DOCUMENT RESUME

ED 143 524 SE 023 002

TITLE	Essays on Number Theory II.
INSTITUTION	Stanford Univ., Calif. School Mathematics Study Group.
SPONS AGENCY	National Science Foundation, Washington, D.C.
PUB DATE	60
NOTE	77p.; For related document, see SE 023 001; Contains occasional light and broken type
EDRS PRICE	MF-$0.83 HC-$4.67 Plus Postage.
DESCRIPTORS	Algebra; *Instructional Materials; *Number Concepts; Secondary Education; *Secondary School Mathematics
IDENTIFIERS	*School Mathematics Study Group

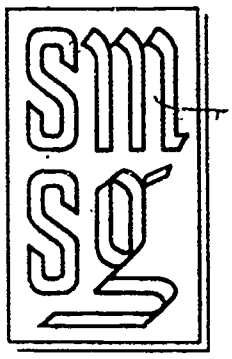
ABSTRACT

This supplement was written for students who are especially good in mathematics and who have a lively interest in the subject. It is suggested that the supplement be read with pencil and paper in hand. All questions should be considered and answered, if possible, when they occur. A casual reading of the supplement is, in most cases, unprofitable. For the most part, the units are independent of each other. Some of the sections in this publication relate to the chapters of the eleventh-grade material of SMSG Intermediate Mathematics. Included in this supplement are suggestions for use of the materials and eight chapters on arithmetic functions, the Euclidean algorithm and linear diophantine equations, the Gaussian integers, Fermat's Method of Infinite Descent, and approximation of irrationals by rationals. (RH)

SCHOOL
MATHEMATICS
STUDY GROUP

ESSAYS ON NUMBER THEORY II

SMSG



SCHOOL MATHEMATICS STUDY GROUP

ESSAYS ON NUMBER THEORY II

Written for the SCHOOL MATHEMATICS STUDY GROUP
Under a grant from the NATIONAL SCIENCE FOUNDATION

Financial support for the School Mathematics Study Group has been provided by the National Science Foundation.

PHOTOLITHOPRINTED BY CUSHING - MALLOY INC.
ANN ARBOR MICHIGAN UNITED STATES OF AMERICA

CONTENTS

* * *

Preface

This volume contains the eight chapters:

(1) Arithmetic Functions - I - The Number of Divisors of an Integer

(2) Arithmetic Functions - II - The Sum of the Divisors of an Integer

(3) Arithmetic Functions - III - The Distribution of Primes and the Function $\pi(n)$

(4) The Euclidean Algorithm and Linear Diophantine Equations

(5) The Gaussian Integers

(6) Fermat's Method of Infinite Descent

(7) Approximation of Irrationals by Rationals

(8) A New Field

These supplements were written for students who are especially good in mathematics and who have a lively interest in the subject. The author's aim in (1) and (2) is to lead the reader to discover for himself some interesting results and to experience the thrill of mathematical discovery. The others are more expository in nature, but they contain exercises to clarify the material and to give the reader a chance to work with the concepts which are introduced. It is suggested that the supplements be read with pencil and paper at hand. All questions should be pondered and answered, if possible when they occur. A casual reading of these supplements is, in most cases, unprofitable, and in some cases impossible.

Answers have been provided. However, it is suggested that these answers should not be consulted until the reader has finished working through the unit or until he reaches a point where he needs an answer in order to proceed.

For the most part the units are independent of each other. However, some have somewhat tenuous ties with certain chapters of the 11th grade material of the SMSG, (Intermediate Mathematics).

In particular, Sections (1) and (2) may be used at any time after the student has completed Chapter 3 of Intermediate Mathematics. While they are independent, Section (2) is easier and more meaningful if Section (1) has been done previously.

Section (3) may be read also after Chapter 3 of Intermediate Mathematics. However, on the last page logarithms are mentioned and for this reason it may be more useful after Chapter 8 of Intermediate Mathematics. (logarithms and exponents).

Section (4) may be used at any time after Chapter 2 of Intermediate Mathematics (in which linear equations are discussed).

Section (5) is designed to follow Chapter 5 on complex numbers and also to pave the way for the section entitled "A New Field".

Section (6) naturally follows Chapter 9 on induction.

Section (8) assumes familiarity with Chapters 5 and 15 of Intermediate Mathematics.

Suggestions for further reading are:

The Enjoyment of Mathematics by Hans Rademacher and Otto Toeplitz, Princeton University Press, Princeton, 1957.

What Is Mathematics? by Courant and Robbins, Oxford, New York, 1941.

Number Theory and Its History by Ø. Ore, McGraw-Hill, New York, 1948.

1.

ARITHMETIC FUNCTIONS.

Leopold Kronecker, one of the great mathematicians of the nineteenth century is supposed to have said in an after dinner speech "God made the integers; all the rest is the work of man." The basic role of the integers in the development of the real number system lends some weight to Kronecker's statement. In your work with functions the domain of definition of the function has usually been the set of real numbers or some subset of this set. There are many interesting functions, however, which have for their domain of definition the set of positive integers. Such functions are called arithmetic functions. In the units which follow we will consider several arithmetic functions which prove useful in stating and answering many questions about integers.

I

THE NUMBER OF DIVISORS OF AN INTEGER

Some people from time to time advocate changing the base of our number system from ten to twelve. To say that our numbers are written in the base ten means that we interpret a symbol like 312 to stand for

$$3 \cdot 10^2 + 1 \cdot 10 + 2.$$

If we were using the base six then 312 would stand for

$$3 \cdot 6^2 + 1 \cdot 6 + 2 ,$$

which would be 116 in the base ten.
In any number base, b , we would need b symbols for the numbers 0, 1, 2, . . . , b-1 .
In particular if we used the base twelve we would need two new symbols, say t and e for 10 and 11.
Then 312 in the base twelve would represent

$$3 \cdot 12^2 + 1 \cdot 12 + 2$$

or 446 in the base ten.
The symbol 4et21 would represent

$$4 \cdot 12^4 + 11 \cdot 12^3 + 10 \cdot 12^2 + 2 \cdot 12 + 1 ,$$

which would be 10347 in the base ten.
The claim is made that the base twelve would make arithmetic easier. The fractions 1/3, 1/4, 1/6, and 1/12 instead of having representations .333 ... , .25, .166. . . , and .083 . . . would have the simple form .4, .3, .2, and .1 .
Whatever the merits of this proposal, it seems unlikely to be adopted. However, it does suggest an interesting mathematical problem. Suppose we wanted to find a number with a large number of divisors, but which was not too large to serve as a base for system of numbers. The advantage would be that the more divisors the number has, the more fractions would have convenient finite representations. As a start we might make a table for the first few integers.

Integer	Divisors	Number of Divisors
1	1	1
2	1, 2	2
3	1, 3	2
4	1, 2, 4	3
5	1, 5	2

Extend this table for all the integers up through 30.

Which number in the table has the smallest number of divisors? If we extend our table will we ever encounter another integer with this number of divisors? Why not?

Make a list of the numbers in the table with two divisors. The numbers in this list are given a special name; they are called prime numbers.

Now list the numbers with three divisors. Do you notice any property which they have in common besides that of having the same number of divisors? Are there other numbers in the table with this property? Try to state a theorem about all the numbers with three divisors.

How many numbers in the list have an even number of divisors? Which numbers do not have an even number of divisors? Check this list with your theorem. Can you guess how many numbers less than fifty/have an even number of divisors? Less than 101?

Which numbers in your table have a prime number of divisors? Do you notice any other property that these numbers have in common? Could you make a guess about the form of a number with a prime number of divisors. How many divisors does 8 have? 32? 27? 64? 2^n? 3^n? See if you can devise a theorem which states exactly when the number of divisors is a prime.

Make another table showing the number of times each integer appears in the number of divisors column of your first table. That is, how many integers up to thirty have one divisor, two divisors, three divisors, etc. We can see from this new table that most of the numbers up through thirty seem to have an even number of

divisors. One of the distinguishing traits of a mathematician is his tendency to generalize his results. This means that once he has solved a particular problem, he begins to think of a large class of similar problems. This tendency to try to see the original problem as a special case of a much larger problem is one difference between a mathematician and a person who likes to solve problems. In the light of the information we now have about the divisors of numbers, see if you can generalize your theorem about the numbers which have three divisors.

The starting point for our discussion was the problem of finding a number base which was not too large, but which had many divisors. From this point of view ten has as many divisors as any other number up to ten. However, the restriction that the number not be too large was designed to keep the arithmetic simple. The smaller the base the easier the addition and multiplication tables are to learn. Taking into account both of these things, six would seem to be a better choice than ten. It would then be unnecessary to learn such troublesome parts of the multiplication table as 7×9, 9×6, etc. Unfortunately, for this base there are also disadvantages. Large numbers would require many more digits in their representation than they require in the base ten. So we are forced to conclude that ten isn't really such a bad number base after all.

Suppose we pursue our aim of finding a number with a large number of divisors, even if it isn't the most practical number base. Which number up through thirty has the largest number of divisors? Up to fifty are there any numbers with nine divisors? Ten divisors? More than ten divisors?

Of the numbers less than 100, which one has the greatest number of divisors?

If you have an answer to the last question, you are probably in a good position to devise a formula for the number of divisors of any particular integer n. (If not, try to consider some special cases. For example, we know how many divisors any prime has. How many divisors does p^k, a power of a prime, have?) The usual notation for the number of divisors of n is $\tau(n)$, where τ is the Greek letter tau. Try to write out an explicit expression for $\tau(n)$.

If you are having trouble actually writing down the expression, you are probably being handicapped by a lack of a suitable notation. While this has nothing to do with the idea which enables you to determine the number of divisors for any particular integer, devising a suitable notation turns out to be of great importance in many parts of mathematics. Lack of a suitable notation for numbers is thought by many to explain the Greek preference for geometry and the relatively small amount of arithmetic and algebra they were able to develop. Perhaps if you write n in the form $n = p_1^{m_1} p_2^{m_2} \ldots p_r^{m_r}$, where the p's are the distinct prime divisors of n and the m's tell you how many times the prime is a factor of n, you will find this notation helpful in writing our your expression for $\tau(n)$.

Find all the numbers less than 100 which have six divisors.

Find the smallest positive integer with fifteen divisors.

Find all primes that are one less than a perfect square. One less than a perfect cube. One less than a fourth power. How many primes are one less than a k^{th} power? Why?

2.

ARITHMETIC FUNCTIONS

II

THE SUM OF THE DIVISORS OF AN INTEGER

"In the beginning God created the heavens and the earth." The Genesis account of creation goes on to tell how God labored for six days, and on the seventh day He rested. As early as the sixth century B. C. the Pythagorean brotherhood classified integers into deficient, abundant, and perfect numbers according to whether the sum of the proper divisors of the integer was less than, greater than, or equal to the integer itself. Proper here means that the integer itself is not counted as one of its divisors. Thus the fact that 6 and 28 were perfect numbers, that is, $6 = 1 + 2 + 3$ and $28 = 1 + 2 + 4 + 7 + 14$, gave them a special significance. The ancients saw in the number six a symbol of the perfection of the creation. The discovery that the phases of the moon repeat every 28 days may also have had a part in the designation of these as perfect numbers.

Can you find any other perfect numbers?

Euclid includes in his ELEMENTS a rule for obtaining even perfect numbers. Before we consider Euclid's rule, let us take a detour and consider the problem of finding the sum of the divisors of a number. The sum of the divisors of an integer is an arithmetic function, that is a function defined over the positive intergers. We first note that the sum of the divisors is equal to the sum of the proper divisors and the number itself. The usual notation for the sum of the divisors of n is $\sigma(n)$ where σ is the Greek letter sigma. To try to find a formula for $\sigma(n)$ directly is not too easy. However, we can use the approach of the experimental scientist and collect some data. Suppose we make a table for $\sigma(n)$.

n	Divisors of n	$\sigma(n)$
1	1	1
2	1, 2	3
3	1, 3	4
4	1, 2, 4	7
5	1, 5	6

Extend the table for all n less than 31.

In our notation a number P is perfect if $\sigma(P) = 2P$. Mark the integers which are deficient with a D, those which are abundant with A, and those which are perfect with P.

How many of each kind are there in your table?

You probably have already noticed that the easiest numbers for which to compute $\sigma(n)$ were the primes. (A prime is a number which has exactly two divisors.)

Complete the following theorem: If p is a prime, $\sigma(p) =$ _____

The easiest case after that of the prime is probably that of an integer which is a power of a prime.

What are the divisors of p^k? Can you find the sum of $\sigma(p^k)$? (HINT: $x^{r+1} - 1 = (x - 1)(x^r + x^{r-1} + \ldots + x + 1)$. To prove this simply multiply out the right hand side.)

Now suppose that $n = p^k q$ where both p and q are primes. What are the divisors of n? How many are there? What is their sum?

Now suppose $n = p^k q^2$. What are the divisors of n? How many are there? What is their sum?

If $n = p^k q^s$, can you guess what $\sigma(n)$ is in this case? Check your answer in a few cases and see if you can prove it.

Now it shouldn't be too hard to devise a formula for $\sigma(n)$ for any n, provided we write n in the form $n = p_1^{m_1} p_2^{m_2} \ldots p_r^{m_r}$ where the p's are distinct primes and the m's tell us how many times the prime is a factor of n.

Use your formula to compute $\sigma(6)$, $\sigma(12)$, $\sigma(18)$, $\sigma(24)$, $\sigma(28)$, $\sigma(30)$, $\sigma(144)$.

From your table of $\sigma(n)$ list all n for which $\sigma(n)$ is odd. Do you notice any property these integers have in common? Complete the following theorem and try to prove it:

If $\sigma(n)$ is odd, then n is . . . . . .

Let us now return to our original problem of finding perfect numbers. We remember that in order for n to be perfect $\sigma(n) = 2n$. Euclid arrived at the following rule: $n = 2^{m-1}(2^m - 1)$ is a perfect number if $2^m - 1$ is prime. Use Euclid's result to find other perfect numbers. Try to prove Euclid's theorem: If $n = 2^{m-1}(2^m - 1)$ and $2^m - 1$ is a prime, then n is a perfect number.

As you can see from your computations with Euclid's theorem, one good mathematics problem often leads to another. Euclid's theorem tells us that $2^{m-1}(2^m - 1)$ is perfect if $2^m - 1$ is a prime. So that we can find as many perfect numbers as we can find primes of the form $2^m - 1$.

Suppose we consider this problem a bit. If m is 2, $2^m - 1 = 3$, which is a prime. This gives the perfect number 6. If m is 3, $2^m - 1 = 7$, which is also prime This gives the perfect number 28. If m is 4, $2^m - 1 = 15$, which is not prime. For $m = 5$, $2^m - 1 = 31$, which is prime and you can see that the perfect number which corresponds to $m = 5$ is already quite large. Test values of m up to 13 to see how many more perfect numbers you can find.

