An Introduction to the Theory of NUMBERS

by I. M. VINOGRADOV

Translated from the Russian
by HELEN POPOVA, Ph.D.
University of Aberdeen

An Introduction to THE THEORY OF NUMBERS

by I. M. VINOGRADOV
Member of the Academy of Sciences, U.S.S.R.
For. Mem. R.S.

PERGAMON PRESS
LONDON & NEW YORK
1955

Translated from the 6th Russian edition
published in 1952 (reprinted 1954)

Published by Pergamon Press Ltd., Maxwell House, Marylebone Road, London N.W.1 and Pergamon Press Inc., 122 E. 55th Street, New York 22, N.Y.

Printed in Northern Ireland at the Pitman Press, Belfast

CONTENTS

CHAPTER 1

THE THEORY OF DIVISIBILITY

§ 1. Fundamental concepts and theorems.

A. The theory of numbers is concerned with the study of the properties of integers (or whole numbers). By integers we understand not only the natural numbers 1, 2, 3, . . . (positive integers), but also zero and the negative integers —1, —2, —3, ...

In the text the italic letters will always denote integers, unless otherwise stated.

The sum, the difference, and the product of two integers, is also an integer, but their ratio may, or may not, be an integer.

B. If the ratio of two integers a and b is an integer q, we have $a = bq$, i.e., *a is a product of b, and an integer*. We can then say that a is *divisible* by b, or that b *divides* a. In this case a is a *multiple* of b, and b is a *divisor* of a. We shall write $b|a$ to denote that b divides a.

The following two theorems hold.

1. *If a is a multiple of m, and m is a multiple of b, then a is a multiple of b.*

In fact, from $a = a_1m$, $m = m_1b$, it follows that $a = a_1m_1b$, where a_1m_1 is an integer, which proves the theorem.

2. *If in an equality of the form*

$$k + l + \ldots + n = p + q + \ldots + s$$

for all the terms except one, it is found that they are multiples of b, then the remaining term is also a multiple of b. In fact, if we let k be the term in question, we have

$$l = l_1b, \ldots, n = n_1b,\ p = p_1b,\ q = q_1b, \ldots, s = s_1b,$$
$$k = p + q + \ldots + s - l - \ldots - n =$$
$$= (p_1 + q_1 + \ldots + s_1 - l_1 - \ldots - n_1)b,$$

which proves the theorem.

C. In general the following theorem holds. *Every integer a can be uniquely expressed in terms of a positive integer b in the form*

$$a = bq + r;\quad 0 \leqslant r < b$$

The theorem includes the particular case when a is divisible by b.

In fact, one representation of a in this form is obtained by taking bq equal to the greatest multiple of b not exceeding a. Suppose now that $a = bq_1 + r$, $0 \leqslant r_1 < b$ is another such representation, we get $0 = b(q - q_1) + r - r_1$ from which follows (**2, B**) that $r - r_1$ is a multiple of b. But, since $|r - r_1| < b$, the latter is possible only if $r - r_1 = 0$, i.e., if $r = r_1$ from which also follows $q = q_1$.

Integer q is called the *quotient*, and a the *remainder* of the division a by b.

Example. Let $b = 14$. We have

$$177 = 14 \,.\, 12 + 9; \qquad 0 < 9 < 14$$
$$-64 = 14 \,.\, (-5) + 6; \qquad 0 < 6 < 14$$
$$154 = 14 \,.\, 11 + 0; \qquad 0 = 0 < 14$$

§ 2. The greatest common divisor.

A. Below we shall consider only the positive divisors of integers. Every integer which divides simultaneously the integers $a, b, \ldots, l$ is their *common divisor.* The greatest amongst these common divisors is called the *greatest common divisor* and denoted by symbol $(a, b, \ldots, l)$. The greatest common divisor of several finite integers evidently exists since these integers have only a finite number of common divisors. If $(a, b, \ldots, l) = 1$, then $a, b, \ldots, l$ are called *relatively prime.* If every number out of $a, b, \ldots, l$ is relatively prime to every other of them, then $a, b, \ldots, l$ are called *relatively prime in pairs.* Evidently, the integers which are relatively prime in pairs are also relatively prime. In the case of two integers, the terms "relatively prime," and "relatively prime in pairs," coincide.

