

# Pacific Journal of Mathematics

**ON THE NUMBER OF SOLUTIONS OF  $u^k + D \equiv w^2 \pmod{p}$**

EMMA LEHMER

# ON THE NUMBER OF SOLUTIONS OF $u^k + D \equiv w^2 \pmod{p}$

EMMA LEHMER

**Introduction.** The number  $N_k(D)$  of solutions  $(u, w)$  of the congruence

$$(1) \quad u^k + D \equiv w^2 \pmod{p}$$

can be expressed in terms of the Gaussian cyclotomic numbers  $(i, j)$  of order  $\text{LCM}(k, 2)$  as has been done by Vandiver [7], or in terms of the character sums introduced by Jacobsthal [4] and studied in special cases by von Schrutka [6], Chowla [1], and Whiteman [8]. In the special cases  $k = 3, 4, 5, 6$ , and  $8$ , the answer can be expressed in terms of certain quadratic partitions of  $p$ , but unless  $D$  is a  $k$ th power residue there remained an ambiguity in sign, which we will be able to eliminate in some cases in the present paper. Theorems 2 and 4 were first conjectured from the numerical evidence provided by the SWAC and later proved by the use of cyclotomy. They improve Jacobsthal's results for all  $p$  for which 2 is not a quartic residue. Similarly Theorem 6 improves von Schrutka's and Chowla's results for those  $p$ 's which do not have 2 for a cubic residue. Only in case  $k = 2$  and in the cases where  $k$  is oddly even and  $D$  is a  $(k/2)$ th but not a  $k$ th power residue is  $N_k(D)$  a function of  $p$  alone and is in fact  $p - 1$ . This result appears in Theorem 1. In case  $k = 4$ , Vandiver [7a] gives an unambiguous solution, which requires the determination of a primitive root.

**1. Character sums.** It is clear that the number of solutions  $N_k(D)$  of (1) can be written

$$N_k(D) = \sum_{u=0}^{p-1} \left[ 1 + \left( \frac{u^k + D}{p} \right) \right] = p + \sum_{u=0}^{p-1} \left( \frac{u^k + D}{p} \right),$$

or

$$(2) \quad N_k(D) = p + \left( \frac{D}{p} \right) + \psi_k(D),$$

---

Received July 10, 1953.

*Pacific J. Math.* 5 (1955), 103-118

where the function

$$(3) \quad \psi_k(D) = \sum_{u=1}^{p-1} \left( \frac{u^k + D}{p} \right)$$

is connected with the Jacobsthal sum

$$(4) \quad \phi_k(D) = \sum_{u=1}^{p-1} \left( \frac{u}{p} \right) \left( \frac{u^k + D}{p} \right)$$

by the relations

$$(5) \quad \psi_k(D) = \left( \frac{D}{p} \right) \phi_k(\bar{D}), \quad k \text{ odd and } D\bar{D} \equiv 1 \pmod{p},$$

and

$$(6) \quad \psi_{2k}(D) = \psi_k(D) + \phi_k(D).$$

Other pertinent relations are

$$(7) \quad \begin{cases} \phi_k(m^k D) = \left( \frac{m}{p} \right)^{k+1} \phi_k(D) \\ \psi_k(m^k D) = \left( \frac{m}{p} \right)^k \psi_k(D) \end{cases} \quad (m \not\equiv 0 \pmod{p})$$

and

$$(8) \quad \begin{cases} \phi_k(\bar{D}) = - \left( \frac{D}{p} \right) \phi_k(D) \\ \psi_k(\bar{D}) = \left( \frac{D}{p} \right) \psi_k(D). \end{cases} \quad (k \text{ even})$$

Also, for  $k$  odd and  $\rho$  a primitive root,

$$(9) \quad \sum_{\nu=0}^{k-1} \phi_k(\rho^\nu) = -k.$$

These relations are either well known or are paraphrases of known relations

and are all easily derivable from the definitions. If  $k$  is odd, it follows from (5) and (6) that

$$(10) \quad \psi_{2k}(D) = \phi_k(D) + \left(\frac{D}{p}\right) \phi_k(\bar{D}).$$

If  $D$  is a  $k$ th power residue, then so is  $\bar{D}$  and hence by (7) for  $k$  odd  $\phi_k(D) = \phi_k(\bar{D}) = \phi_k(1)$ , and we have

$$(11) \quad \psi_{2k}(D) = \phi_k(D) \left[ 1 + \left(\frac{D}{p}\right) \right] = \begin{cases} 2\phi_k(D) & \text{if } \left(\frac{D}{p}\right) = +1 \\ 0 & \text{if } \left(\frac{D}{p}\right) = -1. \end{cases}$$

