

## An application of a formula of Western to the evaluation of certain Jacobsthal sums

by

R. H. HUDSON (Columbia, S. C.) and K. S. WILLIAMS\* (Ottawa, Ontario)

**1. Introduction and summary.** Let  $k \geq 2$  be a positive integer and let  $p$  be a prime such that  $p \equiv 1 \pmod{2k}$ . The Jacobsthal sum  $\Phi_k(D)$  is defined by

$$(1.1) \quad \Phi_k(D) = \sum_{x=1}^{p-1} \left( \frac{x(x^k + D)}{p} \right),$$

where  $D$  is an integer not divisible by  $p$  and  $\left(\frac{\cdot}{p}\right)$  is the Legendre symbol. When  $k = 2$ , Jacobsthal ([5], pp. 240-241) evaluated  $\Phi_2(D)$  when  $D$  is a quadratic residue (mod  $p$ ) but left a sign ambiguity in its evaluation when  $D$  is a quadratic non-residue (mod  $p$ ). Recently, the authors [3] have shown how to remove this ambiguity by using the law of quartic reciprocity in a form given by Gosset [2]. When  $k = 3$ , von Schrutka ([9], p. 258) evaluated  $\Phi_3(D)$  when  $D$  is a cubic residue (mod  $p$ ) but left an ambiguity in its evaluation when  $D$  is a cubic non-residue (mod  $p$ ), and the authors [3] have shown how to remove this ambiguity by using a form of the law of cubic reciprocity given by Emma Lehmer [6].

When  $k = 4$ , Whiteman [12], [13] has shown that

$$(1.2) \quad \Phi_4(D) = \begin{cases} -4(-1)^{(p-1)/8}c, & \text{if } D \text{ is an octic residue (mod } p), \\ +4(-1)^{(p-1)/8}c, & \text{if } D \text{ is a quartic but not} \\ & \text{an octic residue (mod } p), \\ 0, & \text{if } D \text{ is a quadratic but not} \\ & \text{a quartic residue (mod } p), \\ \pm 4d, & \text{if } D \text{ is a quadratic non-residue} \\ & \text{(mod } p), \end{cases}$$

where  $p = c^2 + 2d^2 \equiv 1 \pmod{8}$ ,  $c \equiv 1 \pmod{4}$ .

\* Research supported by Natural Sciences and Engineering Research Council Canada grant A-7233.

Since 2 is a quadratic residue of a prime  $p \equiv 1 \pmod{8}$ ,  $\Phi_4(2)$  is known from (1.2). In Section 4 of this paper we show how to remove the sign ambiguity in the evaluation of  $\Phi_4(q)$ , where  $q$  is an odd prime which is a quadratic non-residue  $\pmod{p}$ , by means of a form of the law of octic reciprocity given by Western [11] (see Section 2). For example, we prove the following:

**THEOREM 2 (b).** *Let  $p = a^2 + b^2 = c^2 + 2d^2$  ( $a \equiv c \equiv 1 \pmod{4}$ ) be a prime  $\equiv 1 \pmod{8}$  such that 5 is a quadratic non-residue  $\pmod{p}$ . Then*

$$\Phi_4(5) = -4(-1)^{(p-1)/8}d,$$

where  $b$  and  $d$  are chosen to satisfy one of  $a \equiv b \equiv d \pmod{5}$  or  $a \equiv b \equiv -2d \pmod{5}$ .

In order to evaluate  $\Phi_4(q)$  by this method, it is necessary to determine  $q^{(p-1)/8} \pmod{p}$  when  $q$  is a quadratic non-residue  $\pmod{p}$ , i.e. when  $q^{(p-1)/8}$  is a primitive eighth root of unity  $\pmod{p}$ . In Section 3 we explicitly evaluate  $q^{(p-1)/8} \pmod{p}$  for  $q = 3, 5, 7, 11, 13, 17$  and  $19$  when  $\left(\frac{q}{p}\right) = -1$ ,  $p \equiv 1 \pmod{8}$ , in terms of the representations  $p = a^2 + b^2 = c^2 + 2d^2$ , by giving necessary and sufficient criteria in terms of  $a, b, c$  and  $d$ , for  $q$  to satisfy

$$(1.3) \quad q^{(p-1)/8} \equiv ((a-b)d/ac)^j \pmod{p},$$

$j = 1, 3, 5, 7$ . We state our results only for  $j = 1$  as the analogous results for  $j = 3, 5$  and  $7$  may be obtained from these by self-evident transformations. Illustrative of the results in this section is the following

**THEOREM 1 (d).** *Let  $p = a^2 + b^2 = c^2 + 2d^2 \equiv 1 \pmod{8}$  be a prime with  $a$  and  $c$  chosen so that  $a \equiv c \equiv 1 \pmod{4}$ , and let  $k = 1, 5$ , or  $-3$  according as  $c \equiv 0, \pm 2d$ , or  $\pm 4d \pmod{11}$ . Then*

$$(1.4) \quad (-11)^{(p-1)/8} \equiv (a-b)d/ac \pmod{p} \Leftrightarrow \begin{cases} a \equiv b \equiv -kd \pmod{11}, \\ a \equiv 3b \equiv -2kd \pmod{11}, \\ a \equiv 4b \equiv 3kd \pmod{11}. \end{cases}$$

The results in Section 3 complement those of von Lienen [8] who gave necessary and sufficient criteria for each prime  $q \leq 41$  to be an octic residue  $\pmod{p}$ , given that  $q$  is a quartic residue  $\pmod{p}$ . This leaves the problem of evaluating  $q^{(p-1)/8} \pmod{p}$  when  $q$  is a quadratic but not a quartic residue  $\pmod{p}$ , in other words, when  $q^{(p-1)/8} \equiv \pm b/a \pmod{p}$ . In Section 5 we give necessary and sufficient criteria for each prime  $q \leq 19$  to satisfy  $q^{(p-1)/8} \equiv +b/a \pmod{p}$ .