Example. Integers 6, 10, 15 are relatively prime, since $(6, 10, 15) = 1$. Integers 8, 13, 21 are relatively prime in pairs, since $(8, 13) = (8, 21) = (13, 21) = 1$.

B. We must first consider the common divisor of two numbers.

1. *If a is a multiple of b, then the set of all common divisors of the numbers a and b coincides with the set of all divisors of b. In particular $(a, b) = b$.*

In fact, every common divisor of the integers a and b is also a divisor of b. On the other hand, since a is a multiple of b, it follows (**1, B, § 1**) that every divisor of b is also a divisor of a, i.e., it is a common divisor of b and a. Thus, the set of all common divisors of the integers a and b coincides with the set of all divisors of b, and since the greatest divisor of b is b itself, it follows that $(a, b) = b$.

2. *If*

$$a = bq + c$$

then the set of all common divisors of a *and* b *coincides with the set of all common divisors of* b *and* c, *in particular* $(a, b) = (b, c)$.

For, from the equality above, it follows that every common divisor of the integers a and b also divides the integer c (**2, B, § 1**) and, consequently, is a common divisor of b and c.

On the other hand, the same equality shows that every common divisor of the integers b and c divides a, and consequently is a common divisor of the integers a and b.

Therefore, the common divisors of integers a and b coincide with the common divisors of integers b and c.

In particular, their greatest common divisors coincide, i.e., $(a, b) = (b, c)$.

C. The greatest common divisor of two integers can be found by means of the *Euclidean Algorithm.* The latter can be described as follows. Let a and b be positive integers. From **C, § 1,** we find the sequence of equalities

$$\left.\begin{array}{ll} a = bq_1 + r_2, & 0 < r_2 < b, \\ b = r_2q_2 + r_3 & 0 < r_3 < r_2, \\ r_2 = r_3q_3 + r_4, & 0 < r_4 < r_3, \\ \cdot \quad \cdot \quad \cdot \quad \cdot & \cdot \quad \cdot \quad \cdot \\ r_{n-2} = r_{n-1}q_{n-1} + r_n & 0 < r_n < r_{n-1}, \\ r_{n-1} = r_nq_n. & \end{array}\right\} \quad (1)$$

This sequence leads ultimately to a remainder r_{n+1} which is zero, since $b, r_2, r_3, \ldots$ is a monotonically decreasing sequence of integers, and cannot contain more than b positive terms.

D. Considering the above equalities (1) in turn, starting from the top, we find (**B**) that the common divisors of the integers a and b are the same as the common divisors of the integers b and r_2, and further are the same as the common divisors of the integers r_2 and r_3, integers r_3 and r_4, . . . , integers r_{n-1} and r_n, and finally are the same as the divisors of the integer r_n.

At the same time we have

$$(a, b) = (b, r_2) = (r_2, r_3) = \ldots = (r_{n-1}, r_n) = r_n.$$

From the above reasoning it follows that

1. *The set of all common divisors of integers a and b coincides with the set of all divisors of their greatest common divisor.*

2. *This greatest common divisor is equal to r_n, i.e., to the last non-zero remainder of the Euclidean Algorithm.*

Example. Applying the Euclidean Algorithm in order to find the greatest common divisor (525,231) we have

231	525							
2	462							
	63	231						
	3	189						
		42	63					
		1	42					
			21	42				
			2	42				

$$525 = 231 \cdot 2 + 63$$
$$231 = 63 \cdot 3 + 42$$
$$63 = 42 \cdot 1 + 21$$
$$42 = 21 \cdot 2$$

Here the last positive remainder is $r_4 = 21$. Hence $(525,231) = 21$.

E. 1.

$$(am, bm) = (a, b)m,$$

where m denotes any positive integer.

2. *If δ denotes a common divisor of integers a and b, we have*

$$\left(\frac{a}{\delta}, \frac{b}{\delta}\right) = \frac{(a, b)}{\delta}; \text{ in particular, } \left(\frac{a}{(a, b)}, \frac{b}{(a, b)}\right) = 1.$$

In fact, multiplying each term of the equalities (1) by m, we obtain new equalities, in which $a, b, r_2, \ldots, r_n$ are replaced by $am, bm, r_2m, \ldots, r_nm$ and therefore $(am, bm) = r_nm$, which proves the first statement.

