ACTA ARITHMETICA
XLIX (1987)

Generalized Jacobsthal sums and sums of squares

by

R. A. Rankin (Glasgow)

Dedicated to Paul Erdős on his 75th birthday

1. Introduction and notation. It is well known that, for a prime $p \equiv 1 \pmod 4$, an explicit representation of p as a sum of two integral squares is given by formulae of Jacobsthal involving Legendre symbols, and there have been numerous generalizations of this result; see, for example, [2] and the references there given. In the present paper we are interested in sums of Jacobsthal type, in which the Legendre symbols are replaced by general Dirichlet characters on a finite field. In the special cases where these characters take values in the Gaussian field, representations of prime powers as sums of squares of rational integers are obtained.

Throughout p denotes an odd prime, k a positive integer, and we write

$$q = p^k \tag{1.1}$$

and denote by F_q the finite field of q elements, whose nonzero members form the cyclic group F_q^* of order $Q = q-1$, generated by the primitive element g.

The letters χ and ψ, with or without suffixes, denote multiplicative characters on F_q^*, extended to F_q by taking the value zero at 0. The abelian group of all such characters is cyclic, being generated by the primitive character χ_1, which is defined uniquely by the equation

$$\chi_1(g) = e^{2\pi i/Q}. \tag{1.2}$$

The principal (trivial) character is denoted by χ_0, and, for any character χ, we write $\delta(\chi) = 1$ or 0 according as χ is, or is not, χ_0.

In applications we shall be particularly interested in the real quadratic character η and the biquadratic character ε. Here $\eta = \chi_1^{Q/2}$ and is a generalization of the Legendre symbol, while ε is defined, when $q \equiv 1 \pmod 4$, to be $\chi_1^{Q/4}$, so that $\varepsilon(g) = i$. We note that, for $q \equiv \pm 1 \pmod 8$, $\eta(2) = 1$, so that $\varepsilon(2)$ is real.

For any positive integer m, R_m denotes the ring $\mathbf{Z}[\zeta_m]$ of integers in the cyclotomic field generated by

$$\zeta_m = e^{2\pi i/m}. \tag{1.3}$$

In particular, R_4 is the ring of Gaussian integers.

We take positive rational integers e and f satisfying

$$ef = Q = q-1 \tag{1.4}$$

and are interested in the sums

$$S(\varkappa, e; \chi, \psi) = \sum_x \bar{\chi}(x)\psi(x^e+g^\varkappa) \quad (\varkappa \in \mathbf{Z}). \tag{1.5}$$

Here $\sum_x$ denotes a summation over all $x \in \mathbf{F}_q$. We shall write $\sum_x^*$ to denote a sum over all $x \in \mathbf{F}_q^*$.

We are also interested in the following sums:

$$a_\varkappa(e; \chi, \psi) = \sum_{n=0}^{f-1} \bar{\chi}(g^n)\psi(g^{ne}+g^\varkappa) \quad (\varkappa \in \mathbf{Z}) \tag{1.6}$$

and

$$T(e, \mu; \chi, \psi) = \sum_{\varkappa=1}^{Q} S(\varkappa, e; \chi, \psi)\overline{S(\varkappa+\mu, e; \chi, \psi)} \quad (\mu \in \mathbf{Z}). \tag{1.7}$$

In particular, we write

$$T(e; \chi, \psi) = T(e, 0; \chi, \psi). \tag{1.8}$$

Complex conjugate quantities are denoted throughout by a bar.

When the characters χ and ψ are powers of ε, the sums (1.5) are Gaussian or rational integers, and this will enable us to express q as a sum of squares of rational integers.

