DOCUMENT RESUME

ED 143 523 SE 023 001

| | |
|---|---|
| TITLE | Essays on Number Theory I. |
| INSTITUTION | Stanford Univ., Calif. School Mathematics Study Group. |
| SPONS AGENCY | National Science Foundation, Washington, D.C. |
| PUB DATE | 60 |
| NOTE | 39p.; For related document, see SE 023 002 |
| EDRS PRICE | MF-$0.83 HC-$2.06 Plus Postage. |
| DESCRIPTORS | Algebra; *Instructional Materials; *Number Concepts; Secondary Education; *Secondary School Mathematics |
| IDENTIFIERS | *School Mathematics Study Group |

ABSTRACT

Not all of mathematics can be taught in formal textbooks. Just as an English course can be enlivened by selections from literature, a mathematics course can gain depth and interest from special readings. This volume can be read in conjunction with the SMSG First Course in Algebra or Intermediate Mathematics. It introduces the subject of number theory. Included are selections on (1) prime numbers, (2) congruence, and (3) the fundamental theorem of arithmetic. A section containing answers to questions completes the publication. (Author/RH)

**SCHOOL MATHEMATICS STUDY GROUP**

# ESSAYS ON NUMBER THEORY I



SMSG

SCHOOL
MATHEMATICS
STUDY GROUP

# ESSAYS ON NUMBER THEORY I

*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

Not all of mathematics can (or should) be taught in formal textbooks. Just as an English course is enlivened by selections from literature, a mathematics course can gain depth and interest from special readings.

The present volume might be read in conjunction with the SMSG First Course in Algebra or Intermediate Mathematics. It introduces the subject of number theory, a branch of mathematics highly esteemed for its naturalness, conceptual clarity, and elegance. We hope that these essays will prove enjoyable and stimulating.

## 1. PRIME NUMBERS

Among the natural numbers are the prime numbers: a positive integer is called a prime if it has no divisors except 1 and itself. Thus 6 is not a prime, for it has the divisor 2, and 2 is different from both 1 and 6. We call 6 a composite number. But 7 is a prime, because its only divisors are 1 and 7. By agreement we shall not count the integer 1 among either the primes or the composite integers. Thus every integer greater than 1 is either prime or composite.

If a number is composite, it has a prime divisor (that is, a divisor which is prime). For you have seen in this course or in an earlier course that every integer greater than 1 can be written as a product of prime factors. Obviously each prime in the product is a divisor of the integer in question.

The smallest prime is 2; it is also the only prime which is an even integer. No larger even number can be prime for it has 2 as a divisor. If we write down the primes in the order of increasing size, we get

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, ....

The dots at the end mean that there are still larger primes. How large do the primes get? You can probably find a prime larger than 100, but could you find one larger than 1,000,000?

(How would you go about finding a prime larger than 100? If you test a given number, 101 say, by dividing it in succession by various numbers, would you have to try all integers less than 101 as possible divisors? Or would it be sufficient to try all primes less than 101? If so, wouldn't it be enough to try all primes less than $\sqrt{101}$? See if you can prove that if an integer n has a proper divisor, it has a proper divisor which is not more than $\sqrt{n}$.)

To put the question in another way, are there a finite number of primes or are there infinitely many? If you think this over a bit, you will probably find it impossible to think of any way to attack the problem. Yet the answer was known to the Greeks! In fact, we find the proof that there are infinitely many primes in Euclid's Elements.

This proof is a proof by contradiction: suppose there were only n primes, say $p_1, p_2, \ldots, p_n$, where n is a certain integer. Now let

$$A = p_1 p_2 p_3 \cdots p_n + 1,$$

that is, A is the integer obtained by multiplying together all the primes and adding 1 to the result.

Now A is either prime or composite. If A is prime, we have a contradiction since A is not one of the primes $p_1, p_2, \ldots, p_n$ (Why?), and these were supposed to be all the primes.

The other possibility is that A is composite. In that case A is divisible by a prime; call it p. Could p be equal to $p_1$? Certainly not, for if we divide A by $p_1$ we get a remainder of 1, since $p_1$ certainly divides the product $p_1 p_2 \cdots p_n$. Since p divides A, p cannot be $p_1$. In the same way, p could not be

$p_2$, $p_3$, or any of the primes in the set $p_1, p_2, \ldots, p_n$. Again we have a contradiction, namely, we assumed that $p_1, p_2, \ldots, p_n$ were all the primes; but here is a number $p$, undoubtedly a prime, which is not one of $p_1, p_2, \ldots, p_n$.

So whether $A$ is prime or composite (and these are the only possibilities) we arrive at a contradiction to our original assumption that there are only a finite number of primes. Therefore, this assumption must be false, and we have proved the theorem.

THEOREM. There are infinitely many primes.

Although this proof is an example of an "indirect proof", it can be turned around to make a direct proof. What we have actually shown is that if we have any set of primes $\{p_1, p_2, \ldots, p_n\}$, there is a prime $p$ which is not in the set and which is not more than $A$. For example, suppose we know that 2, 3, 5, are primes. Then our proof shows that there is a prime $p$ which is not either 2, 3 or 5 (and so is greater than 5) and $p \leq 2 \cdot 3 \cdot 5 + 1 = 31$. So there is a prime larger than 5 but not larger than 31. Actually, of course, there are several primes between 5 and 31. Our proof, then, does this: given any set of primes, it gives a limit below which there must be a new prime. In this way we can produce in succession an indefinite number of primes.

There are a very large number of fascinating questions having to do with primes. Although most of these are quite easy to state, the answers to many are not known. For example, it was conjectured that every even number greater than 2 is the sum of two primes (examples: $10 = 3 + 7$, $46 = 23 + 23$, $100 = 47 + 53$). This is called the Goldbach conjecture, after the name of the man who first

proposed the problem in 1742. It has never been proved or disproved.

However, there are some questions about primes that we can answer. Suppose we write down the sequence of positive integers for the form $4k - 1$:

3, 7, 11, 15, 19, ... .

Are there an infinite number of primes in this sequence?

(By an integer of the form $4k - 1$, we mean an integer which is equal to $4k - 1$ if we chose the right integer $k$. Thus $3 = 4 \cdot 1 - 1$, $27 = 4 \cdot 7 - 1$, and so on. Of course, the value of $k$ is different in each case.)

