THE NUMBER OF SOLUTIONS OF SOME CONGRUENCES MODULO A PRODUCT OF PRIMES⁽¹⁾

BY

L. CARLITZ AND A. L. WHITEMAN

TO PROFESSOR L. J. MORDELL ON HIS SEVENTY-FIFTH BIRTHDAY

1. Introduction. Let $p_1^{\alpha_1} p_2^{\alpha_2}, \dots, p_r^{\alpha_r}$ be the prime factor decomposition of an odd integer m , and let g_i ($i = 1, \dots, r$) be a primitive root of $p_i^{\alpha_i}$. By the Chinese Remainder Theorem the system of congruences

$$g \equiv g_1 \pmod{p_1^{\alpha_1}}, \dots, g \equiv g_r \pmod{p_r^{\alpha_r}}$$

has a solution g that is unique modulo m . The exponent d of g modulo m is the least common multiple of $\phi(p_1^{\alpha_1}), \dots, \phi(p_r^{\alpha_r})$, where $\phi(n)$ is the Euler function. In this paper we consider the problem of determining the number $N(g)$ of solutions in s, t of the congruence $g^s + 1 \equiv g^t \pmod{m}$, where the values of s and t are each selected from the integers $0, 1, \dots, d - 1$.

We discuss for the most part the case in which m is the product of two distinct odd primes p and q . If e denotes the greatest common divisor of $p - 1$ and $q - 1$, then $d = (p - 1)(q - 1)/e$. Let g denote a common primitive root of p and q , and let $N(g) = N_e(g)$ denote the number of solutions in s, t of the congruence $g^s + 1 \equiv g^t \pmod{pq}$, where $0 \leq s, t \leq d - 1$. In [3] the function $N_e(g)$ is required for the construction of certain types of residue difference sets. Indeed, it is this application of $N_e(g)$ that provided the motivation for the present paper (see the corollary of Theorem 3 in §5).

The case $e = 2$ is treated in §4. We find that

$$N_2(g) = \begin{cases} \frac{1}{4}(pq - 2p - 2q + 5) & (p \not\equiv q \pmod{4}), \\ \frac{1}{4}(pq - 2p - 2q + 7) & (p \equiv q \equiv 3 \pmod{4}). \end{cases}$$

Thus the expression for $N_2(g)$ is independent of the selection of g .

When $e > 2$ the number $N_e(g)$ depends upon the particular choice of g . We show in §3 that the set $\bar{G}$ of common primitive roots of p and q can be separated into $\phi(e)$ disjoint classes $G_1, \dots, G_{\phi(e)}$ each containing $\phi(d)$ roots. The class G_i has the following property: if g_i is in G_i , then G_i consists of the $\phi(d)$ numbers g_i^r such that $1 \leq r \leq d - 1$ and $(r, d) = 1$. Furthermore, if g_i is in G_i , then the value $N_e(g_i)$ depends only on the class G_i and not on the choice of g_i in G_i .

Received by the editors April 23, 1963.

⁽¹⁾ This research was partially supported by National Science Foundation grants G 16485 and G 24066.

In the particular case $e = 4$ the set $\bar{G}$ consists of two classes G_1, G_2 . Let $g_1 \in G_1, g_2 \in G_2$. We prove in §5 that

$$4N_4(g_1) = 4ff' - f - f' + \frac{3}{2} + \eta + \frac{1}{2}(1 + 2(-1)^{f+f'})(xX + yY),$$

$$4N_4(g_2) = 4ff' - f - f' + \frac{3}{2} + \eta + \frac{1}{2}(1 + 2(-1)^{f+f'})(xX - yY),$$

where $p = 4f + 1 = x^2 + 4y^2$ and $q = 4f' + 1 = X^2 + 4Y^2$. The numbers x, X are uniquely determined by the condition $x \equiv X \equiv 1 \pmod{4}$, whereas y, Y are ambiguous. Moreover, the number η is 0 or 1 according as ff' is even or odd. It follows that $N_4(g_1) \neq N_4(g_2)$. Essential use is made of this inequality in [3] where it is stated without proof as Lemma 6.

We also obtain corresponding results in the case $e = 6$ (Theorem 4 in §6) and the case $e = 8$ (Theorem 5 in §7). Finally, in §8 we discuss the case in which the modulus m is the product of three distinct primes p, q, r . Under the assumption that $(p-1, q-1) = (q-1, r-1) = (r-1, p-1) = 2$ we derive an explicit formula for $N(g)$ (Theorem 6).

The method consists in expressing $N(g)$ in terms of Jacobi sums. These sums are based on certain multiplicative characters defined in §2. Theorem 1 is the main tool.

2. The χ and ψ characters. Let p, q denote distinct odd primes. Let g be a fixed primitive root of both p and q , and let e denote the greatest common divisor of $p-1$ and $q-1$. The exponent d to which g belongs modulo pq is the least common multiple of $p-1$ and $q-1$. Consequently $d = (p-1)(q-1)/e$.

Let $\beta = \exp(2\pi i/e)$ be a primitive e th root of unity. We define e th power characters $\chi(a) = \chi_e(a)$ modulo p and $\psi(a) = \psi_e(a)$ modulo q as follows: $\chi(a) = \beta^u$ if $a \equiv g^u \pmod{p}$ and $\chi(a) = 0$ if $p|a$; $\psi(a) = \beta^v$ if $a \equiv g^v \pmod{q}$ and $\psi(a) = 0$ if $q|a$. It will be convenient to adopt the convention that $\chi^n(0) = 0$ for $1 \leq n \leq e-1$ and $\chi^n(0) = 1$ for $n = 0$. We shall also let $\bar{\chi}(a) = \chi^{e-1}(a)$ denote the complex conjugate of $\chi(a)$.

We now prove the following criterion.

LEMMA 1. *Let s be a fixed integer such that $0 \leq s \leq d-1$ and $(g^s + 1, pq) = 1$. Then there corresponds an integer t such that $0 \leq t \leq d-1$ and $g^s + 1 \equiv g^t \pmod{pq}$ if and only if $\chi(g^s + 1) = \psi(g^s + 1)$.*

Proof. Consider the pair of congruences

$$(2.1) \quad g^s + 1 \equiv g^u \pmod{p}, \quad g^s + 1 \equiv g^v \pmod{q}.$$

Then $g^s + 1 \equiv g^t \pmod{pq}$ provided integers h, k exist such that

$$u + h(p-1) = v + k(q-1).$$

This will occur if and only if $u \equiv v \pmod{e}$. The assertion of the lemma follows at once.

