ACTA ARITHMETICA
102.1 (2002)

Jacobi sums over finite fields

by

Paul van Wamelen (Baton Rouge, LA)

1. Definitions and notation. Let e be a positive integer, $e > 2$, and fix ζ_e, a primitive eth root of unity. Let $K = \mathbb{Q}(\zeta_e)$. Let p be a prime not dividing e and r an integer such that $p^r \equiv 1 \bmod e$. Let r_0 be the least positive integer such that $p^{r_0} \equiv 1 \bmod e$. Note that $r_0 \mid r$. Let $\mathbb{F}_q$ be the finite field with $q = p^r$ elements. Let γ be a generator of the cyclic group $\mathbb{F}_q^*$. Define a multiplicative character $\chi_e = \chi : \mathbb{F}_q^* \to \mathbb{Q}(\zeta_e)$ by $\chi(\gamma) = \zeta_e$. We extend it by $\chi(0) = 0$ to a map from $\mathbb{F}_q$ to $\mathbb{Q}(\zeta_e)$. For two integers m and n the Jacobi sum $J(\chi^m, \chi^n)$ is defined by

$$J(\chi^m, \chi^n) = \sum_{\alpha \in \mathbb{F}_q} \chi^m(\alpha)\chi^n(1-\alpha).$$

Note that some authors prefer to define the trivial character to have value 1 at 0, but in this paper we do not: if k is divisible by e we have $\chi^k(0) = 0$ (so our Jacobi sum is J^* of [6, p. 79]). The order of the Jacobi sum is the least common multiple of the orders of χ^m and χ^n. The dimension of the Jacobi sum is e.

2. Introduction. We will treat two important problems in the theory of Jacobi sums over finite fields. The first problem is that of giving a Diophantine system (of equations and congruences) whose unique solution determines a particular Jacobi sum. The other problem is that of giving algorithms for fast computation of Jacobi sums.

Up to a root of unity, the value of any Jacobi sum of two characters over a finite field is easy to describe and to compute. We give a method for finding the correct root of unity in all cases and show how this solves both problems above.

Starting with Gauss a lot of work has been done on finding Diophantine systems characterizing the coefficients (with respect to some basis of $\mathbb{Z}[\zeta_e]$)

2000 *Mathematics Subject Classification*: Primary 11T24; Secondary 11T22, 11Y40.
Key words and phrases: Jacobi sums, cyclotomic numbers, fast computation.

of Jacobi sums. At first all work on the problem dealt with one e at a time. See the notes on Chapter 3 in [6] for an excellent summary. The first work giving Diophantine systems for an infinite number of e was that of Evans. In [10] he gives Diophantine systems for the coefficients of Jacobi sums with e any power of 2, $m = 1$, $n = e/2$ and $r = 1$. In [1] Acharya and Katre give Diophantine systems for all e equal to a prime or twice a prime and any m, n and r, but with $r_0 = 1$.

Our main theorem (see Theorem 10) generalizes these results in that it allows any e, m, n, r and r_0.

Thaine [19] has also given an unrelated characterization of the cyclotomic numbers (and therefore the Jacobi sums) for any e, m and n, but $r = 1$. His characterization is not given as a Diophantine system but is given in terms of a system of Diophantine equations and the irreducibility of a certain polynomial.

The problem of giving algorithms for fast computation of Jacobi sums has a much shorter history. It became of much more interest when it was realized that such algorithms are applicable to primality testing and cryptosystems. See [2], [15], [8] and [21].

In fact we will not contribute to the speed of these algorithms, but we will show how to recursively reduce the problem of computing *all* Jacobi sums to the known computations. We show how to compute any of the Jacobi sums treated in our main theorem, faster than just naively summing the defining series, in the case where q is greater than $\phi(e)^{\phi(e)}$.

3. Known results on Jacobi sums. The following theorems are well known. We only state what we need; for other results see [6].

THEOREM 1. (1) *If both m and n are congruent to zero modulo e, then $J(\chi^m, \chi^n) = q - 2$.*

(2) *If exactly one of m and n is congruent to zero modulo e, then we have $J(\chi^m, \chi^n) = -1$.*

(3) *If m is nonzero modulo e and $m + n$ is congruent to zero modulo e, then $J(\chi^m, \chi^n) = -\chi^m(-1)$.*

Proof. See [6, Theorem 2.1.1] but recall that our Jacobi sums are called J^* in [6]. See the note above [6, Theorem 2.5.1]. ∎

THEOREM 2. *If e does not divide any of m, n, or $m + n$, then*

$$|J(\chi^m, \chi^n)| = q^{1/2}.$$

Proof. This is a well-known consequence of the expression of a Jacobi sum in terms of Gauss sums. See [6, Theorem 2.1.3]. ∎

Recall that r_0 is the least positive integer such that $p^{r_0} \equiv 1 \bmod e$. Let $q_0 = p^{r_0}$ and $f_0 = (q_0 - 1)/e$. Let $\mathfrak{p}$ be a prime ideal in $\mathbb{Z}[\zeta_e]$ above the

prime p. Let $\chi_{\mathfrak{p}}$ be the power residue character from $\mathbb{Z}[\zeta_e]/\mathfrak{p}$ to $\mathbb{Q}(\zeta_e)$, that is, for $\alpha \in \mathbb{Z}[\zeta_e]$, $\alpha \notin \mathfrak{p}$, $\chi_{\mathfrak{p}}(\alpha + \mathfrak{p}) = \zeta_e^k$ where ζ_e^k is the unique power of ζ_e such that

$$\zeta_e^k \equiv \alpha^{(q_0-1)/e} \bmod \mathfrak{p}.$$

See [6] or [11, Proposition 14.2.1].

Let E be the multiplicative group of reduced residues modulo e. For $k \in E$ let $\sigma_k \in \mathrm{Gal}(K/\mathbb{Q})$ be such that $\sigma_k(\zeta_e) = \zeta_e^k$, and define $\mathfrak{p}_k$ to be $\sigma_k(\mathfrak{p})$. Let D denote a set of coset representatives of the multiplicative quotient group

$$E/\{1, p, p^2, \ldots, p^{r_0-1}\}.$$

If we want to make the dependence of D on e explicit, we will write D_e. Note that D has $\phi(e)/r_0$ elements and recall that

$$p\mathbb{Z}[\zeta_e] = \prod_{k \in D} \mathfrak{p}_k. \tag{1}$$

For any integer $c \not\equiv 0 \bmod e$, let $L(c)$ denote the least positive integer congruent to c mod e. For any power $q = p^r$ of q_0 let $f = (q-1)/e$ and write the base p expansion of $L(c)f$ as

$$L(c)f = c_0 + c_1 p + \ldots + c_{r-1}p^{r-1}, \qquad 0 \le c_i < p.$$

Define

$$s_{e,q}(c) = c_0 + c_1 + \ldots + c_{r-1}.$$

THEOREM 3. *Let m, n and $m+n$ be integers not divisible by e. Then*

$$J(\chi_{\mathfrak{p}}^m, \chi_{\mathfrak{p}}^n)\mathbb{Z}[\zeta_e] = \prod_{k \in D} \mathfrak{p}_{k^{-1}}^{r_0 + (s_{e,q_0}(mk+nk) - s_{e,q_0}(mk) - s_{e,q_0}(nk))/(p-1)},$$

where k^{-1} is taken modulo e.

Proof. This is [6, Corollary 11.2.4]. ∎

If γ is a generator of $\mathbb{F}_q^*$, then $\gamma^{(q-1)/(q_0-1)}$ is a generator of $\mathbb{F}_{q_0}^*$. Let $\gamma_0 = \gamma^{(q-1)/(q_0-1)}$. We define a multiplicative character $\overline{\chi} : \mathbb{F}_{q_0} \to \mathbb{Z}[\zeta_e]$, by

$$\overline{\chi}(\gamma_0) = \zeta_e, \qquad \overline{\chi}(0) = 0.$$

THEOREM 4. *Let m, n and $m+n$ be integers not divisible by e. Then*

$$J(\chi^m, \chi^n) = (-1)^{r/r_0 - 1} J(\overline{\chi}^m, \overline{\chi}^n)^{r/r_0}.$$

Proof. Note that $N_{\mathbb{F}_q/\mathbb{F}_{q_0}}(\gamma) = \gamma^{(q-1)/(q_0-1)} = \gamma_0$, and so,

$$\chi(\alpha) = \overline{\chi}(N_{\mathbb{F}_q/\mathbb{F}_{q_0}}(\alpha)).$$

Therefore this theorem is just [6, Corollary 11.5.3]. ∎

4. The prime factorization of $J(\chi^m,\chi^n)$. Note that $\gamma^{(q-1)/e}$ is a primitive eth root of unity in $\mathbb{F}_q$ and as $e \mid p^{r_0}-1$ we see that $x^e-1 \mid x^{p^{r_0}-1}-1$, so that $\gamma^{(q-1)/e}$ is in fact in $\mathbb{F}_{q_0}$. As r_0 is the least positive integer such that $e \mid p^{r_0}-1$, $\mathbb{F}_{q_0} = \mathbb{F}_p(\gamma^{(q-1)/e})$. Let $\beta = \sum_{k=0}^{r_0} \beta_k x^k$, $\beta_{r_0} = 1$ be the minimal polynomial of $\gamma^{(q-1)/e}$ over $\mathbb{F}_p$. Let $B = \sum_{k=0}^{r_0} b_k x^k$ be a polynomial in $\mathbb{Z}[x]$ such that each of the b_k, when reduced modulo p, equals β_k.