Further, applying **1** to

$$(a, b) = \left(\frac{a}{\delta}\delta, \frac{b}{\delta}\delta\right) = \left(\frac{a}{\delta}, \frac{b}{\delta}\right)\delta;$$

we obtain the second theorem.

F. 1. *If $(a, b) = 1$, then $(ac, b) = (c, b)$.*

In fact, (ac, b) divides ac and bc, and hence (**1**, **D**) it divides (ac, bc), which by **1**, **E** is equal to c. But (ac, b) divides b, and thus, it divides (c, b). Conversely, (c, b) divides ac and b, and consequently it divides (ac, b). Thus, (ac, b) and (c, b) divide each other, and are therefore equal.

2. *If $(a, b) = 1$, and ac is a multiple of b, then c is a multiple of b.*

In fact, since $(a, b) = 1$, we have $(ac, b) = (c, b)$. But since ac is a multiple of b, then from **(1, B)** we have $(ac, b) = b$. Consequently $(c, b) = b$, i.e., c is a multiple of b.

3. *If every integer $a_1, a_2, \ldots, a_m$ is relatively prime to every one of the integers $b_1, b_2, \ldots, b_n$ then the product $a_1a_2, \ldots a_m$ is relatively prime to the product $b_1b_2 \ldots b_n$.*

We have (Theorem 1)

$$(a_1a_2a_3 \ldots a_m, b_k) = (a_2a_3 \ldots a_m, b_k) =$$
$$= (a_3 \ldots a_m, b_k) = \ldots = (a_m, b_k) = 1.$$

Denoting $a_1a_2 \ldots a_m$ by A, we similarly obtain

$$(b_1b_2b_3 \ldots b_n, A) = (b_2b_3 \ldots b_n, A) =$$
$$= (b_3 \ldots b_n, A) = \ldots = (b_n, A) = 1.$$

G. The problem of finding the greatest common divisor of several integers is solved by reducing it to that for two integers. Namely, in order to find the greatest common divisor of integers $a_1, a_2, \ldots, a_n$, we form a sequence

$$(a_1, a_2) = d_2,\ (d_2, a_3) = d_3,\ (d_3, a_4) = d_4, \ldots, (d_{n-1}, a_n) = d_n.$$

Thus the integer d_n is the greatest common divisor of $a_1, a_2, \ldots, a_n$.

In fact, **(1, D)** the common divisors of integers a_1 and a_2 are the same as those of d_2; consequently, the common divisors of a_1, a_2, and a_3 are the same as those of d_2 and a_3, i.e., are the same as the divisors of d_3. Further, we find that the common divisors of integers a_1, a_2, a_3, a_4 are the same as the divisors of d_4, etc. Finally, the common divisors of $a_1, a_2, \ldots, a_n$ are the same as the divisors of d_n. But the greatest divisor of d_n is d_n itself, therefore it is the greatest common divisor of the numbers $a_1, a_2, \ldots, a_n$.

It is clear from the reasoning above, that for the greatest common divisor of more than two integers, theorem **1, D,** is still true. The Theorem **1, E,** and **2, E,** are also true, because multiplication by m or division by δ of all the integers $a_1, a_2, \ldots, a_n$ implies that all the integers $d_1, d_2, \ldots, d_n$ are, respectively, multiplied by m, or divided by δ.

§ 3. The least common multiple.

A. Every integer, which is a multiple of each of the given integers is called the *common multiple* of these integers. The least positive common multiple is called the *least common multiple.*

B. We must first find a general expression for a common multiple of two integers. Let M be any common positive multiple of the integers a and b. Since it is a multiple of a, we have $M = ak$ where k is an integer. But M is also a multiple of b, and therefore $\frac{ak}{b}$ is an integer, which, taking $(a, b) = d$, $a = a_1 d$, $b = b_1 d$, can be written as $\frac{a_1 k}{b_1}$, where $(a_1, b_1) = 1$, (**2**, **E**, § **2**). Therefore (**2**, **F**, § **2**) k is a multiple of b_1, $k = b_1 t$, where t is an integer. It follows that

$$M = \frac{ab}{d} t.$$

Conversely, it is obvious that every M of the above form is a multiple of both a and b. Therefore the form is a general expression for all common multiples of a and b.