The primes of the form $2^m - 1$ are called Mersenne primes after a French monk, Father Marin Mersenne (1588-1648), who listed eleven values of m less than or equal to 257 for which he claimed $2^m - 1$ was prime. Modern digital computers have been employed to check and extend Mersenne's results and it has been found that two values 67 and 257 which Mersenne stated gave primes, do not, and that there are three others less than 257 which do give primes and which Mersenne missed. Your own calculations have probably convinced you that for large values of m it may be hard to tell whether $2^m - 1$ is prime or not. However, we could decrease the number of trials by noticing that if m itself is not prime, then $2^m - 1$ cannot be Therefore we have to test only $2^p - 1$

where p is prime. Think this over and see if you can prove the statement: If m is not prime, $2^m - 1$ is not prime.

The Mersenne primes with m less than 2300 are now completely determined. The values of m which give Mersenne primes are 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 607, 1279, 2203, and 2281. Accordingly seventeen even perfect numbers are known. The last five of these were found in 1952 by SWAC, the digital computer at U.C.L.A. The Mersenne prime $2^{2281} - 1$ is also the largest prime known. It has at least 686 digits and gives a perfect number with at least 1372 digits.

There are still two unsolved problems concerning perfect numbers We have shown a number in Euclid's form $2^{m-1}(2^m - 1)$ is perfect whenever $2^m - 1$ is prime. It can also be proved that any even perfect number must have this form Try to prove this for yourself. (It is not very easy.) However, it is still unknown whether there are a finite number of even perfect numbers or infinitely many That is we do not know whether or not there are infinitely many Mersenne primes.

The other problem sounds easier. Find an odd perfect number. At the present time no odd perfect numbers are known and many mathematicians think it likely that none exist. However, no one has been able to prove this The best that is known is that if an odd perfect number exists, it must have at least six different prime factors and cannot be less than 1.4×10^{14} .

There is one result about perfect numbers which is true whether the perfect number is even or odd. Prove that the sum of the reciprocals of all the divisors of a perfect number is 2. (HINT: Call the divisors d_1 , d_2 , ..., d_k and notice that for every divisor d_1 , $\frac{n}{d_1} = d_1$, is also a divisor of n .)

We have been able to restate our original problem of determining perfect numbers in terms of the function $\sigma(n)$. But this arithmetic function is useful in other problems besides that of finding perfect numbers. If you have read part I of this unit, you

may remember that we found an expression for the number of divisors of an integer n, $\tau(n)$.

If $n = p_1^{m_1} p_2^{m_2} p_3^{m_3} \ldots p_r^{m_r}$, we found that $\tau(n) = (m_1+1)$. $(m_2 + 1) \ldots (m_r + 1)$. In this part we found that

$\sigma(n) = (1 + p_1 + p_1^2 + \ldots + p_1^{m_1})(1 + p_2 + p_2^2 + \ldots + p_2^{m_2})$ $\ldots (1 + p_r + \ldots + p_r^{m_r})$. If this expression for $\sigma(n)$ is multiplied out we get a sum which contains as summands all the divisors of n and each exactly once. Hence if we replaced each summand by a 1 we would get for the sum exactly $\tau(n)$, the number of divisors of n. This is easily seen by replacing each p in the formula for $\sigma(n)$ by 1 and then the formula reduces to our formula for $\tau(n)$.

Thus we can look at $\sigma(n)$ as a generalization of $\tau(n)$. This is sometimes indicated by writing $\sigma_0(n) = \tau(n)$, the subscript zero indicates that we are taking the sum of zeroth powers of the divisors of n. $\sigma_1(n) = \sigma(n)$ is the sum of the first powers of the divisors of n. Similarly mathematicians found it natural to ask for the sum of the k^{th} powers of the divisors of n. Try to devise a formula for the sum of the k^{th} powers of the divisors of n.

(HINT: $\sigma_k(n) = (1^k + p_1^k + (p_1^2)^k + \ldots + (p_1^{m_1})^k) \ldots (1^k + p_r^k +$ $(p_r^2)^k \ldots + (p_r^{m_r})^k)$. Simplify.)

3.

ARITHMETIC FUNCTIONS

III

THE DISTRIBUTION OF PRIMES AND THE FUNCTION $\pi(n)$

One of the most interesting problems in the study of the integers has to do with the distribution of primes. A prime is an integer which has exactly two divisors, 1 and the integer itself. The first few primes are 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31. In the supplement entitled Prime Numbers several interesting facts about primes are discussed One of these is that there are infinitely many primes It is also shown in that supplement that there are arbitrarily large gaps in the sequence of primes. On the other hand, primes can be as close together as 2 and 3 or 3 and 5. It isn't hard to see that no two consecutive integers can be prime after the pair 2 and 3 . Why not? However, as far as the table of primes has been extended, we still find pairs of primes whose difference is 2 . Such primes are called "twin primes". The first few twin primes are 3 and 5 , 5 and 7 , 11 and 13 .

Exercise 1. Make a table of all primes less than 100.

Exercise 2. Find all pairs of twin primes less than 100.

One of the famous unsolved problems of number theory (the study of properties of the positive integers) is the question: "Are there infinitely many pairs of twin primes?"

Another unsolved problem is that of finding an expression for the n^{th} prime number. You can see from your table of primes that the distribution of primes seems to be very irregular. Since mathematicians have not succeeded in finding a formula for the next prime after any given prime, a related question could be asked: "How many primes are there less than or equal to a given integer n ?" We might give a name to this function which gives the number of primes $\leq n$. It is usually called $\pi(n)$.

Exercise 3. Compute $\pi(n)$ from your table of primes for $n = 10$, 20, 30, 40, 50, 75, 100 .

You can see that finding $\pi(n)$ for large values of n is quite a job. In fact extending the table of primes gets to be a formidable job. To decide that a given integer n is prime, we

need to be sure that no integer less than n divides n, except 1 of course. After a few trials we notice that it isn't necessary to try as divisors all integers less than n. If 2 doesn't divide n then no multiple of 2 will either. If 3 doesn't divide n then no multiple of 3 will. We could continue in this way and it quickly becomes evident that we only need to try as divisors prime numbers less than n, and not all of these. If we don't find a prime $\leq \sqrt{n}$ which divides n, then n must be prime. We can restate this fact as a theorem.

Theorem. If no prime $\leq \sqrt{n}$ divides n, then n is a prime.

Exercise 4. Prove this theorem.

(HINT: If d divides n, then $\frac{n}{d}$ divides n also.)

Exercise 5. Determine whether 1781 and 4079 are primes.

With this theorem, we have considerably reduced the work of deciding whether a given integer is a prime -- we need only try as divisors, primes which are $\leq \sqrt{n}$. For large n this is a great help. However, it only tells us about a particular integer n. Eratosthenes (c. 230 b.c.) devised a method, which we now call the sieve of Ertosthenes, for sieving out all primes less than a given integer if we know the primes up to $\sqrt{n}$. It goes like this. Write down all the integers $\leq n$. For example, take $n = 25$.

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19

20 21 22 23 24 25

In this case $\sqrt{25} = 5$ The primes $\leq \sqrt{25}$ are 2, 3, and 5. Underline all multiples of 2. Then underline all multiples of 3. Then all multiples of 5. (Note that some numbers will be underlined more than once.) Now all the integers which are not underlined are prime These numbers are precisely the primes greater than $\sqrt{25}$ and ≤ 25.

Exercise 6. Use this sieve method to extend your table of primes up to 225.

If we return to our problem of finding $\pi(n)$ we may use the idea of the sieve of Erathosthenes to devise a formula for $\pi(n)$. What we actually did was to take o the integers which were not

prime. There were n integers in our list. First, we took out the multiples of 2. There would have been $\frac{n}{2}$ of these if n had been even. Since n was odd, $\frac{n}{2}$ was not an integer, and in that case we took out a number equal to the greatest integer less than $\frac{n}{2}$, that is $\frac{n-1}{2}$. Similarly when we took out the multiples of 3, we took out a number equal to the greatest integer less than $\frac{n}{3}$, in this case $\frac{n-1}{3}$. We see then that it would be convenient to have an expression for this number of numbers which we sieve out each time. Let us define, then, the function $[x]$ to be the greatest integer $\leq x$. Some examples of this new function are: $[3] = 3$, $[2.61] = 2$, $[-5.1] = -6$, $[\sqrt{2}] = 1$, etc. It is clear that $[x]$ takes on only integral values, although its domain of definition is the set of real numbers. Strictly speaking, then it is not an arithmetic function, but an integral-valued function. The number of integers sieved out each time is now represented by $\left[\frac{n}{2}\right]$, $\left[\frac{n}{3}\right]$, $\left[\frac{n}{5}\right]$, etc.

What we have in mind is to devise an expression for $\pi(n)$ like $n - \left[\frac{n}{2}\right] - \left[\frac{n}{3}\right] - \left[\frac{n}{5}\right] - \ldots - \left[\frac{n}{p_k}\right]$, where p_k is the largest prime $\leq \sqrt{n}$. There are two difficulties with this method. In the first place, 6 was underlined twice in our sieving process. It was taken out as a multiple of 2 and also as a multiple of 3. If we are counting the numbers taken out by our sieve, then we only want to count 6 once. We have taken it out twice. The same thing happened to all multiples of 6. We can remedy this situation by adding back in $\left[\frac{n}{2 \cdot 3}\right] = \left[\frac{n}{6}\right]$, the number of numbers $\leq n$ which are multiples of 6. Adding it in insures that 6 is taken out only once. However, the same sort of thing happens with other numbers like 10, 14, 15, 21, etc. In general if an integer $m = p_1 p_2$, where p_1 and p_2 are primes, it will be taken out when we sieve with p_1 and again when we sieve with p_2. So that in all such cases in order to have the integer taken out only once, we must add it back in once. A better estimate of

$\pi(n)$ would then be an expression like

$$n - \left[\frac{n}{2}\right] - \left[\frac{n}{3}\right] - \cdots - \left[\frac{n}{p_k}\right] + \left[\frac{n}{p_1p_2}\right] + \left[\frac{n}{p_1p_3}\right] + \cdots + \left[\frac{n}{p_{k-1}p_k}\right] .$$

Even this expression won't quite do. We must consider numbers of the form $p_1p_2p_3$. These numbers will be sieved out 3 times; when we sieve by p_1 , by p_2 , and by p_3 . Then they will be added back 3 times when we add back the muptiples of p_1p_2 , p_1p_3 , and p_2p_3 So these numbers haven't actually been taken out at all. Consequently we remedy this situation by subtracting $\left[\frac{n}{p_1p_2p_3}\right]$.

If we continue in this manner we can take out all multiples of every prime once and only once and the number of numbers remaining will be given by the expression

$$M = n - \left(\left[\frac{n}{p_1}\right] + \left[\frac{n}{p_2}\right] + \cdots + \left[\frac{n}{p_k}\right]\right) + \left(\left[\frac{n}{p_1p_2}\right] + \left[\frac{n}{p_1p_3}\right] + \cdots + \left[\frac{n}{p_{k-1}p_k}\right]\right)$$
$$- \left(\left[\frac{n}{p_1p_2p_3}\right] + \left[\frac{n}{p_1p_2p_4}\right] + \cdots + \left[\frac{n}{p_{n-2}p_{k-1}p_k}\right]\right) + (\ . \ . \ .)$$
$$- \ (\ . \ . \ .) \quad \text{etc.}$$

This expression seems to go on indefinitely. However, as soon as $\frac{n}{m} < 1$, $\left[\frac{n}{m}\right] = 0$, and the complicated expression actually has only finitely many terms.

We said that there were two difficulties. We have fixed up the one of these caused by sieving out numbers more than one time. The other is that we have taken out all multiples of the primes, including the primes p_1 , p_2 , . . . , p_k , themselves We can correct this mistake by writing $\pi(n) = M + \pi(\sqrt{n}) - 1$. Of course $\pi(\sqrt{n}) = k$. So that the above formula becomes

$$\pi(n) = M + k - 1 .$$

The - 1 comes from the fact that 1 is not a prime.

Let us try the formula for $n = 25$. The primes $\leq\sqrt{25}$ are 2, 3, and 5 .

$$\pi(25) = 25 - \left(\left[\frac{25}{2}\right] + \left[\frac{25}{3}\right] + \left[\frac{25}{5}\right]\right) + \left(\left[\frac{25}{2\cdot3}\right] + \left[\frac{25}{2\cdot5}\right] + \left[\frac{25}{3\cdot5}\right]\right)$$
$$- \left[\frac{25}{2\cdot3\cdot5}\right] + 3 - 1$$

$\pi(25) = 25 - (12 + 8 + 5) + (4 + 2 + 1) - 0 + 3 - 1$

$= 9$.

Exercise 7. Compute $\pi(150)$ using the formula above. $\pi(225)$.

Exercise 8. Find the number of primes between 100 and 200 .

The formula we have obtained is an improvement over the original method of actually sieving, but it is still very time consuming for large values of n Mathematicians have succeeded in showing that for very large values of n, $\pi(n)$ is asyptotically equal to $\frac{n}{\log n}$; that is $\frac{\pi(n)}{\frac{n}{\log n}}$ approaches 1 as n gets very large (log n is the natural logarithm of n). This theorem is known as "the prime number theorem". Until 1948 the only proofs of this theorem which were known involved some of the deepest and most difficult mathematics An elementary proof was found in 1948 by Atle Selberg. However, this proof is very long and complicated and elementary only in a technical sense.

Exercise 9. $\pi(10,000,000) = 664,580$. Compute $\frac{\pi(n)}{\frac{n}{\log n}}$ for $n = 10,000,000$.

(HINT: $\log n = \frac{1}{M} \log_{10} n$, where $M = 0.4342945...$)

THE EUCLIDEAN ALGORITHM AND LINEAR DIOPHATINE EQUATIONS

At some point in your mathematical experience, you have undoubtedly encountered word or story problems. Here is one taken from the Ganita-Sara-Sangraha of Mahaviracarya, a Hindu writer of the ninth century. "Into the bright and refreshing outskirts of a forest which were full of numerous trees with their branches bent down with the weight of flowers and fruits, trees such as jambu trees, date palms, hintala trees, palmyras, punnaga trees and mango trees -- filled with the many sounds of crowds of parrots and cuckoos found near springs containing lotuses with bees roaming around them -- a number of travelers entered with joy. There were 63 equal heaps of plantain fruits put together and seven single fruits. These were divided evenly amoung 23 travelers. Tell me now the number of fruits in each heap." If we translate the problem into ordinary algebraic language (it is a shame to do such a thing to so beautiful a problem, but it does help to simplify the process of finding a solution), it looks something like this:

$$63x + 7 = 23y ,$$

where x is the number of fruit in each heap and y is the number each traveler receives From the nature of the problem it is clear that only solutions in positive integers are acceptable.

The question now is, how do we find solutions in integers to such equations.

One way might be to draw a graph of the straight line $ax + by = c$ and see if it passes through any points with positive integral coordinates. This particular equation does. Draw a graph of the equation. Can you find a solution from your graph?