LEMMA 1. *One, and only one, of the primes, $\mathfrak{p}$, above p in $\mathbb{Z}[\zeta_e]$ divides the ideal generated by $B(\zeta_e)$. The polynomial B can be chosen in such a way that $\mathfrak{p}$ divides $(B(\zeta_e))$ to only the first power.*

Proof. By what is sometimes called Kummer's Theorem, if Φ_e (the eth cyclotomic polynomial) factors as $\prod_{k=1}^{g} B_k$ modulo p then the primes above p in $\mathbb{Z}[\zeta_e]$ are given by the ideals $(p, B_k(\zeta_e))$ (see [14, Theorem 27] or [9, Theorem 4.8.13]). Clearly β is one of these B_k. For the second part of the theorem note that if $\mathfrak{p}^2$ divides $(B(\zeta_e))$ then only $\mathfrak{p}$ to the first power divides the ideal generated by $B(\zeta_e)+p$. ∎

The first part of this lemma generalizes Lemma 2 in [18]. For the rest of this paper, let $\mathfrak{p}$ be the prime given by the lemma.

LEMMA 2. *There exists an isomorphism $\theta : \mathbb{F}_{q_0} \to \mathbb{Z}[\zeta_e]/\mathfrak{p}$ such that*

$$\overline{\chi}(\gamma_0) = \chi_{\mathfrak{p}}(\theta(\gamma_0)).$$

Proof. As r_0 is the least positive integer such that $e \mid p^{r_0}-1$, we see that $\mathbb{F}_{q_0} \cong \mathbb{F}_p[x]/(\beta)$. As $\mathfrak{p}$ was chosen such that $\mathfrak{p} = (p, B(\zeta_e))$ we have

$$\mathbb{F}_{q_0} \cong \mathbb{F}_p[x]/(\beta) \cong \mathbb{Z}[x]/(p, \Phi_e, B) \cong \mathbb{Z}[\zeta_e]/\mathfrak{p}.$$

Let θ be this composition of isomorphisms. We see that θ maps $\gamma^{(q-1)/e}$ to ζ_e. Note that $\gamma_0^{(q_0-1)/e} = \gamma^{(q-1)/e}$. Applying θ we obtain $\theta(\gamma_0)^{(q_0-1)/e} = \zeta_e$. But, by the definition of $\chi_{\mathfrak{p}}$, this gives

$$\chi_{\mathfrak{p}}(\theta(\gamma_0)) = \zeta_e = \overline{\chi}(\gamma_0). \ ∎$$

THEOREM 5. *Let m, n and $m+n$ be integers not divisible by e. Then*

$$J(\chi^m,\chi^n)\mathbb{Z}[\zeta_e] = \prod_{k\in D} \mathfrak{p}_{k-1}^{r+(s_{e,q}(mk+nk)-s_{e,q}(mk)-s_{e,q}(nk))/(p-1)}.$$

Proof. Using Lemma 2 we can easily prove that $J(\overline{\chi}^m,\overline{\chi}^n) = J(\chi_{\mathfrak{p}}^m,\chi_{\mathfrak{p}}^n)$. Now Theorems 4 and 3 give

$$J(\chi^m,\chi^n)\mathbb{Z}[\zeta_e] = \prod_{k\in D} \mathfrak{p}_{k-1}^{r+\frac{r}{r_0}(s_{e,q_0}(mk+nk)-s_{e,q_0}(mk)-s_{e,q_0}(nk))/(p-1)}.$$

In order to complete the proof it will suffice to prove that

$$\frac{r}{r_0} s_{e,q_0}(c) = s_{e,q}(c) \tag{2}$$

for any $c \neq 0 \bmod e$. Note that

$$\frac{f}{f_0} = 1 + p^{r_0} + p^{2r_0} + \ldots + p^{r-r_0},$$

and $L(c)f_0 < p^{r_0}$. So we can easily write down the base p expansion of $L(c)f$ in terms of the base p expansion of $L(c)f_0$. Then (2) follows from the definition of s. ∎

5. The sum $I(m,n)$. We define a generalized Jacobi sum, $I(m,n)$, and see how it is related to the Jacobi sum $J(\chi^m, \chi^n)$.

Define the ring $\mathcal{R}$ by

$$\mathcal{R} = \mathbb{Z}[x]/(x^e - 1).$$

For $\alpha \in \mathbb{F}_q$, $\chi(\alpha) = \zeta_e^i$ for some integer i uniquely determined modulo e. So for any character $\chi : \mathbb{F}_q \to \mathbb{Q}(\zeta_e)$ we define a map $\chi_0 : \mathbb{F}_q \to \mathcal{R}$ by

$$\chi_0(\alpha) = x^i, \qquad \chi_0(0) = 0.$$

Let Φ_d be the dth cyclotomic polynomial. Note that, by mapping x to ζ_e, $\mathcal{R}/(\Phi_e(x))$ is isomorphic to $\mathbb{Z}[\zeta_e]$. We therefore have a canonical map,

$$\varrho : \mathcal{R} \to \mathbb{Z}[\zeta_e].$$

Note that $\chi = \varrho \circ \chi_0$ recovers the original character from χ_0.

Define the sum $I(m,n) \in \mathcal{R}$ to be

$$I(m,n) = \sum_{\alpha \in \mathbb{F}_q} \chi_0^m(\alpha)\chi_0^n(1-\alpha).$$

Then the Jacobi sum $J(\chi^m, \chi^n)$ is just $\varrho(I(m,n))$.

Conversely, we can recover $I(m,n)$ from the Jacobi sums of dimensions dividing e. For each positive divisor d of e let ζ_d be a primitive dth root of unity and let χ_d be the character that sends γ to ζ_d. For each positive divisor d of e let $J_d \in \mathbb{Z}[x]$ be a polynomial such that if we reduce modulo Φ_d and then identify x with ζ_d, we get $J(\chi_d^m, \chi_d^n)$.

In what follows we want to apply the Chinese Remainder Theorem to congruences modulo Φ_d for positive $d \,|\, e$. It is important to keep in mind that the Φ_d are only relatively prime in $\mathbb{Q}[x]$, not $\mathbb{Z}[x]$. So from now on it is important to distinguish between polynomials in $\mathbb{Z}[x]$ and polynomials in $\mathbb{Q}[x]$. Let $I_{m,n} \in \mathbb{Z}[x]$ be a polynomial of degree less than e such that if we consider $I_{m,n}$ as an element of $\mathcal{R}$ it equals $I(m,n)$. Note that

$$I_{m,n} \equiv J_d \bmod \Phi_d \quad \text{for all positive } d \,|\, e. \tag{3}$$

As $\prod_{d|e} \Phi_d = x^e - 1$ and the Φ_d generate relatively prime ideals in $\mathbb{Q}[x]$, the Chinese Remainder Theorem shows that $I_{m,n}$ is uniquely determined by (3).