2. Character sums.

THEOREM 1. *For $\mu \in \mathbf{Z}$, write*

$$\mu = e\lambda, \quad \varepsilon_\mu = 1 \quad \text{if} \quad e|\mu \quad \text{and} \quad \lambda = \varepsilon_\mu = 0 \quad \text{if} \quad e \nmid \mu. \tag{2.1}$$

Then

$$Q^{-2}T(e, \mu; \chi, \psi) = \{Q\delta(\psi)-1\}\psi(g^{-\mu})\delta(\chi) - \delta(\bar{\chi}\psi^e) + \varepsilon_\mu\{(q/f)-e\delta(\psi)\}\chi(g^\lambda)\bar{\psi}(g^{\lambda e})\delta(\chi^f).$$

Proof. We have, by (1.7),

$$\begin{aligned}
Q^{-2}T(e, \mu; \chi, \psi) &= Q^{-2}\sum_{\varkappa=1}^{Q}\sum_x\sum_y \bar{\chi}(x)\chi(y)\psi(x^e+g^\varkappa)\bar{\psi}(y^e+g^{\varkappa+\mu}) \\
&= Q^{-2}\sum_x\sum_y \bar{\chi}(x)\chi(y)\sum_n^* \psi(x^e+n)\bar{\psi}(y^e g^{-\mu}+n)\bar{\psi}(g^\mu) \\
&= Q^{-2}\bar{\psi}(g^\mu)\sum_x\sum_y \bar{\chi}(x)\chi(y)\Big\{\sum_z \psi(x^e-y^e g^{-\mu}+z)\bar{\psi}(z) - \psi(x^e y^{-e} g^\mu)\Big\} \\
&= Q^{-2}\bar{\psi}(g^\mu)\sum_x\sum_y \bar{\chi}(x)\chi(y)\sum_z^* \psi(1+z^{-1}[x^e-y^e g^{-\mu}]) - \delta(\bar{\chi}\psi^e) \\
&= Q^{-2}\bar{\psi}(g^\mu)\sum_{\substack{x \ y \\ x^e \neq y^e g^{-\mu}}}\sum \bar{\chi}(x)\chi(y)\{Q\delta(\psi)-1\} \\
&\quad + Q^{-1}\bar{\psi}(g^\mu)\sum_{\substack{x \ y \\ x^e = y^e g^{-\mu}}}\sum \bar{\chi}(x)\chi(y) - \delta(\bar{\chi}\psi^e) \\
&= \bar{\psi}(g^\mu)\{Q\delta(\psi)-1\}\delta(\chi) \\
&\quad + Q^{-2}\bar{\psi}(g^\mu)\{q-Q\delta(\psi)\}\sum_x\sum_y \bar{\chi}(x)\chi(y) - \delta(\bar{\chi}\psi^e),
\end{aligned}$$

where $x^e = y^e g^{-\mu}$ in the double sum. Hence, the left-hand side becomes

$$\bar{\psi}(g^\mu)\{Q\delta(\psi)-1\}\delta(\chi) - \delta(\bar{\chi}\psi^e) + \varepsilon_\mu Q^{-2}\{q-Q\delta(\psi)\}\bar{\psi}(g^\mu)\sum_y^*\sum_{n=1}^{e}\chi(g^{nf+\lambda}).$$

The result follows, since the double sum on the right is

$$Qe\chi(g^\lambda)\delta(\chi^f).$$

The theorem is of particular interest when

$$\chi^f = \chi_0 \tag{2.2}$$

and

$$\delta(\chi) = \delta(\psi) = \delta(\bar{\chi}\psi^e) = 0. \tag{2.3}$$

We then have

COROLLARY 1. *If (2.1)–(2.3) hold, then*

$$T(e, \mu; \chi, \psi) = \varepsilon_\mu Qqe\chi(g^\lambda)\psi(g^{-\lambda e}); \tag{2.4}$$

in particular,

$$T(e; \chi, \psi) = Qqe. \tag{2.5}$$

THEOREM 2. *For each* $\varkappa \in \mathbf{Z}$, $a_\varkappa(e; \chi, \psi) \in R_Q$. *Further, if* f *is even, then*

(i) $a_0 \neq 0$ *if, for some prime* p' *dividing* Q, $p' \nmid f-1$,

(ii) $a_\varkappa \neq 0$, *where* $0 < \varkappa < e$, *if, for some prime* p' *dividing* Q, $p' \nmid f$.

Proof. That $a_\varkappa \in R_Q$ is obvious. Write $\lambda = 1 - \zeta_Q$, in the notation of (1.3). Then, for each $n \in \mathbf{Z}$,

$$\zeta_Q^n \equiv 1 \pmod{\lambda},$$

and so (i) $a_0 \equiv f-1 \pmod{\lambda}$, and (ii) $a_\varkappa \equiv f \pmod{\lambda}$ for $0 < \varkappa < e$; note that $g^{ne}+1 = 0$ for $n = f/2$. The results follow, since the norm of λ is a product of positive powers of the primes dividing Q.

