Bollettino U. M. I.
(5) **15**-B (1978), 717-723

Evaluation of Certain Jacobsthal Sums.

PHILIP A. LEONARD (Tempe, Arizona)
KENNETH S. WILLIAMS (Ottawa, Ontario) (*)

Sunto. – *I numeri primi* $q = 3, 5, 7, 11, 13, 17$ *e* 19 *sono esattamente quei numeri primi dispari per cui l'anello* $Z[\zeta]$, $\zeta = \exp(2\pi i/q)$ *è un dominio a fattorizzazione unica. Per tali numeri primi la somma di Jacobsthal*

$$\varphi_\varphi(a) = \sum_{x=0}^{p-1} \left(\frac{x}{p}\right)\left(\frac{x^q + a}{p}\right)$$

e la somma associata

$$\psi_\psi(a) = \sum_{x=0}^{p-1} \left(\frac{x^q + a}{p}\right)$$

(*dove* $(\cdot/p)$ *è il simbolo di Legendre per un numero primo* $p \equiv 1 \pmod q$ *ed* a *è un intero non divisibile per* p) *si esprimono in termini di opportuni fattori primi normalizzati di* p *in* $Z[\zeta]$. *I casi* $q = 3$ *e* 5 *sono già stati studiati da A. R. Rajwade.*

1. – Introduction.

Recently Rajwade [3], [4] has evaluated the character sums

$$\psi_q(a) = \sum_{x=0}^{p-1} \left(\frac{x^q + a}{p}\right),$$

where $(\cdot/p)$ is the Legendre symbol, for a prime $p \equiv 1 \pmod q$, a an integer not divisible by p, and $q = 3, 5$. In this paper we extend his results to evaluate these sums and the Jacobsthal sums

$$\phi_q(a) = \sum_{x=0}^{p-1} \left(\frac{x}{p}\right)\left(\frac{x^q + a}{p}\right)$$

(*) The research of both authors was supported by the National Research Council of Canada under Grant A-7233.

for the primes $q=3, 5, 7, 11, 13, 17$ and 19. These are precisely the odd primes q for which the ring $Z[\zeta]$, where $\zeta=\exp(2\pi i/q)$, is a unique factorization domain [2], and $\psi_q(a)$, $\varphi_q(a)$ are evaluated in terms of suitable normalized prime factors of p in $Z[\zeta]$.

Let p be a prime $\equiv 1 \pmod q$, where q is one of the primes listed above. If π is any prime factor of p in $Z[\zeta]$, we order its conjugates by setting $\pi_k=\sigma_k(\pi)$, $1\leqslant k\leqslant q-1$, where σ_k is the automorphism of $Q(\zeta)$ determined by $\sigma_k(\zeta)=\zeta^k$. If $(\cdot/\pi)$ is the q-th power character defined (for integers $y\not\equiv 0 \pmod p$) by $(y/\pi)_q=\zeta^\lambda$ if $y^{(p-1)/q}\equiv\zeta^\lambda \pmod \pi$, this ordering is such that $(y/\pi_k)_q=(y/\pi_1)_q^k$ for $1\leqslant k\leqslant q-1$. Finally we define, for $1\leqslant k\leqslant q-1$, $\bar k$ to be the unique integer such that $k\bar k\equiv 1 \pmod q$, $1\leqslant \bar k\leqslant q-1$. Our result is the following

THEOREM. – *Let q be one of 3, 5, 7, 11, 13, 17, 19, let p be a prime $\equiv 1 \pmod q$, and let a be an integer $\not\equiv 0 \pmod p$. Then, if π is any prime factor of p in $Z[\zeta]$ with $\pi\equiv -1 \pmod{(1-\zeta)^2}$, we have*

$$\psi_q(a)=(-1)^{q+1/2}\left(\frac{a}{p}\right)\sum_{l=1}^{(q-1)}\left(\frac{4a}{\pi_l}\right)_q\prod_{k=1}^{\frac12(q-1)}\pi_{lk} \tag{1.1}$$

and

$$\phi_q(a)=(-1)^{q+1/2}\sum_{l=1}^{q-1}\left(\frac{4\bar a}{\pi_l}\right)_q\prod_{k=1}^{\frac12(q-1)}\pi_{l\bar k}-1\ . \tag{1.2}$$

2. – Preliminary results.

