THE THEORY OF NUMBERS.—I.

*Sur la théorie des nombres.** M. STIELTJES. (*Annales de la Faculté des Sciences de Toulouse*, vol. 4.)

M. STIELTJES undertook a few years ago to write an extensive treatise on the theory of numbers. His weak health, and finally untimely death, prevented the accomplishment of his task. The following letter which I received from him in answer to a request to send me a separate copy of his paper will put the circumstances clearly before the reader:

"TOULOUSE, May 29, 1894.

"I am exceedingly sorry not to be able to send you a copy of my paper. When I undertook this work it was my intention to carry it much farther, and to publish several volumes. I had the first volume nearly ready, and it was agreed that M. Gauthier-Villars should publish it separately. So I did not receive any separate reprints of the part already published, probably because M. Gauthier-Villars intended to send them to me when the first volume should be finished. But in proportion as I advanced, it became more and more evident that I would not be able to gather together in Toulouse all the materials for my work. I had made up a list of about thirty papers which it would be impossible for me to get, and which were absolutely necessary in order to finish the first volume. I lost heart, my health gave way too, so that I was obliged to spend two winters in Algiers,—and I could not work. So that it is perfectly certain that I shall not resume the task in the future; the idea of doing it is very far from me now. And then my work was nothing else but a bibliographical review, and I only summed up what had been done by others, in particular by H. J. Stephen Smith.

"Going back to the sources, accordingly, you will advantageously supply the absence of my work, which had no other object but to be useful to beginners who know little or nothing of the theory of numbers. To prove you my goodwill, I hope you will permit me to send you a paper on continued fractions, which I have just brought painfully to a close. But it will not appear before the end of the year.†

---

* Also now published separately. See list of *New Publications* in this number of the BULLETIN, p. 239.

† This promise was faithfully fulfilled. The paper appeared in the eighth volume of the *Annales de Toulouse*.

To avoid your being disappointed at that time, I shall state at once that it deals with algebra and analysis, and not with the theory of numbers.

"Pray accept, etc. T. STIELTJES."

The oldest treatise on the theory of numbers that has come down to us is the one contained in the Seventh, Eighth, and Ninth Books of Euclid's Elements.* The first principles of our science will be found there exposed "with the usual rigor and terseness of the ancients." The subjects treated by Euclid, such as the independence of a product of the order of its factors,† the rule for finding the greatest common measure, numbers prime to one another, least common multiples and greatest common divisors, the decomposition of a number into prime factors and its uniqueness, and finally the proposition that our stock of prime numbers can never be exhausted, might be properly designated under the name of Euclidian arithmetic.

We shall say accordingly that the beginning of M. Stieltjes' paper is devoted to Euclidian arithmetic, greatly generalized, however. He does not insist on the definition of number ‡ nor on the laws which are at the base of the operations we perform on numbers,§ but after a simple mention of these topics, passes immediately to the exposition of the chief properties of the least common multiple and the greatest common divisor of numbers. Euclid gives a rule for finding the greatest common divisor of two numbers,‖ and reduces to it the problem of finding the least common multiple of two numbers.¶ Poinsot** was the first, I think, to whom it occurred that the course could be reversed. I shall present his process in a somewhat more symmetrical form. Suppose

---

* I shall always refer to Dr. Heiberg's edition, where the Books mentioned will be found on pages 184–437 of the second volume.

† The associative law is not mentioned—a deficiency happily supplied by the Fifth Book, which is thus stamped at once as coming from another hand (Eudoxus). Gauss was the next to consider the associative law in his theory of composition of forms—and he quotes the Fifth Book of the Elements (*Disqu. Ar.*, art. 239).

‡ On this subject see Helmholtz's and Kronecker's papers in the *Philosophische Aufsätze an Zeller* (Leipzig, 1887), and Professor Dedekind's pamphlet, *Was sind und was sollen die Zahlen* (Braunschweig, 1888).