Suppose our flowery Hindu problem had translated into the equation $3x + 6y = 13$. Does this equation have a solution in positive integers? Why?

Solve $3x + 6y = 24$ for x and y positive integers. Is there more than one solution? How many are there? For what positive solution is x smallest? For which positive solution is y smallest?

Consider the equation $2x - y = 6$. Find a solution with x and y positive integers Is there more than one such solution?

How many positive solutions are there?

After the last three examples, it would seem that an equation $ax + by = c$ with a, b, and c integers may have no solutions, a finite number of positive solutions, or an infinite number of positive solutions. Can you tell which one of these cases you have by looking at the graph of the equation? From your consideration of the graph of the equation try to write down conditions on the line which will cover all possibilities for the number of positive solutions.

If the numbers involved are quite large finding solutions from a graph might be very difficult. Fortunately we can completely solve this problem of finding integral solutions without using graphical methods at all. To do this we need to be able to tell when a solution exists; and if a solution exists, we would like to have a method (besides guessing or trial and error) which will always lead us to a solution. Finally it would be nice if we could devise an expression which would tell us all possible solutions in integers for the equation. All (these) things are possible for those who like mathematics.

First consider the following equations:

(1) $2x + 3y = 5$ (4) $4x + 6y = 9$

(2) $2x + 4y = 5$ (5) $4x + 6y = 8$

(3) $3x + 3y = 5$ (6) $2x - 4y = 4$.

Which of these have integral solutions?

Look at the coefficients of x and y and the constant term in each of the equations for which you found a solution. Is it true that any number which divides both the coefficient of x and the coefficient of y divides the constant term? Do you think this must be true of any equation which has a solution? State this result as a theorem and write out an informal proof for the theorem. (HINT: Call d the greatest common divisor of a and b . If we used the notation gcd(a,b) = d , then gcd (2,4) = 2; gcd (9,12)= 3 ; gcd (2a,3a) = a ; gcd (abc, abe) = ab, etc You can see that this is a very clumsy notation. We might abbreviate, when it is clear that we mean the greatest common divisor of two integers, by omitting the letters gcd Then (40,24) = 8 means gcd (40,24)= 8.

Unfortunately, this notation (a,b) is used in several different ways in various parts of mathematics. However, as we have noted above, if a and b are integers and we write (a,b) = d for the greatest common divisor it isn't easily confused with the other uses of the symbol.)

This theorem which you have arrived at states what is called a NECESSARY condition that the equation $ax + by = c$ have a solution in integers. This is a reasonable use of the word necessary since the equation cannot have a solution unless (a,b) divides c. The condition is truly necessary for a solution of the equation.

Mathematicians love to find a neat condition which is necessary and which also insures that a given problem has a solution. That is, it would be nice if two things were true -- (1) that $ax + by = c$ has no solution unless (a,b) divides c and (2) that if (a,b) divides c, the equation always does have a solution in integers. You have met this idea before in Chapter I where the phrase "if and only if" was used. We could restate our hopeful statement above as: The equation $ax + by = c$ has a solution in integers if and only if (a,b) divides c.

Look again at our six equations above. Does it seem to be true that if (a,b) divides c, there is a solution? We shall now try to devise a way to prove that this is always true.

How do you find the greatest common divisor of two integers? In all the cases we have considered, it has been easy to do just by looking at the two integers. How did you do it in the seventh and eighth grades when adding fractions with different denominators? One way of course is to write out the factors of each integer and pick out those which are common. For instance, to find (248, 312), we write $248 = 2^3 \cdot 31$ and $312 = 2^3 \cdot 3 \cdot 13$. Then clearly (248, 312) = 8. However, suppose the numbers are large and it isn't easy to find the factors of either number. For example, suppose we are asked to find (782, 3315). The usual method works of course, but is not as easy as in the cases we have previously encountered. Another method which solves this problem is attributed to Euclid (who lived about 300 B.C.).

It goes like this:

$$3315 = 782 \cdot 4 + 187$$
$$782 = 187 \cdot 4 + 34$$
$$187 = 34 \cdot 5 + (17)$$
$$34 = 17 \cdot 2 + 0$$

Euclid's method (or algorithm) gives 17 , the last non-zero remainder, as the greatest common divisor of 3315 and 782. That 17 is the greatest common divisor can be proved as follows. First, proceeding from the bottom to the top, we can see that 17 divides each number on the left hand side as follows:

$$34 = 17 \cdot 2$$
$$187 = 17\,(2 \cdot 5 + 1)$$
$$782 = 17\,(2 \cdot 5 + 1)\,4 + 17 \cdot 2 = 17\,\{(2 \cdot 5 + 1) \cdot 4 + 2\}$$
$$3315 = 17\,\{(2 \cdot 5 + 1) \cdot 4 + 2\}\,4 + 17\,(2 \cdot 5 + 1)$$
$$= 17\left(\{(2 \cdot 5 + 1) \cdot 4 + 2\} \cdot 4 + (2 \cdot 5 + 1)\right).$$

Thus we have shown that 17 is a divisor of both 3315 and 782 . It is, then, a common divisor.

Now let us show that it is the greatest common divisor. We do this by showing that any number d* which divides both 3315 and 782 must divide 17 . Then if an integer divides 17 , it cannot exceed 17 . Hence 17 must be the <u>greatest</u> common divisor. To prove this we simply reverse the process of the preceding paragraph. Suppose d* divides 3315 and 782 ; then it must divide $3315 - 782 \cdot 4 = 187$. Why? Next if d* divides 782 and 187 , it divides $782 - 187 \cdot 4 = 34$. But then if d* divides 187 and 34 , it divides $187 - 34 \cdot 5 = 17$. So we see that any number which divides both 3315 and 782 must divide 17 . Therefore 17 must be the greatest common divisor of these two numbers.

You may have noticed that we have used repeatedly a very obvious fact, namely, that if an integer divides each of two integers, it divides their sum and their difference. This is a trivial but extremely useful theorem. Write out a proof for this theorem giving reasons for each step.

Suppose we try Euclid's method on 253 and 122.

$$253 = 122 \cdot 2 + 9$$
$$122 = 9 \cdot 13 + 5$$
$$9 = 5 \cdot 1 + 4$$
$$5 = 4 \cdot 1 + (1)$$
$$4 = 1 \cdot 4 + 0$$

The greatest common divisor is 1 , the last non-zero remainder. Such numbers which have 1 for their greatest common divisor are called relatively prime. Check that (253, 122) = 1 by factoring the two numbers.

Find the g.c.d. of 1596 and 96 . Find (418,.1376); (365, 146) .

To prove that Euclid's method always gives us the greatest common divisor for any two integers a and b , we can proceed as follows:

(Suppose $a > b$.)

$$a = b \cdot q_1 + r_1$$
$$b = r_1 \cdot q_2 + r_2$$
$$r_1 = r_2 \cdot q_3 + r_3$$
$$r_2 = r_3 \cdot q_4 + r_4$$

.

.

.

$r_{n-2} = r_{n-1} \cdot q_n + r_n$, where r_n is the last non-zero remainder. (Is it clear that there will always be a last non-zero remainder? Why?) To show that r_n is the greatest common divisor, we must show that r_n is a common divisor; that is, that it divides both a and b . This is left to the reader. He can argue in exactly the same way that we did in the first example with 17 , 3315 , and 782 . Then we must show that any common divisor of a and b divides r_n . The argument again is the same as in the example.

We now have a fool-proof method for obtaining the greatest common divisor of any two integers. Actually we have done a good bit more. Not only can we find d = (a,b), but we get as a bonus

a solution to the equation $ax + by = d$. In the case of 17, 3315, and 782 we are in a position to solve the equation $3315x + 782y = 17$. The solution is as follows:

Euclidean Algorithm	Solution of $3315x + 782y = 17$
$3315 = 782 \cdot 4 + 187$	$187 = 3315 - 782 \cdot 4$
$782 = 187 \cdot 4 + 34$	$34 = 782 - 187 \cdot 4$
	$= 782 - (3315 - 782 \cdot 4)4$
	$= 782\,(1 + 4 \cdot 4) - 3315\,(4)$
$187 = 34 \cdot 5 + 17$	$17 = 187 - 34 \cdot 5$
	$= (3315 - 782 \cdot 4) - \{782(1 + 4 \cdot 4) - 3315(4)\} \cdot 5$
	$= 3315\,(1 + 4 \cdot 5) - 782\,\{4 + 4 \cdot 4)5\}$
	$= 3315\,(21) - 782\,(89)$

So that if we set $x = 21$ and $y = -89$ we have a solution to the original equation.

You will remember that in the beginning of this discussion we were trying to find solutions in integers to equations of the form $ax + by = c$. We found that in order for the equation to have a solution at all, $(a,b) = d$ had to divide c. The claim was made that if this happened, there was always a solution in integers for the equation. We are now in a position to show that this is true. Suppose you stop reading at this point and try to find out how to get a solution from what we have done so far.

Check your method with the following. From our discussion above of Euclid's algorithm, it is clear that we can always solve $ax + by = d$ where $d = (a,b)$. To find a solution of the original equation let $c = d \cdot c'$. Now take the equation $ax + by = d$ and multiply both sides by c' We get

$$a(xc') + b(yc') = dc' = c .$$

It is clear then that xc' and yc' are solutions to our problem.

This is really a nice result. We have a method for finding a solution to any equation which has a solution.

There is just one thing -- the solution we get may not be in positive integers x and y. Of course there may not be any solutions in positive integers, but in our "beautiful forest" problem, clearly only positive solutions are acceptable. While it

is wonderful always to be able to get one solution, a real mathematician, at this point, would certainly wonder "Isn't there some way to find all the solutions?". Try to find a way to find another solution from the one obtained by Euclid's algorithm. Can you now find all solutions?

(HINT: Suppose x_o and y_o satisfy the equation, i.e., $ax_o + by_o = c$ = and suppose x and y are any other pair of numbers which satisfy it, so that $ax + by = c$. Then subtract the first equation from the second, divide both sides of the resulting equation by d, transpose, try to see what can be said about $(x - x_o)$ and $(y - y_o)$.)

When you have made as much as you can out of the "hint", check your results with the reasoning in the answer sheet. You will find there that the general solution may be given in the form

$$x = x_o + \frac{b}{d} t$$

$$y = y_o - \frac{a}{d} t \quad \text{where } t \text{ is an integer } t .$$

It is easy to check that for any integer t the x and y given above do satisfy the equation provided x_o and y_o do. Check this for yourself. It is clear from this check that this x and y will satisfy the equation for any value of t. Is it also clear that any solution must have this form for some integer t? Try to show that this is true.

We are now in a position to find all the positive solutions for our original equation if any exist. Let us take the equation $3315x + 782y = 17$ again. By our method we get the solution $x = 21$ and $y = -89$. Are there any positive solutions? Well if we look at the general solution obtained above, for this equation it assumes the form $x = 21 + 46\,t$, $y = -89 - 195t$. To find positive solutions we must have t which satisfies $x = 21 + 46t > 0$ and $y = -89 - 195t > 0$. However, if t satisfies both of these inequalities it must be an integer. $> -21/46$ and at the same time $< -89/195$. There is no integer satisfying both of these at the same time.

(Plot these 2 numbers on the real line and look for the integers to the right of $-21/46$ which are also to the left of $-89/195$.) Consequently there are no positive solutions. Of course in this particular problem this is clear from looking at the equation. However, the method we have used will lead you to the values of t which give all positive solutions in any other problem.

Now you are in a position to find out the number of fruits in each heap in our original problem. Go to it.

What is the smallest number of fruit there could have been in each heap? Are there infinitely many positive solutions? Write out the general formula for all solutions.

Here are a few more problems which you can solve using the methods of this unit.

1. $16x + 7y = 601$.
2. Find the positive solutions for the equation $101x + 753y = 100{,}000$.
3. Say quickly, mathematician, what is the smallest multiplier by which 221 being multiplied and 65 added to the product the sum divided by 195 becomes exhausted? (From the Lilavati of Bhaskara (1150 A.D.).)
4. In the forest 37 heaps of wood apples were seen by the travelers. After 17 fruits were removed, the remainder was divided evenly among 79 persons. What is the share obtained by each? (Mahaviracarya)
5. $14x - 45y = 11$.
6. $40x - 63y = 135$.

5.

THE GAUSSIAN INTEGERS

In order to be able to find solutions to all quadratic equations $ax^2 + bx + c = 0$ where a, b, and c are real numbers, we found it necessary to extend our number system to include numbers whose squares are negative. In fact, if we adjoin to the set of real numbers a number with the property that its square is -1, define addition and multiplication for this extended set, we achieve a new number system in which every quadratic equation (or more generally every polynomial equation) with coefficients in the new system has solutions.

This extension of our number system consists of the set of all numbers of the form $a + bi$ where a and b are real numbers and i is a number with the property that $i^2 = -1$. This new system is called the field of complex numbers. Most of our work in mathematics in grades one through eight is arithmetic. Let us now investigate arithmetic in the complex number system. In ordinary arithmetic we were mainly concerned with the positive integers. The question naturally arises "What are the integers of our new extended number system?" To try to devise a reasonable definition, we try to generalize some property of the ordinary integers in the system of rational numbers so that these "rational integers" will still be "integers" in the extended system, and so that as many characteristics of the ordinary rational integers as possible will be retained.

In keeping with our interest in solving equations, the property of the rational integers that we choose to generalize is the property that they are solutions of linear equations, $x + a = 0$, with rational integral coefficients. For our purpose it is convenient to restrict our attention to a subset of the complex numbers, namely the set of numbers $\{a + bi\}$ where a and b are rational. We then define Gaussian integers to be those complex numbers $a + bi$, a and b rational, which satisfy an equation of the form $z^2 + mz + n = 0$ where m and n are ordinary

rational integers. These new integers are called Gaussian integers in honor of Carl Frederich Gauss (1777-1855) the German mathematician who is ranked with Archimedes and Newton as one of the three greatest mathematicians of all time. Gauss was the first person to systematically develop the properties of these new integers, and, in particular to show that the Fundamental Theorem of Arithmetic (Every integer can be written as the product of primes and in essentially only one way.) holds for these integers.

Suppose we now consider the form which the new Gaussian integers must have. We remember that the definition requires that they be numbers of the form $a + bi$, a and b rational, which satisfy an equation $z^2 + mz + n = 0$, m and n ordinary rational integers. If $b = 0$, the Gaussian integer is a rational number $a = \frac{p}{q}$. Suppose that $\frac{p}{q}$ has been reduced to that p and q are rational integers with no common factors. Thence since $a = \frac{p}{q}$ satisfies $z^2 + mz + n = 0$, we have

$$\frac{p^2}{q^2} + m\frac{p}{q} + n = 0$$

$$p^2 + mpq + nq^2 = 0$$

$$p^2 = q(mp + nq) .$$

q then divides p^2. But since p and q have no common factors, q must divide p and q must actually be 1. (If not q is a common factor of q and p.) But if $q = 1$, then a is actually a rational integer.