Hence from (2) we obtain:

**THEOREM 1.** *If  $k$  is odd and if  $D = m^k$ , where  $m$  is a nonresidue of  $p = 2kh + 1$ , then the number  $N_{2k}(m^k)$  of solutions  $(u, w)$  of*

$$u^{2k} + m^k \equiv w^2 \pmod{p}$$

*is exactly  $p - 1$ .*

Since  $\phi_1(D) = -1$ , it follows from (11) that  $\psi_2(D) = -2$ , if  $D$  is a residue, and zero otherwise. Hence by (2),  $N_2(D) = p - 1$  for all  $D$ . This is a well known result in quadratic congruences. We will next discuss the case  $k = 4$ , which is connected with Jacobsthal's theorem.

Jacobsthal [4] proved that if  $D$  is a residue and if  $p = x^2 + 4y^2$ , then

$$(12) \quad \phi_2(D) = -2x \left(\frac{\sqrt{D}}{p}\right), \quad x \equiv 1 \pmod{4};$$

but if  $D$  is a nonresidue then he was able to prove only that

$$(13) \quad \phi_2(D) = \pm 4y.$$

Hence for  $D$  a residue, it follows from the fact that  $\psi_2(D) = -2$ , using (6) and (2), that

$$(14) \quad N_4(D) = p - 1 - 2x \left(\frac{\sqrt{D}}{p}\right), \quad x \equiv 1 \pmod{4}.$$

However, the corresponding result for  $D$  nonresidue would read

$$(15) \quad N_4(D) = p - 1 \pm 4y.$$

In order to eliminate this ambiguity in sign at least for some cases we now turn to the cyclotomic approach.

**2. Cyclotomy.** If we define as usual the cyclotomic number  $(i, j)_k$  as the number of solutions  $(\nu, \mu)$  of the congruence

$$(16) \quad g^{k\nu+i} + 1 \equiv g^{k\mu+j} \pmod{p}$$

then if  $D$  belongs to class  $s$  with respect to some primitive root  $g$  (that is, if  $\text{ind}_g D \equiv s \pmod{k}$ ), we can write the number of nonzero solutions of (1) for  $k$  even as follows:

$$(17) \quad N_k^*(D) = 2k \sum_{\nu=1}^{k/2} (k-s, 2\nu-s)_k.$$

We now assume that 2 is a nonresidue and choose  $g$  so that 2 belongs to the first class, or  $s = 1$ ; then

$$(18) \quad N_4(2) = N_4^*(2) = 8[(3, 1)_4 + (3, 3)_4].$$

These cyclotomic constants have been calculated by Gauss [3] in terms of  $x$  and  $y$  in the quadratic partition  $p = x^2 + 4y^2$  and are for  $p = 8n + 5$

$$(19) \quad 16(3, 3)_4 = p - 2x - 3, \quad 16(3, 1)_4 = p + 2x - 8y + 1.$$

Substituting this into (18) we obtain

$$(20) \quad N_4(2) = p - 1 - 4y, \quad \left(\frac{2}{p}\right) = -1.$$

To determine the sign of  $y$  we recall a lemma of our previous paper [5] which states that  $(0, s)$  is odd or even according as 2 belongs to class  $s$  or not. Hence in our case  $(0, 0)$  is even, while  $(0, 1)$  is odd. These numbers have been given by Gauss as follows,

$$(21) \quad 16(0, 0)_4 = p + 2x - 7, \quad 16(0, 1)_4 = p + 2x + 8y + 1.$$

Hence

$$p + 2x - 7 \equiv 0 \pmod{32} \quad \text{and} \quad p + 2x + 8y + 1 \equiv 16 \pmod{32}.$$

Subtracting the first congruence from the second we have, dividing by 8,

$$(22) \quad y \equiv 1 \pmod{4}.$$

This makes (20) unambiguous, and returning to (2) we find by (6), since  $\psi_2(2) = 0$ , that for  $(2/p) = -1$

$$(23) \quad \psi_4(2) = \phi_2(2) = -4y, \quad y \equiv 1 \pmod{4}.$$

Hence by (7)

$$(24) \quad \phi_2(2m^2) = -4y \left(\frac{m}{p}\right), \quad \left(\frac{2}{p}\right) = -1.$$

This gives a slight strengthening of Jacobsthal's theorem, namely:

**THEOREM 2.** *If 2 is a nonresidue of  $p = x^2 + 4y^2$ , where  $x \equiv y \equiv 1 \pmod{4}$ , then*

$$\phi_2(D) = \begin{cases} -2x \left(\frac{m}{p}\right), & \text{if } D \equiv m^2 \pmod{p} \\ -4y \left(\frac{m}{p}\right), & \text{if } D \equiv 2m^2 \pmod{p}. \end{cases}$$