Before we discuss this question, let us notice a few things about odd numbers. Every odd number is either of the form $4k + 1$ or $4k - 1$. (Can you prove this?) Furthermore, if you multiply two numbers of the form $4k + 1$, the product is also of the form $4k + 1$. (Check this.) Naturally, if you multiply any finite number of integers of the form $4k + 1$, the product is still of this form, because you could multiply the first two integers, then multiply the result by the third integer, than multiply this result by the fourth integer, and so on.

Now suppose $A$ is an integer of the form $4k - 1$, then we can conclude that $A$ has at least one prime divisor of the form $4k - 1$. For example, 19 is already prime, while 27 has the prime divisor 3. (Prove this in the general case by assuming that all prime divisors are of the form $4k + 1$ and arriving at a contradiction. Notice that $A$ has only odd divisors.)

Now we can return to the original question: are there infinitely many primes of the form $4k - 1$? Suppose there are only a

finite number of such primes; call them $p_1, p_2, \ldots, p_n$. Let

(*) $$A = 4(p_1 p_2 \ldots p_n) - 1.$$

Notice that A is of the form $4k - 1$.

We follow the proof of the previous theorem. A is either prime or composite. If A is prime, we have a contradiction, for A is then a prime of the form $4k - 1$ but A is not one of the primes $p_1, p_2, \ldots, p_n$. The only other possibility is that A is composite. Since A is of the form $4k - 1$, A must have a prime divisor p of the form $4k - 1$, as we have just seen. But p is not one of the primes $p_1, p_2, \ldots, p_n$, for p divides A whereas no $p_i$ divides A.

So whether A is prime or composite, there is a prime of the form $4k - 1$ which is not one of the primes $p_1, p_2, \ldots, p_n$. This is the contradiction we were looking for, and we have proved the following result.

THEOREM. <u>There are infinitely many primes of the form $4k - 1$</u>.

See if you can construct a similar proof that there are infinitely many primes of the form $6k - 1$.

Actually, it is true that there are infinitely many primes of the form $ak + b$, where a and b are any integers which have no common divisor (except 1). (For instance, there are infinitely many primes of the form $5k + 3$.) The proof of this, however, is very difficult. The first proof was given by P. G. L. Dirichlet (1805 - 1859), a famous German mathematician.

Notice that we did not try to prove the above results by looking for a <u>formula</u> for the $n^{th}$ prime. Such a formula, if it exists, would be highly complicated, because the distribution of

primes among the integers is so irregular. As an example of this irregularity, we prove:

THEOREM. There are arbitrarily long sequences of consecutive composite integers.

For example, there are 50 consecutive integers all of which are composite. We can actually exhibit such a consequence.

First, we introduce a new notation: $1! = 1$, $2! = 1 \cdot 2$, $3! = 1 \cdot 2 \cdot 3$, etc. In general, $n!$ (read "n factorial") is the product of all the integers from 1 to $n$, inclusive. Now we consider the sequence

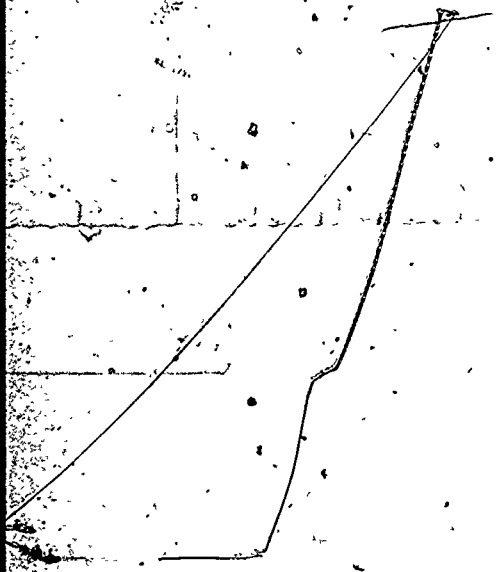
$$51! + 2,\ 51! + 3,\ 51! + 4,\ \ldots,\ 51! + 51.$$

There are 50 consecutive integers in this sequence. The first, $51! + 2$, is divisible by 2, since $51!$ is and 2 is, and the sum of two integers divisible by 2 is again divisible by 2. The second number, $51! + 3$, is divisible by 3, for the same reason. In general, $51! + k$ is divisible by $k$ as long as $k$ is not more than 51. So every integer in the sequence is composite. You can easily see how to modify this proof if you want a block of length $n$ instead of length 50.

We have seen that consecutive primes can be far apart; can they be close together? 2 and 3 are consecutive primes that differ by 1, but obviously there are no other such pairs, for if $p$ is an odd prime, $p + 1$ is even and greater than 2 and so is not a prime. The next possibility is that consecutive primes differ by 2, and there are many examples of such "prime twins": (3,5), (5,7), (17,19), (29,31). But are there infinitely many such pairs? No one knows, although many famous mathematicians have exerted

themselves trying to find out. What is your guess?

Finally, we might consider "prime triples", like 3,5,7. Are there any other prime triples? See if you can prove it one way or the other.



## 2. CONGRUENCES

In many situations in mathematics, what is important is not the particular value of an integer but the fact that it differs from another number by a multiple of 2 or a multiple of 5 or a multiple of some other number. For example, odd numbers are those which differ from 1 by a multiple of 2, squares of odd numbers differ from 1 by a multiple of 8, etc. The same thing happens in ordinary life. What can be said about two times which read the same on the clock? About two dates which have the same month and day but are in consecutive years?

Two numbers which differ by a multiple of 2 are said to be congruent modulo 2. We make the formal definition:

DEFINITION. Two integers $a, b$ are said to be congruent modulo $m$ (where $m$ is a positive integer) if and only if $a - b$ is divisible by $m$.

We write

$$a \equiv b \pmod{m}$$

to indicate that $a$ and $b$ are congruent modulo m. In particular, $a \equiv 0 \pmod{m}$ means that $m$ divides $a$ and conversely. $m$ is called the modulus of the congruence.

Congruence is a relation between the integers a and b (with respect to the modulus m). Many of the properties of the more familiar relation of equality carry over to congruences.