Let $T(g)$ denote the number of values of s such that $0 \leq s \leq d-1$ and $(g^s + 1, pq) \neq 1$. We next observe that the number $N(g) = N_e(g)$ of solutions s, t of the congruence

$$(2.2) \quad g^s + 1 \equiv g^t \pmod{pq} \quad (0 \leq s, t \leq d-1)$$

is related to the sum

$$(2.3) \quad S(g) = \sum_{s=0}^{d-1} \sum_{n=0}^{e-1} \chi^n(g^s + 1) \bar{\psi}^n(g^s + 1)$$

by means of the equation $S(g) = eN(g) + T(g)$. The reason is as follows. For each s in (2.3) such that $(g^s + 1, pq) = 1$ the congruences in (2.1) imply that

$$\sum_{n=0}^{e-1} \chi^n(g^s + 1) \bar{\psi}^n(g^s + 1) = \sum_{n=0}^{e-1} \beta^{(u-v)n} = \begin{cases} e & (u \equiv v \pmod{e}), \\ 0 & (u \not\equiv v \pmod{e}). \end{cases}$$

On the other hand, for each s in (2.3) such that $(g^s + 1, pq) \neq 1$, the inner sum in (2.3) has the value 1. It follows from Lemma 1 that the right member of (2.3) reduces to $eN_e(g) + T(g)$.

The problem of determining $N(g)$ has now been transformed into the problem of determining $S(g)$ and $T(g)$. An explicit formula for $T(g)$ is furnished by the following lemma.

LEMMA 2. *Let $p-1 = ef$, $q-1 = ef'$, $(f, f') = 1$. Then the number $T = T(g)$ of values of s such that $0 \leq s \leq d-1$ and $(g^s + 1, pq) \neq 1$ is given by*

$$(2.4) \quad T = \begin{cases} f + f' & (ff' \text{ even}), \\ f + f' - 1 & (ff' \text{ odd}). \end{cases}$$

Proof. Clearly f and f' cannot both be even. If ff' is odd, then $-1 \equiv g^{d/2} \pmod{pq}$. But if ff' is even, then there is no value of s such that $-1 \equiv g^s \pmod{pq}$, where $0 \leq s \leq d-1$. Put $N = N(s) = 1 + g^s$ and let N_{pq} denote the number of values of s ($s=0, 1, \dots, d-1$) for which N is divisible by pq . Then N_{pq} is equal to 0 or 1 according as ff' is even or odd. Also let N_p denote the number of values of s ($s=0, 1, \dots, d-1$) for which N is divisible by p . As s ranges from 0 to $d-1$, the least positive remainders of g^s modulo p range f' times over each of the integers between 1 and $p-1$. Hence $N_p = f'$. Similarly if N_q denotes the number of values of s ($s=0, 1, \dots, d-1$) for which N is divisible by q , then $N_q = f$. By a well-known combinatorial principle the number T is equal to $N_p + N_q - N_{pq}$, which reduces to the right member of (2.4). This completes the proof of the lemma.

We turn to the problem of determining $S(g)$. Interchanging signs of summation in (2.3) we get $S(g) = \sum_{n=0}^{e-1} S_n$, where

$$(2.5) \quad S_n = S_n(g) = \sum_{s=0}^{d-1} \chi^n(g^s + 1) \bar{\psi}^n(g^s + 1).$$

Evidently $S_n = d$ for $n = 0$ and $\bar{S}_n = S_{e-n}$ for $1 \leq n \leq e-1$. For later applications we write $S(g)$ in the form

$$(2.6) \quad S(g) = d + S_{e/2} + \sum_{n=1}^{e/2-1} (S_n + \bar{S}_n).$$

It should be noted that when $e = 2$ the sum in (2.6) is vacuous.

The evaluation of S_n is facilitated by expressing the sum in (2.5) terms of Jacobi sums depending on χ and ψ . For integers m, n we define the Jacobi sum

$$(2.7) \quad J_\chi(m, n) = \sum_{a+b \equiv 1 \pmod{p}} \chi^m(a) \chi^n(b),$$

the summation extending over all pairs of integers in the range $1 \leq a, b \leq p-1$ such that $a+b \equiv 1 \pmod{p}$. We also define the corresponding Jacobi sum $J_\psi(m, n)$. Thus the sums $J_\chi(m, n), J_\psi(m, n)$ depend upon the choice of the common primitive root g of the primes $p = ef + 1, q = ef' + 1$.

The following well-known properties of $J_\chi(m, n)$ will be employed many times in the sequel.

$$(2.8) \quad J_\chi(0, 0) = p-2, \quad J_\chi(m, 0) = -1 \quad (m = 1, \dots, e-1).$$

$$(2.9) \quad J_\chi(m, n) = \bar{J}_\chi(-m, -n) = J_{\bar{\chi}}(-m, -n).$$

$$(2.10) \quad J_\chi(m, n) = J_\chi(n, m) = (-1)^{nf} J_\chi(-m-n, n).$$

$$(2.11) \quad J_\chi(m, n) J_\chi(-m, -n) = p.$$

In (2.11) it is assumed that no one of $m, n, m+n$ is divisible by e .

The Jacobi sum $J_\chi(m, n)$ is closely related to the Lagrange sum defined by

$$(2.12) \quad \tau(\alpha) = \sum_{a=1}^{p-1} \alpha^{\text{ind } a} \zeta^a \quad (g^{\text{ind } a} \equiv a \pmod{p}),$$

where α denotes a root of the equation $\alpha^{p-1} = 1$, and $\zeta = \exp(2\pi i/p)$. Indeed we have the formula

$$(2.13) \quad J_\chi(m, n) = \tau(\beta^m) \tau(\beta^n) / \tau(\beta^{m+n})$$

when $m+n$ is not divisible by e . A deeper property of (2.12) is given by the formula

$$(2.14) \quad \tau(-1) \tau(\alpha^2) = \alpha^{2m} \tau(\alpha) \tau(-\alpha),$$

where the integer m is defined by the congruence $g^m \equiv 2 \pmod{p}$.

Formulas (2.8), ..., (2.14) are developed, for example, in an important paper of Dickson [1] on the theory of cyclotomy. The notation $J_\chi(m, n)$ in this paper corresponds to Dickson's $R(m, n)$.

We shall require the following two lemmas.

LEMMA 3. If a is an integer not divisible by p , and n is an arbitrary integer, then

$$(2.15) \quad \sum_{u=1}^{p-1} \chi^n(au^e + 1) = \sum_{m=0}^{e-1} \chi^m(-1) \bar{\chi}^m(a) J_\chi(m, n).$$

Proof. In the left member of (2.15) the number u^e runs e times over the f incongruent e th power residues of p . Since the sum $1 + \chi(r) + \cdots + \chi^{e-1}(r)$ equals e or 0 according as r is an e th power residue or not, we find that

$$\begin{aligned} \sum_{u=1}^{p-1} \chi^n(au^e + 1) &= \sum_{u=1}^{p-1} \sum_{m=0}^{e-1} \bar{\chi}^m(a) \chi^m(au) \chi^n(au + 1) \\ &= \sum_{m=0}^{e-1} \bar{\chi}^m(a) \sum_{u=1}^{p-1} \chi^m(u) \chi^n(u + 1). \end{aligned}$$

When u is replaced by $-u$ the inner sum becomes $\chi^m(-1) J_\chi(m, n)$. This completes the proof of Lemma 3.

