ON THE CONSTRUCTION OF FACTOR STENCILS*

BY D. N. LEHMER

The simple observation that if A and B are any two entries in a table of linear forms then the product AB is also an entry is of great importance in connection with the computation of such tables, as was pointed out in a previous paper.† The consequences of this theorem are of even greater importance in the construction of factor stencils, rendering unnecessary the computation of stencils for composite residues, and furnishing a valuable check on the accuracy of the work at every stage.

A factor stencil consists of a sheet of paper ruled in squares, each square representing a prime. In the stencils which the author is at present constructing under the auspices of the Carnegie Institution of Washington there are fifty columns and one hundred rows, which give a cell for each of the five thousand primes listed on the first page of his *List of Primes*, and includes all the primes from 1 to 48,593. For a given number a stencil is made which has holes punched in those squares which correspond to primes which have that number for a quadratic residue. The mere superposition of two different stencils will give at a glance the list of primes having the two corresponding numbers for residues. The problem of factorization is thus reduced to the problem of finding quadratic residues.

For each stencil there is a "conjugate" stencil obtained by punching out the squares left unpunched in the original. A stencil and its conjugate when superposed allow no holes to appear. We express this by the notation $(A)(A')=0$. If a new stencil is constructed by first cutting all the holes of A and then afterward all the holes of B the new stencil will show all the holes of A and B. We express this by the notation

*Presented to the Society, San Francisco Section, October 31, 1925.

† This BULLETIN, vol. 31 (1925), pp. 497–498.

$(A)+(B)=(C)$. In particular we have all the holes of the stencil cut when we add a stencil and its conjugate, which we express by $(A)+(A')=1$. It easily follows also that $(A)(A)=(A)$. Now the theorem referred to in the first paragraph will give also the important equations $(AB)=(A)(B)+(A')(B')$ and $(\overline{AB'})=(A)(B')+(A')(B)$. Thus, for example, the stencil for 15 is obtained by superposing the stencils for 3 and 5 and cutting out the holes that appear through each and then afterward superposing the conjugates of the stencils for 3 and 5 and cutting the holes that appear through each.

It is easily shown also that the distributive law holds for these operations. The formula for the stencil for the product of three factors is found to be

$$(ABC)=(A)(B)(C)+(A)(B')(C')+(A')(B)(C')+(A')(B')(C).$$

If in this we put $(B)=(C)$, the third and fourth terms drop out since $(B)(B')=0$. Also, since $(B)(B)=(B)$ the right side reduces to $(A)\ [(B)+(B')]=(A)$, which is the well known theorem that the set of linear forms for the residue AB^2 is the same as for the residue A. Similarly for four factors we get

$$\begin{aligned}(ABCD)=&(A)(B)(C)(D)+(A')(B')(C)(D)+(A')(B)(C')(D)\\&+(A)(B')(C')(D)+(A)(B')(C)(D')+(A)(B)(C')(D')\\&+(A')(B')\ (C')\ (D');\end{aligned}$$

if we now let $(B)=(C)$, using the same relations as before, we have $(A)(D)+(A')(D')$, which is (AB), as it should be.

From these developments comes a valuable check on the construction of the stencils. Thus the stencil for 21 may be obtained from the combinations of the stencils for 3 and 7 and their conjugates. It may also be obtained by combining the stencils for 15 and 35. The first method does not involve the use of the stencil for 5 and if that stencil contains any error we may look for a discrepancy in the results.

The device for cutting the stencils is already constructed and the stencils for -1 and for $+2$ and -2 with their conjugates are already completed.* The cutter will make as many as twenty-five copies at a time.

THE UNIVERSITY OF CALIFORNIA

* Some fifty stencils are completed at the time of printing of this paper.