We first prove three lemmas. Lemmas 1 and 2 are needed for the proof of Lemma 3. Lemmas 1 and 3 are used in the proof of the Theorem. (We emphasize that throughout this paper q is restricted to be one of 3, 5, 7, 11, 13, 17, 19 so that $Z[\zeta]$ is a U.F.D.)

LEMMA 1. – *If $\alpha\in Z[\zeta]$ is such that $\alpha\not\equiv 0 \pmod{(1-\zeta)}$, then α possesses an associate α' such that $\alpha'\equiv -1 \pmod{(1-\zeta)^2}$.*

PROOF. – For any $\varkappa\in Z[\zeta]$ we can define $(k_1,\dots,k_{q-1})\in Z^{q-1}$ uniquely by $\varkappa=k_1\zeta+\dots+k_{q-1}\zeta^{q-1}$. We define mappings $r_i\colon Z[\zeta]\to Z$ $(i=1,2)$ by

$$r_1(\varkappa)=k_1+\dots+k_{q-1}\,,\qquad r_2(\varkappa)=k_1+2k_2+\dots+(q-1)k_{q-1}\,; \tag{2.1}$$

so that

$$r_1(1)\equiv 1 \pmod q\,,\qquad r_2(1)\equiv 0 \pmod q\,.$$

It is easy to verify that

$$(2.2)\qquad \begin{aligned} r_i(\varkappa_1+\varkappa_2) &= r_i(\varkappa_1)+r_i(\varkappa_2)\,, && (\varkappa_1, \varkappa_2 \in Z[\zeta],\ i=1,2)\\ r_i(n\varkappa) &= nr_i(\varkappa)\,, && (\varkappa \in Z[\zeta],\ n\in Z,\ i=1,2)\end{aligned}$$

and that

$$(2.3)\quad r_1(\zeta\varkappa) \equiv r_1(\varkappa) \pmod q\,, \qquad r_2(\zeta\varkappa) \equiv r_1(\varkappa)+r_2(\varkappa) \pmod q\,.$$

From (2.3) it follows that for $l=0, 1, 2, \ldots$

$$(2.4)\qquad \begin{aligned} r_1(\zeta^l\varkappa) &\equiv r_1(\varkappa) \pmod q\,,\\ r_2(\zeta^l\varkappa) &\equiv lr_1(\varkappa)+r_2(\varkappa) \pmod q\,.\end{aligned}$$

From (2.2), (2.3), (2.4) it follows using the multinomial theorem (or by induction) that for $m=0,1,2,\ldots$

$$(2.5)\qquad \begin{aligned} r_1\big((1+\zeta)^m\varkappa\big) &\equiv 2^m r_1(\varkappa) \pmod q\,,\\ r_1\big((1+\zeta+\zeta^2)^m\varkappa\big) &\equiv 3^m r_1(\varkappa) \pmod q\,,\end{aligned}$$

and

$$(2.6)\qquad \begin{aligned} r_2\big((1+\zeta)^m\varkappa\big) &\equiv m2^{m-1}r_1(\varkappa)+2^m r_2(\varkappa) \pmod q\,,\\ r_2\big((1+\zeta+\zeta^2)^m\varkappa\big) &\equiv m3^m r_1(\varkappa)+3^m r_2(\varkappa) \pmod q\,.\end{aligned}$$

