ACTA ARITHMETICA
LXII.3 (1992)

Lehmer's semi-symmetric cyclotomic sums

by

Andrew J. S. Lazarus (Davis, Calif.)

To the memory of Derrick Henry Lehmer

At the 1991 West Coast Number Theory Conference, Emma Lehmer asked for proofs of the formulas on semi-symmetric cyclotomic sums that appeared without proof in D. H. Lehmer's last notebook. This note is the result. Furthermore, we show how to determine signs which Lehmer had left ambiguous.

Classical cyclotomy defined the *cyclotomic classes* of degree e and prime conductor $p = ef + 1$ to be

$$\mathcal{C}_j^{(g)} = \{g^{et+j} \bmod p : t = 0, \ldots, f-1\}, \qquad j = 0, \ldots, e-1\,, \tag{1}$$

where g is any primitive root $\bmod p$. Here $\mathcal{C}_0^{(g)}$ contains the eth-power residues, but, as the notation emphasizes, the indexing of the other classes depends upon the choice of g. If $g' \in \mathcal{C}_k^{(g)}$ is another generator, then

$$\mathcal{C}_j^{(g')} = \mathcal{C}_{jk}^{(g)}\,. \tag{2}$$

(Indices are taken mod e here and throughout.)

The *Gaussian periods* are defined by

$$\eta_j = \sum_{h \in \mathcal{C}_j} \zeta_p^h, \qquad j = 0, \ldots, e-1\,,$$

where a choice of g has been fixed and $\zeta_p = \exp(2\pi i/p)$. The indexing of the periods other than η_0 also depends on g. By ζ_n we will always mean the specific root of unity $\exp(2\pi i/n)$.

The principal period $\eta_0 = \operatorname{Tr}_K^{\mathbb{Q}[\zeta_p]} \zeta_p$ where K is the unique field of conductor p and degree e over $\mathbb{Q}$. The other η_j, $j = 1, \ldots, e-1$, are its Galois conjugates.

Lehmer investigated the semi-symmetric functions of the periods

$$S_e(m,j)=\sum_{h=0}^{e-1}\eta_h^m\eta_{h+j}\,.$$

1. $e=3$**.** Since $p\equiv 1 \bmod 6$, we have the well-known decomposition $4p=L^2+27M^2$. We will use Hasse's normalization $L\equiv 2 \bmod 3$. We can specify how to choose M, and then impose a condition on the primitive root g used in (1), or we may choose g and then determine M from congruence conditions, but we cannot normalize both M and g in advance. The choices are tied together by the lemma:

Lemma 1 ([4, Proposition 1]). *Let g be an arbitrary primitive root* mod p *and let $\mathfrak{p}=(L+3\sqrt{3}iM)/2$ be a complex prime lying over p. Then the complex residue symbol*

$$\left(\frac{g}{p}\right)_3\overset{\text{def}}{\equiv} g^{(p-1)/3} \bmod \mathfrak{p}$$

is equal to ζ_3 if and only if

$$g^{(p-1)/3}\equiv(L+9M)/(L-9M) \bmod p\,. \tag{3}$$

Remark. A general procedure for obtaining results of this type for prime e appears in [4].

Theorem 2.

$$18S_3(2,j)=p(L+(-1)^j9M)-2,\qquad j=1,2\,, \tag{4}$$

where $L\equiv 2 \bmod 3$ and either

(a) *g is chosen so that*

$$\left(\frac{g}{\mathfrak{p}}\right)_3=\zeta_3,\qquad \mathfrak{p}=(L+3\sqrt{3}iM)/2,\qquad M>0\,, \tag{5}$$

or

(b) *g is arbitrary and M is such that* (3) *holds.*

Proof. Lehmer obtained a formula equivalent to (4), except his $L\equiv 1 \bmod 3$ (i.e., replace L by $-L$ in (4)) and $\pm M$ is undetermined. We will, however, give the proof *ab initio*, using Hasse [3, §1–2] and his normalization.

Assume normalization (a). The field $\mathbb{Q}[\zeta_p]$ contains as a subfield the unique cubic field K of conductor p. There are two cubic characters "belonging" to this field, and they coincide with the cubic residue symbols for the primes lying over p in $\mathbb{Q}[\zeta_3]$, viz., $\left(\frac{g}{\mathfrak{p}}\right)_3$ and $\left(\frac{g}{\overline{\mathfrak{p}}}\right)_3$. Let χ be the character associated with $\mathfrak{p}$ and let