We find the least positive of these multiples by putting $t = 1$,

$$m = \frac{ab}{d},$$

which consequently will be the least common multiple. Introducing m into the expression of M, we have

$$M = mt.$$

The last two expressions lead to a theorem

1. *The common multiples of two integers are the multiples of their least common multiple.*

2. *The least common multiple of two integers is equal to their product, divided by their greatest common divisor.*

C. Consider the least common multiple of several integers $a_1, a_2, \ldots, a_n$. Denoting by $[a, b]$ the least common multiple of integers a and b, we form a sequence of integers

$$[a_1, a_2] = m_2, [m_2, a_3] = m_3, \ldots, [m_{n-1}, a_n] = m_n.$$

The integer m_n obtained in such a way, will be the least common multiple of $a_1, a_2, \ldots, a_n$.

In fact, (**1**, **B**), the common multiples of integers a_1 and a_2, are the multiples of m_2, hence the common multiples of integers a_1, a_2, and a_3 are the same as the common multiples of m_2 and a_3, i.e., as the multiples of m_3. Further we find that the common multiples of

a_1, a_2, a_3, a_4 coincide with the multiples of m_4, and so on; and, finally, that the common multiples of $a_1, a_2, \ldots, a_n$ are the same as those of m_n. But since the least multiple of m_n is m_n itself, m_n is the least common multiple of $a_1, a_2, \ldots, a_n$.

From the above reasoning it is clear that the theorem **1, B** holds in the case of more than two integers. Moreover, it shows that the following theorem is true:

The least common multiple of pairwise prime numbers is equal to their product.

§ 4. The Euclidean Algorithm and continued fractions.

A. Let α be any real number. Denoting by q_1 the greatest integer, which does not exceed α, we have

$$\alpha = q_1 + \frac{1}{\alpha_2}; \qquad \alpha_2 > 1.$$

Similarly, for non-integral $\alpha_2, \ldots, \alpha_{s-1}$, we find

$$\alpha_2 = q_2 + \frac{1}{\alpha_3}; \qquad \alpha_3 > 1;$$

$$\cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot$$

$$\alpha_{s-1} = q_{s-1} + \frac{1}{\alpha_s}; \qquad \alpha_s > 1,$$

from which we obtain the following *development of* α *into a continued fraction*:

$$\alpha = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cdot \; \cdot \; \cdot + \cfrac{1}{q_{s-1} + \cfrac{1}{\alpha_s}}}} \tag{1}$$

If α is irrational, then the set $\alpha, \alpha_2, \ldots$ does not contain integers, and the above process can be infinitely extended.

In the case when α is rational, as we shall see in (**B**), the set $\alpha, \alpha_2, \ldots$ necessarily contains an integer and the process is a finite one.

B. If α is an irreducible rational fraction $\alpha = \frac{a}{b}$, then the development of α into a continued fraction is closely connected with the Euclidean Algorithm. In fact, we have,

$$
\begin{array}{ll}
a = bq_1 + r_2; & \dfrac{a}{b} = q_1 + \dfrac{r_2}{b}, \\[2ex]
b = r_2 q_2 + r_3; & \dfrac{b}{r_2} = q_2 + \dfrac{r_3}{r_2}, \\[2ex]
r_2 = r_s q_3 + r_4; & \dfrac{r_2}{r_3} = q_3 + \dfrac{r_4}{r_3}, \\[2ex]
\cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot & \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\[2ex]
r_{n-2} = r_{n-1} q_{n-1} + r_n; & \dfrac{r_{n-2}}{r_{n-1}} = q_{n-1} + \dfrac{r_n}{r_{n-1}}, \\[2ex]
r_{n-1} = r_n q_n; & \dfrac{r_{n-1}}{r_n} = q_n,
\end{array}
$$

which gives

$$\frac{a}{b} = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cdots + \cfrac{1}{q_n}}}$$

C. The integers $q_1, q_2, \ldots$ in the development of α into a continued fraction, are called quotients, the fractions

$$\delta_1 = q_1, \quad \delta_2 = q_1 + \frac{1}{q_2}, \quad \delta_3 = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3}}, \quad \ldots$$

are called *convergents* to α.

D. We can easily find a simple law for the formation of convergents if we note that δ_s $(s > 1)$ can be obtained from δ_{s-1} by replacing q_{s-1} by $q_{s-1} + \frac{1}{q_s}$.