There remains the case when $b \neq 0$. In this case from the quadratic formula we have that if $a + bi$ is a root then $a - bi$ is also.

Accordingly

$$(z - (a + bi)(z - (a - bi)) = z^2 + mz + n$$

$$z^2 - 2ac + a^2 + b^2 = z^2 + mz + n$$

and

$$m = 2a$$

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

Then

(1) $a = \frac{-m}{2}$ and

(2) $b = \pm\sqrt{\frac{4n - m^2}{2}}$.

Since b is rational

(3) $4n - m^2 = c^2$, where c is some rational integer.

Substituting (3) in (2) we have

(4) $b = \frac{\pm c}{2}$.

The equation (3) can be written $4n = m^2 + c^2$.

This means that m and c are either both even or both odd. They cannot both be odd.

Exercise 1.

Prove that the sum of the square of two odd numbers is not a multiple of 4 .

Therefore both m and c are even and a and b are rational integers.

We have then in both cases that a and b must be rational integers and we are now able to say that the Gaussian integers are complex numbers of the form $a + bi$ where a and b are actually rational integers.

It is easy to check that the sum, difference, and product of two Gaussian integers is a Gaussian integer.

Exercise 2.

Show that the sum, difference, and product of two Gaussian integers is a Gaussian integer.

We see then that our new integers behave at least in these respects like ordinary rational integers. When we come to division we must look a little more closely.

Exercise 3.

Is the quotient of two rational integers a rational integer? Justify your answer.

Exercise 4.

Is the quotient of two Gaussian integers a Gaussian integer? Justify your answer.

The previous exercise shows us that division is not always possible in the set of Gaussian integers. Let us then define division for Gaussian integers precisely. We say that the Gaussian integer α is divisible by the Gaussian integer β if there is a Gaussian integer γ such that $\alpha = \beta\gamma$

Example 1.

Is $2 + 3i$ divisible by $1 + i$?

SOLUTION:

If $2 + 3i$ is divisible by $1 + i$, then there must be a Gaussian integer $x + yi$ such that

$$(1 + i)(x + yi) = 2 + 3i .$$

Then $$(x - y) + (x + y)\,i = 2 + 3i ,$$ and

$$x - y = 2 ,$$

$$x + y = 3 .$$

$$x = \frac{5}{2} , \quad y = \frac{1}{2} .$$

Since these are the only possible values for x and y if $x + yi$ satisfies the original equation, and since these are not rational integers, our answer is "No, $2 + 3i$ is not divisible by $1 + i$."

Exercise 5.

Is $2 + 3i$ divisible by $2 - 3i$? by i ?

Exercise 6.

Is $3 + 11i$ divisible by $2 + 3i$? by $-i$?

We have seen that the conjugate, $a - bi$, of the complex number, $a + bi$, is useful in many questions concerning complex numbers. We use the conjugate to define the norm of a complex integer. The norm of $a + bi$ is defined as $(a + bi)(a - bi) = a^2 + b^2$. We immediately notice several things about the norm of a complex integer. In the first place, it is a rational integer since a and b are. In the second place it is non-negative. If $b = 0$, the norm of the rational integer a is a^2. These properties prove very useful in trying to settle many questions about Gaussian integers.

If we look into the divisibility properties of the Gaussian integers, we are led to consider the integers which correspond to

1 and -1 among the rational integers; 1 and -1 are the only rational integers which divide every rational integer. We call these numbers the units of the system of rational integers. Similarly we define units for the Gaussian integers to be those Gaussian integers which divide every Gaussian integer. We can determine the units for the Gaussian integers quite easily by first using our new notion of the norm.

We first need the preliminary theorem or

Lemma. $N(\alpha\beta) = N(\alpha)\,N(\beta)$, where $N(\alpha)$ denotes the norm of α.

Proof: If we let $\bar{\alpha}$ be the conjugate of α and $\bar{\beta}$ be the conjugate of β,

$$\begin{aligned} N(\alpha) &= \alpha\bar{\alpha} \\ N(\beta) &= \beta\bar{\beta} \\ N(\alpha\beta) &= \alpha\beta\,\overline{\alpha\beta} \qquad \text{Since } \overline{\alpha\beta} = \bar{\alpha}\cdot\bar{\beta} \\ &= \alpha\beta\bar{\alpha}\bar{\beta} \\ &= (\alpha\bar{\alpha})(\beta\bar{\beta}) \\ &= N(\alpha)N(\beta) \end{aligned}$$

The lemma can also be proved directly from the definition of the norm. Let $\alpha = a + bi$, $\beta = c + di$ and write out the details of this proof.

It is now easy to show

Theorem 1. u is a unit if and only if $N(u) = 1$.

Proof: If u is a unit, it divides every integer and in particular the integer 1

Then $1 = u \cdot v$ for some Gaussian integer v.

By the lemma, $N(1) = N(u)N(v)$.

But $N(1) = 1 = N(u)N(v)$. Since the norm of any integer is a positive rational integer $N(u) = N(v) = 1$ and the "if" part of the theorem is proved.

Now suppose $N(u) = 1$.

Let $u = e + fi$. Then $e^2 + f^2 = 1$ and either $e = 0$ and $f = \pm 1$ or $f \neq 0$ and $e = \pm 1$.

Hence if $N(u) =$, $u = 1, -1, i, -i$. But 1 and -1 clearly

divide any Gaussian integer $a + bi$. Also $a + bi = i(b - ai)$ and $a - bi = i(-b + ai)$. Hence these four integers divide every Gaussian integer and are therefore units.

q.e.d.

We have as a bonus from this theorem, the

Corollary: The units of the Gaussian integers are 1, -1, i, and $-i$.

When finding the divisors of a rational integer n, it is only necessary to consider positive divisors of positive integers n, since for any divisor d of n, $-d$ is always a divisor of n. Similarly if n is negative whenever d divides n so does $-d$. We could describe this situation by saying that n and $-n$ are associates; i.e., the associates of an integer n are integers obtained by multiplying n by units. In the case of rational integers n has only the associates n and $-n$. If we extend the associates of α to be the Gaussian integers obtained from α by multiplying α by units. Thus the associates of any Gaussian integer α are α, $-\alpha$, $i\alpha$, and $-i\alpha$.

If we now consider the divisors of a Gaussian integer, α, we need only concern ourselves with divisors which are not units or associates of α.

Exercise 7.

Show that if α and β are associates their norms are equal.

We are now able to define a Gaussian prime as a Gaussian integer which is not a unit and which has no divisors except units and its associates. Several interesting questions can now be asked.

1. Are rational primes Gaussian primes?
2. Are there infinitely many Gaussian primes?
3. Which rational integers are Gaussian primes?

We can answer the first without much trouble. 2 is a rational prime. However $2 = (1 + i)(1 - i)$. Since $1 + i$ and $1 - i$ have norm 2, they are not units. The associates of 2 are 2, -2, $2i$, and $-2i$. Therefore since $1 + i$ and $1 - i$ are neither units nor associates of 2, the rational prime 2 is not a Gaussian prime.

Exercise 8.

Is 5 a Gaussian prime?

Exercise 9.

Is 3 a Gaussian prime?

Let us now look more closely at rational primes of the form $4n + 3$. Suppose a rational prime $p = 4n + 3 = \alpha\beta$. Then $N(p) = N(\alpha)N(\beta) = p^2$. If p is not a Gaussian prime, then there must exist α and β such that $N(\alpha) \neq 1$ and $N(\beta) \neq 1$. In that case, $N(\alpha) = p$ and $N(\beta) = p$. But if $\alpha = x + yi$, $N(\alpha) = x^2 + y^2 = p = 4n + 3$. This is impossible for no integer of the form $4n + 3$ is the sum of two squares.

Exercise 10.

Prove that no rational integer of the form $4n + 3$ is the sum of two squares by considering all possible cases for x and y (both even, both odd, one even and one odd).

Since the norm of α and β cannot be p, the norm of one of them must be 1 and that one is a unit, and the other is an associate of p. Since p has no divisors except units and associates of p, we have proved the following theorem.

Theorem 2. Every rational prime of the form $4n + 3$ is a Gaussian prime.

This proves also that there are infinitely many Gaussian primes, since in the supplement Prime Numbers it is proved that there are infinitely many rational primes of the form $4n + 3$. And we have thus answered question two in the affirmative.

Exercise 11.

Is $1 + i$ a Gaussian prime?

Exercise 12.

Is $1 - i$ a Gaussian prime?

Exercise 13.

Is any composite rational integer a Gaussian Prime?

From the preceding discussion and exercises, we have the result that the only rational integers which are Gaussian primes are rational primes of the form $4n + 3$ and possibly some rational primes of the form $4n + 1$.

To settle the question about the existence of rational primes of the form $4n + 1$ which might also be Gaussian primes we need two results. The first is a theorem which is rather easy to prove.

Theorem 3. If $N(\alpha)$ is a rational prime, α is a Gaussian prime.

Proof: Suppose $\alpha = \beta\gamma$

Then $N(\alpha) = N(\beta)N(\gamma)$.

By hypothesis $N(\alpha) = N(\beta)N(\gamma) = p$, where p is a rational prime.

Since $N(\beta)$ and $N(\gamma)$ are rational integers, one of these is 1 and the other is p. The one whose norm is 1 is a unit and we have the result that α can only be written as a unit times an associate of α. Therefore α is a Gaussian prime.

q.e.d.

The other result which we need is that any rational prime of the form $4n + 1$ is the sum of two squares.

Exercise 14.

Write the following rational primes as the sum of two squares. (a) 5, (b) 13, (c) 17, (d) 29, (e) 101, (f) 1721.

Since the proof of this result requires more machinery from the theory of numbers than we have available, we will not give the proof here. (A proof can be found in any elementary number theory book.)

We are now in a position to settle the question about rational primes of the form $4n + 1$. Suppose $p = 4n + 1 = x^2 + y^2$. We can factor p as follows:

$$p = x^2 + y^2 = (x + yi)(x - yi) .$$

Then the Gaussian integers $x + yi$ and $x - yi$ have norm p and by Theorem 3 are Gaussian primes. Since the norm of p is p^2 and the norm of $x + yi$ and $x - yi$ is p, by Exercise 7 the primes $x + yi$ and $x - yi$ are not associates of p. Then p is the product of primes, which are not associates of p. We have therefore proved

Theorem 5. No rational prime of the form $4n + 1$ is a Gaussian prime.

The answer to question three, then is: The only rational integers which are Gaussian primes are the rational primes of the form $4n + 3$.

Actually, it can be shown that the Gaussian primes are of three kinds:

(1) rational primes of the form $4n + 3$ and their associates,

(2) $1 + i$, $1 - i$ and their associates,

(3) integers of the form $x + yi$ and $x - yi$ where x and y are positive, x is even and $x^2 + y^2$ is a rational prime, and their associates.*

*A linen manufacturing company: N. W. Linnenfabrieken, E. J. E. van Dissel and Zonen, P.O. Box 272, Eindhoven, Holland, makes a tablecloth 28" x 28" in which the Gaussian primes form the woven design. It is available in red, green, blue, and yellow at $2.00 each.

6.

FERMAT'S METHOD OF INFINITE DESCENT

The theory of numbers (the study of properties of the positive integers) is a fascinating and difficult branch of mathematics. The French provincial government official and amateur mathematician Pierre Fermat (1601?-1665) devoted much of his leisure time to systematically cultivating this branch of mathematics.

One of the baffling aspects of number theory is the absence of many general methods for attacking problems in this field. Fermat devised an ingenious method which he called "the method of infinite descent" to handle certain kinds of problems. It is somewhat like mathematical induction in reverse. Instead of showing that a certain proposition, $P(n)$, is true for $n = 1$, and whenever $P(k)$ is true, $P(k+1)$ is also, we begin at the other end. We first suppose that $P(n)$ is true for some integer. We then show that if it is true for any particular integer, it is true for a smaller one. Since on the one hand this argument can be repeated indefinitely and on the other hand there are only finitely many positive integers less than a given positive integer, we have a contradiction. This means that our assumption that the proposition is true for some integer is wrong, and we have the result that the proposition is not true for any integer. In this form it would seem to be especially useful for disproving theorems.

The argument can be modified, however, to prove positive statements. Fermat said that he used it to prove that any prime of the form $4n + 1$ can be written as the sum of two squares. For instance $5 = 2^2 + 1^2$, $13 = 2^2 + 3^2$, $17 = 4^2 + 1^2$, $29 = 2^2 + 5^2$.

Exercise 1.

Write 37, 41 89, 101 as the sum of two squares. Can this be done in more than one way?

Fermat's argument goes as follows. Suppose an arbitrarily chosen prime, $p = 4n + 1$, is not the sum of two squares. He then shows that there is a smaller prime of this form which is not the sum of two squares. Continuing in this way he arrives at the result that 5 is not the sum of two squares. But $5 = 2^2 + 1^2$. This contradiction means that there was no prime of the form $4n + 1$ which was not the sum of two squares. We do not have Fermat's proof of this theorem and in fact it was not until 1749 that the first rigorous proof was given by the Swiss mathematician Leonard Euler (1707-1783).

Fermat discovered many deep and interesting properties of the integers. Very few of his proofs have come down to us; however, his method of infinite descent can be used to prove a special case of one of the most famous theorems in mathematics, Fermat's Last Theorem. In a margin of Bachet's Diophantus, Fermat made his famous note regarding the problem of finding rational solutions of the equation

$$x^2 + y^2 = z^2 . \tag{1}$$

"On the contrary, it is impossible to separate a cube into two cubes, a fourth power into two fourth powers, or, generally, any power above the second into two powers of the same degree: I have discovered a truly marvellous demonstration which this margin is too narrow to contain." Mathematicians are uncertain as to whether Fermat actually had a proof; however, no proof for all powers greater than 2 has yet been found.

The equation $x^2 + y^2 = z^2$, of course, does have solutions; for instance $3^2 + 4^2 = 5^2$. In fact we now obtain all solutions for this case as follows. We first note that we need only look for solutions x, y, and z which have no common factors, since if $x^2 + y^2 = z^2$, then certainly $(kx)^2 + (ky)^2 = (kz)^2$, and conversely.

Exercise 2.

Show that if any two of the integers x, y, and z in (1) have a common divisor, d, then d divides the third.

Accordingly we will consider only solutions which have no common factors. In this situation not all three integers x, y, and z can be even. Why not?

Exercise 3.

Show that not all three integers x, y, and z in (1) can be odd.

Exercise 4.

Show that it is impossible for two of the integers x, y, and z in (1) to be even and one of them odd.

The preceding exercises show that the only possibility for a solution to (1) is for one of the integers to be even and the other two to be odd. Suppose x is even and y and z are odd. Let

(2) $$x = 2u .$$ Then (1) becomes

(3) $$4u^2 + y^2 = z^2$$ or

$$4u^2 = z^2 - y^2$$

(4) $$4u^2 = (z + y)(z - y) .$$

Since z and y are odd, $z + y$ and $z - y$ are even. If we consider any common divisor of $z + y$ and $z - y$, it must divide their sum, $2z$, and their difference, $2y$. We know that 2 is a common divisor, but if there were any other besides 2, it would have to divide both z and y. However, we excluded this case in the beginning.

