[15] V. Ramaswami, *The number of positive integers $\leqslant x$ and free of prime divisors $> x^c$, and a problem of S. S. Pillai*, Duke Math. J. 16 (1949), p. 99–109.
[16] W. Rudin, *Real and complex analysis*, McGraw Hill, 1970.
[17] G. Tenenbaum, *Sur deux fonctions de diviseurs*, J. London Math. Soc. (2) 14 (1976), p. 521–526.

U. E. R. DE MATHÉMATIQUES ET D'INFORMATIQUE
UNIVERSITÉ DE BORDEAUX I
351, cours de la Libération
33405 Talence Cedex, France

Reçu le 30. 7. 1977
et dans la forme modifiée le 17. 6. 1978 (964)

ACTA ARITHMETICA
XXXVIII (1980)

Bioctic Gauss sums and sixteenth power residue difference sets

by

RONALD J. EVANS (La Jolla, Calif.)

1. Introduction. For an integer $k > 1$, define the Gauss sum $G_k = \sum_{n=0}^{p-1} e^{2\pi i n^k/p}$, where p denotes a prime congruent to 1 modulo k. One object of this paper is to evaluate G_{16} (up to some sign ambiguities). This is done in terms of parameters that appear in the representations of p as binary and quartic integral quadratic forms. We shall make heavy use of the results and notation of [2], wherein G_k is evaluated for $k = 4, 6, 8, 12,$ and 24.

The values of G_k are connected with a well-known problem on power residue difference sets, namely that of characterizing the set of primes p for which the set H_k of kth power residues (mod p) (or the modified set $H_k \cup \{0\}$) is a difference set. In the period 1933–1967, this problem has been solved for all the values $k < 20$ except $k = 16$. For references and good expositions, see the books of Baumert [1], pp. 119 ff, and Storer [4]. In 1957, Whiteman [5] obtained a partial solution for $k = 16$ by showing that H_{16} and $H_{16} \cup \{0\}$ are never difference sets when 2 is an octic residue (mod p). The problem for $k = 16$ when 2 is an octic nonresidue remained open (see [1], p. 124, [4], p. 82). Using our evaluation of G_{16}, we complete the solution for $k = 16$ by showing that H_{16} and $H_{16} \cup \{0\}$ are never difference sets. The case where 2 is a quartic residue (mod p) is solved in § 4, and the case where 2 is a quartic nonresidue (mod p) is solved in § 5. In the latter case we utilize several results from [5] which are proved using the theory of cyclotomic numbers; in the former case, the theory of cyclotomic numbers is not used. Our methods are similar to those of [2], Chapter 5, wherein we obtained new and relatively simple solutions to the problem for $k = 4, 6, 8$ and 12.

2. Notation and the formula for G_{16}. For characters λ, χ (mod p), define the Jacobi sum

$$J(\chi, \lambda) = \sum_{n=0}^{p-1} \chi(n)\lambda(1-n)$$

and the Gauss sum

$$G(\chi) = \sum_{n=0}^{p-1} \chi(n) e^{2\pi i n/p}.$$

Write $J(\chi) = J(\chi, \chi)$ and $K(\chi) = \chi(4) J(\chi)$. It is well-known that $J(\chi, \lambda) = G(\chi) G(\lambda)/G(\chi\lambda)$ when $\chi \neq \bar{\lambda}$.

Let $p \equiv 1 \pmod{16}$ and fix a character $\chi \pmod p$ of order 16. Let $\psi = \chi^2$. As in [2], Theorems 3.9 and 3.12, designate integers a_4, b_4, a_8, b_8 for which

$$K(\psi^2) = a_4 + ib_4 \quad (a_4^2 + b_4^2 = p,\ a_4 \equiv -1 \pmod 4)$$

and

$$K(\psi) = a_8 + ib_8\sqrt{2} \quad (a_8^2 + 2b_8^2 = p,\ a_8 \equiv -1 \pmod 4).$$