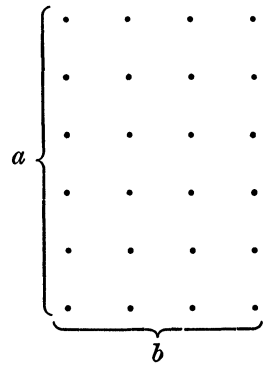
§ See *Grassmann's Arithmetik* (Stettin—I think most copies have Berlin on the title-page—1860) and Clifford's Common-Sense of the Exact Sciences.

‖ Euclidis Elementa, VII., 1, 2.

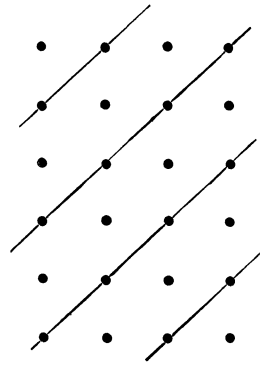
¶ Eucl. Elem. VII., 34.

** *Journal de Liouville*, 1845, p. 48.

we have a rows of b points, placed so as to form at the same time b columns of a points:



We can now cut out the slip of paper containing the points, deform it, and paste on the surface of an anchor ring, so that each column will be on a parallel and each row on a meridian. Let us now start from any point of the configuration—say the lower left-hand corner, using still our plane representation to facilitate the explanation—and then make a move forwards and to the right, then another move in the same direction, and so forth, keeping well in mind that the



whole configuration is on an anchor ring. As the stock of points is a limited one,—there are ab points in all,—we must finally return to some point where we have been before. I say it will be the initial point.

In fact, there are two elementary movements to be con-

sidered—*the one* by which all parallels revolve so as to coincide each with its old position, while each meridian is replaced by the next one, and *the other* such that each meridian coincides with its old position, while each parallel is replaced by the next one. Now it is clear that if after several such movements the point A' comes to coincide with the point A, and the points B and B' are the points to which we should move from A and A' according to the rule described above, then when A' coincides with A, B' must coincide with B. Now if we perform the requisite movements in order to bring the point to which we *returned* in coincidence with our initial point, then, unless our proposition is true, the course described starting from the initial point does not coincide with the course obtained by following the track of the point which is now in coincidence with the initial point, which is absurd.

Let h_1', h_2', ... h_m' be the points through which we passed in succession, so that one step more would bring us again to the initial point h_1'. Then if $m = ab$ our supply of points is exhausted. If $m < ab$, let h_1'' be a point through which we did not pass. By taking h_1'' as initial point we obtain a cycle of points:

$$h_1'', h_2'', \ldots h_u''.$$

I say u must be equal to m, because if we bring h_1'' in coincidence with h_1' by a combination of movements described above, the two cycli

$$h_1', h_2', \ldots h_m'$$

and

$$h_1'', h_2'', \ldots h_u''$$

will coincide, which gives

$$u = m.$$

The two cycli can have no common point, because otherwise there would be two divergent tracks from such a point, which is absurd on account of the perfect determinateness of the track of a point. If $2m = ab$ our stock is exhausted; if $2m < ab$ let h_1''' be a point not on the two tracks already described. The point h_1''' will give us a new track,

$$h_1''', h_2''', \ldots h_m''',$$

and so forth, till the tracks described

$$\begin{array}{l} h_1', h_2', \ldots . h_m' \\ h_1'', h_2'', \ldots . h_m'' \\ h_1''', h_2''', \ldots h_m''' \\ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ h_1^{(n)}, h_2^{(n)}, \ldots h_m^{(n)} \end{array}$$

will include all the points of the configuration, so that

$$ab = nm.$$

In its arithmetical form this process is a very primitive one (logically, not historically), but perfectly sufficient to establish the chief properties of Euclidian arithmetic.