Exercise 1. Prove that

$a \equiv a \pmod{m}$

if $a \equiv b \pmod{m}$, then $b \equiv a \pmod{m}$

if $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $a \equiv c \pmod{m}$.

Congruences can be added, subtracted, and multiplied like ordinary equations. Thus,

if $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then

$$\begin{aligned} a + c &\equiv b + d \pmod{m} \\ a - c &\equiv b - d \pmod{m} \\ ac &\equiv bd \pmod{m} \end{aligned} \tag{1}$$

For $(a+c) - (b+d) = (a-b) + (c-d)$ and each term in the right member is divisible by m, hence the right member is also. Similarly for the second congruence. Finally, $ac - bd = (a-b)c + (c-d)b$. Since m divides $a-b$, it divides $(a-b)c$; for the same reason, m divides $(c-d)b$. This establishes the third congruence above.

Using (1) we can answer questions such as: is $2^{32} + 1$ a prime? (A prime is an integer > 1 which has no factors except 1 and itself.) This number is of some historical interest, for Fermat stated that all numbers of the form $2^{2^n} + 1$ are primes, whereas Euler showed that $2^{32} + 1$ (i.e. $n = 5$) is divisible by 641. We can easily prove Euler's result by means of congruences without expanding this very large number and dividing it by 641.

Namely, we have:

$2^2 \equiv 4 \pmod{641}$, $2^4 \equiv 16 \pmod{641}$,

$2^8 \equiv 256 \pmod{641}$, $2^{16} \equiv (256^2) = 65536 \equiv 154 \pmod{641}$,

$2^{32} \equiv (154)^2 = 23716 \equiv 640 \pmod{641}$.

Each congruence is obtained from the preceding one by multiplying it by itself. The largest number we had to calculate was $(256)^2$. From the last congruence we get

$$2^{32} + 1 \equiv 641 \equiv 0 \pmod{641},$$

as promised.

Another thing we can do easily by means of congruence is to prove the familiar rule for "casting out nines". Let $N$ be a positive integer and write it in the base 10:

$$N = a_0 + 10a_1 + 10^2a_2 + \ldots + 10^ka_k.$$

(The digits of $N$ are therefore $a_0, a_1, \ldots, a_k$.)

Since $10 \equiv 1 \pmod{9}$, we have $10^2 \equiv 1^2 = 1 \pmod{9}$, and, in general, $10^r \equiv 1 \pmod{9}$. Hence, using the first equation of (1), we get

$$(2) \quad N \equiv a_0 + a_1 + a_2 + \ldots + a_k \pmod{9}.$$

Now $N$ is divisible by 9 if and only if $N \equiv 0 \pmod{9}$, which, according to (2), occurs if and only if the sum of the digits $a_0 + a_1 + \ldots + a_k \equiv 0 \pmod{9}$.

Exercise 2. Prove that an integer is divisible by 3 if and only if the sum of its digits is divisible by 3.

Exercise 3. Prove that an integer is divisible by 11 if and only if the sum of the digits in the "odd places" is congruent modulo 11 to the sum of the digits in the "even places". By "odd places" we mean the units place, the hundreds place, etc.

Exercise 4. Prove that a number is divisible by 4 if and only if the part of the number occupying the units and tens places is divisible by 4.

In arithmetic we have the cancellation law: if $ab = ac$ and $a \neq 0$ then $b = c$. What is the analogue for congruences?

Suppose we have $ab \equiv ac \pmod{m}$, which is the same thing as

$$a(b-c) \equiv 0 \pmod{m}.$$

It does not follow that $m|a$ or $m|(b-c)$. For some of the prime factors of $m$ might divide $a$ and the remaining prime factors divide $b - c$. However, if $m$ is prime to $a$ (i.e., $m$ and $a$ have no common divisors other than 1), then $m|(b-c)$. This is a consequence of the theorem: if $m|xy$ and $m$ is prime to $x$, then $m|y$. For a proof see the Supplement The Fundamental Theorem of Arithmetic. So we have the result:

Theorem 1. If $ab \equiv ac \pmod{m}$ and $m$ is prime to $a$, then $b \equiv c \pmod{m}$. In other words, we can cancel a common factor from a congruence provided the common factor is prime to the modulus.

The equation $ax = b$, where $a, b, x$ are integers, cannot be solved for $x$ unless $a$ happens to divide $b$. By contrast, the congruence $ax \equiv b \pmod{m}$ can always be solved for $x$ provided only that $(a,m) = 1$. We shall now show how this comes about.

The numbers 0, 7, 35, -14 are mutually congruent modulo 7 (that is, any pair of the numbers is congruent). Likewise: 2, -5, 16, -47 are congruent modulo 7. Consider the set of all integers congruent a fixed integer modulo 7; this set is called a residue class modulo 7. For example, the numbers congruent to 0 modulo 7 form one residue class $R_0$; the numbers congruent to 1

modulo 7 form another residue class $R_1$. $R_0$ and $R_1$ have no common elements, for if an integer $a \equiv 0$ and $a \equiv 1$, then $0 \equiv 1 \pmod 7$, by Exercise 1. Consider the residue classes $R_0$, $R_1$, $R_2$, ..., $R_6$. ($R_1$ is the set of numbers $\equiv 1 \pmod 7$.) Every integer $n$ is in one of these classes. For we can write $n = 7q + i$ where $0 \leq i \leq 6$. Then $n \in R_i$. (This explains the word "residue", which means remainder.) In this way, the set of integers is partitioned into 7 sets, the residue classes modulo 7, no two of which contain common elements.

Of course, there was nothing special about the choice of the modulus 7 in the above discussion. We have, in fact, the general result: Let $m$ be an integer $> 1$, and $R_i$ ($i = 0, 1, \ldots, m-1$) the set of integers which are congruent to $i$ modulo $m$. Every integer $n$ is an element of $R_i$ for some $i$. Moreover, $R_i$ and $R_j$ have no common elements if $i \neq j$. Finally, $n \in R_i$ if and only if $n = qm + i$ for some $q$.

The set $(0, 1, 2, \ldots, m-1)$ is called a complete residue system.