Thus from (2.4), (2.5), (2.6) we obtain for $l, m = 0, 1, 2, \ldots$

$$(2.7)\qquad \begin{aligned} r_1\big(\zeta^l(1+\zeta)^m\varkappa\big) &\equiv 2^m r_1(\varkappa) \pmod q\,,\\ r_1\big(\zeta^l(1+\zeta+\zeta^2)^m\varkappa\big) &\equiv 3^m r_1(\varkappa) \pmod q\,,\end{aligned}$$

and

$$(2.8)\qquad \begin{aligned} r_2\big(\zeta^l(1+\zeta)^m\varkappa\big) &\equiv (m2^{m-1}+l2^m)r_1(\varkappa)+2^m r_2(\varkappa) \pmod q\,,\\ r_2\big(\zeta^l(1+\zeta+\zeta^2)^m\varkappa\big) &\equiv (m3^m+l3^m)r_1(\varkappa)+3^m r_2(\varkappa) \pmod q\,.\end{aligned}$$

Now let $\alpha\in Z[\zeta]$ be such that $\alpha\not\equiv 0 \ \big(\mathrm{mod}\ (1-\zeta)\big)$ so that $r_1(\alpha)\not\equiv 0 \pmod q$. If $q=3, 5, 11, 13$, or 19, then 2 is a primitive root (mod q), and we can choose non-negative integers l and m such that

$$2^m r_1(\alpha)+1 \equiv 0 \pmod q\,,$$

$$(2l+m)r_1(\alpha)+2r_2(\alpha) \equiv 0 \pmod q\,,$$

so that by (2.2), (2.7), (2.8) we have

$$r_1(\zeta^l(1+\zeta)^m\alpha+1) \equiv r_2(\zeta^l(1+\zeta)^m\alpha+1) \equiv 0 \pmod{q},$$

so that $\alpha'+1 \equiv 0 \pmod{(1-\zeta)^2}$ where $\alpha' = \zeta^l(1+\zeta)^m\alpha$. α' is an associate of α as $1+\zeta$ is a unit of $Z[\zeta]$.

If $q=7$ or 17, then 3 is a primitive root (mod q), and we can choose positive integers l and m such that

$$3^m r_1(\alpha)+1 \equiv 0 \pmod{q},$$
$$(l+m)r_1(\alpha)+r_2(\alpha) \equiv 0 \pmod{q},$$

so that by (2.2), (2.7), (2.8) we have

$$r_1(\zeta^l(1+\zeta+\zeta^2)^m\alpha+1) \equiv r_2(\zeta^l(1+\zeta+\zeta^2)^m\alpha+1) \equiv 0 \pmod{q},$$

so that $\alpha'+1 \equiv 0 \pmod{(1-\zeta)^2}$ where $\alpha' = \zeta^l(1+\zeta+\zeta^2)^m\alpha$. α' is an associate of α as $1+\zeta+\zeta^2$ is a unit of $Z[\zeta]$.

This completes the proof of Lemma 1.

LEMMA 2. – *If* $\alpha, \beta \in Z[\zeta]$ *are such that*

(*a*) $\alpha\bar{\alpha} = \beta\bar{\beta}$,

(*b*) $\alpha, \beta \not\equiv 0 \pmod{(1-\zeta)}$,

(*c*) $\alpha \equiv \beta \pmod{(1-\zeta)^2}$,

(*d*) $\alpha \sim \beta$,

then

$$\alpha = \beta .$$

PROOF. – Any unit of $Z[\zeta]$ can be expressed in the form $\zeta^i r$, where $0 \leqslant i \leqslant q-1$ and r is a real number. Thus from (*d*) we have $\alpha = \zeta^i r\beta$. Using (*a*) we obtain $\alpha\bar{\alpha} = r^2\beta\bar{\beta} = r^2\alpha\bar{\alpha}$. Now (*b*) guarantees that $\alpha \neq 0$, so that $\alpha\bar{\alpha} \neq 0$, and we must have $r^2 = 1$, $r = \pm 1$, that is, $\alpha = \pm\zeta^i\beta$, $0 \leqslant i \leqslant q-1$. From (*b*) and (*c*) we have

$$(\pm\zeta^i - 1)\beta \equiv 0 \pmod{(1-\zeta)^2}, \quad \beta \not\equiv 0 \pmod{(1-\zeta)},$$

so that $\pm\zeta^i - 1 \equiv 0 \pmod{(1-\zeta)^2}$. As $i = 0, 1, \ldots, q-1$ this can only hold with the positive sign and $i = 0$, so that $\alpha = \beta$.