At this point we must pause to prove

Theorem 1. If the greatest common divisor of a and b is 1 and $ab = c^2$, then a is a square and b is a square.

Proof: By the Fundamental Theorem of Arithmetic (see the supplement entitled The Fundamental Theorem of Arithmetic), we may write c as the product of prime factors $p_1, p_2, \ldots p_n$. Then

$$c^2 = (p_1 p_2 \ldots p_n)^2 = ab .$$

Clearly p_1 divides ab. If p_1 divides a it does not divide b since a and b have no common factors. In this case p_1^2 must then divide a. If p_1 does not divide a, then it must

divide b and similarly in this case p_1^2 will divide b. We can make the same argument for each prime p_i. Hence if any prime divides a, so does its square; and this prime does not divide b. The same statement can be made for b. Accordingly, if we let p_{i_1} be the first prime that divides a, p_{i_2} be the second, etc.; $p_{i_{k+1}}$ be the first prime that divides b, $p_{i_{k+2}}$ be the second, etc.; we must have

$$a = p_{i_1}^2 p_{i_2}^2 \cdots p_{i_k}^2 = (p_{i_1} p_{i_2} \cdots p_{i_k})^2$$

$$b = p_{i_{k+1}}^2 p_{i_{k+2}}^2 \cdots p_{i_n}^2 = (p_{i_{k+1}} p_{i_{k+2}} \cdots p_{i_n})^2 .$$

q.e.d.

We now return to our problem of finding the solutions to the equation $x^2 + y^2 = z^2$. Since the greatest common divisor of $z + y$ and $z - y$ is 2, we can write (4) in the form

$$4u^2 = 4 \cdot \frac{z + y}{2} \cdot \frac{z - y}{2} = 4 \cdot Z \cdot Y ,$$

where the greatest common divisor of Z and Y is 1.

Then $u^2 = Z \cdot Y$ and by theorem 1

$Z = v^2$ and $y = w^2$ and

(5) $z + y = 2v^2$

(6) $z - y = 2w^2$.

Exercise 5.

Show that v and w have no common factors.

Then substituting (5) and (6) in (4) we have

$$4u^2 = (2v^2)(2w^2) \quad \text{or}$$

$$u^2 = v^2 w^2 \quad \text{and}$$

(7) $u = v \cdot w$.

Substituting (7) in (2) we have

(8) $x = 2vw$,

$\frac{1}{2}\{(5) - (6)\}$ gives

(9) $$y = v^2 - w^2 ,$$

$\frac{1}{2}\{(5) + (6)\}$ gives

(10) $$z = v^2 + w^2 .$$

Since y and z are both odd, one of v and w is even and the other odd.

In the beginning we supposed that x, y, and z were any solution without common factors and we have found the form which they must assume.

We have then

Theorem 2. The solutions of $x^2 + y^2 = z^2$ are given by

$$x = 2kvw ,$$

$$y = k(v^2 - w^2) ,$$

$$z = k(v^2 + w^2) ;$$

where k is any integer and v and w are any integers chosen so that they have no common factor and so that one is even and the other odd.

Fermat's Last Theorem can be stated as follows: There are no integers x, y, and z for which $x^n + y^n = z^n$ if n is greater than 2. The proof for the special case $n = 4$ serves as a good illustration of Fermat's method of infinite descent.

Theorem 3. There is no solution in integers for $x^4 + y^4 = z^4$. As above, if the equation has a solution x, y, z and any pair of these integers has a common factor, that common factor then divides the third integer and both sides of the equation can be divided by the fourth power of that common factor. So if there is a solution, we can assume that the x, y, and z are relatively prime in pairs; that is, every pair has greatest common divisor 1.

We also notice that if we can show that $x^4 + y^4 = z^2$ is impossible then so is $x^4 + y^4 = z^4$, since if the sum of two fourth powers isn't a square, it certainly can't be a fourth power.

We therefore prove the simpler statement that $x^4 + y^4 = z^2$ has no solution in integers. The proof by infinite descent follows.

Proof: Suppose there is a solution x, y, and z relatively prime in pairs, say $x^4 + y^4 = z^2$. This equation can be rewritten

$$(x^2)^2 + (y^2)^2 = (z)^2 .$$

However from Theorem 2 we know that

$$(11) \qquad \begin{cases} x^2 = 2ab , \\ y^2 = a^2 - b^2 , \\ z^2 = a^2 + b^2 ; \end{cases}$$

for some integers a and b with greatest common divisor 1 and one of these even and the other odd. Suppose that b is even.

Since $x^2 = 2ab = a(2b)$ and a and b have no common factors, by Theorem 1, $2b$ is a square and a is a square. Set

$$(12) \qquad \begin{cases} 2b = c^2 , \\ a = d^2 . \end{cases}$$

From (11) we have that $a^2 = b^2 + y^2$, and again by Theorem 2

$$(13) \qquad \begin{cases} b = 2rs , \\ y = r^2 - s^2 , \\ a = r^2 + s^2 ; \text{ where } r \text{ and } s \text{ have no} \end{cases}$$

common factor. But from (12) and (13) we have

$$2b = c^2 = 4rs .$$

By Theorem 1, then $r = x_1^2$,

$s = x_1^4 + y_1^4$ and since by (12) $a = d^2$,

we have $x_1^4 + y_1^4 = d^2$, where $1 < d < a < z$.

But now we have a solution x, y, d to the equation $x^4 + y^4 = z^2$ in which d is less than z. What we have actually shown is that if $x^4 + y^4 = z^2$ has a solution we can always find another solution with smaller z. But this is impossible since there are only finitely many positive integers less than a given integer z. Therefore there is no solution to $x^4 + y^4 = z^2$ and

consequently no solution to $x^4 + y^4 = z^4$.

Fermat also used this method of proof to show that if both of the legs of a right triangle are integers, the area cannot be a square. The proof of this statement is similar to the one given above.

7.

APPROXIMATIONS OF IRRATIONALS BY RATIONALS

In Chapter 1 of your text you learned that a real number can be represented by an infinite decimal. The main features of this representation are the following:

Let the real number be $g + \alpha$, where g is an integer and $0 < \alpha < 1$. Since the integral part g offers no difficulties, we can consider only α and write it as a decimal: $\alpha = 0.a_1a_2a_3\ldots$

(1) Each decimal section is a rational number. (By the nth decimal section of the decimal $0.a_1a_2a_3\ldots$, we mean the number $0.a_1a_2\ldots a_n$, i.e., $a_1/10 + a_2/10^2 + \ldots a_n/10^n$.)

(2) The difference $|\alpha - 0.a_1a_2\ldots a_n|$ can be made as small as we please if we choose n large enough.

(3) $\alpha - 0.a_1a_2\ldots a_n \leq 10^{-n}$.

(4) The denominator of each decimal section is a power of 10.

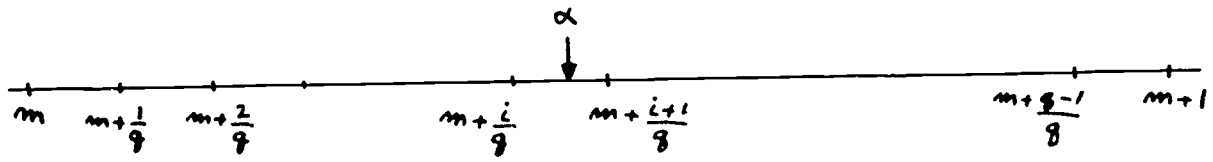
You may not have noticed property (3) before. It is easily proved, for $\alpha - 0.a_1a_2\ldots a_n = 0.\underbrace{0\ldots0}_{n}\ a_{n+1}\ a_{n+2}\cdots$

$\leq 0.\underbrace{0\ldots0}_{n}99\ldots = 0.\underbrace{0\ldots0}_{n-1}1$. (The numbers under the braces indicate the number of 0's.) Of course, (2) is a consequence of (3).

Properties (2) and (4) seem to be rather special; they arise from the fact that we are using decimal sections to approximate α. There seems to be no particular reason to do this, and in fact we might get better approximations if we used general rational numbers p/q as approximations.

Before doing this, however, let us realize that there is no particular point in approximating rationals by other rationals. From now on we shall assume that α, the number being approximated, is irrational.

It is very easy to produce rational numbers p/q for which $|\alpha - p/q| < 1/q$. Suppose α lies between the consecutive integers m and $m+1$. Let q be any integer > 1, and divide the interval $(m, m+1)$ on the number line into q parts or subintervals (see figure). Each part



is of length $\frac{1}{q}$; the points of subdivision are then $m + \frac{1}{q}$, $m + \frac{2}{q}$, ..., $m + \frac{q-1}{q}$. The point which represents α will fall inside one of the subintervals; it cannot fall on an endpoint of a subinterval since α is irrational whereas the endpoints are rational. If α falls in the subinterval whose left endpoint is $m + i/q$, then clearly

$$m + i/q < \alpha < m + \frac{i+1}{q},$$

so that $|\alpha - (m + i/q)| < 1/q$, or

$$(1) \qquad \left|\alpha - \frac{p}{q}\right| < \frac{1}{q},$$

where $p = qm + i$. Since this process can be carried out no matter what integer q may be (as long as $q > 1$), we have proved this result.

Theorem: If α is irrational, then to every integer $q > 1$ there corresponds an integer p such that (1) is true.

Let us check this result with some famous approximations of $\pi = 3.14159265...$ which were known to the Greeks, namely 22/7, 333/106, 355/113.

p/q	$\lvert \alpha - p/q \rvert$	$1/q^2$
22/7	.00126...	.1429...
333/106	.0000832...	.009434...
355/113	.000000266...	.008850...

These approximations are considerably better than what would be expected from the Theorem! Is a better result than (1) possible?

Before trying for a better result, let us spend a few words trying to make the whole concept of approximation more precise. If α is the number being approximated and p/q is the approximation, then certainly we want to make $|\alpha - p/q|$ "small". But small - compared to what? We can make $|\alpha - p/q|$ as small as we please provided we can take q large enough, as Theorem 1 shows. If we want to have $|\alpha - p/q| < 0.001$, we have only to choose $q \geq 1000$. In other words, we can make $|\alpha - p/q|$ small but we pay for it by having to use a large denominator q. This suggests that we might try for a result in which α is still approximated by p/q but the denominator of the right member of (1) is larger than q.

To get such a result, we shall introduce a completely obvious but very important principle:

THE BOX PRINCIPLE. <u>If $n + 1$ objects are placed in n boxes, there is a box which contains at least two objects.</u>

Even though this theorem is so obvious, give a formal proof of it.

You probably feel that nothing of any importance could possibly come out of anything that sounds so trivial as the Box Principle, but wait! Let n be any positive integer. Divide the interval $0 \ldots 1$ into n equal subintervals; these will be our n "boxes".

Now for each integer j in the range $1 \leq j \leq n + 1$, let p_j be the greatest integer less than $j\alpha$, that is,

$$0 < j\alpha - p_j < 1, \quad j = 1, 2, \ldots, n + 1$$

(Note that $j\alpha - p_j$ cannot be either 0 or 1, for $j\alpha - p_j$ is irrational.) Consider the $n + 1$ numbers

$$\alpha - p_1 , 2\alpha - p_2 , \ldots , (n+1)\alpha - p_{n+1} ;$$

they all lie between 0 and 1 and so are distributed among our n boxes. Hence, according to the Box Principle, there must be two of them, say $r\alpha - p_r$, $s\alpha - p_s$, which lie in the same box. If this box is the subinterval $j/n \ldots (j+1)/n$, we have

$$\frac{j}{n} < r\alpha - p_r < \frac{j+1}{n}$$

$$\frac{j}{n} < s\alpha - p_s < \frac{j+1}{n}$$

The second inequality may be written

$$-\frac{j+1}{n} < -s\alpha + p_s < -\frac{j}{n} .$$

Adding the first and last inequalities, we get

$$(2) \qquad -1/n < (r-s)\alpha - (p_r - p_s) < 1/n .$$

Since r and s are both integers between 1 and n + but are not equal, we see that $|r-s|$ is between 1 and n ; $1 \le |r-s| \le n$. Set $q = r - s$ or $s - r$, whichever is positive; $p = p_r - p_r - p_s$ if $r - s > 0$, $p = p_s - p_r$ if $r - s < 0$. Then $1 \le q \le n$, and (2) becomes $-1/n < q\alpha - p < 1/n$, or $|q\alpha - p| < 1/n$.

Hence,

$$(3) \qquad \left| \alpha - \frac{p}{q} \right| < \frac{1}{nq} .$$

This gives us the theorem:

Theorem. For each irrational number α and each positive integer n , there is a rational number p/q such that

$$(4) \qquad \left| \alpha - \frac{p}{q} \right| < \frac{1}{nq}$$

with $1 \le q \le n$.

Of course, (4) is considerably better than (1), simply because $1/nq$ is considerably smaller than $1/q$ when n is large. We can obtain a more useful form of (4) by noting that, since $n \ge q$, $nq \ge q^2$, so that

$$|\alpha - p/q| < 1/nq \le 1/q^2, \text{ or}$$

$$(5) \qquad \left| \alpha - \frac{p}{q} \right| < \frac{1}{q^2}$$

So far we have shown the existence of only one rational approximation p/q with the property (5). Actually, there are infinitely many such rational approximations, as we now show. Choose an integer $n' < n$ and find, by the last theorem, a rational $p'q'$ such that

$$|\alpha - p'q'| < 1/n'q' \text{ , with } 1 < q' \leq n' .$$

Now $\alpha - p/q$ is not zero, so there must be an integer t for which

$$(6) \qquad |\alpha - p/q| > 1/t$$

We shall increase t, if necessary, to make $t > n$ (this only strengthens the inequality (6)); then we can use t for the n' above.

So now we have the following:

$$\left|\alpha - \frac{p}{q}\right| > \frac{1}{n} , \quad \left|\alpha - \frac{p'}{q'}\right| < \frac{1}{n'q'} \leq \frac{1}{n'} < \frac{1}{n} .$$

This shows that p/q is not the same as p'/q', since the first is further from α than $1/n$, whereas the second is nearer to α than $1/n$. That is, p'/q' is <u>nearer</u> to α than p/q is. Thus, p'/q' is a new approximation to α, and moreover,

$$\left|\alpha - \frac{p'}{q'}\right| < \frac{1}{n'q'} \leq \frac{1}{q'^2}$$

so that (5) is satisfied. Now starting with p'/q' we could produce a still better approximation p''/q'' to α which also satisfies (5). We can continue this process indefinitely. This proves the following theorem:

<u>Theorem</u>: <u>For each irrational number α there are infinitely</u> many different rational numbers p_iq_i, $i = 1, 2, 3, \ldots$ for which

$$(7) \qquad \left|\alpha - \frac{p_i}{q_i}\right| < \frac{1}{q_i^2}$$

Can we do better even than (7)? Is it true, for instance, that there are infinitely many different p/q for which $|\alpha - p/q| < 1/q^3$? There are infinitely many irrationals α for which the last inequality holds, but there are also infinitely many α for which it does not.