THEOREM 6. *If* $I_{m,n} = \sum_{i=0}^{e-1} a_i x^i$ *then*

$$\sum_{i=0}^{e-1} a_i = q - 2,$$

and

$$\sum_{i=0}^{e-1} i a_i \equiv \begin{cases} 0 \bmod e & \text{if } e \text{ is odd,} \\ \frac{q-1}{2}(\gcd(m,e) + \gcd(n,e)) \bmod e & \text{if } e \text{ is even.} \end{cases}$$

Proof. Let $f = (q-1)/e$. Set $g_m = \gcd(m,e)$ and $g_n = \gcd(n,e)$. Now

$$\sum_{\alpha \in \mathbb{F}_q} (1 - \chi_0^m(\alpha))(1 - \chi_0^n(1-\alpha)) \equiv 0 \bmod (x-1)^2.$$

Multiplying out the argument of the sum and noting that the only values χ^k takes are powers of $\zeta_e^{\gcd(k,e)}$ and that each of these is taken the same number of times, we get

$$q - \sum_{i=0}^{e/g_m - 1} g_m f x^{i g_m} - \sum_{i=0}^{e/g_n - 1} g_n f x^{i g_n} + I(m,n) \equiv 0 \bmod (x-1)^2.$$

Or, considering this equation as an equation in $\mathbb{Z}[x]$, we have

$$q - \sum_{i=0}^{e/g_m - 1} g_m f x^{i g_m} - \sum_{i=0}^{e/g_n - 1} g_n f x^{i g_n} + \sum_{i=0}^{e-1} a_i x^i = P(x-1)^2 + Q(x^e - 1), \tag{4}$$

for some polynomials P and Q in $\mathbb{Z}[x]$. If we evaluate this equation at $x = 1$ we immediately get $\sum_{i=0}^{e-1} a_i = q - 2$. Differentiating (4) with respect to x, we get

$$- \sum_{i=0}^{e/g_m - 1} i g_m^2 f x^{i g_m - 1} - \sum_{i=0}^{e/g_n - 1} i g_n^2 f x^{i g_n - 1} + \sum_{i=0}^{e-1} i a_i x^{i-1} = P'(x-1)^2 - 2P(x-1) + Q'(x^e - 1) + Q e x^{e-1}.$$

Evaluation at $x = 1$ yields

$$-g_m^2 f \sum_{i=0}^{e/g_m - 1} i - g_n^2 f \sum_{i=0}^{e/g_n - 1} i + \sum_{i=0}^{e-1} i a_i = eQ(1).$$

So

$$\begin{aligned} \sum_{i=0}^{e-1} i a_i &= eQ(1) + f\frac{(e-g_m)e}{2} + f\frac{(e-g_n)e}{2} \\ &= eQ(1) + \frac{q-1}{2}(2e - g_m - g_n) \\ &= e(Q(1) + q - 1) - \frac{q-1}{2}(g_m + g_n). \end{aligned}$$

Note that if e is odd, then both g_m and g_n must be odd and so $g_m + g_n$ is even. Then, as $e \mid q-1$, the result follows. If e is even then p must be odd and so $-\frac{q-1}{2} \equiv \frac{q-1}{2} \bmod e$, and we are done. ∎

We want to show that if we know the J_d for $0 < d < e$, $d \mid e$ and we know J_e up to a root of unity, then this theorem can be used to find the correct root of unity. First we need some lemmas.

LEMMA 3. *Suppose t is a positive divisor of* $\operatorname{lcm}(2, e)$. *Let ζ_t be a primitive tth root of unity in $K = \mathbb{Q}(\zeta_e)$. Then*

$$N_{K/\mathbb{Q}}(\zeta_t - 1) = \begin{cases} l^{\phi(e)/\phi(t)} & \text{if } t \text{ is a power of the rational prime } l, \\ 1 & \text{if } t \text{ is not a prime power.} \end{cases}$$

Here ϕ is the Euler totient function.

Proof. For any $\alpha \in K$ define $n(\alpha) = N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha)$, and recall that $N_{K/\mathbb{Q}}(\alpha) = n(\alpha)^{[K:\mathbb{Q}(\alpha)]}$. By [6, Theorem 2.1.9]

$$n(\zeta_t - 1) = \begin{cases} l & \text{if } t \text{ is a power of } l, \\ 1 & \text{otherwise.} \end{cases}$$

But $[K : \mathbb{Q}] = \phi(e)$ and $[\mathbb{Q}(\zeta_t) : \mathbb{Q}] = \phi(t)$, and so the result follows. ∎

Define

$$\Psi_e = \prod_{d \mid e,\, 0 < d < e} \Phi_d.$$

Note that $\Psi_e \Phi_e = x^e - 1$ and that Ψ_e has degree $e - \phi(e)$.

LEMMA 4. *Let l be a rational prime dividing e; then $l^{\phi(e)/(l-1)}$ is the exact power of l dividing $N_{K/\mathbb{Q}}(\Psi_e(\zeta_e))$.*

Proof. We write

$$\Psi_e = \Big(\prod_{d \mid e/l} \Phi_d \Big) \Big(\prod_{d \mid e,\, d < e,\, d \nmid e/l} \Phi_d \Big) = (x^{e/l} - 1) \Big(\prod_{d \mid e,\, d < e,\, d \nmid e/l} \Phi_d \Big).$$

From Lemma 3 we see that $N_{K/\mathbb{Q}}(\zeta_e^{e/l} - 1) = l^{\phi(e)/(l-1)}$. If d is such that $d \mid e$, $d < e$ and $d \nmid e/l$, then there exists some prime $l' \neq l$ such that $l' \mid e$ and $d \mid e/l'$. Then $\Phi_d \mid x^{e/l'} - 1$, and so, again by Lemma 3, $N_{K/\mathbb{Q}}(\Phi_d(\zeta_e))$ is relatively prime to l. ∎

Define e_0 to be the product of all the primes dividing e.

LEMMA 5. *$\Psi_e(\zeta_e)$ divides e_0 in $\mathbb{Z}[\zeta_e]$.*

Proof. Note that $\Psi_e = \prod_{d \mid e, d < e} \Phi_d$ divides

$$\prod_{l \text{ prime}, l \mid e} \prod_{d \mid e/l} \Phi_d = \prod_{l \text{ prime}, l \mid e} x^{e/l} - 1.$$

As $\zeta_e^{e/l}$ is a primitive lth root of unity, Lemma 3 says $\zeta_e^{e/l} - 1 \,|\, l$. The result follows. ∎

COROLLARY 1. *There exist polynomials S and G in $\mathbb{Z}[x]$ such that*

$$S\Psi_e + G\Phi_e = e_0.$$

Proof. This is just a restatement of the lemma. ∎

Let $e_2 = \operatorname{lcm}(e, 2)$ and assume i is an integer such that $0 \le i < e_2$. By the division algorithm in $\mathbb{Z}[x]$ define the polynomial $R \in \mathbb{Z}[x]$ to be the unique polynomial of degree less than $\phi(e)$ such that

$$R = \begin{cases} ((-x)^i - 1)SJ_e - Q\Phi_e & \text{if } e \text{ is odd,} \\ (x^i - 1)SJ_e - Q\Phi_e & \text{if } e \text{ is even,} \end{cases} \tag{5}$$

for some $Q \in \mathbb{Z}[x]$ (and S as in the corollary).

Define

$$I_{m,n,i} = I_{m,n} + \frac{1}{e_0} R\Psi_e. \tag{6}$$

THEOREM 7. *$I_{m,n,i}$ is the unique polynomial in $\mathbb{Q}[x]$ of degree less than e such that*

$$I_{m,n,i} \equiv \begin{cases} (-x)^i J_e \bmod \Phi_e & \textit{if } e \textit{ is odd,} \\ x^i J_e \bmod \Phi_e & \textit{if } e \textit{ is even,} \end{cases}$$

and

$$I_{m,n,i} \equiv J_d \bmod \Phi_d \quad \textit{for all } d \,|\, e \textit{ with } 0 < d < e.$$

Proof. This follows directly from the definitions: By the Chinese Remainder Theorem there can be at most one such polynomial, so we only have to show that $I_{m,n,i}$ satisfies the conditions. But if e is odd then

$$\begin{aligned} I_{m,n,i} &= I_{m,n} + \frac{1}{e_0} R\Psi_e \\ &\equiv J_e + \frac{1}{e_0}((-x)^i - 1)J_e S\Psi_e \bmod \Phi_e \quad \text{(by (3) and (5))} \\ &\equiv J_e + J_e((-x)^i - 1) \bmod \Phi_e \quad \text{(by Corollary 1)} \\ &\equiv (-x)^i J_e \bmod \Phi_e. \end{aligned}$$

The case e even is similar. That $I_{m,n,i} \equiv J_d \bmod \Phi_d$ for $d < e$ follows from the fact that $\Phi_d \,|\, \Psi_e$, (6) and (3). ∎

Note that $I_{m,n,0} = I_{m,n}$.