COROLLARY 2. *Let* χ *and* ψ *take values in the Gaussian ring* R_4, *and let* f *be even. Then* $a_0(e; \chi, \psi) \equiv 1 \pmod{(1-i)}$, *and* $a_\varkappa(e; \chi, \psi) \equiv 0 \pmod{(1-i)}$ *for* $0 < \varkappa < e$. *In particular*, $a_0(e; \chi, \psi) \neq 0$.

We now obtain some further properties of the numbers $a_\varkappa(e; \chi, \psi)$.

THEOREM 3. *Suppose that* $\chi^f = \chi_0$. *Then*

(i) $a_{\varkappa+me}(e; \chi, \psi) = \{\bar{\chi}(g)\psi(g^e)\}^m a_\varkappa(e; \chi, \psi) \quad (m \in \mathbf{Z})$, (2.6)

(ii) $a_\varkappa(e; \chi, \psi) = \psi(g^\varkappa) a_{-\varkappa}(e; \bar{\chi}\psi^e, \psi)$, (2.7)

(iii) $S(\varkappa, e; \chi, \psi) = e a_\varkappa(e; \chi, \psi)$, (2.8)

(iv) $a_\varkappa(e; \bar{\chi}, \bar{\psi}) = \overline{a_\varkappa(e; \chi, \psi)}$. (2.9)

Proof.

(i)
$$a_{\varkappa+me}(e; \chi, \psi) = \sum_{n=0}^{f-1} \bar{\chi}(g^n)\psi(g^{ne}+g^{\varkappa+me})$$
$$= \psi(g^{me}) \sum_{n=0}^{f-1} \bar{\chi}(g^n)\psi(g^{(n-m)e}+g^\varkappa)$$
$$= \{\bar{\chi}(g)\psi(g^e)\}^m \sum_{n=0}^{f-1} \bar{\chi}(g^{n-m})\psi(g^{(n-m)e}+g^\varkappa),$$

from which (2.6) follows.

(ii)
$$a_\varkappa(e; \chi, \psi) = \psi(1+g^\varkappa) + \sum_{m=1}^{f-1} \bar{\chi}(g^{f-m})\psi(g^{(f-m)e}+g^\varkappa)$$
$$= \psi(1+g^\varkappa) + \bar{\chi}(g^f)\psi(g^\varkappa) \sum_{m=1}^{f-1} \chi(g^m)\bar{\psi}^e(g^m)\psi(g^{me}+g^{-\varkappa})$$
$$= \psi(g^\varkappa) \sum_{m=0}^{f-1} \chi(g^m)\bar{\psi}^e(g^m)\psi(g^{me}+g^{-\varkappa})$$
$$= \psi(g^\varkappa) a_{-\varkappa}(e; \bar{\chi}\psi^e, \psi).$$

(iii) Put $x = g^r$ in (1.5) and write

$$r = mf + n \quad \text{where} \quad 0 \leqslant m < e \text{ and } 0 \leqslant n < f.$$

Then

$$S(\varkappa, e; \chi, \psi) = \sum_{r=0}^{Q} \bar{\chi}(g^r)\psi(g^{re}+g^\varkappa)$$
$$= \sum_{n=0}^{f-1} \sum_{m=0}^{e-1} \bar{\chi}(g^{mf+n})\psi(g^{ne}+g^\varkappa)$$
$$= e \sum_{n=0}^{f-1} \bar{\chi}(g^n)\psi(g^{ne}+g^\varkappa),$$

by (2.2).

Finally, (2.9) is obvious.