We shall give an example. Let $\alpha = \sqrt{2}$. Suppose we wish to approximate $\sqrt{2}$ by a rational number p/q.

Case I. $p/q < \sqrt{2}$. We have $\sqrt{2}q > p$, and

$$2q^2 - p^2 = (q\sqrt{2} - p)(q\sqrt{2} + p) \geq 1,$$

because $2q^2 - p^2$ is a positive integer and so is at least 1. Hence, remembering that $p/q < \sqrt{2}$ and $\sqrt{2} < 1.42$, we get

$$q\sqrt{2} - p \geq \frac{1}{q\sqrt{2} + p} > \frac{1}{q\sqrt{2} + q\sqrt{2}} = \frac{1}{2\sqrt{2}q} > \frac{1}{4q},$$

and since $q > 0$,

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

Case II. $p/q \geq 2$. Since $\sqrt{2} < 1.42$,

$$\left|\sqrt{2} - \frac{p}{q}\right| > 0.58 > \frac{1}{4} \geq \frac{1}{4q^2}$$

since $q \geq 1$.

Case III. $\sqrt{2} < p/q < 2$. Then $p^2 > 2q^2$ and $p^2 - 2q^2 = (p - q\sqrt{2})(p + q\sqrt{2}) \geq 1$,

or

$$\left|\sqrt{2} - \frac{p}{q}\right| \geq \frac{1}{q^2} \cdot \frac{1}{\frac{p}{q} + \sqrt{2}} > \frac{1}{q^2} \cdot \frac{1}{2 + \sqrt{2}} > \frac{1}{4q^2}.$$

There are no more cases, for $\sqrt{2} \neq p/q$. (Why?)

In all cases, then, we have:

If p/q is a rational number, then

$$\left|\sqrt{2} - \frac{p}{q}\right| > \frac{1}{4q^2}. \tag{7}$$

Equation (7) shows that the approximation (6) cannot be essentially improved for all irrationals α. We can express this by saying that the approximation of a general irrational by a rational is measured by the square of the denominator of the rational.

Can you generalize (7) to other irrationals than $\sqrt{2}$? Can you give an infinite set of irrationals for which (7) is true?

8.

A NEW FIELD

The field you are most familiar with is the rational field, but you have also studied the real field and the field of complex numbers. If you read Section 5, Gaussian Integers, you learned about the domain of integers in a certain subfield of the complex field. Here we shall study a new field which shows some differences from the fields you have studied before.

Consider the subset K of the set of complex numbers consisting of all numbers of the form $a + b\sqrt{-5}$ $(=a + ib\sqrt{5})$, where a and b are rational numbers. We define two elements of K, $a + b\sqrt{-5}$, to be equal if they are equal as complex numbers, i.e., if and only if $a = c$ and $b = d$. It is easy to check that K is closed under addition, subtraction and multiplication. (Do this.) K contains $0 = 0 + 0 \cdot \sqrt{-5}$ and $1 = 1 + 0 \cdot \sqrt{-5}$. The set consisting of all non-zero elements of K is closed under division. (Check.) Moreover, all the rules of calculation are satisfied in K since they are satisfied for complex numbers. In short, K is a field; it is a subfield of the field of complex numbers.

Call the field of rationals R. In R we singled out certain elements which we called integers. Denote the set of integers in R by I. It is a little hard to see how we can define integers in K, but experience has shown that the following definition is satisfactory.

First, notice that every element $\alpha = a + b\sqrt{-5}$ of K satisfies a polynomial equation of degree 2 whose coefficients are rational numbers. Indeed, write

$$P(x) = (x - \alpha)(x - \bar{\alpha}) = \left((x-a) - b\sqrt{-5}\right)\left((x-a) + b\sqrt{-5}\right)$$
$$= (x-a)^2 + 5b^2 = x^2 - 2ax + a^2 + 5b^2 .$$

Certainly $P(x) = 0$ when $x =$ and the coefficients of P are rational numbers. Notice that the coefficient of the leading term is 1; such polynomials are called monic. When $b = 0$ so that $\alpha = a$, the equation becomes $(x-a)^2 = 0$; hence is a root of

the equation of lower degree,

$$P(x) = x - a = 0$$

The number α satisfies many polynomial equations, but $P(x) = 0$ has the smallest possible degree. This is obvious when $b = 0$ since $P(x)$ is then of the first degree. When $b \neq 0$, $P(x) = 0$ must have the root $\overline{\alpha} = a - ib$ if it has the root α (Chapter 5, Section 6), so $P(x) = 0$ is at least of degree 2. However, there might be more than one monic equation of lowest degree satisfied by α. Obviously this cannot be if $b = 0$. If $b \neq 0$, any quadratic equation $Q(x) = 0$ satisfied by α must have the factors $x - \alpha$ and $x - \overline{\alpha}$ and no others. Hence, Q is of the form $c(x-\alpha)(x - \overline{\alpha})$, where c is a real or complex number. But since Q is monic we must have $c = 1$ and so Q is identical with P.

So we see that each element α of K satisfies a unique equation $P(x) = 0$ which is either linear or quadratic. Of special interest are those elements α of K whose unique monic equations have not only rational coefficients but rational integral coefficients. (We now have to say "rational integers" to denote integers in R because we are going to define integers in K.)

Definition. An element of K is an integer in K if and only if the unique monic equation which it satisfies has rational integral coefficients. We write J for the set of integers in K.

Is an integer in R (rational integer) also an integer in K? What monic equation does it satisfy? This shows that I is a subset of J, or as we write it, $I \subset J$. Algebraic structures like I and J which are closed under addition and multiplication, which possess an additive identity (0) and a multiplicative identity (1), and which satisfy the associative, commutative, and distributive laws and the cancellation law ($ab = ac$ and $a \neq 0$ imply $b = c$), are called integral domains.

Let us consider an element $\alpha = a + b\sqrt{-5}$ of J. The equation which α satisfies is, as we have seen,

$$x^2 - 2ax + a^2 + 5b^2 = 0.$$

Since $\alpha \in J$, we have that $2a$ and $a^2 + 5b^2$ belong to I;

hence, $-(2a)^2 + 4(a^2 + 5b^2) = 20b^2 \in I$. From this you will be able to deduce that $2b \in I$, if you remember that b is rational. (Do this.) So we have that $2a$ and $2b$ are rational integers; write $a = a_1/2$, $b = b_1/2$, where $a_1, b_1 \in I$.

Let $a^2 + 5b^2 = c$, $c \in I$. We have $4a^2 + 5 \cdot 4b^2 = a_1^2 + 5b_1^2 = 4c$. Now $4c$ is divisible by 4; hence so is $a_1^2 + 5b_1^2$. But the square of any odd integer has a remainder 1 when divided by 4. By trying out the four possible cases (a_1 even or odd, b_1 even or odd), we see that $a_1^2 + 5b_1^2$ is divisible by 4 only if a_1 and b_1 are both even. Therefore, $a \in I$ and $b \in I$. <u>The integers in K are the numbers of the form $a + b\sqrt{-5}$, where a and b are rational integers</u>.

We can now do arithmetic in J just as we did in I. We shall use Greek letters $\alpha, \beta, \gamma, \ldots$ to denote elements of J. We say α divides β if there is a $\gamma \in J$ such that $\alpha\gamma = \beta$. If α divides β and γ, then α divides $\beta + \gamma$ and $\beta - \gamma$. (Even though this is obvious, give a proof of it.)

In I we had two special integers 1 and -1 which divide all integers. We call such an element a <u>unit</u>: a unit is an integer which divides all integers. There are two units in I. What are the units in J?

Let λ be a unit in J. Then λ divides every element of J and, in particular, λ divides 1.

Before going further, we introduce the very convenient notion of <u>norm</u>: if $\alpha \in K$, the norm of α (written $N\alpha$) is merely the product of α by its complex conjugate $\overline{\alpha}$. Writing $\alpha = a + b\sqrt{-5}$, we have $N\alpha = (a+b\sqrt{-5})(a-b\sqrt{-5})$, or

$$N\alpha = a^2 + 5b^2 .$$

In particular, if $\alpha \in J$, we see that $N\alpha$ is a rational integer which, also, is positive. There is no difficulty in checking that

(1) $$N\alpha\beta = N\alpha \cdot N\beta$$

(Do this.)

Let us return to the matter of the units of J. If λ is a unit we have $\lambda\gamma = 1$ for some integer $\gamma \in J$, since we have seen that λ must divide 1. Using (1) we get

$$N\lambda \quad N\gamma = 1 .$$

This shows that $N\lambda = 1$, since any norm of an integer in K is positive. But, putting

$$\lambda = a + b\sqrt{-5}, \text{ we have}$$

$$N\lambda = a^2 + 5b^2 = 1 .$$

The only solutions of this equation in rational integers a, b are $a = \pm 1$, $b = 0$.

What we have proved is that if λ is a unit of J, then $\lambda = \pm 1$. But obviously ± 1 <u>are</u> units of J.

Hence, our result: <u>The units of J are ± 1</u>.

We notice that $N\lambda = 1$ if λ is a unit. The converse is also true: if $N\lambda = 1$, λ is a unit. You will have no difficulty in proving this.

We can now define <u>prime</u>: a prime in J is an element γ of J, not a unit, whose only divisors are ± 1 and $\pm\gamma$. This, of course, agrees with the definition of prime in I.

For example, the integer 3 is a prime in J. Consider a factorization of 3: $3 = \alpha\beta$, where $\alpha \in J$, $\beta \in J$. Then, by (1), $N\alpha\beta = N\alpha \cdot N\beta = N3 = 9$.
Since $N\alpha$ is a positive rational integer, we have $N\alpha = 9, 3,$ or 1. If $N\alpha = 9$, $N\beta = 1$, and β is a unit.
If $N\alpha = a^2 + 5b^2 = 3$, we have a contradiction, because this equation cannot be solved in rational integers. (Prove this.)
If $N\alpha = 1$, α is a unit. Therefore, $3 = \alpha\beta$ implies that either α or β is a unit, which shows that 3 is a prime in J.
In the same way, prove that 7 is a prime in J.

(These statements can be generalized. See if you can prove that any prime rational integer of the form $4n - 1$ is a prime in J. If you have read the Supplement <u>Prime Numbers</u>, you will know that there are infinitely many rational primes of the form $4n - 1$. Conclude, therefore, that <u>here are infinitely many primes in J</u>.)

Besides certain of the rational integers, there are other integers in K which are primes. For example, $4 + \sqrt{-5}$ and $4 - \sqrt{-5}$ are primes. (Prove.) Other examples are $1 + 2\sqrt{-5}$, $2 + 3\sqrt{-5}$, $6 + \sqrt{-5}$.

Of course, the importance of primes is simply that they are the multiplicative building blocks: every rational integer not a unit is a product of primes. (See Chapter 9, Section 3.) Is the same result true in J ? It is.

To prove it, let S be the set of non-units in J which do not have factorizations into primes. If S is empty our result is established, so we assume S is not empty. Let N be the set of positive integers which are the norms of elements of S . Then N is a non-empty set of integers > 1 (because S contains no units); as such it has a least element a (Chapter 9, Section 3). Every element of J whose norm is less than a (and > 1) does not belong to S .

Let α be an element of S such that $N\alpha = a$. Then α has no factorization into primes. If α is prime, we have the trivial factorization $\alpha = \alpha$; hence, α is not prime. It follows that $\alpha = \beta\gamma$, where neither β nor γ is a unit or is $\pm\alpha$. Since $N\alpha = N\beta \cdot N\gamma$, so that $N\beta$ divides $N\alpha$, we have $1 < N\beta < N\alpha$ and also $1 < N\gamma < N\alpha$.

This shows that $\beta \notin S$, for $N\beta < a$. Hence, β has a factorization into primes. By the same reasoning, γ has a factorization into primes. Multiplying these two factorizations together, we see that α has a factorization into primes. This contradiction was obtained on the assumption that S was not empty; hence S is empty and our result is proved.

In the rational field, factorization into primes is <u>unique</u>: no matter how we factorize an integer we always get the same primes, each occurring the same number of times. E.g., $60 = 30 \cdot 2 = 15 \cdot 2 \cdot 2 = 5 \cdot 3 \cdot 2^2$, $60 = 6 \cdot 10 = 2 \cdot 3 \cdot 2 \cdot 5 = 2^2 \cdot 3 \cdot 5$. Only the order in which the factors occur is different. But this is not true in every field.

Consider 21 as an integer in K . We have

(2) $21 = 3 \cdot 7$

$21 = (4 + \sqrt{-5})(4 - \sqrt{-5})$

As we have seen, the integers in the right members are primes in J. Furthermore, they differ by more than just units, i.e., 3 is not equal to any other factor times a unit. Here, then, we have two essentially different factorizations of 21 in J . Factorization into primes in J is not unique.

The central theorem used in the proof of unique factorization in the rational field is the following: if a prime p divides a product ab , then p divides either a or b (or both). This theorem, however, is false in J . For from (2) we deduce that $4 + \sqrt{-5}$ divides $3 \cdot 7$ (since it divides 21), but it does not divide either 3 or 7 . If we assume, e.g., that

$$(4 + \sqrt{-5})\alpha = 7 ,$$

we get, taking norms,

$$21 \cdot N\alpha = N7 = 49 ,$$

so that $N\alpha$ is not a rational integer as it has to be.

Unique factorization can be restored to K by introducing certain new elements called ideals. Every non-unit integer in K is a unique product of prime ideals. You will learn this beautiful theory if you continue your mathematical studies in college.

ANSWERS TO QUESTIONS

Arithmetic Functions I

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

1. No. All other integers will at least be divisible by 1 and the integer itself. Hence the number of divisors will be greater than or equal to 2 .

2, 3, 5, 7, 11, 13, 17, 19, 23, 29.

4, 9, 25 . Yes. They are all perfect squares. Yes. 16. Every number with exactly three divisors is a perfect square.

25 numbers have an even number of divisors. 1, 4, 9, 16, 25 do not.

42. 90.

The 14 numbers 2, 3, 4, 5, 7, 9, 11, 13, 16, 17, 19, 23, 25, 29. They are all primes or powers of a prime. Guess: It must be a power of a prime. 4. 6. 4. 6. n + 1. n + 1. The number of divisors of an integer n is a prime if and only if $n = q^{p-1}$ where both p and q are primes.

n	Number of times n appears as a number of divisors
1	1
2	10
3	3
4	9
5	1
6	4
7	0
8	2

The number of divisors of the integer n is odd if and only if n is a square.

24 and 30 have 8 divisors. Yes. 36 has 9 divisors. Yes. 48 has 10 divisors. No.

60, 72, and 96 all have 12 divisors.