$$t = -\tau(\chi) = -\sum_{j=0}^{p-1} \chi(j)\zeta_p^j \,,$$

the negative of the Lagrange resolvent (sometimes called a Gauss sum). Hasse wrote elements of K in the form $[x, y]$ with $x \in \mathbb{Q}$, $y \in \mathbb{Q}[\zeta_3]$, representing the number $(x + yt + \overline{y}\overline{t})/3$. Elements written in this form can be added coordinate-wise and multiplied according to the scheme

$$t\overline{t} = p, \qquad t^2 = \mathfrak{p}\overline{t} \,.$$

The resolvents $\tau(\chi)$ are connected to the Gaussian periods through the inversion relation

$$\eta_j = e^{-1} \sum_{h=0}^{e-1} \zeta_p^{-hj} \tau(\chi^h) \,, \tag{6}$$

which implies, since $\tau(\chi^3) =$ Möbius $\mu(p) = -1$, that

$$\eta_0 = [-1, -1], \qquad \eta_1 = [-1, -\zeta_3^{-1}], \qquad \eta_2 = [-1, -\zeta_3] \,.$$

The theorem follows from a calculation in Hasse's ordered pair basis which was implemented in the Maple computer algebra language.

The truth of the theorem for normalization (b) follows from the lemma. Normalize g and $\mathfrak{p}$ by (5). If, for arbitrary g', $\left(\frac{g'}{\mathfrak{p}}\right)_3 = \zeta_3$, the proof for normalization (a) holds with g replaced by g'. If not, then $\left(\frac{g'}{\overline{\mathfrak{p}}}\right)_3 = \zeta_3$, and (3) gives $M < 0$, i.e., the opposite normalization to (5). The negative value for M is correct in (4) because, from (2), $\mathcal{C}_j^{(g)} = \mathcal{C}_{3-j}^{(g')}$, and η_1 and η_2 are likewise exchanged. ■

2. $e = 4$**.** Because the Lehmers were interested in both cyclotomy and units, they considered only the real fields where $p \equiv 1 \bmod 8$. (The unit groups of the imaginary quartic fields are generated, up to torsion, by quadratic units.) Here we will use the normalization

$$p = a^2 + b^2, \qquad a \equiv 1 \bmod 4, \qquad b \equiv 0 \bmod 4 \,.$$

The analogue to Lemma 1 is:

LEMMA 3. *If g is a generator* $\bmod p$ *and* $\mathfrak{p} = a + bi$ *is a prime of* $\mathbb{Q}[i]$ *lying over* p, *then*

$$\left(\frac{g}{\mathfrak{p}}\right)_4 \overset{\text{def}}{=} g^{(p-1)/4} \bmod \mathfrak{p} = i \quad \textit{if and only if} \quad g^{(p-1)/4} \equiv \frac{a+b}{a-b} \bmod p \,.$$

Proof. Write G for $g^{(p-1)/4}$.

$$\left(\frac{g}{\mathfrak{p}}\right)_4 = i \Leftrightarrow \mathfrak{p} \mid G - i \Leftrightarrow p \mid \bar{\mathfrak{p}}(G - i)\,.$$

Considering real and imaginary parts gives $p \mid (aG - b)$ and $p \mid (a + bG)$, whence $G(a - b) \equiv (a + b) \bmod p$. Hence the lemma. ■

Remark. It is easy to see that $(a+b)/(a-b)$ and its reciprocal are the square roots of $-1 \bmod p$.

Theorem 4.

$$16S_4(2,j) = -1 - p(1 - 2a + (-1)^{(j-1)/2}4b), \qquad j = 1,3\,;$$
$$16S_4(2,2) = 2pa - p - 1\,;$$
$$64S_4(3,j) = 1 - 7p^2 + 6p - (-1)^{(j-1)/2}4bp(3 + a), \qquad j = 1,3\,;$$
$$64S_4(3,2) = -3p^2 + (6 - 4a^2)p + 1$$

where either

(a) *g is chosen so that*

$$\left(\frac{g}{\mathfrak{p}}\right)_4 = i, \qquad \mathfrak{p} = a + bi, \qquad b > 0\,,$$

or

(b) *g is arbitrary and b is such that $g^{(p-1)/4} \equiv (a + b)/(a - b) \bmod p$.*

Proof. These formulas appear in Lehmer's notebook up to sign. Assume normalization (a), which is from Hasse [3, §7–8]. Let χ be the character associated with $\mathfrak{p}$ belonging to the quartic field, and set t equal to the resolvent $\tau(\chi)$. Hasse wrote elements of the quartic field K of conductor p in the 4-tuple $[x_0, x_1, y_0, y_1]$, $x_i, y_i \in \mathbb{Q}$, representing the number

$$\tfrac{1}{4}(x_0 - x_1\sqrt{p} + (y_0 + iy_1)t + (y_0 - iy_1)\bar{t})\,.$$

Since $\tau(\chi^4) = \mu(p) = -1$ and Gauss showed that $\tau(\chi^2) = \sqrt{p}$, we have, from (6),

$$\eta_0 = [-1,-1,1,0], \qquad \eta_1 = [-1,1,0,-1],$$
$$\eta_2 = [-1,1,-1,0], \qquad \eta_3 = [-1,-1,0,1]\,.$$

