THE NUMBERS OF SOLUTIONS OF CONGRUENCES INVOLVING ONLY kTH POWERS*

BY

RALPH HULL

Introduction. The problem to determine the number of solutions of the congruence

$$\sum_{\nu=1}^{s} x_\nu^k \equiv a \pmod{p}, \qquad k \geqq 1,\ s \geqq 1,\ p \text{ a prime}, \tag{1}$$

is of interest in connection with Waring's Problem and also in connection with the finding of resolvent equations for the irreducible cyclotomic equation†

$$x^{p-1} + x^{p-2} + \cdots + x + 1 = 0, \qquad p \text{ an odd prime}. \tag{2}$$

It is the purpose of this paper to obtain general formulas for the number of solutions of (1) which cover all cases, and at the same time to obtain certain results for more general congruences of the type

$$\sum_{\nu=1}^{s} a_\nu x_\nu^k \equiv a \pmod{n} \qquad (s \geqq 1,\ k \geqq 1), \tag{3}$$

where $a_1, \cdots, a_s$, a and n are any integers. By the number of solutions of (3) is meant the number of sets of integers $x_1, \cdots, x_s$ satisfying (3) and such that $0 \leqq x_\nu < n (\nu = 1, \cdots, s)$. A solution $x_1, \cdots, x_s$ of (3) is said to be primitive in case at least one of $x_1, \cdots, x_s$ is prime to n.

We pass at once to the consideration of congruences of the type (3) with n a power of a prime. For such congruences, with $a_\nu = 1 (\nu = 1, \cdots, s)$, Landau,‡ in connection with his exposition of the Hardy-Littlewood theorems on Waring's Problem, has given reduction formulas by means of which the numbers of solutions for higher powers of the prime may be obtained from those for lower powers. Similar formulas can be shown to hold under certain conditions when the coefficients are more general.

V. A. Lebesgue§ discussed at some length congruences of the type

---

* Presented to the Society, August 31, 1932; received by the editors May 29, 1932.

† For an exposition of Gauss' method for the solution of this equation see Bachmann, *Die Kreisteilung*, pp. 43–58. For other references, see the Bulletin of the National Research Council, Bulletin 28, February, 1923, Chapter II.

‡ Landau, *Vorlesungen über Zahlentheorie*, vol. I, pp. 280–292.

§ Lebesgue, *Journal de Mathématiques*, vol. 2 (1837), pp. 253–292; vol. 3 (1838), pp. 113–144. The second paper (1838) deals with the applications.

$$\sum_{\nu=1}^{s} a_\nu x_\nu^m \equiv a \pmod{p = hm + 1}, \quad m \geqq 2, \ p \text{ an odd prime}, \tag{4}$$

with a view to the application of his results to the finding of resolvent equations for (2). His method consisted, first, in obtaining a congruence giving the residue modulo p of the number of solutions of (4) by means of which, for small primes and $s=1$ or 2, this number could be found; second, in showing that the number of solutions of (4) in case $s>2$ may ultimately be found from the numbers of solutions of congruences in one or two unknowns; and third, in obtaining a formula for the number of solutions of (4) which involves the roots of (2).

The methods of this paper are similar to those of Lebesgue with certain modifications and extensions. It is shown that a congruence (3), with n a prime, is equivalent, for the problem under discussion, either to a linear congruence, in which case complete results are known, or to a congruence of the type (4). The greater part of the following discussion is concerned with congruences of the latter type.

The formulas here obtained for the number of solutions of

$$\sum_{\nu=1}^{s} x_\nu^m \equiv a \pmod{p = hm + 1}, \quad m \geqq 2, \ p \text{ an odd prime}, \tag{5}$$

are of the nature of recursion formulas. For $m=2$ they may be obtained from those of Jordan quoted in §3. For $m \geqq 3$, the formulas depend upon certain integers for the determination of which a general method is given. These results also include a method of determining the coefficients of the reduced form of the $m$ic resolvent of (2), with $p=hm+1$.

The case $m=5$ is treated in detail by a special method, and the integers mentioned above are expressed in terms of an integral solution of two simultaneous quadratic Diophantine equations in four variables which are shown to have exactly eight distinct solutions for any given prime of the form $5h+1$. These simultaneous equations play the same rôle for the case $m=5$ as that played by the well known single equations $x^2+27y^2=4p$ and $x^2+4y^2=p$, for primes of the forms $3h+1$ and $4h+1$, respectively, in the determination of the cubic and biquadratic resolvents of (2) for these cases, respectively.

In the final section, which is independent of the earlier sections except the first, are discussed sufficient conditions on s in order that (3), for a given $k \geqq 2$ and $a_\nu = 1$ $(\nu = 1, \cdots, s)$, may have a solution for every choice of integers a and n.

1. **Congruences with a composite modulus.** Before passing to the case of

a prime modulus to which the greater part of this paper is devoted, we state* some results for the congruence (3).

THEOREM 1. *Let* $n=p_1^{l_1}\cdots p_r^{l_r}$ *where* $p_1, \cdots, p_r$ *are distinct primes and* $l_i \geqq 1$ $(i=1, \cdots, r)$. *Then the number of solutions of* (3) *is the product of the numbers of solutions of the r congruences*

$$\sum_{\nu=1}^{s} a_\nu x_\nu^k \equiv a \pmod{p_i^{l_i}} \qquad (i = 1, \cdots, r).$$

The theorem follows easily from the

LEMMA. *Let* $F=F(x_1, \cdots, x_s)$ *be a polynomial with integral coefficients in the s variables* $x_1, \cdots, x_s$, *and let N and N′ be the numbers of solutions of*

$$F \equiv 0 \pmod{n} \tag{6}$$

and

$$F \equiv 0 \pmod{n'} \tag{7}$$

respectively. Then if n and n′ are relatively prime the number of solutions of

$$F \equiv 0 \pmod{nn'} \tag{8}$$

is NN'.

Evidently to every solution of (8) corresponds a solution of (6) and a solution of (7). Conversely, let $(x_1, \cdots, x_s)$ and $(x_1', \cdots, x_s')$ be solutions of (6) and (7) respectively. Then $(x_1+\xi_1 n, \cdots, x_s+\xi_s n)$ and $(x_1'+\xi_1' n', \cdots, x_s'+\xi_s' n')$, where ξ_ν and ξ_ν' $(\nu=1, \cdots, s)$ are any integers, satisfy (6) and (7) respectively. Since n is prime to n',

$$\xi_\nu n \equiv x_\nu' - x_\nu \pmod{n'} \qquad (\nu = 1, \cdots, s)$$

determine $\xi_1, \cdots, \xi_s$ uniquely modulo n'. Then there exist integers $\xi_1', \cdots, \xi_s'$ such that

$$X_\nu = x_\nu + \xi_\nu n = x_\nu' + \xi_\nu' n' \qquad (\nu = 1, \cdots, s),$$

and $X_1, \cdots, X_s$ are determined uniquely modulo nn' and satisfy (8), since n and n' are relatively prime.

The following notation is that of Landau (loc. cit.) except that we here let $k \geqq 1$ instead of restricting k to be $\geqq 2$, the latter restriction not being necessary for the present purpose. For fixed $k \geqq 1$ and $s \geqq 1$, $M(p^l; a)$ and $N(p^l; a)$ denote the number of solutions and the number of primitive solutions, respectively, of

* The lemma is stated by Hermite, Journal für Mathematik, vol. 47 (1854), pp. 351–7; Oeuvres, vol. 1, p. 243. Theorems 2 and 3 are proved by Landau (loc. cit.).

$$\sum_{\nu=1}^{s} x_\nu^k \equiv a \pmod{p^l} \qquad (p \text{ a prime}, l \geqq 1). \tag{9}$$

Let

$$k = p^\theta k_0 \qquad (\theta \geqq 0, k_0 \text{ prime to } p), \tag{10}$$

$$\gamma = \theta + 1 \text{ or } \theta + 2 \text{ according as } p > 2 \text{ or } p = 2,$$

$$p^\gamma = P.$$

THEOREM 2. *If* $l \geqq \gamma$,

$$N(p^l; a) = p^{(s-1)(l-\gamma)} N(P; a).$$

THEOREM 3. *Assume* $a \not\equiv 0$. *Let* $a = p^{\beta k+\sigma} a_0$, $\beta \geqq 0$, $0 \leqq \sigma < k$, a_0 *prime to* p. *Then if* $l \geqq \beta k + \sigma + 1$, *whence* $a \not\equiv 0 \pmod{p^l}$,

$$M(p^l; a) = \sum_{\alpha=0}^{\beta} p^{\alpha(k-1)s} N(p^{l-\alpha k}; a/p^{\alpha k}).$$

THEOREM 4. *Let* $l = \delta k + \epsilon$, $\delta \geqq 0$, $0 \leqq \epsilon < k$, δ *and* ϵ *not both zero so that* $l \geqq 1$. *Then if* $\epsilon > 0$ *and* $\delta \geqq 0$,

$$M(p^l; 0) = \sum_{\alpha=0}^{\delta} p^{\alpha(k-1)s} N(p^{l-\alpha k}; 0) + p^{(l-\delta-1)s};$$

if $\epsilon = 0$, $\delta > 0$,

$$M(p^l; 0) = \sum_{\alpha=0}^{\delta-1} p^{\alpha(k-1)s} N(p^{l-\alpha k}; 0) + p^{(l-\delta)s}.$$

In view of Theorem 1 we may restrict attention to the case of (3) when n is a power of a prime. If, further, the coefficients in (3) are all unity, we need only consider powers of the prime at most equal to the corresponding P, defined as in (10), and then determine the numbers of solutions for higher powers by Theorems 2, 3 and 4. In particular, if p is an odd prime not dividing k and the coefficients are all unity, the problem for any power of the prime reduces to the case of a prime modulus. Similar results to those of Theorems 3 and 4 hold for arbitrary coefficients. An inspection of Landau's proof of Theorem 2 will show that similar results to those of this theorem hold for any set of coefficients each of which is prime to the modulus, but, if the coefficients do not satisfy this condition, such results do not necessarily hold.

2. **Preliminary results for a prime modulus.** We state* here a number of general theorems and introduce notation in terms of which relations are given which will be needed in §§3 and 4.