THEOREM 8. *If $I_{m,n,i}$ has integer coefficients then either $i = 0$ or e is a power of a prime l and $e_2 \,|\, il$.*

Proof. Note that, as $I_{m,n} \in \mathbb{Z}[x]$, $I_{m,n,i}$ has integer coefficients if and only if all coefficients of $R\Psi_e$ are divisible by e_0. This in turn is true if and

only if all coefficients of R are divisible by e_0 (Ψ_e is monic). If all coefficients of R are divisible by e_0, then by reducing (5) modulo Φ_e, we see that

$$e_0 \,|\, (\zeta_{e_2}^i - 1)S(\zeta_e)J(\chi^m, \chi^n) \quad \text{in } \mathbb{Z}[\zeta_e]$$

where ζ_{e_2} is a primitive e_2th root of 1. Or, taking norms,

$$N_{K/\mathbb{Q}}(e_0) \,|\, N_{K/\mathbb{Q}}(\zeta_{e_2}^i - 1)N_{K/\mathbb{Q}}(S(\zeta_e))N_{K/\mathbb{Q}}(J(\chi^m, \chi^n)) \quad \text{in } \mathbb{Z}. \tag{7}$$

Now suppose that e has at least two distinct prime divisors. Then (for a given $i \neq 0$) by Lemma 3 we can find a rational prime l dividing e such that l is relatively prime to $N_{K/\mathbb{Q}}(\zeta_{e_2}^i - 1)$. Also l is relatively prime to $N_{K/\mathbb{Q}}(J(\chi^m, \chi^n))$ by Theorem 5. So we see that $N_{K/\mathbb{Q}}(l) = l^{\phi(e)}$ must divide $N_{K/\mathbb{Q}}(S(\zeta_e))$. Recall that $S(\zeta_e) = e_0/\Psi_e(\zeta_e)$ and by Lemma 4 the power with which l occurs in $N_{K/\mathbb{Q}}(\Psi_e(\zeta_e))$ is positive. This proves that if e has at least two distinct prime divisors, $I_{m,n,i}$ has integer coefficients only if $i = 0$.

Now suppose $e = l^a$ for some positive integer a. Then, as before, if l is relatively prime to $N_{K/\mathbb{Q}}(\zeta_{e_2}^i - 1)$, $I_{m,n,i}$ cannot have integer coefficients. Note that $\zeta_{e_2}^i$ is a primitive tth root of unity, where

$$t = \frac{e_2}{\gcd(i, e_2)}.$$

Only if t is a power of l, is $N_{K/\mathbb{Q}}(\zeta_{e_2}^i - 1)$ not relatively prime to l. In this case, as $S(\zeta_e) = e_0/\Psi_e(\zeta_e)$, we see that (7) only holds if the power of l dividing $N_{K/\mathbb{Q}}(\zeta_{e_2}^i - 1)$ is greater than or equal to the power of l dividing $\Psi_e(\zeta_e)$. That happens (by Lemma 3 and Corollary 1) only if

$$\frac{\phi(e)}{\phi(t)} \geq \frac{\phi(e)}{l-1},$$

that is, $t \leq l$, implying $e_2 \,|\, il$. ∎

THEOREM 9. *Let* $I_{m,n} = \sum_{k=0}^{e-1} a_k x^k$. *Suppose* $I_{m,n,i}$ *has integer coefficients and* $I_{m,n,i} = \sum_{k=0}^{e-1} a'_k x^k$. *Then*

$$\sum_{k=0}^{e-1} k a'_k \equiv \sum_{k=0}^{e-1} k a_k \bmod e,$$

only if $i = 0$.

Proof. For each d dividing e define, using the Chinese Remainder Theorem, a polynomial $T_d \in \mathbb{Q}[x]$ such that

$$T_d \equiv \begin{cases} 0 \bmod \Phi_{d_0} & \text{for all } d_0 \,|\, e,\ d_0 \neq d, \\ 1 \bmod \Phi_d. \end{cases}$$

Then

$$I_{m,n} \equiv \sum_{d|e} T_d J_d \bmod x^e - 1, \tag{8}$$

$$(9)\qquad I_{m,n,i} \equiv \begin{cases} (-x)^i T_e J_e + \sum_{d|e,\, d<e} T_d J_d \bmod x^e - 1 & \text{if } e \text{ is odd,} \\ x^i T_e J_e + \sum_{d|e,\, d<e} T_d J_d \bmod x^e - 1 & \text{if } e \text{ is even.} \end{cases}$$

Now assume that $I_{m,n,i}$ has integer coefficients and that i is not zero. Theorem 8 then shows that $e = l^b$ for some prime l and some positive integer b, and i is some multiple of e_2/l. If e is odd, then l is odd, but e_2 is even, and so i must be even. This shows that we can replace $(-x)^i$ by x^i. If $d \,|\, l^b$ and $d < l^b$, Φ_d divides $x^{e_2/l} - 1$, which divides $x^i - 1$. Also $\Phi_d T_d$ is divisible by $x^e - 1$. This shows that $x^e - 1$ divides $(x^i - 1)T_d$ and

$$T_d J_d \equiv x^i T_d J_d \bmod x^e - 1,$$

if $d < e$. And so

$$I_{m,n,i} \equiv x^i I_{m,n} \bmod x^e - 1.$$

Now, as the I's have integer coefficients and $x^e - 1$ is monic, we see that this implies that there exists a polynomial, Q, in $\mathbb{Z}[x]$ (not just $\mathbb{Q}[x]$) such that

$$I_{m,n,i} - x^i I_{m,n} = Q(x^e - 1).$$

Differentiating this with respect to x and substituting $x = 1$ we get

$$\sum_{k=0}^{e-1} k a'_k - i I_{m,n}(1) - \sum_{k=0}^{e-1} k a_k = eQ(1).$$

By Theorem 6, $I_{m,n}(1) = q - 2$ and this is congruent to -1 modulo e. As Q has integer coefficients we therefore have

$$\sum_{k=0}^{e-1} k a'_k - \sum_{k=0}^{e-1} k a_k \equiv -i \bmod e.$$

As noted before, if e is odd, i must be even, so if $i \equiv 0 \bmod e$ then $i \equiv 0 \bmod 2e$. As $i < 2e$ and i was assumed nonzero, this is a contradiction. If e is even, then $i < e$ and again we see i cannot be zero modulo e. ∎

Lemma 6. *Suppose j and d are divisors of e. Then*

$$\frac{x^e - 1}{x^j - 1} \equiv \begin{cases} \frac{e}{j} \bmod \Phi_d & \text{if } d \,|\, j, \\ 0 \bmod \Phi_d & \text{if } d \nmid j. \end{cases}$$

Proof. Suppose $d \,|\, j$. Then

$$\begin{aligned} \frac{x^e - 1}{x^j - 1} &= x^{e-j} + x^{e-2j} + \ldots + x^j + 1 \\ &\equiv \frac{e}{j} \bmod x^d - 1 \equiv \frac{e}{j} \bmod \Phi_d. \end{aligned}$$

On the other hand, if $d \nmid j$, then $\Phi_d \nmid x^j - 1$, but $\Phi_d \,|\, x^e - 1$, so Φ_d divides the quotient of $x^e - 1$ by $x^j - 1$. ∎

Define

$$\varepsilon_g(k) = \begin{cases} 1 & \text{if } g \mid k, \\ 0 & \text{if } g \nmid k. \end{cases}$$

Also let

$$\begin{aligned} g_m &= \gcd(e, m), & g_n &= \gcd(e, n), \\ g &= \gcd(e, m+n), & g_0 &= \gcd(g_m, g_n). \end{aligned}$$

We can now state and prove the main theorem.

THEOREM 10. *There is a unique polynomial $H \in \mathbb{Z}[x]$ such that $H(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_{e-1}x^{e-1}$ and the coefficients satisfy the following three conditions*:

(i) (a)

$$\sum_{j=0}^{e-1} a_j^2 = q + g_0 e f^2 - f(g_m + g_n + g), \tag{10}$$

(b) *for $k = 1, \ldots, e-1$*

$$\sum_{j=0}^{e-1} a_j a_{j-k} = \varepsilon_{g_0}(k) g_0 e f^2 - \varepsilon_{g_m}(k) f g_m - \varepsilon_{g_n}(k) f g_n - \varepsilon_g(k) f g$$

where we consider the subscripts of the a's modulo e.