DEFINITION. A complete residue system modulo $m$ ($m > 1$) is a set which contains one and only one element from each residue class $R_i$ ($i = 0, 1, 2, \ldots, m-1$). Thus $(m, m + 2, 2 - m, 3, 4, \ldots, m - 2, -1)$ is another complete residue system. No complete residue system can have fewer than $m$ elements, for it must contain an element congruent to $0, 1, 2, \ldots, m-1$. Nor can it have more than $m$ elements. For if we distribute the $r > m$ elements among the $m$ residue classes, one class is bound to have at least two elements. We see, therefore, that a complete residue system modulo $m$ is a

set of m mutually incongruent integers, and conversely.

Certain complete residue systems are of particular interest.

Theorem 2. If a is prime to m, then S = (a, 2a, ..., ma) is a complete residue system modulo m.

Proof. S certainly contains m numbers. Suppose two of them were congruent, $ra \equiv sa \pmod{m}$. Since (a,m) = 1, we have, by Theorem 1, $r \equiv s \pmod{m}$. But $1 \leq r \leq m$, $1 \leq s \leq m$, so that $0 \leq |r - s| < m$. Hence, $m|(r - s)$ only if $r - s = 0$. This shows that no two elements of S are congruent modulo m. Therefore, S is a complete residue system.

Theorem 2 is what we need to discuss the equation.

(3) $ax \equiv b \pmod{m}$, a prime to m.

We look for a solution x.

Since a is prime to m, the set (a, 2a, ..., ma) is a complete residue system and so one of its members ax, say, is congruent to b. This proves that (3) always has a solution in integers.

Theorem 3. The congruence

$ax \equiv b \pmod{m}$, a prime to m in which a,b,m are given, always has an integral solution x.

Of course there are many solutions of (3), for x + m, x + 2m, x - m are solutions if x is a solution. But there is only one solution in any given complete residue system.

Exercise 5. Prove: if (a,m) = 1, there is only one x satisfying $ax \equiv b \pmod{m}$ and $0 \leq x < m$.

In particular, the equation $ax \equiv 1 \pmod{m}$ (a,m) = 1, has a unique solution in the range $1 \leq x < m$. (Why can't x = 0?) The

number $x$ is called the reciprocal of $a$ (mod m) and often written $\bar{a}$; thus, $a\bar{a} \equiv 1 \pmod{m}$. To solve (3), we need only to know $\bar{a}$, for $x = \bar{a}b$ evidently satisfies (3).

The reciprocal of an integer mod m can be found by trial. A way which is sometimes quicker is provided, for m a prime, by the following theorem, which is important in its own right.

FERMAT'S LITTLE THEOREM. If $p$ is prime, then

$$a^p \equiv a \pmod{p},$$

To prove this, notice first that if $p|a$, the result is trivial, since $a^p - a = a(a^{p-1} - 1)$ is evidently divisible by $p$. But if $p \nmid a$, we can cancel the factor $a$ and get

$$(4) \qquad a^{p-1} \equiv 1 \pmod{p}, \quad (a,p) = 1$$

as the congruence we have to prove. Again we use Theorem 2. Since $S = (a, 2a, \ldots, pa)$ is a complete residue system as well as $T = (1, 2, 3, \ldots, p)$, each element of $S$ must be congruent to some element of $T$ and conversely. Now $pa \equiv p \pmod{p}$. Hence, the product of all the elements of $S$ other than $pa$ is congruent to the product of all the elements of $T$ other than $p$:

$$(5) \qquad a \cdot 2a \ldots (p-1)a \equiv 1 \cdot 2 \ldots (p-1) \pmod{p}.$$

But the left member has $p - 1$ factors and equals $a^{p-1} \cdot 1 \cdot 2 \ldots (p-1)$. Cancelling the factor $1 \cdot 2 \ldots (p-1)$, which is prime to $p$, from both members of (5), we get (4). This completes the proof of Fermat's theorem.

We can use this theorem to calculate the reciprocal of a number to a prime modulus. Clearly $\bar{a} \equiv a^{p-2}$ if $(a,p) = 1$, for

$$a\bar{a} \equiv aa^{p-2} = a^{p-1} \equiv 1 \pmod{p}.$$

Example 1. Solve $4x \equiv 7 \pmod{13}$. First calculate $\bar{4}$. Since 13

is a prime and $(4, 13) = 1$, we have $\overline{4} \equiv 4^{11}$. Now $4^2 = 16 \equiv 3$, $4^4 \equiv 9 \equiv -4$, $4^8 \equiv 16 \equiv 3$, $4^3 \equiv 3 \cdot 4 \equiv -1$.

Hence, $\overline{4} \equiv 4^8 \cdot 4^3 \equiv 3 \cdot -1 \equiv 10 \pmod{13}$. Finally, $x \equiv \overline{4} \cdot 7 \equiv 10 \cdot 7 \equiv 5 \pmod{13}$. Check: $4 \cdot 5 = 20 \equiv 7 \pmod{13}$.

The preceding discussion can be applied to the solution in integers of equations like

$$4x + 13y = 35. \tag{6}$$

Since this is a single equation in two variables, we see that there are infinitely many solutions if there is one solution. For if $x_o$, $y_o$ is one solution, then certainly $x_o + 13t$, $y_o - 4t$ is also a solution if $t$ is any integer. (Check this by substitution.) Equations of this type are called Diophantine equations after the Greek mathematician Diophantus who studied them. Such an equation arises, e.g., from the problem: in how many ways can you make change for a dollar using only nickels and dimes? The equation is $5x + 10y = 100$, with the restriction $x \geq 0$, $y \geq 0$.

We can solve (6) as follows. If $x$ and $y$ are integers which satisfy (6), then

$$4x - 35 = 13y \quad \text{and}$$

$$4x \equiv 35 \pmod{13}.$$

Since $\overline{4} \bmod 13$ is 10, as we saw in Example 1, we have $x \equiv 35 \cdot 10 \equiv -4 \cdot -3 \equiv -1 \pmod{13}$. Hence $x$ is of the form $13t - 1$ where $t$ is an integer; write

$$x = 13t - 1.$$

Substituting this in (6) gives

$$y = \frac{35 - 4x}{13} = \frac{35 - 4(13t - 1)}{13} = 3 - 4t.$$

Thus ($x = -1 + 13t$, $y = 3 - 4t$) is a set solutions of (6) for each integer t. For instance, (-1, 3), (12, -1), (168, - 49) are solutions obtained by taking $t = 0, 1, 13$ respectively. Notice that there are no positive solutions (i.e., solutions in which x and y are both positive).