If $a \equiv g^k \pmod{p}$, then $\chi(a) = \beta^k$; moreover, $\chi(-1) = \beta^{ef/2} = (-1)^f$. Hence (2.15) may also be written in the form

$$(2.16) \quad \sum_{u=1}^{p-1} \chi^n(g^k u^e + 1) = \sum_{m=0}^{e-1} (-1)^{mf} J_\chi(m, n) \beta^{-mk}.$$

LEMMA 4. Let $p-1 = ef$, $q-1 = ef'$, $(f, f') = 1$. Let $S_n(g)$ be the sum defined in (2.5). Then

$$(2.17) \quad S_n(g) = \frac{1}{e} \sum_{s=0}^{e-1} (-1)^{s(f+f')} J_\chi(s, n) J_{\bar{\psi}}(s, n).$$

Proof. To evaluate the right member of (2.5) we put

$$(2.18) \quad s = k + (q-1)r + (p-1)t \quad (0 \leq k < e; 0 \leq r < f, 0 \leq t < f').$$

Since $d = eff'$ there are d values of s in (2.18). No two of these values of s are in the same residue class modulo d . Hence we find that

$$\begin{aligned} S_n(g) &= \sum_{k=0}^{e-1} \sum_{r=0}^{f-1} \sum_{t=0}^{f'-1} \chi^n(g^{k+(q-1)r} + 1) \bar{\psi}^n(g^{k+(p-1)t} + 1) \\ &= \frac{1}{e^2} \sum_{k=0}^{e-1} \sum_{u=1}^{p-1} \chi^n(g^k u^e + 1) \sum_{v=1}^{q-1} \bar{\psi}^n(g^k v^e + 1). \end{aligned}$$

Substituting from (2.16) and changing the order of summation we get

$$S_n(g) = \frac{1}{e^2} \sum_{s,t=0}^{e-1} (-1)^{sf+tf'} J_\chi(s, n) J_{\bar{\psi}}(t, n) \sum_{k=0}^{e-1} \beta^{-k(s-t)}.$$

The inner sum vanishes unless $s = t$. The identity in (2.17) is an immediate consequence.

In order to summarize the results of this section we find it convenient to put

$$(2.19) \quad M = \frac{(p-2)(q-2)-1}{e}.$$

Then we can write

$$(2.20) \quad M + \eta = d - T,$$

where T is given in (2.4), and $\eta = 0$ or 1 according as ff' is even or odd. From the line immediately following (2.3) we have the equation $S(g) = eN(g) + T(g)$. The following theorem now follows from (2.6) and (2.20).

THEOREM 1. *Let $S_n(g)$ be the sum in (2.17). Then the number $N_e(g)$ of solutions in s, t ($0 \leq s, t \leq d-1$) of the congruence $g^s + 1 \equiv g^t \pmod{pq}$ is furnished by the formula*

$$(2.21) \quad eN_e(g) = M + \eta + S_{e/2}(g) + \sum_{n=1}^{e/2-1} (S_n(g) + \bar{S}_n(g)),$$

where the sum is vacuous for $e = 2$.

3. The common primitive roots of p and q . The value $N_e(g)$ depends in general on the choice of the common primitive root g of p and q . In this section we shall establish three lemmas giving information about the set of such common primitive roots.

LEMMA 5. *Let p and q denote two distinct odd primes; let e denote the greatest common divisor of $p-1$ and $q-1$, and put $(p-1)(q-1) = de$. Then the number $n_e(p, q)$ of common primitive roots of p and q in a reduced residue system modulo pq is given by*

$$(3.1) \quad n_e(p, q) = \phi(e)\phi(d),$$

where $\phi(m)$ is Euler's function.

Proof. By the Chinese Remainder Theorem the number $n_e(p, q)$ is equal to $\phi(p-1)\phi(q-1)$. We now apply the well-known formula

$$(3.2) \quad \phi(mn) = \frac{P\phi(m)\phi(n)}{\phi(P)},$$

where P is the product of the primes common to m and n . Put $p-1 = ef$, $q-1 = ef'$, $(f, f') = 1$. Then the product P of primes common to e and f is also the product of primes common to ef' and f . By (3.2) we get

$$\phi(p-1) = \frac{P\phi(e)\phi(f)}{\phi(P)}, \quad \phi(d) = \frac{P\phi(q-1)\phi(f)}{\phi(P)}.$$

Hence the product $\phi(p-1)\phi(q-1)$ reduces to the right member of (3.1). This proves the lemma.

Let $\bar{G}$ denote the set of common primitive roots of p and q . If g is in $\bar{G}$, then g has the exponent d modulo pq . Furthermore, the number g^r is in $\bar{G}$ if and only if $(r, d) = 1$. When $(r, d) = 1$ the set of powers of g modulo pq is the same as the set of powers of g^r . In view of Lemma 5 the following conclusion may now be asserted.

LEMMA 6. *The $\phi(e)\phi(d)$ roots in $\bar{G}$ can be separated into $\phi(e)$ disjoint classes $G_1, G_2, \dots, G_{\phi(e)}$, each containing $\phi(d)$ roots. These classes can be characterized as follows: If g_i is in G_i , then G_i consists of the $\phi(d)$ numbers*

$$g_i^r \quad (r = 1, \dots, d-1; (r, d) = 1).$$

In the rest of this section we assume that $e = 4$ or 6 so that $\phi(e) = 2$. Then by Lemma 6 the set $\bar{G}$ of common primitive roots of p and q modulo pq can be separated into two classes G, G' . If $g \in G, g' \in G'$, then every root in G is a power of g , while every root in G' is a power of g' . We now fix g, g' and put

$$(3.3) \quad g \equiv g'^r \pmod{p}, \quad g \equiv g'^s \pmod{q}.$$

The exponents r, s in (3.3) are such that $(r, p-1) = (s, q-1) = 1$; in particular, $(r, e) = (s, e) = 1$. Since $e = 4$ or 6 it follows that $r \equiv \pm 1 \pmod{e}, s \equiv \pm 1 \pmod{e}$. We next show that

$$(3.4) \quad r \not\equiv s \pmod{e}.$$

Otherwise, since $(p-1, q-1) = e$, the congruence $r \equiv s \pmod{e}$ implies the existence of integers h, k such that

$$(3.5) \quad r + h(p-1) = s + k(q-1).$$

Putting $t = r + h(p-1)$ we deduce from (3.3) and (3.5) that $g \equiv g'^t \pmod{pq}$, so that g is a power of g' in violation of the definition of the classes G, G' . As a consequence of (3.4) we have the following useful lemma.