This completes the proof of Lemma 2.

Next let π be any prime of $Z[\zeta]$ dividing the rational prime $p \equiv 1 \pmod{q}$, and let $(\cdot/\pi)_q$ denote the corresponding q-th power character. We consider the Jacobi sums $J_\pi(k, l)$, where k, l are rational integers, defined by

$$J_\pi(k, l) = \sum_{\substack{x,y=0 \\ x+y\equiv 1 (\mathrm{mod}\ p)}}^{p-1} \left(\frac{x}{\pi}\right)_q^k \left(\frac{y}{\pi}\right)_q^l = \sum_{x=0}^{p-1} \left(\frac{x}{\pi}\right)_q^k \left(\frac{x+1}{\pi}\right)_q^l .$$

If none of $k, l, k+l$ is divisible by q, then ([1], p. 94)

$$J_\pi(k, l)\overline{J_\pi(k, l)} = p .$$

Moreover, an argument of Davenport-Hasse ([1], p. 153) shows that

$$J_\pi(k, l) \equiv -1 \pmod{(1-\zeta)^2} .$$

LEMMA 3. – *Let q be one of* 3, 5, 7, 11, 13, 17, 19, *and let p be a prime* $\equiv 1 \pmod q$. *Let π be any prime factor of p in $Z[\zeta]$ such that* $\pi \equiv -1 \pmod{(1-\zeta)^2}$. (*The existence of such a π is guaranteed by Lemma* 1; *indeed, there are infinitely many choices for π.*) *Set* $\pi_k = \sigma_k(\pi)$, $1 \leqslant k \leqslant q-1$, *so that* $p = \pi_1\pi_2 \dots \pi_{q-1}$. *Then for* $1 \leqslant l \leqslant q-1$ *we have*

$$J_\pi(l, l) = (-1)^{(q+1)/2} \prod_{k=1}^{\frac12(q-1)} \pi_{\bar{k}l} .$$

PROOF. – As $\sigma_l(\pi_s) = \pi_{ls}$ and $J_\pi(l, l) = \sigma_l(J_\pi(1, 1))$ it suffices to prove the result for $l = 1$. Now set

$$\alpha = J_\pi(1, 1) \qquad \text{and} \qquad \beta = (-1)^{(q+1)/2} \prod_{k=1}^{\frac12(q-1)} \pi_{\bar{k}} ,$$

so that $\alpha\bar{\alpha} = \beta\bar{\beta} = p$, $\alpha \equiv \beta \equiv -1 \pmod{(1-\zeta)^2}$. Next

$$\begin{aligned} \alpha = J_\pi(1, 1) &= \sum_{x=0}^{p-1} \left(\frac{x}{\pi}\right)_q^{k\bar{k}} \left(\frac{x+1}{\pi}\right)_q^{k\bar{k}} \\ &= \sum_{x=0}^{p-1} \left(\frac{x}{\pi_{\bar{k}}}\right)_q^{k} \left(\frac{x+1}{\pi_{\bar{k}}}\right)_q^{k} \\ &\equiv \sum_{x=0}^{p-1} x^{k(p-1)/q}(x+1)^{k(p-1)/q} \pmod{\pi_{\bar{k}}} . \end{aligned}$$

As $\sum_{x=0}^{p-1} x^n \equiv 0 \pmod p$ for $0 < n < p-1$ we have $\alpha \equiv 0 \pmod{\pi_{\bar{k}}}$ whenever $1 \leqslant k \leqslant \frac12(q-1)$. Thus, as $\alpha\bar{\alpha} = p$, we have $\alpha \sim \prod_{k=1}^{\frac12(q-1)} \pi_{\bar{k}}$, that is

$\alpha \sim \beta$. The result $\alpha = \beta$ now follows from Lemma 2 completing the proof of Lemma 3.