The numbers a and b being two given integers, I divide the succession of numbers

$$1, 2, 3, \ldots$$

by a and b till I come to a number m such that the two divisions will leave no remainders, which must happen sooner or later, because the number ab is divisible both by a and b. It may happen that $m = ab$ so that ab is the least number divisible by a and b. If not, and accordingly $m < ab$, I write under the succession of numbers

$$1, 2, 3, \ldots m$$

another succession of numbers,

$$m + 1, m + 2, m + 3, \ldots 2m.$$

If a number of the first succession is divisible by a and b, so will be the corresponding number of the second succession by virtue of the law of distribution. Now m being the only number of the first succession divisible by a and b, $2m$ will be the only number of the second succession divisible by a and b. Now ab being divisible by a and b, it may happen to be equal to one of the two numbers m and $2m$, but cannot be equal to any other number of the two successions. The first equality having been already excluded, $2m$ is the only number of the two successions to which ab may happen to be equal now. If not, and accordingly $ab > 2m$, I write down another succession of numbers,

$$2m + 1, 2m + 2, \ldots 3m,$$

under the two first, and by reasoning in the same way as before we come to the conclusion that $3m$ is the only number of the three successions to which ab may now happen to be equal. By continuing in the same way we shall finally exhaust all the numbers

$$1, 2, 3. \ldots ab$$

say after having written down n successions of numbers, so that

$$mn = ab.$$

The number m will be the least common multiple of a and b, and it remains to show that n is the greatest common divisor of a and b. In fact, m being a multiple of a, it follows from the equality

$$m = a \times \frac{b}{n}$$

that n is a divisor of b. In the same way it follows from

$$m = b \times \frac{a}{n}$$

that n is a divisor of a. If n is not the greatest common divisor of a and b, let h be the greatest. Then it follows from

$$h > n$$

that

$$\frac{ab}{h} < m,$$

and as $\frac{ab}{h}$ is an integer and a multiple of a and b, in virtue of the equalities

$$\frac{ab}{h} = a \times \frac{b}{h} = b \times \frac{a}{h},$$

it would be a multiple of a and b smaller than m, contrary to what has already been proved.

Every multiple k of a and b is a multiple of m. In fact, I write the succession of numbers

$$1, 2, 3, \ldots k$$

in rows of m numbers,

$$\begin{array}{rrrl} 1, & 2, & 3, & \ldots\ m \\ m+1, & m+2, & m+3, & \ldots\ 2m \\ 2m+1, & 2m+2, & 2m+3, & \ldots\ 3m, \end{array}$$

till I reach the number k, which can find its place only in the last column, because the numbers of the other columns are not divisible by a and b at the same time. The number k will be equal accordingly to a multiple of m such as lm.

It follows that every divisor v of a and b is a divisor of n. In fact, $\frac{ab}{v}$ being a multiple of a and b will be a multiple of their least common multiple $\frac{ab}{n}$, and according n divisible by v.

The converse propositions that every multiple of m is a multiple of a and b and every divisor of n is a divisor of a and b are of a still more elementary kind.

Two numbers whose greatest common divisor is equal to unity are said to be prime to one another. Such are, for instance, the numbers 8 and 15. The least common multiple of two numbers a and b prime to one another is equal to $\frac{ab}{1} = ab$.

The important proposition VII., 30 of Euclid can now be easily established in a somewhat generalized form.

If a is prime to b and divides bc, then a divides c. In fact, a and b being prime to one another their least common multiple will be equal to ab. Now bc being a multiple of a and b will be a multiple of their least common multiple ab, and accordingly c is a multiple of a. These propositions are generally proved by means of Euclid's rule for finding the greatest common divisor of two numbers.*

Among those who have adopted a point of view similar to the one exposed here, I may quote Professor Bachmann (*Zahlentheorie*, 1892) and M. Emile Borel (*Introduction à l'étude de la théorie des nombres*, 1895).

Euclid's rule for finding the greatest common divisor† is so well known that I need not insist upon it. Its importance can hardly be overestimated, and up to the present day it is the only convenient rule for finding the greatest common divisor of two numbers. The other rule—usually given in the text-books—reduces the problem to a harder one, the individual decomposition of each number into factors.