We immediately deduce

COROLLARY 3. *If* $\chi^f = \chi_0$, *then*

(2.10) $$|a_{\varkappa+me}(e; \chi, \psi)| = |a_\varkappa(e; \chi, \psi)| = |a_\varkappa(e; \bar{\chi}, \bar{\psi})| \quad \textit{for all } m \in \mathbf{Z},$$

and

(2.11) $$|a_\varkappa(e; \chi, \psi)| = |a_{-\varkappa}(e; \bar{\chi}\psi^e, \psi)|.$$

THEOREM 4. *Let* χ *and* ψ *satisfy* (2.2) *and* (2.3). *Then*

(2.12) $$\sum_{\varkappa=0}^{e-1} |a_\varkappa(e; \chi, \psi)|^2 = q,$$

and

(2.13) $$\sum_{\varkappa=0}^{e-1} a_\varkappa(e; \chi, \psi)\overline{a_{\varkappa+\nu}(e; \chi, \psi)} = 0 \quad \textit{if} \quad \nu \not\equiv 0 \pmod{e}.$$

Proof. (2.12) follows from (2.5), (2.8) and (2.10), while (2.13), follows from (2.4), (2.6) and (2.8). The theorem generalizes formulae involving Legendre symbols to be found in [3], for example.

THEOREM 5. *Let* $Q = ef$, *where* $e = e_1 e_2$ *and* $e_1 f_1 = e_2 f_2 = Q$. *Then*

(2.14) $$\sum_{\nu=0}^{e_1-1} \bar{\chi}(g^\nu)\psi(g^{\nu e_2}) a_{\varkappa-\nu e_2}(e_1 e_2; \chi^{e_1}, \psi) = a_\varkappa(e_2; \chi, \psi).$$

Proof. The left-hand side of (2.14) is, by (1.6),

$$\sum_{n=0}^{f-1} \sum_{\nu=0}^{e_1-1} \bar{\chi}(g^{e_1 n+\nu})\psi(g^{e_2(e_1 n+\nu)}+g^\varkappa),$$

from which the result follows since $e_1 n + \nu$ runs from zero to

$$e_1(f-1)+e_1-1 = e_1 f - 1 = f_2 - 1.$$

COROLLARY 5. *Let* $Q \equiv 0 \pmod 4$. *Then*

$$a_\varkappa(4;\chi^2,\psi)+\bar\chi(g)\psi(g^2)a_{\varkappa-2}(4;\chi^2,\psi) = a_\varkappa(2;\chi,\psi).$$

3. $e=1$. In this case the character sums are Jacobi sums, which have been extensively discussed by various authors; see, for example, the early account [1], where examples are given for various values of p. Note also, that, when the characters take values in the Gaussian ring R_4, the relation $|a_0|^2 = q$ gives a representation of q as a sum of two rational integral squares.

4. $e=2$. We begin by proving a general result.

THEOREM 6. *Let* $c \in F_q^*$ *and put* $g^\gamma = -c^2$. *Then*

$$\bar\chi(2c)S(\gamma,2;\chi,\chi)$$

is real.

Proof. Let $C = F_q^* - \{c, -c\}$ and define

$$f(\lambda) = c\frac{\lambda+c}{\lambda-c} \quad (\lambda \in C).$$

It is easily verified that, if $\mu = f(\lambda)$, then $\lambda = f(\mu)$ and that f maps C bijectively onto itself. Moreover

$$\frac{\lambda^2-c^2}{2\lambda c} = \frac{2\mu c}{\mu^2-c^2}.$$

Hence

$$\bar\chi(2c)S(\gamma,2;\chi,\chi) = \sum_\lambda{}^* \chi\left(\frac{\lambda^2-c^2}{2\lambda c}\right)$$
$$= \sum_{\lambda\in C}\chi\left(\frac{\lambda^2-c^2}{2\lambda c}\right) = \sum_{\mu\in C}\chi\left(\frac{2\mu c}{\mu^2-c^2}\right)$$
$$= \sum_{\mu\in C}\bar\chi\left(\frac{\mu^2-c^2}{2\mu c}\right),$$

from which the theorem follows.

COROLLARY 6. *Let* $\chi^f = \chi_0 \neq \chi$. *Then*

(4.1) $\qquad a_\gamma(2;\chi,\chi)\bar\chi(2c)$ *is real.*

In particular,

(4.2) $\qquad \bar\chi(2)a_0(2;\chi,\chi)$ *is real if* $q \equiv 1 \pmod 4$,

and

(4.3) $\qquad \bar\chi(2c)a_1(2;\chi,\chi)$ *is real if* $q \equiv -1 \pmod 4$,

where $c = g^{(Q+2)/4} = g^{(f+1)/2}$.

