AN ANNOUNCEMENT REGARDING FACTOR STENCILS

BY D. N. LEHMER

An edition of fifty sets of Factor Stencils has been completed and will shortly be distributed by the Carnegie Institution of Washington under whose auspices the work of construction has been done. The device is intended to facilitate the finding of factors of numbers of an order as high as two billion and a half.

The theory of the stencils is based on the well known fact that if R is known to be a quadratic residue of a number N then the factors of N are to be found in certain linear forms. Thus if -1 is known to be a residue of N, the factors of N are all of the form $4n+1$; and if 2 is a residue of N, the factors of N are of the form $8n \pm 1$; and so on. These linear forms may be combined and a set of linear forms deduced from them to limit the number of trials necessary to determine the character of the number N.

As the number R increases, however, the number of forms to be considered also increases so that the combination of the forms corresponding to two numbers R such as 113 and 199 would involve some 11,088 resulting forms. The straightforward combination of the linear forms becomes impossible except for very small values of R. Nevertheless large values of R will exclude the same proportion of trials as small values, and the stencil device is intended to make it possible to use values of R as high as ± 238. As each residue discovered serves to reject approximately half the number of trials, it is seen that for a number of the order of 2,000,000,000 where some 5,000 trial divisors must be examined, one residue reduces the number to about 2,500 trials; two to about 1,250; three to 625; four to 312; five to 78; six to 39; seven to 20; eight to 10; nine to 5; and ten to 2. The finding, therefore of

ten quadratic residues of N ought to be sufficient to find the factors of a number of the order of two billion. For smaller numbers, of course, a smaller list will serve. The only difficulty lies in the combination of the linear forms belonging to the residues. This difficulty is completely solved by the factor stencils. One does not seek to find the resultant forms of all the forms belonging to the residues, but only the primes that may lie in them. This is accomplished by a plan which is believed to be entirely new, and the work of examining a number is practically complete as soon as the list of residues is found. The construction of the Factor Stencils is as follows.

The first page of the list of primes published by the Carnegie Institution of Washington in 1914 contains 5,000 primes beginning with 1 and ending with 48,593. Any composite number not greater than 2,361,279,649, which is the square of 48,593, will have at least one of its factors in this list of primes. The list is arranged in fifty columns with one hundred rows in each column. A sheet of paper for a stencil is then ruled to show 5,000 cells, 50 columns and 100 rows. For a given R, holes are punched in those cells corresponding to primes which have R for a quadratic residue. Thus for $R=-1$ holes appear in the cells corresponding to the position in the list of primes of the numbers 1, 5, 13, 17, 29, 37, $\cdots$, and for $R=2$ the holes appear in the cells corresponding to the numbers 1, 7, 17, 23, 31, 41, 47, 71, 73, $\cdots$; the first set all having -1 for a residue and the second all having 2 for a residue. If these two stencils are superposed it is clear that those holes which appear through both indicate primes which are in both sets and have both -1 and 2 for residues. The first holes that thus appear are those corresponding to the primes 17 and 31. If now the stencil for a third residue is laid on the other two approximately half the remaining holes are covered and the holes that shine through the three stencils indicate primes that have all three numbers for quadratic residues. The problem of finding the factors of a number within the range of the first 2,000,000,000 numbers is reduced to the finding of some eight or ten quadratic residues.

In the book which accompanies the stencils various methods of finding quadratic residues are discussed and the method by means of the expansion of the square root of the number in a continued fraction is found to be by far the most effective. Various examples are given illustrating the power of the stencils, and a reproduction of the first page of the list of primes accompanies the work.

The plan of the stencils was first conceived in November 1924 and has been carried on since then under grants from the Carnegie Institution of Washington. Plans for the distribution of the sets are not yet completed, but every effort will be made to place them where they will be of most use.

THE UNIVERSITY OF CALIFORNIA

ON A PROBLEM IN THE THEORY OF GROUPS ARISING IN THE FOUNDATIONS OF INFINITESIMAL GEOMETRY*

BY H. P. ROBERTSON AND H. WEYL

In another paper in this issue,† the fundamental problem of infinitesimal geometry is formulated as the problem of uniquely associating with an arbitrary coordinate system on the manifold M a normal coordinate system on the tangent plane T_P by means of the fundamental coefficients of displacement on M.

The importance of the other aspect of this problem raised by O. Veblen and H. P. Robertson, yet remains: to associate a transformation of the given group $\mathfrak{G}$ with an arbitrary tranformation of the coordinates x in such a way that it gives rise to a representation by $\mathfrak{G}$, that is, that to composition of arbitrary transformations of x corresponds composition of the associated transformations of $\mathfrak{G}$. From

* Presented to the Society, June 21, 1929.

† This issue, pp. 716–725.