Exercise 6. In how many ways can a total weight of 25 pounds be built up out of 2-pound and 3-pound weights?

In the general case

(3a) $$ax + by = c,$$

we assume a prime to b. Then we solve the congruence $ax \equiv c \pmod{b}$ which is possible by Theorem 3. Let $x \equiv x_0 \pmod{b}$, then $x = x_0 + b\,t$. Substituting in (3a), we find $y = (c - ax_0)/b - at$. Note that $(c - ax_0)/b$ is an integer since $ax_0 \equiv c \pmod{b}$. For reasons of space, we do not complete the discussion by considering the generalization of Fermat's theorem to the case in which the modulus is not a prime, nor do we treat congruences $ax \equiv b \pmod{m}$ where a is not prime to m, or the corresponding Diophantine equation $ax + by = c$ where a and b are not relatively prime. For these matters and many other fascinating topics, the reader is referred to books on Number Theory such as:

Uspensky and Heaslet, Elementary Number Theory (McGraw-Hill).

## 3. THE FUNDAMENTAL THEOREM OF ARITHMETIC

One of the first steps in your study of algebra was to extend the system of integers to the larger system of rational numbers. The purpose of this step was to make division possible in all cases: the equation $a = bx$, where $a$ and $b$ are rational numbers and $b \neq 0$, always has a solution $x$ which is rational. By the same token, if we stay within the set of integers, division is not always possible: given integers $a$ and $b \neq 0$, sometimes there is an integer $c$ such that $a = bc$, sometimes not. In the first case we say that $b$ divides $a$, or $b$ is a divisor of $a$, or $a$ is divisible by $b$. We write $b \mid a$ for "b divides a" (notice that the bar, $\mid$, is vertical, not slanting).

The study of the properties of integers is called Arithmetic. In this Supplement we shall study the important property of divisibility. Throughout, the letters of the alphabet shall stand for integers.

Certain simple facts are observed at once and easily proved. We leave these as exercises.

Exercise 1. Prove: if $a \mid b$, $a \mid c$, then $a \mid (b+c)$, $a \mid (b-c)$, and $a \mid bf$, where $f$ is any integer.

Exercise 2. Prove: if $a \mid b$, then $a \mid (-b)$ and $(-a) \mid b$.

An important tool in the study of divisibility is the so-called division algorithm.

DIVISION ALGORITHM. If $a$, $b$ are positive integers then

(1a) $$a = qb + r,$$

where

(1b) $$0 \leq r < b.$$

The integers $q$ and $r$ are uniquely determined.

The division algorithm merely states the familiar fact that when two integers are divided in the usual way we get a quotient and remainder and that the remainder is less than the divisor. We have stated the algorithm only for $a$, $b$ positive but it actually holds for all $a$, $b$ provided $b \neq 0$.

To give a formal proof of the Division Algorithm as stated above, consider the multiples $0b$, $b$, $2b$, ... of $b$. Since $0b = 0 < a$ but $kb > a$ for some positive integer $k$, there must be a largest integer $q$ such that $qb \leq a$. Set $a - qb = r$. ($q$ is the "quotient," $r$ the "remainder.") First, $r \geq 0$. Next, if $r \geq b$ we would have $a - (q+1)b = a - qb - b = r - b \geq 0$, i.e., $(q+1)b \leq a$, so $qb$ was not the largest multiple of $b$ which is $\leq a$. Therefore, $r < b$, and we have proved equation (1).

Notice that if $b > a$, we have $q = 0$, $r = a < b$ : $a = 0 \cdot b + a$.

We still have to show that $q$ and $r$ are unique. Suppose we could have

(2) $$a = q_1 b + r_1 = q_2 b + r_2, \quad 0 \leq r_1 < b, \quad 0 \leq r_2 < b.$$

If $q_1 > q_2$, we get $q_1 \geq q_2 + 1$ and

$$a = q_1 b + r \geq (q_2+1)b + r_1 > q_2 b + r_2 + r_1 \geq q_2 b + r_2 = a,$$

so that $a > a$, a contradiction. So $q_1 \leq q_2$. By interchanging $q_1$ and $q_2$, we conclude $q_2 \leq q_1$. Therefore, $q_1 = q_2$. Subtracting $q_1 b = q_2 b$ from (2) gives $r_1 = r_2$. Hence, q and r are unique.

Interest next centers on the common divisors of two integers. Since $-d$ is a divisor whenever $d$ is, and only then, we may as well consider only positive divisors. For example, 8 and 12 have the common divisors 1, 2, 4; 4 and 9, however, have no common divisor other than 1. We say that 4 and 9 are relatively prime or that 4 is prime to 9. We call 4 the greatest common divisor (gcd) of 8 and 12 (written $(8,12) = 4$) because every common divisor of 8 and 12 divides 4. Clearly, $(4, 9) = 1$.

DEFINITION. Let a and b be integers not both 0. By the gcd of a and b, written $(a,b)$, we mean the positive integer d having the following properties:

(1) $d \mid a$, $d \mid b$,

(2) if $d_1 \mid a$, $d_1 \mid b$, then $d_1 \mid d$.

We can see without much difficulty that there cannot be more than one gcd. (Hence, the use of "the" in "the positive integer d" in the above definition.) Suppose there were two gcd's $d_1$ and $d_2$. Since $d_1$ is a gcd, $d_2 \mid d_1$; since $d_2$ is a gcd, $d_1 \mid d_2$. Both $d_1$ and $d_2$ are positive; therefore $d_1 = d_2$.

Exercise 3. Why did we assume in the definition of gcd that a and b were not both 0?

Factorizing integers in order to find their gcd is troublesome when the numbers are large. And we can never be sure that every pair of integers has a gcd, no matter how many special cases we work out. We shall now give a practical method of finding the gcd

which involves only the division algorithm. This method, which is called the Euclidean Algorithm, also proves the existence of the gcd.

Let a and b be the two integers whose gcd is desired. We shall assume a, b are both positive; the remaining cases are easily handled once this case is settled. Before treating the general case, let us consider the particular integers 72 and 33.

