THE LINEAR FORM OF NUMBERS REPRESENTED BY A HOMOGENEOUS POLYNOMIAL IN ANY NUMBER OF VARIABLES.[1]

BY MORGAN WARD.

1. In this paper I obtain the following necessary conditions that all of the numbers properly represented by a homogeneous polynomial in any number of variables may be of one or the other[2] of the linear forms

$$(1) \qquad nz,\ nz+a_1,\ \cdots,\ nz+a_r.$$

n here is any integer, and $a_1, \cdots, a_r$ are r distinct integers less than n and prime to it.[3]

THEOREM 1. *If all of the numbers properly represented by the homogeneous polynomial of degree N*

$$(2) \qquad H = H(x_1, x_2, \cdots, x_k) = \sum_{(s)} h_{(s)} x_1^{s_1} \cdot x_2^{s_2} \cdots x_k^{s_k}$$
$$(\textit{all the } h_{(s)} \textit{ integers})$$

are of one or the other of the forms (1), *and if*

$$n = p_1^{b_1} \cdots p_L^{b_L}$$

is the resolution of n into its prime factors, then it is necessary that the least common multiple of the numbers

$$p_1^{b_1-1}(p_1-1),\ \cdots,\ p_L^{b_L-1}(p_L-1)$$

divide rN.

We shall denote this least common multiple by $\lambda(n)$.

THEOREM 2. *Under the hypotheses of Theorem* 1, *the r numbers $a_1, \cdots, a_r$ in* (1) *must form q complete co-sets of the group G_τ of the N^{th} powers of the elements in the totient group of n.*

[1] Received January 21 and April 13, 1931.

[2] The form nz may be omitted without invalidating the theorems. Each of the other forms is assumed actually to occur.

[3] The problem becomes rather unwieldy if we remove the restriction that the a_i be prime to n. The simplest case is when all the numbers representable by the form are divisible by n; for polynomials in two variables, we have essentially the problem of determining all residual polynomials modulo n. See Dickson, Introduction to the Theory of Numbers, Chicago, (1929), Chapter II.

From Theorem 1, we see that[4] $\lambda(n) \leqq rN$. Since $\lambda(n)$ tends to infinity with n, we have the following corollary:

COROLLARY. *For a given r and N in* (1) *and* (2), *there are only a finite number of values of n satisfying the hypotheses of Theorem* 1.

Furthermore, we see from Theorem 2 that we must have

$$r = q\tau, \tag{3}$$

where τ is the order of the group G_τ.

2. Theorem 2 is readily established as follows.

Assume that the hypotheses of Theorem 1 are satisfied. Then for each a_i we can find a set of co-prime integers $c_1, c_2, \cdots, c_k$ such that[5]

$$H(c_1, c_2, \cdots, c_k) \equiv a_i \bmod n, \qquad (a_i, n) = 1.$$

Let s denote any integer prime to n. Then it is possible to choose k integers $z_1, z_2, \cdots, z_k$ so that the numbers

$$d_1 = z_1 n + s c_1, \ d_2 = z_2 n + s c_2, \ \cdots \ d_k = z_k n + s c_k$$

are co-prime. The number $m = H(d_1, d_2, \cdots, d_k)$ is accordingly properly represented by the form H. Hence since H is homogeneous of degree N,

$$m \equiv s^N H(c_1, c_2, \cdots, c_k) \equiv s^N a_i \not\equiv 0 \bmod N.$$

But m must be congruent modulo n to some one of the a_i; therefore the numbers

$$s^N a_i, \qquad (i = 1, 2, \cdots, r), \quad (s, n) = 1, \tag{4}$$

are all congruent modulo n to one or the other of the numbers a_i in (1).

Now if $G_{\varphi(n)}$ denotes the totient group of n, the Nth powers of all the elements of $G_{\varphi(n)}$ form a sub-group G_τ of order $\tau \leqq \varphi(n)$. Hence for a given a_i, the numbers (4) are congruent modulo n to the τ numbers of some co-set of G_τ in $G_{\varphi(n)}$. Since the numbers a_i are all distinct and all in $G_{\varphi(n)}$, Theorem 2 follows.

The proof of Theorem 1 is now immediate. For if g is any element of G_τ, $g^\tau \equiv 1 \bmod n$. Hence since the elements of G_τ are congruent to the Nth powers of the elements of $G_{\varphi(n)}$, $s^{N\tau} \equiv 1 \bmod n$, so that by (3)

[4] That rN is actually the "best possible" maximum for $\lambda(n)$ is shown by the case $N = 3$, $r = 2$, $n = 7$, $a_1 = 1$, $a_2 = 6$. For $H = (x_1 + x_2 + \cdots + x_k)^3$, we find that $\lambda(n) = rN = 6$.

[5] We use when convenient the standard notation $(a, b, \cdots, c)$ for the greatest common divisor of the numbers $a, b, \cdots, c$.

$$s^{rN} \equiv 1 \mod n$$

for every integer s prime to n.

Accordingly, if $\lambda(n)$ is the least positive value of u such that $s^u \equiv 1 \mod n$ for all integers s prime to n, $\lambda(n)$ divides rN.

But if $n = p_1^{b_1} \cdots p_L^{b_L}$ is the resolution of n into its prime factors, $\lambda(n)$ is precisely[6] the L. C. M. of $p_1^{b_1-1}(p_1 - 1), \cdots, p_L^{b_L-1}(p_L - 1)$.

3. As an application of these theorems, let us consider the problem[7] of obtaining primitive binary forms

$$H(x_1; x_2) = \sum_{s=0}^{N} h_s x_1^{N-s} x_2^s$$

of degree N such that the prime factors of all of the numbers properly represented by H are either divisors of n or of the form $nz \pm 1$ (so that n is necessarily even). Examples of such forms, due to Lehmer, place cited, are $x^3 + 16x^2y - 51xy^2 - y^3$ for $n = 14$ and $x^3 - 18x^2y + 69xy^2 - y^3$ for $n = 18$.

These forms are obviously included in the more general category of forms which properly represent only numbers of the types nz, $nz + a_1$, $nz + a_2$ with a_1, a_2 prime to n. Hence by Theorem 1 and equation (3), we must have $\lambda(n)$ a divisor of $2N$ and $\tau \leq 2$.

For example, suppose that $N = 3$. $\lambda(n) = 1$ has the solution $n = 2$; $\lambda(n) = 2$ the four solutions 3, 4, 6, 12 while $\lambda(n) = 6$ has the twelve solutions 7, 9, 14, 18, 21, 28, 36, 42, 63, 84, 126, 252. Of the even values of n, the cases $n = 2$, 4 and 6 are trivial since every prime save 2 is of the form $2k + 1$ and $4k \pm 1$ and every prime save 2 and 3 is of the form $6k \pm 1$. On the other hand in the cases 12, 28, 36, 42, 84, 126 and 252, $\tau > 2$. Hence $n = 14$ and $n = 18$ are the only non-trivial values of n for which such cubic forms can exist. In a similar manner one can show that 22 is the only non-trivial value of n for which such quintic forms can exist, and that there are no non-trivial values of n for septimic forms.

[6] Dickson, Work cited, p. 19.

[7] See D. H. Lehmer, An Extended Theory of Lucas' Functions. Annals, Vol. 31 (1930), p. 436. Dr. Lehmer has informed me that since the paper was written he has considerably extended his results on this problem.