > 0$. Another is to note that $(n, n + 1) = 1$ and no two consecutive integers are perfect squares.

12. Since $p > n^{1/3}$, $n/p < n^{2/3}$. If n/p is composite, it has a prime factor less than $(n^{2/3})^{1/2} = n^{1/3}$, which is a contradiction.

14. $2^{ab} - 1 = (2^a - 1)(2^{(b-1)a} + 2^{(b-2)a} + \ldots + 1)$.

SECTION 3

Some of the problems at the end of this section are problems of recreational mathematics, so it would be appropriate to point out to students here that there is such a thing. It will no doubt surprise many that there are people who actually get enjoyment out of mathematics, but that is one reason for education--to learn about the new and strange. It is possible that a few students have latent within them the taste for recreational mathematics, and they should be given the chance to develop it. After all, recreational mathematics is a potential source of pleasure and those are rare enough that we should not let any slip by us. Much of recreational mathematics is number theory, and that provides yet another reason for studying it: in the March 1978 issue of a periodical that deserves wider circulation among students of mathematics, Crux Mathematicorum (currently $8 per year from the Managing Editor, F. G. B. Maskell, Mathematics Department, Algonquin College, 200 Lees Avenue, Ottawa, Ontario K1S 1N3, Canada), five of the ten problems for solution are problems in number theory and one of them--let p_n be the nth prime; for which n is $p_n^2 + 2$ prime--is problem 32 on page 198.

Less obscure than Crux Mathematicorum is Martin Gardner's monthly recreational mathematics column in Scientific American, always high in quality. The most important recreational mathematics journal is the Journal of Recreational Mathematics (Baywood Publishing Company, 120 Marine Street, Farmingdale, New York 11735) now in its tenth year.

One of the most popular forms of recreational mathematics problems is the cryptarithm, where an addition or multiplication has letters replacing digits and the problem is to find which digit stands for each letter. The first cryptarithm

$$\begin{array}{r} \mathrm{SEND} \\ \underline{\mathrm{MORE}} \\ \mathrm{MONEY} \end{array}$$

was the invention of the great English recreational mathematician, Henry Dudeney (1847-1930). A cryptarithm is good when it can be solved with the largest possible use of logic and the smallest possible use of trial and error. (Any cryptarithm can be solved by machine by substituting the at most $10! = 3,628,800$ possible values for the letters.) Dudeney's is good because logic shows that $M = 1$ and $O =$ zero. It follows that S must be 9 and that $E + 1 = N$. From $N + R +$ carry $= E + 10$ we get $N = 8$ and carry $= 1$. There are only a few cases to be considered to find that $D, E, N, Y = 7, 5, 6, 2$ and the unique solution is

$$\begin{array}{r} 9567 \\ \underline{1085} \\ 10652. \end{array}$$

Such things are fun to solve in the same way that crossword puzzles are fun to solve. Here is another which can be solved by most students, in print for the first time here: it is a chemical experiment, A + SOLID + A+SOLID = LIQUID. Inspection shows, successively, $L = 1$, $I = 8$, $S = 9$, $U = 3$, and $2A + D = 20$. It follows that $A = 7$ and $D = 6$, and then all that is left for O and Q are 2 and 4. The field is inexhaustible. For example, the cryptarithm

$$\begin{array}{r} \mathrm{N\ I\ N\ E} \\ \mathrm{E\ I\ G\ H\ T} \\ \mathrm{T\ H\ R\ E\ E} \\ \hline \mathrm{T\ W\ E\ N\ T\ Y} \end{array}$$

(J. of Recreational Mathematics 4 (1971) 137) was rotated ninety degrees

$$\begin{array}{r} \mathrm{T} \\ \mathrm{E\ T\ W} \\ \mathrm{N\ I\ H\ E} \\ \mathrm{I\ G\ R\ N} \\ \mathrm{N\ H\ E\ T} \\ \hline \mathrm{E\ T\ E\ Y} \end{array}$$

by Sidney Kravitz (J. of Recreational Mathematics 8 (1975-76) 309-310); not only do both have exactly two solutions, in both the sum of the digits in TWENTY is 20. Moreover, the missing digit is the same in both. Astonishing!

Recreational mathematics is not part of number theory, but students are not likely to hear about it otherwise, nor are they likely to discover it on their own. The alternative to bringing it up in class would be to have a course in recreational mathematics, but that would be a mistake, since reducing something to a course can take the fun out of it. Courses sometimes suck the life out of a topic.

Problems

2. $x = 1 + t$, $y = -2t$; $x = 4t$, $y = 3t$; no solutions.
4. No solutions; $x = 4t$, $y = 3t$, $t = 1, 2, \ldots$; $x = 3$, $y = 2$.
6. If p, d, and q denote the number of pennies, dimes, and quarters, respectively, then $p = 79 - 5t$, $d = 7 + 8t$, and $q = 14 - 3t$. Solutions in positive integers occur for $t = 0, 1, 2, 3$, and 4.
8. If s, j, and b stand for the number of sophomores, juniors, and backward seniors, then $s + j + b = 26$ and $125s + 90j + 50b = 2500$. There is only one solution in positive integers: $(s, j, b) = (8, 15, 3)$.
10. The problem is to solve $100c + d - 23 = 200d + 2c$ in nonnegative integers, and the solution shows that the check was for $25.51.

SECTION 4

The question "What is all this good for anyway?" may not have come up or it may already have been settled, but this section gives an opportunity to bring up an application of congruences, namely in generating random numbers. To answer "So who needs random numbers?" refer to authority: D. E. Knuth in volume 2 of The Art of Computer Programming devotes a long chapter to them. They are useful, he says, in a variety of ways: for simulation of natural phenomena in a computer, for selecting random samples, for giving data to test the effectiveness of computer algorithms, for making decisions (for example, optimal strategies in game theory involve random selections), and for recreation.

It is not easy to generate random numbers--any sequence written down by a person "at random" will fail one or more tests for randomness--and many different methods have been used. A currently popular one is the linear congruential method; it generates a sequence of numbers which is really not random at all since each number is determined by the one before, but the sequence passes all of the tests for randomness. Although strictly determined, the sequence looks absolutely chaotic, and that is the essence of randomness. The method is simple enough to describe: choose a starting value $r(0)$, a multiplier k, an increment a, a modulus m, and go to it: $r(n + 1) \equiv kr(n) + a \pmod{m}$, $n = 0, 1, \ldots$.

The sequence will repeat with period m, but if m is chosen large enough the repetition will not occur in practice. If a and k are chosen properly, the period of the sequence will be m, the largest possible value. Conditions which suffice for this are

$(a, m) = 1$
$k - 1 \equiv 0 \pmod{p}$ for all p which divide m
if m is a multiple of 4, then $4 \mid (k - 1)$.

There is an example of a theorem of number theory which has been applied in the world outside of number theory. Starting with $r(0) = 069315$, $k = 2701$, $a = 314159$, and $m = 1000000$ gives a sequence which starts 069315, 533974, 577933, 311192, 843751, 285610, 746769, 337228, 166987, 346046, 984405, 192064, 079023, 755282, 330841, ... : it will repeat after 1000000 terms and no term appears more than once, but to the eye it is total, utter, random chaos. Perfect chaos is very hard to create.

Problems

2. 1, 9, 72.
4. True.
6. 1, 2, 3, 6, 11, 22, 33, or 66.
10. 1, 7, 11, 13, 17, 19, 23, or 29.
14. $(n + 1)^3 - n^3 = 3n(n + 1) + 1 \equiv 1 \pmod{3}$.
16. (c) Sum every other digit in an integer and subtract the sum of the remaining digits. If the difference is divisible by 11, then the integer is divisible by 11.
18. Every palindrome with an even number of digits is divisible by 11.
20. $x^m - 1 = (x - 1)(x^{m-1} + x^{m-2} + \ldots + 1)$. Since $x \equiv 1 \pmod{m^k}$, $m^k \mid (x - 1)$. Since $x \equiv 1 \pmod{m}$, $x^{m-1} + x^{m-2} + \ldots + 1 \equiv 1 + 1 + \ldots + 1$ (m terms) $\equiv 0 \pmod{m}$. Thus $x^m - 1$ is divisible by m $k + 1$ times.

SECTION 5

The method for solving linear diophantine equations is very satisfying. Students in linear algebra classes often have trouble in going from, say, $x + 3y = 5$ to $x = 2 - 3t$, $y = 1 + t$, but the congruence method forces the result on them. The method generalizes, and it might be worthwhile to point this out. For example, take $3x + 4y + 5z = 100$. That is, $3x + 4y \equiv 0 \pmod{5}$ from which $y = 3x + 5t$. Substitute in the original equation, divide by 5, and we get $3x + 4t + z = 20$. That is, $3x + z \equiv 0$

(mod 4) from which $z = x + 4s$. Substitute and divide by 4 to get $x + t + s = 5$, and that gives the solution:

$$\begin{aligned} x &= 5 - s - t \\ y &= 15 - 3s + 2t \\ z &= 5 + 3s - t. \end{aligned}$$

Not only have we solved a linear diophantine equation, we have found a basis for the kernel of the linear transformation $T : R^3 \longrightarrow R^1$ defined by $T(x, y, z) = 3x + 4y + 5z$: it is

$$\{(-1, -3, 3), (-1, 2, -1)\} .$$

Further, we have found two lines which lie on the plane whose equation is $3x + 4y + 5z = 100$:

$$(5, 15, 5) + s(-1, -3, 3) \quad \text{and} \quad (5, 15, 5) + t(-1, 2, -1).$$

Number theory, transformations, planes--all mathematics is one!

Somewhere in any number theory course, students should see multigrades. If there are some students adept with the pocket calculator, you can set them to calculating the sums of

1, 15, 22, 50, 57, 71;
2, 11, 27, 45, 61, 70;
5, 6, 35, 37, 66, 67.

If done correctly, each of the three lines will sum to 216. That is no big surprise. Then set them to calculating the sums of the squares of the integers in the three sets. All will be 11500. That is mildly interesting, but when the sums of the cubes all turn out to be 682128 there ought to be some surprise, which should increase when the sums of the fourth powers all come out to be 42502564. (Students may be uninterested and daydreaming, but in an ideal world there would be gasps of astonishment.) Such astounding coincidences cannot go on forever since sooner or later the sums of the nth powers of the integers in the first set will dominate, because 71^n grows much faster than 70^n, but for fifth powers the sums are still identical: 2724334416. Anyone not amazed at that is fundamentally unamazable. A challenge to students would be to find a, b, c, r, s, t such that $a + b + c = r + s + t$ and $a^2 + b^2 + c^2 = r^2 + s^2 + t^2$; they might uncover some of the easily-discovered properties of multigrades. The problem of finding such things excited a great deal of interest once: there is a survey article, "The Tarry-Escott problem" by H. L. Dorwart and O. E. Brown in the American Mathematical Monthly 44 (1937) 613-626 that is as good now as it was 40 years ago. Multigrades continue to appear, off and on, in the literature of recreational mathematics; for example, there is "Multigrades" by D. C. Cross in Recreational Mathematics Magazine #13 (February 1963) 7-9. It is a field in which amateurs can find amusement.

Problems

2. 10; 13; 6, 15; $10x \equiv 492 \equiv -500 \pmod{992}$, so $x \equiv -50 \equiv 942 \pmod{992}$ and the solutions are 942 and 1934.
4. $x \equiv 5 \pmod 6$, $x \equiv 82 \pmod{385}$, $x \equiv 605 \pmod{1066}$.
6. For example, $15x \equiv 14$, $13x \equiv 14$, $12x \equiv 14$, and $20x \equiv 0 \pmod{20}$ have, respectively, 0, 1, 4, and 20 solutions.
8. 1092.
10. $x = 2$, $y = 5$; no solutions.
12. 301 or any number congruent to it (mod 420).
14. 62.
16. (a) Any integer congruent to 2223 (mod 3600).

(b) No. The first and third conditions cannot both be satisfied.

18. Let the integers be a, b, and c and solve $3a = 20r + r$, $5b = 20(r + 1) + (r + 1)$, and $7c = 20(r + 2) + (r + 2)$.

20. $ax \equiv 0 \pmod{b}$ has (a, b) solutions.

SECTION 6

If $aa' \equiv 1 \pmod{p}$, a' can be called the reciprocal of $a \pmod{p}$, and that allows us to define rational numbers $(\text{mod } p)$: let $a/b \pmod{p}$ be ab'. This leads to picturesque congruences which sometimes interest some students: $3 \equiv 1/5 \equiv 2/3 \pmod{7}$. It is a good exercise to see which properties of rational numbers carry over to rational numbers $(\text{mod } p)$. $3 \cdot 3 \equiv 9 \equiv 2 \pmod{7}$ and $(1/5)(2/3) \equiv 2/15 \equiv 2/1 \equiv 2 \pmod{7}$: no true mathematician could rest without verifying that what happens in that example happens in general.