Illustrative of these results is the following:

**THEOREM 3 (d).** *Let  $p = a^2 + b^2 = c^2 + 2d^2 \equiv 1 \pmod{8}$  be a prime  $\equiv 1 \pmod{8}$  with  $a$  and  $c$  chosen so that  $a \equiv c \equiv 1 \pmod{4}$ , and let  $k = 1$ ,*

5, or  $-3$  according as  $d \equiv 0$ ,  $c \equiv \pm d$ , or  $c \equiv \pm 5d \pmod{11}$ . Then

$$(1.5) \quad (-11)^{(p-1)/8} \equiv b/a \pmod{p} \Leftrightarrow \begin{cases} b \equiv -kc \pmod{11}, \\ b \equiv -5kc \pmod{11}. \end{cases}$$

The fact that the values of  $k$  in Theorem 3 (d) coincide with those in Theorem 1 (d) in magnitude, sign, and order is fascinating—it is not a coincidence. In Section 6 we include a proof that this phenomenon, apart from a possible ambiguity in the sign of the  $k$ 's, occurs for all primes  $q > 3$  which are  $\equiv \pm 3 \pmod{8}$ .

**2. Western's formulae.** Let  $p \equiv 1 \pmod{8}$  be a prime. Set  $\zeta = e^{2\pi i/8} = (1+i)/\sqrt{2}$  and let  $R$  denote the ring of integers of the quartic field  $Q(\zeta)$ . The elements of  $R$  are of the form  $a_0 + a_1\zeta + a_2\zeta^2 + a_3\zeta^3$ , where  $a_0, a_1, a_2, a_3$  are rational integers; moreover,  $R$  is a unique factorization domain. In  $R$ ,  $p$  factors as a product of four primes

$$(2.1) \quad p = \pi_1\pi_3\pi_5\pi_7,$$

where

$$(2.2) \quad \pi_i = \pi(\zeta^i) \quad (i = 1, 3, 5, 7), \quad \pi(\zeta) = a_0 + a_1\zeta + a_2\zeta^2 + a_3\zeta^3.$$

Replacing  $\pi(\zeta)$  by a suitable associate, we can suppose that

$$(2.3) \quad \pi = \pi_1 = \pi(\zeta) \equiv 1 \pmod{2}$$

(see, for example, [1], p. 69), so that

$$(2.4) \quad a_0 \equiv 1 \pmod{2}, \quad a_1 \equiv a_2 \equiv a_3 \equiv 0 \pmod{2}.$$

Next we note that

$$(2.5) \quad \pi\pi_5 = a + bi, \quad \pi\pi_3 = c + di\sqrt{2},$$

where

$$(2.6) \quad p = a^2 + b^2 = c^2 + 2d^2,$$

$$(2.7) \quad a = a_0^2 - a_2^2 + 2a_1a_3 \equiv 1 \pmod{4},$$

$$(2.8) \quad c = a_0^2 - a_1^2 + a_2^2 - a_3^2 \equiv 1 \pmod{4}.$$

For  $q$  an odd prime and  $j = 0, 1, \dots, 7$ , it follows from Western's formulae ([11], p. 248) and (2.5) that for  $q \equiv 1, 3, 5$ , and  $7 \pmod{8}$  respectively, we have

$$(2.9) \quad q^{(p-1)/8} \equiv ((a-b)d/ac)^j \pmod{p} \\ \text{if } p^{(q-1)/8}(a-bi)^{(q-1)/4}(c-di\sqrt{2})^{(q-1)/2} \equiv \zeta^j \pmod{q},$$

$$(2.10) \quad (-q)^{(p-1)/8} \equiv ((a-b)d/ac)^j \pmod{p} \\ \text{if } p^{(q-3)/8}(a+bi)^{(q+1)/4}(c-di\sqrt{2})^{(q-1)/2} \equiv \zeta^j \pmod{q},$$

$$(2.11) \quad q^{(p-1)/8} \equiv ((a-b)d/ac)^j \pmod{p}$$

$$\text{if } p^{(q-5)/8}(a-bi)^{(q-1)/4}(c+di\sqrt{2})^{(q+1)/2} \equiv \zeta^j \pmod{q},$$

$$(2.12) \quad (-q)^{(p-1)/8} \equiv ((a-b)d/ac)^j \pmod{p}$$

$$\text{if } p^{(q-7)/8}(a+bi)^{(q+1)/4}(c+di\sqrt{2})^{(q+1)/2} \equiv \zeta^j \pmod{q}.$$

**3. Evaluation of  $q^{(p-1)/8} \pmod{p}$  when  $\left(\frac{q}{p}\right) = -1$ .** Let  $p = a^2 + b^2 = c^2 + 2d^2 \equiv 1 \pmod{8}$  be a prime with  $a$  and  $c$  chosen so that  $a \equiv c \equiv 1 \pmod{4}$ . Let  $q$  be an odd prime such that  $\left(\frac{q}{p}\right) = -1$ . In this section we give necessary and sufficient conditions for  $q$  to satisfy

$$((-1)^{(q-1)/2}q)^{(p-1)/8} \equiv (a-b)d/ac \pmod{p}$$

for each prime  $q \leq 19$ . When  $q \equiv \pm 1 \pmod{8}$  these conditions involve congruences of the form  $a \equiv \lambda b \pmod{q}$  and  $c \equiv \mu d \pmod{q}$  (see Theorem 1 (c), (f)), and when  $q \equiv \pm 3 \pmod{8}$  they involve congruences of the form  $a \equiv \lambda b \equiv rd \pmod{q}$  (see Theorem 1 (a), (b), (d), (e), (g)).

We just give the details of the proof of Theorem 1 for part (g) as, apart from the differences mentioned above, the other parts are proved similarly.

**THEOREM 1.** Let  $p = a^2 + b^2 = c^2 + 2d^2 \equiv 1 \pmod{8}$  be a prime with  $a$  and  $c$  chosen so that  $a \equiv c \equiv 1 \pmod{4}$ . Then we have

$$(a) \quad (-3)^{(p-1)/8} \equiv (a-b)d/ac \pmod{p} \Leftrightarrow a \equiv -b \equiv d \pmod{3},$$

$$(b) \quad 5^{(p-1)/8} \equiv (a-b)d/ac \pmod{p} \Leftrightarrow \begin{cases} a \equiv b \equiv d \pmod{5}, \\ a \equiv b \equiv -2d \pmod{5}, \end{cases}$$

$$(c) \quad (-7)^{(p-1)/8} \equiv (a-b)d/ac \pmod{p}$$

$$\Leftrightarrow \begin{cases} a \equiv 2b \pmod{7} \text{ and } c \equiv kd \pmod{7}, \\ a \equiv 3b \pmod{7} \text{ and } c \equiv -kd \pmod{7}, \end{cases}$$