* For the details of the proofs of Theorems 5, 7, 8 and 11, see Lebesgue's paper of 1837 (loc. cit.).

THEOREM 5. *Let $F=F(x_1, \cdots, x_s)$ be a polynomial with integral coefficients in the s variables $x_1, \cdots, x_s$, and let S denote the number of solutions of $F\equiv 0 \pmod p$, p a prime. Then*

$$S \equiv (-1)^{s+1} \sum C \pmod p,$$

where $\sum C$ denotes the sum of the coefficients of the terms $Cx_1^a \cdots x_s^g$ of the expansion of F^{p-1} in which each of the exponents $a, \cdots, g$ is a multiple >0 of $p-1$.

The proof follows from the well known theorem that if $r \geqq 1$,

$$\sum_{x=0}^{p-1} x^r \equiv 0 \text{ or } 1 \pmod p$$

according as $r \not\equiv 0$ or $r \equiv 0 \pmod{p-1}$, and by noting that $F^{p-1} \equiv 0$ or $F^{p-1} \equiv 1 \pmod p$ according as $F \equiv 0$ or $F \not\equiv 0 \pmod p$.

Henceforth, in discussing the congruence

$$\sum_{\nu=1}^{s} a_\nu x_\nu^k \equiv a \pmod p, \qquad p \text{ a prime}, \tag{11}$$

we shall assume

$$a_1 \cdots a_s \not\equiv 0 \pmod p, \tag{12}$$

since other cases are easily reduced to this.

THEOREM 6. *Let m be the greatest common divisor of k and $p-1$, and let $p-1=hm$. Then the number of solutions of* (11) *is the same as the number of solutions of*

$$\sum_{\nu=1}^{s} a_\nu x_\nu^m \equiv a \pmod{p = hm+1}. \tag{13}$$

This theorem follows from the well known theorem that the number of solutions of the binomial congruence $x^l \equiv b \pmod p$ is 1 in case $b \equiv 0 \pmod p$, 0 or d in case $b \not\equiv 0 \pmod p$ according as $b^q \not\equiv 1$ or $b^q \equiv 1 \pmod p$, where d is the greatest common divisor of l and $p-1$ and $p-1=dq$. For, consider the linear congruence

$$\sum_{\nu=1}^{s} a_\nu z_\nu \equiv a \pmod p. \tag{14}$$

It is clear that to a solution of (14) there corresponds exactly the same number of solutions of (11) as of (13) by

$$x_\nu^k \equiv z_\nu, \quad x_\nu^m \equiv z_\nu \pmod p \qquad (\nu = 1, \cdots, s)$$

and the theorem quoted.

In case $m=1$, the number of solutions of (13) is p^{s-1}. Henceforth we assume $m \geqq 2$, $p=hm+1$, $h \geqq 1$. It proves convenient to write (13) in a different form. Let g be a primitive root modulo p. Then, in view of (12), there exist non-negative integers $\alpha_1, \cdots, \alpha_m$ such that $a_\nu \equiv g^{\alpha_\nu} \pmod{p}$ $(\nu=1, \cdots, s)$, and, in case $a \not\equiv 0 \pmod{p}$, we may write $a \equiv g^{\alpha} \pmod{p}$. We write (13) in the form

$$A = \sum_{\nu=1}^{s} g^{\alpha_\nu} x_\nu^m \equiv 0 \pmod{p = hm+1}, \tag{15}$$

or in the form

$$A = \sum_{\nu=1}^{s} g^{\alpha_\nu} x_\nu^m \equiv g^{\alpha} \pmod{p = hm+1}, \tag{16}$$

making the change of notation indicated. It is obvious that the integers $a_1, \cdots, a_s$ and a may be reduced modulo m without affecting the number of solutions of (15) or of (16). We make use of this repeatedly in what follows.

Let R be any root of (2). It is shown* in the theory of cyclotomy that if g is any primitive root modulo $p=hm+1$, the m periods $\eta_0, \cdots, \eta_{m-1}$ of the roots of (2) defined by

$$\eta_i = \sum_{j=0}^{h-1} R^{g^{jm+i}} \qquad (i = 0, \cdots, m-1)$$

are the roots of an equation of the form

$$\eta^m + b_1\eta^{m-1} + \cdots + b_{m-1}\eta + b_m = 0,$$

where $b_1, \cdots, b_m$ are integers independent of R and g. Also, for any integer k,

$$\eta_{i+km} = \sum_{j=0}^{h-1} R^{g^{jm+km+i}} = \eta_i.$$

For any integer a, we define

$$\xi_a = 1 + m\eta_a.$$

Then $\xi_0, \cdots, \xi_{m-1}$ are the roots of an equation of the form

$$\xi^m - c_2\xi^{m-2} - \cdots - c_{m-1}\xi - c_m = 0, \tag{17}$$

where $c_2, \cdots, c_m$ are integers.

* For example, see Bachmann, loc. cit.

THEOREM 7. *Let* $A(0)$ *denote the number of solutions of* (15). *Then*

$$pA(0) = p^s + hT(a_1, \cdots, a_s),$$

where

$$T(a_1, \cdots, a_s) = \sum_{j=0}^{m-1} \xi_{a_1+j} \cdots \xi_{a_s+j}.$$

For any root, R, of (2), and any integer a,

$$\sum_{r=0}^{p-1} R^{ra} = 0 \text{ or } p$$

according as $a \not\equiv 0$ or $a \equiv 0 \pmod{p}$. Hence it is easy to see that

$$pA(0) = \sum \sum_{r=0}^{p-1} R^{rA},$$

where the outer summation is taken over $x_\nu = 0, \cdots, p-1$ $(\nu = 1, \cdots, r)$. The formula of the theorem follows if the right member of this equation is reduced by a procedure similar to that of Lebesgue (loc. cit. (1837), pp. 287–290).

From the form of $T(a_1, \cdots, a_s)$ it follows that, for a fixed primitive root g modulo p and a given set of exponents $a_1, \cdots, a_s$, this sum is independent of the root R of (2). On the other hand, for a given set of exponents $a_1, \cdots, a_s$, this sum depends in general upon the primitive root g modulo p, but it is understood in what follows that, for a given prime p, g is fixed throughout.

THEOREM 8. *Let*

$$B = \sum_{u=1}^{t} g^{b_u} y_u^m, \quad C = A + B, \quad C' = A - B,$$

and let $A(0)$, $A(g^a)$ *denote the numbers of solutions of* (15) *and* (16) *respectively. Similarly define* $B(0)$, $C(0)$, *etc. Then, if* h *is even,*

$$C(0) = C'(0) = A(0) \cdot B(0) + h \sum_{j=0}^{m-1} A(g^j) B(g^j);$$

if h *is odd,*

$$C'(0) = A(0)B(0) + h \sum_{j=0}^{m-1} A(g^j) B(g^j),$$

$$C(0) = A(0)B(0) + h \sum_{j=0}^{m-1} A(g^j) B(g^{j+m/2}).$$

The integers $1, \cdots, p-1$ are congruent modulo p, in some order, to the integers

$$g^0 = 1, g, g^2, \cdots, g^{p-2},$$

where, since $p=hm+1$, exactly h of the exponents are congruent to $j \pmod m$ for $j=0, \cdots, m-1$. To determine $C'(0)$ we require $A \equiv B \pmod p$ and consider

$$A \equiv B \equiv 0, \quad A \equiv B \equiv g^r \pmod p \quad (r = 0, \cdots, p-2).$$

The formula of the theorem follows by remarks made above. To determine $C(0)$ we require $A \equiv -B \pmod p$ and a distinction arises according as h is even or odd on account of the relation

$$-1 \equiv g^{(p-1)/2} \pmod p,$$

which holds for any primitive root modulo p, since $(p-1)/2 \equiv 0$ or $m/2 \pmod m$ according as h is even or odd where m is evidently even if h is odd.

By means of Theorem 8 the number of solutions of (15), or of (16), for $s>2$, can ultimately be found from the numbers of solutions of congruences in 1 or 2 unknowns. This idea is developed further in the next section and for that purpose we introduce the following notation. Suppose $m \geqq 2$, $p=hm+1$ and g are fixed. Let $M_s^{(a)}$ and $M_1^{(a)}$ $(s \geqq 2, a \geqq 0)$ denote the numbers of solutions of

$$\sum_{\nu=1}^{s} x_\nu^m + g^a x_s^m \equiv 0, \quad g^a x_1^m \equiv 0 \pmod p,$$

respectively; let $N_s^{(a)}$ and N_{ab} $(s \geqq 1; a, b \geqq 0)$ denote the numbers of solutions of

$$\sum_{\nu=1}^{s} x_\nu^m \equiv g^a, \quad x_1^m + g^a x_2^m \equiv g^b \pmod p,$$

respectively; let M_{ab} denote the number of solutions of

$$x_1^m + g^a x_2^m + g^b x_3^m \equiv 0 \pmod p.$$

In view of remarks made above we have

$$N_{ab} = N_{ij}, \; M_{ab} = M_{ij}, \qquad i \equiv a, j \equiv b \pmod m, \quad 0 \leqq i, j < m,$$

and we define N_{ab} and M_{ab} by these equations for a and b not necessarily $\geqq 0$.

THEOREM 9. *For h even or odd, $N_1^{(a)}=0$ or m according as $a\not\equiv 0$ or $a\equiv 0 \pmod m$, and $M_1^{(a)}=1$ for every a. If h is even, $M_2^{(a)}=1$ or $1+m(p-1)$ according as $a\not\equiv 0$ or $a\equiv 0 \pmod m$; if h is odd, $M_2^{(a)}=1$ or $1+m(p-1)$ according as $a\not\equiv m/2$ or $a\equiv m/2 \pmod m$.*

The results stated in this theorem* are well known consequences of the theory of indices and they are independent of the primitive root g.

