of Yale University, and particularly of the members of the mathematical department were gratefully acknowledged by a unanimous vote of thanks and appreciation at the closing meeting.

Detailed reports of the courses, prepared by the lecturers, will appear in later numbers of the BULLETIN.

VIRGIL SNYDER.

THEORY AND CONSTRUCTION OF TABLES FOR THE RAPID DETERMINATION OF THE PRIME FACTORS OF A NUMBER.*

BY PROFESSOR ERNEST LEBON.

BY making use of some hitherto unnoticed properties of certain arithmetic progressions, I have succeeded in constructing a table giving very rapidly the solution of the following double problem: *To determine whether a given number is prime or composite, and in the latter case to find its prime factors.* The process which I employ is applicable to large numbers.†

1. Let B be the product $\alpha\beta\cdots\lambda$ of the consecutive prime numbers $\alpha, \beta, \cdots, \lambda$, beginning with 2; P the product $(\alpha-1)(\beta-1)\cdots(\lambda-1)$; I any of the P numbers that are relatively prime to B and less than B; K a number successively equal to the positive integers, starting from zero.

We easily see that *the system of P arithmetic progressions whose general term is $BK+I$ contains all the prime numbers except those that occur in B.*

We shall say that B is the base of the system and that I is the index of a term of this system.

Two indices will be said to be complementary when their sum is equal to the base.

2. Let N, D and M be any numbers relatively prime to B. In order to avoid ambiguity, I will write D in the form $BK'+I'$.

It is evident that *$N(=BK+I)$ is or is not divisible by D according as K and M do or do not satisfy the equation*

---

* Translated by Professor W. B. FITE.

† Cf. *Comptes rendus*, vol. 151 (1905), p. 78. See also § 10, p. 77.

$$(a) \qquad BK + I = MD,$$

B, I and D being known.

3. Let k and m be the minimum values of K and M satisfying equation (a), and n a number successively equal to the positive integers starting from zero. If necessary for clearness, I use k_I for the numbers K relative to a divisor D.

The equality

$$K = k + nD$$

gives the values of K to which correspond all the numbers N that are divisible by D.

From this equality we get the formula

$$(1) \qquad n = \frac{K - k}{D},$$

where K is the integral quotient obtained by dividing N by B; the remainder in this division is the value of I.

We see that *according as the value of n obtained by applying formula* (1) *is integral or fractional, the number N is, or is not, a multiple of the divisor D.*

Then *the table of numbers k set up for a system of base B enables one to recognize whether N is prime or not by dividing the difference $K - k$ by the prime numbers less than $\sqrt{N}$ and greater than λ; if N is not prime, this procedure gives its prime factors.*

We see that the larger the base B the more rapidly this method gives the result.

Before applying formula (1), it should not be forgotten that if we are considering a number N' we must in order to get N remove from it the factors that are common to it and B.

4. The numbers k I shall call *characteristics.*

5. In order to find methodically and quickly the characteristics k which correspond to the P arithmetic progressions of a system with the base B, we can use the following formula, which is obtained by replacing in equation (a) K and M by k and m, and D by $BK' + I'$:

$$(2) \qquad k = \frac{I'm - I}{B} + K'm.$$

Formula (2) gives the characteristic k when the value of m is such that the binomial $I'm - I$ is divisible by B.

6. The three following theorems, which are easily demonstrated, enable one to make a considerable reduction in the number of operations required for the calculation of the characteristics k:

I. *To the product $I'm$ of the two indices I' and m correspond an index I and a characteristic k; this characteristic is associated with the number $I'm$ by the arithmetic progression of base B and index I given by this product.*

II. *The P arithmetic progressions of a system of base B being arranged in the order of the increasing values of the indices I of their terms, the sum of the two characteristics k and that of the two values of m relative to the same divisor D and to two progressions equidistant from the extremes are equal to $D - 1$ and B respectively.*

III. *If the values of I, k_I, I', and m satisfy the equation*

$$Bk_I + I = I'm,$$

and if we consider the equation

$$Bk_{B-I} + (B - I) = (B - I')m,$$

where the two indices $B - I$ and $B - I'$ are complementary to the I and I' respectively of the preceding equality, the unknown characteristic k_{B-I} is given by the formula

$$k_{B-I} = m - 1 - k_I.$$

7. It follows from Theorems II and III that in order to calculate the binomial $I'm - I$, it is sufficient to associate with the first half of the P values of I' the first half of the P values of m, arranged in the order of magnitude.