Another example of picturesque congruences

$$\frac{5}{1} \equiv \frac{10}{2} \equiv \frac{4}{3} \equiv \frac{9}{4} \equiv \frac{3}{5} \equiv \frac{8}{6} \equiv \frac{2}{7} \equiv \frac{7}{8} \equiv \frac{1}{9} \equiv \frac{6}{10} \pmod{11}$$

illustrates what surprising discoveries can be made even at the lowest level of number theory. If the row of congruences is looked on as a permutation, with numerators going to denominators, then it can be written $(5\ 1\ 9\ 4\ 3)(10\ 2\ 7\ 8\ 6)$. Do the same thing starting with 9 and you get

$$\frac{9}{1} \equiv \frac{7}{2} \equiv \frac{5}{3} \equiv \frac{3}{4} \equiv \frac{1}{5} \equiv \frac{10}{6} \equiv \frac{8}{7} \equiv \frac{6}{8} \equiv \frac{4}{9} \equiv \frac{2}{10} \pmod{11};$$

the permutation is $(9\ 1\ 5\ 3\ 4)(7\ 8\ 6\ 10\ 2)$. The same one! And you get the same one starting with 3 or 4. If you start with 2, 6, 7, 8, or 10 you get the same one--$(1\ 8\ 9\ 6\ 4\ 10\ 3\ 2\ 5\ 7)$. What's more, 1, 3, 4, 5, and 9 are precisely the quadratic residues of 11. Why in the world is that? Does it happen in general? Give me my pencil and paper! Number theory offers the best place for a bright undergraduate to experience the joy of mathematical discovery and the mixed pain and pleasure of mathematical research. It is a pity that most students never experience the joy. It is more a pity that many of them do not believe that it exists.

Problems

2. 1, by Fermat's Theorem; $5^{12} \equiv 5^2 \equiv 3 \pmod{11}$; $1945^{12} \equiv 9^{12} \equiv 9^2 \equiv 4 \pmod{11}$.

4. $7^4 \equiv 1 \pmod{100}$, so $7^{355} \equiv (7^4)^{88} \cdot 7^3 \equiv 7^3 \equiv 43 \pmod{100}$.

6. $(314)^{162} \equiv (-1)^{162} \equiv 1 \pmod{7}$.

8. $(2001)^{2001} \equiv (-1)^{2001} \equiv -1 \equiv 25 \pmod{26}$.

10. (a) 0, 0, 0, 0.

(b) $(n - 1)! \equiv 0 \pmod{n}$ if $n > 4$ is composite. To prove this, if $n = ab$ with $a \neq b$, then both a and b occur among the factors of $(n - 1)!$. If $n = a^2$, then both a and $2a$ occur among the factors of $(n - 1)!$ because $n > 4$ and thus $a^2 - 1 > 2a$.

12. Fermat's Theorem says that $a^n \equiv b^n \equiv 1 \pmod{n + 1}$.

14. $(p - k)!(k - 1)! \equiv (-1)^k \pmod{p}$, $k = 0, 1, \ldots, p$. The proof is a generalization of Problem 11.

16. $2^{340} \equiv 1 \pmod{341}$, but $341 = 11 \cdot 31$ is not prime.

18. $2^{2p-1} \equiv 2(2^{p-1})^2 \equiv 2 \pmod{p}$, so $p \mid (2^{2p-1} - 2)$. The number is even, so 2 divides it also.

20. Apply Problem 19 with $n = 10$.

SECTION 7

The formula $\sigma(p^n) = (p^{n+1} - 1)/(p - 1)$ appears in this section only because it is shorter to write than

$$\sigma(p^n) = 1 + p + p^2 + \ldots + p^n.$$

That is its only advantage, and it gives an excuse for a short lecture against formulas. Students love formulas, but formula thinking is just the opposite of what mathematical reasoning ought to be and students should be discouraged from using formulas whenever possible. Which is easier to calculate, $1 + 3 + 9$ or $(3^3 - 1)/(3 - 1)$? The first. Which suggests a sum of divisors better, $1 + 3 + 9$ or $(27 - 1)/2$? The first. Formulas often obscure meaning. Students should be told that no formula has ever or will ever solve any serious problem. That is because a serious problem is, by definition, one on which a formula will not work. Students should be aware that the serious problems of the future--the ones they are going to have to solve--are not going to yield to any formula they can learn now, and instead of committing things to memory, they should concentrate instead on developing their powers of reason, of abstraction, of seeing analogies and patterns, and so on. Giving such a lecture will not change students' behavior at all, or at most not much, since the safest way to a grade is to memorize formulas, they think, but a few students may remember twenty or thirty years on and think, "How right my number theory teacher was about formulas! How wise he or she was!" Such are the delayed rewards of teaching.

Problems

2. 24, 1680, 48, 18600.

4. 18, 25662; 36, 264992.

8. Yes: $d(2^{k-1}) = k$.

10. $d(p^{59}) = 60$ for any p, as is obvious. Less obvious is $60 = d(p^{29}q) = d(p^{19}q^2) = d(p^{14}q^3) = d(p^{11}q^4) = d(p^9q^5) = d(p^9q^2r) = d(p^5q^4r) = d(p^4q^2rs)$ for distinct primes p, q, r, s.

12. Any n which is a power of 2 times an odd square.

16. Let n be any prime greater than 3.

18. Proceed as in the text to get $\sigma_2(p^e) = 1 + p^2 + \ldots + p^{2e}$ and $\sigma_2(p_1^{e_1}p_2^{e_2}\ldots p_r^{e_r}) = \sigma_2(p_1^{e_1})\,\sigma_2(p_2^{e_2})\ldots\sigma_2(p_r^{e_r})$.

SECTION 8

Amicable numbers are still being looked for. Euler, who had great computational skill, found 59 pairs and almost 1500 are known now. Recently a computer search was made for pairs of the form kpq, kr where p, q, and r are distinct primes, each relatively prime to k. (J. of Recreational Mathematics 10 (1977-78) 183-189.) Seven new pairs were found, the smallest being 201,477,789,315 and 202,655,860,605. Factored, the pair is $3^5 \cdot 5 \cdot 11 \cdot 59 \cdot 197 \cdot 1297$ and $3^5 \cdot 5 \cdot 11 \cdot 59 \cdot 257003$. An exercise, to be done either by hand or to test a computer program which calculates $\sigma(n)$, would be to verify that the pair is indeed amicable. It would be harder if the pair was given in unfactored form; in that case the student should be told that 257003 is a prime. Another new pair is

$$3^4 \cdot 5 \cdot 11^3 \cdot 137 \cdot 71 \cdot 542519 \quad \text{and} \quad 3^4 \cdot 5 \cdot 11^3 \cdot 137 \cdot 39061439$$

or 2,844,637,606,234,215 and 2,884,708,168,019,865. There are many unanswered questions about amicable numbers, and some may be unanswerable.

The first problem in the Additional Problems for this section deals with numerology. That problem concerns deficient years, an idea I thought of by myself, though no doubt it appears somewhere in the vast literature of numerology. That literature consists of books and pamphlets, mostly printed on cheap paper, with titles like *The Secret of Numbers Revealed*, or *Numbers, Their Occult Power and Mystic Virtues*, for sale in stores which specialize in the occult. It is all great nonsense, but students are invariably fascinated by it so it may be worthwhile to devote some class time to it. Students who never ask questions will, and faces which usually bear looks of long-suffering boredom will brighten up.

This is because there seems to be a natural tendency in the human mind to wish to believe the incredible, as if the world as it is does not provide enough things to marvel at. Astrology, pyramid power, biorhythms: there is always some expression of the human lust for the irrational and there always will be until evolution has proceeded far enough that rational thought comes naturally to the human species. Astrology is the most widespread of the occult sciences; many newspapers, to their shame, publish astrology columns which pretend to give accurate predictions of the future, arrived at with no hard work or rational thought. It is mostly harmless stuff like "Relative may cause difficulty. Relax in the evening," but it is still encouraging the idea that knowledge about the future can be arrived at by revelation, and revelation is superior to other methods. Teachers of mathematics ought to be opposed to such notions, since our job is to illustrate the advantages of rationality. What astrologer could have found Maxwell's Equations?

Numerology is very like astrology even though it has not yet made the newspapers. Astrologers divide all people into twelve classes according to their dates of birth and numerologists divide all people into nine classes according to what their names turn out to be congruent to (mod 9). The method for converting a name into a number is quite simple, perhaps because numerologists are not capable of anything more complicated mathematically. Let A have the value 1, let B be 2, ..., let Z be 26, add, and reduce the total (mod 9). The modulus 9 was picked partly because each person is assigned a single digit 1, 2, ..., 9 (if the sum is 0 (mod 9), numerologists change it to 9) and partly because the calculation is simple, since addition modulo 9 never involves more than adding one digit to another: $9 + 8 \equiv 17 \equiv 1 + 7 \equiv 7 \pmod 9$. So as to never have to consider two-digit numbers, numerologists use the following chart

1	2	3	4	5	6	7	8	9
A	B	C	D	E	F	G	H	I
J	K	L	M	N	O	P	Q	R
S	T	U	V	W	X	Y	Z	

For example, Carl Friedrich Gauss has for his number

$$3 + 1 + 9 + 3 + 6 + 9 + 9 + 5 + 4 + 9 + 9 + 3 + 8 + 7 + 1 + 3 + 1 + 1$$

and that is 1 (mod 9). Just as all Aquarians share certain traits, according to the astrologers, so do all 1s, according to the numerologists. Words which characterize 1s include

positive, creative, optimistic, progressive, self-determination, forceful, independent, decisive, a leader, courage, pioneer

agression, arrogance, bossiness, vacillation

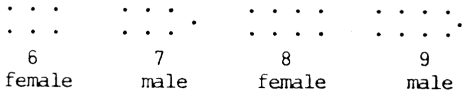
Isn't that Gauss? Creative and independent, and also arrogant. You would never confuse him with a 2, whose characteristic words are

emotional, maternal, sympathetic, understanding sensitivity, cooperation, rhythm, attentive to detail, rest

self-depreciation, cowardice, shyness, apathy, mischievousness, appeasement

Numerology is onto something, isn't it?

Numerology goes back at least as far as Pythagoras, who was very impressed with how number permeated the universe. He, or his followers, got carried away and went beyond verifiable facts about numbers, such as pairs of vibrating strings produce harmonious tones when their lengths have ratios which are quotients of small whole numbers like 3 to 2, to non-verifiable ones such as odd numbers are male and even numbers are female. (The reason for that was that odd numbers have male shapes and even numbers have female shapes:



Bring that up in class and interest will be redoubled, as it always is at any hint of sex.) That survives today, as the characteristics of 1s and 2s show: the words describing 1s are those assigned to stereotypical males and the words for 2s are traditionally assigned to females. Pythagoras's school developed a whole number mysticism, and its ideas have been copied by generations of numerologists.

Open any numerology book--they are all essentially the same--and you will find what the characteristics of each number are. Just as there is general agreement among astrologers about the characteristics of those born under each sign of the Zodiac, there is agreement among numerologists about what the characteristics of each number are. That is because they have independently had the same revelation or that they have all copied from each other. Numerology, like astrology, has undergone great elaboration. There are not only name numbers, but birth date numbers, cycle numbers, karma numbers, destiny numbers, intensification numbers, numbers without end, harmonizing or conflicting with each other; the chief difference among numerologists is how they choose to elaborate the basic system. Most numerological writing about specific numbers is so vague that anyone can see himself described, just as in astrology. For example,

> You are very versatile. You can handle many types of people and can use your talents in more than one field at a time.
>
> You have a clear, logical head that can size up situations with an uncanny sense of fairness and justice.

You would agree, perhaps with a modest blush, that those describe you, would you not? But the first is a description of a 3 and the second is a 6.

Numerology has lasted a long time and it is not likely to wither away. It appeals to the irrational in all of us. A group of people who know each other can test the claims of numerology by having the words descriptive of the various numbers written on slips of paper and choosing the slip most characteristic of each person. I have done this, and the results showed considerably more agreement with numerology than chance would have caused to occur. It is enough to shake one's faith in reason. In astrology, nature may imitate art: after reading fifty times that Capricorns are reserved, a Capricorn may start to act reserved, but numerology has not been as well written up. Clearly, more research is needed, and to make it possible here are lists of words characteristic of the other digits.

> 3: communication, extrovert, entertainer, creative imagination, charm, popularity, physical beauty, pleasure, facility with language
>
> conceit, verbose, superficial, impatience, extravagance
>
> 4: self-discipline, practicality, physical work, endurance, order, method, construction, industry, honesty, reliable
>
> isolation, reactionary, cautious, stingy, stubborn, vulgarity, envy
>
> 5: freedom, change, adaptability, variety, resourceful, risk, travel, curiosity, sensual, speculation
>
> impulsive, restless, fickle, hypercritical, irresponsibility
>
> 6: responsibility, conscientious, reliability, adjustment, teaching, conservative, concern for balance
>
> meddling, self-righteous, obstinacy, overanxiety

7: wisdom, secrecy, study, research, writing, observation, faith, dignity, pride, specialization, introspection

scepticism, pessimism, melancholy, aloof, dishonesty

8: control, power, success, good judgement, achievement, executive ability, fairness, material freedom, efficiency

greed, ruthless, vindictiveness, poor judgement

9: selflessness, completion, compassion, tolerance, generous, justness, benevolence

extremes in emotions, vulgar, sentimentality, bitterness, waste

These lists are too short for someone to internalize the occult meanings of integers; that takes a long immersion in the writings of numerologists, which is probably not a good thing to do. In fact, it is best to stay away from them completely, lest anyone be seduced from the path of rationality, so hard to stay on, so pleasant and easy to fall off.