By means of Theorems 8 and 9 we easily obtain

THEOREM 10. *If h is even*

$$(p-1)N_s^{(a)} = M_{s+1}^{(a)} - M_s^{(0)}, \quad (p-1)N_{ab} = M_{ab} - M_2^{(a)},$$
$$(p-1)N_{0b} = M_{0b} - M_2^{(0)} = M_3^{(b)} - M_2^{(0)};$$

if h is odd,

$$(p-1)N_s^{(a)} = M_{s+1}^{(a+m/2)} - M_s^{(0)}, \quad (p-1)N_{ab} = M_{a,b+m/2} - M_2^{(a)},$$
$$(p-1)N_{0b} = M_{0,b+m/2} - M_2^{(0)} = M_3^{(b+m/2)} - M_2^{(0)}.$$

For example, suppose h is even and let

$$A = \sum_{r=1}^{s} x_r^m, \quad B = g^a y^m.$$

Then by Theorem 8 and the above definitions,

$$M_{s+1}^{(a)} = M_s^{(0)} M_1^{(a)} + h \sum_{j=0}^{m-1} N_s^{(j)} N_1^{(j-a)}.$$

The first relation of the theorem follows from Theorem 9. The other relations are proved similarly.

THEOREM 11.

$$M_s^{(0)} + \sum_{r=0}^{p-1} N_s^{(r)} = M_s^{(0)} + h \sum_{j=0}^{m-1} N_s^{(j)} = p^s,$$
$$M_2^{(a)} + h \sum_{j=0}^{m-1} N_{aj} = p^2.$$

THEOREM 12. *If h is even,*

$$N_{ij} \equiv -\sum_{r=1}^{m-1} \sum_{t=0}^{r-1} \binom{r\ h}{t\ h} g^{(r-t)hi+tjh} \pmod p;$$

if h is odd,

* For a proof based on Theorem 5, see Lebesgue (loc. cit. (1837), pp. 256–7, 260).

$$N_{ij} \equiv -\sum_{r=1}^{m-1}\sum_{t=0}^{r-1}\binom{r}{t}\binom{h}{h}g^{(r-t)h(i+m/2)+tjh} \pmod{p},$$

where

$$\binom{u}{0} = 1, \quad \binom{u}{v} = u!/(v!(u-v)!) \qquad (0 < v < u).$$

In Theorem 5 take $F = x_1^m + g^i x_2^m - g^j$ and the theorem follows at once.

We note that certain relations hold modulo p between the binomial coefficients that appear in these formulas when $m > 2$. These relations may be obtained by noting that, for $t = 1, \cdots, m$,

$$H_t = (th)\cdots(th-h+1) \equiv (-1)^h H_{m-t+1} \pmod{p}.$$

In view of a theorem of Lebesgue (loc. cit. (1837), p. 260) to the effect that N_{ij} is a multiple of m less than mp, Theorem 12 affords a means of determining N_{ij} completely. This method is not practicable, however, for large primes. The following theorem affords an easier method for any given case provided a table of the indices of the integers $1, \cdots, p-1$ with respect to g is available. Let u be any integer of the set

$$1, 2, \cdots, p-2. \tag{18}$$

We denote* by K_{ab} the number of integers in the set (18) for which

$$\operatorname{Ind}_g u \equiv a, \quad \operatorname{Ind}_g (u+1) \equiv b \pmod{m}. \tag{19}$$

THEOREM 13. *According as h is even or odd,*

$$N_{ij} = K_{i-j,-j}m^2 + rm \quad \text{or} \quad N_{ij} = K_{i-j+m/2,-j}m^2 + rm,$$

where, in both cases, $r = 0$ in case $i-j \not\equiv 0, j \not\equiv 0 \pmod{m}$, $r = 1$ in case $i-j \not\equiv 0$, $j \equiv 0$ or $i-j \equiv 0, j \not\equiv 0 \pmod{m}$ and $r = 2$ in case $i-j \equiv j \equiv 0 \pmod{m}$.

Case 1. *h even.* We have $\operatorname{Ind}(-1) \equiv 0 \pmod{m}$ whence N_{ij} is the number of solutions of

$$g^{m-j}x^m \equiv g^{m+i-j}y^m + 1 \pmod{p}, \tag{20}$$

where $m-j > 0$ and $m+i-j > 0$. Suppose (20) has a solution x, y such that

$$xy \not\equiv 0 \pmod{p}. \tag{21}$$

Then

$$u \equiv g^{m+i-j}y^m \pmod{p} \tag{22}$$

* Gauss made use of these integers for $m = 3$ in his discussion of cyclotomic equations. *Recherches Arithmétiques*, p. 468; Werke, I, p. 445.

determines a unique integer of the set (18) since $u \equiv p-1$ would imply $x \equiv 0 \pmod{p}$ by (20), and we have (19) with $a = i-j$, $b = -j$. Conversely, for every u of (18) such that (19) hold with $a = i-j$, $b = -j$, (22) determines exactly m distinct values of y modulo p, and

$$g^{m-i}x^m \equiv u + 1 \pmod{p}$$

determines exactly m values of x modulo p. Hence to each u as described there correspond exactly m^2 distinct solutions of (20) and (21). It is clear that to distinct u's satisfying the conditions prescribed the corresponding solutions of (20) and (21) are distinct. To complete the proof of the theorem for Case 1, there remains only the consideration of possible solutions of (20) not satisfying (21). The details follow easily from Theorem 9.

Case 2. h odd. In this case $\text{Ind}\,(-1) \equiv m/2 \pmod{m}$ and N_{ij} is the number of solutions of

$$g^{m-i}x^m \equiv g^{m+m/2+i-j} + 1 \pmod{p}.$$

The proof now proceeds exactly as for Case 1.

THEOREM 14. *For any set of integers $a_1, \cdots, a_s$ and any primitive root g modulo p, $T(a_1, \cdots, a_s)$ is an integer divisible by mp.*

The theorem will follow from Theorem 7 when we have shown that $pA(0) - p^s$ is divisible by $p-1 = hm$. It is easily shown that

$$A(g^i) \equiv 0 \pmod{m} \qquad (i = 0, \cdots, m-1),$$

and, by the same argument used in proving Theorem 11,

$$A(0) + h\sum_{i=0}^{m-1} A(g^i) = p^s.$$

Hence,

$$pA(0) - p^s = p^{s+1} - p^s - hp\sum_{i=0}^{m-1} A(g^i) \equiv 0 \pmod{p-1}.$$

3. Recursion formulas for a prime modulus. We find here recursion formulas for $M_s^{(0)}$ and $N_s^{(i)}$ $(i = 0, \cdots, m-1;\ s \geqq 1;\ m \geqq 2)$. These complete the discussion of (1) for all cases in view of Theorem 6 and known formulas for linear congruences. It proves convenient to deal with $M_s^{(i)}$ $(i = 0, \cdots, m-1)$ and obtain $N_s^{(i)}$ by means of Theorem 10.

We first define $\lambda_2^{(i)}$ by

$$M_2^{(i)} = p + \lambda_2^{(i)}(p-1) \qquad (i = 0. \cdots, m-1). \tag{23}$$

By Theorem 9 we have

(24) $\lambda_2^{(i)} = -1$ or $m-1$ according as $i \not\equiv 0$ or $i \equiv 0 \pmod m$ (h even),

and

(25) $\lambda_2^{(i)} = -1$ or $m-1$ according as $i \not\equiv m/2$ or $i \equiv m/2 \pmod m$ (h odd).

Next, let

$$M_{ij} = p^2 + \lambda_{ij}(p-1) \qquad (i, j = 0, \cdots, m-1), \tag{26}$$

where the M_{ij} are as defined in §2. For any integers a and b we define λ_{ab} by

$$\lambda_{ab} = \lambda_{ij} \qquad (i \equiv a, j \equiv b \pmod m, \quad 0 \leqq i, j < m),$$

and a similar extension of definition is to be understood, in this section and §4, in all cases where subscripts or superscripts have reference to exponents of the primitive root g modulo p employed in the definitions. It is easily shown that

$$M_{ij} = M_{ji} = M_{-i,j-i} = M_{j-i,-i} = M_{-j,i-j} = M_{i-j,-j}.$$

Hence, by (26),

$$\lambda_{ij} = \lambda_{ji} = \lambda_{i-j,-j} = \lambda_{-j,i-j} = \lambda_{-i,j-i} = \lambda_{j-i,-i}. \tag{27}$$

By Theorem 7,

$$pM_{ij} = p^3 + hT(0, i, j).$$

Hence

$$mp\,\lambda_{ij} = T(0, i, j),$$

and the λ_{ij} are integers by Theorem 14. Theorem 10 yields

$$N_{ij} = p - \lambda_2^{(i)} + \lambda_{ij} \qquad (h \text{ even}), \tag{28}$$

and

$$N_{ij} = p - \lambda_2^{(i)} + \lambda_{i,j+m/2} \qquad (h \text{ odd}). \tag{29}$$

Finally, by Theorem 11,

$$\sum_{j=0}^{m-1} \lambda_{ij} = 0 \qquad (i = 0, \cdots, m-1), \tag{30}$$

whence, by (27),

$$\sum_{i=0}^{m-1} \lambda_{ij} = 0 \qquad (j = 0, \cdots, m-1). \tag{31}$$

The cases h even and h odd are considered separately in Theorems 15 and 16 respectively.