Proof. (4.1) follows from the theorem and (2.8). To deduce (4.2), put $c = g^{Q/4}$, so that $-c^2 = -g^{Q/2} = 1$ and $\gamma = 0$; $\chi(c) = \pm 1$ since $c^2 = g^f$. For (4.3) take c as stated and note that $-c^2 = g$ and $\gamma = 1$.

As an example of (4.3) take

$$q=7,\quad g=3,\quad e=2,\quad f=3 \quad \text{and} \quad \chi(g)=\omega=e^{2\pi i/3}.$$

Then

$$a_0 = 1+2\omega^2,\quad a_1 = 2\omega,\quad \bar\chi(2g^2)=\bar\chi(2c)=\omega^2,$$

and

$$|a_0|^2+|a_1|^2 = 3+4 = 7.$$

If χ and ψ take real values only, and (2.2) and (2.3) hold, we must have $\chi(n)=\psi(n)=\eta(n)$. When $q=p$ this is the case considered by Jacobsthal and $\eta(n)$ is the Legendre symbol $\left(\frac{n}{p}\right)$.

We now consider the cases when χ and ψ take values in R_4 and are not both real. In order to satisfy (2.2) and (2.3) we must have $f \equiv 0 \pmod 4$, i.e. $q \equiv 1 \pmod 8$. There are only six possibilities, namely

$$\chi = \varepsilon^s,\quad \psi = \varepsilon^r,$$

where $s = 1$ or 3 and $r = 1, 2,$ or 3. When $s=3$, the sums $S(\varkappa,2;\chi,\psi)$ take conjugate complex values to their values for $s=1$, so that we may restrict our attention to the three cases

$$\chi=\varepsilon,\quad \psi=\varepsilon^r \quad (r=1,2,3),$$

which we consider in

THEOREM 7. *Let* $e=2$ *and* $f \equiv 0 \pmod 4$. *Then in each of the following three cases there exist integers* c *and* d, *with* c *odd, such that*

(i) $a_0(2;\varepsilon,\varepsilon) = c$, $a_1(2;\varepsilon,\varepsilon) = d(1-i)$,

(ii) $a_0(2;\varepsilon,\varepsilon^2) = c$, $a_1(2;\varepsilon,\varepsilon^2) = d(1+i)$,

(iii) $a_0(2;\varepsilon,\varepsilon^3) = c+id$, $a_1(2;\varepsilon,\varepsilon^3) = 0$.

Proof. (i) That a_0 is an odd integer follows from (4.2) and Corollary 2, since $\varepsilon(2)$ is real. Further, by (2.6) and (2.13),

$$0 = a_0\bar a_1 + a_1\bar a_2 = a_0\bar a_1 - ia_1\bar a_0 = a(\bar a_1 - ia_1),$$

so that $\bar a_1 = ia_1$. It follows that $a_1 = d(1-i)$, where $d \in \mathbf{Z}$.

(ii) We have

$$a_0 = \sum_{n=0}^{f-1} \bar{\varepsilon}(g^n)\varepsilon^2(g^{2n}+1) = \varepsilon^2(2) + \sum_{n=1}^{f-1} \bar{\varepsilon}(g^n)\varepsilon^2(g^{2n}+1).$$

In the last sum put $m = f-n$. Then, since $\varepsilon(g^2) = -1$,

$$\bar{\varepsilon}(g^n)\varepsilon^2(g^{2n}+1) = (-1)^m \bar{\varepsilon}(g^m)\varepsilon^2(g^{2m}+1).$$

Hence,

$$a_0 = \varepsilon^2(2) + 2\sum_{\lambda=1}^{(f/2)-1} (-1)^\lambda \varepsilon^2(g^{4\lambda}+1)$$

and so is a real Gaussian integer, which must be odd, by Corollary 2.

Further, by (2.7) and (2.6), $a_1 = -\overline{a_{-1}} = i\bar{a}_1$, so that $a_1 = d(1+i)$, where $d \in \mathbf{Z}$.