Hence by (2) we have:

**THEOREM 3.** *If 2 is a nonresidue of  $p = x^2 + 4y^2$ ,  $x \equiv y \equiv 1 \pmod{4}$  then the number of solutions of  $u^4 + D \equiv w^2 \pmod{p}$  is given by*

$$N_4(D) = \begin{cases} p - 1 - 2x \left(\frac{m}{p}\right), & \text{if } D \equiv m^2 \pmod{p} \\ p - 1 - 4y \left(\frac{m}{p}\right), & \text{if } D \equiv 2m^2 \pmod{p}. \end{cases}$$

We now suppose that 2 is a quadratic residue but a quartic nonresidue, hence we may choose  $g$  such that  $\sqrt{2}$  belongs to class 1 and calculate  $N(\sqrt{2})$  by (18). The cyclotomic constants of order 4 for  $p = 8n + 1$  are

$$(25) \quad 16(3, 1)_4 = p - 2x + 1, \quad 16(3, 3)_4 = p + 2x + 8y - 3.$$

Hence by (18)

$$(26) \quad N_4(\sqrt{2}) = p - 1 + 4y;$$

but in this case  $y$  turns out to be even, so that it is not sufficient to determine  $y$  modulo 4 and it is necessary to introduce the cyclotomic numbers of order 8 to determine the sign of  $y$ . It also becomes necessary to distinguish the cases  $p = 16n + 1$  and  $16n + 9$ .

$$\text{Case 1. } p = 16n + 1 = x^2 + 4y^2 = a^2 + 2b^2, \quad x \equiv a \equiv 1 \pmod{4}.$$

Since  $\sqrt{2}$  belongs to class 1, 2 belongs to class 2 and by our lemma  $(0, 0)_8$  is even, while  $(0, 2)_8$  is odd. Dickson [2] gives

$$(27) \quad 64(0, 0)_8 = p - 23 + 6x.$$

Since  $(0, 0)_8$  is even, we have

$$(28) \quad 6x \equiv -p + 23 \pmod{128}.$$

In order to complete our discussion it was necessary to calculate  $(0, 2)_8$  and  $(1, 2)_8$  by solving 15 linear equations involving the constants  $(i, j)_8$  given by Dickson, which we list in the Appendix. We obtained

$$(29) \quad 64(0, 2)_8 = p - 7 - 2x - 16y - 8a, \quad 64(1, 2)_8 = p + 1 - 6x + 4a.$$

Substituting  $p - 23$  for  $-6x$  from (28) into  $64(1, 2)_8$  we obtain

$$(30) \quad 2a \equiv 11 - p \pmod{32}.$$

Since  $(0, 2)_8$  is odd we have, multiplying (29) by 3,

$$(31) \quad \begin{aligned} 3p - 21 - 6x - 48y - 24a &\equiv 3p - 21 + (p - 23) - 48y - 12(11 - p) \\ &\equiv 64 \pmod{128}; \end{aligned}$$

or, dividing out a 16 and solving for  $y$ , we get

$$(32) \quad y \equiv 3(p + 1) \equiv -2 \pmod{8}.$$

Case 2.  $p = 16n + 9$ . In this case Dickson gives

$$(33) \quad 64(0, 4)_8 = p + 1 + 6x + 24a,$$

while we have calculated [ see Appendix ]

$$(34) \quad 64(0, 2)_8 = p + 1 - 2x + 16y ,$$

$$(35) \quad 64(2, 0)_8 = p - 7 + 6x ,$$

$$(36) \quad 64(1, 2)_8 = p + 1 + 2x - 4a .$$

From (35)

$$(37) \quad 6x \equiv 7 - p \pmod{64} .$$

Substituting this into (36) we find

$$(38) \quad 12a \equiv 2p + 10 \pmod{64} .$$

Since  $(0, 4)_8$  is even we obtain, using (38),

$$(39) \quad p + 1 + 6x + 24a \equiv p + 1 + 6x + 4p + 20 \equiv 0 \pmod{128} .$$

This gives an improvement of (37), namely,

$$(40) \quad 6x \equiv -(5p + 21) \pmod{128} .$$

Finally substituting all this into  $(0, 2)_8$  which is odd, we have, after multiplying (34) by 3,

$$3p + 3 - 6x + 48y \equiv 3p + 3 + 5p + 21 + 48y \equiv 8p + 24 + 48y \equiv 64 \pmod{128} ,$$

or dividing out an 8 and noting that  $p \equiv 9 \pmod{16}$  we obtain

$$y \equiv + 2 \pmod{8} .$$

Hence the sign of  $y$  in (26) is now determined as follows if  $(\sqrt{2}/p) = -1$ :

$$(41) \quad N_4(\sqrt{2}) = p - 1 + 4y, \text{ where } y/2 \equiv -(-1)^{(p-1)/8} \pmod{4} .$$