THEOREM 15. *If h is even,*

$$M_s^{(i)} = p^{s-1} + (p-1)\sum_{t=2}^{m} F_{s-t}\lambda_t^{(i)} \quad (m \geqq 2;\ i = 0, \cdots, m-1;\ s \geqq 1), \tag{32}$$

where, for $m \geqq 2$, $\lambda_2^{(i)}$ is given by (24);

$$\lambda_3^{(i)} = \lambda_{0i} = (1/m)\sum_{j=0}^{m-1}\lambda_{ij}\lambda_2^{(j)} \quad (i = 0, \cdots, m-1;\ m \geqq 3); \tag{33}$$

$$\lambda_t^{(i)} = p\lambda_2^{(i)}\lambda_{t-2}^{(0)} - C_{t-2}\lambda_2^{(i)} + (1/m)\sum_{j=0}^{m-1}\lambda_{ij}\lambda_{t-1}^{(j)} \tag{34}$$

$$(i = 0, \cdots, m-1;\ m \geqq 4;\ 4 \leqq t \leqq m);$$

$$F_{s-t} = \sum \frac{(r_2 + \cdots + r_m)!}{r_2! \cdots r_m!} C_2^{r_2} \cdots C_m^{r_m}, \tag{35}$$

where the summation extends over all sets of integers $r_2, \cdots, r_m$, each $\geqq 0$, for which

$$2r_2 + 3r_3 + \cdots + mr_m = s - t, \tag{36}$$

with the understanding that $r_t! = 1 \cdot 2 \cdots r_t$ if $r_t \geqq 1$, $r_t! = 1$ if $r_t = 0$, and with the further understanding that $F_{s-t} = 0$ in case there exists no set, with the properties described, satisfying (36). *The $\lambda_t^{(i)}$ $(i = 0, \cdots, m-1;\ t = 2, \cdots, m)$ are integers for any given $m \geqq 2$, $p = hm+1$ and g. In* (35), $C_2, \cdots, C_m$ *are the coefficients of* (17) *and*

$$tC_t = mp\lambda_t^{(0)} \quad (t = 2, \cdots, m). \tag{37}$$

Before proceeding with the proof we note that the form of F_{s-t} depends upon $s-t$ and m only, and it is clear that

$$F_0 = 1, \quad F_1 = 0, \quad \sum_{t=2}^{m} F_{s-t}\lambda_t^{(i)} = \sum_{t=2}^{s} F_{s-t}\lambda_t^{(i)} \quad (2 \leqq s \leqq m). \tag{38}$$

From the definition of F_t it is easy to prove the

LEMMA.

$$\sum_{t=2}^{k} C_t F_{k-t} = F_k \quad (2 \leqq k \leqq m), \quad \sum_{t=2}^{m} C_t F_{k-t} = F_k \quad (k \geqq m).$$

Finally, we see by (31), (24), (33) and (34) that

$$\sum_{i=0}^{m-1} \lambda_t^{(i)} = 0 \qquad (t = 2, \cdots, m). \tag{39}$$

The proof of the theorem will be divided into three parts. First, we shall prove by induction, based on Theorem 8, that $M_s^{(i)}$ can be expressed in the form (32) ($s=1, \cdots, m$; $i=0, \cdots, m-1$), by defining numbers $\lambda_t^{(i)}$ as in (23), (24), (33) and (34), and numbers C_t' ($t=2, \cdots, m$) by

$$tC_t' = mp\lambda_t^{(0)}, \tag{40}$$

and replacing F_l by F_l' where the prime indicates that F_l' is of the same form as F_l with C_t replaced by C_t'. Second, we shall prove, by the use of Theorem 7, that $M_s^{(0)}$ ($s=1, \cdots, m$) can be put in the form (32) with $i=0$ and with $\lambda_t^{(0)}$ replaced by μ_t where μ_t is defined by

$$mp\mu_t = tC_t \qquad (t = 2, \cdots, m), \tag{41}$$

and $C_2, \cdots, C_m$ are the coefficients of (17). It will be shown that $\mu_t = \lambda_t^{(0)}$ ($t=2, \cdots, m$), and that $\mu_2, \cdots, \mu_m$ are integers. Hence $C_t' = C_t$ and $\lambda_2^{(0)}, \cdots, \lambda_m^{(0)}$ are integers, whence it follows easily that the $\lambda_t^{(i)}$ are integers. Finally, we show that (32) holds for $s > m$.

Let $m \geqq 2$. Then we have (23) and (24). Next suppose $m \geqq 3$. Then (32) and (33) hold for $s=3$ by (26), the second equality in (33) being an immediate consequence of (24) and (30). For the remainder of this part of the proof we assume $m \geqq 4$ and $s \geqq 3$. In Theorem 8 take

$$A = \sum_{\nu=1}^{s-2} x_\nu^m,$$

$$B = x_{s-1}^m + g^i x_s^m.$$

Thus we obtain

$$M_s^{(i)} = M_{s-2}^{(0)} M_2^{(i)} + h \sum_{j=0}^{m-1} N_{s-2}^{(j)} N_{ij} \qquad (i = 0, \cdots, m-1).$$

Substituting for $M_2^{(i)}$ and $N_{s-2}^{(j)}$ from (23) and Theorem 10, we get by an easy reduction

$$M_s^{(i)} = \lambda_2^{(i)} p M_{s-2}^{(0)} + (1/m) \sum_{j=0}^{m-1} M_{s-1}^{(j)} N_{ij} \qquad (i = 0, \cdots, m-1; s \geqq 3). \tag{42}$$

Let $s=4$. By (23), (28), (30) and (39),

$$
\begin{aligned}
M_4^{(i)} &= \lambda_2^{(i)} p M_2^{(0)} + (1/m) \sum_{j=0}^{m-1} M_3^{(j)} N_{ij} \\
&= \lambda_2^{(i)} p\{p + \lambda_2^{(0)}(p-1)\} + (1/m) \sum_j \{p^2 + \lambda_3^{(j)}(p-1)\}\{p - \lambda_2^{(i)} + \lambda_{ij}\} \\
&= \lambda_2^{(i)} p^2 + \lambda_2^{(i)}\lambda_2^{(0)} p(p-1) + p^3 - \lambda_2^{(i)} p^2 + (1/m) \sum_j \lambda_{ij}\lambda_1^{(j)}(p-1) \\
&= p^3 + \left\{C_2'\lambda_2^{(i)} + (1/m) \sum_j \lambda_{ij}\lambda_3^{(j)} - C_2'\lambda_2^{(i)} + p\lambda_2^{(i)}\lambda_2^{(0)}\right\}(p-1) \\
&= p^3 + \{C_2'\lambda_2^{(i)} + \lambda_4^{(i)}\}(p-1) \\
&= p^3 + (p-1) \sum_{t=2}^{4} F_{4-t}'\lambda_t^{(i)}
\end{aligned}
$$

in accord with (40) and (34). This completes the first part of the proof if $m=4$.

Now suppose $m>4$ and assume as a hypothesis for induction that, for $i=0, \cdots, m-1$ and $s=2, \cdots, k (4 \leqq k \leqq m-1)$, we have (32) with F replaced by F', (24), (33) and (34) for $4 \leqq t \leqq k$, and (40) for $t=2, \cdots, k$. Then clearly we have (39) for $t=2, \cdots, k$. From (42),

$$
\begin{aligned}
M_{k+1}^{(i)} &= \lambda_2^{(i)} p M_{k-1}^{(0)} + (1/m) \sum_{j=0}^{m-1} M_k^{(j)} N_{ij} \\
&= \lambda_2^{(i)} p \left\{p^{k-2} + (p-1) \sum_{t=2}^{k-1} F_{k-1-t}'\lambda_t^{(0)}\right\} \\
&\quad + (1/m) \sum_{j=0}^{m-1} \left\{p^{k-1} + (p-1) \sum_{t=2}^{k} F_{k-t}'\lambda_t^{(j)}\right\}\{p - \lambda_2^{(i)} + \lambda_{ij}\}.
\end{aligned}
$$

For convenience we define $H_{k+1}^{(i)}$ $(i=0, \cdots, m-1)$ by

$$
(p-1)H_{k+1}^{(i)} = M_{k+1}^{(i)} - p^k. \tag{43}
$$

Then, using also (39) and (30), we have

$$
\begin{aligned}
H_{k+1}^{(i)} &= \lambda_2^{(i)} p \sum_{t=2}^{k-1} F_{k-1-t}'\lambda_t^{(0)} + (1/m) F_{k-2}' \sum_{j=0}^{m-1} \lambda_{ij}\lambda_2^{(j)} \\
&\quad + \sum_{t=3}^{k-1} \sum_{j=0}^{m-1} F_{k-t}'(1/m)\lambda_{ij}\lambda_t^{(j)} + F_0'(1/m) \sum_{j=0}^{m-1} \lambda_{ij}\lambda_k^{(j)}.
\end{aligned}
$$

By the hypothesis for the induction we have

$$
(1/m) \sum \lambda_{ij}\lambda_2^{(j)} = \lambda_3^{(i)}
$$

and

$$(1/m)\sum_{j=0}^{m-1}\lambda_{ij}\lambda_t^{(j)} = \lambda_{t+1}^{(i)} + C'_{t-1}\lambda_2^{(i)} - p\lambda_2^{(i)}\lambda_{t-1}^{(0)} \quad (3 \leqq t \leqq k-1).$$

Hence, using also $F_0' = 1$,

$$H_{k+1}^{(i)} = \lambda_2^{(i)} p \sum_{t=2}^{k-1} F'_{k-1-t}\lambda_t^{(0)} + F'_{k-2}\lambda_3^{(i)} + \sum_{t=3}^{k-1} F_{k-t}\{\lambda_{t+1}^{(i)} + C'_{t-1}\lambda_2^{(i)} - p\lambda_2^{(i)}\lambda_{t-1}^{(0)}\} + (1/m)\sum_{j=0}^{m-1}\lambda_{ij}\lambda_k^{(j)}.$$

In reducing the right member of this equation we note, first,

$$\lambda_2^{(i)} p \sum_{t=2}^{k-1} F'_{k-1-t}\lambda_t^{(0)} - p\lambda_2^{(i)} \sum_{t=3}^{k-1} F'_{k-t}\lambda_{t-1}^{(0)} = \lambda_2^{(i)} p \sum_{t=2}^{k-1} F'_{k-1-t}\lambda_2^{(0)} - p\lambda_2^{(i)} \sum_{t=2}^{k-2} F'_{k-1-t}\lambda_t^{(0)} = \lambda_2^{(i)} p\lambda_{k-1}^{(0)}.$$

Next, by the Lemma,

$$\sum_{t=3}^{k-1} F'_{k-t}C'_{t-1}\lambda_2^{(i)} = \lambda_2^{(i)}\left\{\sum_{t=2}^{k-1} F'_{k-1-t}C'_t - F_0 C'_{k-1}\right\} = \lambda_2^{(i)}F'_{k-1} - C'_{k-1}\lambda_2^{(i)}.$$

Hence, on substituting and rearranging,

$$H_{k+1}^{(i)} = p\lambda_2^{(i)}\lambda_{k-1}^{(0)} + F'_{k-2}\lambda_3^{(i)} + \sum_{t=3}^{k-1} F_{k-t}\lambda_{t+1}^{(i)} + \lambda_2^{(i)}F'_{k-1} - C'_{k-1}\lambda_2^{(i)} + (1/m)\sum_{j=0}^{m-1}\lambda_{ij}\lambda_k^{(j)}$$

$$= \sum_{t=2}^{k} F'_{k+1-t}\lambda_t^{(i)} + \lambda_{k+1}^{(i)} = \sum_{t=2}^{k+1} F'_{k+1-t}\lambda_t^{(i)},$$

where $\lambda_{k+1}^{(i)}$ is given by (34). Hence, by (43),

$$M_{k+1}^{(i)} = p^k + (p-1)\sum_{t=2}^{k+1} F'_{k+1-t}\lambda_t^{(i)} \quad (i = 0, \cdots, m-1). \tag{44}$$

This completes the induction for the first part of the proof.