Problems

4. 402, 408, 414, 416, and 420 are abundant and the others are deficient.

6. If $\sigma(2^a3^b) = 3\cdot 2^a3^b$ then $(2^{a+1} - 1)(3^{b+1} - 1) = 2^{a+1}3^{b+1}$ and that is impossible.

8. $3^a\cdot 5\cdot 7$ is abundant for every $a \geq 3$.

10. Yes: $2^{p-1}(2^p - 1) = 1 + 2 + \ldots + (2^p - 1)$.

12. If $n = 2p(2p + 1)$ and $2p + 1$ is a prime, then $\sigma(n) - 2n = -2p^2 + 8p + 6$, and this is negative if $p \geq 5$.

14. Since $2^6 \equiv 1 \pmod 9$, $2^{p-1} \equiv 1$ or $7 \pmod 9$ for $p \geq 5$. Also, $2^p \equiv 2$ or $5 \pmod 9$. Thus $2^{p-1}(2^p - 1) \equiv 1\cdot 1$ or $7\cdot 4 \equiv 1 \pmod 9$. The case $p = 3$ can be considered separately.

SECTION 9

Number theory is full of names of mathematicians: Euler's function, Legendre symbols, Gauss's lemma, Fermat's theorem, the Euclidean algorithm; there is great opportunity to include historical material. It is a good idea. Students tend to like it because it is a break from the routine of mathematics and it will not be on the next test. It can let a student who knows some history put mathematical discoveries (which are hardly ever mentioned in general historical works) into their proper place in the scheme of human development. It can show that mathematics is a human activity and theorems are not handed down by gods, carved on stone tablets,

It is hard to do that because most writers of mathematical history concentrate on mathematical life and ignore the rest. Pick up a book of mathematical history at random and see if that is not so. Here is an excerpt from the middle of page 154 of Hilbert, by

Constance Reid (Springer, New York, 1970)

> The next summer Hilbert lectured on relativity theory as part of a University series for all of the faculties.

The middle of page 154 of *Niels Henrik Abel*, by Oystein Ore (University of Minnesota Press, Minneapolis, 1957):

> With very few acquaintances and low ebb in his purse Abel could do little else than write mathematics, and the last months in Paris turned out to be extremely fruitful. A few days after his great memoir had been submitted to the Institute, he completed a lesser paper on equations, which he presented to Gergonne's *Annals*.

The middle of page 154 of *Carl Friedrich Gauss*, by G. Waldo Dunnington (Hafner, New York, 1955):

> By January, 1832, he had thrown himself with all force into the investigation of magnetism, and by February of that year had succeeded in reducing the intensity of terrestrial magnetism to absolute units.

The middle of page 154 of *Joseph Fourier*, by I. Grattan-Guinness (M. I. T. Press, Cambridge, 1972):

> On calculera de même la valeur de d pour le cas de quatre inconnues et on multiplera cette valeur par $9^2/(9^2 - 7^2)$, $11^2/(11^2 - 7^2)$, $13^2/(13^2 - 7^2)$, ...

It is hard to make mathematics human. Mathematicians mostly lead dull lives, and colorful anecdotes bringing them alive as people are rare. Howard Eves has collected almost all known mathematical anecdotes in *In Mathematical Circles* (two volumes), *Mathematical Circles Revisited*, and *Mathematical Circles Adieu* (Prindle, Weber, and Schmidt, Boston, 1969, 1971, 1977) and the National Council of Teachers of Mathematics have done their best to gather useful material in *Historical Topics for the Mathematics Classroom* (NCTM, Washington D. C., 1969), but the amount of human interest is limited. It is a shame that mathematicians as people have been so neglected. (If you think that they have not been neglected, then can you tell which of Legendre, Laplace, Lagrange, and L'Hospital was the tallest? Which had the most children? Which had the happiest life?) The names of mathematicians are not the names of people, they are the names of gods who create theorems, and it is too bad.

We need a supply of better anecdotes. It is so bad now that even the anecdotes that were made up and tell about things that never happened are no good. For example, the one about how DeMoivre started sleeping 15 minutes more each night until he got up to 24 hours and then died is incredible on the face of it and pointless even if it were true. It was clearly made up by a non-mathematician, and not a clever non-mathematician either. The well-known anecdote about Euler's algebraic proof of the existence of God is another example. Why would Diderot agree to hear such a thing when he was no mathematician? Why would Euler present nonsense like "$(a^n + b)/c = n$ donc Dieu existe"? Ridiculous! That such feeble stories should gain acceptance and be constantly repeated shows how easy it is for counterfeit anecdotes to get into circulation and stay there. Mathematical authors should make up good anecdotes about famous mathematicians, illustrating their human qualities; there is a need for them, it is not being filled by historians, and unless such things start to appear I will make some up.

Another great need is a good supply of mathematical quotations. There is a collection (*Memorabilia Mathematica*, by Robert Edouard Moritz, 1914, reprinted by Dover, New York, 1955 as *On Mathematics and Mathematicians*), but it is filled with pedestrian things like

> We may safely say, that the whole form of modern mathematical thinking was created by Euler. It is only with the greatest difficulty that one is able to follow the writings of any author immediately preceeding Euler, because it was not yet known how to let the formulas speak for themselves. This art Euler was the first one to teach.

which is taken from page 154. There are a few good things, like Kronecker's "God made integers, all else is the work of man," (which should be repeated to every number theory class at least once), and some jokes

> Why are *wise* few, *fools* numerous in the excess?
> 'Cause, wanting *number*, they are *numberless*.

(Lovelace, 1659, quoted on page 269) which will go over the heads of most of a class. There is a need for made-up quotations which tellingly illustrate mathmatical points. Put students to work on the job.

Problems

2. 18, 144, 1440.
4. 3360, 33048.
6. $a^8 \equiv 1$ if a is odd and 0 if a is even (mod 16).
8. None: $\varphi(n) < n$ for all n.
10. $\sum_{p \le x}(p + 1) - \sum_{p \le x}(p - 1) = \sum_{p \le x} 2 = \sum_{p \le x} d(p)$.
12. $ax \equiv ca^{\varphi(m)} \equiv c \pmod{m}$.
14. All solutions are 17, 32, 34, 40, 48, and 60.
16. Use the Corollary to Theorem 3: if m and n have a common factor, then $\prod_{p|n}(1 - 1/p) \cdot \prod_{p|m}(1 - 1/p)$ has more factors, each smaller than 1, then $\prod_{p|mn}(1 - 1/p)$.
18. Put $n = 2^k N$ with N odd. Then $\varphi(n) = 2^{k-1}\varphi(N)$ and $n/2 = 2^{k-1}N$. The two are equal if and only if $\varphi(N) = N$, and that is true if and only if $N = 1$.
20. If n has more than two distinct odd prime factors, then $\varphi(n)$ would be divisible by 8. Thus $n = 2^a p^b q^c$ and $\varphi(n) = 2^{a-1}p^{b-1}(p - 1)q^{c-1}(q - 1)$. It is not hard to show that product can never equal $14 = 2 \cdot 7$.

SECTION 10

Some students may have seen the words "primitive root" before in primitive roots of 1. The same words are used because the idea is the same: the powers of a primitive root sweep through everything possible. Thus $-i$ is a primitive fourth root of 1 because its powers $(-i)^1 = -i$, $(-i)^2 = -1$, $(-i)^3 = i$, and $(-i)^4 = 1$ include all of the fourth roots of 1. In the same way that $-i$ is a primitive root of the equation $x^4 = 1$, 2 is a primitive root of the congruence $x^4 \equiv 1 \pmod 5$ since its powers $2^1 \equiv 2$, $2^2 \equiv 4$, $2^3 \equiv 3$, and $2^4 \equiv 1 \pmod 5$ include all solutions of the congruence. Students familiar with complex numbers should feel satisfaction at the exact parallel.

The parallel extends to finding which roots are primitive roots. If r is a primitive root of $x^n = 1$, then so is r^k for those k with $(k, n) = 1$: the proof is the same as the proof of Lemma 1, but with equalities instead of congruences. Thus there are $\varphi(n)$ primitive nth roots of 1.

Problems

2. 3, 5, 6, 7, 10, 11, 12, and 14 have order 16; 2, 8, 9, and 15 have order 8; 4 and 13 have order 4; 16 has order 2; 1 has order 1.
4. They are 7, 10, 11, 14, 15, 17, 19, 20, and 21.
6. 4, 4, 2, 2, 4, 4, 2. No.
8. 11 and 27.
10. If k is even, then $(h^k)^{(p-1)/2} \equiv 1 \pmod p$, which is impossible since h is a primitive root. Another way to solve the problem is to note that since h^k is a primitive root, $(k, p - 1) = 1$ so k must be odd.
12. No. If $h \equiv g^r$ and $k \equiv g^s \pmod p$, it is possible that $(1 + r + s, p - 1) \neq 1$. For example, 2, 8, and 19 are primitive roots of 29, but the least residue of their product is 17, not a primitive root of 29.
14. Since $a^p \equiv -1 \pmod q$, a has order $2p$ or 2. If a has order 2, then $a \equiv -1 \pmod q$ and $q \mid (a + 1)$. If a has order $2p$, then $2p \mid \varphi(q)$, or $2p \mid (q - 1)$.
16. From Theorem 3, any prime factor must have the form $34k + 1$. Also, the smallest prime factor must be less than $\sqrt{131071} = 362.037\ldots$. The only primes to test are 103, 137, 239, and 307.
18. Let $x = g^k$. If $gx \equiv x + 1 \pmod p$, then $(g - 1)x \equiv 1 \pmod p$. This has exactly one solution since $(g - 1, p) = 1$.
20. (a) If g is a primitive root of p, the product is
$$g \cdot g^2 \ldots g^{\varphi(m)} \equiv g^{\varphi(m)(\varphi(m)+1)/2} \equiv (g^{\varphi(m)/2})^{\varphi(m)+1}$$
$$\equiv (-1)^{\varphi(m)+1} \equiv -1 \pmod m.$$
(b) If $m = 8$, the result is not true.

SECTION 11

It is conceivable that a student might wonder, while on the subject of quadratic congruences, whether the quadratic formula, so useful for solving quadratic equations, is any good on congruences. It is, since completing the square works (mod m), and students might enjoy solving something like $3x^2 + x + 8 \equiv 0 \pmod m$ using it. The solutions should be $x \equiv (-1 \pm \sqrt{1 - 96})/6 \pmod{11}$. Since $\sqrt{-95} \equiv \sqrt{4} \equiv 2$ and $1/6 \equiv 2 \pmod{11}$, this is $x \equiv (-1 \pm 2) \cdot 2 \equiv 2$ or $5 \pmod{11}$, and those are indeed the solutions.

This is an example of how if one proceeds as if something is true, true results may come out. Euler did the same thing, dealing with divergent series as if they were convergent, and found new and useful things. Try something--it might work: timid students, fearful of doing something wrong, should be told to emulate Euler.

Problems

2. Only the last.
4. $x \equiv 25$ or $9948 \pmod{9973}$.
6. $-1, -1, 1, 1$
8. $x \equiv 2$ or $5 \pmod{11}$ for both.
10. $1, -1$.
12. $p \equiv 1 \pmod 4$ so $(3/p) = (p/3) = ((12k + 1)/3) = (1/3) = 1$.
16. $1 = (1/p) = (ab/p) = (a/p)(b/p) = (b/p)$.
18. Let $(p - 1)/2 = q$. Then $(q/p) = (p/q)$ because $q \equiv 1 \pmod 4$. But $(p/q) = ((2q + 1)/q) = (1/q) = 1$.
20. $(p/q) = ((q + 4a)/p) = (4a/q) = (a/q)$. Also $(q/p) = ((p - 4a)/p) = (-4a/p) = (-1/p)(a/p)$. Thus $(p/q)(q/p) = (-1/p)(a/p)(a/q)$. Since $p \equiv q \pmod 4$, if $p \equiv q \equiv 1 \pmod 4$, then by the quadratic reciprocity theorem, $1 = (p/q)(q/p) = 1\cdot(a/p)(a/q)$ so $(a/p) = (a/q)$. The case $p \equiv q \equiv 3 \pmod 4$ is similar.

SECTION 12

This section contains the hardest material in the text. Gauss's proof of the quadratic reciprocity theorem is an example, perhaps the first that students have seen, of an extended proof where more than one idea is needed to go from hypotheses to conclusion and it is worth going through if only to induce awe that a human mind could produce such a thing. In many students awe may not be induced, but the principle of exposing students to the best is as good in mathematics as it is in music, literature, or art, and the hope is that if appreciation is not immediate, then the seeds of later appreciation have been sown. At least students may appreciate that there is something there to appreciate.