The least common multiple of a and b being equal to m, the least common multiple of ac and bc will be equal to mc. In fact, mc is evidently a multiple of ac and bc. If these two numbers admitted a multiple $t < mc$, then t would be of the form kc where $k < m$ and a multiple of a and b, which is

* Grassmann's Arithmetik, p. 40.
† Eucl. Elem., VII. 1, 2.

absurd. It follows that if n is the greatest common divisor of a and b then nc is the greatest common divisor of ac and bc.

The definition of the least common multiple and the greatest common divisor can be easily extended so as to apply to the case of more than two numbers

$$a_1, a_2, \ldots a_n.$$

M. Stieltjes uses the very convenient designation

$$| a_1, a_2, \ldots a_n |$$

for the least common multiple and

$$(a_1, a_2, \ldots a_n)$$

for the greatest common divisor.

These two arithmetical functions are independent of the order of the numbers

$$a_1, a_2, \ldots a_n,$$

and it is also evident that if we repeat any one of our numbers several times, the two functions will not change.

Let us now consider the succession of numbers

$$1, 2, \ldots m,$$

where the last number m is the first which is divisible by all the numbers

$$a_1, a_2, a_3, \ldots a_n.$$

That we must finally reach such a number m follows from the fact that the product $a_1 a_2 \ldots a_n$ is divisible by a_1, $a_2, \ldots a_n$, although there may be smaller numbers having the same property. It is now easily proved that every multiple μ of

$$a_1, a_2, \ldots a_n$$

is a multiple of m by writing down the rows

$$\begin{array}{cccc} 1, & 2, & 3, \ldots & m, \\ m+1, & m+2, & m+3, \ldots & 2m, \\ 2m+1, & 2m+2, & 2m+3, \ldots & 3m, \\ \cdot & \cdot & \cdot & \cdot \end{array}$$

till we reach the number μ, which can find its place only in the last column, because the numbers of the other columns are not divisible by *all* the numbers $a_1, a_2, \ldots a_n$. The proof of the converse proposition that every multiple of m is a multiple of

$$a_1, a_2, \ldots a_n$$

is immediate.

By examining all the numbers in succession from one up to the smallest of the numbers

$$a_1, a_2, \ldots a_n,$$

we can easily pick out all the common divisors

$$\delta_1, \delta_2, \ldots \delta_h$$

of the numbers

$$a_1, a_2, \ldots a_n.$$

Let us now put

$$| \delta_1, \delta_2, \ldots \delta_h | = d.$$

As all the numbers

$$a_1, a_2, \ldots a_n$$

are multiples of

$$\delta_1, \delta_2, \ldots \delta_h,$$

they will be multiples of their least common multiple d, and accordingly d will be equal to the greatest of the numbers

$$\delta_1, \delta_2, \ldots \delta_h.$$

This establishes not only the existence of the greatest common divisor d of the numbers

$$a_1, a_2, \ldots a_n,$$

but also the fact that every divisor of these numbers is a divisor of d.

In order to find the least common multiple m of several numbers

$$a_1, a_2, \ldots a_n,$$

we may replace any two of them a_h and a_k by their least common multiple $| a_h, a_k |$; then the problem of finding the least common multiple of

$$a_1, a_2, \ldots a_n$$

will be reduced to the problem of finding the least common multiple of the new row of $n-1$ numbers. In fact, every multiple of a_h and a_k is a multiple of $| a_h, a_k |$, and conversely. The number of the numbers of the new row is now equal to $n-1$, and can be diminished by one by repeating the process, and so on until we come to the single number m as the final result. The process is an unsymmetrical one, but as the result can be expressed in a symmetrical form, it is independent of the order in which the operation is performed.

A similar process can be given for the finding of the greatest common divisor of several numbers.

We shall now establish a lemma which will be useful to us in the future.

If b and c are prime to one another, then the greatest common divisor of a and bc is equal to the product of the greatest common divisor of a and b by the greatest common divisor of a and c.