As in [3], Theorem 3.5, write

$$K(\chi) = a_{16} + b_{16}\sqrt{2} + ic_{16}\sqrt{2+\sqrt{2}} + id_{16}\sqrt{2-\sqrt{2}},$$

where a_{16}, b_{16}, c_{16} and d_{16} are integers such that

$$p = a_{16}^2 + 2b_{16}^2 + 2c_{16}^2 + 2d_{16}^2, \quad a_{16} \equiv -1 \pmod 8,$$

$$2a_{16} b_{16} = d_{16}^2 - c_{16}^2 - 2c_{16} d_{16} \quad \text{and} \quad b_{16}, c_{16}, d_{16} \equiv 0 \pmod 2.$$

Put $R_6 = G(\psi^2) + G(\bar{\psi}^2)$, $R_3 = G(\psi) + G(\bar{\psi})$, and $R_9 = G(\psi^3) + G(\bar{\psi}^3)$, as in [2], (3.9), (3.18). Let $Y = R_3 + R_9$. Note that Y and R_6 are real and independent of the choice of χ. By [2], (3.10), (3.19), we have

$$R_6 = (\operatorname{sgn} R_6)\{2p + 2a_4 p^{1/2}\}^{1/2}$$

and

$$Y = (\operatorname{sgn} Y)\{(p^{1/2} + a_8)(4p^{1/2} + 2\eta R_6)\}^{1/2},$$

where

$$\eta = \psi^2(2) = \begin{cases} 1, & \text{if 2 is a quartic residue (mod } p), \\ -1, & \text{otherwise.} \end{cases}$$

Define $\alpha = \pm 1$ by

$$\alpha = \begin{cases} \psi(2), & \text{if} \quad \eta = 1, \\ \psi(2)/i, & \text{if} \quad \eta = -1. \end{cases}$$

Define $\gamma = \pm 1$ by

$$\gamma = \begin{cases} \alpha, & \text{if} \quad \eta = 1; \\ -\alpha \operatorname{sgn}(b_4 R_6), & \text{if} \quad \eta = -1. \end{cases}$$

When $\eta = 1$, α is independent of χ, and when $\eta = -1$, αb_4 is independent of χ. Hence γ is independent of χ. Let

$$S = \gamma(\operatorname{sgn} Y)\{(p^{1/2} + a_8)(4p^{1/2} + 2R_6)\}^{1/2}.$$

Thus,

$$(1) \qquad Y = \begin{cases} \alpha S, & \text{if} \quad \eta = +1, \\ -\alpha S(R_6 - p^{1/2} - a_4)/b_4, & \text{if} \quad \eta = -1. \end{cases}$$

Observe that S is real and independent of χ.

We can now present the formula for G_{16}.

THEOREM 1. *We have* $G_{16} = p^{1/2} + R_6 + Y \pm M$, *where*

$$(2) \qquad M^2 = \pm 2N + 8(-1)^{(p-1)/16}(p + a_{16} p^{1/2}) + 2S \times \times (p^{1/2} + a_{16} - (p^{1/2} - a_8)(R_6 - a_4 - p^{1/2}) b_{16}/b_4 b_8)$$

and

$$(3) \qquad N^2 = 4(p + a_{16}^2 + 2a_{16} p^{1/2} - 2b_{16}^2) \times \times (4p + 2a_8 p^{1/2} + p^{1/2} R_6 + 2(-1)^{(p-1)/16} p^{1/2} S).$$

Observe that while b_{16}, b_4 and b_8 each depend on χ, $b_{16}/b_4 b_8$ does not.

As a numerical example, we give the following values (rounded off to the nearest millionth) when $p = 113$: $a_4 = 7$, $a_8 = -9$, $a_{16} = -1$, $b_{16}/b_4 b_8 = 1/8$, $\eta = 1$, $\alpha = -1$, $R_6 = 19 \cdot 360321$, $Y = -S = 11 \cdot 508043$, $|N| = 415 \cdot 660969$, $|M| = 42 \cdot 121436$, and $G_{16} = 41 \cdot 498510 + i(42 \cdot 121436)$. Here M is purely imaginary, and the first term on the right side of (2) is $-2|N|$.