Write, by the division algorithm,

(3.1) $72 = 2 \cdot 33 + 6$

(3.2) $33 = 5 \cdot 6 + 3$

(3.3) $6 = 2 \cdot 3$

From this chain of equations we deduce that (72, 33) = 3. For from (3.3), we have that 3|6. Then from (3.2): 3|3 and 3|5·6 imply 3|33 (see Exercise 1). From (3.1): 3|6 and 3|2·33 imply 3|72. So 3 is a common divisor of 72 and 33. Suppose d is another common divisor. Then from (3.1): d|72 and d|2·33; hence, d|6, since $6 = 72 - 2 \cdot 33$. From (3.2): d|33 and d|5·6 imply d|(33 - 5·6), i.e. d|3. This shows that any common divisor d of 72 and 33 divides 3. Therefore 3 is the gcd: (72, 33) = 3.

We can obtain an additional result by writing the equations (3) in reverse order:

$$6 = 2 \cdot 3$$

$$33 = 5 \cdot 6 + 3 \longrightarrow 3 = 33 - 5 \cdot 6$$

$$72 = 2 \cdot 33 + 6 \longrightarrow 6 = 72 - 2 \cdot 33$$

$$3 = 33 - 5\,(72 - 2 \cdot 33)$$

or

$$3 = -5 \cdot 72 + 11 \cdot 33.$$

The gcd 3 is a linear function of 72 and 33 with coefficients which are integers.

In the general case we would have the chain of equations:

(4.1) $a = qb + r, \qquad 0 \leq r < b$

(4.2) $b = q_1 r + r_1, \qquad 0 \leq r_1 < r$

(4.3) $r = q_2 r_1 + r_2, \qquad 0 \leq r_2 < r_1$

(4.4) $r_1 = q_3 r_2 + r_3, \qquad 0 \leq r_3 < r_2.$

This process must come to an end. For the sequence $b, r, r_1, r_2, \ldots$ is a decreasing sequence of non-negative integers and so must eventually reach 0.

The last two steps are:

(4.(n+1)) $r_{n-2} = q_n r_{n-1} + r_n, \qquad 0 \leq r_n < r_{n-1}$

(4.(n+2)) $r_{n-1} = q_{n+1} r_n.$

We claim that $r_n$ is the gcd of $a$ and $b$. The proof is exactly the same as in the special case. Certainly $r_n \mid r_{n-1}$ by (4.(n+2)) and so $r_n \mid r_{n-2}$ by (4.(n+1)).
Working upwards we conclude that $r_n \mid a$, $r_n \mid b$. If $d$ is a common divisor of $a$ and $b$, then $d \mid r$ by (4.1). Working downwards, we arrive at the fact that $d \mid r_n$ by (4.(n+1)).

Moreover, we can express $r_n$ in terms of $a$ and $b$. From (4.(n+1)) we have $r_n = r_{n-2} - q_n r_{n-1}$. Both $r_{n-1}$ and $r_{n-2}$ can be expressed in terms of earlier $r$'s by means of equations in the set (4). After a finite number of steps we have $r_n$ expressed as a linear function of $a$ and $b$ with integral coefficients.

Notice that in the above proof we used the properties proved

in Exercise 1 in an essential way (if an integer divides two other integers, it divides their sum, difference, and any multiple of either integer).

Summarizing our results, we have:

THEOREM 1. Every pair of integers a, b other than the pair 0, 0, possesses a unique gcd. If $d = (a,b)$ is the gcd of a and b, there exist integers x and y such that

$$ax + by = d.$$

In particular, if a and b are relatively prime, there exist integers x and y such that

$$ax + by = 1.$$

Exercise 4. Prove the assertions of Theorem 1 in the cases in which a and b are not both positive.

Consider the cases: $a > 0$, $b < 0$; $a < 0$, $b > 0$; $a < 0$, $b < 0$.

Theorem 1 enables us to prove the result which will lead directly to the Fundamental Theorem of Arithmetic.

THEOREM 2. If $a|bc$ and $(a,b) = 1$, then $a|c$.

This theorem does not seem so remarkable if we imagine a, b, c factorized into primes, but remember that we have not yet discussed factorization into primes.

The proof of the theorem is very simple. Since $(a,b) = 1$, we have, by Theorem 1,

$$ax + by = 1$$

for certain integers x, y. Multiply by c:

$$acx + bcy = c$$

Now a certainly divides acx, and $a|bcy$ since $a|bc$ by hypothesis. Therefore, by Exercise 1, $a|c$.

As a corollary we get

THEOREM 3. If the prime $p|bc$ and $p \nmid b$, then $p|c$. ($p \nmid b$ means "p does not divide b".) For if $p \nmid b$, p must be prime to b, since, as a prime, p has no divisors other than 1 and itself. We can then apply Theorem 2.

Exercise 5. Let p be a prime. Then $(p, a) = 1$ if and only if $p \nmid a$.

A slight extension of Theorem 3 is the following, which we leave as an exercise.

Exercise 6. Let p and $p_1, p_2, \ldots, p_n$ be primes. If $p|(p_1 p_2 \ldots p_n)$, then p is equal to one of the primes $p_i$.

We are now in a position to prove the

FUNDAMENTAL THEOREM OF ARITHMETIC: Every integer $> 1$ can be written as a product of primes. If the primes are written in the order of increasing magnitude, the factorization is unique.

We regard a prime as its own "product of primes". Thus $2 = 2$ is a factorization into primes.

The proof is in two parts; first, we have to show that $n > 1$ is a product of prime factors. If n is a prime, we are through. If not, $n = a_1 a_2$, where $1 < a_1 < n$, $1 < a_2 < n$. If $a_1, a_2$ are both primes, we have our factorization; otherwise, we repeat the same process on $a_1$ and $a_2$, obtaining $n = a_3 a_4 a_5 a_6$, with $1 < a_3 < a_1$, $1 < a_4 < a_1$, $1 < a_5 < a_2$, $1 < a_6 < a_2$. In the successive steps of the process, the factors get smaller and smaller, but since they are positive integers they must eventually reach 2 if they are not primes at some intermediate stage. Thus n has a

factorization into primes.