Demonstration.—

$$\begin{aligned}(a, bc) &= (ab, ac, bc)^* = (ab, c(a, b))^\dagger = (ac, b(a, c))^\ddagger \\ &= (ab, ac, c(a, b), b(a, c)) = (b(a, c), c(a, b)) \\ &= (a, b) \times (a, c).^\S\end{aligned}$$

The proposition may be immediately extended to the case of any number of numbers prime each to each,

$$b, c, d, \ldots,$$

so that we shall have

$$(a, bcd \ldots) = (a, b) \times (a, c) \times a, d) \times \ldots$$

It happens very often in the theory of numbers, as well as in the theory of groups, that the least common multiple m of n numbers

$$a_1, a_2, \ldots a_n$$

has to be decomposed into n factors

$$m = b_1 b_2 \ldots b_n$$

such that each b divides the corresponding a, and the factors are prime each to each.

The problem may be solved in the following way: If no two a's have a common factor, then

$$m = a_1 a_2 \ldots a_n,$$

and we can put

$$b_1 = a_1, \quad b_2 = a_2 \ldots b_n = a_n.$$

If two of the a's, say a_h and a_k, have a common factor d, and that factor happens to be prime to $\frac{a_h}{d}$, then, as $\frac{a_h}{d}$ is prime to $\frac{a_k}{d}$ and d, it will be prime to their product $\| \; a_k$, and accordingly $\frac{a_h a_k}{d}$ will be the least common multiple of $\frac{a_h}{d}$ and

---

* Because the greatest common divisor of ab and ac is a.

† Because the greatest common divisor of ac and bc is c times the greatest common divisor of a and b.

‡ For a similar reason.

§ Because the product evidently divides both $b \,.\, (a, c)$ and $c \,.\, (a, b)$ and leaves two quotients, $\frac{b}{(a, b)}$ and $\frac{c}{(a, c)}$, prime to one another, on account of b and c being so.

‖ Eucl. Elem. VII. 24.

a_k. So that if we replace the row of numbers

$$a_1, a_2, \ldots a_{h-1}, a_h, a_{h+1}, \ldots a_{k-1}, a_k, a_{k+1}, \ldots a_n$$

by

$$a_1, a_2, \ldots a_{h-1}, \frac{a_h}{d}, a_{h+1}, \ldots a_{k-1}, a_k, a_{k+1}, \ldots a_n,$$

the least common multiple of the second row will be equal to the least common multiple of the first row, each number of the second row will divide the corresponding number of the first row, and finally, the product of the numbers of the second row will be equal to the product of the numbers of the first row divided by d.

Now if a_h and a_k have a greatest common divisor d which is not prime to $\frac{a_h}{d}$, but the two numbers d and $\frac{a_h}{d}$ have a greatest common divisor $\delta > 1$, then it is easy to see that the greatest common divisor of a_h and $\frac{a_k}{\delta}$ will be equal to $\frac{d}{\delta}$. In fact, both a_h and $\frac{a_k}{\delta}$ are divisible by $\frac{d}{\delta}$, giving the quotients $\frac{a_h}{d} \cdot \delta$ and $\frac{a_k}{d}$. I say these two quotients will be prime to one another, for $\frac{a_h}{d}$ is prime to $\frac{a_k}{d}$, on account of d being the greatest common divisor of a_h and a_k, and δ being a divisor of $\frac{a_h}{d}$ will be prime to $\frac{a_k}{d}$ too,* so that the product $\frac{a_h}{d} \times \delta$ is prime † to $\frac{a_k}{d}$. The least common multiple of a_h and $\frac{a_k}{d}$ will be accordingly equal to $\frac{a_h \times \frac{a_k}{\delta}}{\frac{d}{\delta}} = \frac{a_h a_k}{d}$. So that if we replace the row of numbers

$$a_1, a_2, \ldots a_h \ldots a_k \ldots a_n$$

by the row of numbers

$$a_1, a_2, \ldots a_h \ldots \frac{a_k}{\delta} \ldots a_n,$$

the least common multiple of the new row of numbers will be equal to the least common multiple of the first row, each

* Eucl. Elem. VII. 23.
† Eucl. Elem. VII. 24.

number of the second row will divide the corresponding number of the first row, and finally, the product of the numbers of the second row will be equal to the product of the numbers of the first row divided by δ.