3. Proof of the formula for G_{16}. We begin with some lemmas, the first of which is proved in [2], Theorem 2.5.

LEMMA 2. *Let q be an odd prime and let λ be a character* (mod q) *of order $2m$. Then*

$$\text{(i)} \qquad K(\lambda) = \left(\frac{-1}{q}\right) K(\lambda^{m-1})$$

and

$$\text{(ii)} \qquad K(\lambda) = \lambda(-1) J(\lambda, \lambda^{m-1}).$$

LEMMA 3. *We have*

$$G(\psi) G(\psi^3) = p^{1/2} K(\psi) \quad \text{and} \quad G(\bar{\psi}) G(\psi^3) = \eta p^{1/2} G(\bar{\psi}^2).$$

Proof. By Lemma 2(ii), $G(\psi) G(\psi^3) = p^{1/2} J(\psi, \psi^3) = p^{1/2} K(\psi)$. Hence

$$G(\bar{\psi}) G(\psi^3) = \frac{G(\bar{\psi})}{G(\psi)} \frac{G^2(\psi)}{G(\psi^2)} \eta p^{1/2} = \eta p^{1/2} G(\bar{\psi}^2). \quad \blacksquare$$

LEMMA 4. *We have* $G(\psi^2) = R_6/2 + i(2p - 2a_4 p^{1/2})^{1/2} (\operatorname{sgn} b_4 R_6)/2$.

Proof. Since $\operatorname{Re}(G(\psi^2)) = R_6/2$ and $|G(\psi^2)|^2 = p$, we have

$$G(\psi^2) = R_6/2 + i(2p - 2a_4 p^{1/2})^{1/2} \delta/2$$

for some $\delta = \pm 1$. Thus,

$$4G^2(\psi^2) = 4a_4 p^{1/2} + 2i\delta R_6 (2p - 2a_4 p^{1/2})^{1/2} = 4a_4 p^{1/2} + 4i\delta p^{1/2} b_4 (\operatorname{sgn} R_6 b_4).$$

Since $4G^2(\psi^2) = 4p^{1/2} K(\psi^2) = 4p^{1/2} a_4 + 4p^{1/2} i b_4$, we have $\delta = \operatorname{sgn}(R_6 b_4)$, as desired. ∎

LEMMA 5. *Let $\delta = \pm 1$. Then*

$$(G(\psi) + \delta G(\psi^3))^2 = K(\psi)(2\delta p^{1/2} + \eta R_6).$$

Proof. We have

$$\begin{aligned}(G(\psi) + \delta G(\psi^3))^2 &= G^2(\psi) + G^2(\psi^3) + 2\delta G(\psi) G(\psi^3) \\ &= J(\psi) G(\psi^2) + J(\psi^3) G(\bar{\psi}^2) + 2\delta G(\psi) G(\psi^3) \\ &= \eta\big(K(\psi) G(\psi^2) + K(\psi^3) G(\bar{\psi}^2)\big) + 2\delta G(\psi) G(\psi^3).\end{aligned}$$

Since $K(\psi) = K(\psi^3)$ by Lemma 2(i), it follows with the use of Lemma 3 that

$$(G(\psi) + \delta G(\psi^3))^2 = 2K(\psi)\big(\delta p^{1/2} + \eta \operatorname{Re}(G(\psi^2))\big) = K(\psi)(2\delta p^{1/2} + \eta R_6). \blacksquare$$

LEMMA 6. *We have*

$$R_3 - R_9 = -4\eta b_8 (\operatorname{sgn} b_4 R_6) \{p - a_4 p^{1/2}\}^{1/2} / Y.$$

Proof. In the proof in [2], Theorem 3.18, we saw that

$$R_3^2 = 2p + 2\eta \operatorname{Re}\{G(\psi^2) K(\psi)\}$$

and

$$R_9^2 = 2p + 2\eta \operatorname{Re}\{G(\bar{\psi}^2) K(\psi)\}.$$

Thus, $R_3^2 - R_9^2 = 2\eta \operatorname{Re}\{K(\psi)(G(\psi^2) - G(\bar{\psi}^2))\}$. The result now follows from Lemma 4 and the fact that $R_3 - R_9 = (R_3^2 - R_9^2)/Y$. ∎

LEMMA 7. *We have*

$$2 \operatorname{Re}\{\bar{\psi}(2) G(\psi) + \bar{\psi}^3(2) G(\psi^3)\} = S.$$