(ii) *We have*

$$\sum_{k=0}^{e-1} k a_k \equiv \begin{cases} 0 \bmod e & \text{if } e \text{ is odd}, \\ \frac{q-1}{2}(g_m + g_n) \bmod e & \text{if } e \text{ is even}. \end{cases}$$

(iii) *For every d dividing e let $B_d \in \mathbb{Z}[x]$ be such that its reduction modulo p is the minimal polynomial of $\gamma^{(q-1)/d}$ over $\mathbb{F}_p$ and $\prod_{k \in D_d} B_d(\zeta_d^k)$ is not divisible by p^2 in $\mathbb{Z}[\zeta_d]$. Then $H(\zeta_d)$ must satisfy the following conditions*:

(a) *if none of m, n and $m+n$ are divisible by d, then*

$$q \mid H(\zeta_d) \prod_{k \in D_d} B_d(\zeta_d^{k^{-1}})^{(s_{d,q}(mk) + s_{d,q}(nk) - s_{d,q}(mk+nk))/(p-1)},$$

where k^{-1} is taken modulo d,

(b) *if $m \equiv -n \not\equiv 0 \bmod d$, then*

$$H(\zeta_d) = -\chi_d^m(-1),$$

(c) *if exactly one of m and n is divisible by d, then*

$$H(\zeta_d) = -1,$$

(d) *if both m and n are divisible by d, then*

$$H(\zeta_d) = q - 2.$$

If H is the unique polynomial satisfying these three conditions, then

$$H(\zeta_e) = J(\chi^m, \chi^n).$$

Proof. By (1) and Lemma 1, the condition that $\prod_{k\in D_d} B_d(\zeta_d^k)$ is not divisible by p^2 in $\mathbb{Z}[\zeta_d]$ is equivalent to $\mathfrak{p}^2$ not dividing the ideal generated by $B_d(\zeta_d)$. In particular, as pointed out in the proof of Lemma 1, it is always possible to find such B_d.

We will prove that $H = I_{m,n}$ is a unique solution to the three conditions stated. First we show that (i) is equivalent to (12) below.

Note that for $k = 0, 1, \ldots, e-1$,

$$\sum_{j=0}^{e-1} a_j a_{j-k}$$

is the coefficient of x^k in $H(x)H(x^{e-1})$ reduced modulo $x^e - 1$. Therefore (i) is equivalent to

$$H(x)H(x^{e-1}) \equiv g_0 ef^2 \frac{x^e-1}{x^{g_0}-1} - g_m f \frac{x^e-1}{x^{g_m}-1} - g_n f \frac{x^e-1}{x^{g_n}-1} - gf\frac{x^e-1}{x^g-1} + ef + 1 \bmod x^e - 1. \tag{11}$$

Suppose that $d \mid e$. If $d \mid m$ and $d \mid n$ then d divides g_0, g_m, g_n and g, so by Lemma 6, (11) implies

$$H(x)H(x^{e-1}) \equiv e^2f^2 - ef - ef - ef + ef + 1 = (ef-1)^2 = (q-2)^2 \bmod \Phi_d.$$

If $d \mid m$ but $d \nmid n$, then $d \nmid g_0$, $d \mid g_m$, $d \nmid g_n$, and $d \nmid g$, so again by Lemma 6, (11) implies

$$H(x)H(x^{e-1}) \equiv -ef + ef + 1 = 1 \bmod \Phi_d.$$

Similarly if $d \mid n$ but $d \nmid m$ or $d \mid m+n$ but $d \nmid m$, then

$$H(x)H(x^{e-1}) \equiv 1 \bmod \Phi_d.$$

Finally if d divides none of m, n or $m+n$ then d divides none of g_0, g_m, g_n or g and so

$$H(x)H(x^{e-1}) \equiv ef + 1 = q \bmod \Phi_d.$$

So we have shown that for every d dividing e,

$$H(\zeta_d)\overline{H(\zeta_d)} = \begin{cases} (q-2)^2 & \text{if } d \mid m \text{ and } d \mid n, \\ 1 & \text{if } d \text{ divides exactly one of } m,\ n \text{ or } m+n, \\ q & \text{if } d \text{ divides none of } m,\ n \text{ or } m+n, \end{cases} \tag{12}$$

where the bar denotes complex conjugation.

Conversely, this gives the value of $H(x)H(x^{e-1})$ modulo Φ_d for every $d \mid e$, so that it implies (11). Condition (i) is therefore equivalent to (12).

Assume we set $H = I_{m,n}$. Then, by Theorems 1 and 2, $H = I_{m,n}$ satisfies (i). By Theorem 6 it also satisfies (ii). If d does not divide m, n or $m+n$, then, by Theorem 5, Lemma 1 and the identity $\prod_{k\in D_d} \mathfrak{p}_k^r = q\mathbb{Z}[\zeta_d]$ we see that (iii)(a) holds. The other parts of (iii) hold by Theorem 1. So we see that there is at least one H satisfying (i)–(iii).

We will show, by induction, that if H satisfies the conditions of the theorem, then $H(\zeta_d) = J(\chi_d^m, \chi_d^n)$ for every $d \,|\, e$. For $d = 1$, (iii)(d) and Theorem 1(1) give

$$H(\zeta_1) = q - 2 = J(\chi_1^m, \chi_1^n).$$

Now fix some d with $d \,|\, e$. Let $H_d(x) = \sum_{j=0}^{d-1} b_j x^j$ and suppose that $H_d \equiv H \bmod x^d - 1$. Then if H satisfies the conditions of the theorem, then H_d satisfies the conditions of the theorem rewritten with H replaced by H_d and e replaced by d. For (i) this follows from the equivalence of (i) and (12). For condition (ii) it follows on noticing that $b_j = \sum_{k=0}^{e/d-1} a_{j+kd}$. Condition (iii) is clear.

Thus, to complete the induction it suffices to show that if $H(\zeta_d) = J(\chi_d^m, \chi_d^n)$ for all d such that $d \,|\, e$ and $d < e$, then $H(\zeta_e) = J(\chi^m, \chi^n)$.

If e divides any one of m, n or $m+n$ this follows immediately from (iii)(b), (c), (d). Now suppose e divides none of m, n or $m+n$. As we remarked, only $\mathfrak{p}$, to the first power, of all the primes above p in $\mathbb{Z}[\zeta_e]$ divides $(B_e(\zeta_e))$ so that (iii)(a) implies

$$\prod_{k\in D} \mathfrak{p}_{k^{-1}}^{r+(s_{e,q}(mk+nk)-s_{e,q}(mk)-s_{e,q}(nk))/(p-1)} \,|\, H(\zeta_e)\mathbb{Z}[\zeta_e].$$

By Theorem 5 there exists an (integral) ideal, $\mathfrak{a}$, such that $H(\zeta_e)\mathbb{Z}[\zeta_e] = J(\chi^m, \chi^n)\mathfrak{a}$. By Theorem 2 and (12) we get $\mathfrak{a}\overline{\mathfrak{a}} = \mathbb{Z}[\zeta_e]$. It follows that the ideals generated by $J(\chi^m, \chi^n)$ and $H(\zeta_e)$ are equal, or that there exists a unit $u \in \mathbb{Z}[\zeta_e]$ such that $H(\zeta_e) = uJ(\chi^m, \chi^n)$. By Theorem 2 and (12) this unit has absolute value 1. Then, by [6, Theorem 2.1.13], u must be some power of ζ_e if e is even and some power of $-\zeta_e$ if e is odd. In other words, by Theorem 7, we have shown that there exists an integer i such that $H = I_{m,n,i}$. As H has integer coefficients and satisfies (ii), Theorem 9 implies that $i = 0$, or $H = I_{m,n}$, as required. ∎

Some remarks:

1. Condition (i) of the theorem gives a system of Diophantine equations with only a finite number of solutions (clearly even (i)(a) has only a finite number of solutions). Conditions (ii) and (iii) then give congruence conditions ruling out all but one of the finite number of solutions. This unique solution gives the Jacobi sum.

2. Condition (i) can be seen as a generalization of [20, Proposition 1c)].

3. Of course (iii) takes the value of the primitive root γ into account. We therefore do not have any "sign ambiguities" as discussed by D. H. Lehmer [13] in his review of Whiteman's paper [22].

4. As mentioned by Lehmer in [13], "many problems in cyclotomy can tolerate these ambiguities" so that it is of interest to characterize the Jacobi sums up to the choice of γ (this turns out to be up to conjugacy). Can we replace our condition (iii) with a nicer condition if we allow these ambiguities? For the case of e being a prime or twice a prime and $r_0 = 1$ see condition (v) of the main theorem of [1].