The remainder obtained by dividing $I'm$ by B is the index I relative to a progression of the system of base B.

When K' is zero, the first term of formula (2) gives, in each of the P progressions of base B, the P characteristics k corresponding to the P values of I.

Inasmuch as the characteristics k corresponding to the index I are the same when D is equal to either I' or m, it follows from Theorem I that it is sufficient to take the products $I'm$

starting from the value of m equal to the value of I'; that is to say, it is sufficient to take the values of $I'm$ starting from I'^2. We know that we apply the first term of formula (2) only to the values of m which are equal to the first $P/2$ indices. Moreover to the products of 1 by the indices correspond characteristics k which are evidently zero.

Consequently, among the P^2 characteristics k relative to the P divisors which equal the indices there are at most $P(P-2)/8$ characteristics whose determination requires a multiplication and a division.

8. As to the P characteristics k relative to a divisor D superior to $B - 1$ and with index I', we can deduce them immediately from the P characteristics found for $D = I'$ by making use of the last term of formula (2).

9. In order to apply formula (1), we can make use of a table of characteristics relative to the base B containing at the top of the columns only the first half of the P indices I arranged in order of magnitude, and below each index I_n the complementary index $B - I_n$; then in these columns, in regard to the prime divisors D, the values of k relative to the first half of the P indices I.

Then, having a number N which does not contain any of the prime factors of B, we divide N by B. This gives the quotient K and the remainder I, which I shall call I_n if it belongs to the first half of the P indices I arranged in order of magnitude, and $I_{n'}$ if it belongs to the second half of these indices.

When the remainder is I_n, the index is also I_n and the characteristic k is equal to the value k_n given in the table.

According as D is, or is not, a multiple of the difference $K - k_n$, D is, or is not, a prime divisor of the number whose index is I_n or of the number whose index is $I_{n'}$.

10. The table of characteristics relative to the base 30030, with the prime divisors from 17 to 30029 enables one to solve the problem in question between 1 and 30030^2 or 901800900.

Suppose that the table of characteristics k relative to the base B is formed of columns headed by all the indices I in order of magnitude and of rows headed by the prime divisors D arranged in the order of magnitude. The characteristic k corresponding to a number N of index I_n and to a prime divisor D is found at the intersection of the column I_n and the row D.

Let N be a number of the form $30030K + I$. In making the trial we will stop at the prime divisor D_n immediately inferior to $\sqrt{N}$.

We consider whether K is equal to one of the characteristics which correspond to the index I; for this it is sufficient to start from the prime divisor immediately superior to K.

When K is equal to one or several of these characteristics, N admits prime divisors which correspond to these characteristics. Then we have immediately the composition of N.

When K is not equal to any of these characteristics, we form the differences $K-k$ for the prime divisors 17, 19, 23, $\cdots$. These differences are always less than 30029, because K is here less than B and k is less than D and hence less than B. A difference $K-k$ is, or is not, equal to an index. In the former case, we recognize without calculation whether the difference $K-k$ is divisible by the divisor that corresponds to it. In the latter case we recognize nearly always whether a difference $K-k$ is divisible by the corresponding divisor D without performing the division; then we decompose $K-k$ into factors, one of which is either one of the prime numbers 2, 3, 5, 7, 11 and 13, or a product of some of these, and the other an index. In most cases it is not necessary to perform this decomposition in order to see if a difference is divisible by the prime divisor which corresponds to it.

If there is no difference $K-k$ that is divisible by any of the prime factors from 17 to D_n, N is prime. If we find a difference $K-k$ that is divisible by the prime divisor D less than D_n, N is divisible by D. We divide N by D, the resulting quotient also by D, and so on. Let N_1 be the last quotient thus obtained. We treat N_1 as we have just treated N, beginning with the prime divisor immediately following D, and we find that N_1 is the product of characteristics or is prime.

11. In order to recognize instantly whether a difference $K-k$ is divisible by the corresponding divisor D, it is sufficient to have, in addition to the table of characteristics relative to the base 30030 up to the divisor 30029, a table of remainders obtained by dividing the consecutive integers from 17 to 30029 by the divisors D; in fact, a difference $K-k$ is divisible by the corresponding divisor D, when the values of R and of k which correspond to this division are equal.

PARIS,
May, 1906.