where  $k = 1, 5$ , or  $-3$  according as  $c \equiv 0, \pm 2d$ , or  $\pm 4d \pmod{11}$ ,

$$(e) \quad 13^{(p-1)/8} \equiv (a-b)d/ac \pmod{p} \Leftrightarrow \begin{cases} a \equiv -b \equiv -kd \pmod{13}, \\ a \equiv -2b \equiv 5kd \pmod{13}, \\ a \equiv 6b \equiv -4kd \pmod{13}, \end{cases}$$

where  $k = 1, 4, 5$ , or  $-3$  according as  $c \equiv 0, \pm 2d, \pm 3d$ , or  $\pm 4d \pmod{13}$ ,

$$(f) \quad 17^{(p-1)/8} \equiv (a-b)d/ac \pmod{p}$$

$$\Leftrightarrow \begin{cases} a \equiv -2b \pmod{17} \text{ and } c \equiv -kd \pmod{17}, \\ a \equiv 3b \pmod{17} \text{ and } c \equiv kd \pmod{17}, \\ a \equiv -6b \pmod{17} \text{ and } c \equiv kd \pmod{17}, \\ a \equiv -8b \pmod{17} \text{ and } c \equiv -kd \pmod{17}, \end{cases}$$

where  $k = 1, -2, 3, \text{ or } 5$  according as  $c \equiv \pm d, \pm 2d, \pm 3d, \text{ or } \pm 5d \pmod{17}$ ,

$$(g) \quad (-19)^{(p-1)/8} \equiv (a-b)d/ac \pmod{p} \Leftrightarrow \begin{cases} a \equiv -b \equiv -kd \pmod{19}, \\ a \equiv 3b \equiv -6kd \pmod{19}, \\ a \equiv -6b \equiv 2kd \pmod{19}, \\ a \equiv 7b \equiv 9kd \pmod{19}, \\ a \equiv -8b \equiv -4kd \pmod{19}, \end{cases}$$

where  $k = 1, 7, 3, -2, \text{ or } -4$  according as  $c \equiv 0, \pm d, \pm 4d, \pm 5d, \text{ or } \pm 7d \pmod{19}$ .

Proof of Theorem 1 (g). For brevity, all congruences will be assumed to be modulo 19 in the following proof unless otherwise stated.

It is straightforward to check that for each congruence on the right-hand side of (g), we have

$$p^2(a+bi)^5(c-di\sqrt{2})^9 \equiv 10(1+i)\sqrt{2} \equiv \zeta$$

and so, by (2.10), with  $q = 19$ , we have

$$(-19)^{(p-1)/8} \equiv (a-b)d/ac \pmod{p}.$$

For example, for  $a \equiv -b \equiv -d, c \equiv 0$ , we have, as  $b^{18} \equiv 1$ ,

$$\begin{aligned} p^2(a+bi)^5(c-di\sqrt{2})^9 &\equiv 4(-1+i)^5(-i\sqrt{2})^9 \\ &\equiv -4(4-4i)(16i\sqrt{2}) \equiv 10(1+i)\sqrt{2} \equiv \zeta. \end{aligned}$$

Conversely, suppose that

$$(3.1) \quad (-19)^{(p-1)/8} \equiv (a-b)d/ac \pmod{p}.$$

Then  $(-19)^{(p-1)/2} \equiv -1 \pmod{p}$ , and by the law of quadratic reciprocity, we have

$$(3.2) \quad \left(\frac{p}{19}\right) = -1.$$

It is clear from (3.2) and  $p = a^2 + b^2 = c^2 + 2d^2$  that  $b \not\equiv 0$  and  $d \not\equiv 0$ . Setting  $c \equiv \mu d$  in (3.2) we obtain

$$(3.3) \quad \left(\frac{\mu^2 + 2}{19}\right) = -1,$$

so that  $\mu \equiv 0, \pm 1, \pm 4, \pm 5, \pm 7$ .

Next, from (3.1), we have  $(-19)^{(p-1)/4} \equiv b/a \pmod{p}$ . Setting  $a \equiv \lambda b$ , and appealing to the law of quartic reciprocity (see for example [2]), we obtain

$$(3.4) \quad \left(\frac{a-bi}{a+bi}\right)^5 = \left(\frac{\lambda-i}{\lambda+i}\right)^5 \equiv i,$$

so that  $\lambda \equiv -1, 3, -6, 7, -8$ .

Next by the law of octic reciprocity, see (2.10), we have

$$(3.5) \quad p^2(a+bi)^5(c-di\sqrt{2})^9 \equiv \zeta.$$

Using the congruences  $a \equiv \lambda b$ ,  $c \equiv \mu d$ , and setting  $d \equiv \beta b$ , so that  $c \equiv \mu\beta b$ , in (3.5), we obtain

$$(3.6) \quad (\lambda^2+1)^2(\lambda+i)^5(\mu-i\sqrt{2})^9 \left(\frac{\beta}{19}\right) \equiv -9(1+i)\sqrt{2},$$

as  $b^{18} \equiv 1$ ,  $\beta^9 \equiv \left(\frac{\beta}{19}\right)$ . Next, as

$$(3.7) \quad (\lambda+i)^5 \equiv (\lambda^5+9\lambda^3+5\lambda) + (5\lambda^4+9\lambda^2+1)i$$

and

$$(3.8) \quad (\mu-i\sqrt{2})^9 \equiv (\mu^9+4\mu^7+10\mu^5+12\mu^3+11\mu) - (9\mu^8+3\mu^6+10\mu^4+16\mu^2+16)i\sqrt{2},$$

we obtain

$$(3.9) \quad (\lambda^2+1)^2(\lambda+i)^5 \equiv \begin{cases} -3+3i, & \text{if } \lambda \equiv -1, 3, -6, 7, \\ 3-3i, & \text{if } \lambda \equiv -8, \end{cases}$$

and

$$(3.10) \quad (\mu-i\sqrt{2})^9 \equiv \begin{cases} 3i\sqrt{2}, & \text{if } \mu \equiv 0, \pm 1, \pm 5, \\ -3i\sqrt{2}, & \text{if } \mu \equiv \pm 4, \pm 7. \end{cases}$$