5. Let $h = \gamma^{(q-1)/e}$. Then $h^{e/d} = \gamma^{(q-1)/d}$ and B_d is the minimal polynomial of $h^{e/d}$ over $\mathbb{F}_p$. Let r_d be the least positive integer such that $d \,|\, p^{r_d} - 1$. Then B_d modulo p has degree r_d, in fact $B_d(x)$ reduced modulo p is given by

$$\prod_{i=1}^{r_d} (x - h^{p^i e/d}).$$

As $h^e = 1$, we see that this expression only depends on p modulo e. In particular for all p with p fixed modulo e, the coefficients of B_d reduced modulo p are given by fixed polynomials in h.

6. Note that in (iii)(a) the divisibility condition requires divisibility in $\mathbb{Z}[\zeta_d]$, but q divides an algebraic integer in $\mathbb{Z}[\zeta_d]$ if and only if q divides all the coefficients of such an algebraic integer expressed as a linear combination of a $\mathbb{Z}$-basis of $\mathbb{Z}[\zeta_d]$. So this condition can be written as $\phi(d)$ divisibility conditions on linear combinations of the a_j. By the previous remark the coefficients, in turn, are polynomials in $h = \gamma^{(q-1)/e}$. So we see that, for fixed e, m, n and $p \bmod e$ our three conditions can be given as an explicit Diophantine system (of equations and congruences) in the variables a_1 to a_{e-1}, h and q. See the examples in the next section.

7. For a fixed e and q the cyclotomic numbers can be given in terms of the $J(\chi^m, \chi^n)$ (see [6, Theorem 2.5.1 and (11.6.5)]). So in a sense our theorem solves the main problem of cyclotomy by giving a Diophantine system characterizing the cyclotomic numbers. Of course much of the work that has been done on the cyclotomic problem involves reducing the number of variables by finding relations between different Jacobi sums. We have not touched this aspect of the problem. On the other hand if the title of a paper announces that it gives the cyclotomic numbers of a certain order it is usually done in terms of such a minimal set of variables, often with no Diophantine system satisfied by these variables given. So this work can be seen as complementing such a paper.

6. Examples of the main theorem

6.1. $e = 15$. Suppose $e = 15$, $m = n = 1$ and p is any prime such that $p \equiv 1 \bmod 15$. Then $r_0 = 1$; let $r = 1$ also. Let γ be a generator of the cyclic

group $\mathbb{F}_p^*$ and let h be an integer such that $h \equiv \gamma^{(p-1)/15}$ and $h^{15}-1$ is not zero modulo p^2. Then if $a_0, \ldots, a_{14}$ satisfy (i), (ii) of the theorem and the congruences below, $J(\chi,\chi) = \sum_{k=0}^{14} a_k \zeta_{15}^k$. Condition (iii)(a) with $d = 15$ turns into the following 8 congruences.

$$(h-h^2-h^3+h^4)a_0+(-1+h+h^2-h^3)a_4+(-1+h^2)a_5-a_6-h^2a_7-h^4a_8 + (1-h+h^3-h^4)a_9+(1-h+h^3-h^4)a_{10}+a_{11}+h^2a_{12}+h^4a_{13} + (-h^2+h^4)a_{14} \equiv 0 \bmod p,$$

$$(-h+h^3)a_0+(h-h^2-h^3+h^4)a_1+(1-h-h^2+h^3)a_4+(h-h^3)a_5+h^2a_6 +(-1+h^2)a_7+(-h^2+h^4)a_8+(-1+h-h^3)a_9+(-h+h^3-h^4)a_{11}+(1-h^2)a_{12} + (h^2-h^4)a_{13}+h^2a_{14} \equiv 0 \bmod p,$$

$$h^2a_0+(-h+h^3)a_1+(h-h^2-h^3+h^4)a_2+(1-h-h^2+h^3)a_5+(h-h^3)a_6+h^2a_7 +(-1+h^2)a_8+(-h^2+h^4)a_9+(-1+h-h^3)a_{10}+(-h+h^3-h^4)a_{12}+(1-h^2)a_{13} + (h^2-h^4)a_{14} \equiv 0 \bmod p,$$

$$(h-h^3)a_0+h^2a_1+(-h+h^3)a_2+(h-h^2-h^3+h^4)a_3+(-1+h+h^2-h^3)a_4 + (-1+h^2)a_5+(-h-h^2+h^3)a_6+(h-h^2-h^3)a_7+(h^2-h^4)a_8 +(-h+h^2+h^3-h^4)a_9+(1-h-h^2+h^3)a_{10}+(h-h^3)a_{11}+h^2a_{12}+(-h+h^3)a_{13} + (1-2h^2+h^4)a_{14} \equiv 0 \bmod p,$$

$$(1-h-h^2+h^3)a_0+(h-h^3)a_1+h^2a_2+(-h+h^3)a_3+(1-2h^2+h^4)a_4 +(h-h^3)a_5+h^2a_6+(-h+h^3)a_7+(h-h^2-h^3+h^4)a_8+(-1+h+h^2-h^3)a_9 + (-1+h^2)a_{10}+(-h-h^2+h^3)a_{11}+(h-h^2-h^3)a_{12}+(h^2-h^4)a_{13} + (-h+h^2+h^3-h^4)a_{14} \equiv 0 \bmod p,$$

$$(1-h-h^2+h^3)a_1+(h-h^3)a_2+h^2a_3+(-1+h^2)a_4+(-h^2+h^4)a_5 +(-1+h-h^3)a_6+(-h+h^3-h^4)a_8+(1-h^2)a_9+(h^2-h^4)a_{10}+h^2a_{11} + (-h+h^3)a_{12}+(h-h^2-h^3+h^4)a_{13} \equiv 0 \bmod p,$$

$$(1-h-h^2+h^3)a_2+(h-h^3)a_3+h^2a_4+(-1+h^2)a_5+(-h^2+h^4)a_6 +(-1+h-h^3)a_7+(-h+h^3-h^4)a_9+(1-h^2)a_{10}+(h^2-h^4)a_{11}+h^2a_{12} + (-h+h^3)a_{13}+(h-h^2-h^3+h^4)a_{14} \equiv 0 \bmod p,$$

$$(1-h-h^2+h^3)a_3+(1-h^2)a_4+a_5+h^2a_6+h^4a_7+(-1+h-h^3+h^4)a_8 + (-1+h-h^3+h^4)a_9-a_{10}-h^2a_{11}-h^4a_{12}+(h^2-h^4)a_{13} + (-h+h^2+h^3-h^4)a_{14} \equiv 0 \bmod p.$$

Condition (iii)(a) with $d = 5$ says that the following 4 congruences must hold:

$$(h^3+h^6)a_0-h^3a_1+h^3a_2+(-1-h^3)a_3+(1-h^6)a_4+(h^3+h^6)a_5-h^3a_6+h^3a_7 + (-1-h^3)a_8+(1-h^6)a_9+(h^3+h^6)a_{10}-h^3a_{11}+h^3a_{12}+(-1-h^3)a_{13} + (1-h^6)a_{14} \equiv 0 \bmod p,$$

$$(1+h^3)a_0+h^6a_1-a_3+(-h^3-h^6)a_4+(1+h^3)a_5+h^6a_6-a_8+(-h^3-h^6)a_9 + (1+h^3)a_{10}+h^6a_{11}-a_{13}+(-h^3-h^6)a_{14} \equiv 0 \bmod p,$$

$$a_1+(h^3+h^6)a_2+(-1-h^3)a_3-h^6a_4+a_6+(h^3+h^6)a_7+(-1-h^3)a_8-h^6a_9+a_{11} + (h^3+h^6)a_{12}+(-1-h^3)a_{13}-h^6a_{14} \equiv 0 \bmod p,$$

$$h^3a_0-h^3a_1+(1+h^3)a_2+(-1+h^6)a_3+(-h^3-h^6)a_4+h^3a_5-h^3a_6+(1+h^3)a_7 + (-1+h^6)a_8+(-h^3-h^6)a_9+h^3a_{10}-h^3a_{11}+(1+h^3)a_{12}+(-1+h^6)a_{13} + (-h^3-h^6)a_{14} \equiv 0 \bmod p.$$

Finally, (iii)(a) with $d = 3$ says that the following 2 congruences must hold:

$$(-1-h^5)a_0+a_1+h^5a_2+(-1-h^5)a_3+a_4+h^5a_5+(-1-h^5)a_6+a_7+h^5a_8 + (-1-h^5)a_9+a_{10}+h^5a_{11}+(-1-h^5)a_{12}+a_{13}+h^5a_{14} \equiv 0 \bmod p,$$

$$-a_0-h^5a_1+(1+h^5)a_2-a_3-h^5a_4+(1+h^5)a_5-a_6-h^5a_7+(1+h^5)a_8-a_9 - h^5a_{10}+(1+h^5)a_{11}-a_{12}-h^5a_{13}+(1+h^5)a_{14} \equiv 0 \bmod p.$$

Condition (iii)(d) is just

$$\sum_{k=0}^{14} a_k = p-2.$$

This example completes [7], [17] where the cyclotomic numbers of order 15 are given in terms of the coefficients of $J(\chi,\chi)$ and a few other variables, but where no Diophantine system is given for the coefficients of $J(\chi,\chi)$.