We come to the conclusion that so long as there are two numbers in the row

$$a_1, a_2, \ldots a_n$$

admitting a greatest common divisor larger than unity, the row can be replaced by another row

$$a_1', a_2', \ldots a_n',$$

so that the least common multiple of the second row will be the same as the least common multiple of the first row, each number of the second row will divide the corresponding number of the first row, and, finally, the product of the numbers of the second row will be less than the product of the numbers of the first row. If we repeat the operation so long as the new row has numbers admitting a greatest common divisor larger than unity, we must finally come to a row of numbers

$$b_1, b_2, \ldots b_n$$

no two of which have a common divisor; otherwise the operation could be always continued, which is impossible on account of the diminishing of the product of the numbers at each successive operation. We shall have accordingly

$$m = b_1 b_2 \ldots b_n,$$

and the factors will have the required property.

It is now easy to prove the theorem, which by using the preceding notations can be expressed as follows:

$$| (a, b), (a, c), (a, d), (a, e), \ldots | = (a, | bcde \ldots |).$$

In fact, I put

$$| b, c, d, e, \ldots | = b_1 c_1 d_1 e_1 \ldots$$

so that $b_1, c_1, d_1, e_1, \ldots$ are prime each to each; and besides, b_1 divides b, c_1 divides c, d_1 divides d, e_1 divides e, etc. Then

$$(a, | bcde \ldots |) = (a, b_1 c_1 d_1 e_1 \ldots) =$$
$$= (a, b_1) \times (a, c_1) \times (a, d_1) \times (a, e_1). \ldots$$

Now as each of the numbers

$$(a, b), (a, c), (a, d), (a, e), \ldots$$

divides

$$(a, | bcde \ldots |),$$

their least common multiple will divide it too, so that the left side of the equality which it is required to prove divides the right side. But if we write down the two rows

$$(a, b_1),\ (a, c_1),\ (a, d_1),\ (a, e_1)\ \ldots,$$
$$(a, b),\ (a, c),\ (a, d),\ (a, e)\ \ldots,$$

each number of the first row will divide the corresponding number of the second row, and accordingly the least common multiple of the numbers of the first row, that is to say, $(a, \mid bcde\ \ldots \mid)$ will divide the least common multiple of the numbers of the second row, which we designated by

$$\mid (a, b),\ (a, c),\ (a, d),\ (a, e). \ \ldots \mid .$$

So that the right side of the equality which it is required to prove divides the left side. Accordingly the two sides are really equal.*

When we have more than two numbers, say n,

$$a_1, a_2, \ \ldots\ a_n,$$

it is found convenient to consider besides the least common multiple and the greatest common divisor $n - 2$ intermediate numbers. We might have arrived at such an extension of the original Euclidian theory by generalizing the geometrical interpretation given above, but I shall confine myself in this sketch to an arithmetical exposition of the subject. Let us put

$$e_n = \mid a_1, a_2, \ \ldots\ a_n \mid$$
$$e_{n-1} = \mid (a_1, a_2),\ \ldots\ (a_1, a_n), (a_2, a_3),\ \ldots\ (a_2, a_n),\ \ldots\ (a_{n-1}, a_n) \mid$$
$$e_{n-2} = \mid (a_1, a_2, a_3),\ \ldots\ (a_1, a_2, a_n), (a_1, a_3, a_4),\ \ldots\ (a_1, a_3, a_n), (a_2, a_3, a_4)\ \ldots\ (a_2, a_3, a_n)\ \ldots\ (a_{n-2}, a_{n-1}, a_n) \mid$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$e_1 = \mid (a_1, a_2, \ \ldots\ a_n) \mid = (a_1, a_2, \ \ldots\ a_n).$$

