A CONDENSED TABLE OF LINEAR FORMS*

BY P. H. DAUS

1. *Introduction.* In constructing his factor stencils,† D. N. Lehmer found it necessary to reconstruct the tables of linear forms for quadratic residues, due to the fact that all tables existing at that time contained errors.‡ The method of construction depended upon the observation that if a and b are numbers such that both belong or both do not belong to the form, then $c \equiv ab$, using the modulus of the form, belongs to the form. In particular, all powers of a number of the form belong to the form. The purpose of this paper is to indicate how a minimum number of entries may be made, from which all others may be obtained, and hence make it possible readily to check or construct the form for a given D. This is done with the aid of a table of odd primitive roots of primes, such tables being readily available.

2. *The Number of Required Entries.* It is well known that the linear forms are of the following types:

(1) $D \equiv 1 \pmod 4$, $2Dn + r_1, \cdots, r_{t_1}$, $t_1 = \phi(D)/2$,

(2) $D \equiv 2 \pmod 4$, $4Dn + r_1, \cdots, r_{t_2}$, $t_2 = 2\phi(D)$,

(3) $D \equiv 3 \pmod 4$, $4Dn + r_1, \cdots, r_{t_3}$, $t_3 = \phi(D)$,

where each r is an odd integer less than the indicated modulus, such that D is a quadratic residue of $2Dn+r$, whenever $2Dn+r$ is a prime for type (1), and similar statements for types (2) and (3), and where ϕ is the totient function, $\phi(D) = \phi(-D)$.

Let $D = \pm p_1 p_2 \cdots$, the p's being distinct primes, and let l be the least common multiple of p_1-1, p_2-1, $\cdots$; then the

* Presented to the Society, November 29, 1930.

† Published by the Carnegie Institution of Washington, 1929. See also *An announcement regarding factor stencils*, this Bulletin, vol. 35 (1929), p. 684.

‡ For tables of linear forms see M. Kraitchik, *Théorie des Nombres*, vol. 1, 1922, pp. 164–186, and *Recherches sur la Théorie des Nombres*, vol. 1, 1924, pp. 205–215. For a list of errors in these tables see D. H. Lehmer, this Bulletin, vol. 35 (1929), p. 865. These corrections have been republished by Kraitchik in his *Recherches sur la Théorie des Nombres*, vol. 2, 1929, pp. 180–182.

maximum exponent to which any integer belongs modulo D is l, and the existence of such integers follows from the existence of odd primitive roots of primes. For if ρ_i is an odd primitive root of p_i, then $\rho_i+2k_ip_i$ is also a primitive root of p_i, and since the set of linear diophantine equations

$$\rho_1 + 2k_1p_1 = \rho_2 + 2k_2p_2 = \cdots = \rho \tag{4}$$

always has a solution, it is possible to find a common primitive root of the p's, and ρ belongs to the exponent l modulo D. It is not necessary that an integer r be a common primitive root to belong to the exponent l, for evidently each p_i-1 contains the factor 2, and this factor need be introduced into the exponent only once.

If r_1 be any integer belonging to the exponent l, such that $(D/r_1)=1$, then the powers of r_1 are all incongruent with respect to the modulus of the form and account for l entries of the form. If $t_j/l=m$, $(j=1,2,3)$, then it is merely necessary to seek m entries $r_1, \cdots, r_i, \cdots, r_m$, such that $r_i \not\equiv r_1^k$, $(k=1, \cdots, l)$, and such that $(D/r_i)=1$. If D is positive and if $r_1^{l/2} \not\equiv -1$, using the modulus of the form, then the number of required entries may be reduced by half by using the $\pm$ sign with each entry.

3. *Linear Forms for a Prime.* Case 1. If $D=\pm p\equiv 1 \pmod 4$, and if ρ is any odd primitive root of p, then evidently $r\equiv\rho^2$ belongs to the form and r is the required entry, r^k, $(k=1, \cdots, (p-1)/2)$, giving all entries of the form. Case 2. If $D=\pm p\equiv 3 \pmod 4$, and if ρ is any odd primitive root of p, then D is a residue of either ρ or $\rho+2p$. Call the proper one r. Then r belongs to the exponent $p-1=t_3$ and hence the form is indicated by $4Dn+r^k$.