6.2. $e = 7$. We would like to give an example with $r_0 > 1$, but unfortunately the smallest nontrivial example occurs with $e = 7$ (see [4]), so this example is also rather big. Suppose $e = 7$, $m = n = 1$ and p is any prime such that $p \equiv 2 \bmod 7$. Then $r_0 = 3$; let $r = 3$ also. Let γ be a generator of the cyclic group $\mathbb{F}_{p^3}^*$ and set $h = \gamma^{(p^3-1)/7}$. Choose integers b_2 and b_1 such that

$$\overline{b}_2 = -h^4-h^2-h, \tag{13}$$

$$\overline{b}_1 = h^6+h^5+h^3, \tag{14}$$

$$0 \not\equiv b_2-b_1-1 \bmod p^2. \tag{15}$$

Then we can take $B_7(x) = x^3+b_2x^2+b_1x-1$. The integer b_2-b_1-1 in (15) is the coefficient of x^2 in $B_7(x)B_7(x^3)$ reduced modulo Φ_7, and so (15) ensures that $B_7(\zeta_7)$ is not divisible by the square of a prime above p in $\mathbb{Z}[\zeta_7]$.

If $a_0, \dots, a_6$ satisfy (i) and (ii) of the theorem and the congruences below, $J(\chi,\chi) = \sum_{k=0}^{6} a_k \zeta_7^k$.

Condition (iii)(a) with $d = 7$ requires that the following 6 congruences hold:

$$(-1+2b_1+3b_1^2+4b_2-2b_1b_2-b_2^2+b_1b_2^2)a_0+(-1-4b_1-b_1^2-2b_2-2b_1b_2-b_1^2b_2 +3b_2^2)a_1+(3+2b_1-b_1^3+b_2+2b_1b_2+b_1^2b_2-2b_2^2)a_2+(-3-b_1+b_1^2+b_1^3-b_2-2b_1b_2^2)a_3 + (2+b_1-b_1^2-b_2-2b_1^2b_2-b_2^2+2b_1b_2^2)a_4+(-3+b_1+b_2+2b_1^2b_2+b_2^2-b_2^3)a_5 + (3-b_1-2b_1^2-2b_2+2b_1b_2-b_1b_2^2+b_2^3)a_6 \equiv 0 \bmod p^3,$$

$$(2+b_1+b_1^2+2b_2-b_2^2+b_2^3)a_0+(-2-2b_1+2b_1^2+2b_2-4b_1b_2-b_1^2b_2+2b_2^2+b_1b_2^2)a_1 + (2-2b_1-b_1^2-b_1^3-b_2+b_2^2)a_2+(b_1+b_1^2+2b_1b_2+b_1^2b_2-2b_2^2-2b_1b_2^2)a_3 + (-1+b_1^3-2b_2-2b_1^2b_2-b_2^2)a_4+(-1+2b_1-b_1^2+2b_1b_2^2-b_2^3)a_5 + (-2b_1^2-b_2+2b_1b_2+2b_1^2b_2+b_2^2-b_1b_2^2)a_6 \equiv 0 \bmod p^3,$$

$$(-1+2b_1+b_1^2+3b_2+2b_1^2b_2)a_0+(1-3b_1-2b_1b_2-b_1^2b_2+2b_2^2+b_2^3)a_1 + (1+2b_1^2-b_1^3+3b_2-2b_1b_2+b_1b_2^2)a_2+(-1-3b_1-2b_2+b_2^2-2b_1b_2^2)a_3 + (2+2b_1-b_2+2b_1b_2-b_1^2b_2-3b_2^2)a_4+(-4+b_1+b_1^3-b_2-b_2^3)a_5 + (2+b_1-3b_1^2-2b_2+2b_1b_2+b_1b_2^2)a_6 \equiv 0 \bmod p^3,$$

$$(1+3b_1+2b_2-b_2^2+2b_1b_2^2)a_0+(-2-2b_1+b_2-2b_1b_2+b_1^2b_2+3b_2^2)a_1 + (4-b_1-b_1^3+b_2+b_2^3)a_2+(-2-b_1+3b_1^2+2b_2-2b_1b_2-b_1b_2^2)a_3 + (1-2b_1-b_1^2-3b_2-2b_1^2b_2)a_4+(-1+3b_1+2b_1b_2+b_1^2b_2-2b_2^2-b_2^3)a_5 + (-1-2b_1^2+b_1^3-3b_2+2b_1b_2-b_1b_2^2)a_6 \equiv 0 \bmod p^3,$$

$$(-2+2b_1+b_1^2+b_1^3+b_2-b_2^2)a_0+(-b_1-b_1^2-2b_1b_2-b_1^2b_2+2b_2^2+2b_1b_2^2)a_1 + (1-b_1^3+2b_2+2b_1^2b_2+b_2^2)a_2+(1-2b_1+b_1^2-2b_1b_2^2+b_2^3)a_3 + (2b_1^2+b_2-2b_1b_2-2b_1^2b_2-b_2^2+b_1b_2^2)a_4+(-2-b_1-b_1^2-2b_2+b_2^2-b_2^3)a_5 + (2+2b_1-2b_1^2-2b_2+4b_1b_2+b_1^2b_2-2b_2^2-b_1b_2^2)a_6 \equiv 0 \bmod p^3,$$

$$(1+4b_1+b_1^2+2b_2+2b_1b_2+b_1^2b_2-3b_2^2)a_0+(-3-2b_1+b_1^3-b_2-2b_1b_2-b_1^2b_2 +2b_2^2)a_1+(3+b_1-b_1^2-b_1^3+b_2+2b_1b_2^2)a_2+(-2-b_1+b_1^2+b_2+2b_1^2b_2+b_2^2-2b_1b_2^2)a_3 + (3-b_1-b_2-2b_1^2b_2-b_2^2+b_2^3)a_4+(-3+b_1+2b_1^2+2b_2-2b_1b_2+b_1b_2^2-b_2^3)a_5 + (1-2b_1-3b_1^2-4b_2+2b_1b_2+b_2^2-b_1b_2^2)a_6 \equiv 0 \bmod p^3.$$

As before (iii)(d) is just

$$\sum_{k=0}^{6} a_k = p^3 - 2.$$

It is tempting to plug (13) and (14) into these expressions, but it is important to lift to $\mathbb{Z}$ when we do and not right at the end.

7. Fast computation of Jacobi sums. Giving Diophantine conditions satisfied by the coefficients of Jacobi sums or the cyclotomic numbers are of a mostly theoretical interest. They certainly do not make it any easier to compute these entities. But the ideas used in this paper can in fact be used to compute some Jacobi sums faster than naively summing their defining series, in particular when q is much bigger than e. The point is that we can use lattice reduction techniques to quickly find the value of a Jacobi sum up to a root of unity and then we can use Theorem 9 to find the correct root of unity.

The central observation that makes this possible (apparently due to H. Lenstra) is the following. Note that

$$\mathfrak{q} = \prod_{k\in D} \mathfrak{p}_{k^{-1}}^{r+(s_{e,q}(mk+nk)-s_{e,q}(mk)-s_{e,q}(nk))/(p-1)}$$

is a principal ideal with $\lambda = J(\chi^m, \chi^n)$ as a generator, and that this generator has all its archimedean absolute values equal to $\sqrt{q}$. Let T be the trace from $\mathbb{Z}[\zeta_e]$ to $\mathbb{Z}$. If we think of $\mathfrak{q}$ as a free $\mathbb{Z}$-module then $T(a\overline{b})$, for a and b in $\mathfrak{q}$, defines a symmetric bilinear form. The corresponding quadratic form $T(a\overline{a})$ is clearly positive definite. So we can think of $\mathfrak{q}$ as a lattice ([9, Definition 2.5.2]).