From this we have as before by (2) and (6) for  $(\sqrt{2}/p) = -1$ :

$$(42) \quad \psi_4(\sqrt{2}) = \phi_2(\sqrt{2}) = -4y, \text{ where } y/2 \equiv (-1)^{(p-1)/8} \pmod{4} ,$$

and we can write a slight improvement of Jacobsthal's theorem in the case in which 2 is a quadratic but not a quartic residue of  $p$ :



THEOREM 4. *If 2 is a quadratic residue, but a quartic nonresidue of  $p = x^2 + 4y^2 = 8n + 1$ , then*

$$\varphi_2(D) = \begin{cases} -2x\left(\frac{m}{p}\right) & \text{if } D \equiv m^2 \pmod{p} \\ -4y\left(\frac{m}{p}\right) & \text{if } D \equiv \sqrt{2}m^2 \pmod{p}, \end{cases}$$

where  $x \equiv 1 \pmod{4}$  and  $y/2 \equiv (-1)^n \pmod{4}$ .

THEOREM 5. *If 2 is a quadratic residue, but a quartic nonresidue of  $p = x^2 + 4y^2 = 8n + 1$ , then the number of solutions  $(u, w)$  of  $u^4 + D \equiv w^2 \pmod{p}$  is given by*

$$N_4(D) = \begin{cases} p - 1 - 2x\left(\frac{m}{p}\right) & \text{if } D \equiv m^2 \pmod{p} \\ p - 1 - 4y\left(\frac{m}{p}\right) & \text{if } D \equiv \sqrt{2}m^2 \pmod{p}, \end{cases}$$

where  $x \equiv 1 \pmod{4}$  and  $y/2 \equiv (-1)^n \pmod{4}$ .

In order to obtain an improvement on Jacobsthal's theorem in the case in which 2 is a quartic residue, or to improve the results for  $\phi_4$  and  $\psi_4$  in order to obtain  $N_8$ , it appears necessary to examine the cyclotomic constants of order 16, or to go through a determination of a specified primitive root as in Vandiver [7a]. The known results for  $\phi_4$  and  $\psi_4$  are as follows:

$$\phi_4(D) = \begin{cases} -4a\left(\frac{m}{p}\right) & \text{if } D \equiv m^4 \pmod{p} \\ 0 & \text{if } D \equiv m^2 \not\equiv m_1^4 \pmod{p} \\ \pm 4b & \text{otherwise,} \end{cases}$$

and

$$\psi_4(D) = \begin{cases} -2x\left(\frac{m}{p}\right) - 2 & \text{if } D \equiv m^2 \pmod{p} \\ \pm 4y & \text{otherwise.} \end{cases}$$

It follows from this that

$$(43) \quad N_8(D) = \begin{cases} p - 1 - 2x - 4a \left(\frac{m}{p}\right) & \text{if } D \equiv m^4 \pmod{p} \\ p - 1 + 2x \left(\frac{m}{p}\right) & \text{if } D \equiv m^2 \not\equiv m_1^4 \pmod{p} \\ p - 1 \pm 4b \pm 4y & \text{otherwise.} \end{cases}$$

**3. Case  $k = 3$ .** The known results for the case  $k = 3$  can be stated as follows:

$$(44) \quad \phi_3(D) = \begin{cases} -2A - 1 & \text{if } D \text{ is a cubic residue} \\ A \pm 3B - 1 & \text{if } D \text{ is a cubic nonresidue,} \end{cases}$$

where  $p = A^2 + 3B^2 = 6n + 1$ ,  $A \equiv 1 \pmod{3}$ .

This can be obtained either by summing the appropriate cyclotomic constants of order 6, or by using the results of Schrutka or Chowla, as was done in Whiteman [8]. From this it follows by (2) and (5) that

$$(45) \quad N_3(D) = \begin{cases} p - \left(\frac{D}{p}\right) 2A & \text{if } D \text{ is a cubic residue} \\ p + \left(\frac{D}{p}\right) (A \pm 3B) & \text{if } D \text{ is a cubic nonresidue.} \end{cases}$$