Problems

2. $p = 4^n + 1 \equiv 1 \pmod 4$, so $(3/p) = (p/3) = (2/3)$. Or, note that $4^n \equiv 4 \pmod{12}$ for all positive n and apply Problem 1.
4. (a) 2 is a quadratic residue (mod p), so $1 = (2/p) \equiv 2^{(p-1)/2} \pmod p$, by Euler's Criterion.
   (b) 167.
6. (a) $p = 2$, and those odd p with $(-1/p) = 1$. That is, $p = 2$ or $p \equiv 1 \pmod 4$.
   (b) All: $p|(p^2 + p)$.
   (c) Those congruent to 1 (mod 4) because $n^2 + 2n + 2 = (n + 1)^2 + 1$.
8. The sum of the residues is twice $1^2 + 2^2 + \dots + ((p - 1)/2)^2$, and since the sum of the first n squares is $n(n + 1)(2n + 1)/6$,

the sum is $(p - 1)p(p + 1)/12$. Since $12 | (p - 1)(p + 1)$, the sum is zero (mod p).

10. Let $h = (p - 1)/2$. Then

$$\begin{aligned} -1 \equiv (p-1)! &\equiv (p-1)(p-2)\ldots(p-h)h! \\ &\equiv (-1)(-2)\ldots(-h)h! \\ &\equiv (-1)^h h!h! \pmod{p}. \end{aligned}$$

Since $p \equiv 1 \pmod 4$, the first factor is 1 and the result follows.

SECTION 13

This section and the next two are included for relaxation from the rigors of the last few sections. What they contain is not used later, and they do not contain much from what has gone before. If a class does not need the relaxation, they can be left out without loss or students may read them by themselves.

There are all sorts of ways of representing numbers. Bases may be negative integers, and I have heard that such bases are useful inside computers. The result for negative bases is the same as for positive bases: every integer n has a unique representation $n = d_0 + d_1b + d_2b^2 + \ldots + d_kb^k$ where $0 \leq d_i < b$, $i = 0, 1, \ldots, k$. The result is the same because the algorithm for finding the digits is the same: repeated division by the base. For example, to find the representation of 1453 in base -8 we have

$$\begin{aligned} 1453 &= (-181)(-8) + 5 \\ -181 &= (23)(-8) + 3 \\ 23 &= (-2)(-8) + 7 \\ -2 &= (1)(-8) + 6 \\ 1 &= (0)(-8) + 1 \end{aligned}$$

so $1453_{10} = 16735_{-8}$. Similarly, $1453_{10} = 19553_{-10}$. Students may extract some enjoyment out of counting in negative bases: in base -3, it goes 1, 2, 120, 121, 122, 110, 111, 112, 100, 101, 102, 220, ...

Problems

2. 123300_4, 24101_5, 12120_6, 3360_8, 1376_{11}.

4. 299, 653, 905, 8425.

6. 254, 11, 1.

8.

	2	3	4	5	6	7
2	4	6	10	12	14	16
3	6	11	14	17	22	25
4	10	14	20	24	30	34
5	12	17	24	31	36	43
6	14	22	30	36	44	52
7	16	25	34	43	52	61

10. 106, 376, 1340, 287286.

12. 15/32, 4/7, 53/63.

14. (c) In any base with $b \equiv 1 \pmod 2$.

16. To prove that there is such a representation, mathematical induction will work. To show that it is unique, choose

r so that $(3^r + 1)/2 \leq n < (3^{r+1} + 1)/2$. Then

$$(-3^r + 1)/2 \leq n - 3^r < (3^r + 1)/2.$$

18. Group the terms in a base-2 representation by threes:
$(d_0 + d_1 2 + d_2 2^2) + (d_3 + d_4 2 + d_5 2^2)8 + \dots$;
each of the numbers in parentheses is one of 0, 1, 2, 3, 4, 5, 6, 7.

20. $4b + 5 = n^2$, $5b + 5 = (n + 1)^2$, $b = 2n + 1$, $n = 9$, $b = 19$.

SECTION 14

Problem 6 is the easy verification that in base 12 the last digit of a square is always itself a square. There are other bases with this property, namely 2, 3, 4, 5, 8, and 16; students would be able to find them, though they might not be able to prove that they are the only such bases, which is in fact true.

Problems

2. .658, remainder $19\chi0$.
4. .6, 30/143.
10. (a) 265; 266 in leap years.
    (b) Only 260, 261, ..., 269.
    (c) No: if the number is abcd, then in base χ we have
    $1728a + 144b + 12c + d = 1000(a + 1) + 100b + 10c + d$, and
    this has no solution with a, b, c, and d one-digit integers.

SECTION 15

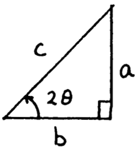
Problems

2. 3, 3, 6.
4. There are no such integers, because $(10, 42) \neq 1$ and $(10, 45) \neq 1$. But $10^7 \equiv 10 \pmod{42}$ and $10^2 \equiv 10 \pmod{45}$.
10. $.\overline{01}$, $.\overline{0011}$, $.\overline{000111}$.
12. $.\overline{0\varepsilon}$, $.\overline{0\chi35186}$.
14. If the decimal expansion of a number is neither terminating nor repeating, then the number is not rational. Thus .101001000100001... is irrational in any base, seven in particular.

SECTION 16

To a mind quick to see analogies, the expressions $m^2 - n^2$ and $2mn$ that occur in the parametric representation of the sides of Pythagorean triangles might suggest $\cos^2\theta - \sin^2\theta$ and $2\sin\theta\cos\theta$ and one might wonder if there might be a trigonometric derivation of the formulas. There is, and Olga Taussky published it in "Sums of squares" (American Mathematical Monthly 77 (1970) 805-

830). Define the acute angle 2θ by $\sin 2\theta = a/c$, $\cos 2\theta = b/c$, where a, b, and c are integers such that $a^2 + b^2 = c^2$. At least one of a and b is even, since if both were odd we would have $c^2 \equiv 2 \pmod 4$, impossible. We can suppose that a is even.



$$\sin^2\theta = \tfrac{1}{2}(1 + \cos 2\theta) = r,$$
$$\cos^2\theta = \tfrac{1}{2}(1 - \cos 2\theta) = s,$$
$$\sin\theta\cos\theta = \tfrac{1}{2}\sin 2\theta = t$$

are all rational, and $t = \sqrt{rs}$. Also,

$$\sin\theta = \sqrt{r} = (\sqrt{rs}/\sqrt{s}) = (t/s)\cos\theta .$$

Thus

$$(\sin^2\theta)/n^2 = (\cos^2\theta)/m^2.$$

But those quantities are equal, respectively, to r/n^2 and s/m^2 so they are both rational. Let the common rational value of the quantities in the last equation be k. Thus

$$\sin^2\theta = kn^2, \quad \cos^2\theta = km^2.$$

It follows that

$$a = c\sin 2\theta = c(2\sin\theta\cos\theta) = ck(2mn)$$
$$b = c\cos 2\theta = c(\cos^2\theta - \sin^2\theta)$$
$$= ck(m^2 - n^2).$$

There they are: all that remains is to show that ck is an integer. Suppose that $ck = u/v$ with $(u, v) = 1$. Then $av = u(2mn)$ and $bv = u(m^2 - n^2)$. Suppose that $p \mid v$. Then $p \mid 2mn$ and $p \mid (m^2 - n^2)$. If p is odd, then the first shows that $p \mid m$ or $p \mid n$ and in either case, the second shows that p divides both m and n, but this is impossible. If $p = 2$ and $p \mid n$ then $p \mid m$. Finally, if $p = 2$, $p \nmid n$ and $p \nmid m$, then a would be odd. That shows that no prime divides v, so $v = 1$ and ck is an integer.

The derivation is not as natural as the one in the text, but it is nice to know that the similarity of form is no accident.

A student who is bright and has caught on to how mathematicians think might ask, after $x^2 + y^2 = z^2$ is all settled, about $ax^2 + by^2 = cz^2$. Even if no one brings it up, it gives a chance for the teacher to bring it up and illustrate how when one question is settled others are suggested, so there is no danger of the world ever running out of mathematics. It also gives a chance to give the nice answer, proved by Legendre in 1785. If the equation is written in the symmetrical form $ax^2 + by^2 + cz^2 = 0$ where each of a, b, and c has no square factor, are relatively prime, and are not all positive or all negative, then the equation has solutions if and only if $-bc$, $-ac$, and $-ab$ are quadratic residues of a, b, and c respectively. In 1953 it was shown that if solutions exist, then there is one with $z < \sqrt{ab}$. Students can find hundreds of diophantine equations in the more than 800 pages of the second volume of L. E. Dickson's History of the Theory of Numbers (three volumes, Chelsea, New York, 1966 reprint of the 1919 edition), a fascinating book to browse through.

Problems

2. (96, 247, 265) and (264, 23, 265).
4. There are 13, with long sides 1104, 1100, 1092, 1073, 1071, 1020,

1001, 975, 952, 943, 884, 855, and 817.

8. It is not necessary to use the parametric representation of the sides, though that works: if $ab/2 = c$ then $a^2b^2 = 4c^2 = 4a^2 + 4b^2$. Solve for a^2: $a^2 = 4 + 16/(b^2 - 4)$. That implies $b^2 - 4 = -16, -8, -4, -2, -1, 1, 2, 4, 8$, or 16, all of which are impossible.

12. (a) 234.

    (b) Another has sides 33, 56, 63, 16, with one diagonal 65.

    (c) Yes: paste together Pythagorean triangles with the same hypotenuse. To see there are infinitely many, take $m \equiv 1$ and $n \equiv 2 \pmod 5$ so that c will be divisible by 5, say $c = 5k$. If a and b are the other sides of the fundamental triangle, then the quadrilateral with sides $a, b, 3k, 4k$ will have diagonal $5k$, integer sides, and area $3abk^2$.

14. From $mn(m^2 - n^2) = 3(2mn + (m^2 - n^2) + (m^2 + n^2))$ there follows $n(m - n) = 6$, so $(m, n) = (6, 7)$ or $(2, 5)$ and the triangles have sides $(84, 13, 85)$ and $(20, 21, 29)$.

16. If $(a - d)^2 + a^2 = (a + d)^2$, then $a(a - 4d) = 0$.

18. (a) (20, 21, 29) and (12, 35, 37) have area 210.

    (b) The triangles with generators 35, 11 and 33, 23 have the same area.

    (c) Let the sides of the two triangles be a, b, c and r, s, c. Then $a^2 + b^2 = r^2 + s^2$ and $ab = rs$. There follow $(a + b)^2 = (r + s)^2$ and $(a - b)^2 = (r - s)^2$ and these imply $a = r$ and $b = s$.

SECTION 17

Since this section has Fermat in its title, it is a good place to humanize him by pointing out that even he, like other mathematicians, could make mistakes. (Legendre once thought that he had proved Euclid's parallel postulate and he almost presented his proof in public, but at the last minute he had doubts. More recently, Kurt Mahler thought that he had proved that Euler's constant, $\lim_{n\to\infty} (-\ln n + 1 + 1/2 + 1/3 + \dots + 1/n)$ was irrational but he too had second thoughts.) Fermat was wrong about his proof that $x^n + y^n = z^n$ had no nontrivial solutions for $n \geq 3$ and he was wrong in saying that the Fermat numbers $F_n = 2^{2^n} + 1$ are prime for all n. F_n is prime for $n = 0, 1, 2, 3$, and 4, but Euler discovered F_5 was divisible by 641. F_n is also composite for $n = 6, 7, 8, \dots, 16$ and many larger values of n. The first Fermat number whose status is unknown is F_{17}. It is a large integer, with 39457 digits: 401...(39451 digits)...697. (The first three digits can be found from the logarithm of 2^{131072} and the last three by finding $2^{131072} \pmod{1000}$, using the fact that $2^{103} \equiv 2^3 \pmod{1000}$.) The factorization of F_7 was completed as recently as 1971 (M. A. Morrison and John Brillhart, "The factorization of F_7," Bulletin of the American Mathematical Society 77 (1971) 264), when it was shown that

$$\begin{aligned} 2^{128} + 1 &= 340282366920938463463374607431768211457 \\ &= (59649589127497217)(5704689200685129054721), \end{aligned}$$

both of the factors being primes.

The great lengths that people will go to to factor numbers are illustrated in "A method of factoring and the factorization of F_7," by Morrison and Brillhart, Mathematics of Computation 29 (1975) 183-205. It is pure puzzle-solving: the challenge is the number, just because it is there, and once it has been factored it ceases to have any interest. It is like a solved crossword puzzle, fit only for being thrown away; the fun is all in the doing.

The journal Mathematics of Computation often contains interesting number theory results. One can get the square root of 2 to 1,000,000 decimal places (Math. Comp. 25 (1971) 939), find that the smallest odd perfect number, if there is one, must be greater than 10^{50} (Math. Comp. 31 (1973) 1005), and be one of the first to know that there are seventeen primes in arithmetic progression. It is nice to read results that are immediately understandable.

It is no use looking for primes of the form $2^{3^n} + 1$, because Fermat primes are the only ones of the form $2^a + 1$. That is because if a has an odd divisor, $a = rs$ with s odd, then

$$2^a + 1 = 2^{rs} + 1 = (2^r + 1)(2^{r(s-1)} - 2^{r(s-2)} + \dots + 1)$$

and that is composite. So a must be a power of two, since those are the only numbers with no odd divisors.