LEMMA 7. *Let $e = 4$ or 6 and let $g \in G, g' \in G'$ be fixed primitive roots of both p and q . Let a be an integer relatively prime to p and q . Then the corresponding characters $\chi(a), \psi(a)$ and $\chi'(a), \psi'(a)$ are so related that one of the following two cases holds:*

- (i) $\chi(a) = \chi'(a)$ and $\psi(a) = \bar{\psi}'(a)$,
- (ii) $\chi(a) = \bar{\chi}'(a)$ and $\psi(a) = \psi'(a)$.

Proof. Consider the pair of congruences

$$(3.6) \quad a \equiv g^u \pmod{p}, \quad a \equiv g^v \pmod{q},$$

so that $\chi(a) = \beta^u, \psi(a) = \beta^v$. Let $\chi'(a), \psi'(a)$ be the characters constructed

using g' in place of g . Then the congruences in (3.3) and (3.6) imply that $\chi'(a) = \beta^{ru}$, $\psi'(a) = \beta^{sv}$. Applying (3.4) we obtain case (i) or case (ii) of the lemma according as $r \equiv \pm 1 \pmod{e}$. This completes the proof.

Lemma 7 will be used in §§5 and 6 to distinguish the value of $N_e(g)$ from $N_e(g')$.

4. The case $e = 2$. We now apply the results of §2 to evaluate $N_2(g)$. Let $p - 1 = 2f$, $q - 1 = 2f'$, $(f, f') = 1$. Furthermore, put $M = ((p - 2)(q - 2) - 1)/2$. By Theorem 1 with $e = 2$ we have $2N_2(g) = M + \eta + S_1(g)$, where

$$(4.1) \quad 2S_1(g) = J_\chi(0, 1)J_{\bar{\psi}}(0, 1) + (-1)^{f+f'}J_\chi(1, 1)J_{\bar{\psi}}(1, 1).$$

Since $\beta = -1$ when $e = 2$ the character $\chi(a)$ modulo p reduces to the Legendre symbol $(a|p)$. The Jacobi sum in (2.7) becomes in turn

$$J_\chi(m, n) = \sum_{a=1}^{p-1} \left(\frac{a}{p}\right)^m \left(\frac{1-a}{p}\right)^n.$$

Clearly $J_\chi(0, 1) = -1$. Moreover

$$J_\chi(1, 1) = \sum_{a=1}^{p-1} \left(\frac{a}{p}\right) \left(\frac{1-a}{p}\right) = \sum_{a=1}^{p-1} \left(\frac{\bar{a}-1}{p}\right) = - \left(\frac{-1}{p}\right) = -(-1)^f,$$

where $\bar{a}$ has been chosen so that $a\bar{a} \equiv 1 \pmod{p}$. Substituting these values into (4.1) we get $S_1(g) = 1$. The results of this section may now be summarized in the following theorem.

THEOREM 2. *When $e = 2$ the number of solutions of (2.2) is equal to*

$$(4.2) \quad N_2(g) = \begin{cases} \frac{1}{4}(pq - 2p - 2q + 5) & (ff' \text{ even}), \\ \frac{1}{4}(pq - 2p - 2q + 7) & (ff' \text{ odd}). \end{cases}$$

It is evident from (4.2) that the value of $N_2(g)$ does not depend upon the particular choice of g .

5. The case $e = 4$. Let $p - 1 = 4f$, $q - 1 = 4f'$, $(f, f') = 1$, and let g be a common primitive root of p and q . We proceed to evaluate $N_4(g)$ by means of the machinery developed in §2. In view of Theorem 1 we must first evaluate $S_1(g)$ and $S_2(g)$.

By (2.8) and (2.10) we have $J_\chi(0, 1) = -1$, $J_\chi(2, 1) = (-1)^f J_\chi(1, 1)$ and $J_\chi(3, 1) = -(-1)^f$. Hence (2.17) with $e = 4$, $n = 1$ becomes

$$(5.1) \quad S_1(g) = \frac{1}{2} + \frac{1}{2}(-1)^{f+f'}J_\chi(1, 1)J_{\bar{\psi}}(1, 1).$$

Again, from (2.8), (2.9) and (2.10) we get $J_\chi(0, 2) = J_\chi(2, 2) = -1$,

$J_x(1,2) = (-1)^f J_x(1,1)$ and $J_{\bar{x}}(3,2) = (-1)^f J_{\bar{x}}(1,1)$. Consequently (2.17) with $e = 4$, $n = 2$ reduces to

$$(5.2) \quad S_2(g) = \frac{1}{2} + \frac{1}{4}(J_x(1,1)J_{\bar{\psi}}(1,1) + J_{\bar{x}}(1,1)J_{\psi}(1,1)).$$

For simplicity we write $J_x = J_x(1,1)$, $J_{\psi} = J_{\psi}(1,1)$. Then Theorem 1 with $e = 4$ in conjunction with (5.1) and (5.2) yields

$$(5.3) \quad 4N_4(g) = M + \eta + \frac{3}{2} + \frac{1}{4}(1 + 2\chi(-1)\psi(-1))(J_x J_{\bar{\psi}} + J_{\bar{x}} J_{\psi}),$$

where $M = ((p-2)(q-2)-1)/4$. The value of $N_4(g)$ furnished by (5.3) depends upon the particular choice of g . The nature of this dependence is revealed by Lemma 7. In the sense of this lemma let $g \in G$, $g' \in G'$. Then the value of $N_4(g')$ is given by

$$(5.4) \quad 4N_4(g') = M + \eta + \frac{3}{2} + \frac{1}{4}(1 + 2\chi(-1)\psi(-1))(J_x J_{\psi} + J_{\bar{x}} J_{\bar{\psi}}).$$

Following Dickson (compare [1, (50)]) we now put

$$(5.5) \quad J_x(1,1) = -x + 2\beta y, \quad J_{\psi}(1,1) = -X + 2\beta Y,$$

where $\beta^2 = -1$. From (2.11) it follows that

$$(5.6) \quad p = x^2 + 4y^2, \quad q = X^2 + 4Y^2.$$

Dickson [1, pp. 400–401] proved that the signs of x and X in (5.6) are uniquely determined by the conditions $x \equiv X \equiv 1 \pmod{4}$; however, y and Y are two-valued, depending on the choice of the primitive root g . Substituting from (5.5) into (5.3) and (5.4) we obtain

THEOREM 3. *When $e = 4$ the number of solutions of (2.2) satisfies the formulas*

$$(5.7) \quad 4N_4(g) = M + \eta + \frac{3}{2} + \frac{1}{2}(1 + 2(-1)^{f+f'})(xX + 4yY),$$

$$(5.8) \quad 4N_4(g') = M + \eta + \frac{3}{2} + \frac{1}{2}(1 + 2(-1)^{f+f'})(xX - 4yY).$$

The following corollary of Theorem 3, stated without proof in [3, Lemma 6], plays a central role in the construction of a special family of difference sets [3, Theorem 4].