In fact, assuming $P_0 = 1$, $Q_0 = 0$, we can successively represent all the convergents in the following form (here the equality $\frac{A}{B} = \frac{P_s}{Q_s}$ denotes that A represents the symbol P_s, and B represents symbol Q_s).

$$\delta_1 = \frac{q_1}{1} = \frac{P_1}{Q_1}, \quad \delta_2 = \frac{q_1 + \dfrac{1}{q_2}}{1} = \frac{q_2 q_1 + 1}{q_2 \,.\, 1 + 0} = \frac{q_2 P_1 + P_0}{q_2 Q_1 + Q_0} = \frac{P_2}{Q_2},$$

$$\delta_3 = \frac{\left(q_2 + \dfrac{1}{q_3}\right) P_1 + P_0}{\left(q_2 + \dfrac{1}{q_3}\right) Q_1 + Q_0} = \frac{q_3 P_2 + P_1}{q_3 Q_2 + Q_1} = \frac{P_3}{Q_3},$$

etc., and in general

$$\delta_s = \frac{q_s P_{s-1} + P_{s-2}}{q_s Q_{s-1} + Q_{s-2}}.$$

Therefore, the numerators and denominators of convergents can be successively evaluated by the formulae

$$\left.\begin{aligned} P_s &= q_s P_{s-1} + P_{s-2} \\ Q_s &= q_s Q_{s-1} + Q_{s-2} \end{aligned}\right\} \qquad (2)$$

For these calculations the following table is useful

q_s		q_1	q_2	$\dots$			q_s	$\dots$		q_n
P_s	1	q_1	P_2	$\dots$	P_{s-2}	P_{s-1}	P_s	$\dots$	P_{n-1}	a
Q_s	0	1	Q_2	$\dots$	Q_{s-2}	Q_{s-1}	Q_s	$\dots$	Q_{n-1}	b

Example. Let us express as a continued fraction the number $\dfrac{105}{38}$.

Here

38	105				
2	76				
	29	38			
	1	29			
		9	29		
		3	27		
			2	9	
			4	8	
				1	2
				2	2

$$\frac{105}{38} = 2 + \cfrac{1}{1 + \cfrac{1}{3 + \cfrac{1}{4 + \cfrac{1}{4 + \cfrac{1}{2}}}}}.$$

and the above table gives

q_s		2	1	3	4	1	2
P_s	1	2	3	11	47	58	163
Q_s	0	1	1	4	17	21	59

E. Consider the difference $\delta_s - \delta_{s-1}$ of two subsequent convergents. For $s > 1$ we find,

$$\delta_s - \delta_{s-1} = \frac{P_s}{Q_s} - \frac{P_{s-1}}{Q_{s-1}} = \frac{h_s}{Q_s Q_{s-1}}$$

where $h_s = P_s Q_{s-1} - Q_s P_{s-1}$. Substituting for P_s and Q_s their expressions (2) and simplifying, we obtain $h_s = -h_{s-1}$. The latter, combined with $h_1 = q_1 . 0 - 1 . 1 = -1$, gives $h_s = (-1)^s$.
Hence

$$P_s Q_{s-1} - Q_s P_{s-1} = (-1)^s \qquad (s > 0) \qquad (3)$$

$$\delta_s - \delta_{s-1} = \frac{(-1)^s}{Q_s Q_{s-1}} \qquad (s > 1). \qquad (4)$$

Example. In the table of the example given in **D**, we have

$$105 . 11 - 38 . 41 = (-1)^5 = -1.$$

F. It follows from (3) that (P_s, Q_s) is a divisor of the number $(-1)^s = \pm 1$, (**2, B, § 1**). Therefore $(P_s, Q_s) = 1$, i.e., the *convergents* $\frac{P_s}{Q_s}$ *are irreducible fractions.*

G. Consider the sign of the difference $\delta_s - \alpha$ for $\delta \neq \alpha$ (i.e., excluding the case when, for a rational α, δ_s is its last convergent). Evidently δ_s is obtained by changing α_s into q_s in (1). But, as it is evident from **A**, after such a change

α_s will decrease

α_{s-1} will increase

α_{s-2} will decrease

. . . .

$\alpha \begin{cases} \text{for odd } s \text{ will decrease} \\ \text{for even } s \text{ will increase.} \end{cases}$

Therefore $\delta_s - \alpha < 0$ for odd s and $\delta_s - \alpha > 0$ for even s, and consequently the sign of $\delta_s - \alpha$ is that of $(-1)^s$.