4. *Linear Forms for D Composite.* The determination of linear forms for a composite D is made to depend upon one or both of the following principles, illustrated by the case when D is the product of two primes. The method may be extended to the product of any number of primes, or the forms for the product of three primes may be made to depend upon those for two primes and so on. If $D=p_1p_2$, consider first the case when p_1-1 and p_2-1 have no common factor other than 2. Then by inspection of simple tables or the method indicated by (4), a common primitive root may be found. This root belongs to the

exponent l and from it proper entries may be found as in Case 2 above. Suppose secondly that p_1-1 is a factor of p_2-1, and that ρ is an odd primitive root of p_2. Consider the set of integers

$$\text{(A)} \qquad \rho,\ \rho + 2p_2,\ \rho + 4p_2,\ \cdots,$$

the number of entries being p_1, $2p_1$ or $2p_1$ according as $D \equiv 1$, 2 or 3 (mod 4). If $D \equiv 1 \pmod 4$, this set taken modulo $2p_1$ will be the odd numbers from 1 to $2p_1-1$ in some order, and hence will contain exactly the required number of r's, namely, $(p_1-1)/2$. They are incongruent to each other modulo $2D$ and also to r_1, $(k=1, 2, \cdots, l=p_2-1)$. For $r_1^k \equiv r_2 = r_1 + 2hp_2 \pmod{p_2}$ is impossible. Similarly, if $D \equiv 2$ or 3 (mod 4), the set taken modulo $4p_1$ will be the odd integers 1 to $4p_1-1$ in some order, and will contain exactly the required number, p_1-1, of r's, all of which are incongruent to each other and to r_1^k modulo $4D$.

In general if p_1-1 and p_2-1 have the common factor $2d$, we may form the set (A) from the primitive roots of p_2, and determine the r's. If $D \equiv 1 \pmod 4$, there will be $(p_1-1)/2$ of them, which divide into d subsets of $(p_1-1)/(2d)$ each, numbers of each subset being congruent modulo D, but incongruent to numbers of other subsets. For now $r_1^{(p_2-1)} \equiv 1$, and $r_1^k \equiv r_2 = r_1 + 2hp_2$ has solutions, the number being $l/(p_2-1) = (p_1-1)/(2d)$, all of which belong to one subset. Similarly, if $D \equiv 2$ or 3 (mod 4), the (p_1-1) r's divide into $2d$ subsets or, if we make $\pm$ entries, into d subsets. The selection of one r from each subset, r_1 being a common primitive root or at least belonging to exponent l, gives the complete set of entries.

5. *Numerical Illustrations.* In this manner a condensed table of linear forms may be constructed. We conclude with a few numerical illustrations based upon multiples of 13, the smallest odd primitive root of which is 7. The notation $2Dn + r_1^k\,(1, r_2, \cdots, r_m)$ indicates that the linear form is

$$2Dn + r_1,\ \cdots,\ r_1^k,\ r_2r_1,\ \cdots,\ r_2r_1^k,\ \cdots,\ r_mr_1^k.$$

$D = 13 \equiv 1 \pmod 4$, $7^2 \equiv 23 \pmod{26}$, $26n + 23^k$.

$D = -13 \equiv 3 \pmod 4$, $(D/7) = 1$, $52n + 7^k$.

$D = 26$, (A) 7, 33, 59, 85; 59 and 85 are r's, but since $\rho^6 \not\equiv -1 \pmod{104}$, only one is needed. $85 \equiv -19$, hence $104n \pm 19^k$.

$D=-26$, (A) as above, 7 and 85 are r's, $104n+7^k(1, 85)$.

$D=39$, two entries required, $(39/7)=1$, $156n\pm 7^k$.

$D=-39$, (A) 7, 33, 59; $59=r$, $78n+59^k$.

$D=65$, (A) 7, 33, 59, 85, 111; 7 and 33 are r's, $\rho^6\equiv -1 \pmod{130}$, so that $\pm$ signs are not available. $130n+7^k(1, 33)$.

$D=-65$, (A) 7, 33, 59, 85, 111, 137, 163, 189, 215, 241; the r's are readily found to be those $\equiv 11, 13, 17, 19 \pmod{20}$; the form is $260n+33^k(1, 59, 111, 137)$.

$D=143=11\times 13$, $l=60$, $m=2$, 7 is a common primitive root and so is 41, 7 is not an r, $7+2\times 143=293$ is, 41 is an r. Hence we may use either $572n\pm 293^k$ or $572n\pm 41^k$.

$D=-247=-13\times 19$, $l=36$, $m=3$, the r's of the set (A) are indicated by underscoring, while 33 is found to be a common primitive root.

(A) 7, $\underline{33}$, $\underline{59}$, 85, 111, 137, 163, $\underline{189}$, 215, $\underline{241}$, 267, $\underline{293}$, $\underline{319}$, $\underline{345}$, $\underline{371}$, 397, 423, $\underline{449}$, 475. The nine r's divide into three subsets by making use of 33^{12}, namely

$$(33, 59, 345), \quad (189, 293, 449), \quad (241, 319, 371),$$

and hence the form is

$$494n+33^k(1, 189, 241).$$

UNIVERSITY OF CALIFORNIA AT LOS ANGELES