Since

$$(-3+3i)(\pm 3i\sqrt{2}) = \mp 9(1+i)\sqrt{2}, \quad (3-3i)(\pm 3i\sqrt{2}) = \pm 9(1+i)\sqrt{2},$$

we must have from (3.6), (3.9), and (3.10), that

$$(3.11) \quad \left(\frac{\beta}{19}\right) = +1 \quad \text{if} \quad \begin{cases} \lambda \equiv -1, 3, -6, 7 \text{ and } \mu \equiv 0, \pm 1, \pm 5, \text{ or} \\ \lambda \equiv -8 \text{ and } \mu \equiv \pm 4, \pm 7, \end{cases}$$

and

$$(3.12) \quad \left(\frac{\beta}{19}\right) = -1 \quad \text{if} \quad \begin{cases} \lambda \equiv -1, 3, -6, 7 \text{ and } \mu \equiv \pm 4, \pm 7 \text{ or} \\ \lambda \equiv -8 \text{ and } \mu \equiv 0, \pm 1, \pm 5. \end{cases}$$

From  $a^2+b^2 = c^2+2d^2$  we obtain

$$(3.13) \quad \beta^2 \equiv \frac{\lambda^2+1}{\mu^2+2}.$$

Appealing to (3.11), (3.12), and (3.13) we have the following table of values of  $\beta$ :

(3.14)

$\lambda \backslash \mu$	-1	3	-6	7	-8
0	1	9	16	5	2
$\pm 1$	11	4	5	17	3
$\pm 4$	13	3	18	8	7
$\pm 5$	9	5	11	7	18
$\pm 7$	14	12	15	13	9

The  $r$ th row in this array is determined by multiplying the entries of the first row by the first entry in the  $r$ th row,  $r = 1, \dots, 5$  (and similarly for the  $r$ th column).

Finally set

(3.15)  $k \equiv 1, 7, 3, -2, \text{ or } -4$

according as  $\mu \equiv 0, \pm 1, \pm 4, \pm 5, \text{ or } \pm 7$  respectively. Then from (3.14) and (3.15) we have for all 25 values of  $\beta$ ,

(3.16)  $\frac{\lambda}{\beta k} \equiv -1, -6, 2, 9, \text{ or } -4$

according as  $\lambda \equiv -1, 3, -6, 7, \text{ or } -8$ .

This completes the proof of Theorem 1 (g).

Remark. Set  $a \equiv \lambda b \equiv \mu d$  if  $q \equiv \pm 3 \pmod{8}$  and set  $a \equiv \lambda b, c \equiv \mu d$ , if  $q \equiv \pm 1 \pmod{8}$ . If  $(a-b)d/ac$  on the left-hand side of Theorem 1 (a)-(g), is replaced by  $((a-b)d/ac)^j, j = 3, 5, \text{ or } 7$ , then the congruences on the right-hand side are satisfied if and only if  $\lambda$  is replaced by  $-\lambda$  if  $j = 3, \mu$  is replaced by  $-\mu$  if  $j = 5, \lambda$  is replaced by  $-\lambda$  and  $\mu$  is replaced by  $-\mu$  if  $j = 7$ .

EXAMPLE 1 ( $q = 5$ , see Theorem 1 (b)).

(i) Let  $p = 1297 = 1^2 + 36^2 = (-35)^2 + 2 \cdot 6^2$  so that  $a \equiv b \equiv d \pmod{5}$ . Then we have

$$\frac{(a-b)d}{ac} = \frac{(-35)(6)}{-35} \equiv 6 \pmod{1297},$$

and it is easily checked that for  $p = 1297$  we have

$$5^{(p-1)/8} = 5^{162} \equiv 6 \pmod{p}.$$

(ii) Let  $p = 137 = (-11)^2 + 4^2 = (-3)^2 + 2(8)^2$  so that  $a \equiv b \equiv -2d \pmod{5}$ . Then we have

$$\frac{(a-b)d}{ac} = \frac{(-15)(8)}{(-11)(-3)} \equiv \frac{-120}{33} \equiv 96 \pmod{137},$$

and it is easily checked that for  $p = 137$  we have

$$5^{(p-1)/8} = 5^{17} \equiv 96 \pmod{p}.$$

(iii) Let  $p = 17 = 1^2 + 4^2 = (-3)^2 + 2(2)^2$  so that the right-hand side of (b) is not satisfied, rather,  $a \equiv -b \equiv -2d \pmod{5}$ . Setting  $a \equiv \lambda b$  and noting that only the sign of  $\lambda$  differentiates  $a \equiv -b \equiv -2d$  from the congruence  $a \equiv b \equiv -2d$  in (b), we must have

$$5^{(p-1)/8} \equiv \frac{(a+b)d}{ac} \pmod{p},$$

and it is easily checked that this is, indeed, the case.

**4. Evaluation of  $\Phi_4(q)$  when  $\left(\frac{q}{p}\right) = -1$ .** We now use the results of Section 3 to show how to evaluate  $\Phi_4(q)$  for a prime  $q$  which is a quadratic non-residue  $\pmod{p}$ . Explicit results are obtained for  $q \leq 19$ .

From the work of Whiteman ([13], p. 90) or Lehmer ([7], p. 65), we have

$$(4.1) \quad \Phi_4(D) \equiv - \left\{ D^{(p-1)/8} \binom{(p-1)/2}{(p-1)/8} + D^{3(p-1)/8} \binom{(p-1)/2}{3(p-1)/8} \right\} \pmod{p}.$$

As  $\binom{(p-1)/2}{(p-1)/8} = \binom{(p-1)/2}{3(p-1)/8}$  we obtain

$$(4.2) \quad \Phi_4(D) \equiv - \binom{(p-1)/2}{(p-1)/8} \left\{ D^{(p-1)/8} + D^{3(p-1)/8} \right\} \pmod{p}.$$

Next as

$$(4.3) \quad \binom{(p-1)/2}{(p-1)/8} \equiv 2e(-1)^{(p-1)/8} \pmod{p},$$

see, for example, Jacobi [4], p. 168, Stern [10], or Whiteman [13], p. 97, we obtain

$$(4.4) \quad \Phi_4(D) \equiv -2e(-1)^{(p-1)/8} \left\{ D^{(p-1)/8} + D^{3(p-1)/8} \right\} \pmod{p}.$$

The congruence (4.4) can be used to evaluate  $\Phi_4(D)$  when  $|\Phi_4(D)|$  and  $D^{(p-1)/8} \pmod{p}$  are known. Appealing to Theorem 1, we use (4.4) to evaluate  $\Phi_4(q)$  for  $q = 3, 5, 7, 11, 13, 17, 19$ ,  $\left(\frac{q}{p}\right) = -1$ . We just give the details for  $q = 5$  as the details are similar for the other values of  $q$ .