H. We have

$$|\alpha - \delta_{s-1}| \leqslant \frac{1}{Q_s Q_{s-1}}.$$

In fact, for $\delta_s = \alpha$ the statement (with equality sign) follows from (4). For $\delta_s \neq \alpha$ it follows (with inequality sign) from (4), and from the fact that, by **G**, $\delta_s - \alpha$ and $\delta_{s-1} - \alpha$ have opposite signs.

§ 5. Prime numbers.

A. The number 1 has only one divisor, namely 1. In this respect the number 1 is different from all the other integers.

Every integer greater than 1, has at least two divisors, namely 1 and itself; if these are all divisors of an integer, it is called a *prime integer*. An integer > 1, which has divisors other than 1 and itself, is called a *composite integer*.

B. *The least divisor, distinct from* 1, *of an integer greater than* 1, *is prime.*

In fact, let q be the least divisor of an integer $a > 1$, and let q be distinct from 1. If q were a composite number, it would have some divisor q_1, satisfying $1 < q_1 < q$; but then a, being a multiple of q, is a multiple of q_1 (**1, B, § 1**) which contradicts the hypothesis that q is the least divisor of a.

C. *The least divisor, distinct from* 1 (*which according to* **B** *is prime*), *of a composite number a, does not exceed a.*

For, let q be such a divisor, then $a = qa_1$, $a_1 \geqslant q$, which on multiplication, term by term, and dividing by a_1, gives

$$a \geqslant q^2, \qquad q \leqslant \sqrt{a}.$$

D. *The number of primes is infinitely large.* The truth of this theorem follows from the fact that for any set of distinct primes $p_1, p_2, \ldots, p_k$ there exists a new prime distinct from those in the set. Such will be a prime divisor of the sum

$$p_1 p_2 \ldots p_k + 1$$

which, since it divides all the sum, cannot coincide with any of the primes $p_1, p_2, \ldots, p_k$. (**2, B, § 1.**)

E. To form the table of prime numbers not exceeding a given integer N, there exists a simple method, which is called "The Sieve of Erathosphenes." It can be described as follows.

We write down the integers in their natural order

$$1, 2, \ldots, N \tag{1}$$

The first integer distinct from 1 in this sequence is 2; it has divisors 1 and 2, and no more, and thus is prime.

We delete (as composite) from (1) all the integers which are multiples of 2, except 2 itself. The first of the remaining numbers will be 3. It is not a multiple of 2 (for otherwise it would have been deleted), consequently 3 has divisors 1 and itself and no others, thus it is also prime.

We now delete from (1) all the integers which are multiples of 3, except 3 itself. The first remaining integer is 5. It is not divisible by 2, or 3 (for then it would have been deleted), hence it has divisors 1 and itself, and also is prime.

Continuing this process we shall obtain more and more distinct prime numbers.

We note that if we have eliminated by the described method all the integers, which are multiples of primes less than p, then all non-eliminated integers, less than p^2, are prime. For then, every composite integer $n < p^2$ has been deleted from the table, being a multiple of the least prime divisor of n, which is $\leqslant \sqrt{n} < p$.

Corollaries

1. Eliminating the multiples of a prime p, start from p^2.

2. The table of primes $\leqslant N$ is completed, after we have eliminated all the integers which are multiples of the primes, less than, or equal to, $\sqrt{N}$.

§ 6. Uniqueness of factorization into prime factors.

A. *Every integer a is either relatively prime to a given prime p, or it is divisible by p.*

In fact, (a, p), since it is a divisor of p, can be either 1 or p. In the first case a is relatively prime to p, in the second a is a multiple of p.

B. *If a product of several factors is a multiple of p, then at least one of the factors is divisible by p.*

For, by **A**, each factor is either prime to p, or it is a multiple of p. If all the factors were relatively prime to p, then their product (**3, F, § 2**) would be relatively prime to p; therefore at least one of the factors must be a multiple of p.

C. *Every integer greater than* 1, *factorizes uniquely into prime factors, if the order of the factors is not taken into consideration.*†

In fact, let a be an integer greater than 1. Denoting by p_1 its smallest prime factor, we have $a = p_1 a_1$. If $a_1 > 1$, then, denoting by p_2 its least prime divisor, we have $a_1 = p_2 a_2$. If $a_2 > 1$, then

† Fundamental theorem of arithmetic.