We are again faced with an ambiguity in sign in case  $D$  is a cubic nonresidue, which can be resolved in case 2 is a cubic nonresidue. For in this case by (9)

$$(46) \quad \phi_3(1) + \phi_3(2) + \phi_3(4) = -3.$$

By (44),  $\phi_3(1) = -2A - 1$ , while Chowla proved that  $\phi_3(4) = L - 1$ , where  $4p = L^2 + 27M^2$ ,  $L \equiv 1 \pmod{3}$ . Hence by (46)

$$(47) \quad \phi_3(2) = 2A - L - 1 \quad (2 \text{ a cubic nonresidue}).$$

Hence by (7) we can write a slight generalization of Chowla's or Schrutka's theorem:

**THEOREM 6.** *If 2 is a cubic nonresidue of  $p = A^2 + 3B^2$ , and if  $4p = L^2 + 27M^2$ ,  $A \equiv L \equiv 1 \pmod{3}$ , then*

$$\phi_3(D) = \begin{cases} -(2A + 1) & \text{if } D \equiv m^3 \pmod{p} \\ 2A - L - 1 & \text{if } D \equiv 2m^3 \pmod{p} \\ L - 1 & \text{if } D \equiv 4m^3 \pmod{p}. \end{cases}$$

Using (5) and (2) we obtain the corresponding theorem for  $N_3(D)$ :

**THEOREM 7.** *If 2 is a cubic nonresidue of  $p = A^2 + 3B^2$ , and if  $4p = L^2 + 27M^2$ ,  $A \equiv L \equiv 1 \pmod{3}$ , then*

$$N_3(D) = \begin{cases} p - \left(\frac{D}{p}\right) 2A & \text{if } D \equiv m^3 \pmod{p} \\ p + \left(\frac{D}{p}\right) L & \text{if } D \equiv 2m^3 \pmod{p} \\ p + \left(\frac{D}{p}\right) (2A - L) & \text{if } D \equiv 4m^3 \pmod{p}. \end{cases}$$

For  $k = 6$ , it follows from (10) by substituting the values for  $\phi_3(D)$  from (44) (remembering that  $D$  and  $\bar{D}$  are either both cubic residues, or both non-residues), that:

$$(48) \quad \psi_6(D) = \begin{cases} -(2A + 1) \left[ 1 + \left(\frac{D}{p}\right) \right] & \text{if } D \text{ is a cubic residue} \\ (A - 1) \left[ 1 + \left(\frac{D}{p}\right) \right] \pm 3B \left[ 1 - \left(\frac{D}{p}\right) \right] & \text{otherwise.} \end{cases}$$

Substituting this into (2) we have

$$(49) \quad N_6(D) = \begin{cases} p - 2A \left[ 1 + \left(\frac{D}{p}\right) \right] - 1 & \text{if } D \text{ is a cubic residue} \\ p + A \left[ 1 + \left(\frac{D}{p}\right) \right] \pm 3B \left[ 1 - \left(\frac{D}{p}\right) \right] - 1 & \text{otherwise.} \end{cases}$$

In case 2 is a cubic nonresidue, however, we can substitute more exact values for  $\phi_3(D)$  from Theorem 6 into (10) to obtain:

**THEOREM 7.** *If 2 is a cubic nonresidue of  $p = A^2 + 3B^2$  and if  $4p = L^2 + 27M^2$ ,  $A \equiv L \equiv 1 \pmod{3}$ , then*

$$\psi_6(D) = \begin{cases} -(2A + 1) \left[ 1 + \left(\frac{D}{p}\right) \right] & \text{if } D \equiv m^3 \pmod{p} \\ 2A + L \left[ \left(\frac{D}{p}\right) - 1 \right] - \left[ 1 + \left(\frac{D}{p}\right) \right] & \text{if } D \equiv 2m^3 \pmod{p} \\ \left(\frac{D}{p}\right) 2A - L \left[ \left(\frac{D}{p}\right) - 1 \right] - \left[ 1 + \left(\frac{D}{p}\right) \right] & \text{if } D \equiv 4m^3 \pmod{p}. \end{cases}$$

Substituting these values into (2) we obtain:

**THEOREM 8.** *If 2 is a cubic nonresidue of  $p = A^2 + 3B^2$  and if  $4p = L^2 + 27M^2$ ,  $A \equiv L \equiv 1 \pmod{3}$ , then the number of solutions of  $u^6 + D \equiv v^2 \pmod{p}$  is given by*

$$N_6(D) = \begin{cases} p - 1 - 2A \left[ 1 + \left(\frac{D}{p}\right) \right] & \text{if } D \equiv m^3 \pmod{p} \\ p - 1 + 2A + L \left[ \left(\frac{D}{p}\right) - 1 \right] & \text{if } D \equiv 2m^3 \pmod{p} \\ p - 1 + \left(\frac{D}{p}\right) 2A - L \left[ \left(\frac{D}{p}\right) - 1 \right] & \text{if } D \equiv 4m^3 \pmod{p}. \end{cases}$$