Proof. This follows from (1) if $\eta = 1$, so suppose that $\eta = -1$. Then the left member above equals $-2\alpha \operatorname{Re}\{i(G(\psi) - G(\psi^3))\} = 2\alpha \operatorname{Im}\{G(\psi) - G(\psi^3)\}$. By Lemma 5,

$$\operatorname{Im}\{G(\psi) - G(\psi^3)\}^2 = -b_8 \sqrt{2}\,(2p^{1/2} + R_6).$$

Hence,

$$\begin{aligned}2\alpha \operatorname{Im}\{G(\psi) - G(\psi^3)\} &= \frac{2\alpha \operatorname{Im}\{G(\psi) - G(\psi^3)\}^2}{2 \operatorname{Re}\{G(\psi) - G(\psi^3)\}} \\ &= -2\alpha b_8 \sqrt{2}\,(2p^{1/2} + R_6)/(R_3 - R_9).\end{aligned}$$

By Lemma 6 and (1), this last expression equals S. ∎

LEMMA 8. *We have*

$$2 \operatorname{Re}\{\bar{\psi}(2) G(\psi) - \bar{\psi}^3(2) G(\psi^3)\} = S(a_8 - p^{1/2})(R_6 - a_4 - p^{1/2})/b_4 b_8 \sqrt{2}.$$

Proof. Let L denote the left member above. First suppose that $\eta = 1$. Then $L = \alpha(R_3 - R_9)$ and the result follows from Lemma 6 and (1).

Now suppose that $\eta = -1$. Then

$$L = 2\alpha \operatorname{Im}\{G(\psi) + G(\psi^3)\}.$$

By Lemma 5,

$$\operatorname{Im}\{G(\psi) + G(\psi^3)\}^2 = b_8 \sqrt{2}\,(2p^{1/2} - R_6).$$

Hence,

$$L = \frac{2\alpha \operatorname{Im}\{G(\psi) + G(\psi^3)\}^2}{2 \operatorname{Re}\{G(\psi) + G(\psi^3)\}} = 2\alpha b_8 \sqrt{2}\,(2p^{1/2} - R_6)/Y$$

and the result follows from (1). ∎

Proof of Theorem 1. We have

$$G_{16} = \sum_{u=0}^{p-1} e^{2\pi i u/p} \sum_{j=1}^{15} \chi^j(n) = G_8 + F_1 + F_3 + F_5 + F_7 = G_8 \pm M, \tag{4}$$

where $F_j = G(\chi^j) + G(\bar{\chi}^j)$ and

$$M^2 = (F_1 + F_3 + F_5 + F_7)^2. \tag{5}$$

By [2], Theorem 3.18,

$$G_8 = p^{1/2} + R_6 + Y. \tag{6}$$

Hence $G_{16} = p^{1/2} + R_6 + Y \pm M$. By (5),

$$M^2 = (F_1 + F_7)^2 + (F_3 + F_5)^2 \pm 2N, \tag{7}$$

where

$$N^2 = (F_1 + F_7)^2 (F_3 + F_5)^2.$$

It remains to verify (2) and (3).

We have

$$\begin{aligned}F_1^2 &= G^2(\chi) + G^2(\bar{\chi}) + 2p\chi(-1) = J(\chi) G(\psi) + J(\bar{\chi}) G(\bar{\psi}) + 2p\chi(-1) \\ &= G(\psi)\bar{\psi}(2) K(\chi) + G(\bar{\psi})\psi(2) K(\bar{\chi}) + 2p\chi(-1).\end{aligned}$$

Since $K(\chi) = K(\chi^7)$ by Lemma 2(i),

$$F_7^2 = G(\bar{\psi})\psi(2) K(\chi) + G(\psi)\bar{\psi}(2) K(\bar{\chi}) + 2p\chi(-1).$$

Thus,

$$F_1^2 + F_7^2 = 4p\chi(-1) + 4 \operatorname{Re}\{K(\chi)\} \operatorname{Re}\{\bar{\psi}(2) G(\psi)\}. \tag{8}$$