Suppose there were two factorizations of $n$:

(5) $$p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$$

where the $p$'s and $q$'s are primes and $p_1 \leq p_2 \leq \cdots \leq p_r$, $q_1 \leq q_2 \leq \cdots \leq q_s$. Since $p_1$ divides $p_1 p_2 \cdots p_r$, it divides $q_1 q_2 \cdots q_s$. By Exercise 6, $p_1 = q_i$ for some $i$. By the same reasoning, $q_1 = p_j$ for some $j$. The fact that the $p$'s and $q$'s are arranged in increasing order means that $i = j = 1$, $p_i = p_1$, $q_j = q_1$. (For $p_1 \leq p_j = q_1 \leq q_i = p_i$; since the first and last members of this chain of inequalities are the same, we have equality throughout.)

Now divide both members of (5) by $p_1 = q_1$, getting

$$p_2 p_3 \cdots p_r = q_2 q_3 \cdots q_s ,$$

and proceed as before. We get $p_2 = q_2$, $p_3 = q_3$, etc. If $s > r$, we would have

$$1 = q_{r+1} q_{r=2} \cdots q_s ,$$

which is impossible. Hence $s \leq r$; by symmetry, $r \leq s$, and we conclude $r = s$. This is the end of the proof.

Here is an application of the Fundamental Theorem.

Exercise 7. If the product of two relatively prime integers is a perfect square, each of the integers is a perfect square.

You may feel that the Fundamental Theorem is completely obvious and needs no proof. However, there are many number systems besides the rationals. In these systems we can define integers, divisibility, and primes: we can do arithmetic. But in most of these number systems, while we can factor an integer into primes, the factoriza-

tion is not unique! Certain integers in these fields have two or more factorizations into entirely different primes. (See the Supplement: A New Field.) This shows that we cannot regard the uniqueness of factorization into primes in the rational field as something which is obvious. It needs to be proved.

## ANSWERS TO QUESTIONS

### PRIME NUMBERS

1. If $n$ has a proper divisor $d$ (i.e., $1 < d < n$), we can write $dd' = n$. Now either $d$ or $d'$ is $\leq \sqrt{n}$, because if both $d, d' > \sqrt{n}$, $dd' > n$.

2. $A \neq p_i$ $(i = 1, 2, \ldots, n)$ because the equation $A = p_1 p_2 \ldots p_n + 1$ shows that $A > p_1 p_2 \ldots p_n \geq p_i$, since each prime $> 1$.

3. Since an integer when divided by $4$ must have one of the remainders $0, 1, 2, 3$, we can write any integer in one of the forms $4k$, $4k + 1$, $4k + 2$, $4k + 3$. Now $4k = 2 \cdot 2k$ and $4k + 2 = 2(2k + 1)$, so these integers are even. On the other hand, $4k + 1$ and $4k + 3$ have remainders of $1$ when divided by $2$; they are odd. But $4k + 3 = 4(k + 1) - 1$.

4. Let the two numbers be $4k_1 + 1$ and $4k_2 + 1$.
$(4k_1 + 1)(4k_2 + 1) = 16\, k_1 k_2 + 4k_1 + 4k_2 + 1 =$

$$4(4k_1 k_2 + k_1 + k_2) + 1.$$

5. $A$ is the product of its prime divisors. (Some primes may occur more than once in the product, e.g., $60 = 2 \cdot 2 \cdot 3 \cdot 5$.)

Since A is odd, all prime divisors of A are odd. If all prime divisors were of the form $4k + 1$, the product would also be of this form, contradicting the fact that A is of the form $4k - 1$.

6. Suppose that there are only a finite number of primes of the form $6k - 1$, namely, $p_1$, $p_2$, ... , $p_n$. Consider $A = 6(p_1p_2...p_n) - 1$. If A is prime, we have a contradiction, for A is not $p_1$ or $p_2$ or ... or $p_n$.

Suppose A is composite. A is of the form $6k - 1$. Since A is odd, A has only odd divisors, and therefore only odd prime divisors. Now, every odd prime is of the form $6k - 1$, or else $6k + 1$. (Proof: $6k$, $6k + 2$, and $6k + 4$ are all even, and $6k + 3$ is not prime.)

Since $(6k_1 + 1)(6k_2 + 1) = 6(6k_1k_2 + k_1 + k_2) + 1$, the product of integers of the form $6k + 1$ is again an integer of this form. Therefore, A has a prime factor of the form $6k - 1$. But this cannot be $p_1$, $p_2$, ..., $p_n$; again we have a contradition.

7. Consider the sequence

$$(n + 1)! + 2,\ (n + 1)! + 3,\ ...,\ (n + 1)! + n + 1$$

and follow the reasoning in the text.

8. There is only one "prime triple". For suppose $n - 2$, $n$, $n + 2$ are all prime. $n$ must be of the form $3k + 1$, $3k - 1$, or $3k$. In the first case, $n + 2$ is of the form $3k + 3$, i.e., $n + 2$ is divisible by 3. But then $n + 2 = 3$ since it is prime. Then $n = 1$, which is not prime. Next, suppose $n$ is of the form

$3k - 1$, then $n - 2$ is of the form $3k - 3$, i.e., $n - 2$ is divisible by 3. Hence $n - 2 = 3$, so $n = 5$, $n + 2 = 7$. This gives the prime triple 3, 5, 7. Finally, if $n = 3k$, then $n = 3$, and $n - 2 = 1$, not a prime. Hence, the only prime triple is (3,5,7).

## CONGRUENCES

**Exercise 1.** $a - a = 0$ and $0$ is divisible by $m$. If $a \equiv b \pmod{m}$, $a - b$ is divisible; hence, so is $b - a$. Therefore $b \equiv a \pmod{m}$. If $a \equiv b$, $b \equiv c \pmod{m}$, then $a - b$ and $b - c$ are divisible by $m$. Therefore, so is their sum $(a - b) + (b - c) = a - c$. It follows that $a \equiv c \pmod{m}$.

**Exercise 2.** Let the integer be $N = a_0 + 10a_1 + \ldots + 10^k a_k$. Since $10 \equiv 1 \pmod{3}$, $10^k \equiv 1 \pmod{3}$, and $N \equiv a_0 + a_1 + \ldots + a_k \pmod{3}$. Hence, $N \equiv 0$ if and only if $a_0 + a_1 + \ldots + a_k \equiv 0 \pmod{3}$.