For the second part of the proof, we have, by Theorem 7,

$$pM_s^{(0)} = p^s + h(\xi_0^s + \xi_1^s + \cdots + \xi_{m-1}^s) = p^s + hT_s, \tag{45}$$

where $\xi_0, \cdots, \xi_{m-1}$ are the roots of (17). For the sums, T_s, of like powers of

the roots of (17) we have, by Newton's formulas, since $C_1=T_1=0$,

$$T_2 = 2C_2,\ T_3 = 3C_3,\ T_4 = C_2T_2 + 4C_4, \cdots,$$
$$T_m = C_2T_{m-2} + \cdots + mC_m. \tag{46}$$

Define μ_t by (41) and K_t by

$$mpK_t = T_t \qquad (t = 2, \cdots, m).$$

Then the K_t are integers by Theorem 14 and the μ_t are integers by (46). Dividing the equations (46) by mp we get

$$K_2 = \mu_2, \quad K_3 = \mu_3,$$
$$K_4 = C_2K_2 + \mu_4 = C_2\mu_2 + \mu_4, \text{ etc.},$$

and by an easy induction based on the Lemma,

$$K_s = \sum_{t=2}^{s} F_{s-t}\mu_t \qquad (s = 2, \cdots, m).$$

Hence, by (45),

$$M_s^{(0)} = p^{s-1} + (p-1)\sum_{t=2}^{s} F_{s-t}\,\mu_t \qquad (s = 2, \cdots, m). \tag{47}$$

Comparing (44) for $i=0$ with (47), we see at once that $\mu_2=\lambda_2^{(0)}$ $(m\geqq 2)$. Hence $C_2=C_2'$. Similarly, if $m\geqq 3$, $\mu_3=\lambda_3^{(0)}$ whence also $C_3=C_3'$. It is clear that the highest subscript of the C's or C''s appearing in an F or F' of (47) or (44) is $s-2$ $(2\leqq s\leqq m)$. Hence, considering in succession $s=2, \cdots, m$ we find $\mu_s=\lambda_s^{(0)}$ whence $C_s=C_s'$ $(s=2, \cdots, m)$. Hence $\lambda_2^{(0)}, \cdots, \lambda_m^{(0)}$ are integers and the coefficients of (17) are given by (37). The $\lambda_2^{(i)}$ and $\lambda_3^{(i)}=\lambda_{0i}$ $(i=0, \cdots, m-1)$ are obviously integers by (24) and (28). From (32) and the results already obtained it follows easily that the $\lambda_s^{(i)}$ $(s=2, \cdots, m;\ i=0, \cdots, m-1)$ are integers.

To complete the proof of the theorem we have only to consider $s>m$. By Theorem 7,

$$pM_s^{(i)} = p^s + h(\xi_0^{s-1}\xi_i + \cdots + \xi_{m-1}^{s-1}\xi_{i+m-1}).$$

If $s>m$ whence $s-1\geqq m$, we have

$$\xi_j^{s-1} = C_2\xi_j^{s-3} + \cdots + C_m\xi_j^{s-1-m} \qquad (j = 0, \cdots, m-1),$$

since $\xi_0, \cdots, \xi_{m-1}$ satisfy (17). The proof of the theorem is now completed by an obvious induction.

THEOREM 16. *If h is odd,*

$$M_s^{(i)} = p^{s-1} + (p-1)\sum_{t=2}^{m} F_{s-t}\lambda_t^{(i)} \quad (i = 0, \cdots, m-1; m \geqq 2; s \geqq 1),$$

and all the statements of Theorem 15 *hold except that, here,* $\lambda_2^{(i)}$ $(i=0, \cdots, m-1)$ *is given by* (25) *and*

$$\lambda_3^{(i)} = \lambda_{0i} = (1/m)\sum_{j=0}^{m-1}\lambda_{ij}\lambda_2^{(j+m/2)} \qquad (i = 0, \cdots, m-1; m \geqq 3);$$

$$\lambda_t^{(i)} = p\lambda_2^{(i)}\lambda_{t-2}^{(0)} - C_{t-2}\lambda_2^{(i)} + (1/m)\sum_{j=0}^{m-1}\lambda_{ij}\lambda_{t-1}^{(j+m/2)}$$
$$(i = 0, \cdots, m-1; m \geqq 4; 4 \leqq t \leqq m).$$

The proof is exactly like that of Theorem 15 except for details where distinctions arise for h odd.

In view of the recursion formulas of Theorems 15 and 16 we see that to determine $M_s^{(i)}$ $(i=0, \cdots, m-1; m \geqq 2; s \geqq 1)$ it is necessary only to find the values of the integers λ_{ij} $(i, j=0, \cdots, m-1)$. We obtain $N_s^{(i)}$ $(i=0, \cdots, m-1; s \geqq 1)$ by Theorem 10. To determine the λ_{ij} for a given $m \geqq 2$ and $p = hm+1$ we have Theorem 12 or Theorem 13 together with (28) and (29). It follows from Theorems 15 and 16 that $\lambda_{ij}=0$ $(i, j=0, 1)$ in case $m=2$. For this case, Jordan* found by induction the following formulas for the number, S, of solutions of

$$\sum_{\nu=1}^{s} a_\nu x_\nu^2 \equiv a, \quad a_1 \cdots a_s \not\equiv 0 \pmod{p = 2h+1}.$$

If $s=2n$,

$$S = p^{2n-1} - p^n\mu \qquad \text{in case } a \not\equiv 0,$$
$$S = p^{2n-1} + (p^n - p^{n-1})\mu \qquad \text{“ “ } a \equiv 0 \pmod{p};$$

if $s=2n+1$,

$$S = p^{2n} + p^n\mu' \qquad \text{in case } a \not\equiv 0,$$
$$S = p^{2n} \qquad \text{“ “ } a \equiv 0 \pmod{p};$$

where μ and μ' are the Legendre symbols

$$\mu = ((-1)^n a_1 \cdots a_{2n} \mid p),$$
$$\mu' = ((-1)^n a_1 \cdots a_{2n+1} a \mid p) \qquad (a \not\equiv 0 \pmod{p}).$$

* Jordan, Comptes Rendus, vol. 62 (1866), pp. 687–90; *Traité des Substitutions*, 1870, pp. 156–161. V. A. Lebesgue gives two proofs of the same formulas in Comptes Rendus, vol. 62 (1866), pp. 868–72.

In terms of the notation of this paper, by (24) and (25),

$$\lambda_2^{(0)} = 1, \quad \lambda_2^{(1)} = -1, \quad C_2 = p \qquad (m = 2, h \text{ even})$$

and

$$\lambda_2^{(0)} = -1, \quad \lambda_2^{(1)} = 1, \quad C_2 = -p \qquad (m = 2, h \text{ odd}).$$

Since, for $m=2$, $F_l=0$ or $F_l=C_2^{l/2}$ according as $l \geqq 0$ is odd or even, we see that the formulas of Theorems 15 and 16 reduce to those obtained from Jordan's formulas for $a \equiv 0, a_1 \equiv a_2 \equiv \cdots \equiv a_{s-1} \equiv 1, a_s \equiv g^i \pmod{p}$.

Formulas for the N_{ij} in the cases $m=3$ and $m=4$ were obtained by Lebesgue* by means of a special discussion for each of these cases. In terms of the notation used here, his results are summarized in the following Theorems 17 and 18.

THEOREM 17. *If $m=3$, the nine integers $\lambda_{ij}(i, j=0, 1, 2)$, defined for a fixed odd prime $p=3h+1$ and a fixed primitive root g modulo p, determine integers x and y such that*

$$\lambda_3^{(0)} = \lambda_{00} = \lambda_{12} = \lambda_{21} = x,$$

$$\lambda_3^{(1)} = \lambda_{01} = \lambda_{10} = \lambda_{22} = -(x - 9y)/2, \tag{48}$$

$$\lambda_3^{(2)} = \lambda_{02} = \lambda_{20} = \lambda_{11} = -(x + 9y)/2,$$

$$x^2 + 27y^2 = 4p, \tag{49}$$

and

$$x \equiv 1 \pmod 3, \quad 9y \equiv -(2g^{2h} + 1)x \pmod p. \tag{50}$$

For a given prime $p=3h+1$, (49) has exactly four distinct solutions in integers, and of these one and only one satisfies (50) where g is any given primitive root modulo p. Take g to be the primitive root used in defining the λ_{ij}. Then the λ_{ij} are given by (48).

THEOREM 18. *If $m=4$, the sixteen integers λ_{ij} $(i, j=0, 1, 2, 3)$, defined for a fixed odd prime $p=4h+1$ and a fixed primitive root g modulo p, determine integers x and y such that*

$$\lambda_{00} = -6x,$$

$$\lambda_{01} = \lambda_{10} = \lambda_{33} = 2x + 8y,$$

$$\lambda_{02} = \lambda_{20} = \lambda_{22} = 2x, \tag{51}$$

$$\lambda_{03} = \lambda_{30} = \lambda_{11} = 2x - 8y,$$

$$\lambda_{12} = \lambda_{21} = \lambda_{13} = \lambda_{31} = \lambda_{23} = \lambda_{32} = -2x,$$

* Lebesgue, Journal de Mathématiques, vol. 2 (1837), pp. 275–287.

$$x^2 + 4y^2 = p, \tag{52}$$

and

$$x \equiv 1 \pmod 4, \quad 2y \equiv g^{3h}x \pmod p. \tag{53}$$

For a given prime $p=4h+1$, (52) has exactly four distinct solutions in integers, and of these one and only one satisfies (53) where g is any given primitive root modulo p. Take g to be the primitive root used in defining the λ_{ij}. Then the λ_{ij} are given by (51).