COROLLARY. *If $N_4(g)$, $N_4(g')$ correspond to $g \in G$, $g' \in G'$ respectively, then the following inequality holds:*

$$(5.9) \quad N_4(g) \neq N_4(g').$$

Proof. Subtracting (5.8) from (5.7) we get

$$N_4(g) - N_4(g') = (1 + 2(-1)^{f+f'})yY.$$

The inequality (5.9) follows at once.

Theorem 3 has the following interpretation. By a well-known theorem [2, p. 128] there are exactly two representations of pq in the form $a^2 + 4b^2$ with $a \equiv 1 \pmod{4}$ and b indeterminate. Let

$$(5.10) \quad pq = a^2 + 4b^2, \quad pq = a'^2 + 4b'^2 \quad (a \equiv a' \equiv 1 \pmod{4})$$

denote these two representations. From (5.6) we have

$$pq = (xX \pm 4yY)^2 + 4(xY \mp yX)^2.$$

Hence formula (5.7) may be written alternatively in the form

$$(5.11) \quad 16N_4(g) = \begin{cases} pq - 2p - 2q + 9 - 2a & (ff' \text{ even}), \\ pq - 2p - 2q + 13 + 6a & (ff' \text{ odd}), \end{cases}$$

where a appears in one of the two decompositions in (5.10), say the first. In view of the corollary the corresponding formula for $N_4(g')$ is obtained from (5.11) by replacing g by g' and a by a' .

6. The case $e = 6$. Throughout this section let $p - 1 = 6f$, $q - 1 = 6f'$, $(f, f') = 1$. The number β is thus a primitive sixth root of unity so that $\beta^2 = \beta - 1$. We shall evaluate $N_6(g)$, where g is a primitive root of both p and q . In order to apply Theorem 1 we first obtain expressions for $S_1(g)$, $S_2(g)$, $S_3(g)$ in terms of Jacobi sums.

In (2.4) replace α by β and then multiply both members of the resulting equation by $\tau(\beta^2)/\tau(\beta^3)\tau(\beta^4)$. By (2.10) and (2.13) we get

$$(6.1) \quad J_x(4, 1) = \chi^4(2)J_x(2, 1), \quad J_x(2, 2) = \chi^2(2)J_x(2, 1),$$

where $\chi(2) = \beta^m$ and $g^m \equiv 2 \pmod{p}$. For brevity we shall write J_x in place of $J_x(2, 1)$. Using (2.8), (2.9), (2.10) in connection with (6.1) we may express each of the eighteen sums $J_x(s, n)$ ($0 \leq s \leq 5$, $1 \leq n \leq 2$) in terms of J_x . The formulas are given in the following table.

	$n = 1$	$n = 2$	$n = 3$
$J_x(0, n)$	-1	-1	-1
$J_x(1, n)$	$\chi(-1)\chi^4(2)J_x$	J_x	$\chi(-1)J_x$
$J_x(2, n)$	J_x	$\chi^2(2)J_x$	J_x
$J_x(3, n)$	$\chi(-1)J_x$	J_x	$-\chi(-1)$
$J_x(4, n)$	$\chi^4(2)J_x$	-1	$J_{\bar{x}}$
$J_x(5, n)$	$-\chi(-1)$	$\chi^2(2)J_{\bar{x}}$	$\chi(-1)J_{\bar{x}}$

We employ Lemma 4 with $e = 6$. Substituting the results in the table into (2.17) we get for $n = 1, 2, 3$

$$(6.2) \quad S_1(g) = \frac{1}{3}(1 + J_x J_{\bar{\psi}} + \chi^4(2)\psi^2(2)J_x J_{\bar{\psi}}).$$

$$(6.3) \quad S_2(g) = \frac{1}{6}(2 + 2_x(-1)\psi(-1)J_x J_{\bar{\psi}} + \chi^2(2)\psi^4(2)J_x J_{\bar{\psi}} \\ + \chi(-1)\psi(-1)\chi^2(2)\psi^4(2)J_{\bar{x}} J_{\psi}).$$

$$(6.4) \quad S_3(g) = \frac{1}{3}(1 + J_x J_{\bar{\psi}} + J_{\bar{x}} J_{\psi}).$$

We are now in the position to evaluate $N_6(g)$ by means of Theorem 1 with $e = 6$. Noting that $\chi(-1)\psi(-1)$ is equal to ± 1 according as ff' is odd or even, and using (6.2), (6.3), (6.4) we get

$$(6.5) \quad 36N_6(g) = 6M + 6\eta + 10 + \delta J_x J_{\bar{\psi}} + \bar{\delta} J_{\bar{x}} J_{\psi},$$

where $M = ((p-2)(q-2)-1)/6$, and where

$$(6.6) \quad \delta = \begin{cases} 2 + \chi^2(2)\psi^4(2) + \chi^4(2)\psi^2(2) & (ff' \text{ even}), \\ 6 + \chi^2(2)\psi^4(2) + 3\chi^4(2)\psi^2(2) & (ff' \text{ odd}). \end{cases}$$

The expression for $N_6(g)$ in (6.5) depends upon the choice of g . Let $g \in G$, $g' \in G'$ in the sense of Lemma 7. It follows from this lemma that

$$(6.5)' \quad 36N_6(g') = 6M + 6\eta + 10 + \delta' J_x J_{\psi} + \bar{\delta}' J_{\bar{x}} J_{\bar{\psi}},$$

where

$$(6.6)' \quad \delta' = \begin{cases} 2 + \chi^2(2)\psi^2(2) + \chi^4(2)\psi^4(2) & (ff' \text{ even}), \\ 6 + \chi^2(2)\psi^2(2) + 3\chi^4(2)\psi^4(2) & (ff' \text{ odd}). \end{cases}$$

When ff' is even it is clear from (6.6), (6.6)' that $\delta = \bar{\delta}$ and $\delta' = \bar{\delta}'$. More precisely, $\delta = 4$ or 1 according as $\chi^2(2)\psi^4(2) = 1$ or not, and $\delta' = 4$ or 1 according as $\chi^2(2)\psi^2(2) = 1$ or not. When ff' is odd, $\delta = 10, 5 - 2\beta, 3 + 2\beta$ according as $\chi^2(2)\psi^4(2) = 1, \beta^2, \beta^4$ respectively, and $\delta' = 10, 5 - 2\beta, 3 + 2\beta$ according as $\chi^2(2)\psi^2(2) = 1, \beta^2, \beta^4$ respectively. To simplify further we consider separately the cases (i) ff' even, $\delta = 1$, (ii) ff' even, $\delta = 4$, (iii) ff' odd, $\delta = 10$, (iv) ff' odd, $\delta = 5 - 2\beta$, (v) ff' odd, $\delta = 3 + 2\beta$; (i)' ff' even, $\delta' = 1$, (ii)' ff' even, $\delta' = 4$, (iii)' ff' odd, $\delta' = 10$, (iv)' ff' odd, $\delta' = 5 - 2\beta$, (v)' ff' odd, $\delta' = 3 + 2\beta$.