**4. Congruences in three variables.** In conclusion we can apply our results to the number of solutions of congruences in three variables. We have:

**THEOREM 9.** *The number  $N_{k,k}(D)$  of solutions  $(u, v, w)$  of*

$$(50) \quad u^k + Dv^k \equiv w^2 \pmod{p}$$

is

$$N_{k,k}(D) = \begin{cases} p^2 & \text{if } k \text{ is odd} \\ p^2 + (p - 1) \left[ 1 + \left(\frac{D}{p}\right) + \psi_k(D) \right] & \text{if } k \text{ is even.} \end{cases}$$

*Proof.* Replacing  $D$  by  $Dv^k$  in (2) and summing over  $v = 1, 2, \dots, p - 1$ , we obtain

$$\sum_{v=1}^{p-1} N_k(Dv^k) = p(p - 1) + \left(\frac{D}{p}\right) \sum_{v=1}^{p-1} \left(\frac{v}{p}\right)^k + \sum_{v=1}^{p-1} \psi_k(v^k D).$$

By (7) this becomes

$$\sum_{\nu=1}^{p-1} N_k(D\nu^k) = p(p-1) + \left(\frac{D}{p}\right) \sum_{\nu=1}^{p-1} \left(\frac{\nu}{p}\right)^k + \psi_k(D) \sum_{\nu=1}^{p-1} \left(\frac{\nu}{p}\right)^k.$$

But

$$\sum_{\nu=1}^{p-1} \left(\frac{\nu}{p}\right)^k = \begin{cases} 0 & k \text{ odd} \\ p-1 & k \text{ even,} \end{cases}$$

while the number of solutions with  $\nu = 0$  is  $p$  for  $k$  odd and  $2p-1$  for  $k$  even. Hence

$$N_{k,k}(D) = \begin{cases} p(p-1) + p = p^2 & \text{for } k \text{ odd} \\ p(p-1) + (p-1) \left[ \left(\frac{D}{p}\right) + \psi_k(D) \right] + 2p-1, & k \text{ even.} \end{cases}$$

Hence the theorem.

Using the expressions derived for special values of  $k$  earlier we can write down the following special cases:

$$N_{2,2}(D) = p^2.$$

By (14),

$$N_{4,4}(D) = p^2 - 2x \left(\frac{\sqrt{D}}{p}\right) (p-1) \quad \text{if } \left(\frac{D}{p}\right) = +1, \quad x \equiv 1 \pmod{4}.$$

By (24),

$$N_{4,4}(2m^2) = p^2 - 4y(p-1) \quad \text{if } \left(\frac{2}{p}\right) = -1 \text{ and } y \equiv 1 \pmod{4}.$$

By (42),

$$N_{4,4}(\sqrt{2}m^2) = p^2 - 4y(p-1) \quad \text{if } \frac{\sqrt{2}}{p} = -1 \text{ and } y/2 \equiv (-1)^{(p-1)/8} \pmod{4}.$$

By (48),

$$N_{6,6}(m^3) = p^2 - 2A \left[ 1 + \left( \frac{m}{p} \right) \right] (p-1).$$

By Theorem 7,

$$\left. \begin{aligned} N_{6,6}(2m^3) &= p^2 + \left\{ 2A + L \left[ \left( \frac{m}{p} \right) - 1 \right] \right\} (p-1) \\ N_{6,6}(4m^3) &= p^2 + \left\{ \left( \frac{m}{p} \right) 2A - L \left[ \left( \frac{m}{p} \right) - 1 \right] \right\} (p-1) \end{aligned} \right\} \text{if } 2 \text{ is a cubic nonresidue.}$$

By (43),

$$N_{8,8}(m^4) = p^2 - \left[ 2x + 4a \left( \frac{m}{p} \right) \right] (p-1).$$

We note that  $N_{6,6}(m^3) = p^2$  if  $m$  is a nonresidue. It can be readily seen that this is a special case of a general theorem, namely:

**THEOREM 10.** *If  $k$  is oddly even and  $D$  is a  $k/2$ th power residue, but not a  $k$ th power residue, then*

$$N_{k,k}(D) = p^2.$$

This follows from Theorem 9 and the fact that the corresponding  $\psi_k(D)$  is zero in this case by (11).

We hope to take up the cases  $k = 5$  and  $k = 10$  in a future paper.

**APPENDIX: Cyclotomic constants of order 8.**

The 64 constants  $(i, j)_8$  have at most 15 different values for a given  $p$ . These values are expressible in terms of  $p, x, y, a$  and  $b$  in

$$p = x^2 + 4y^2 = a^2 + 2b^2, \quad (x \equiv a \equiv 1 \pmod{4}).$$

There are two cases.