By Lemma 2 (ii),

$$G(\chi)\,G(\chi^7) = p^{1/2}\,J(\chi,\chi^7) = p^{1/2}\,\chi(-1)\,K(\chi),$$

so that

$$G(\bar\chi)\,G(\chi^7) = \frac{G(\bar\chi)}{G(\chi)}\,\frac{G^2(\chi)}{G(\psi)}\,\psi(2)\,p^{1/2}\,\chi(-1) = p^{1/2}\,\psi(2)\,G(\bar\psi).$$

Therefore,

$$\begin{aligned}(9)\qquad 2F_1F_7 &= 4\,\mathrm{Re}\,\{G(\chi)\,G(\chi^7)+G(\bar\chi)\,G(\chi^7)\}\\ &= 4p^{1/2}\,\chi(-1)\,\mathrm{Re}\,\{K(\chi)\}+4p^{1/2}\,\mathrm{Re}\,\{\bar\psi(2)\,G(\psi)\}.\end{aligned}$$

Thus by (8) and (9),

$$(F_1+F_7)^2 = 4\{p^{1/2}+\mathrm{Re}\,\{K(\chi)\}\}\{\chi(-1)\,p^{1/2}+\mathrm{Re}\,\{\bar\psi(2)\,G(\psi)\}\}.$$

Similarly,

$$(F_3+F_5)^2 = 4\{p^{1/2}+\mathrm{Re}\,\{K(\chi^3)\}\}\{\chi(-1)\,p^{1/2}+\mathrm{Re}\,\{\bar\psi^3(2)\,G(\psi^3)\}\}.$$

Thus,

$$(F_1+F_7)^2 = 4\{p^{1/2}+a_{16}+b_{16}\sqrt{2}\}\{p^{1/2}(-1)^{(p-1)/16}+\mathrm{Re}\,\{\bar\psi(2)\,G(\psi)\}\}$$

and

$$(F_3+F_5)^2 = 4\{p^{1/2}+a_{16}-b_{16}\sqrt{2}\}\{p^{1/2}(-1)^{(p-1)/16}+\mathrm{Re}\,\{\bar\psi^3(2)\,G(\psi^3)\}\}.$$

Adding, we have

$$\begin{aligned}(10)\qquad (F_1+F_7)^2+(F_3+F_5)^2 &= 8(-1)^{(p-1)/16}(p+a_{16}p^{1/2})+\\ &+4(p^{1/2}+a_{16})\,\mathrm{Re}\,\{\bar\psi(2)\,G(\psi)+\bar\psi^3(2)\,G(\psi^3)\}+\\ &+4b_{16}\sqrt{2}\,\mathrm{Re}\,\{\bar\psi(2)\,G(\psi)-\bar\psi^3(2)\,G(\psi^3)\}.\end{aligned}$$

Also,

$$\begin{aligned}(11)\qquad N^2 = (F_1+F_7)^2(F_3+F_5)^2 &= 4(p+a_{16}^2+2p^{1/2}a_{16}-2b_{16}^2)\times\\ &\times\{4p+4p^{1/2}(-1)^{(p-1)/16}\,\mathrm{Re}\,\{\bar\psi(2)\,G(\psi)+\bar\psi^3(2)\,G(\psi^3)\}+\\ &+2\,\mathrm{Re}\,\{G(\psi)\,G(\psi^3)\}+2\eta\,\mathrm{Re}\,\{G(\psi)\,G(\bar\psi^3)\}\},\end{aligned}$$

By Lemmas 3 and 4, the rightmost two terms in the last factor in (11) add up to $p^{1/2}(2a_8+R_6)$. The result thus follows from (7), (10), and (11), with the use of Lemmas 7 and 8. ∎

4. Nonexistence of difference sets when 2 is a quartic residue.

THEOREM 2. *Let p be prime such that $p \equiv 1 \pmod{16}$ and 2 is a quartic residue* (mod p). *Then neither H_{16} nor $H_{16}\cup\{0\}$ is a difference set.*

Proof. Assume the contrary. Then, by [2], Theorem 5.2,

$$(12)\qquad p \equiv 17 \pmod{32},$$

and by [2], Theorem 5.1,

$$(13)\qquad |G_{16}+\nu|^2 = 15p+\nu^2,$$

where

$$\nu = \begin{cases} -1, & \text{if } H_{16} \text{ is a difference set,}\\ 15, & \text{if } H_{16}\cup\{0\} \text{ is a difference set.}\end{cases}$$