Following Dickson [1, (85)] we put

$$(6.7) \quad J_x(2, 1) = -a + b(2\beta - 1), \quad J_{\bar{x}}(2, 1) = -A + B(2\beta - 1),$$

where, in view of (2.11), we have

$$(6.8) \quad p = a^2 + 3b^2, \quad q = A^2 + 3B^2,$$

Dickson [1, p. 409], proved that $a \equiv 1$ or $4 \pmod{6}$ according as f is even or odd; similarly, $A \equiv 1$ or $4 \pmod{6}$ according as f' is even or odd. On the other hand, b and B are uniquely determined by (6.8) except for sign. Substituting from (6.7) into (6.5) and (6.5)' we obtain the following theorem.

THEOREM 4. *When $e = 6$ the number of solutions of (2.2) satisfies the formulas*

$$(6.9) \quad 36N_6(g) = \begin{cases} 6M + 10 + 2\delta(aA + 3bB) & (\text{cases i, ii}), \\ 6M + 16 + 20(aA + 3bB) & (\text{case iii}), \\ 6M + 16 + 8(aA + 3bB) \pm 6(aB - bA) & (\text{cases iv, v}). \end{cases}$$

$$(6.9)' \quad 36N_6(g') = \begin{cases} 6M + 10 + 2\delta'(aA - 3bB) & (\text{cases i', ii'}), \\ 6M + 16 + 20(aA - 3bB) & (\text{case iii'}), \\ 6M + 16 + 8(aA - 3bB) \pm 6(aB + bA) & (\text{case iv', v'}). \end{cases}$$

The ambiguous sign is plus in cases iv, v' and minus in cases v, iv'.

In view of the corollary to Theorem 3 it is natural to inquire if the value $N_6(g)$ necessarily differs from $N_6(g')$. Actually, Theorem 4 implies in some instances but not in general that $N_6(g) \neq N_6(g')$. Thus if ff' is even and $\delta = \delta'$, then $36N_6(g) - 36N_6(g') = 12\delta bB$. Again if ff' is odd and $\delta = \delta' = 10$, then $36N_6(g) - 36N_6(g') = 120bB$. On the other hand, consider the example $p = 7$, $q = 19$, $g = 3$, $g' = 10$, in which $\chi(2) = \chi'(2) = \beta^2$, $\psi(2) = \bar{\psi}'(2) = \beta$. Then $J_x = 1 + 2\beta$, $J_y = -3 - 2\beta$ so that $a = -2$, $b = 1$, $A = 4$, $B = -1$. Moreover, ff' is odd, $\delta = 5 - 2\beta$, $\delta' = 10$. We deduce from case iv of (6.9) and case iii' of (6.9)' that $N_6(g) = N_6(g') = 0$.

From (6.8) we obtain $pq = (aA \pm 3bB)^2 + 3(aB \mp bA)^2$. Hence (6.9) may be recast in the following form:

$$(6.10) \quad 36N_6(g) = \begin{cases} pq - 2p - 2q + 13 + 2\delta c & (\text{cases i, ii}), \\ pq - 2p - 2q + 19 + 20c & (\text{case iii}), \\ pq - 2p - 2q + 19 + 8c \pm 6d & (\text{cases iv, v}), \end{cases}$$

where $c^2 + 3d^2$ is one of the two representations of pq as a square plus three times a square. The sign of c is uniquely determined by the condition that $c \equiv 4$ or $1 \pmod{6}$ according as ff' is even or odd. On the other hand, d is ambiguously determined.

7. The case $e = 8$. In this section we shall obtain expressions for $N_8(g)$, where g is a common primitive root of $p = 8f + 1$, $q = 8f' + 1$ and $(f, f') = 1$. In order to apply Theorem 1 with $e = 8$ we first derive expressions for $S_1(g)$, $S_2(g)$, $S_3(g)$, $S_4(g)$.

Let $\beta = \exp(2\pi i/8)$; then $\chi(2) = \beta^m$ where $g^m \equiv 2 \pmod{p}$. It turns out that each of the thirty-two Jacobi sums $J_\chi(s, n)$ ($0 \leq s \leq 7$, $1 \leq n \leq 4$) may be expressed in terms of either $J_\chi(2, 2)$ or $J_\chi(3, 1)$. The results are given compactly in the following table.

	$n = 1$	$n = 2$
$J_x(0, n)$	-1	-1
$J_x(1, n)$	$\chi(-1)\chi^6(2)J_x(3, 1)$	$\chi(-1)\chi^6(2)J_x(2, 2)$
$J_x(2, n)$	$\chi(-1)\chi^6(2)J_x(2, 2)$	$J_x(2, 2)$
$J_x(3, n)$	$J_x(3, 1)$	$\chi^2(2)J_x(3, 1)$
$J_x(4, n)$	$\chi(-1)J_x(3, 1)$	$J_x(2, 2)$
$J_x(5, n)$	$\chi^6(2)J_x(2, 2)$	$\chi(-1)\chi^6(2)J_x(2, 2)$
$J_x(6, n)$	$\chi^6(2)J_x(3, 1)$	-1
$J_x(7, n)$	$-\chi(-1)$	$\chi^2(2)J_{\bar{x}}(3, 1)$

	$n = 3$	$n = 4$
$J_x(0, n)$	-1	-1
$J_x(1, n)$	$J_x(3, 1)$	$\chi(-1)J_x(3, 1)$
$J_x(2, n)$	$\chi^2(2)J_x(3, 1)$	$J_x(2, 2)$
$J_x(3, n)$	$\chi(-1)\chi^2(2)J_x(3, 1)$	$\chi(-1)J_x(3, 1)$
$J_x(4, n)$	$\chi(-1)J_x(3, 1)$	-1
$J_x(5, n)$	$-\chi(-1)$	$\chi(-1)J_{\bar{x}}(3, 1)$
$J_x(6, n)$	$\chi(-1)\chi^2(2)J_{\bar{x}}(2, 2)$	$J_{\bar{x}}(2, 2)$
$J_x(7, n)$	$\chi^2(2)J_{\bar{x}}(2, 2)$	$\chi(-1)J_{\bar{x}}(3, 1)$

The entries in the table follow from one or more of the formulas (2.8), ..., (2.14). For example, the formula for $J_x(2, 1)$ is obtained from (2.14) upon replacing α by β and then applying (2.10) and (2.13). Again, if in (2.14) α is replaced by β^3 and both members of the resulting equation are multiplied by $\tau(\beta)/\tau(\beta^4)\tau(\beta^7)$, then the formula for $J_x(1, 1)$ follows. The other entries are similarly established.