Problems

2. Because it cannot be concluded that the denominators decrease in size.
4. If $3|x$, then $x = 3X$ and $9X^3 + y^3 = 3z^3$. Thus $3|y$, so $y = 3Y$ and $3X^3 + 9Y^3 = z^3$. But this gives $3|z$, $z = 3Z$, and $X^3 + 3Y^3 = 9Z^3$; the first step in the infinite descent.
6. No. Just as in Problem 4, p divides x, y, z, and w.
8. If two of x, y, and z are odd and the other even, the equation is impossible (mod 4). So, x, y, and z are all even. A similar argument shows that $x/2$, $y/2$, and $z/2$ are also all even, and so on.
10. The first equation can be shown to be impossible by infinite descent or by writing it as $y^2 = 1 + 1/(x^2 - 1)$, which implies that $x^2 - 1$ is 1 or -1, both impossible. In the second equation, x, y, and z must all be even.

SECTION 18

If a student wants a challenge, challenge him or her to copy the method of the text to get a theorem about the representation of integers as differences of two squares. There are no hard theorems to prove. First one can note that $x^2 - y^2 \equiv 0, 1,$ or $3 \pmod 4$ for any x and y, so a necessary condition for the representation is that $n \equiv 2 \pmod 4$. Second one can note that

$$(a^2 - b^2)(c^2 - d^2) = (ac \pm bd)^2 - (ad \pm bc)^2$$

so it is necessary only to investigate the representation of primes as differences of two squares. If p is an odd prime and

$$p = (a^2 - b^2) = (a + b)(a - b)$$

we can write

$$p = a + b$$
$$1 = a - b$$

and solve: $a = (p + 1)/2$ and $b = (p - 1)/2$. Thus all odd primes are representable as differences of two squares, and so all integers which are products of odd primes are representable. Every power of two greater than 2 is also representable because

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

However, 2 is not a difference of two squares. Thus the analogue is

> Theorem: n cannot be written as a difference of two squares if and only if the prime-power decomposition of n contains a prime congruent to 2 (mod 4) raised to the power 1.

Copying the text is not the only way to the theorem. It is also possible to note that if $n = (a + b)(a - b)$, then $r = a + b$, $s = a - b$ and it is impossible to solve those equations in integers when and only when n does not have two factors r and s of different parity. That is the case when and only when n is twice an odd number. That argument makes the theorem even more trivial than it was before, but the first proof was a nice example of analogy in action.

The book by Sierpinski cited in the References has a corollary to the main theorem of this section, namely

> A positive integer n is a hypotenuse of a Pythagorean triangle if and only if n has at least one prime divisor congruent to 1 (mod 4).

Every positive square would be a hypotenuse of a Pythagorean triangle if Pythagorean triangles with one side of zero length were allowed: the condition in the corollary guarantees that this does not happen.

There is a recent exposition of Waring's Problem in "Waring's Problem" by Charles Small, Mathematics Magazine 50 (1977) 12-15.

Problems

2. $2001 = 3 \cdot 23 \cdot 29$, $2002 = 2 \cdot 3 \cdot 7 \cdot 11 \cdot 13$, 2003, and $2004 = 2^2 \cdot 3 \cdot 167$ are not sums of two squares, but $2000 = 44^2 + 8^2 = 40^2 + 20^2$.
4. $58^2 + 33^2$ or $63^2 + 22^2$.
6. Anything except 3 or 6.
8. True: this is what Lemma 1 says.

SECTION 19

Saying that 11 is the sum of four squares because $11 = 3^2 + 2^2 + 2^2 + 0^2$ is slightly artificial, and a Pythagorean would insist that 11 is a sum of three squares, not four. It is natural to ask which integers are the sum of four squares of natural numbers, and the answer was conjectured by Descartes, though it was not proved (G. Pall, "On sums of squares," American Mathematical Monthly 40 (1933) 10-18) until much later. What is true is that all integers except $1, 3, 5, 9, 11, 17, 29, 41, 2^{2n+1}, 3\cdot 2^{2n+1}, 7\cdot 2^{2n+1}, n = 0, 1, 2, \ldots$ are sums of four squares of positive integers. It would be interesting to see how many of those students could discover, and if anyone would see the pattern of the last three.

It is not likely, but perhaps the discovery of one powerful mind makes up for the frustration of hundreds of ordinary minds. Or perhaps not. It could be argued either way: should teachers of mathematics do their best to make the largest number of student feel good about mathematics or should they concentrate on developing to the full the potential of those who have potential? The first, I think, right now: there is no shortage of mathematics or mathematicians and mathematical talent has a way of developing in spite of instruction--think of Galois. It would be interesting to see what students think, and it is a good topic for a refreshing 15-minute discussion. Students who have a hard time factoring 100 will have opinions and will not hesitate to give them.

Problems

Exponents and plus signs are extraneous here: $3^2 + 1^2 + 1^2$ will be denoted $(3, 1, 1)$.

2. $11 = (3, 1, 1)$, $13 = (3, 2) = (2, 2, 2, 1)$, $17 = (4, 1) = (3, 2, 2)$, $19 = (4, 1, 1, 1) = (3, 3, 1)$, $23 = (3, 3, 2, 1)$, $29 = (5, 2) = (4, 3, 2)$.
4. $(112, 63, 35, 21)$.
6. $3\cdot 197 = (17, 14, 9, 5)$.
8. Consider cases. If at least three of x, y, z, w are divisible by three, call the ones divisible by three x, y, z. If exactly two are divisible by three, let x be one of them and let y and z be the ones not divisible by three. If $y + z \not\equiv 0 \pmod 3$, change z to $-z$ and $x + y + z$ will be divisible by three. If at least three are not divisible by three, call them x, y, z; sign changing can be done, if necessary, to get $x + y + z \equiv 1 + 1 + 1 \equiv 0 \pmod 3$.
10. Since two of x, y, and z must be odd (otherwise the three numbers have a common factor of two), the right-hand side is $2 \pmod 4$, which is impossible.

SECTION 20

The book by C. D. Olds mentioned in the References shows how it is possible to find solutions to Fermat equations from continued fractions. It is written simply enough that undergraduates can understand it, but to get far enough to be able to solve Fermat equations takes some time: it is a project for a few spare days, not a few spare hours.

Examples such as the smallest solution to $x^2 - 61y^2 = 1$ in the text, or the smallest solution to $x^2 - 991y^2$, which is

$$x = 379516400906811930638014896080$$

$$y = 12055735790331359447442538767$$

illustrate that non-mathematical induction cannot be relied upon. To find solutions to the equation by trial, one would have to test so many values of y that the conclusion that the equation had no non-trivial solutions would be forced on any inductive scientist. If a computer could check 1,000,000 values of y each second, it would take in excess of 100 trillion years to find the smallest solution. The fact that the sun has risen each day for some billions of years can thus give us no confidence that it will rise tomorrow. But we still do feel that confidence. Non-mathematical induction is full of difficulties not found in mathematical induction.

Problems

2. $4 + 15^{\frac{1}{2}}$, $8 + 3\cdot 7^{\frac{1}{2}}$, $10 + 3\cdot 11^{\frac{1}{2}}$, $649 + 180\cdot 13^{\frac{1}{2}}$.

4. (4, 1) and (31, 8); (8, 3) and (127, 48); (10, 1) and (199, 20).

6. (x_k, y_k) is a solution where $(x_k + y_k) + y_k\cdot 3^{\frac{1}{2}} = (2 + 3^{\frac{1}{2}})^k$, $k = 1, 2, \ldots$

8. (a) m_k and n_k are generators for the triangle, and they can be determined from $m_k - n_k + n_k\cdot 2^{\frac{1}{2}} = (3 + 2\cdot 2^{\frac{1}{2}})^k$ for any k.

   (b) (3, 4, 5), (696, 697, 993).

10. (a) For the area of the triangle, see the answer to Problem 9.

    (b) $3((2a + 1)^2 - 4) = c^2$ is impossible (mod 4).

12. $x_1 + y_1N^{\frac{1}{2}} > 1$ and $1 = x_1^2 - Ny_1^2 = (x_1 + y_1N^{\frac{1}{2}})(x_1 - y_1N^{\frac{1}{2}})$.

14. Start with $x_{k+1} + y_{k+1}N^{\frac{1}{2}} = (x_k + y_kN^{\frac{1}{2}})(x_1 + y_1N^{\frac{1}{2}})$ which gives $x_{k+1} = x_1x_k + Ny_1y_k$ and $y_{k+1} = x_1y_k + y_1x_k$.

SECTION 21

One can have mystical experiences, almost, contemplating the properties of the primes. Euclid proved that there are infinitely many, the Prime Number Theorem (or Theorem 1 of this section) shows that they are scattered more and more thinly through the integers as the integers get larger, but they almost certainly continue to clump together so that no matter how far out we go, there are still twin primes--primes whose difference is two. Even more, there are infinitely often patches of primes as dense as they were back near the start of the sequence of integers, followed by long stretches with hardly any primes at all. The sequence of primes, though steadily weakening, constantly reasserts its youth at ever-increasing lengths only to fall back once again, for ever and ever. If that is not clear, it is because mystical experiences are well known for not being easily reduced to words.

The Prime Number Theorem says, roughly, that the probability that an integer whose size is around n is prime is $1/(\ln n)$. The factor table in Appendix C gives numerical evidence of this. For example, between 6000 and 7000 there are 117 primes and 1000 times $1/(\ln 6500)$ is close to 114. A student who remembers his or her statistics could run a chi-square test on the primes to see if they are behaving as they should.

Let $\approx$ stand for "behaves about the same as when things get big;" then the Prime Number Theorem says that $\pi(n) \approx n/(\ln n)$. Let p_n denote the nth prime. Then it follows from the Prime Number Theorem that $p_n \approx n \ln n$. To see this, note that $n = \pi(p_n)$, so $n \approx p_n/(\ln p_n)$. Take logarithms: $\ln n \approx \ln p_n - \ln \ln p_n \approx \ln p_n$ because the logarithm of a quantity is negligible with respect to the quantity when things get big. Substituting, we get

$$n \approx p_n/(\ln p_n) \approx p_n/(\ln n)$$

whence

$$p_n \approx n \ln n.$$

From this we can get the picturesque result that the sum of the reciprocals of the primes diverges:

$$\sum_{p \le x} \frac{1}{p} = \sum_{n=1}^{\pi(x)} \frac{1}{p_n} \approx \int_2^{\pi(x)} \frac{dr}{r \ln r} \approx \ln \ln \pi(x)$$

$$\approx \ln \ln x.$$

This compares with

$$\sum_{n \le x} \frac{1}{n} \approx \ln x;$$

if students thought that series diverged slowly, then they should change their minds. By the time x is 1,000,000, $\ln \ln x$ is only 2.6, and it will not get to 3 until $x = 528{,}491{,}312$. Anyone looking at $\ln \ln x$ would swear that it was constant, but it gets larger than any number sooner or later, though more likely later.

The probability that two integers whose difference is two are both prime ought to be $1/(\ln n)^2$, assuming that the primes are independently distributed through the odd integers, which they are not even though they behave as if they were. So, the number of twin primes up to n ought to be about $n/(\ln n)^2$ and the nth twin prime ought to be around $n(\ln n)^2$. Further, the sum of the reciprocals of the twin primes should be like

$$\sum \frac{1}{n(\ln n)^2}.$$

But that sum converges, since it behaves like

$$\int_2^{\infty} dr/r(\ln r)^2 = -1/(\ln r)\Big|_2^{\infty}.$$

It is true (and not just guessed, as above) that the series converges. Brun showed long ago that the nth twin prime is greater than $cn(\ln n)^2$ divided by $(\ln \ln n)^2$ for some constant c, and this implies that the sum of reciprocals converges. It is a shame that this theorem is true because if it were false and the series diverged, we would know that there were infinitely many twin primes since no series with only a finite number of terms in it can diverge. Even though it is almost certainly true that there are infinitely many twin primes, the proof has not yet been found.

We would expect not only prime twins but prime quadruplets like 11, 13, 17, 19; 101, 103, 107, 109; 5651, 5653, 5657, 5659 to appear forever, since the probability of such a quadruplet around n should be about $1/(\ln n)^4$. They get rare: between 900,000 and

1,000,000 one would expect to find only around

$$(100{,}000)(1/(\ln 950{,}000)^4) = 2.79\ldots .$$

They are, however, there: after finding 907391, 907393, 907397, 907399 I stopped looking for the other 1.79. There should be patches of integers with even higher densities of primes if the probabilistic argument does indicate true results.

The first proofs of the Prime Number Theorem depended on finding regions in the complex plane where the Riemann zeta function had no zeros. No undergraduate is going to grasp that proof, but a very good student might get something out of "A motivated account of an elementary proof of the prime number theorem," by Norman Levinson, American Mathematical Monthly 76 (1969) 225-245. "Elementary" in the title does not mean easy; it indicates only that there are no complex variables in the proof. Another interesting reference is "A history of the prime number theorem," by L. J. Goldstein, American Mathematical Monthly 80 (1973) 599-615; correction 80 (1973) 1115.