*Case I.*  $p = 16n + 1$ .

Table of  $(i, j)_8$ 

$j \backslash i$	0	1	2	3	4	5	6	7
0	(0, 0)	(0, 1)	(0, 2)	(0, 3)	(0, 4)	(0, 5)	(0, 6)	(0, 7)
1	(0, 1)	(0, 7)	(1, 2)	(1, 3)	(1, 4)	(1, 5)	(1, 6)	(1, 2)
2	(0, 2)	(1, 2)	(0, 6)	(1, 6)	(2, 4)	(2, 5)	(2, 4)	(1, 3)
3	(0, 3)	(1, 3)	(1, 6)	(0, 5)	(1, 5)	(2, 5)	(2, 5)	(1, 4)
4	(0, 4)	(1, 4)	(2, 4)	(1, 5)	(0, 4)	(1, 4)	(2, 4)	(1, 5)
5	(0, 5)	(1, 5)	(2, 5)	(2, 5)	(1, 4)	(0, 3)	(1, 3)	(1, 6)
6	(0, 6)	(1, 6)	(2, 4)	(2, 5)	(2, 4)	(1, 3)	(0, 2)	(1, 2)
7	(0, 7)	(1, 2)	(1, 3)	(1, 4)	(1, 5)	(1, 6)	(1, 2)	(0, 1)

These 15 fundamental constants  $(0, 0), \dots, (2, 5)$  are given by the relations contained in the following table.

	If 2 is a quartic residue	If 2 is not a quartic residue
$64(0, 0)$	$p - 23 - 18x - 24a$	$p - 23 + 6x$
$64(0, 1)$	$p - 7 + 2x + 4a + 16y + 16b$	$p - 7 + 2x + 4a$
$64(0, 2)$	$p - 7 + 6x + 16y$	$p - 7 - 2x - 8a - 16y$
$64(0, 3)$	$p - 7 + 2x + 4a - 16y + 16b$	$p - 7 + 2x + 4a$
$64(0, 4)$	$p - 7 - 2x + 8a$	$p - 7 - 10x$
$64(0, 5)$	$p - 7 + 2x + 4a + 16y - 16b$	$p - 7 + 2x + 4a$
$64(0, 6)$	$p - 7 + 6x - 16y$	$p - 7 - 2x - 8a + 16y$
$64(0, 7)$	$p - 7 + 2x + 4a - 16y - 16b$	$p - 7 + 2x + 4a$
$64(1, 2)$	$p + 1 + 2x - 4a$	$p + 1 - 6x + 4a$
$64(1, 3)$	$p + 1 - 6x + 4a$	$p + 1 + 2x - 4a - 16b$
$64(1, 4)$	$p + 1 + 2x - 4a$	$p + 1 + 2x - 4a + 16y$
$64(1, 5)$	$p + 1 + 2x - 4a$	$p + 1 + 2x - 4a - 16y$
$64(1, 6)$	$p + 1 - 6x + 4a$	$p + 1 + 2x - 4a + 16b$
$64(2, 4)$	$p + 1 - 2x$	$p + 1 + 6x + 8a$
$64(2, 5)$	$p + 1 + 2x - 4a$	$p + 1 - 6x + 4a$

Case II.  $p = 16n + 9$ .

Table of  $(i, j)_8$

$j \backslash i$	0	1	2	3	4	5	6	7
0	(0, 0)	(0, 1)	(0, 2)	(0, 3)	(0, 4)	(0, 5)	(0, 6)	(0, 7)
1	(1, 0)	(1, 1)	(1, 2)	(1, 3)	(0, 5)	(1, 3)	(0, 3)	(1, 7)
2	(2, 0)	(2, 1)	(2, 0)	(1, 7)	(0, 6)	(1, 3)	(0, 2)	(1, 2)
3	(1, 1)	(2, 1)	(2, 1)	(1, 0)	(0, 7)	(1, 7)	(1, 2)	(0, 1)
4	(0, 0)	(1, 0)	(2, 0)	(1, 1)	(0, 0)	(1, 0)	(2, 0)	(1, 1)
5	(1, 0)	(0, 7)	(1, 7)	(1, 2)	(0, 1)	(1, 1)	(2, 1)	(2, 1)
6	(2, 0)	(1, 7)	(0, 6)	(1, 3)	(0, 2)	(1, 2)	(2, 0)	(2, 1)
7	(1, 1)	(1, 2)	(1, 3)	(0, 5)	(0, 3)	(1, 6)	(1, 3)	(1, 0)