By (12), $\chi(-1) = -1$, so for $j = 1,3,5,7$, $G(\bar\chi^j) = \chi^j(-1)\,\overline{G(\chi^j)} = -\overline{G(\chi^j)}$. Thus, by (4), M is purely imaginary and

$$(14)\qquad |G_{16}+\nu|^2 = (G_8+\nu)^2-M^2.$$

Thus, by (13), (14) and (6),

$$(15)\qquad M^2 = (p^{1/2}+R_6+Y+\nu)^2-(15p+\nu^2).$$

Since $\eta = 1$ by hypothesis, we have, upon expanding,

$$(16)\quad M^2 = -8p+2p^{1/2}(a_4+2a_8+\nu)+2R_6(2p^{1/2}+a_8+\nu)+2Y(p^{1/2}+R_6+\nu),$$

where we have evaluated R_6^2 and Y^2 using the formulae for R_6 and Y in § 2. By (16), (1) and (2),

$$(17)\qquad \pm N = A+BR_6+Y(C+DR_6),$$

where

$$A = p^{1/2}(a_4+2a_8+\nu+4a_{16}),\quad B = 2p^{1/2}+a_8+\nu,$$
$$C = p^{1/2}(1-\alpha)+\nu-\alpha a_{16}-\alpha(p^{1/2}-a_8)(a_4+p^{1/2})\,b_{16}/b_4\,b_8,$$

and

$$D = 1+\alpha(p^{1/2}-a_8)\,b_{16}/b_4\,b_8.$$

By (17), (1) and (3),

$$\begin{aligned}(18)\qquad N^2 &= (A+BR_6)^2+Y^2(C+DR_6)^2+2(A+BR_6)(C+DR_6)\,Y\\ &= 4(p+a_{16}^2+2a_{16}p^{1/2}-2b_{16}^2)(4p+2a_8p^{1/2}+p^{1/2}R_6-2\alpha p^{1/2}Y).\end{aligned}$$

Note now that $Q(R_6)$ has degree 2 over its subfield $Q(\sqrt{p})$ and that $R_6^2, A, B, C, D \in Q(\sqrt{p})$ and $Y^2 \in Q(R_6)$. However, $Y \notin Q(R_6)$, in view of (6) and the fact that $|Q(G_8):Q| = 8$ (see the proof of Theorem 5.2 in [2]). Thus we may equate coefficients of Y in (18) to obtain

$$(19)\qquad (A+BR_6)(C+DR_6) = -4\alpha p^{1/2}(p+a_{16}^2+2a_{16}p^{1/2}-2b_{16}^2).$$

Equating coefficients of R_6 in (19), we have

$$(20)\qquad AD = -BC.$$

If we expand in (20), multiply by $b_4 b_8$, and equate the rational terms, we obtain

$$\alpha p b_{16}(a_4+2a_8+v+4a_{16})$$
$$= (a_8+v)\{b_4 b_8(\alpha a_{16}-v)+\alpha b_{16}(p-a_4 a_8)\}+2p(\alpha-1)b_4 b_8+2\alpha p b_{16}(a_4-a_8).$$

Reducing (mod p), we have

$$(a_8+v)(\alpha a_{16}-v)\,b_4\,b_8 \equiv (a_8+v)\,\alpha b_{16}\,a_4\,a_8 \pmod p. \tag{21}$$

Assume that $a_8+v = np$ for some integer n. Since $a_8 \equiv -1 \pmod 4$, it follows that $|n| \geqslant 2$, and we obtain the contradiction

$$2p \leqslant |a_8+v| < |a_8|+p \leqslant a_8^2+p = 2p-2b_8^2 < 2p.$$

Thus it is permissible to cancel (a_8+v) from both sides of (21). Squaring both sides of (21) and using the fact that $a_8^2+2b_8^2 = a_4^2+b_4^2 = p$, we obtain

$$(\alpha a_{16}-v)^2 \equiv 2b_{16}^2 \pmod p. \tag{22}$$

The first two primes p for which (12) holds and $\eta = 1$ are 113 and 337. For $p = 113$, we have $a_{16} = -1$ and $|b_{16}| = 4$. Hence (22) cannot hold for $p = 113$, so

$$p \geqslant 337. \tag{23}$$

Since $2|b_{16}$, it follows from (22) that $(\alpha a_{16}-v)^2-2b_{16}^2 = 4np$ for some nonzero integer n. Thus,

$$4p \leqslant |(\alpha a_{16}-v)^2-2b_{16}^2| \leqslant a_{16}^2+2b_{16}^2+v^2+2|va_{16}| \leqslant p+v^2+2|va_{16}|. \tag{24}$$