The Riemann zeta function is the subject of the Riemann Hypothesis, the most important unsolved mathematical problem because if it is true then many other things will follow from it. Hilbert has been quoted as saying that if he were raised from the dead, his first question would be "Is the Riemann Hypothesis true?" Let $s = \sigma + it$ be a complex variable, using the odd notation traditional in number theory. Then for $\sigma > 1$, the zeta function is

$$\zeta(s) = \sum_{n=1}^{\infty} 1/n^s.$$

Raising an integer to a complex power is done using $a^b = e^{b \ln a}$, so that $2^i = e^{i \ln 2} = \cos(\ln 2) + i \sin(\ln 2) = .769 + .640\, i$ to three places. It is curious that nice formulas exist for $\zeta(2k)$, k an integer-- $\zeta(2) = \pi^2/6$ and $\zeta(4) = \pi^4/90$ are the first two-- but there is nothing similar for odd integers. The series does not converge for $\sigma \leq 1$, but there is a function which agrees with the series definition when $\sigma > 1$ and which exists when $\sigma \leq 1$, so the domain of the zeta function does not have to be restricted to $\sigma > 1$. The Riemann Hypothesis is that all of the complex zeros of this extended zeta function lie on the line $\sigma = 1/2$. This has been checked for quite a few zeros and we can be sure that none of the first few million stray off the line. It is also known that if any zero does not lie on the line, then it is not very far away from it. Anyone who settles the Riemann hypothesis will have fame which will not die as long as humans care about prime numbers, but it may be that the hypothesis is forever undecidable: there may be a zero, light-years up the complex plane that is just a tiny bit off the line, and it is so far away that we will never be able to find it.

The first proofs of the Prime Number Theorem, by the way, were based on the fact that the zeta function is never zero on the line $\sigma = 1$.

Problems

2. To complete the induction amounts to showing that when $n \geq 1$, $(2n + 1)/(n + 1)\sqrt{n} > 2/\sqrt{n + 1}$. Squaring and simplifying shows that it is indeed true. The problem approaches the best possible result: if we use Stirling's formula, $n! \approx n^n e^{-n}\, 2\, n$, where $\approx$ means "behaves like" then

$$\binom{2n}{n} \approx \frac{2^{2n-1}}{n} \cdot \sqrt{\frac{2}{\pi}}\, .$$

4. p is a factor in the denominator and 2p is a factor in the numerator. 3p does not appear in the numerator since 3p > 2n.

SECTION 22

In spite of the fact that formulas are in general bad, there is evidently a great hunger for them, even among more or less professional mathematicians, because formulas for primes keep appearing in the literature. Almost all of them are absolutely useless and most are not even pretty. Nor do they contain many new ideas: Wilson's Theorem is all some of them have.

To get a formula for p_n, the nth prime, all you need is a representation of the characteristic function of the primes: $\chi(n) = 1$ if n is a prime and 0 otherwise. Given that, you have immediately a formula for $\pi(n)$: merely sum $\chi(n)$ from 2 to n. Given that, you can quickly get a formula for p_n: if ψ_k is the characteristic function of $\{1, 2, \ldots, k - 1\}$ then

$$p_k = 2 + \sum_{i=2}^{\infty} \psi_k(\pi(i)).$$

That may look impressive--lots of formulas look impressive--but it disguises nothing except simple counting as the example below shows. It is yet another example of how formulas can obscure ideas.

i	2	3	4	5	6	7	8	9	10	11
$\pi(i)$	1	2	2	3	3	4	4	4	4	5

$$11 = p_5 = 2 + \sum_{i=2}^{\infty} \psi_5(\pi(i))$$

the counting stops when $\pi(i) \geq 5$. A formula person might object that ψ_k is not sufficiently formula-like, but that can be remedied:

$$\psi_k(n) = 1 + \sum_{i=k-1}^{\infty} (-1)^{i+s(k)} \binom{n-1}{i}\binom{i-1}{k-2},$$

where $s(k) = (1 - (-1)^k)/2$.

Here are some examples of formulas for primes. Some of their authors may have had the idea they were making a serious contribution to mathematics. One author noted in 1950 that

$$\delta(m) \begin{Bmatrix} = 0, & m \text{ composite} \\ \neq 0, & m \text{ prime} \end{Bmatrix} = \prod_{j=1}^{m-1} \prod_{k=1}^{m-1} (jk - m).$$

Hence

$$\pi(n) = n - \frac{1}{2\pi}\int_0^{2\pi} \sum_{m=1}^{n} \cos(x\,\delta(m))\, dx,$$

because the integral of the cosine is 2π only when m is composite. Another author used Fermat's Theorem in 1969 to note that

$$\prod_{2 \le p \le \sqrt{n}} \frac{1 - \cos(2n^{p-1}\pi/p)}{1 - \cos(2\pi/p)} = \chi(n).$$

An author used Wilson's Theorem in 1964 to note that

$$\frac{\sin^2(\pi((n-1)!)^2/n)}{\sin^2(\pi/n)}$$

was another way to write $\chi(n)$. Yet another way was noted in 1975: if $n \ge 3$, then

$$\operatorname{sgn}\left(\frac{2(n-1)!}{n} - \left[\frac{2(n-1)!}{n}\right]\right) = \chi(n).$$

Wilson's Theorem again, by an author in 1972

$$\frac{1 - \cos((2k)!\pi/(2k+1))}{1 + \cos(\pi/(2k+1))} = \chi(2k+1).$$

I have others in my collection, but those are plenty.

The statement in the text that the longest known arithmetic progression of primes has 16 terms is no longer correct: in "Seventeen primes in arithmetic progression" Sol Weintraub announces (Mathematics of Computation 31 (1977) 1030) that the sequence $3430751869 + 87297210k$ is prime for $k = 0, 1, \ldots, 16$. Seventeen primes in arithmetic progression is a lot, but it is a long way from that to proving Erdös's conjecture that there exist arithmetic progressions of primes of any length. Erdös has offered \$3000 for a proof or disproof, but even an offer of \$3,000,000 might not elicit a solution.

V. Pratt in "Every prime has a succinct certificate" (SIAM Journal of Computing 4 (1975) 214-220) shows that there is a proof that p is prime that uses at most $4\log_2 p + 1$ lines. It is startling that such a theorem could be proved, but it has been, and it is even presentable to undergraduates.

SAMPLE TESTS

Now that the text is complete it is time for the final examination. A sample final follows, along with three sample hour examinations. They were given to a class of twenty in 1971; the class met for 50 minutes three times a week for 14 weeks. Besides covering Sections 1 to 20, each member of the class wrote ten computer programs. This took a good deal of time and energy and the students, not an exceptional group, may have learned less number theory than they would have with no programming.

Test 1 (after Section 5)

1. Find the solutions of $19x + 7y = 1$.
2. Prove or disprove: if $d|a$, $d|b$, and $d|c$, then $d^2|a(b, c)$.
3. Prove that if each exponent in the prime-power decomposition of n is divisible by three, then n is the cube of an integer.
4. Prove that $n^5 \equiv n \pmod 8$ for all odd positive integers n.
5. Find the solutions of $ax \equiv a^2 \pmod{a + 2}$.

Answers

1. $x = -4 - 7t$, $y = 11 + 19t$ for some integer t.

2. Since $d|b$ and $d|c$, $d|(b, c)$; since $(b, c) = rd$ and $a = sd$, $a(b, c) = rsd^2$ and the assertion is true.
3. $n = p_1^{3e_1}p_2^{3e_2}\dots p_k^{3e_k}$ is the cube of $p_1^{e_1}p_2^{e_2}\dots p_k^{e_k}$.
4. The result follows from the table (mod 8):

n	n^2	n^4	n^5
1	1	1	1
3	1	1	3
5	1	1	5
7	1	1	7

5. If a is odd, $(a, a + 2) = 1$, the congruence becomes $x \equiv a \pmod{a + 2}$, and the only solution is a. If a is even, $(a, a + 2) = 2$, the congruence becomes $x \equiv a$ (mod $(a + 2)/2$) and there are two solutions, a and $a - (a + 2)/2 = (a/2) + 1$.

Scores: high 100, low 64, average 83.

Test 2 (after Section 12)

1. Evaluate $\phi(\phi(1000))$, 3^{48} (mod 97), and $(51/67)$.
2. Give an example of
   (a) an integer without primitive roots
   (b) a function whose domain and range are in the set on integers which is not multiplicative.
3. (a) Find two primitive roots of 17.
   (b) Find an integer with order 4 (mod 17).
4. Suppose that $p \equiv 13 \pmod{20}$ is prime. Does $x^2 \equiv 5 \pmod{p}$ have a solution?
5. Suppose that a has order e (mod p) and $a \neq 1$. What is the least residue (mod p) of $1 + a + a^2 + \dots + a^{e-1}$?

Answers

1. 160. Use Euler's Criterion: $3^{48} \equiv (3/97) \equiv (97/3) \equiv (1/3) \equiv 1 \pmod{97}$. $(51/67) = (3/67)(17/67) = -(67/3)(67/17) = -1$.
2. (a) Any number not 1, 2, 4, an odd prime-power, or twice an odd prime-power will do.
   (b) Almost anything will do. For example, let $f(n) = 2$ for all n.
3. (a) Trial shows that 2 is not a primitive root of 17 but 3 is, and so all the primitive roots are the least residues of the odd powers of 3, namely 3, 10, 5, 11, 14, 7, 12, and 6. (b) Solve $x^2 \equiv -1 \equiv 16$.
4. $(5/p) = (p/5) = ((13 + 20k)/5) = (13/5) = (3/5) = (5/3) = (2/3) = -1$, so the congruence has no solution.
5. $0 \equiv a^e - 1 \equiv (a - 1)(1 + a + a^2 + \dots + a^{e-1}) \pmod{p}$. The first factor is not zero (mod p), so the second factor must be zero (mod p).

Scores: high 100, low 18, average 70.

Test 3 (after Section 20)

1. Give an example of a six-digit number n, $n > 0$, such that $n = x^2 + y^2$ is impossible for integers x and y.
2. Give an example of a Pythagorean triangle

(a) with hypotenuse 29
(b) with one leg 29.

3. In what base b is $141_b = 226_{b-2}$?

4. Watson said, "Look at these two hundred-digit numbers a and b and this 1600-digit number c. These seventeen pages of arithmetic show that $a^8 + b^8 = c^8$." Holmes said, after only a few seconds of thought, "Your calculations are in error." How did he know?

5. Find two solutions of $9x^2 - 2y^2 = 1$ with $x \geq 1$ and $y \geq 1$.

6. Find all x, y, and z in arithmetic progression such that $xy \neq 0$ and $x^2 + xy + y^2 = z^2$.

Answers

1. Any $n \equiv 3 \pmod 4$ will do.

2. (a) $m^2 + n^2 = 29$: take $m = 5$, $n = 2$. The legs are 20 and 21.
   (b) $m^2 - n^2 = 29$: take $m = 15$, $n = 14$. The other sides are 420 and 421.

3. Given is $b^2 + 4b + 1 = 2(b - 2)^2 + 2(b - 2) + 6$. The solution is $b = 9$.

4. $(a^2)^4 + (b^2)^4 = (c^2)^4$ is impossible.

5. Put $z = 3x$ and get the Fermat equation $z^2 - 2y^2 = 1$. The first three solutions are $(3, 2)$, $(17, 12)$, and $(99, 70)$, gotten by raising $3 + 2\sqrt{2}$ to powers 1, 2, and 3. The first and third give an integer value for x, and the first two solutions are $(x, y) = (1, 2)$ and $(33, 70)$.

4. Substitute $x = a - d$, $y = a$, $z = a + d$ and the equation reduces to $2a^2 - 5ad = 0$. That implies $2a = 5d$, so d is even, $d = 2D$, $a = 5D$, and $(x, y, z) = (3D, 5D, 7D)$.

Scores: high 100, lOw 38, average 76.

Final Examination

1. Give precise statements of
   (a) the Unique Factorization Theorem
   (b) Fermat's Theorem
   (c) the Quadratic Reciprocity Theorem.

2. (a) Write 1971 in the base 12.
   (b) Write 1971 in the base 2.
   (c) Find all solutions of $19x + 71y = 1971$.

3. (a) Does $x^2 \equiv 19 \pmod{71}$ have a solution?
   (b) Does $x^2 + y^2 = 1971$ have a solution?

4. Give an example of a diophantine equation, not a congruence, with
   (a) no solutions
   (b) exactly one solution
   (c) infinitely many solutions.

5. Find all solutions of
   (a) $d(pq) = 36$
   (b) $\phi(pq) = 36$
   (c) $\sigma(pq) = 36$,
   where p and q are distinct primes.

6. Prove or disprove: if a and b are not relatively prime and $(a, b) \mid (a, c)$, then b and c are not relatively prime.

7. Suppose that $z^2 = 2x^2 + 3y^2$ and $(x, y) = 1$. Show that x, y, and z are all odd.
8. Suppose that 2 is a primitive root of p. What is $\text{ind}_2(p - 1)$?
9. Let $s(x)$ denote the number of squares less than or equal to x. Prove that $s(x) = [\sqrt{x}]$.