By means of Lemma 4 with $e = 8$ we obtain the following results:

$$\begin{aligned}
 S_1(g) = & \frac{1}{4} \{ 1 + \chi^6(2)\psi^2(2)J_x(3, 1)J_{\bar{\psi}}(3, 1) \\
 (7.1) \quad & + \chi(-1)\psi(-1)\chi^6(2)\psi^2(2)J_x(2, 2)J_{\bar{\psi}}(2, 2) \\
 & + \chi(-1)\psi(-1)J_x(3, 1)J_{\bar{\psi}}(3, 1) \},
 \end{aligned}$$

$$(7.2) \quad S_2(g) = \frac{1}{8} \{ 2 + 2J_x(2,2)J_{\bar{\psi}}(2,2) + 2\chi^6(2)\psi^2(2)J_x(2,2)J_{\bar{\psi}}(2,2) \\ + \chi(-1)\psi(-1)\chi^2(2)\psi^6(2)(J_x(3,1)J_{\bar{\psi}}(3,1) + J_{\bar{x}}(3,1)J_{\psi}(3,1)) \},$$

$$(7.3) \quad S_3(g) = \frac{1}{4} \{ 1 + (\chi(-1)\psi(-1) + \chi^2(2)\psi^6(2))J_x(3,1)J_{\bar{\psi}}(3,1) \\ + \chi(-1)\psi(-1)\chi^2(2)\psi^6(2)J_{\bar{x}}(2,2)J_{\psi}(2,2) \},$$

$$(7.4) \quad S_4(g) = \frac{1}{8} \{ 2 + 2(J_x(3,1)J_{\bar{\psi}}(3,1) + J_{\bar{x}}(3,1)J_{\psi}(3,1) \\ + (J_x(2,2)J_{\bar{\psi}}(2,2) + J_{\bar{x}}(2,2)J_{\psi}(2,2))) \}.$$

We now apply Theorem 1 with $e = 8$. The result of substituting (7.1), (7.2), (7.3), (7.4) into (2.21) may be summarized as follows. Let $M = ((p-2)(q-2)-1)/8$. Then

$$(7.5) \quad 64N_8(g) = 8M + 8\eta + 14 + \delta(J_x(3,1)J_{\bar{\psi}}(3,1) + J_{\bar{x}}(3,1)J_{\psi}(3,1)) \\ + \varepsilon(J_x(2,2)J_{\bar{\psi}}(2,2) + J_{\bar{x}}(2,2)J_{\psi}(2,2)),$$

where

$$(7.6) \quad \delta = \begin{cases} -2 + \chi^2(2)\psi^6(2) + \chi^6(2)\psi^2(2) & (ff' \text{ even}), \\ 6 + 3\chi^2(2)\psi^6(2) + 3\chi^6(2)\psi^2(2) & (ff' \text{ odd}), \end{cases}$$

and

$$(7.7) \quad \varepsilon = \begin{cases} 3 - 2\chi^6(2)\psi^2(2) & (ff' \text{ even}), \\ 3 + 6\chi^6(2)\psi^2(2) & (ff' \text{ odd}). \end{cases}$$

In view of (5.5) we put

$$(7.8) \quad J_x(2,2) = -x + 2\beta^2 y, \quad J_{\psi}(2,2) = -X + 2\beta^2 Y,$$

where

$$(7.9) \quad p = x^2 + 4y^2, \quad q = X^2 + 4Y^2 \quad (x \equiv X \equiv 1 \pmod{4}).$$

Following Dickson [1, p. 411], we also put

$$(7.10) \quad J_x(3,1) = -a + b(\beta + \beta^3), \quad J_{\psi}(3,1) = -A + B(\beta + \beta^3),$$

where

$$(7.11) \quad p = a^2 + 2b^2, \quad q = A^2 + 2B^2.$$

Dickson [1, pp. 411-413] proved that $a \equiv \pm 1 \pmod{4}$ according as f is even or odd; similarly $A \equiv \pm 1 \pmod{4}$ according as f' is even or odd. On the other hand, the signs of b, B are ambiguous and depend on the selection of g .

Since $(2|p) = 1$, $(2|q) = 1$ it follows that $\chi^2(2) = \pm 1$, $\psi^2(2) = \pm 1$. Hence the numbers δ, ε in (7.6), (7.7) are real. Indeed, if ff' is even, then $\delta = 0$ or -4 and

$\varepsilon = 1$ or 5 according as $\chi^2(2)\psi^6(2) = \pm 1$; if ff' is odd, then $\delta = 12$ or 0 and $\varepsilon = 9$ or -3 according as $\psi^2(2)\psi^6(2) = \pm 1$. Substituting from (7.8), (7.10) into (7.5) we obtain the following theorem.

THEOREM 5. *When $e = 8$ the number $N_8(g)$ of solutions of (2.2) satisfies*

$$(7.12) \quad 64N_8(g) = \begin{cases} 8M + 14 + 2(xX + 4yY) \\ \quad (ff' \text{ even}, \chi^2(2)\psi^6(2) = 1), \\ 8M + 14 - 8(aA + 2bB) + 10(xX + 4yY) \\ \quad (ff' \text{ even}, \chi^2(2)\psi^6(2) = -1), \\ 8M + 22 + 24(aA + 2bB) + 18(xX + 4yY) \\ \quad (ff' \text{ odd}, \chi^2(2)\psi^6(2) = 1), \\ 8M + 22 - 6(xX + 4yY) \\ \quad (ff' \text{ odd}, \chi^2(2)\psi^6(2) = -1). \end{cases}$$

Because y, Y, b, B are ambiguous, formula (7.12) is valid only for some unspecified choices of g . More explicit expressions may be derived if we make use of the classification of primitive roots given in Lemma 6 with $e = 8$. However, we shall not take the space to deduce the resulting formulas.

8. The modulus pqr . Let g be a common primitive root of distinct odd primes p, q, r . The exponent d to which g belongs modulo pqr is the least common multiple of $p-1, q-1, r-1$. Making the assumption

$$(8.1) \quad (p-1, q-1) = (q-1, r-1) = (r-1, p-1) = 2,$$

we find that $d = (p-1)(q-1)(r-1)/4$. In this section we derive explicit expressions for the number $N(g)$ of solutions of the congruence

$$(8.2) \quad g^s + 1 \equiv g^t \pmod{pqr},$$

where s and t are each selected from $0, 1, \dots, d-1$. The method is essentially that of §2.