For $n = p_1^{m_1} p_2^{m_2} \ldots p_r^{m_r}$, $r(n) = (m_1 + 1) \cdot (m_2 + 1) \ldots (m_r + 1)$.

12, 18, 20, 28, 32, 44, 45, 52, 63, 68, 75, 76, 92, 99 .

144 .

3. 7. None. At most one. Since $x^k - 1 = (x - 1)$ $(x^{k-1} + \ldots\ldots + 1)$,

if $x > 2$ the number is not a prime.

The first few perfect numbers are 6; 28; 496; 8128; 33,550,336. The first four were known by 100 A.D. Until 1870 only four more had been found. Between 1870 and 1950 four additional ones were found.

n	Divisors of n	$\sigma(n)$	
1	1	1	D
2	1, 2	3	D
3	1, 3	4	D
4	1, 2, 4	7	D
5	1, 5	6	D
6	1, 2, 3, 6	12	P
7	1, 7	8	D
8	1, 2, 4, 8	15	D
9	1, 3, 9	13	D
10	1, 2, 5, 10	18	D
11	1, 11	12	D
12	1, 2, 3, 4, 6, 12	28	A
13	1, 13	14	D
14	1, 2, 7, 14	24	D
15	1, 3, 5, 15	24	D
16	1, 2, 4, 8, 16	31	D
17	1, 17	18	D
18	1, 2, 3, 6, 9, 18	39	A
19	1, 19	20	D
20	1, 2, 4, 5, 10, 20	42	A
21	1, 3, 7, 21	32	D
22	1, 2, 11, 22	36	D
23	1, 23	24	D
24	1, 2, 3, 4, 6, 8, 12, 24	60	A
25	1, 5, 25	31	D
26	1, 2, 13, 26	42	D
27	1, 3, 9, 27	40	D
28	1, 2, 4, 7, 14, 28	56	P
29	1, 29	30	D
30	1, 2, 3, 5, 6, 10, 15, 30	72	A

23 are deficient, 5 are abundant, and 2 are perfect.

If p is a prime $\sigma(n) = p + 1$.

$1, p, p^2, \ldots, p^k$.

$$\frac{p^{k+1} - 1}{p - 1}$$

$1, p, p^2, \ldots, p^k, q, pq, p^2q, \ldots, p^kq$. $2(k + 1)$.

$$(1 + p + p^2 = \ldots + p^k) + q(1 + p + p^2 + \ldots + p^k)$$

$$= (1 + q)(1 + p + \ldots + p^k)$$

$$= (1 + q)\frac{p^{k+1} - 1}{p - 1}$$

$1, p, p^2, \ldots, p^k, q, pq, p^2q, \ldots, p^kq, q^2, pq^2, p^2q^2, \ldots,$
p^kq^2. $3(k + 1)$.

$$(1 + q + q^2)\frac{p^{k+1} - 1}{p - 1} = \frac{q^3 - 1}{q - 1} \cdot \frac{p^{k+1} - 1}{p - 1}.$$

$$\frac{p^{k+1} - 1}{p - 1} \cdot \frac{q^{s+1} - 1}{q - 1}$$

$$\sigma(n) = \frac{p_1^{m_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{m_2+1} - 1}{p_2 - 1} \cdot \ldots \cdot \frac{p_r^{m_r+1} - 1}{p_r - 1}.$$

$6 = 2 \cdot 3$; $\sigma(6) = \frac{2^2 - 1}{2 - 1} \cdot \frac{3^2 - 1}{2 - 1} = 3 \cdot 4 = 12$.

$12 = 2^2 \cdot 3$; $\sigma(12) = \frac{2^3 - 1}{2 - 1} \cdot \frac{3^2 - 1}{3 - 1} = 7 \cdot 4 = 28$.

$18 = 2 \cdot 3^2$; $\sigma(18) = \frac{2^2 - 1}{2 - 1} \cdot \frac{3^3 - 1}{3 - 1} = 3 \cdot 13 = 39$.

$24 = 2^3 \cdot 3$; $\sigma(24) = \frac{2^4 - 1}{2 - 1} \cdot \frac{3^2 - 1}{3 - 1} = 15 \cdot 4 = 60$.

$28 = 2^2 \cdot 7$; $\sigma(28) = \frac{2^3 - 1}{2 - 1} \cdot \frac{7^2 - 1}{7 - 1} = 7 \cdot 8 = 56$.

$30 = 2 \cdot 3 \cdot 5$; $\sigma(30) = \frac{2^2 - 1}{2 - 1} \cdot \frac{3^2 - 1}{3 - 1} \cdot \frac{5^2 - 1}{5 - 1} = 3 \cdot 4 \cdot 6 = 72$.

$144 = 2^4 \cdot 3^2$; $\sigma(144) = \frac{2^5 - 1}{2 - 1} \cdot \frac{3^3 - 1}{3 - 1} = 31 \cdot 13 = 403$.

Arithmetic Functions III

One of any two consecutive integers must be even. Therefore aside from the pair 2 and 3, any other pair of consecutive integers must contain an even integer greater than 2, which is composite.

Exercise 1.

The primes less than 100 are 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97.

Exercise 2.

The twin primes less than 100 are 3, 5; 5, 7; 11, 13; 17, 19; 29, 31; 41, 43; 59, 61; 71, 73.

Exercise 3.

$\pi(10) = 4$, $\pi(20) = 8$, $\pi(30) = 10$, $\pi(40) = 12$, $\pi(50) = 15$, $\pi(75) = 21$, $\pi(100) = 25$.

Exercise 4.

Proof: Suppose n is not prime; then $n = pq$ where p is a prime $1 < p < n$. By hypothesis $p > \sqrt{n}$. But then $q < \sqrt{n}$ (otherwise $n = pq > \sqrt{n} \cdot \sqrt{n} = n$) . Therefore q must $= 1$, since if $q \neq 1$ it has a prime divisor which is $< \sqrt{n}$. Therefore q must $= 1$, since if $q \neq 1$ it has a prime divisor which is $< \sqrt{n}$ and which divides n , contrary to hypothesis. If q must be 1 , then n is prime. q.e.d.

Exercise 5.

$1781 = 13 \cdot 137$; 4079 is prime.

Exercise 6.

The primes greater than 100 and less than 225 are 101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157, 163, 167, 173, 179, 181, 191, 193, 197, 199, 211, 223 .

Exercise 7.

$\pi(150) = 35$; $\pi(225) = 48$.

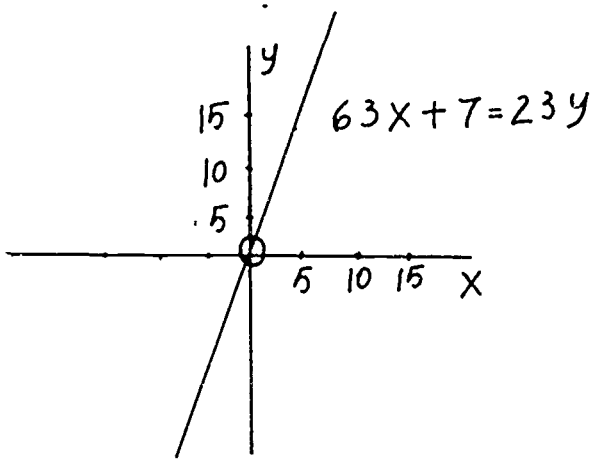
Exercise 8.

$\pi(200) = 46$ and $\pi(100) = 25$. The answer is 21 .

Exercise 9.

$$\frac{\frac{\pi(n)}{n}}{\log n} = \frac{664,580}{10,000,000\,\overline{M}} = \frac{664,580}{\frac{4342945}{7}} = \frac{664,580}{623,278} = 1.07^{-} .$$

$63x + 7 = 23y$



No.

No. $3x + 6y = 3(x + 2y) = 13$. Three does not divide thirteen, so that there are no integers x and y for which this equation is satisfied.

$3x + 6y = 24$. Solutions: (4, 2); (6, 1); (2, 3) . Yes. Three solutions. (2, 3). (6, 1).

$2x - y = 6$. (4, 2) . Yes there are infinitely many. $x = 4 + t$. $y = 2 + 2t$ is a solution for any integer t . Any non-negative t gives a positive solution.

Yes. If the slope, $-a/b$ is positive and there is a solution at all, then there are infinitely many positive solutions. If the slope is negative and there is a positive solution, then there are only finitely many. An equation may have solutions, and yet if the slope is negative it may have no positive solutions. Then of course there may be no solutions in integers at all.

(1), (5), and (6). Yes. Yes. If $ax + by = c$ has a solution in integers, then $(a, b) = d$ divides c .

Proof: Let $a = da'$; $b = db'$. Then $da'x + db'y = c$.

Hence if there is a solution d divides c .

Yes. For (1) . (2, 3) = 1, 1 divides 5 and (1, 1) is a solution.

For (5) . (4, 6) = 2, 2 divides 8 and (2, 0) is a solution.

For (6). $(2, 4) = 2$, 2 divides 4 and $(2, 0)$ is a solution.

Factor each number. Take all prime factors common to both numbers and raise each to the smallest exponent to which it appears in either number

See proof which follows.

Theorem: If d divides a and d divides b , then d divides $a + b$ and $a - b$.

Proof: Let $a = da'$ and $b = db'$. Then $a + b = da' + db' = d(a' + b')$ (Distributive Law). Therefore d divides $a + b$. $a - b = da' - db' = d(a' - b')$ (Distributive Law). Therefore d divides $a - b$.

$253 = 11 \cdot 23$; $122 = 2 \cdot 61$. $(1596, 96) = 12$. $(418, 1376) = 2$. $(365, 146) = 73$.

Yes. Given any positive integers a and b with say, a greater than b , then there always exists integers q_1 and r_1 such that $a = bq_1 + r_1$ with $0 \leq r_1 < b$. Similarly $b = r_1q_2 + r_2$ with $0 \leq r_2 < r_1$. Continuing in this way we have a decreasing sequence of positive integers. There are only $b - 1$ positive integers less than b . So that after at most $b - 1$ steps the remainder must be zero. If a and b aren't positive integers, we can still find their greatest common divisor by using the algorithm on $|a|$ and $|b|$, which are positive.

If x_o and y_o is a solution then $x_o + b$ and $y_o - a$ is also a solution.

General Solution: Suppose x_o and y_o satisfy the equation and suppose x and y are any other solution. Then $ax_o + by_o = c$ and $ax + by = c$.

If we subtract we get $a(x - x_o) + b(y - y_o) = 0$.

$$a(x - x_o) = -b(y - y_o) .$$

Divide by d

$$\frac{a}{d}(x - x_o) = -\frac{b}{d}(y - y_o) .$$

Since a/d and b/d have no common factors, $x - x_o$ must be divisible by $\frac{b}{d}$; let $x - x_o = \frac{b}{d} t$. Then substituting we have $\frac{a}{d} \cdot \frac{b}{d} \cdot t = - \frac{b}{d} (y - y_o)$, and $y - y_o = - \frac{a}{d} t$. Consequently

$$x = x_o + \frac{b}{d} t ,$$

$$y = y_o - \frac{a}{d} t \text{ ; is a solution for every}$$

integer t .

CHECK:

$$a(x_o + \frac{b}{d} t) + b(y_o - \frac{a}{d} t) = c .$$

$$ax_o + by_o + \frac{ab}{d} t - \frac{ab}{d} t = ax_o + by_o = c .$$

Yes, it is clear that any solution must have this form since x and y were assumed to be any solution of the equation and it followed that they had this form for some t .

5. Yes. $x = 5 - 23t$, $y = 14 - 63t$.

Answers to Problems:

1. $x = 3 + 7t$, $y = 79 - 16t$.
2. $x = 170$, $y = 110$; $x = 923$, $y = 9$.
   ($x = 923 + 753t$, $y = 9 - 101t$).
3. 5 and 6 . ($5 + 15t$, $6 + 17t$).
4. 4 . ($9 - 795$, $4 - 37t$).
5. $x = 4 + 45t$, $y = 1 + 14t$.
6. $x = 27 + 63t$, $y = 15 + 40t$.

Gaussian Integers

Exercise 1.

Let the numbers be $a = 2n + 1$ and $b = 2m + 1$.

Then $a^2 + b^2 = (2n + 1)^2 + (2m + 1)^2 = 4(n^2 + m^2 + n + m) + 2$

Therefore for a and b odd, $a^2 + b^2$ leaves a remainder 2 when divided by 4 and consequently is never a multiple of 4.

Exercise 2.

Let the Gaussian integers be $a + bi$ and $c + di$; a, b, c, d rational integers. (1) $(a + bi) \pm (c + di) = (a \pm c) + (b \pm d)i$.

Since $a \pm c$ and $b \pm d$ are rational integers the sum and difference are Gaussian integers.

(2) $(a + bi)(c + di) = (ac - bd) + (ad + bc)i$.

Again since $ac - bd$ and $ad + bc$ are rational integers the product is a Gaussian integer.

Exercise 3.

No. $\frac{2}{3}$ is not a rational integer.

Exercise 4.

No. 2 and 3 are Gaussian integers and $\frac{2}{3}$ is not a Gaussian integer.

Exercise 5.

No The quotient is $\frac{-5}{13} + \frac{12}{13}i$ which is not a Gaussian integer.

Yes. $2 + 3i = i(3 - 2i)$.

Exercise 6.

Yes. $3 + 11i = (2 + 3i)(3 + i)$.

Yes. $3 + 11i = -i(-11 + 3i)$.

Proof of Lemma: $N(\alpha\beta) = N(\alpha)N(\beta)$

Let $\alpha = a + bi$, $\beta = c + di$.

Then $\alpha\beta = (ac - bd) + (ad + bc)i$.

$$N(\alpha\beta) = (ac - bd)^2 + (ad + bc)^2$$
$$= a^2c^2 + b^2d^2 + a^2d^2 + b^2c^2$$
$$= (a^2 + b^2)(c^2 + d^2)$$
$$= N(\alpha)N(\beta).$$

Exercise 7.

If α and β are associates, then $\alpha = \beta \cdot u$, where u is a unit.

Then by the Lemma $N(\alpha) = N(\beta)N(u)$

$= N(\beta) \cdot 1$ since $n(u) = 1$ by Theorem 1.

$= N(\beta)$. q.e.d.

Exercise 8.

No. $5 = (2 + i)(2 - i)$. $N(2 + i) = N(2 - i) = 5$.

Therefore $2 + i$ and $2 - i$ are not units. $N(5) = 25$ and they are not associates of 5 by Exercise 7. Therefore 5 is not a prime, since it has divisors which are neither units nor associates of 5 .

Exercise 9.

Yes. For suppose $3 = \alpha\beta$.

Then $N(3) = N(\alpha)N(\beta) = 9$.

Then $N(\alpha) = 1, 3,$ or 9. If $N(\alpha) = 1$, is a unit.

If $N(\alpha) = 9$, then $N(\beta) = 1$ and β is a unit.

Hence $N(\alpha)$ must be 3 if 3 is not to be a prime.