For a prime  $p \equiv 1 \pmod{8}$  with  $\left(\frac{5}{p}\right) = -1$  we can choose the signs of  $b$  and  $d$  so that

$$(4.5) \quad a \equiv b \equiv d \pmod{5} \quad \text{or} \quad a \equiv b \equiv -2d \pmod{5},$$

and it follows from Theorem 1 (b), that

$$(4.6) \quad 5^{(p-1)/8} \equiv \frac{(a-b)d}{ac} \pmod{p}.$$

Hence we have

$$(4.7) \quad 5^{(p-1)/8} + 5^{3(p-1)/8} \equiv 2\bar{d}/c \pmod{p},$$

and thus from (4.4) and (4.7) we obtain

$$(4.8) \quad \Phi_4(5) \equiv -4(-1)^{(p-1)/8} \bar{d} \pmod{p}.$$

Since  $\Phi_4(5) = \pm 4\bar{d}$ , by (1.2), we must have

$$(4.9) \quad \Phi_4(5) = -4(-1)^{(p-1)/8} \bar{d}.$$

This completes the proof of the case  $q = 5$  of the following theorem.

**THEOREM 2.** Let  $p = a^2 + b^2 = c^2 + 2\bar{d}^2$  ( $a \equiv c \equiv 1 \pmod{4}$ ) be a prime  $\equiv 1 \pmod{8}$  such that  $\left(\frac{q}{p}\right) = -1$ . Then

$$(4.10) \quad \Phi_4((-1)^{(q-1)/2} q) = -4(-1)^{(p-1)/8} \bar{d}$$

provided  $b$  and  $\bar{d}$  are chosen to satisfy the congruences  $\pmod{q}$  given in Theorem 1 (a)-(g).

**EXAMPLE 2.** Let  $p = 17 = 1^2 + (-4)^2 = (-3)^2 + 2(2)^2$ . Note that  $a \equiv c \equiv 1 \pmod{4}$  and the signs of  $b$  and  $\bar{d}$  have been chosen so that

$$(4.11) \quad a \equiv b \equiv -2\bar{d} \pmod{5}.$$

By (4.9) we must have

$$(4.12) \quad \Phi_4(5) = -4\bar{d} = -8.$$

Indeed for  $p = 17$  we have, appealing to (1.1),

$$\begin{aligned} \Phi_4(5) &= \sum_{x=1}^{16} \left( \frac{x(x^4+5)}{17} \right) \\ &= 2 \left( \left( \frac{6}{17} \right) + \left( \frac{8}{17} \right) + \left( \frac{3}{17} \right) + \left( \frac{7}{17} \right) + \left( \frac{5}{17} \right) + \left( \frac{3}{17} \right) + \left( \frac{12}{17} \right) + \left( \frac{15}{17} \right) \right) \\ &= -8. \end{aligned}$$

We complete this section by briefly illustrating the ideas involved in explicitly evaluating  $\Phi_4(D)$  for composite  $D$ . We just treat the case  $D = -6$ .

Let  $p$  be a prime  $\equiv 1 \pmod{8}$  such that  $\left(\frac{-6}{p}\right) = -1$ . As  $\left(\frac{-3}{p}\right) = -1$ , we can choose  $b$  and  $\bar{d}$  so that  $a \equiv -b \equiv \bar{d} \pmod{3}$ . Then by Theorem 1 (a) we have

$$(4.13) \quad (-3)^{(p-1)/8} \equiv (a-b)\bar{d}/ac \pmod{p}.$$

Since (see for example [1] and [7])

$$(4.14) \quad 2^{(p-1)/8} \equiv \begin{cases} (-1)^{(p-1)/8} \pmod{p} & \text{if } b \equiv 0 \pmod{16}, \\ (-1)^{(p-1)/8} b/a \pmod{p} & \text{if } b \equiv 4 \pmod{16}, \\ (-1)^{(p+7)/8} \pmod{p} & \text{if } b \equiv 8 \pmod{16}, \\ (-1)^{(p+7)/8} b/a \pmod{p} & \text{if } b \equiv 12 \pmod{16}, \end{cases}$$

we obtain from (4.13) and (4.14)

$$(4.15) \quad (-6)^{(p-1)/8} \equiv \begin{cases} (-1)^{(p-1)/8} ((a-b)d/ac) \pmod{p} & \text{if } b \equiv 0 \pmod{16}, \\ (-1)^{(p-1)/8} ((a+b)d/ac) \pmod{p} & \text{if } b \equiv 4 \pmod{16}, \\ (-1)^{(p+7)/8} ((a-b)d/ac) \pmod{p} & \text{if } b \equiv 8 \pmod{16}, \\ (-1)^{(p+7)/8} ((a+b)d/ac) \pmod{p} & \text{if } b \equiv 12 \pmod{16}. \end{cases}$$

It follows at once from (4.15) that

$$(4.16) \quad (-6)^{(p-1)/8} + (-6)^{3(p-1)/8} \equiv \begin{cases} (-1)^{(p-1)/8} 2d/c \pmod{p} & \text{if } b \equiv 0, 4 \pmod{16}, \\ (-1)^{(p+7)/8} 2d/c \pmod{p} & \text{if } b \equiv 8, 12 \pmod{16}, \end{cases}$$

so that, by (4.4), we have  $\Phi_4(-6) \equiv -4d \pmod{p}$  if  $b \equiv 0$  or  $4 \pmod{16}$  and  $\Phi_4(-6) \equiv 4d \pmod{p}$  if  $b \equiv 8$  or  $12 \pmod{16}$ . Thus, by (1.2), we have

$$(4.17) \quad \Phi_4(-6) = \begin{cases} -4d & \text{if } b \equiv 0, 4 \pmod{16}, \\ +4d & \text{if } b \equiv 8, 12 \pmod{16}. \end{cases}$$

