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