But $N(\alpha) = a^2 + b^2 = 3$ is impossible for rational integers a and b . Therefore 3 has no divisors except units and associates of 3 and is therefore a Gaussian prime.

Exercise 10.

We consider all possible cases for rational integers x and y.

Case I: x and y both even; let $x = 2x'$, $y = 2y'$.

$x^2 + y^2 = 4(x'^2 + y'^2) \neq 4n + 3$ for any rational integer n .

Case II: x and y both odd; let $x = 2x' + 1$, $y = 2y' + 1$.

$x^2 + y^2 = (2x' + 1)^2 + (2y' + 1)^2$

$= 4(x'^2 + y'^2 + x' + y') + 2 \neq 4n + 3$ for any rational integer n .

Case III: one even and one odd; say $x = 2x'$, $y = 2y' + 1$

$x^2 = y^2 = 4(x'^2 + y'^2 + y') + 1 \neq 4n + 3$ for any rational integer n . Therefore $x^2 + y^2 \neq 4n + 3$ for any integers x and y . q.e.d.

Exercise 11.

Yes Suppose $1 + i = \alpha\beta$

$N(1 + i) = N(\alpha)N(\beta)$

$2 = N(\alpha)N(\beta)$

But since $N(\alpha)$ and $N(\beta)$ are rational integers, one of them is 2 and the other is 1. Suppose $N(\alpha) = 1$; then α is a unit. Therefore $1 + i$ is a prime since it can only be written as a unit times an associate of $1 + i$.

Exercise 12.

Yes. $N(1 - i) = 2$ and we can repeat the same argument given in Exercise 11.

Exercise 13.

No. Since every rational integer is a Gaussian integer, a composite rational integer $a = bc$ has as divisors the Gaussian integers b and c which are not units or associates of a.

Exercise 14.

(a) $5 = 2^2 + 1^2$

(b) $13 = 2^2 + 3^2$

(c) $17 = 4^2 + 1^2$

(d) $29 = 2^2 + 5^2$

(e) $101 = 10^2 + 1^2$

(f) $1721 + 11^2 + 40^2$

Fermat's Method of Infinite Descent

Exercise 1.

$37 = 6^2 + 1^2$; $41 = 5^2 + 4^2$; $89 = 5^2 + 8^2$; $101 = 10^2 + 1^2$.

Exercise 2.

Given: d divides x , d divides z , and $x^2 + y^2 = z^2$.

Show: d divides y .

Let $x = dx'$, $z = dz'$.

$d^2x'^2 + y^2 = d^2z'^2$,

$y^2 = d^2(z'^2 - x'^2)$

Therefore, d^2 divides y^2 and d divides y .

Exercise 3.

If a number is odd its square is odd. If x , y , and z are all odd then $x^2 + y^2$ is even; but $x^2 + y^2 = z^2$ and z^2 is odd. This contradiction shows that not all three numbers can be odd.

Exercise 4.

If a number is even, its square is even; if a number is odd, its square is odd. Consequently, the sum or difference of the squares of two even numbers is an even number and it is impossible, therefore for z^2 to be odd. But if z^2 is even, then so is z .

Exercise 5.

Given: z and y have no common factors; $z + y = 2v^2$; $z - y = 2w^2$.

Show that v and w have no common factors.

Suppose v and w have the common factor $d \neq 1$.

Then adding: $z - y = 2v^2$

$z - y = 2w^2$

$2z = 2(v^2 + w^2)$, $z = v^2 + w^2$;

Subtracting: $2y = 2(v^2 - w^2)$, $y = v^2 - w^2$.

If d divides v and d divides w , then d divides v^2 , $w^2 = z$ and d divides $v^2 - w^2 = y$, contrary to the hypothesis. Therefore v and w have no common factors.

Approximation of Irrationals by Rationals

1. Assume that no box contains more than one object. Then the total number of objects is not more than n. This contradicts the fact that $n + 1$ objects were placed in the boxes.

2. Theorem: If m is a positive integer which is not a perfect square, there is a constant $c > 0$ depending on m such that

$$\left| \sqrt{m} - \frac{p}{q} \right| < \frac{1}{cq^2},$$

no matter what the rational number p/q may be.

Proof: Let r be the integer such that $r - 1 < \sqrt{m} < r$. Note that $r \geq 2$.

Case I. $p/q > \sqrt{m}$.

Then $m^2q - p^2 = (q\sqrt{m} - p)(q\sqrt{m} + p) \geq 1$,

$$\left| \sqrt{m} - \frac{p}{q} \right| \geq \frac{1}{q^2} \frac{1}{\sqrt{m} + \frac{p}{q}} > \frac{1}{q^2} \frac{1}{2\sqrt{m}} > \frac{1}{(2r+1)q^2}.$$

Case II. $\sqrt{m} < p/q < r + 1$.

$$\left| \sqrt{m} - \frac{p}{q} \right| \geq \frac{1}{q^2} \frac{1}{\sqrt{m} + \frac{p}{q}} > \frac{1}{q^2} \frac{1}{r + r + 1} = \frac{1}{(2r + 1)\, q^2}.$$

Case III. $p/q \geq r + 1$.

$$\left| \sqrt{m} - \frac{p}{q} \right| \geq 1 > \frac{1}{(2r + 1)\, q^2},$$

since $\sqrt{m} < r$ while $p/q \geq r + 1$.

Thus, we can take $c = 2r + 1$.

A New Field

1. $(a + b\sqrt{-5}) + (c + d\sqrt{-5}) = (a + c) + (b + d)\sqrt{-5}$
$= a_1 + b_1\sqrt{-5}$

$(a + b\sqrt{-5}) - (c + d\sqrt{-5}) = (a - c) + (b - d)\sqrt{-5}$
$= a_2 + b_2\sqrt{-5}$

$(a + b\sqrt{-5})(c + d\sqrt{-5}) = (ac - 5bd) + (bc + ad)\sqrt{-5}$
$= a_3 + b_3\sqrt{-5}$.

Since a, b, c, d are rational, so are $a_1, b_1, a_2, b_2, a_3, b_3$.

2. Since

$$\frac{a + b\sqrt{-5}}{c + d\sqrt{-5}} = \frac{ac + 5bd + (bc - ad)\sqrt{-5}}{c^2 + 5d^2} = a_1 + b_1\sqrt{-5}$$

when $c + d\sqrt{-5} \neq 0$ (i.e., not both c and d are 0), we have a_1, b_1 are rational since a, b, c, d are.

3. An integer α in R is also an integer in K, since α satisfies the monic equation of smallest possible degree $x - \alpha = 0$. This equation has coefficients in R since α is in R.

4. Write $b = \frac{p}{q}$, where p, q are integers with no common factors (except 1). We have $20b^2 = 5 \cdot 4\, p^2/q^2$ is a rational integer. So q^2 must divide 20 since it has no factors which divide p^2. q^2 cannot divide 5 because 5 has no factors which are squares. Hence, q^2 must divide 4, i.e., $q^2 = 4$. Then $q = 2$; and $2b = 2p/q = p$ is an integer, as claimed.

5. Let α divide β and γ. Then $\beta = \alpha\delta_1$, $\gamma = \alpha\delta_2$. So $\beta + \gamma = \alpha\delta_1 + \alpha\delta_2 = \alpha(\delta_1 + \delta_2)$. Hence, α divides $\beta + \gamma$. Similarly, α divides $\beta - \gamma$

6. Use the theorem (Chapter 5, Section 5) that the conjugate of a product of complex numbers is the product of the conjugates: $N(\alpha\beta) = (\alpha\beta)(\bar{\alpha}\bar{\beta}) = (\alpha\beta)(\bar{\alpha}\bar{\beta}) = (\alpha\bar{\alpha})(\beta\bar{\beta}) = N\alpha\, N\beta$.

7. If $n\lambda = 1$, $\lambda = a + b\sqrt{-5}$, we have $a^2 + 5b^2 = 1$, the only solutions of which in rational integers are $a = \pm 1$, $b = 0$. Thus $\lambda = \pm 1$, so λ is a unit.

8. Since a, b are rational integers, we have $a^2 + 5b^2 \geq 5b^2 \geq 3$ if $b \neq 0$. Therefore, $b = 0$. Hence, $a^2 = 3$, which is impossible.

9. Let p be a rational prime of the form $4n - 1$, and consider the factorization $p = \alpha\beta$, where α, $\beta \in J$. Taking norms we get $p^2 = N\alpha \cdot N\beta$. Since $N\alpha$ is a rational integer, we have either $N\alpha = p^2$, p, or 1. In the first case we have $N\beta = 1$, so β is a unit; in the last case, α is a unit. Consider $N\alpha = p$ and let $\alpha = a + b\sqrt{-5}$. This gives $a^2 + 5b^2 = p$. If a, b are both even, the left member is even. If a, b are both odd, the left member is even, since a^2 and $5b^2$ are both odd. If a is even, b odd, or if a is odd, b even, the left member is of the form $4n + 1$. Hence, it is impossible that $n\alpha = p$. Thus the factorization $p = \alpha\beta$ is possible only if α or β is a unit in J.

10. If $4 + \sqrt{-5} = \alpha\beta$, we have $21 = N\alpha \cdot N\beta$. Now $N\alpha \neq 3$ or 7, for as we just saw, $N\alpha = p$ is impossible when p is of the form $4n - 1$. Therefore $N\alpha = 1$ or $N\beta = 1$, so that either α or β are units. Same proof for $4 - \sqrt{-5}$.

1, 2, 4, 8, 9, 16, 18, 25 . They are either a square or twice a square. If $\sigma(n)$ is odd, then n is a square or twice a square.

Proof:

Given: $\sigma(n) = \frac{p_1^{m_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{m_2+1} - 1}{p_2 - 1} \cdot \ldots \cdot \frac{p_r^{m_r+1} - 1}{p_r - 1}$ odd.

Then each factor of the product must be odd.

If $p_1 = 2$; then m_1 may be any integer ≥ 0 .

If p_i is odd, all the powers of p_i will be odd. Since $1 + p_i + p_i^2 + \ldots + p_i^{m_i}$ must be odd, then m_i+1 must be odd; i.e., m_i is even. Let $m_i = 2t_i$.

Then n has the form $n = 2^{m_1} p_2^{2t_2} p_3^{2t_3} \ldots p_r^{2t_r}$ and we may write

$$n = \begin{cases} 2\left(2^{\frac{m_1-1}{2}} p_2^{t_2} p_3^{t_3} \ldots p_r^{t_r}\right)^2 & \text{if } m_1 \text{ is odd} \\ \left(2^{\frac{m_1}{2}-1} p_2^{t_2} p_3^{t_3} \ldots p_r^{t_r}\right)^2 & \text{if } m_1 \text{ is even.} \end{cases}$$

q.e.d.

In the second case n is clearly a square. In the first case n is twice a square.

If $n = 2^{m-1}(2^m-1)$ and 2^m-1 is a prime, then n is a perfect number.

Proof:

We need only show that $\sigma(n) = 2n$. The prime divisors of n are 2 and 2^m-1 . We can make this statement only because we are given that 2^m-1 is a prime.

Then $\sigma(n) = \frac{2^m-1}{2-1} \quad \frac{(2^m-1)^2 - 1}{(2^m-1) - 1} =$

$$(2^m-1) \cdot \frac{\{(2^m-1) + 1\} \cdot \{(2^m-1) - 1\}}{\{(2^m-1) - 1\}} =$$

$$(2^m-1)\ (2^m-1+1) = 2^m(2^m-1) = 2n\ .$$

If $m = 6$, 2^m-1 is not a prime.

If $m = 7$, 2^m-1 is a prime.

If $m = 8$, 2^m-1 is not a prime.

If $m = 9$, 2^m-1 is not a prime.

If $m = 10$, 2^m-1 is not a prime.

If $m = 11$, 2^m-1 is not a prime.

If $m = 12$, 2^m-1 is not a prime.

If $m = 13$, 2^m-1 is a prime.

If m is not prime, then 2^m-1 is not prime either.

Proof: Since m is not prime, let $m = m_1 \cdot m_2$, where m_1 and m_2 are greater than 1.

Then $2^m-1 = 2^{m_1 m_2}-1 = (2^{m_1})^{m_2}-1 = (2^{m_1}-1)\ \{(2^{m_1})^{m_2-1} + (2^{m_1})^{m_2-2} + \ldots + 2^{m_1} + 1\}$.

Since $2^{m_1} \geq 4$, $2^{m_1}-1 \geq 3$ and 2^m-1 is not a prime. q.e.d.

Every even perfect number has the form $2^{m-1}(a^m-1)$ where 2^m-1 is a prime.

Proof:

(Lemma: $\sigma(m \cdot n) = \sigma(m) \cdot \sigma(n)$. To prove this, one only needs to write out the expressions for $\sigma(m \cdot n)$, $\sigma(m)$, and $\sigma(n)$ and verify that $\sigma(mn) = \sigma(m) \cdot \sigma(n)$.)

Let $n = 2^m q$, where q is odd. Since n is perfect

(1) $\sigma(n) = 2(n) = 2^{m+1}q$.

But by the lemma, $\sigma(n) = \sigma(2^m)\ \sigma(q)$. Substituting in (1) we have

(2) $\sigma(2^m)\ \sigma(q) = 2^{m+1}q$

Now $\sigma(2^m) = 2^{m+1}-1$. Substituting in (2) we have

(3) $(2^{m+1}-1)\ \sigma(q) = 2^{m+1}q$.

From (3) we see that $2^{m+1}-1$ divides q . Suppose we set $q = (2^{m+1}-1)q'$.

On the right hand side of (3) replace q by $(2^{m+1}-1)q'$, and dividing both sides by $(2^{m+1}-1)$ we have

(4) $\sigma(q) = 2^{m+1}q$. But q and q' are divisors of q and $q + q' = q' \cdot 2^{m+1} = \sigma(q)$. Hence these are the only divisors of q and q must be a prime and q' must be 1 . Therefore $q = 2^{m+1}-1$ and q is a prime. But then

$$n = 2^m(2^{m+1}-1) \quad \text{q.e.d.}$$

Let the divisors of n be $d_1 , d_2 , \ldots , d_k$.

Then $\frac{1}{d_1} + \frac{1}{d_2} + \ldots + \frac{1}{d_k} = \frac{d'_1 + d'_2 + \ldots + d'_k}{n}$

$$\frac{\sigma(n)}{n} = 2$$

Since n is perfect. (It should be shown that all d'_i are distinct and actually include all divisors of n and each only once.)

Another way of stating this result is:

$$\sigma_{-1}(n) = \frac{\sigma_1(n)}{n} .$$

In fact a more general result holds: $\sigma_{-\ell}(n) = \frac{\sigma_\ell(n)}{n^\ell}$.

$$\sigma_k(n) = \frac{p_1^{k(m_1+1)}-1}{p_1^k - 1} \cdot \frac{p_2^{k(m_2+1)}-1}{p_2^k - 1} \cdots \frac{p_r^{k(m_r+1)}-1}{p_r^k - 1} .$$