(iii) We have

$$a_1 = \sum_{n=0}^{f-1} \bar{\varepsilon}(g^n)\bar{\varepsilon}(g^{2n}+g)$$

$$= \bar{\varepsilon}(g+1) + \bar{\varepsilon}(g)\bar{\varepsilon}(g^2+g) + \sum_{n=2}^{f-1} \bar{\varepsilon}(g^n)\bar{\varepsilon}(g^{2n}+g).$$

Put $m = f+1-n$ in the last sum. Then

$$\varepsilon(g^n)\varepsilon(g^{2n}+g) = -\varepsilon(g^m)\varepsilon(g^{2m}+g),$$

from which it follows that $a_1 = 0$. Similarly, putting $m = f-n$, we deduce that

$$a_0 = \bar{\varepsilon}(2) + 2\sum_{n=1}^{(f/2)-1} \bar{\varepsilon}(g^n)\bar{\varepsilon}(g^{2n}+1) = c+id,$$

where c is odd and d is even, since $\varepsilon(2) = \pm 1$.

Note that, as a result of Theorem 7, we have representations of q, not as a real quaternary form, but as a binary form of the types c^2+2d^2 ($r = 1, 2$) and c^2+d^2 ($r = 3$). As examples we find that, for $p = q = 17$, we have

$$a_0 = -3,\quad a_1 = -2+2i;\qquad a_0 = 3,\quad a_1 = 2+2i;\qquad a_0 = 1+4i,\quad a_1 = 0,$$

in the three cases, respectively.

When $q = p^k$, where k is even, a trivial representation is given by taking one of the summands to be $p^{k/2}$ and the rest equal to zero. That this is not the only solution obtainable by sums of Jacobsthal type is shown by the case $q = 25$, $e = 2$, $\chi = \psi = \eta$, where we find $a_0 = 3$, $a_1 = 4$.

5. $e = 4$. (i) The classical real case arises when

$$\chi = \psi = \eta \quad \text{and} \quad q \equiv 1 \pmod 8,$$

so that f is even. From (2.6) and (2.7) we have

$$a_{\varkappa+4} = -a_\varkappa \quad \text{and} \quad a_\varkappa = (-1)^\varkappa a_{-\varkappa},$$

so that $a_1 = a_3$ and $a_2 = 0$. Hence

$$q = a_0^2+a_1^2+a_2^2+a_3^2 = a_0^2+2a_1^2.$$

(ii) We now take

$$q \equiv 1 \pmod{16} \quad \text{and} \quad \chi \in \varepsilon,\quad \psi = \varepsilon^r \quad (r = 1, 2, 3),$$

so that (2.2) and (2.3) are satisfied. From (2.6)

(5.1) $$a_{\varkappa+4} = -ia_\varkappa$$

and therefore, by Theorem 4,

$$|a_0|^2+|a_1|^2+|a_2|^2+|a_3|^2 = q,$$

and

$$a_0\bar{a}_1 + a_1\bar{a}_2 + a_2\bar{a}_3 + ia_3\bar{a}_0 = a_0\bar{a}_2 + a_1\bar{a}_3 + ia_2\bar{a}_0 + ia_3\bar{a}_1 = 0.$$

We deduce that $a_0\bar{a}_2 + a_1\bar{a}_3 = x(1-i)$, where x is real, and, by Corollary 2, $a_0 \equiv 1 \pmod{(1-i)}$, so that $a_0 \neq 0$.

For example, when $q = p = 17$, we have

$$a_0 = -1,\quad a_1 = 3-i,\quad a_2 = 2,\quad a_3 = -1-i,\quad x = -4 \quad (r = 1),$$
$$a_0 = -1,\quad a_1 = 1-i,\quad a_2 = 2i,\quad a_3 = 3+i,\quad x = 2 \quad (r = 3).$$

It may be verified by using (5.1) that these satisfy the formula

(5.2) $$a_\varkappa(4;\varepsilon,\varepsilon^r) = i^{\varkappa r}\,\overline{a_{-\varkappa}(4;\varepsilon,\varepsilon^{-r})} \quad (r = 1, 2, 3),$$

which follows from (2.7).