Multiplication of elements in Hasse's basis is accomplished through the relations

$$t\bar{t} = p, \qquad t^2 = -\mathfrak{p}\sqrt{p}, \qquad \sqrt{p}t = -\mathfrak{p}\bar{t}\,.$$

This scheme was implemented in Maple and the various S_4's were calculated with the results shown in the theorem.

The truth of the theorem for normalization (b) proceeds from Lemma 3 in the same fashion as the end of the proof of Theorem 2. ■

Corollary 5. $S_4(3,1) = S_4(3,3) = -(7p+1)(p-1)$ *whenever* $a = -3$.

3. $e = 5$. Dickson [2] decomposed primes $p \equiv 1 \bmod 5$ as

$$16p = x^2 + 50u^2 + 50v^2 + 125w^2,$$

$$\text{subject to } xw = v^2 - 4uv - u^2, \quad x \equiv 1 \bmod 5\,.$$

If (x, u, v, w) is one solution to this system, the others are $(x, -v, u, -w)$, $(x, v, -u, -w)$ and $(x, -u, -v, w)$. If g is a primitive root mod p, Katre and Rajwade proved in [5] that (x, u, v, w) can be defined unambiguously—given g—by the additional condition

$$g^{(p-1)/5} \equiv (a - 10b)/(a + 10b) \bmod p\,, \tag{7}$$

$$a = x^2 - 125w^2, \quad b = 2xu - xv - 25vw\,.$$

Remark. Another expression for primitive fifth roots mod p was obtained by Emma Lehmer in [6]. Her expression was more complicated and evaluated to $0/0$ when $u = -2v$.

The author is not aware of special bases for quintic fields in the literature, but $S_5(m, j)$ can be evaluated with the *cyclotomic numbers* (h, k). These are defined (for fixed g) by

$$(h, k) = \#\{\nu \in (\mathbb{Z}/p\mathbb{Z})^* : \nu \in \mathcal{C}_h^{(g)},\ \nu + 1 \in \mathcal{C}_k^{(g)}\}\,.$$

There are a number of well-known general formulas satisfied by the cyclotomic numbers (see, e.g., [1, 7]), including

$$\eta_a \eta_{a+k} = \varepsilon^{(k)} f + \sum_{h=0}^{e-1} (h, k) \eta_{a+h}, \tag{8}$$

$$\varepsilon^{(k)} = \begin{cases} 1 & k = 0,\ f \text{ even or } k = e/2,\ f \text{ odd}, \\ 0 & \text{otherwise.} \end{cases}$$

For $p \equiv 1 \bmod 5$, obviously f is even.

The quintic cyclotomic numbers were established in principle by Dickson [2] and made unambiguous (as a function of g) in [5] by (7):

$$\begin{aligned}
&(00) = (p - 14 + 3x)/25\,,\\
&(01) = (10) = (44) = (4p - 16 - 3x + 50v + 25w)/100\,,\\
&(02) = (20) = (33) = (4p - 16 - 3x + 50u - 25w)/100\,,\\
&(03) = (30) = (22) = (4p - 16 - 3x - 50u - 25w)/100\,,\\
&(04) = (40) = (11) = (4p - 16 - 3x - 50v + 25w)/100\,,\\
&(12) = (21) = (34) = (43) = (14) = (41) = (2p + 2 + x - 25w)/50\,,\\
&(13) = (31) = (23) = (32) = (24) = (42) = (2p + 2 + x + 25w)/50\,.
\end{aligned} \tag{9}$$

The Lehmer results are

Theorem 6.

$$\begin{aligned}
100S_5(2,1) &= -4-8p-3px+50pv+25pw\,,\\
10^4S_5(3,1) &= 80+720p-320p^2-60px-45px^2-625pw^2-1500pw\\
&\quad -3000pv+500pxv+250pxw-2500pv^2-5000puw\\
&\quad +2500pvw\,,\\
10^6S_5(4,1) &= 80000\,p^2v-9600\,p^2x+40000\,p^2w-675\,px^3+8750\,px^2v\\
&\quad +4375\,px^2w-25000\,pxu^2-25000\,pxuw-37500\,pxv^2\\
&\quad +12500\,pxvw-40000\,pxv-15625\,pxw^2-20000\,pxw\\
&\quad +12000\,px+250000\,pu^2v+125000\,pu^2w-100000\,pu^2\\
&\quad +250000\,puvw-125000\,puw^2+400000\,puw+375000\,pv^3\\
&\quad +62500\,pv^2w+100000\,pv^2+843750\,pvw^2-200000\,pvw\\
&\quad +120000\,pv+78125\,pw^3+60000\,pw-32000\,p-1600\,.
\end{aligned}$$