**EXAMPLE 3.** Let  $p = 17 = 1^2 + (-4)^2 = (-3)^2 + 2(-2)^2$  so that  $a \equiv c \equiv 1 \pmod{4}$ ,  $a \equiv -b \equiv d \pmod{3}$ , and  $b \equiv 12 \pmod{16}$ . From (4.17) we have  $\Phi_4(-6) = +4d = -8$ , and, indeed,

$$\begin{aligned} \Phi_4(-6) &= \sum_{x=1}^{16} \left( \frac{x(x^4-6)}{17} \right) \\ &= 2 \left( \left( \frac{12}{17} \right) + \left( \frac{3}{17} \right) + \left( \frac{4}{17} \right) + \left( \frac{14}{17} \right) + \left( \frac{1}{17} \right) + \left( \frac{5}{17} \right) + \left( \frac{3}{17} \right) + \left( \frac{12}{17} \right) \right) \\ &= -8. \end{aligned}$$

**5. Evaluation of  $q^{(p-1)/8} \pmod{p}$  when  $\left(\frac{q}{p}\right) = +1$ .** Let  $p = a^2 + b^2 = c^2 + 2d^2 \equiv 1 \pmod{8}$  be a prime with  $a$  and  $c$  chosen so that  $a \equiv c \equiv 1 \pmod{4}$ . Let  $q$  be an odd prime such that  $\left(\frac{q}{p}\right) = +1$ . In this section

we give necessary and sufficient conditions for  $q$  to satisfy  $((-1)^{(q-1)/2}q)^{(p-1)/8} \equiv b/a \pmod{p}$  for each prime  $q \leq 19$ . When  $q \equiv \pm 1 \pmod{8}$  these conditions involve congruences of the form  $a \equiv \lambda b \pmod{q}$  (see Theorem 3 (c), (f)), and when  $q \equiv \pm 3 \pmod{8}$  they involve congruences of the form  $b \equiv \gamma c \pmod{q}$  (see Theorem 3 (a), (b), (d), (e), (g)). Apart from this difference, the proofs of (a)–(g) are similar, and may easily be written down by analogy with the proof of (g) which is given below.

**THEOREM 3.** Let  $p = a^2 + b^2 = c^2 + 2d^2 \equiv 1 \pmod{8}$  be a prime with  $a$  and  $c$  chosen so that  $a \equiv c \equiv 1 \pmod{4}$ . Then we have

$$(a) \quad (-3)^{(p-1)/8} \equiv b/a \pmod{p} \Leftrightarrow b \equiv c \pmod{3},$$

$$(b) \quad 5^{(p-1)/8} \equiv b/a \pmod{p} \Leftrightarrow \begin{cases} b \equiv -c \pmod{5}, \\ b \equiv 2c \pmod{5}, \end{cases}$$

$$(c) \quad (-7)^{(p-1)/8} \equiv b/a \pmod{p} \Leftrightarrow \begin{cases} a \equiv b \pmod{7} & \text{and } cd \equiv 0 \pmod{7}, \\ a \equiv -b \pmod{7} & \text{and } cd \not\equiv 0 \pmod{7}, \end{cases}$$

$$(d) \quad (-11)^{(p-1)/8} \equiv b/a \pmod{p} \Leftrightarrow \begin{cases} b \equiv -kc \pmod{11}, \\ b \equiv -5kc \pmod{11}, \end{cases}$$

where  $k = 1, 5$  or  $-3$  according as  $d \equiv 0 \pmod{11}$ ,  $c \equiv \pm d$  or  $\pm 5d \pmod{11}$ ,

$$(e) \quad 13^{(p-1)/8} \equiv b/a \pmod{p} \Leftrightarrow \begin{cases} b \equiv kc \pmod{13}, \\ b \equiv 6kc \pmod{13}, \end{cases}$$

where  $k = 1, 4, -5$ , or  $-3$  according as  $d \equiv 0$ ,  $c \equiv \pm d$ ,  $c \equiv \pm 5d$ , or  $\pm 6d \pmod{13}$ ,

$$(f) \quad 17^{(p-1)/8} \equiv b/a \pmod{p} \Leftrightarrow \begin{cases} a \equiv 5kb \pmod{17}, \\ a \equiv -7kb \pmod{17}, \end{cases}$$

where  $k = 1$  if  $cd \equiv 0$  or  $c \equiv \pm 6d \pmod{17}$ ,  $k = -1$  if  $c \equiv \pm 4d$  or  $\pm 8d \pmod{17}$ ,

$$(g) \quad (-19)^{(p-1)/8} \equiv b/a \pmod{p} \Leftrightarrow \begin{cases} b \equiv kc \pmod{19}, \\ b \equiv 2kc \pmod{19}, \\ b \equiv 7kc \pmod{19}, \end{cases}$$

where  $k = 1, 7, 3, -2$ , or  $-4$  according as  $d \equiv 0$ ,  $c \equiv \pm 2d, \pm 9d, \pm 8d$ , or  $\pm 3d \pmod{19}$  respectively.

**Proof of Theorem 3 (g).** For brevity, all congruences are to be taken modulo 19 unless otherwise stated.

Case (i):  $d \not\equiv 0$ . It is easy to check that for each congruence on the right-hand side of (g), we have

$$p^2(a+bi)^5(c-di\sqrt{2})^9 \equiv i,$$

and so by (2.10), with  $q = 19$ , we deduce that

$$(-19)^{(p-1)/8} \equiv b/a \pmod{p}.$$

For example, for  $a \equiv 0$ ,  $b \equiv -2c$ , we have

$$p^2(a+bi)^5(c-di\sqrt{2})^9 \equiv i^5(9 \pm 6i\sqrt{2})^9 \equiv i,$$

as  $a \equiv 0$ ,  $c \equiv 9b$  imply  $b^2 \equiv 5b + 2d^2$ , that is,  $d \equiv \pm 6b$ ;  $b^{18} \equiv 1$ ;

and, appealing to (3.8) and noting that  $6^9 \equiv \left(\frac{6}{19}\right) = +1$ ,

$$(9 \pm 6i\sqrt{2})^9 \equiv 6^9(\pm i\sqrt{2})^9 \equiv 1.$$

Conversely, suppose that

$$(5.1) \quad (-19)^{(p-1)/8} \equiv b/a \pmod{p}.$$

Then  $(-19)^{(p-1)/2} \equiv +1 \pmod{p}$ , and by the law of quadratic reciprocity, we have

$$(5.2) \quad \left(\frac{p}{19}\right) = +1.$$

Setting  $c \equiv \mu d$  in (5.2), we obtain

$$\left(\frac{\mu^2+2}{19}\right) = +1,$$

so that

$$(5.3) \quad \mu \equiv \pm 2, \pm 3, \pm 8, \pm 9.$$

Also, from (5.1), we have  $(-19)^{(p-1)/4} \equiv -1 \pmod{p}$ , and so by the law of quartic reciprocity, see [2], we have