Answers

1. These can be looked up.
2. (a) 1183.
   (b) 11110110011.
   (c) $x = 29 + 71t$, $y = 20 - 19t$.
3. (a) $(19/71) = -(71/19) = -(-5/19) = -(-1/19)(5/19) = (19/5)$ $= (4/5) = 1$, so there is a solution. (There are two: 27 and 44.)
   (b) No: $1971 \equiv 3 \pmod 4$ and it has 3 raised to an odd power in its prime-power decomposition.
4. There are many examples, of varying merit.
5. (a) $d(pq) = 4$ always.
   (b) $(p - 1)(q - 1) = 36$ implies $(p, q) = (37, 2), (19, 3), (7, 7), (3, 19)$, or $(2, 37)$.
   (c) $(p + 1)(q + 1) = 36$ implies $(p, q) = (11, 2), (5, 5)$, or $(2, 11)$.
6. The assertion is true. If $d = (a, b)$, then $d|a$ and $d|b$. If $f = (a, c)$, then $f|c$. $d|f$ and $f|c$ imply $d|c$ whence $d|(b, c)$.
7. If y is even, then x is odd and this implies $2x^2 + 3y^2 \equiv 2 \pmod 4$, which is impossible. Therefore y is odd.
   If x is even, then $2x^2 + 3y^2 \equiv 3 \pmod 4$ which also is impossible. Thus x and y are odd, and this shows that z is odd also.
8. $\text{ind}_2(p - 1) = a$ implies $2^a \equiv p - 1 \equiv -1 \pmod p$. Since 2 is a primitive root, $a = (p - 1)/2$.
9. Suppose that $0^2 < 1^2 < \dots < n^2 \leq x < (n + 1)^2$. Then $s(x) = n$. But $n \leq \sqrt{x} < n + 1$ and that says $n = [\sqrt{x}]$.

Scores: high 100, low 56, average 84.

SECTION 23

Since this section is a miscellany of problems, there follow five miscellaneous small problems.

1. A pastime which can become compulsive once you get into it is writing $n!$ as a product of integers between n and $2n$, inclusive. For example, $3! = 6$, $6! = 8 \cdot 9 \cdot 10$, $8! = 12 \cdot 14 \cdot 15 \cdot 16$, and $11! = 15 \cdot 16 \cdot 18 \cdot 20 \cdot 21 \cdot 22$. It is easy to find such representations when they exist and easy to see that they are impossible when they do not exist, and the transition from one integer to the next is so easy that it is hard to stop. Once 40 has been conquered--$40! = 42 \cdot 44 \cdot 45 \cdot 48 \cdot 49 \cdot 50 \cdot 51 \cdot 52 \cdot 54 \cdot 55 \cdot 56 \cdot 57 \cdot 58 \cdot 59 \cdot 60 \cdot 62 \cdot 63 \cdot 64 \cdot 65 \cdot 66 \cdot 68 \cdot 69 \cdot 72 \cdot 74 \cdot 80$--41 beckons.
2. $12 \cdot 42 = 21 \cdot 24$ and $46 \cdot 96 = 64 \cdot 69$. It is easy to find more such products.
3. It is striking, if you are struck by such things (and many people are not), that $9876/12345 = 4/5$. Can that happen in

any other base or is 10 really special?

4. Equalities like $224 = 2^5 + 2^7 + 4^3$, $264 = 2^5 + 6^3 + 4^2$, $332 = 3^4 + 3^5 + 2^3$, and $333 = 3^2 + 3^4 + 3^5$ seem fairly common, a computer could no doubt grind out as many as anyone would want, and some might be interesting.

5. It is amusing to see the small integer solutions to $x \mid (y + a)$ and $y \mid (x + b)$ for various a and b; which ones are picked influence how hard the system will be to solve.

Problems

4-6 will denote Problem 6 of Section 4, M-42 will denote Problem 42 of the Miscellaneous Problems, and A-2 will denote Problem 2 of Appendix A. The meaning of the other labels can be found by non-mathematical induction.

1-4. The result follows from the fact that d is odd, so $(d, 2) = 1$, $d \mid 2c$, and $d \mid 2b$.

1-6. Since $a \mid b$, $(a, b) = a$.

1-8. (a) Let $d = (a, b, c)$, $e = (a, b)$, and $f = (e, c)$: we want to prove that $d = f$. This can be done by showing that $d \mid f$ and $f \mid d$.

1-10. The last digit of 3^m is 9, and the last digit of $3^{4n} = 81^n$ is 1, so the last digit of $3^m \cdot 81^n$ will be 9.

2-2. (a) 23.
(b) $2 \mid (k! + 2)$, $3 \mid (k! + 3)$, ..., $k \mid (k! + k)$: at least $k - 1$ consecutive composites.

2-4. $a + b > p_n$ and none of the first n primes divides $a + b$ because $(a, b) = 1$.

3-2. 1 man, 5 women, and 14 children.

3-4. If a and b denote the number of eggs sold at 5 cents each by Anna and Barbara respectively, and c is the price in cents per egg that the remainder was sold for, then $5a + (30 - a)c = 5b + (40 - b)c$ and this can be rearranged to

$$5(a - b) = c(a - b) + 10c.$$

This is possible only for $c = 3$ and the amount each recieved was $2a + 90$. Since $1 \leq a \leq 29$, the minimum yield was 92¢.

4-2. False. For example, take $a = 1$, $b = 4$, and $m = 3$.

4-4. (a) 9876543210.
(b) 98763210.

4-10. $118050660 = 2^2 \cdot 3^2 \cdot 5 \cdot 7 \cdot 13 \cdot 7207$.

5-2. 6560.

5-4. To prove the second, for example, let $a = r/s$, $b = t/u$, and $c = (ru + st)/su$. Then $as \equiv r \pmod{m}$, $bu \equiv t \pmod{m}$, and $csu \equiv ru + st \pmod{m}$. Substitute:

$$csu \equiv (as)u + s(bu) \pmod{m};$$

since $(s, m) = (a, m) = 1$, $c \equiv a + b \pmod{m}$, and that was what was to be shown.

6-2. Put $a = 1$ to get $(p - 1)! \equiv -1 \pmod{p}$. Substitute that back to get $a^p(-1) \equiv a(p - 1) \pmod{p}$ and then cancel the -1.

6-4. (a) The quickest way is to note that $p \mid \binom{p}{n}$ for $n = 1, 2, \ldots, p - 1$ since the denominator of $p!/(n!(n - p)!)$ has no factor of p to cancel the p in the numerator.
(b) Adding

$1^p - 0^p \equiv 1,\ \ 2^p - 1^p \equiv 1,\ \ldots,\ a^p - (a-1)^p \equiv 1 \pmod{p}$ gives $a^p \equiv a \pmod{p}$.

6-6. In fact, $11^{341} - 11 \equiv 13 \pmod{341}$.

6-8. The least residues of $2, 4, 6, \ldots, 2(p-1) \pmod{p}$ are a permutation of $1, 2, 3, \ldots, p-1$. Thus

$$1^m + 2^m + \ldots + (p-1)^m \equiv 2^m + 4^m + \ldots + (2(p-1))^m$$
$$\equiv 2^m(\ 1^m + 2^m + \ldots + (p-1)^m\ ) \pmod{p},$$

so

$$(2^m - 1)(1^m + 2^m + \ldots + (p-1)^m) \equiv 0 \pmod{p};$$

since $2^m - 1 \not\equiv 0 \pmod{p}$, the result is proved.

6-10. $a^{(p-1)/n} \equiv (c^n)^{(p-1)/n} \equiv c^{p-1} \equiv 1 \pmod{p}$.

7-4. (a)

n	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$f(n)$	1	1	1	2	2	2	1	3	2	2	2	2	2	4

(b) The odd divisors are $1, p, \ldots, p^m$.

(c) $f(2^n p_1^{e_1} p_2^{e_2} \ldots p_k^{e_k}) = (e_1 + 1)(e_2 + 1)\ldots(e_k + 1)$.

8-2. If p^e and m are an amicable pair, then $\sigma((p^e - 1)/(p-1))$ $= \sigma(1 + p + \ldots + p^{e-1}) = \sigma(n) = \sigma(p^e)$.

8-6. None.

8-8. All a such that $2^a > (p+1)/2$.

8-10. If n is composite, then $\sigma(n) > n + 1$, so

$$\sigma(2^k(2^{k+1} - 1)) = \sigma(2^k)\sigma(2^{k+1} - 1) > (2^{k+1} - 1)\ 2^{k+1}.$$

8-12. $\sum_{d|m} d^{-1} = \sigma(m)/m$, so the sum is $m/\sigma(m) + n/\sigma(n) =$ $m/(m+n) + n/(m+n) = 1$.

8-14. (a) 1, 3, 5, 8, 15, 24, 40, 120; 1, 5, 8, 9, 40, 45, 72, 360.

(b) Integers that are products of distinct primes.

(c) 2^k.

(d) 6, 60, and 90 are the only such numbers less than 10^{12}.

9-2. $(n\,\phi(n))^{1/2} = (p^a p^{a-1}(p-1))^{1/2} = (p^{2a-1}(p-1))^{1/2}$. The integer in parentheses is not a square, since p appears in its prime-power decomposition to an odd power.

9-4. If n is composite, it has a divisor $a \le n^{1/2}$, and the $(n/a) - 1$ integers $a, 2a, \ldots, (n/a)a$ are not relatively prime to n. Thus $\phi(n) \le n - (n/a) \le n - n^{1/2}$.

9-6. $(dt, dm) = d$ if and only if $(t, m) = 1$, so there is a one-to-one correspondence between positive integers less than m and relatively prime to it and positive integers less than n whose greatest common divisor with n is d.

9-8. If $m = pM$ and $n = pN$ then $(M, N) = 1$,

$$\phi(mn) = \phi(p^2MN) = p(p-1)\phi(M)\phi(N),$$

and

$$\phi(m)\phi(n) = \phi(pM)\phi(pN) = (p-1)^2\phi(M)\phi(N).$$

Thus $\phi(mn) = (p/(p-1))\phi(m)\phi(n)$.

9-10. If $1 \le m \le n$ and $(m, n) = 1$, then $(n - m, n) = 1$. If $n > 2$, the integers less than n and prime to it can thus be arranged in $\phi(n)/2$ pairs so that the sum of each pair is n.

9-12. If $p > q$ and $a > 1$, then $p^{a-1}(p-1) = q^{b-1}(q-1) \Longrightarrow$

$p \mid (q - 1)$, which is impossible.

9-14. n can have only one prime factor, and $n = 1, 2, 4, p^k$, or $2p^k$ where $p \equiv 3 \pmod 4$ and k is a positive integer.

10-2. 1979 and 1982.

10-4. $2^5 \equiv 1 \pmod{31}$, so 2 has order 5.

10-6. If $(a, p) = 1$, then $a \equiv g^k \pmod p$ for some k, where g is a primitive root of p. Suppose that $x = g^y$. Then $g^{ny} \equiv g^k \pmod p$, and this holds if and only if $ny \equiv k \pmod{p - 1}$. Since $(n, p - 1) = 1$, there is exactly one solution y of this congruence.

10-8. Start with $(a^m)^n \equiv a^{mn} \pmod p$ and multiply successively by a^{-mn} and $(a^m)^{-n}$.

10-10. Let $\operatorname{ind}_g a = r$ and $\operatorname{ind}_g b = s$. Then $g^r \equiv a$ and $g^s \equiv b \pmod p$, so $ab \equiv g^{r+s} \pmod p$. But this says that $\operatorname{ind}_g ab \equiv r + s \pmod{p - 1}$, which was what was to be shown.

10-12. $x \equiv 10 \pmod{19}$.

10-14. If $2^r \equiv p - 1 \equiv -1 \pmod p$, then $2^{r+1} \equiv -2 \equiv p - 2$ and $2^{r+2} \equiv -4 \equiv p - 4 \pmod p$.

11-2. $x^2 \equiv 3 \pmod{11}$, $x^2 - x + 3 \equiv 0 \pmod{11}$, $x^2 + 3x + 2 \equiv 0 \pmod{11}$.

11-4. 1, 1, 1, -1, -1, -1.

11-6. (a) Four: 1, 7, 9, and 15.
(b) No: 16 is not an odd prime.

11-8. If $p = 5$, $i = 2$, and $a + 2b \equiv 0 \pmod 5$ is satisfied by $a = 3$, $b = 2$.

11-10. Yes. The proof is the same as in Problem 20 of Section 11.

12-2. (a) $n^2 + 2an + b = (n + a)^2 + b - a^2$ so if $n^2 + 2an + b$ is divisible by p, then $a^2 - b$ is a quadratic residue of p.

12-4. (a) $(-3/p) = (-1/p)(3/p)$: apply Problem 1 of Section 12.
(b) Let s be the unique solution of $2s \equiv r \pmod p$. If $x^2 + xr + r^2 \equiv 0 \pmod p$ then $0 \equiv x^2 + 2sx + 4s^2 \equiv (x + s)^2 + 3s^2 \pmod p$, so $(-3s^2/p) = (-3/p) = 1$, and this holds for $p \equiv 1$ or $7 \pmod{12}$.

13-2. $b(b + 1)(b + 2) + 1$ if b is odd, and $b(b + 1)(b + 2)/2 + 1$ if b is even.

13-4. If $b^2 + b + 1 = n^2$, then $4n^2 - 3 = (2b + 1)^2 = s^2$ is a square, and $(2n - s)(2n + s) = 3$ implies $n^2 = 1$.

14-2. If $p \geq 5$, its last duodecimal digit is 1, 5, 7, or ε.

14-4. (b) $(b - 1) \mid (n - m)$ because $b^r - b^s$ is always divisible by $b - 1$.