Proof. We will illustrate the proof for $S_5(2,1)$; the same technique is used for the other formulas but the calculations (which were done by machine) are much messier. Using (8) and the identities involving the (h,k) in (9) we have

$$\begin{aligned}
(10)\ \eta_0^2\eta_1 = {}&(01)f\\
&+[(03)(13)+(00)(01)+(01)(04)+(02)(12)+(04)(12)]\eta_0\\
&+[f+(00)(04)+(03)(02)+(04)(03)+(00)(01)+(01)(02)]\eta_1\\
&+[(00)(12)+(04)(13)+(02)(04)+(03)(12)+(01)^2]\eta_2\\
&+[(03)^2+(00)(13)+(02)(12)+(04)(13)+(01)(02)]\eta_3\\
&+[(02)(13)+(00)(12)+(01)(03)+(03)(13)+(02)(04)]\eta_4\,.
\end{aligned}$$

Noting that $S_5(2,1)=\mathrm{Tr}_{\mathbb{Q}}^{K}\,\eta_0^2\eta_1$, and that $\mathrm{Tr}_{\mathbb{Q}}^{K}\,\eta_j=-1$, we can obtain an expression for $S_5(2,1)$ in terms of cyclotomic numbers by multiplying the rational term in (10) by 5 and subtracting the coefficients of the η's. This yields

$$\begin{aligned}
S_5(2,1) = {}&5(01)f-(00)(04)-2(02)(12)-2(02)(04)-(02)(13)\\
&-(03)(02)-(03)(12)-(03)^2-(04)(12)-(04)(03)\\
&-2(04)(13)-2(03)(13)-2(01)(02)-(01)(03)\\
&-(01)^2-(01)(04)-(00)(13)-2(00)(12)-2(00)(01)-f\,.
\end{aligned}$$

The theorem now follows by substituting in the values of (h,k) in (9) and simplifying. ■

Corollary 7. *$S_5(m,j)$, $j=2,3,4$, are obtained by substituting $\sigma_2=(x,-v,u,-w)$, $\sigma_3=(x,v,-u,-w)$, and $\sigma_4=(x,-u,-v,w)$ respectively for $\sigma_1=(x,u,v,w)$ in $S_5(m,1)$.*

Proof. Theorem 2 of [5] implies that a generator g' is in $\mathcal{C}_j^{(g)}$ whenever g satisfies (7) and g' will satisfy (7) after the substitution σ_j is made. The corollary follows from (2). (The substitution σ_j is related to the automorphism of $\mathbb{Q}[\zeta_5]$ given by $\zeta_5 \mapsto \zeta_5^j$.) ∎

Remark. Lehmer also investigated a variation on the S_n in which the Gaussian periods η were replaced by the so-called *reduced Gaussian periods* $x=e\eta+1$. The corresponding minimal polynomials have simpler coefficients and may be obtained in exactly the same ways.

References

[1] P. Bachmann, *Die Lehre von der Kreisteilung*, Teubner, Leipzig 1927.

[2] L. E. Dickson, *Cyclotomy, higher congruences, and Waring's problem*, Amer. J. Math. 57 (1935), 391–424.

[3] H. Hasse, *Arithmetische Bestimmung von Grundeinheit und Klassenzahl in zyklischen kubischen und biquadratischen Zahlkörpern*, in: Mathematische Abhandlungen, Vol. 3, Walter deGruyter, Berlin 1975 (originally published 1950), 285–379.

[4] S. A. Katre and A. R. Rajwade, *Complete solution of the cyclotomic problem in $\boldsymbol{F}_q$ for any prime modulus l, $q=p^\alpha$, $p\equiv 1 \pmod{l}$*, Acta Arith. 45 (1985), 183–199.

[5] —, —, *Unique determination of cyclotomic numbers of order five*, Manuscripta Math. 53 (1985), 65–75.

[6] E. Lehmer, *On Euler's criterion*, J. Austral. Math. Soc. 1 (1959), 64–70.

[7] T. Storer, *Cyclotomy and Difference Sets*, Markham, Chicago 1967.

DEPARTMENT OF MATHEMATICS
UNIVERSITY OF CALIFORNIA
DAVIS, CALIFORNIA 95616, U.S.A.
E-mail: LAZARUS@UCDMATH.UCDAVIS.EDU

Received on 31.3.1992 (2247)