If we now take $r = 2$, we find from (5.2) that a_0 is real, and is therefore an odd rational integer, c say, while, since $a_2 = \bar{a}_{-2} = -i\bar{a}_2$, we find that $a_2 = (1-i)d$ ($d \in \mathbf{Z}$); further, $\bar{a}_3 = -ia_1$. Hence

$$q = |a_0|^2+|a_1|^2+|a_2|^2+|a_3|^2 = c^2+2d^2+2|a_1|^2.$$

In particular, for $p = q = 17$,

$$a_0 = 1,\quad a_1 = -2i,\quad a_2 = -2+2i,\quad a_3 = -2.$$

(iii) Finally, we take

$$q \equiv 1 \pmod{16},\quad \chi = \varepsilon^2,\quad \psi = \varepsilon,$$

so that (2.2) and (2.3) are satisfied. From Corollary 5 and Theorem 7(i) we find that

(5.3) $$a_0 + ia_{-2} = c,\quad a_1 + ia_{-1} = d(1-i),$$

so that, by (2.6) and (2.7),

(5.4) $$a_0 - ia_2 = c, \quad a_1 = b(1-i), \quad a_3 = b(1+i),$$

where $b \in \mathbf{Z}$. Further, (2.13) gives

(5.5) $$0 = a_0\bar{a}_2 + a_1\bar{a}_3 + a_2\bar{a}_4 + a_3\bar{a}_5 = a_0\bar{a}_2 - \bar{a}_0 a_2 - 4ib^2,$$

so that

(5.6) $$q = |a_0|^2 + |a_1|^2 + |a_2|^2 + |a_3|^2 = 4b^2 + |a_0|^2 + |a_2|^2 = c^2 + 8b^2,$$

since

$$c^2 = (a_0 - ia_2)(\bar{a}_0 + i\bar{a}_2) = |a_0|^2 + |a_2|^2 + i(a_0\bar{a}_2 - \bar{a}_0 a_2) = |a_0|^2 + |a_2|^2 - 4b^2,$$

by (5.5).

Thus q, which initially appeared to be expressed as a sum of eight squares, turns out to be expressible as a real binary quadratic form. As an illustration, we have for $q = 17$,

$$a_0 = -1-2i, \quad a_1 = -1+i, \quad a_2 = -2-2i, \quad a_3 = -1-i,$$

giving $b = -1$, $c = -3$.

References

[1] P. Bachmann, *Die Lehre von der Kreistheilung*, Leipzig 1872.

[2] Bruce C. Berndt and Ronald J. Evans, *Sums of Gauss, Jacobi and Jacobsthal*, J. Number Theory 11 (1979), pp. 349–396.

[3] Albert Leon Whiteman, *Cyclotomy and Jacobsthal sums*, Amer. J. Math. 74 (1952), pp. 89–99.

DEPARTMENT OF MATHEMATICS
UNIVERSITY OF GLASGOW
Glasgow G12 8QW, Scotland

Received on 6.9.1985 (1541)

ACTA ARITHMETICA
XLIX (1987)

On two analytic functions

by

K. Mahler (Canberra)

1. Denote by U: $|z| < 1$ the open unit disk in the complex z-plane, and by T an arbitrary closed subset of U. Next let $g \geq 2$ be a fixed integer, and let n run over all non-negative integers. Finally let

$$p(z) = p_0 + p_1 z + \ldots + p_d z^d,$$

where $d \geq 1$, be a polynomial with complex coefficients satisfying

$$p(0) = p_0 = 1 \quad \text{and} \quad p(1) = 0.$$

Hence $p(z)$ is divisible by $1-z$, say of the form

$$p(z) = (1-z)\,q(z),$$

where

$$q(z) = q_0 + q_1 z + \ldots + q_{d-1} z^{d-1}$$

is a second polynomial with complex coefficients such that

$$q(0) = q_0 = 1.$$

We shall use the notations

$$P = |p_0| + |p_1| + \ldots + |p_d| \quad \text{and} \quad Q = |q_0| + |q_1| + \ldots + |q_{d-1}|$$

for the sums of the absolute values of the coefficients of $p(z)$ and $q(z)$, respectively.

It is then obvious that

$$|p(z) - 1| \leq P - 1 \quad \text{and} \quad |q(z)| \leq Q \quad \text{for} \quad z \in U.$$

In these inequalities z may be replaced by z^{g^n} since with z also z^{g^n} belongs to the disk U. In fact, the following stronger inequality

$$|p(z^{g^n}) - 1| \leq (P-1)\,|z|^{g^n}$$

holds if $z \in U$, and n is any non-negative integer.