Then it is easy to see that each e_k is a multiple of e_{k-1} So, for instance, e_n is a multiple of e_{n-1}, because

$$(a_1, a_2), (a_1, a_3),\ \ldots\ (a_1, a_n) \text{ divide } a_1$$
$$(a_2, a_3), (a_2, a_4),\ \ldots\ (a_2, a_n) \text{ divide } a_2$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$(a_{n-1}, a_n) \text{ divides } a_{n-1}.$$

* Grassmann's Arithmetik, No. 103.

By using the rule that while forming the least common multiple of a lot of numbers any numbers of the lot may be replaced by their least common multiple, we arrive at the following expressions for our numbers $e_n, e_{n-1}, \ldots e_1$:

$$e_n = | a_1, a_2, \ldots a_n |$$

$$e_{n-1} = | (a_1, | a_2, \ldots a_n |), (a_2, | a_3 \ldots a_n |), \ldots (a_{n-1}, a_n) |$$

$$e_{n-2} = | (a_1, a_2, | a_3, \ldots a_n |), (a_1, a_3, | a_4, \ldots a_n |), \ldots (a_1, a_{n-1}, a_n), \quad (a_2, a_3, | a_4, \ldots a_n |), (a_2, a_4, | a_5, \ldots a_n |), \ldots (a_2, a_{n-1}, a_n), \ldots (a_{n-2}, a_{n-1}, a_n) |$$

. . . . . .

. . . . . .

$$e_1 = | (a_1, a_2, \ldots a_n) | = (a_1, a_2, \ldots a_n).$$

It follows that while e_n is the least common multiple of n numbers

$$a_1, a_2, \ldots a_n,$$

e_{n-1} is the least common multiple of $n - 1$ numbers.

$$b_1 = (a_1, | a_2, \ldots a_n |), b_2 = (a_2, | a_3, \ldots a_n |), \ldots b_{n-1} = (a_{n-1}, a_n).$$

Now I say that e_{n-2} may be deduced from e_{n-1} in the same way as e_{n-1} is deduced from e_n; that is to say, that while

$$e_{n-1} = | (a_1, | a_2, \ldots a_n |), (a_2, | a_3, \ldots a_n |), \ldots (a_{n-1}, a_n), |$$

we have also

$$e_{n-2} = | (b_1, | b_2, \ldots b_{n-1} |), (b_2, | b_3, \ldots b_{n-1} |), \ldots (b_{n-2}, b_{n-1}) | .$$

I shall put for the sake of abbreviation

$$h_1 = (b_1, | b_2, \ldots b_{n-1} |), h_2 = (b_2, | b_3, \ldots b_{n-1} |), \ldots h_{n-2} = (b_{n-1}, b_n).$$

Now it is easy to prove that h_1 is the least common multiple of the numbers

$$(a_1, a_2, | a_3, \ldots a_n |), (a_1, a_3, | a_4, \ldots a_n |), \ldots (a_1, a_{n-1}, a_n).$$

In fact,

$$h_1 = (b_1, | b_2, \ldots b_{n-1} |) = | (b_1, b_2), (b_1, b_3), \ldots (b_1, b_{n-1}) | .$$

And as

$$(b_1, b_2) = (a_1, a_2, \mid a_3, \ldots a_n \mid, \mid a_2, \ldots a_n \mid)$$
$$= (a_1, a_2, \mid a_3!, \ldots a_n \mid)$$
$$(b_1, b_3) = (a_1, a_3, \mid a_4, \ldots a_n \mid)$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$(b_1, b_{n-1}) = (a_1, a_{n-1}, a_n),$$

our assertion is proved. In a similar way h_2 is the least common multiple of the numbers

$$(a_2, a_3 \mid a_4 \ldots a_n \mid), (a_2, a_4, \mid a_5 \ldots a_n \mid), \ldots (a_2, a_{n-1}, a_n);$$