We define three Legendre characters as follows: $\chi(n) = (n|p)$, $\psi(n) = (n|q)$, $\lambda(n) = (n|r)$. The argument used to prove Lemma 1 yields the following criterion. Let s be a fixed integer such that $0 \leq s \leq d-1$ and $(g^s + 1, pqr) = 1$. Then there corresponds an integer t such that $0 \leq t \leq d-1$ and $g^s + 1 \equiv g^t \pmod{pqr}$ if and only if $\chi(g^s + 1) = \psi(g^s + 1) = \lambda(g^s + 1)$.

Let $T(g)$ denote the number of values of s such that $0 \leq s \leq d-1$ and $(g^s + 1, pqr) = 1$. It is clear that the number $N(g)$ of solutions of (8.2) is related to the sum

$$(8.3) \quad S(g) = \sum_{s=0}^{d-1} \{1 + \chi^2(g^s + 1)\psi(g^s + 1)\lambda(g^s + 1) \\ + \chi(g^s + 1)\psi^2(g^s + 1)\lambda(g^s + 1) + \chi(g^s + 1)\psi(g^s + 1)\lambda^2(g^s + 1)\}$$

by means of the equation

$$(8.4) \quad S(g) = 4N(g) + T(g).$$

We proceed to compute $T(g)$. For an integer v let N_v denote the number of values of s ($s = 0, 1, \dots, d-1$) for which $N = N(s) = 1 + g^s$ is divisible by v . It follows from a familiar combinatorial principle that $T(g) = N_p + N_q + N_r - N_{pq} - N_{pr} - N_{qr} + N_{pqr}$. We first evaluate N_{pqr} . Put $p-1 = 2f$, $q-1 = 2f'$, $r-1 = 2f''$. By (8.1) at most one of f, f', f'' is even. If $ff'f''$ is odd, then $-1 \equiv g^{d/2} \pmod{pqr}$. But if $ff'f''$ is even, then there is no value of s such that $-1 \equiv g^s \pmod{pqr}$, where $0 \leq s \leq d-1$. Hence N_{pqr} is equal to 0 or 1 according as $ff'f''$ is even or odd. We next determine N_{pq} . When ff' is even the congruence $g^s + 1 \equiv 0 \pmod{pq}$, $0 \leq s \leq d-1$, is not solvable. But when ff' is odd this congruence is solvable if and only if s is an odd multiple of $(p-1)(q-1)/4$. There are $(r-1)/2$ such values of s between 0 and $d-1$. Thus $N_{pq} = 0$ or f'' according as ff' is even or odd; similarly, $N_{pr} = 0$ or f' according as ff'' is even or odd, and $N_{qr} = 0$ or f according as $f'f''$ is even or odd. Finally, we evaluate N_p . As s ranges from 0 to $d-1$, the least positive remainders of g^s modulo p range $f'f''$ times over each of the integers between 1 and $p-1$. Hence $N_p = f'f''$. Similarly, $N_q = ff''$ and $N_r = ff'$. From the results of this paragraph we obtain the following relations.

$$(8.5) \quad T(g) = \begin{cases} ff' + ff'' + f'f'' - f & (f \text{ even}), \\ ff' + ff'' + f'f'' - f' & (f' \text{ even}), \\ ff' + ff'' + f'f'' - f'' & (f'' \text{ even}), \\ ff' + ff'' + f'f'' - f - f' - f'' - 1 & (ff'f'' \text{ odd}). \end{cases}$$

To compute $S(g)$ we write (8.3) in the form $S(g) = d + S_1(g) + S_2(g) + S_3(g)$, where

$$(8.6) \quad \begin{aligned} S_1(g) &= \sum_{s=0}^{d-1} \chi^2(g^s + 1)\psi(g^s + 1)\lambda(g^s + 1), \\ S_2(g) &= \sum_{s=0}^{d-1} \chi(g^s + 1)\psi^2(g^s + 1)\lambda(g^s + 1), \\ S_3(g) &= \sum_{s=0}^{d-1} \chi(g^s + 1)\psi(g^s + 1)\lambda^2(g^s + 1). \end{aligned}$$

Consider the first equation in (8.6). Let u, v, w run through the quadratic residues of p, q, r , respectively. Then this equation may be transformed into

$$\begin{aligned}
 S_1(g) &= \sum_{k=0}^1 \sum_{u,v,w} \chi^2(g^k u + 1) \psi(g^k v + 1) \lambda(g^k w + 1) \\
 &= \frac{1}{8} \sum_{k=0}^1 \sum_{a=1}^{p-1} \chi^2(g^k a^2 + 1) \sum_{b=1}^{p-1} \psi(g^k b^2 + 1) \sum_{c=1}^{p-1} \lambda(g^k c^2 + 1).
 \end{aligned}$$

Employing the easily established formulas

$$\sum_{a=1}^{p-1} \chi(na^2 + 1) = -1 - \chi(n), \quad \sum_{a=1}^{p-1} \chi^2(na^2 + 1) = p - 2 - \chi(-n),$$

we find that

$$S_1(g) = \frac{1}{8} \sum_{k=0}^1 (p - 2 - \chi(-g^k))(-1 - \psi(g^k))(-1 - \lambda(g^k)).$$

This reduces readily to the first equation of

$$\begin{aligned}
 S_1(g) &= \frac{1}{2}(p - 2 - \chi(-1)), \\
 S_2(g) &= \frac{1}{2}(q - 2 - \psi(-1)), \\
 S_3(g) &= \frac{1}{2}(r - 2 - \lambda(-1)).
 \end{aligned}
 \tag{8.7}$$

Because of symmetry the last two equations of (8.6) are transformed into the last two equations of (8.7).

The following theorem now follows from (8.4), (8.5) and (8.7).

THEOREM 6. *The number $N(g)$ of solutions of (8.2) is given by*

$$(8.8) \quad 16N(g) = \begin{cases} (p-2)(q-2)(r-2) + 3p + q + r - 8 & (f \text{ even}), \\ (p-2)(q-2)(r-2) + p + 3q + r - 8 & (f' \text{ even}), \\ (p-2)(q-2)(r-2) + p + q + 3r - 8 & (f'' \text{ even}), \\ (p-2)(q-2)(r-2) + 3p + 3q + 3r - 12 & (ff'f'' \text{ odd}). \end{cases}$$

It is clear from (8.8) that the value of $N(g)$ is independent of the choice of g .

REFERENCES

1. L. E. Dickson, *Cyclotomy, higher congruences, and Waring's problem*, Amer. J. Math. **57** (1935), 391-424.
2. W. J. LeVeque, *Topics in number theory*, Vol. 1, Addison-Wesley, Reading, Mass., 1956.
3. A. L. Whiteman, *A family of difference sets*, Illinois J. Math. **6** (1962), 107-121.

DUKE UNIVERSITY,
 DURHAM, NORTH CAROLINA
 UNIVERSITY OF SOUTHERN CALIFORNIA,
 LOS ANGELES, CALIFORNIA