To complete the results for $m=3$ and $m=4$, we give the formulas for $\lambda_t^{(i)}$, $C_t (t=2, \cdots, m)$ which are found by means of Theorems 15–18. Thus, for $m=3$, $\lambda_3^{(i)} = \lambda_{01}$ is given by (48), and $C_2 = 3p$, $C_3 = px$. For $m=4$, h even, $\lambda_3^{(i)} = \lambda_{0i}$ is given by (51), and we find

$$\lambda_4^{(0)} = 4x^2 - p, \quad \lambda_4^{(1)} = -8xy - p, \quad \lambda_4^{(2)} = -4x^2 + 3p,$$
$$\lambda_4^{(3)} = 8xy - p,$$
$$C_2 = 6p, \qquad C_3 = -8xp, \qquad C_4 = 4x^2p - p^2.$$

For $m=4$, h odd, $\lambda_3^{(i)} = \lambda_{0i}$ is given by (51), and we find, in this case,

$$\lambda_4^{(0)} = 4x^2 - 9p, \quad \lambda_4^{(1)} = -8xy + 3p, \quad \lambda_4^{(2)} = -4x^2 + 3p.$$
$$\lambda_4^{(3)} = 8xy + 3p,$$
$$C_2 = -2p, \qquad C_3 = -8xp, \qquad C_4 = 4x^2p - 9p^2.$$

4. **Fifth powers.** We now discuss, by special methods, the case $m=5$, $p=5h+1$, and find formulas for the λ_{ij} $(i, j=0, \cdots, 4)$ in terms of an integral solution of the two quadratic equations (63) and (64) below. The results correspond to those of Theorems 17 and 18 for $m=3$ and $m=4$ respectively, and also yield the coefficients of the reduced form of the quintic resolvent* of (2) for any given prime $p=5h+1$.

We assume throughout that p is a fixed odd prime of the form $5h+1$. It is at once evident that h is even. From (27) we obtain

$$\begin{aligned} &\lambda_{01} = \lambda_{10} = \lambda_{44}, \ \lambda_{02} = \lambda_{20} = \lambda_{33}, \\ &\lambda_{03} = \lambda_{30} = \lambda_{22}, \ \lambda_{04} = \lambda_{40} = \lambda_{11}, \\ &\lambda_{12} = \lambda_{21} = \lambda_{14} = \lambda_{41} = \lambda_{34} = \lambda_{43}, \\ &\lambda_{13} = \lambda_{31} = \lambda_{24} = \lambda_{42} = \lambda_{23} = \lambda_{32}. \end{aligned} \tag{54}$$

* The quintic resolvent of (2), for $p=5h+1$, was found by Burnside (Proceedings of the London Mathematical Society, (2), vol. 14 (1915), pp. 251–259) by methods not involving congruences. His formulas depend upon the solution of two equations in four unknowns which are much more complicated than those of this paper.

Then (30) yields

$$\begin{aligned} \lambda_{00} &= -\lambda_{01} - \lambda_{02} - \lambda_{03} - \lambda_{04}, \\ \lambda_{12} &= \tfrac{1}{3}(-2\lambda_{01} + \lambda_{02} + \lambda_{03} - 2\lambda_{04}), \\ \lambda_{13} &= \tfrac{1}{3}(\lambda_{01} - 2\lambda_{02} - 2\lambda_{03} + \lambda_{04}). \end{aligned} \tag{55}$$

To obtain further relations, we write the congruence

$$x_1^5 + x_2^5 + gx_3^5 + g^4x_4^5 \equiv 0 \pmod{p}$$

in the two forms

$$x_1^5 + x_2^5 \equiv g(y_3^5 + g^3y_4^5) \pmod{p},$$

and

$$x_1^5 + gx_3^5 \equiv y_2^5 + g^4y_4^5 \pmod{p},$$

to each of which it is equivalent since h is even. Hence, by Theorem 8 and the definitions of §2,

$$M_2^{(0)}M_2^{(3)} + h\sum_{j=1}^{4} N_{0j}N_{3,1-j} = M_2^{(1)}M_2^{(4)} + h\sum_{j=0}^{4} N_{ij}N_{4j}.$$

We substitute from (23) and (28), apply (30) and (39), and get

$$\begin{aligned} &\lambda_{00}\lambda_{34} + \lambda_{01}\lambda_{30} + \lambda_{02}\lambda_{31} + \lambda_{03}\lambda_{32} + \lambda_{04}\lambda_{33} \\ &\quad - \lambda_{10}\lambda_{40} - \lambda_{11}\lambda_{41} - \lambda_{12}\lambda_{42} - \lambda_{13}\lambda_{43} - \lambda_{14}\lambda_{44} = 25p. \end{aligned} \tag{56}$$

Dealing similarly with

$$x_1^5 + x_2^5 + g^2x_3^5 + g^3x_4^5 \equiv 0 \pmod{p},$$

we obtain

$$M_2^{(0)}M_2^{(1)} + h\sum_{j=0}^{4} N_{0j}N_{1,2-j} = M_2^{(2)}M_2^{(3)} + h\sum_{j=0}^{4} N_{2j}N_{3j},$$

whence

$$\begin{aligned} &\lambda_{00}\lambda_{13} + \lambda_{01}\lambda_{14} + \lambda_{02}\lambda_{10} + \lambda_{03}\lambda_{11} + \lambda_{04}\lambda_{12} \\ &\quad - \lambda_{20}\lambda_{30} - \lambda_{21}\lambda_{31} - \lambda_{22}\lambda_{32} - \lambda_{23}\lambda_{33} - \lambda_{24}\lambda_{34} = 25p. \end{aligned} \tag{57}$$

Write

$$\lambda_{0i} = x_i \qquad (i = 1, \cdots, 4), \tag{58}$$

and substitute (54) and (55) in (56) and (57). In this manner we obtain two equations which, added, yield

$$(59)\qquad \begin{aligned} &11x_1^2 + 11x_2^2 + 11x_3^2 + 11x_4^2 - 5x_1x_2 - 5x_1x_3 \\ &\quad + 13x_2x_3 + 13x_1x_4 - 5x_2x_4 - 5x_3x_4 = 450p, \end{aligned}$$

and, subtracted, one from the other, yield

$$(60)\qquad \begin{aligned} &21x_1^2 - 21x_2^2 - 21x_3^2 + 21x_4^2 - 9x_1x_2 + 9x_1x_3 \\ &\quad - 33x_2x_3 + 33x_1x_4 + 9x_2x_4 - 9x_3x_4 = 0. \end{aligned}$$

It follows easily from (59), since $x_1, \cdots, x_4$ are integers, that

$$x_1 + x_2 + x_3 + x_4 \equiv 0 \pmod 3.$$

Hence in

$$(61)\qquad \begin{aligned} x_1 + x_2 + x_3 + x_4 &= -3x, \\ x_1 - x_2 - x_3 + x_4 &= 25w, \\ -x_1 + x_2 - x_3 + x_4 &= 25y, \\ -x_1 - x_2 + x_3 + x_4 &= 25z, \end{aligned}$$

x is an integer, and it follows easily from Theorem 13 and (28) that y, z and w are integers. The solution of (61), together with (54) and (55), yields

$$(62)\qquad \begin{aligned} \lambda_{00} &= 3x, \\ x_1 = \lambda_{01} = \lambda_{10} = \lambda_{44} &= -(3x - 25w + 25y + 25z)/4, \\ x_2 = \lambda_{02} = \lambda_{20} = \lambda_{33} &= -(3x + 25w - 25y + 25z)/4, \\ x_3 = \lambda_{03} = \lambda_{30} = \lambda_{22} &= -(3x + 25w + 25y - 25z)/4, \\ x_4 = \lambda_{04} = \lambda_{40} = \lambda_{11} &= -(3x - 25w - 25y - 25z)/4, \\ y_1 = \lambda_{12} = \lambda_{21} = \lambda_{14} = \lambda_{41} = \lambda_{34} = \lambda_{43} &= (x - 25w)/2, \\ y_2 = \lambda_{13} = \lambda_{31} = \lambda_{24} = \lambda_{42} = \lambda_{23} = \lambda_{32} &= (x + 25w)/2, \end{aligned}$$

where we have introduced the notation y_1 and y_2 for use later. Finally, we substitute for $x_1, \cdots, x_4$ from (62) in (59) and (60) and obtain

$$(63)\qquad x^2 + 25y^2 + 25z^2 + 125w^2 = 16p,$$

and

$$(64)\qquad y^2 + yz - z^2 = xw,$$

respectively.