**Exercise 3.** Let the integer be $N = a_0 + 10a_1 + \ldots + 10^{2j}a_{2j}$ (this integer has an odd number of places). Since $10 \equiv -1 \pmod{11}$, $10^k \equiv 1$ if $k$ is even, $10^k \equiv -1$ if $k$ is odd. Hence, $N \equiv a_0 - a_1 + a_2 - a_3 + \ldots + a_{2j}$ and $N \equiv 0$ if and only if

$$a_0 + a_2 + a_4 + \ldots + a_{2j} \equiv a_1 + a_3 + a_5 + \ldots + a_{2j-1} \pmod{11}.$$

The proof when $N$ has an even number of places is practically the same.

**Exercise 4.** $N = a_0 + 10a_1 + \ldots + 10^k a_k$. Since $10 \equiv 2$,

$10^k \equiv 2^k \pmod 4$. Thus $10^k \equiv 0 \pmod 4$ if $k \geq 2$. Hence, $N \equiv a_0 + 10a_1 \pmod 4$ and $N \equiv 0 \pmod 4$ if and only if $a_0 + 10a_1 \equiv 0 \pmod 4$.

Exercise 5. Suppose $x_1$, $x_2$ both satisfy $ax_1 \equiv b$, $ax_2 \equiv b \pmod m$ and $0 \leq x_1 < m$, $0 \leq x_2 < m$. Subtracting the two congruences, we get $a(x_1 - x_2) \equiv 0 \pmod m$. Since $(a,m) = 1$ we can cancel the factor $a$ and then have $x_1 - x_2 \equiv 0 \pmod m$. But $0 \leq x_1 - x_2 < m$, so $x_1 - x_2 = 0$. The two $x$'s are the same.

Exercise 6. We have to solve the equation $2x + 3y = 25$ in integers $x$, $y$ such that $x \geq 0$, $y \geq 0$. We have $2x \equiv 25 \pmod 3$, $x \equiv -1 \pmod 3$ (since $2x \equiv -x \pmod 3$). Hence, $x = -1 + 3t$, $t$ an integer. Then

$$y = \frac{25 - 2x}{3} = \frac{25 - 2(-1 + 3t)}{3} = 9 - 2t.$$

Since $x \geq 0$, $t \geq 1$. Since $y \geq 0$, $t \leq 4$. Hence there are four solutions $(2,7)$, $(5,5)$, $(8,3)$, $(11,1)$.

## THE FUNDAMENTAL THEOREM OF ARITHMETIC

Exercise 1. Since $a|b$, $a|c$, we have $b = ad_1$, $c = ad_2$, where $d_1$, $d_2$ are integers. Therefore $b + c = ad_1 + ad_2 = a(d_1 + d_2)$, so $a|(b + c)$. Likewise, $a|(b - c)$. Also $bf = ad_1f = a(d_1f)$; hence $a|bf$.

Exercise 2. For a certain integer $g$, we have $b = ag$. Hence, $-b = -ag = a(-g)$, and $b = ag = (-a)(-g)$. Thus $a|(-b)$ and $(-a)|b$.

Exercise 3. Every integer $\neq 0$ divides 0, hence, all integers are common divisors of the pair 0, 0. There is no greatest common divisor of this pair of integers.

Exercise 4. Case I. $a > 0$, $b < 0$. Since $b = |-b|$, we have $d|b$ if and only if $d|(|b|)$. Hence if $d = (a, |b|)$, we have $d = (a, b)$. Since there are integers $x$, $y$ such that $d = ax + |b|y$, we have $d = ax - by = ax + b(-y)$.

Case II. $a < 0$, $b > 0$. This is the same as Case I with $a$ and $b$ interchanged.

Case III. $a < 0$, $b < 0$. We have $(a, b) = (-|a|, -|b|) = (|a|, |b|)$. If $d = |a|x = |b|y$, then $d = -ax - by = a(-x) + b(-y)$.

Exercise 5. If $p|a$, then $p$ and $a$ have the common factor $p$. Hence, if $(p, a) = 1$, $p \nmid a$. Suppose $p \nmid a$. Then $a$ does not have $p$ as a factor. Since the only factors of $p$ are 1 and $p$, it follows that $(p, a) = 1$.

Exercise 6. Write $p_1p_2 \ldots p_n = p_1 \cdot p_2p_3 \ldots p_n$. Now applying Theorem 3 we get that $p|p_1$ or $p|p_2p_3 \ldots p_n$. If $p|p_1$, $p = p_1$ and the result is proved. If not, write $p_2p_3 \ldots p_n = p_2 \cdot p_3p_4 \ldots p_n$ and proceed in the same way. If $p$ does not divide any of $p_1, p_2, \ldots, p_{n-1}$, then $p|p_{n-1}p_n$; therefore, $p|p_n$ so that $p = p_n$.

Note: If the student is familiar with Mathematical Induction, he can construct an elegant proof by assuming the result to be true when the product has $k$ factors.

Exercise 7. We are given $ab = c^2$ with $(a, b) = 1$. Write the factorization of $c$, $c = p_1^{e_1} p_2^{e_2} \ldots p_k^{e_k}$ where $e_1, \ldots e_k$ are positive integers ($e_1$ is simply the number of times the prime $p_1$ occurs in the factorization). Also, write down the factorizations of $a$ and $b$: $a = q_1^{f_1} \ldots q_s^{f_s}$, $b = r_1^{g_1} \ldots r_t^{g_t}$. We then have

$$q_1^{f_1} \ldots q_s^{f_s} r_1^{g_1} \ldots r_t^{g_t} = p_1^{2e_1} \ldots p_k^{2e_k}.$$

Since the two members of this equation are both factorizations of the same number $ab$ (or $c^2$), the same primes must occur in both. Hence, $p_1$ is some $q$ or $r$; say, $p_1^{2e_1} = q_i^{f_i}$. It follows that $f_i = 2e_1$. If we do this for every prime $q$, we see that $a$ is a

product of primes raised to <u>even</u> powers. Therefore, $a$ is a square. By the same reasoning, $b$ is a square.