First assume that $|a_{16}| \geqslant 15$. Then by (24),

$$4p \leqslant p+v^2+2a_{16}^2 < 3p+v^2,$$

so $p < v^2 \leqslant 225$, which contradicts (23). Now assume that $|a_{16}| < 15$. Since $a_{16} \equiv -1 \pmod 8$, we have $|a_{16}| \leqslant 9$. Then by (24), $4p \leqslant p+225+270$, which again contradicts (23). ∎

5. Nonexistence of difference sets when 2 is not a quartic residue.

THEOREM 2′. *Let p be a prime such that $p \equiv 1 \pmod{16}$ and 2 is not a quartic residue* (mod p). *Then neither H_{16} nor $H_{16} \cup \{0\}$ is a difference set.*

Proof. Whiteman ([5], pp. 409, 410) proved in this case that $H_{16} \cup \{0\}$ is not a difference set. Assume for the purpose of contradiction that H_{16} is a difference set. Then formulas (12)–(15) hold with $v = -1$. Since $\eta = -1$, (15) yields, upon expansion,

$$M^2 = -8p+2p^{1/2}(a_4+2a_8-1)-2R_6(1+a_8)+2Y(R_6-1+p^{1/2}). \tag{25}$$

By (25), (1) and (2),

$$\pm N = a+bR_6+S(c+dR_6), \tag{26}$$

where

$$a = p^{1/2}(a_4+2a_8-1+4a_{16}), \quad b = -1-a_8,$$
$$c = -p^{1/2}-a_{16}+(a_8-p^{1/2})(a_4+p^{1/2})b_{16}/b_4 b_8-\alpha(1+p^{1/2})(a_4+p^{1/2})/b_4,$$

and

$$d = (p^{1/2}-a_8)b_{16}/b_4 b_8+\alpha(a_4+1)/b_4.$$

By (26) and (3),

$$N^2 = (a+bR_6)^2+S^2(c+dR_6)^2+2(a+bR_6)(c+dR_6)S \tag{27}$$
$$= 4(p+a_{16}^2+2a_{16}p^{1/2}-2b_{16}^2)(4p+2a_8 p^{1/2}+p^{1/2}R_6-2p^{1/2}S).$$

By the argument used to obtain (19), we may equate coefficients of S in (27) to obtain

$$(a+bR_6)(c+dR_6) = -4p^{1/2}(p+a_{16}^2+2a_{16}p^{1/2}-2b_{16}^2). \tag{28}$$

Equating coefficients of R_6 in (28), we have

$$ad = -bc. \tag{29}$$

In view of the assumption that H_{16} is a difference set, it follows from [5], p. 409, that $a_4 = -1$, $a_8 = -1+b_8^2$, and $p = 1+b_8^4 = 1+b_4^2$. We have $b_4 = \delta b_8^2$ for some $\delta = \pm 1$. Thus, after expanding in (29), multiplying by $b_4 b_8$, and comparing the irrational terms, we find that

$$a_8 b_{16}(a_4+2a_8-1+4a_{16}) \tag{30}$$
$$= (-1-a_8)(-b_4 b_8+b_8^2 b_{16}) = b_8^4(\delta b_8-b_{16}).$$

Since $(a_8, b_8) = 1$, it follows that

$$a_8|(b_{16}-\delta b_8). \tag{31}$$

First suppose that $b_{16}-\delta b_8 = 0$. Then by (30), $a = 0$, so by (29), $a = c = 0$. Then the left side of (28) is

$$bdR_6^2 = -(p^{1/2}-a_8)(2p-2p^{1/2}).$$

Comparing the rational terms in (28), we thus obtain

$$-(2pa_8+2p) = 8a_{16}p,$$

and so $-b_8^2 = 4a_{16}$. But since $0 = a = p^{1/2}(4a_{16}+2b_8^2-4)$, it follows that $0 = -b_8^2+2b_8^2-4$, so $b_8^2 = 4$. Then $p = 1+b_8^4 = 17$. However, H_{16} is not a difference set for $p = 17$, a contradiction.