By (28) and Theorem 13, since $p \equiv 1 \pmod 5$ and $\lambda_2^{(0)} = 4$, we have $\lambda_{00} \equiv -2 \pmod 5$. Hence, by (62),

$$(65)\qquad x \equiv 1 \pmod 5.$$

We now proceed to find certain relations which hold modulo p in view of

(62) and Theorem 12. It is easily shown by the remarks following that theorem, defining P and Q as indicated, that

$$(66)\qquad \begin{aligned} P &= \binom{2h}{h} \equiv \binom{4h}{h} \equiv \binom{4h}{3h}, \\ Q &= \binom{3h}{h} \equiv \binom{3h}{2h} \equiv \binom{4h}{2h} \qquad (\mathrm{mod}\ p = 5h+1), \end{aligned}$$

and the theorem and (28) yield

$$(67)\qquad \begin{aligned} x &= \lambda_{00}/3 \equiv -P-Q, \\ x_1 &= \lambda_{01} \equiv -P(2r+r^3) - Q(2r^2+r), \\ x_2 &= \lambda_{02} \equiv -P(2r^2+r) - Q(2r^4+r^2), \\ x_3 &= \lambda_{03} \equiv -P(2r^3+r^4) - Q(2r+r^3), \\ x_4 &= \lambda_{04} \equiv -P(2r^4+r^2) - Q(2r^3+r^4), \\ y_1 &= \lambda_{12} \equiv -P(1+r^2+r^3) - Q(1+r+r^4), \\ y_2 &= \lambda_{13} \equiv -P(1+r+r^4) - Q(1+r^2+r^3) \qquad (\mathrm{mod}\ p), \end{aligned}$$

where

$$(68)\qquad r \equiv g^h \qquad (\mathrm{mod}\ p),$$

and g is the primitive root modulo p used in defining the λ_{ij}. It is clear that r is a root of

$$(69)\qquad u^5 \equiv 1 \qquad (\mathrm{mod}\ p)$$

such that

$$(70)\qquad r^5 \equiv 1,\ r^4+r^3+r^2+r+1 \equiv 0 \qquad (\mathrm{mod}\ p).$$

We solve (67), 2, and (67), 5, for P and Q and get

$$(71)\qquad \begin{aligned} (-2r+r^2-r^3+2r^4)P &\equiv -(2r^3+r^4)x_1 + (2r^3+r^4)x_2, \\ (-2r+r^2-r^3+2r^4)Q &\equiv (2r^4+r^2)x_1 - (2r+r^3)x_2 \qquad (\mathrm{mod}\ p). \end{aligned}$$

In view of (70), we find on multiplying (71) by $r-r^4$,

$$(72)\qquad \begin{aligned} 5P &\equiv (-1+2r^2+r^3-2r^4)x_1 + (-1-2r+r^2+2r^3), \\ 5Q &\equiv (2-r-r^4)x_1 + (2-r^2-r^4)x_2 \qquad (\mathrm{mod}\ p). \end{aligned}$$

By solving the pairs (67), 3, (67), 4, and (67), 6, (67), 7, and then multiplying by r^2-r^3 and $r-r^2-r^3+r^4$ respectively, we get

$$(73)\qquad \begin{aligned} 5P &\equiv (-1+r-2r^3+2r^4)x_2 + (-1+2r-2r^2+r^4)x_3, \\ 5Q &\equiv (2-r-r^2)x_2 + (2-r^3-r^4)x_3 \qquad (\mathrm{mod}\ p), \end{aligned}$$

and

$$(74)\qquad \begin{aligned} 5P &\equiv (-2+r+r^4)y_1+(-2+r^2+r^3)y_2,\\ 5Q &\equiv (-2+r^2+r^3)y_1+(-2+r+r^4)y_2 \end{aligned} \pmod p.$$

From (74), on substituting for y_1 and y_2 from (62), we find

$$(75)\qquad \begin{aligned} -2P &\equiv x+5(r-r^2-r^3+r^4)w,\\ -2Q &\equiv x+5(-r+r^2+r^3-r^4)w \end{aligned} \pmod p.$$

Next, add the two congruences in (72) and the two congruences in (73), and then substitute from (62). In this way we get

$$(76)\quad 5(y+z)(r+2r^2-2r^3-r^4)\equiv 4x-3x(1+r^2+r^3)+25w(1+r^2+r^3),$$

and

$$(77)\quad 5(y-z)(2r-r^2+r^3-2r^4)\equiv 4x-3x(1+r+r^4)-25w(1+r+r^4),$$

respectively. Finally, solve (76) and (77) for y and z and multiply the result by $r-r^2-r^3+r^4$. There results

$$(78)\qquad \begin{aligned} 25y &\equiv (-2r+r^2-r^3+2r^4)x+25(r-r^4)w,\\ 25z &\equiv (-r-2r^2+2r^3+r^4)x-25(r^2-r^3)w \end{aligned} \pmod p.$$

We have now completed the proof of

THEOREM 19. *If $m=5$, the twenty-five integers λ_{ij} $(i,j=0,\cdots,4)$, defined for a fixed prime $p=5h+1$ and a fixed primitive root g modulo p, determine integers x, y, z and w such that* (63), (64), (65), (68), (75), *and* (78) *hold.*

In order to prove the next theorem we shall need the following lemmas.

LEMMA 1. *If (x, y, z, w) is an integral solution of* (63), *x, y, z and w are either all odd or all even.*

The truth of this lemma is easily verified by taking (63) modulo 8. A further result, easily obtained by noting that $16p\equiv 16 \pmod{32}$ and taking (63) modulo 32, is that the greatest common divisor of x, y, z and w is 1 or 4.

LEMMA 2. *If (x, y, z, w) is an integral solution of* (63) *and* (64) *together, then $xw\not\equiv 0 \pmod p$.*

To prove $x\not\equiv 0 \pmod p$ we first suppose $p>11$. By (63),

$$|x| \leqq 4p^{1/2} < p \text{ if } p > 16.$$

Hence if $p=5h+1>11$, $x\equiv 0 \pmod p$ implies $x=0$. Then (64) implies $y=z=0$, and by (63), $125w^2=16p$, which is impossible. Similarly, $w\not\equiv 0 \pmod p$. If $p=11$, the only solutions of (63) and (64) together are (1, 1, 1, 1) and others obtained from this by changes of sign.

LEMMA 3. *If* (x, y, z, w) *is an integral solution of* (63) *and* (64) *together, then* $x^2-125w^2\not\equiv 0 \pmod{p}$.

By Lemma 1, $x^2-125w^2\equiv 0 \pmod 4$. Hence $x^2-125w^2\equiv 0 \pmod{p}$ implies $x^2-125w^2=4ap$, a an integer. By (63),

$$|x^2 - 125w^2| < x^2 + 125w^2 \leqq 16p,$$

the first inequality holding since $xw\neq 0$ by Lemma 2. Also, by (63),

$$x^2 - 125w^2 \equiv x^2 \equiv 16p \equiv 1 \pmod 5.$$

Hence $a=-1$ and $x^2-125w^2=-4p$. Subtracting this from (63), we obtain

$$25y^2 + 25z^2 + 250w^2 = 20p,$$

which is impossible since $p\not\equiv 0 \pmod 5$.

THEOREM 20. *Let* $p=5h+1$ *be a fixed positive odd prime. Then* (63) *and* (64) *together have exactly* 8 *distinct solutions in integers, and, if* (x, y, z, w) *is one solution, all solutions are*

$$\begin{aligned}&(\pm x, \pm y, \pm z, \pm w), \quad (\pm x, \mp z, \pm y, \mp w),\\ &(\mp x, \mp z, \pm y, \pm w), \quad (\mp x, \pm y, \pm z, \mp w).\end{aligned} \tag{79}$$

Of these, one and only one satisfies (65) *and* (78), 1, *where* r *satisfies* (68) *and* g *is any given primitive root modulo* p.

By Theorem 19, (63) and (64) together have an integral solution (x, y, z, w). By trial, it is easily verified that each of the eight sets (79) satisfies (63) and (64). That these are distinct solutions follows since $xw\neq 0$ by Lemma 2 whence y and z are not both zero by (64). We now assume that (x, y, z, w) is a solution of (63) and (64) together and prove the remaining parts of the theorem.

Square (63) modulo p, rearrange the result, and apply (64). Thus

$$\begin{aligned}&(x^2 + 125w^2)^2 - 625(y^2 + z^2)^2 \equiv 0,\\ &(x^2 + 125w^2)^2 - 2500y^2z^2 - 625(y^2 - z^2)^2 \equiv 0,\\ &(x^2 + 125w^2)^2 - 2500y^2z^2 - 625(xw - yz)^2 \equiv 0,\end{aligned}$$

and finally,

$$3125(yz)^2 - 1250xw(yz) + 625x^2w^2 - (x^2 + 125w^2)^2 \equiv 0 \pmod{p}. \tag{80}$$

By (80), we must have

$$6250yz \equiv 1250xw + 50\eta \pmod{p},$$

where

$$50^2\eta^2 \equiv (1250)^2x^2w^2 - 4\{625x^2w^2 - (x^2 + 125w^2)^2\}(3125),$$
$$\eta^2 \equiv 5(x^2 - 125w^2)^2 \pmod{p}.$$

The congruence

$$u^2 \equiv 5 \pmod{p = 5h + 1} \tag{81}$$

has a solution since

$$(5 \mid p) = (p \mid 5) = 1.$$

Accordingly, by Lemma 3, (x, y, z, w) determines a solution of (81) such that

$$125yz \equiv 25xw + \zeta(x^2 - 125w^2) \pmod{p}, \tag{82}$$

where

$$\zeta^2 \equiv 5 \pmod{p}.$$

From (64) and (82),

$$125(y^2 - z^2) \equiv 100xw - \zeta(x^2 - 125w^2), \tag{83}$$

and from (63),

$$25(y^2 + z^2) \equiv -(x^2 + 125w^2),$$

whence

$$\begin{aligned} 250y^2 &\equiv 100xw - 5(x^2 + 125w^2) - \zeta(x^2 - 125w^2), \\ 250z^2 &\equiv -100xw - 5(x^2 + 125w^2) + \zeta(x^2 - 125w^2) \pmod{p}. \end{aligned} \tag{84}$$

Now let r be any root of (69) satisfying (70). It is easily verified that

$$(r - r^2 - r^3 + r^4)^2 \equiv 5 \pmod{p}. \tag{85}$$

The congruence (69) has four roots r, r^2, r^3 and r^4 each satisfying (70). We see that the replacement of r by r^4 leaves the expression

$$r - r^2 - r^3 + r^4 \tag{86}$$

unaltered modulo p, while the replacement of r by r^2 or r^3 replaces this expression by its negative modulo p. By these remarks, we may suppose r to be such that

$$\zeta \equiv r - r^2 - r^3 + r^4 \pmod{p}. \tag{87}$$

Then multiplication will verify that (84) is equivalent to

$$\begin{aligned} 625y^2 &\equiv \{(-2r + r^2 - r^3 + 2r^4)x + 25(r - r^4)w\}^2, \\ 625z^2 &\equiv \{(-r - 2r^2 + 2r^3 + r^4)x - 25(r^2 - r^3)w\}^2 \pmod{p}. \end{aligned} \tag{88}$$

The expressions

$$-2r + r^2 - r^3 + 2r^4 \text{ and } r - r^4$$

are replaced by their negatives modulo p on the replacement of r by r^1 which leaves (86) unaltered modulo p. Hence we may suppose r to be such that (78), 1, holds. Then (82) requires (78), 2. Clearly r is determined uniquely by (x, y, z, w). Conversely, by the remarks of this paragraph, it is easily seen that, if r is any preassigned root of (69) satisfying (70), we may assume that (x, y, z, w) is one of the associates, (79), such that (78) holds.