$$(5.4) \quad \left(\frac{a-bi}{a+bi}\right)^5 \equiv -1.$$

Clearly  $b \not\equiv 0$  and we can set  $a \equiv \lambda b$  in (5.4) to get

$$(5.5) \quad \lambda \equiv 0, \pm 2, \pm 5.$$

Next, by the law of octic reciprocity, see (2.10), we have

$$(5.6) \quad p^2(a+bi)^5(c-di\sqrt{2})^9 \equiv i.$$

Using  $a \equiv \lambda b$ ,  $c \equiv \mu d$ , and setting  $b \equiv \gamma c$  so that  $a \equiv \lambda\mu\gamma d$  and  $b \equiv \mu\gamma d$  in (5.6) we obtain, as  $d^{18} = 1$  and  $(\mu\gamma)^9 \equiv \left(\frac{\mu\gamma}{19}\right)$ ,

$$(5.7) \quad (\lambda^2+1)^2(\lambda+i)^5(\mu-i\sqrt{2})^9\left(\frac{\mu\gamma}{19}\right) \equiv i.$$

From (3.7) and (3.8) we obtain

$$(5.8) \quad (\lambda^2 + 1)^2(\lambda + i)^5 \equiv \begin{cases} i & \text{if } \lambda \equiv 0, \pm 5, \\ -i & \text{if } \lambda \equiv \pm 2, \end{cases}$$

and

$$(5.9) \quad (\mu - i\sqrt{2})^9 \equiv \begin{cases} +1 & \text{if } \mu \equiv -2, +3, -8, -9, \\ -1 & \text{if } \mu \equiv +2, -3, +8, +9. \end{cases}$$

From (5.7), (5.8), and (5.9) we must have

$$(5.10) \quad \left(\frac{\mu\gamma}{19}\right) = +1 \quad \text{if} \quad \begin{cases} \lambda \equiv 0, \pm 5 \text{ and } \mu \equiv -2, +3, -8, -9, \\ \text{or} \\ \lambda \equiv \pm 2 \text{ and } \mu \equiv +2, -3, +8, +9, \end{cases}$$

and

$$(5.11) \quad \left(\frac{\mu\gamma}{19}\right) = -1 \quad \text{if} \quad \begin{cases} \lambda \equiv 0, \pm 5 \text{ and } \mu \equiv +2, -3, +8, +9, \\ \text{or} \\ \lambda \equiv \pm 2 \text{ and } \mu \equiv -2, +3, -8, -9. \end{cases}$$

From  $a^2 + b^2 = c^2 + 2d^2$  we obtain

$$(5.12) \quad \gamma^2 = \frac{\mu^2 + 2}{\mu^2(\lambda^2 + 1)}.$$

Next, from (5.10), (5.11), and (5.12), we have the following table of values of  $\gamma$ :

$\mu \backslash \lambda$	0	$\pm 2$	$\pm 5$
$\pm 2$	7	-5	-8
$\pm 3$	-4	-8	-9
$\pm 8$	-2	-4	5
$\pm 9$	3	6	2

Finally, setting

$$(5.14) \quad k \equiv 7, -4, -2, \text{ or } +3 \text{ according as } c \equiv \pm 2d, \pm 3d, \pm 8d, \\ \text{or } \pm 9d,$$

we obtain for all 12 values of  $\gamma$ ,

$$(5.15) \quad \frac{\gamma}{k} \equiv 1, 2, \text{ or } 7 \text{ according as } \lambda \equiv 0, \pm 2, \text{ or } \pm 5.$$

This proves Theorem 3 (g) in case (i).

Case (ii):  $d \equiv 0$ . The proof is the same as in case (i) except that we clearly cannot set  $c \equiv \mu d$ . However, setting  $b \equiv \gamma c$ , (5.6) becomes in this case,

$$(5.16) \quad (\lambda^2 + 1)^2(\lambda + i)^5 \left(\frac{\gamma}{19}\right) \equiv i.$$

Hence by (5.8) we have

$$(5.17) \quad \left(\frac{\gamma}{19}\right) = +1 \Leftrightarrow \lambda \equiv 0, \pm 5.$$

Next from  $a^2 + b^2 = c^2 + 2d^2$  we have

$$(5.18) \quad \gamma^2 = \frac{1}{\lambda^2 + 1}.$$

Putting (5.17) and (5.18) together, we get (just as in (5.15) taking  $k = 1$ ),

$$(5.19) \quad \gamma \equiv 1, 2, \text{ or } 7 \text{ according as } \lambda \equiv 0, \pm 2, \text{ or } \pm 5.$$

This completes the proof of Theorem 3 (g) in case (ii).

**EXAMPLE 4.** ( $q = 5$ : see Theorem 3 (b).)

(i) Let  $p = 281 = 5^2 + 16^2 = 9^2 + 2(10)^2$  so that  $b \equiv -c \pmod{5}$ . Then we have

$$\frac{b}{a} \equiv \frac{16}{5} \equiv 228 \pmod{281},$$

and it is easily checked that for  $p = 281$  we have

$$5^{(p-1)/8} \equiv 5^{35} \equiv 228 \pmod{281}.$$

(ii) Let  $p = 1289 = (-35)^2 + 8^2 = 33^2 + 2(10)^2$  so that  $b \equiv c \pmod{5}$ . Then we have

$$5^{(p-1)/8} \equiv 5^{161} \equiv 479 \equiv \frac{8}{35} \equiv -\frac{b}{a} \pmod{p}.$$

(iii) Let  $p = 89 = 5^2 + 8^2 = 9^2 + 2(2)^2$  so that  $b \equiv 2c \pmod{5}$ . Then we have

$$5^{(p-1)/8} \equiv 5^{11} \equiv 55 \equiv \frac{8}{5} \equiv \frac{b}{a} \pmod{p}.$$

(iv) Let  $p = 241 = (-15)^2 + 4^2 = 13^2 + 2(6)^2$  so that  $b \equiv 2c \pmod{5}$ . Then we have

$$5^{(p-1)/8} \equiv 5^{30} \equiv 177 \equiv \frac{4}{15} \equiv -\frac{b}{a} \pmod{p}.$$

**Remark.** Although the number of cases to be considered grows quite rapidly as  $q$  increases, there are no technical difficulties in using the methods given in the proofs of Theorems 1, 2, and 3 to extend the results in this paper beyond  $q = 19$ .