As before, let σ_k, for any $k \in E$, be the embeddings of K into $\mathbb{C}$. The archimedean absolute values are then given by

$$|\alpha|_k = \sqrt{\sigma_k(\alpha)\overline{\sigma_k(\alpha)}}.$$

For any $\alpha \in \mathbb{Z}[\zeta_e]$ set $x_k = |\alpha|_k$ for every $k \in E$. We have $\mathfrak{q} = \lambda\mathbb{Z}[\zeta_e]$, so if $\beta = \lambda\alpha$ with $\alpha \in \mathbb{Z}[\zeta_e]$ is any element in the lattice $\mathfrak{q}$ we have

$$T(\beta\overline{\beta}) = \sum_{k\in E} |\lambda\alpha|_k^2 = q\sum_{k\in E} x_k^2.$$

Note that $\prod_{k\in E} x_k = N(\alpha)^2 \geq 1$, and under this constraint, the minimum of $\sum_{k\in E} x_k^2$ occurs when all $x_k = 1$. So we see that λ is a shortest vector in the lattice $\mathfrak{q}$ and that the other shortest vectors are λ multiplied by a root of unity in $\mathbb{Z}[\zeta_e]$. So we can find $J(\chi^m, \chi^n)$ up to a root of unity by finding a shortest vector in the lattice $\mathfrak{q}$.

First we need to compute a basis for $\mathfrak{q}$. This can be done by first decomposing p into prime ideals in the ring $\mathbb{Z}[\zeta_e]$ by factoring Φ_e modulo p, using (say) Berlekamp's algorithm (see [5] or [9, Section 3.4]). This takes probabilistic polynomial time, or deterministic polynomial time if the ERH is assumed. By Kummer's theorem [9, Theorem 4.8.13], [14, Theorem 27] such a factorization gives us two generators for each of the ideals above p. Using these it is an easy (and polynomial time) matter to find a $\mathbb{Z}$-basis for $\mathfrak{q}$ (see [9, Section 4.7.2]).

Finding shortest vectors in a lattice of fixed dimension can be done in polynomial time in the size of the input, that is, in our case, time polynomial

in $\log q$. The running time is exponential in the dimension of the lattice (something like $O(d^d)$, where $d = \phi(e)$ is the dimension of the lattice, see [12]). For a more detailed discussion and some notes on implementing a very similar algorithm [8] is recommended.

We can now recursively compute any Jacobi sum as follows. If $e = 1$, then by Theorem 1, the Jacobi sum is just $q - 2$. Now assume that we have already computed all the Jacobi sums $J(\chi_d^m, \chi_d^n)$ for all $d \mid e$ with $d < e$. Then we use the algorithm above to find $J(\chi^m, \chi^n)$ up to a root of unity, say given by J. Then for each i, $0 \le i < \operatorname{lcm}(e, 2)$, we can compute a polynomial $I_i \in \mathbb{Q}[x]$ of degree less than e such that

$$I_i(\zeta_e) = \begin{cases} (-\zeta_e)^i J & \text{if } e \text{ is odd,} \\ \zeta_e^i J & \text{if } e \text{ is even,} \end{cases}$$
$$I_i(\zeta_d) = J(\chi_d^m, \chi_d^n) \quad \text{if } d \mid e \text{ and } 0 < d < e.$$

This computation can be done by precomputing the polynomials T_d as in the proof of Theorem 9 (by finding the inverse of $(x^e - 1)/\Phi_d \bmod \Phi_d$ and multiplying by $(x^e - 1)/\Phi_d$) and then computing I_i similarly to (9).

By Theorem 9, for only one i, $0 \le i < \operatorname{lcm}(e, 2)$, will $I_i = \sum_{k=0}^{e-1} a_k x^k$ have integer coefficients and satisfy

$$\sum_{k=0}^{e-1} k a_k = \begin{cases} 0 \bmod e & \text{if } e \text{ is odd,} \\ \frac{q-1}{2}(g_m + g_n) \bmod e & \text{if } e \text{ is even.} \end{cases}$$

For this i we get $J(\chi^m, \chi^n) = \sum_{k=0}^{e-1} a_k \zeta_e^k$.

So we have seen that if q is on the order of $\phi(e)^{\phi(e)}$ or bigger, then the above algorithm will compute the Jacobi sum faster than just summing up its defining series. The algorithm was implemented in GP ([3]) and can compute Jacobi sums with $\phi(e) < 20$, $q < 10^{50}$ in less than 2 minutes. The case $e = 29$ and $q < 10^{20}$ also took about 2 minutes. The case $e = 90$, $p = 15217$ and $r = r_0 = 12$ took less than 15 seconds. These times could certainly be improved if we made use of the fact that $\mathfrak{p}$ itself is usually principal (see [8]). So we see that this algorithm gives a practical method for computing Jacobi sums with $\phi(e)$ up to about 30.

There is a lot of interest in computing Jacobi sums fast because of its application to primality testing (see [15], [16]). It should be noted though that for this application the Jacobi sum is only needed up to a root of unity and furthermore Jacobi sums over finite rings are also used. For an application to cryptosystems, see [8].

References

[1] V. V. Acharya and S. A. Katre, *Cyclotomic numbers of order* $2l$, l *an odd prime*, Acta Arith. 69 (1995), 51–74.

[2] L. M. Adleman, C. Pomerance and R. S. Rumely, *On distinguishing prime numbers from composite numbers*, Ann. of Math. (2) 117 (1983), 173–206.
[3] C. Batut, K. Belabas, D. Bernardi, H. Cohen, and M. Olivier, *User's Guide to PARI-GP*, 1997.
[4] L. D. Baumert, W. H. Mills, and R. L. Ward, *Uniform cyclotomy*, J. Number Theory 14 (1982), 67–82.
[5] E. R. Berlekamp, *Factoring polynomials over large finite fields*, Math. Comp. 24 (1970), 713–735.
[6] B. C. Berndt, R. J. Evans, and K. S. Williams, *Gauss and Jacobi Sums*, Wiley, New York, 1998.
[7] N. Buck, L. Smith, B. K. Spearman, and K. S. Williams, *The cyclotomic numbers of order fifteen*, Math. Comp. 48 (1987), 67–83. With microfiche supplement.
[8] J. Buhler and N. Koblitz, *Lattice basis reduction, Jacobi sums and hyperelliptic cryptosystems*, Bull. Austral. Math. Soc. 58 (1998), 147–154.
[9] H. Cohen, *A Course in Computational Algebraic Number Theory*, Grad. Texts in Math. 138, Springer, 1995.
[10] R. J. Evans, *Rational reciprocity laws*, Acta Arith. 39 (1981), 281–294.
[11] K. F. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, Springer, 1982.
[12] R. Kannan, *Minkowski's convex body theorem and integer programming*, Math. Oper. Res. 12 (1987), 415–440.
[13] D. H. Lehmer, *Review of "The cyclotomic numbers of order ten" by A. L. Whiteman*, Math. Reviews 22 (1961), 780.
[14] D. A. Marcus, *Number Fields*, Universitext, Springer, New York, 1977.
[15] P. Mihăilescu, *Cyclotomy of Rings & Primality Testing*, PhD thesis, Swiss Federal Institute of Technology, Zurich, 1997.
[16] —, *Cyclotomy primality proving—recent developments*, in: Algorithmic Number Theory (ANTS-III Proceedings), Springer, Berlin, 1998, 95–110.
[17] J. B. Muskat, *On Jacobi sums of certain composite orders*, Trans. Amer. Math. Soc. 134 (1969), 483–502.
[18] J. C. Parnami, M. K. Agrawal and A. R. Rajwade, *Jacobi sums and cyclotomic numbers for a finite field*, Acta Arith. 41 (1982), 1–13.
[19] F. Thaine, *Properties that characterize Gaussian periods and cyclotomic numbers*, Proc. Amer. Math. Soc. 124 (1996), 35–45.
[20] —, *On the coefficients of Jacobi sums in prime cyclotomic fields*, Trans. Amer. Math. Soc. 351 (1999), 4769–4790.
[21] P. van Wamelen, *On the CM character of the curves* $y^2 = x^q - 1$, J. Number Theory 64 (1997), 59–83.
[22] A. L. Whiteman, *The cyclotomic numbers of order ten*, in: Proc. Sympos. Appl. Math. 10, Amer. Math. Soc., Providence, RI, 1960, 95–111.

Department of Mathematics
Louisiana State University
Baton Rouge, LA 70803-4918, U.S.A.
E-mail: wamelen@math.lsu.edu

Received on 28.3.2000
and in revised form on 28.6.2001 (3787)