Now suppose that $b_{16}-\delta b_8 \neq 0$. Then by (31), $a_8 \leqslant |b_{16}|+|b_8|$. Now,

$$a_8 = (p-1)^{1/2}-1, \quad |b_8| = (p-1)^{1/4}, \quad \text{and} \quad |b_{16}| < (p-1)^{1/2}/\sqrt{2}$$

(since $p > a_{16}^2+2b_{16}^2$), so

$$(1-1/\sqrt{2})(p-1)^{1/2}-(p-1)^{1/4}-1 < 0.$$

This forces $p < 318$. The only prime $p < 318$ satisfying $p = 1 + b_8^4$ is $p = 17$, which again yields a contradiction. ∎

References

[1] L. Baumert, *Cyclic difference sets*, Lecture Notes in Mathematics, 182, Springer-Verlag, Berlin 1971.

[2] B. Berndt and R. Evans, *Sums of Gauss, Jacobi, and Jacobsthal*, J. Number Theory (to appear in 1979).

[3] — — *Sums of Gauss, Eisenstein, Jacobi, Jacobsthal, and Brewer*, Illinois J. Math. 23 (1979), pp. 374–437.

[4] T. Storer, *Cyclotomy and difference sets*, Markham, Chicago 1967.

[5] A. Whiteman, *The cyclotomic numbers of order sixteen*, Trans. Amer. Math. Soc. 86 (1957), pp. 401–413.

Received on 30. 7. 1977
and in revised form on 23. 1. 1978 (967)

ACTA ARITHMETICA
XXXVIII (1980)

Linear forms on abelian varieties over local fields

by

DANIEL BERTRAND (Palaiseau) and YUVAL FLICKER (Cambridge)

0. Introduction. Let A be a simple abelian variety of dimension d, defined over a number field F. Denote by End A the ring of endomorphisms of A. Assume that *A admits sufficiently many complex multiplications in the sense that the algebra* End $A \otimes \mathbf{Q}$ *is isomorphic to a totally imaginary quadratic extension K of a totally real field K_1, with* $[K_1 : \mathbf{Q}] = d$. For any field C, denote by A_C the set of C-rational points on the variety A. We shall study here linear forms in algebraic points of the (normalized) exponential map on A_C, when the field C is non-archimedean.

Lower bounds for linear forms in algebraic points of exponential maps are fundamental in the theory of diophantine approximations. Such studies were initiated by Baker, who obtained lower bounds for linear forms in (ordinary) logarithms by means of a new extrapolation technique (see, e.g. [1]). Masser [8] later showed that similar techniques can be applied so as to yield lower bounds in the case of an elliptic curve with complex multiplication. This corresponds to the case of an abelian variety A as above, with dimension $d = 1$. Masser's work was generalized by Masser [9] and Lang [7] to deal with arbitrary dimension d. A variant of the method, leading to sharper bounds, was then given by Coates and Lang [5], using a theorem of Ribet [11] on the degree of the division fields attached to rational points of A, and these bounds were subsequently improved by Masser [10].

Our object here is to establish a p-adic analogue of the main Masser–Coates–Lang theorem on linear forms in algebraic points on abelian varieties of complex multiplication type. In the elliptic case, such p-adic linear forms were studied by Bertrand [3]. An essential ingredient in the study of the higher dimensional case is a many variables p-adic version of the "Schwarz lemma" principle, which has recently been established by Robba [12]. However, Robba's result applies only for sufficiently well-distributed extrapolation sets. In order to check this hypothesis in our situation, we have been led to require (see § 6) that *the rational prime p splits completely in the totally real field K_1, and all primes of K_1 which lie above p have the same splitting type in K.* We assume this from now on. It is likely that our