**6. Values of  $k$  in Theorems 1 and 3 when  $q \equiv \pm 3 \pmod{8}$ .** We observe with considerable interest that the values of  $k$  which occur in Theorem 1 (d), (e), (g) are identical with the values of  $k$  which occur in Theorem

3 (d), (e), (g), both in magnitude and sign. The values of  $k$  in Theorem 3 have been written in an order which corresponds to their order in Theorem 1. In this section we investigate the pattern which underlies this ordering for every  $q > 3$  which is  $\equiv \pm 3 \pmod{8}$ .

Let  $k_{1,j+1}(q)$  be the value of  $k$  corresponding to  $c \equiv \pm r_j d \pmod{q}$  when  $\left(\frac{q}{p}\right) = -1$ ,  $j = 1, 2, \dots$ , and let  $k_{2,j+1}(q)$  be the value of  $k$  corresponding to  $c \equiv \pm s_j d \pmod{q}$  when  $\left(\frac{q}{p}\right) = +1$ , where  $k_{1,1}(q)$  and  $k_{2,1}(q)$  are equal to 1 and correspond to  $c \equiv 0 \pmod{q}$  and  $d \equiv 0 \pmod{q}$  respectively. For example, when  $q = 19$  we have from Theorem 1 (g) and Theorem 3 (g) that  $k_{1,3} = k_{2,3} = 3$ ,  $r_2 = 4$ ,  $s_2 = 9$ . Observing that  $r_2^2 \cdot s_2^2 \equiv (-3)(5) \equiv 4 \pmod{19}$  and that the same congruence is satisfied  $\pmod{q}$  for every choice of  $j$  in Theorem 1 and 3, parts (d), (e), (g) as well as in part (b) when reformulated in analogy to (d), (e), and (g), we are led (with the above notation) to a general theorem relating the values of  $q$  in Theorems 1 and 3 when  $q$  is a prime  $\equiv \pm 3 \pmod{8}$ ,  $q > 3$ .

**THEOREM 4.** *Let  $q$  be a prime  $> 3$  which is  $\equiv \pm 3 \pmod{8}$ . Then*

$$(6.1) \quad (k_{1,j+1})^2 = (k_{2,j+1})^2 \Leftrightarrow (r_j)^2 (s_j)^2 \equiv 4 \pmod{q}, \quad j = 1, 2, \dots$$

*Proof.* Let  $q$  be  $> 3$  so that  $r_j$  and  $s_j$  exist. Applying (3.4) with the exponent 5 replaced by  $(q+1)/4$  if  $q \equiv 3 \pmod{8}$  and by  $(q-1)/4$  if  $q \equiv 5 \pmod{8}$ , one can show that one of  $\lambda \equiv 1$  or  $\lambda \equiv -1$  is always a solution. Then, by (3.13) and (3.16), we have ( $r_j$  replaces  $\mu$  in (3.13)),

$$(6.2) \quad (k_{1,j+1}(q))^2 \equiv \frac{1}{2}((r_j(q))^2 + 2) \pmod{q}, \quad j = 1, 2, \dots$$

Similarly, applying (5.4) with the same replacement, it is obvious that this congruence is always satisfied if  $\lambda \equiv 0$  ( $a \equiv \lambda b$ ). Taking  $\gamma/k_{2,j} \equiv 1 \pmod{q}$ ,  $j = 1, 2, \dots$  (see (5.15)), and using (5.12), we have ( $s_j$  replaces  $\mu$  in (5.12))

$$(6.3) \quad (k_{2,j+1}(q))^2 \equiv \frac{((s_j(q))^2 + 2)}{(s_j(q))^2} \pmod{q}, \quad j = 1, 2, \dots$$

The result follows then from (6.2) and (6.3), as the  $k_{1,j+1}$  and  $k_{2,j+1}$  are chosen in the range  $-\frac{1}{2}q < k < \frac{1}{2}q$ .

#### References

- [1] Alexander Aigner, *Kriterien zum 8. und 16. Potenzcharakter der Reste 2 und -2*, Deutsche Math. 4 (1939), pp. 44-52.
- [2] Thorold Gosset, *On the law of quartic reciprocity*, Mess. Math. 41 (1911), pp. 65-90.
- [3] Richard H. Hudson and Kenneth S. Williams, *Resolution of ambiguities, in the evaluation of certain Jacobsthal sums*, Pacific J. Math. (to appear).

- [4] C. G. J. Jacobi, *Über die Kreistheilung und ihre Anwendung auf die Zahlentheorie*, J. Reine Angew. Math. 30 (1846), pp. 166–182.
- [5] Ernst Jacobsthal, *Über die Darstellung der Primzahlen der Form  $4n+1$  als Summe zweier Quadrate*, *ibid.* 132 (1907), pp. 238–245.
- [6] Emma Lehmer, *Criteria for cubic and quartic residuacity*, *Mathematika* 5 (1958), pp. 20–29.
- [7] — *On Euler's criterion*, J. Austral. Math. Soc. 1 (1959), pp. 64–70.
- [8] Horst von Lienen, *Primzahlen als achte Potenzreste*, J. Reine Angew. Math. 266 (1974), pp. 107–117.
- [9] Lothar von Schrutka, *Ein Beweis für die Zerlegbarkeit der Primzahlen von dre Form  $6n+1$  in ein einfaches und ein dreifaches Quadrat*, *ibid.* 140 (1911), pp. 252–265.
- [10] M. Stern, *Eine Bemerkung zur Zahlentheorie*, *ibid.* 32 (1846), pp. 89–90.
- [11] A. E. Western, *Some criteria for the residues of eighth and other powers*, Proc. London Math. Soc. 9 (1911), pp. 244–272.
- [12] Albert L. Whiteman, *Theorems analogous to Jacobsthal's theorem*, Duke Math. J. 16 (1949), pp. 619–626.
- [13] — *Cyclotomy and Jacobsthal sums*, Amer. J. Math. 74 (1952), pp. 89–99.

DEPARTMENT OF MATHEMATICS AND STATISTICS  
UNIVERSITY OF SOUTH CAROLINA  
Columbia, South Carolina, U.S.A.

DEPARTMENT OF MATHEMATICS AND STATISTICS  
CARLETON UNIVERSITY  
Ottawa, Ontario, Canada

Received on 2. 6. 1980

(1209)