Now suppose that (x_1, y_1, z_1, w_1) is an integral solution of (63) and (64) together distinct from the associates, (79), of (x, y, z, w). By the preceding paragraph, we may assume that (78) holds with x, y, z and w replaced by x_1, y_1, z_1 and w_1 respectively. We substitute for y_1 and z_1 from these relations and for y and z from (78), and easily verify that

$$xx_1 + 25yy_1 + 25zz_1 + 125ww_1 \equiv 0 \pmod{p}.$$

Denote the absolute value of the left member of this congruence by A, whence $A \equiv 0 \pmod{p}$. Since (x, y, z, w) and (x_1, y_1, z_1, w_1) are solutions of (63), we have

$$\begin{aligned} 256p^2 &= (x^2 + 25y^2 + 25z^2 + 125w^2)(x_1^2 + 25y_1^2 + 25z_1^2 + 125w_1^2) \\ &= A^2 + 25(xy_1 - x_1y)^2 + 25(xz_1 - x_1z)^2 + 125(xw_1 - x_1w)^2 \\ &\quad + 625(yz_1 - y_1z)^2 + 3125(yw_1 - y_1w)^2 + 3125(zw_1 - z_1w)^2. \end{aligned} \tag{89}$$

Hence $A \leqq 16p$. By (63), $x \equiv \pm 1$, $x_1 \equiv \pm 1 \pmod 5$. Hence $A \equiv \pm 1 \pmod 5$. Further, by Lemma 1, $x, \cdots, w$ are all even or all odd and $x_1, \cdots, w_1$ are all even or all odd. Hence A is even and we must have $A = 4p$, $6p$, $14p$ or $16p$. Suppose $A = 4p$. Then by (89), $240p^2 \equiv 0 \pmod{25}$ which is impossible. In a similar way, $A = 6p$ and $A = 14p$ are excluded. Hence $A^2 = 256p^2$ and, by (89),

$$xy_1 = x_1y, \; xz_1 = x_1z, \; xw_1 = x_1w, \cdots \text{etc.} \tag{90}$$

Since $x \neq 0$ by Lemma 1, and $(x, \cdots, w)$, $(x_1, \cdots, w_1)$ are solutions of (63), (90) implies

$$x_1^2 = x^2, \; x_1 = \pm x,$$

and (x_1, y_1, z_1, w_1) is one of the associates

$$(\pm x, \pm y, \pm z, \pm w) \tag{91}$$

of (x, y, z, w), a contradiction of the assumption concerning (x_1, y_1, z_1, w_1).

To complete the proof of the theorem, we have only to note that, first, two and only two of the associates, (79), of a solution (x, y, z, w) of (63) and

(64) together satisfy also (78) for a preassigned root of (69) satisfying (70), and these may be taken to be (91); second, by (63), $x \equiv \pm 1 \pmod 5$, hence one and only one of these associates satisfies also (65).

COROLLARY. *Let g be the primitive root modulo p used in defining the λ_{ij}. Then r, given by* (68), *is a unique root of* (69) *satisfying* (70). *If (x, y, z, w) is the unique solution of* (63) *and* (64) *together which satisfies* (65) *and* (78), *the λ_{ij} are given by* (62).

In terms of the integers x, y, z and w of (62), we calculate some of the integers which appear in the formula of Theorem 15 in case $m=5$, $p=5h+1$. We have, by (24), $\lambda_2^{(0)} = m-1 = 4$, $\lambda_2^{(i)} = -1$ ($i \not\equiv 0 \pmod 5$), and the $\lambda_3^{(i)} = \lambda_{0i}$ ($i = 0, \cdots, 4$) are given by (62). The recursion formula (34) yields

$$\lambda_4^{(0)} = -4p + x^2 - 125w^2, \qquad \lambda_5^{(0)} = -xp + (x^3 - 625wyz)/8, \tag{92}$$

and by (37), we find

$$\begin{aligned} C_2 &= 10p, \quad C_3 = 5xp, \quad C_4 = -5p + 5(x^2 - 125w^2)p/4, \\ C_5 &= -xp^2 + (x^3 - 625wyz)p/8. \end{aligned} \tag{93}$$

The expressions for $\lambda_4^{(i)}$ and $\lambda_5^{(i)}$ ($i = 1, \cdots, 4$) yielded by (34) are more complicated.

It is easily seen by (79) that the values taken by each of the expressions $x^2 - 125w^2$ and $x^3 - 625wyz$ are independent of the choice of one of the four solutions of (63) and (64) together such that $x \equiv 1 \pmod 5$. Hence we may state

THEOREM 21. *The equation satisfied by $\xi_0, \cdots, \xi_4$, defined as in §2 for $m=5$ and a fixed prime of the form $p=5h+1$, is* (17), *where $C_2, \cdots, C_5$ are given by* (93) *and (x, y, z, w) is any integral solution of* (63) *and* (64) *together such that $x \equiv 1 \pmod 5$. The equation of the periods $\eta_0, \cdots, \eta_4$ of the roots of* (2) *is then obtained from* (17) *by the substitution $\xi = 1 + 5\eta$.*

We employ Theorem 5 to obtain congruences yielding the residues modulo $p=5h+1$ of the binomial coefficients P and Q defined in (66). That theorem yields

$$M_4^{(0)} \equiv -4PQ, \qquad M_5^{(0)} \equiv P^2Q \pmod p.$$

By Theorem 15, we find

$$M_4^{(0)} \equiv -\lambda_4^{(0)}, \qquad M_5^{(0)} \equiv -\lambda_5^{(0)} \pmod p,$$

since $C_2 \equiv C_3 \equiv 0 \pmod p$. We combine these relations with (92) and obtain

THEOREM 22. *Let p be a fixed prime of the form $5h+1$. Then if (x, y, z, w) is any solution of* (63) *and* (64) *together such that $x \equiv 1 \pmod 5$, the binomial coefficients P and Q, defined above, satisfy*

$$2(x^2 - 125w^2)P \equiv -x^3 + 625wyz,$$
$$2(x^3 - 625wyx)Q \equiv -(x^2 - 125w^2)^2 \pmod p.$$

5. **On the existence of solutions.** We indicate sufficient conditions on s in order that (1), with $k \geqq 2$ a fixed integer, may have a solution whatever the integers a and n may be. For a fixed prime p, we use the notation θ, γ and P defined in (10).

By Theorem 1, a necessary and sufficient condition that (1) have a solution for every a and n is that

$$M_s(p^l; a) > 0 \tag{94}$$

for every prime p, every positive integer l and every integer a, where we have modified the notation of §1 to indicate the dependence of the number of solutions of (1) on the number, s, of variables. From the meaning of the notation a sufficient condition for (94) is

$$N_s(p^l; a) > 0 \tag{95}$$

for every p, l and a. Clearly, for a fixed p, (95) with $l = \gamma$ implies (95) with $1 \leqq l \leqq \gamma$. By Theorem 2, (95) with $l = \gamma$ implies (95) with $l \geqq \gamma$. Hence a sufficient condition in order that (1) have a solution for every a and n is that (95) hold for every p with $l =$ the corresponding γ, and every a.

Landau* has proved the following

THEOREM 23. *Let p be a fixed prime. If $a \not\equiv 0 \pmod P$,*

$$N_s(P; a) > 0$$

for every $s \geqq r$, where

$$(p - 1)r = (P - 1)m \qquad (P = p^\gamma), \tag{96}$$

and where m denotes the greatest common divisor of k and $p-1$. Further,

$$N_s(P; 0) > 0$$

for every $s \geqq r+1$.

By this theorem and the preceding discussion, it follows that a sufficient condition in order that (1) have a solution for every a and n is

$$s \geqq R + 1,$$

where R is the maximum of r in (96) for all primes p.

* Landau, *Vorlesungen über Zahlentheorie*, vol. I, pp. 287–91.

By way of example, let $k=5$. We consider primes, p, under four cases as follows. First let $p=2$. Then clearly $r=3$. Second, suppose $p\neq 2$, $p\neq 5$ and $m=1$. Evidently $r=1$. Third, let $m=5$. Then $r=5$ since $\gamma=1$. Finally, let $p=5$. Then $r=6$ since $\gamma=2$. Since these four cases exhaust all primes, it is clear that for $k=5$ we have $R=6$, whence, by the preceding discussion, $s\geqq 7$ is a sufficient condition that (1), with $k=5$, have a solution for every a and n. It is easily shown, however, that $s\geqq 5$ is a sufficient condition in case $k=5$. For, clearly $s\geqq 5$ is sufficient for primes of the first two cases. Next, by Theorem 23, $s\geqq 5$ is sufficient for any prime of Case 3 if a is not divisible by the prime. By Theorem 9,

$$x^5+y^5\equiv 0 \pmod{p=5h+1}$$

has a primitive solution since h is even. Hence $s\geqq 5$ is sufficient for all primes of Case 3 and every integer a. Finally, it is easily verified by trial that

$$x_1^5+\cdots+x_5^5\equiv a \pmod{25},$$

where $25=P=p^\gamma$ for $p=5$, has a primitive solution for $a=0, \cdots, 24$.

The condition $s\geqq 5$ is also necessary in case $k=5$. For, by trial,

$$x_1^5+\cdots+x_4^5\equiv 5 \pmod{11}$$

has no solution, and

$$M_5(11;5)=N(11;5).$$

A number of writers have discussed the congruence

$$x^n+y^n+z^n\equiv 0 \pmod{p},\ p \text{ a prime},$$

which is of interest in connection with Fermat's Last Theorem. For references to this congruence see Dickson's *History of the Theory of Numbers*, vol. II, Chapter XXVI; and the Bulletin of the National Research Council, Bulletin 62, February, 1928, Chapter II.

University of Chicago,
Chicago, Ill.