15-2.

n	2	3	4	5	6	7	8	9	A	B	C
1/n	.8	$.\overline{5}$	.4	$.\overline{3}$	$.2\overline{A}$	$.\overline{249}$	.2	$.\overline{1C7}$	$.1\overline{9}$	$.\overline{1745D}$	$.1\overline{5}$

n	D	E	F
1/n	$.\overline{13B}$	$.1\overline{249}$	$.\overline{1}$

15-4. Yes. No: $1/2 = 2/2^2 = 8/4^2$.

16-2. (a) If a is even, put $a = 2mn$ and $b = m^2 - n^2$. If a is odd, put $a = m^2 - n^2$, $b = 2mn$.

17-4. $x^p \equiv x$, $y^p \equiv y$, $z^p \equiv z \pmod p$.

17-6. If one, two, or all three of x, y, and z are odd, then the left-hand side of the equation is odd.

17-8. $x = y = z = 2$ is one solution. $x = y = 2^{16}$, $z = 2^{13}$ is a solution derived from Problem 7 with $a = b = 1$, $r = 4$, and $s = 13$.

17-10. As in Problem 9, put $rn^2 + 1 = ms$. This has solutions if $(n^2, m) = 1$.

18-2. Any square congruent to 0, 1, or 4 $\pmod 8$.

18-4. 37, 149, ... are missed.

18-6. Take x so that $n - x^2 = m$ is odd and positive. Then let $y = (m + 1)/2$.

18-8. If $n = (a/c)^2 + (b/c)^2$, then $c^2n = a^2 + b^2$, and c^2n is representable if and only if n is. The answer is, "The same integers as in Theorem 1."

18-10. The generalization is false: $(-5/3) = 1$, but $x^2 + 5y^2 = 3$ is impossible.

19-2. The theorem is that the number of representations of n, where the representations which differ only in order or sign are counted as distinct, is eight times the sum of divisors of n which are not multiples of 4.

20-4. The values are 2 and -2.

M-2. $(n - 1)^3 + n^3 + (n + 1)^3 = 3n(n^2 + 2)$: if $3 \nmid n$, then $n^2 + 2 \equiv 0 \pmod 3$.

M-6. $n = 3$, 4, or 5.

M-8. $2^a \equiv 5$ or $6 \pmod 7$ for any n.

M-10. (a) 9.

(b) 90.

(c) If $k = 2n$, there are $9 \cdot 10^{n-1}$; if $k = 2n - 1$, there are $9 \cdot 10^{n-1}$.

M-12. (g) and (h).

M-14. $a^4 + b^4 + (a + b)^4 = 2(a^2 + ab + b^2)^2$.

M-18.

$$n \sum_{d|n} (1/d) = \sum_{d|n} (n/d) = \sum_{d|n} d = \sigma(n).$$

M-24. $x \equiv -1$, $y \equiv 2 \pmod m$.

M-26. Those with sides 3, 4, 5, 6, 8, 10, 12, 15, 16, 17, 20, 24, 30, 32, and 34.

M-28. $k = (x^2 - 1)/8 + (y^2 - 1)/8 + (z^2 - 1)/8$, and each of the summands is a triangular number.

M-30. Yes: $(a + (b/c))^{\frac{1}{2}} = a + (b/c)^{\frac{1}{2}}$ if and only if $b/c = a + a/(a^2 - 1)$.

M-32. $3 | (p^2 + 2)$.

M-34. (a) If $3p + 1 = a^2$, then $3p = (a + 1)(a - 1)$ and $p = 5$.

(b) If $3p + 2 = a^2$, then $a^2 \equiv 2 \pmod 3$, which is impossible.

M-36. The Rational Root Theorem says that if r/s is a root of $a_nx^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0 = 0$, then $r|a_0$ and $s|a_n$. So, if r/s is a root of $a^2 + b^2 = 2(a + b)x + x^2$, then $r|(a^2 + b^2)$ and $s|1$. Note that if x^2 is rational and $a + b \neq 0$, then $x = (a^2 + b^2 - x^2)/(2(a + b))$ is a rational number. If $a + b = 0$, then $x^2 = a^2 + b^2$ is rational.

M-38. No. It neither repeats nor terminates.

M-40. No. Yes. $10^n \equiv 28 \pmod{36}$, $n = 2, 3, \ldots$.

M-42. $ka \equiv k + 1 \pmod{p}$, so $(k + 1)^k \equiv (ka)^k \equiv k^ka^k \equiv k^kk \pmod{p}$.

M-46. $(x, y) = (4s, -3s)$ for any s. $x^2 + y^2 > ((x + y)/2)^2$.

M-44. If r is the smallest integer such that $[x] < x + (r/n)$, then the sum of $[x + (k/n)]$ for $k = 0$ to $k = n - 1$ is $r[x] + (n - r)([x] + 1) = n[x] - r$. On the other hand, $n[x] < nx + r$ so $[nx] = n[x] - r$, the same value as the sum.

M-48. The equation becomes $a^2 + b^2 + c^2 = 2abc$ which can be shown to be impossible by infinite descent.

M-50. $20413 = 137 \cdot 149$, so the loan was for \$137, 7 years ago, at 7%.

M-52. Sixteen solutions are given by $(x, y) = (2, -3)$, $(3, -6)$, $(4, -12)$, $(5, -30)$, $(7, 42)$, $(8, 24)$, $(9, 18)$, $(10, 15)$ and their reversals. The seventeenth is $(12, 12)$.

M-54. The first of a pair of twin primes is congruent to $-1 \pmod{6}$.

M-56. The equation can be turned into $2km^2 - 1 = (2n + 1)^2$.

M-60. If $p|a_i$ and $p|a_j$, then $p|(i - j)P_n$. Since $|i - j| < n < p_n$, p must be one of $p_1, p_2, \ldots, p_n$. But none of those primes divide a_i or a_j.

M-62. (a) $7^n \equiv 1 + 6n \pmod{36}$: use mathematical induction or expand $(1 + 6)^n$.

(b) $7^n \equiv 18n^2 - 12n + 1 \pmod{216}$.

M-64. The number is $2^{27} - 1$ and 27 is composite.

M-66. (a) No: at least one corner will have two even coordinates.

(b) The one nearest the origin has corners $(14, 20)$, $(14, 21)$, $(15, 20)$, and $(15, 21)$.

(c) The bottom line is all dotted except at (p, p). The top line has $\phi(p + 1)$ dots. The first, at $(1, p + 1)$ gives one three-dot box. Each of the next $\phi(p + 1) - 2$ give two three-dot boxes. The last, at $(p, p + 1)$ gives none since the last box has only two dots. The total number of three-dot boxes is thus $1 + 2(\phi(p + 1) - 2) = 2\phi(p + 1) - 3$.

M-68. Consider $n \equiv 0, 1, 2, \ldots, 23 \pmod{24}$.

M-70. If $kp + b = m^2$, then $m^2 \equiv b \equiv c^2 \pmod{p}$, so $m \equiv c$ or $-c \pmod{p}$. That is, for some integer n, $m = c + np$ or $-c + np$.

M-72. $10^{3^{n+1}} = (10^{3^n} - 1)(10^{2\cdot 3^n} + 10^{3^n} + 1)$.

M-74 (a) $m = 4n(n + 1)$.

(b) Yes: $m = (4n + 3)^2 \cdot n$.

M-78. $n + (n + 1) + \ldots + (n + d) = (2n + d)(d + 1)/2$, and this always has an odd factor.

M-80. Its last digit is 3.

M-84. If $n = d_0 + d_1 \cdot 10 + d_2 \cdot 10^2 + \ldots$, $0 \leq d_i \leq 9$, then $37|n$ if and only if $37|(d_0d_1d_2) + (d_3d_4d_5) + \ldots$.

M-86. (c) $ab((a + b)/2)((a - b)/2) = (c/2)^2$.

M-88. (a) $4n^2 - 3n + 1$.

(b) $4n^2 - 2n + 1$.

(c) $4n^2 + n + 1$.

(d) $(n, -n)$.

(e) $(-n + 1, n)$.

(f) $(9, 16)$.

M-90. (a) Put $y = x + d$, $z = x + 2d$. Then $(d + x)(3d - 2x) = 0$, so $(x, y, z) = (3t, 5t, 7t)$, t an integer.

(b) With x and y as in (a), $(d + x)(3d - (k + 1)x) = 0$. If $k \not\equiv 2 \pmod 3$, then $(x, y, z) = (3t, (k + 4)t, (2k + 5)t)$; if $k \equiv 2 \pmod 3$, then $(x, y, z) = (t, (k + 4)t, (2k + 5)t)$ for nonzero integers t.

M-92. (b) If $n \equiv 1 \pmod 3$, then $3|p^r$, so $p = 3$. But $n \equiv 1, 4$, or $7 \pmod 9$, so $n^2 + n + 1 \equiv 3 \pmod 9$. Hence $r = n = 1$.

(c) If $r = 2k$, then $(2n + 1)^2 - (2p^k)^2 = 3$. Factor the left-hand side.

(d) Suppose that $p \neq 3$ and $p \equiv 2 \pmod 3$. Since r is odd, $p^r \equiv 2 \pmod 3$. Moreover, $n^2 + n + 1 \equiv 1 \pmod 3$.

M-94. (a) If $x^n \equiv a \pmod p$, then $1 \equiv x^{p-1} \equiv (x^n)^{(p-1)/n} \equiv a^{(p-1)/n} \pmod p$.

(b) No: $2^6 \equiv 2 \pmod{31}$.

M-96. (a) The equation is $(2n + 1)^2 = 6m^2 - 1$, but no square is congruent to $-1 \pmod 6$.

(b) $(2n + 1)^2 \equiv -1 \pmod{2k}$ must have a solution.

M-98. (a) $x^2 = 10^n rs + x$.

(b) $r = 78$ and $s = 5$ give $x = 625$, $x^2 = 390625$.

M-100. Solutions are

x	10	10	14	14	17	17	21	21	31	36	44	105
y	6	35	7	34	7	34	6	35	41	45	52	111.

A-2. $1^3 + 2^3 + \ldots + n^3 = (n(n + 1)/2)^2$.

A-10. $1^2 + 4^2 + \ldots + (3n + 1)^2 = (n + 1)(6n^2 + 9n + 2)/2$.

A-12. $f(n) = 17(n - 1)(n - 2)(n - 3)(n - 4)/24$ is one of infinitely many such functions.

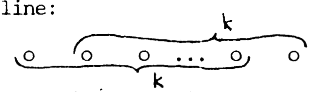
APPENDIX A

It can be argued that proof by mathematical induction ought to start the text since it is such an important method of proof. The reason it does not is that students have such a hard time grasping the idea that it might get the class off to a bad start; once the morale of a class is shattered it is hard to get it back together. But if a class can take the shock, by all means start with induction and use it at every opportunity.

To see if a class has really gotten the point, it can be given the problem of deciding where the flaw is in the well-known proof that everyone has the same sex. This was left out of the text on account of the confusion it might cause in the minds of students who have not grasped induction.

Theorem: In a group of n people, all have the same sex.

Proof: The theorem is trivially true for $n = 1$. Suppose that it is true for $n = k$. Given a group of $k + 1$ people, arrange them in a line:

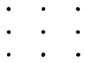


By the induction assumption, the first k people all have the same sex. Similarly, so do the last k. Hence, because of the overlap, all have the same sex.

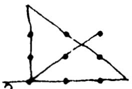
The flaw is so obvious that it is hard to understand why it is not seen immediately, but many students will not see that the proof does not work when $k = 1$.

Problems

2. $1^3 + 2^3 + \dots + n^3 = (n(n + 1)/2)^2$.
4. It is not likely that anyone will note that $1/(1\cdot 2) = (1/1) - (1/2)$, $1/(2\cdot 3) = (1/2) - (1/3)$, ..., so that the series becomes
   $1 - 1/2 + 1/2 - 1/3 + 1/3 - 1/4 + \dots + 1/(n - 1) - 1/n$
   $= 1 - 1/n$.
   It is not likely because the problem comes at the end of a section on mathematical induction and hence all proofs must use that method. If any student does hit upon the telescoping series idea, he or she should be praised for not having a mind confined with self-imposed limitations. He or she should also be able to solve the well-known puzzle about connecting the nine dots



with four lines



10. $1^2 + 4^2 + \dots + (3n + 1)^2 = (n + 1)(6n^2 + 9n + 2)/2$.
12. Some students are delighted with the method for constructing a polynomial passing through given points by making a difference table. For example,

x	$f(x)$	$\Delta f(x)$	$\Delta^2 f(x)$	$\Delta^3 f(x)$
0	2	2	2	3
1	4	4	5	
2	8	9		
3	17			

$$\text{gives } f(x) = 2 + 2(x - 0) + (1/2!)2(x - 0)(x - 1) + (1/3!)3(x - 0)(x - 1)(x - 2) = (x^3 - x^2 + 4x + 4)/2.$$

If that example did not make the general method clear, here is another:

x	$f(x)$	$\Delta f(x)$	$\Delta^2 f(x)$
2	8	-4	2
3	4	-2	
4	22		

$f(x) = 8 - 4(x - 2) + (1/2!)2(x - 2)(x - 3) = x^2 - 9x + 22$. It gives a sense of power, being able to find a formula for any collection of points. If any student wants to know why the process works, he or she can be told that is a consequence of the binomial expansion, first found by Newton, and its derivation can be found in any book on finite differences or numerical analysis.