and finally

$$h_{n-2} = \mid (a_{n-2}, a_{n-1}, a_n) \mid .$$

The two expressions for e_{n-2} are accordingly equal. In the same way by putting

$$c_1 = (b_1, \mid b_2, \ldots b_{n-1} \mid), c_2 = (b_2, \mid b_3, \ldots b_{n-1} \mid), \ldots$$
$$c_{n-2} = (b_{n-2}, b_{n-1}),$$

we have

$$e_{n-2} = \mid c_1, c_2, \ldots c_{n-2} \mid$$

and

$$e_{n-3} = \mid (c_1, \mid c_2, \ldots c_{n-2} \mid), (c_2, \mid c_3, \ldots c_{n-2} \mid), \ldots,$$
$$(c_{n-3}, c_{n-2}) \mid .$$

So that each of the numbers $e_n, e_{n-1}, \ldots e_1$ is deduced from the preceding in a similar way, the number of the numbers on which we have to operate gradually diminishing by one from n in the case of e_n to unity in the case of e_1. The operation is an unsymmetrical one, but as it gives the same result as the symmetrical one, the lack of symmetry has no influence on the result

Let us take the following numbers, for instance:

$$a_1 = 480, a_2 = 720, a_3 = 2700, a_4 = 3240, a_5 = 6750, a_6 = 11250.$$

Then by using Euclid's rule for finding the greatest common divisor, the whole calculation can be performed in the following way:

	480	720	2700	3240	6750	11250
$e_6 =$	1820000	910000	405000	405000	33750	
	240	360	2700	270	2250	
$e_5 =$	270000	135000	67500	6750		
	120	180	270	90		
$e_4 =$	1080	540	270			
	60	90	90			
$e_3 =$	180	90				
	30	90				
$e_2 =$	90					
$e_1 =$	30					

The last number in the third row is the greatest common divisor of the two last numbers in the first row, and the last number in the second row is their least common multiple. The last number but one in the third row is the greatest common divisor of 3240 and 33750, and 405000 is their least common multiple. The last number but two in the third row is the greatest common divisor of 2700 in the first row and 405000 in the second row, and 405000 a little to the left is the least common multiple of the same numbers. The second number in the third row is the greatest common divisor of 720 and 405000, and 910000 is their least common multiple. The first number in the third row is the greatest common divisor of 480 and 910000, and 1820000 $= e_6$ is their least common multiple, etc., etc.

M. Stieltjes gives other expressions for the same numbers, for which I refer to his paper. We have now worked our way through the first chapter* with the figure of the great Greek mathematician overshadowing us all the while. The second chapter begins under the auspices of Gauss.

JOSEPH DE PEROTT.

CLARK UNIVERSITY, *May* 23, 1895.

NOTE ON HÖLDER'S THEOREM CONCERNING THE CONSTANCY OF FACTOR-GROUPS.†

BY MR. GEORGE L. BROWN.

HÖLDER'S proof of the constancy of the factor-groups for the different series of composition of a group is based upon the following lemma:‡ *If a group G possesses two different maximal self-conjugate subgroups A and B, having C as their greatest common subgroup, then the quotient-groups G | A and B | C, likewise G | B and A | C, are holoedrically isomorphic.*

The proof of this lemma may be very much simplified by making use of the following theorem, due to Giudice:§ *If A and B are two commutative groups of orders p and q respectively, having C, of order r, as their greatest common subgroup, then the order of the group F = {A, B} formed by combining the operations of A and B in every possible way is* $\frac{pq}{r}$.

---

* I had no desire to exhaust the subject. The reader will find many propositions which I omitted in Grassmann's Arithmetik and Stieltjes' paper.

† *Math. Annalen*, vol. 34, pp. 34–37.

‡ Hölder, l. c., § 9.

§ Netto, Theory of Substitutions, § 38; F. Giudice, *Palermo Rend.* vol. 1, pp. 222, 223.