3. – Proof of the Theorem.

Let π be any prime of $Z[\zeta]$ dividing $p \equiv 1 \pmod q$ such that $\pi \equiv -1 \pmod{(1-\zeta)^2}$. Then

$$\sum_{x=0}^{p-1}\left(\frac{x^q+a}{p}\right) = \sum_{y=0}^{p-1}\left(\frac{y+a}{p}\right)\sum_{l=0}^{q-1}\left(\frac{y}{\pi}\right)_q^l . \tag{3.1}$$

Now if $F(z)$ is a complex-valued function of period p with $\sum_{z=0}^{p-1} F(z) = 0$ then we have

$$\sum_{y=0}^{p-1}\left(\frac{y+a}{p}\right)F(y) = \left(\frac{a}{p}\right)\sum_{z=0}^{p-1} F(4az(z+1)) , \tag{3.2}$$

as the number of solutions z of $4az(z+1) \equiv y \pmod p$ is $1 + (a(y+a)/p)$. Taking $F(y) = \sum_{l=0}^{q-1}(y/\pi)_q^l$ in (3.2), (3.1) becomes by Lemma 3

$$\begin{aligned}\psi_q(a) &= \left(\frac{a}{p}\right)\sum_{l=1}^{q-1}\left\{\sum_{z=0}^{p-1}\left(\frac{4az(z+1)}{\pi}\right)_q^l\right\}\\ &= \left(\frac{a}{p}\right)\sum_{l=1}^{q-1}\left(\frac{4a}{\pi}\right)_q^l J_\pi(l, l)\\ &= (-1)^{(q+1)/2}\left(\frac{a}{p}\right)\sum_{l=1}^{q-1}\left(\frac{4a}{\pi_l}\right)_q \prod_{k=1}^{\frac{1}{2}(q-1)} \pi_{l\bar{k}} ,\end{aligned}$$

which proves (1.1).

The transformation $x \to \bar{x}$ gives

$$\sum_{x=1}^{p-1}\left(\frac{ax^q+1}{p}\right) = \sum_{x=1}^{p-1}\left(\frac{x}{p}\right)^{q+1}\left(\frac{a\bar{x}^q+1}{p}\right) = \sum_{x=1}^{p-1}\left(\frac{x}{p}\right)\left(\frac{x^q+a}{p}\right)$$

so that

$$\begin{aligned}\varphi_q(a) &= \left(\frac{a}{p}\right)\sum_{x=0}^{p-1}\left(\frac{x^q+\bar{a}}{p}\right) - 1\\ &= (-1)^{(q+1)/2}\sum_{l=1}^{q-1}\left(\frac{4\bar{a}}{\pi_l}\right)_q \prod_{k=1}^{\frac{1}{2}(q-1)} \pi_{l\bar{k}} - 1 \qquad \text{(by (1.1))} ,\end{aligned}$$

which proves (1.2).

This completes the proof of the Theorem.

REFERENCES

[1] K. Ireland - M. I. Rosen, *Elements of number theory*, Bogden and Quigley, Tarrytown, New York, 1972.

[2] J. Myron Masley - Hugh L. Montgomery, *Cyclotomic fields with unique factorization*, J. Reine Angew. Math., **286/287** (1976), pp. 248-256.

[3] A. R. Rajwade, *On rational primes* p *congruent to* 1 (*mod* 3 *or* 5), Proc. Cambridge Philos. Soc., **66** (1969), pp. 61-70.

[4] A. R. Rajwade, *On the congruence* $y^2 \equiv x^5 - a \pmod{p}$, Proc. Cambridge Philos. Soc., **74** (1973), pp. 473-475.

Pervenuta alla Segreteria dell' U. M. I.
il 27 settembre 1977