where

If 2 is a quartic residue

If 2 is not a quartic residue

64(0, 0)	$p - 15 - 2x$	$p - 15 - 10x - 8a$
64(0, 1)	$p + 1 + 2x - 4a + 16y$	$p + 1 + 2x - 4a - 16b$
64(0, 2)	$p + 1 + 6x + 8a - 16y$	$p + 1 - 2x + 16y$
64(0, 3)	$p + 1 + 2x - 4a - 16y$	$p + 1 + 2x - 4a - 16b$
64(0, 4)	$p + 1 - 18x$	$p + 1 + 6x + 24a$
64(0, 5)	$p + 1 + 2x - 4a + 16y$	$p + 1 + 2x - 4a + 16b$
64(0, 6)	$p + 1 + 6x + 8a + 16y$	$p + 1 - 2x - 16y$
64(0, 7)	$p + 1 + 2x - 4a - 16y$	$p + 1 + 2x - 4a + 16b$
64(1, 0)	$p - 7 + 2x + 4a$	$p - 7 + 2x + 4a + 16y$
64(1, 1)	$p - 7 + 2x + 4a$	$p - 7 + 2x + 4a - 16y$
64(1, 2)	$p + 1 - 6x + 4a + 16b$	$p + 1 + 2x - 4a$
64(1, 3)	$p + 1 + 2x - 4a$	$p + 1 - 6x + 4a$
64(1, 7)	$p + 1 - 6x + 4a - 16b$	$p + 1 + 2x - 4a$
64(2, 0)	$p - 7 - 2x - 8a$	$p - 7 + 6x$
64(2, 1)	$p + 1 + 2x - 4a$	$p + 1 - 6x + 4a$



## REFERENCES

1. S. Chowla, *The last entry in Gauss' diary*, Proc. Nat. Acad. Sci. U.S.A. **35** (1949), 244-246.
2. L. E. Dickson, *Cyclotomy, higher congruences and Waring's problem*, Amer. J. Math. **57** (1935), 391-424.
3. C. F. Gauss, *Theoria residuorum biquadraticorum*, Werke, **2**, 90.
4. E. Jacobsthal, *Anwendungen einer Formel aus der Theorie der quadratischen Reste*, Dissertation (Berlin 1906).
5. Emma Lehmer, *On residue difference sets*, Canadian J. Math. **5** (1953), 425-432.
6. L. von Schrutka, *Eine Beweis für die Zerlegbarkeit der Primzahlen von der Form  $6n + 1$  in ein einfaches und ein dreifaches Quadrat*, Jn. für die reine und angew. Math. **140** (1911), 252-265.
7. H. S. Vandiver, *On the number of solutions of some general types of equations in a finite field*, Proc. Nat. Acad. Sci. U.S.A. **32** (1946), 47-52.
- 7a. ———, *On the number of solutions of certain nonhomogeneous trinomial equations in a finite field*, Proc. Nat. Acad. Sci. U.S.A. **31** (1945), 170-175.
8. A. L. Whiteman, *Cyclotomy and Jacobsthal's sums*, Amer. J. Math., **64** (1952), 89-99, and *Theorems analogous to Jacobsthal's theorem*, Duke Math. J. **16** (1949), 619-626.

BERKELEY, CALIFORNIA



# Pacific Journal of Mathematics

Vol. 5, No. 1

September, 1955

Frank Herbert Brownell, III, <i>Flows and noncommuting projections on Hilbert space</i> .....	1
H. E. Chrestenson, <i>A class of generalized Walsh functions</i> .....	17
Jean Bronfenbrenner Crockett and Herman Chernoff, <i>Gradient methods of maximization</i> .....	33
Nathan Jacob Fine, <i>On groups of orthonormal functions. I</i> .....	51
Nathan Jacob Fine, <i>On groups of orthonormal functions. II</i> .....	61
Frederick William Gehring, <i>A note on a paper by L. C. Young</i> .....	67
Joachim Lambek and Leo Moser, <i>On the distribution of Pythagorean triangles</i> .....	73
Roy Edwin Wild, <i>On the number of primitive Pythagorean triangles with area less than <math>n</math></i> .....	85
R. Sherman Lehman, <i>Approximation of improper integrals by sums over multiples of irrational numbers</i> .....	93
Emma Lehmer, <i>On the number of solutions of <math>u^k + D \equiv w^2 \pmod{p}</math></i> .....	103
Robert Delmer Stalley, <i>A modified Schnirelmann density</i> .....	119
Richard Allan Moore, <i>The behavior of solutions of a linear differential equation of second order</i> .....	125
William M. Whyburn, <i>A nonlinear boundary value problem for second order differential systems</i> .....	147