transcendental numbers which are algebraically independent. But such questions appear to be very difficult. The first of the questions we have asked is a generalization of a conjecture of Schneider and the second is a generalization of a conjecture of Gelfond. In our notation Schneider's conjecture [10] reads $\dim(e^z, e^{az}) \leqslant 1$ if a is irrational, and Gelfond's conjecture [3] (partially solved by himself) is the algebraic independence of $a^{\beta}, a^{\beta^2}, \ldots, a^{\beta^{h-1}}$ (where a is algebraic, $\log a \neq 0$ and β is an algebraic irrational of degree h).

References

[1] E. T. Copson, *An introduction to the theory of functions of a complex variable*, Oxford 1961.

[2] M. Deuring, *Die Klassenkörper der komplexen Multiplikation*, Enzykl. der Math. Wiss., Band I, 2, 23, Teubner 1958.

[3] A. O. Gelfond, *Transcendental and algebraic numbers*, translated from the first Russian edition by Leo. F. Boron, New York 1960.

[4] G. H. Hardy and E. M. Wright, *Introduction to the theory of numbers*, third edition, Oxford 1954.

[5] H. Hasse, *Neue Begründung der komplexen Multiplikation*, *I*, J. für Math. 157 (1927), pp. 115-139; *II*, ibid. 165 (1931), pp. 64-68.

[6] R. Fricke and F. Klein, *Die elliptischen Funktionen und ihre Anwendungen*, Leipzig u. Berlin (1922), Band II, 184p.

[7] L. Kronecker, *Näherungsweise ganzzahlige Auflösung linearer Gleichungen*, Werke, Bd. III (i), Leipzig 1899, pp. 47-109.

[8] K. Mahler, *On the division-values of Weierstrass's $\wp$-function*, Quarterly J. of Maths. 6 (1935), pp. 74-77.

[9] K. Ramachandra, *Contributions to the theory of transcendental numbers (I)*, this volume, pp. 65-72.

[10] Th. Schneider, *Einführung in die transzendenten Zahlen*, Springer Verlag 1957.

[11] — *Transzendenzuntersuchungen periodischer Funktionen I*, J. für Math. 172 (1935), pp. 65-69; *II*, ibid. 172 (1935), pp. 70-74.

[12] C. L. Siegel, *Transcendental numbers*, Ann. of Maths., Studies Number 16, Princeton Univ. Press 1949.

[13] H. Weyl, *Über die Gleichverteilung von Zahlen mod. Eins*, Math. Annalen, 77 (1916), pp. 313-352.

[14] E. T. Whittaker and G. N. Watson, *A course of modern analysis*, Cambridge 1958.

Errata. Professor A. Schinzel has kindly drawn my attension to some oversights in my paper *On the units of cyclotomic fields* (ibid. 12 (1966), pp. 165-173). I take the opportunity of correcting one: In equation (21) on page 172 omit -1 in the exponent.

TATA INSTITUTE OF FUNDAMENTAL RESEARCH, BOMBAY

Reçu par la Rédaction le 18. 5. 1967

ACTA ARITHMETICA
XIV (1968)

The cyclotomy of hyper-Kloosterman sums

by

D. H. and Emma Lehmer (Berkeley, Calif.)

1. Introduction. In a recent paper [4] we presented some evidence in support of the thesis that the Kloosterman sums

$$S(h) = \sum_{x=1}^{p-1} \varepsilon(x+h\bar{x}) \qquad (x\bar{x} \equiv 1 \pmod{p}) \tag{1.1}$$

where

$$\varepsilon(\nu) = \exp(2\pi i\nu/p), \qquad p \text{ a prime} \tag{1.2}$$

could be thought of as generalizations of the exponential function $\varepsilon(h)$.

A further support of this point of view is provided by the n-dimensional exponential sums

$$S^{(n)}(h) = \sum_{x_1,\ldots,x_n=1}^{p-1} \varepsilon\Big(\sum_{i=1}^{n} x_i + h\prod_{i=1}^{n} \bar{x}_i\Big) \tag{1.3}$$

discussed recently by Carlitz [3], which we shall call here hyper-Kloosterman sums.

It is quite obvious from the definition (1.3) that

$$S^{(0)}(h) = \varepsilon(h) \quad \text{and} \quad S^{(1)}(h) = S(h), \tag{1.4}$$

also that

$$S^{(n)}(0) = (-1)^n, \tag{1.5}$$

and that

$$\sum_{h=0}^{p-1} S^{(n)}(h) = 0. \tag{1.6}$$

Carlitz [3] finds that

$$\sum_{h=0}^{p-1} |S^{(n)}(h)|^2 = p^{n+1} - p^n - \ldots - p \tag{1.7}$$

and gives a formula for $\sum_{h=0}^{p-1} [S^{(2)}(h)]^3$ which unfortunately is not quite correct.

In section 2 we shall derive a correct formula for the sums of cubes and give a generalization of (1.7).

In section 3 we show that the hyper-Kloosterman sums in their turn can be used to construct a cyclotomic theory in line with that developed for Kloosterman sums in [4]. We shall feel free to make use of the results obtained in [4].

2. Relations between hyper-Kloosterman sums. It follows from the definition (1.3) that

$$S^{(n)}(h) = \sum_{x=1}^{p-1} \varepsilon(x) S^{(n-1)}(h\bar{x}). \tag{2.1}$$

More generally we have the following

THEOREM 2.1.

$$S^{(n)}(h) = \sum_{x=1}^{p-1} S^{(m)}(x) S^{(n-m-1)}(h\bar{x}). \tag{2.2}$$

Proof. By (1.3)

$$S^{(n)}(h) = \sum_{x_1,\ldots,x_n=1}^{p-1} \varepsilon\Big(\sum_{i=1}^{m+1} x_i\Big)\varepsilon\Big(\sum_{i=m+2}^{n} x_i + h\prod_{i=1}^{m+1}\bar{x}_i \prod_{i=m+2}^{n}\bar{x}_i\Big).$$

Now let

$$x_{m+1} \equiv x\prod_{i=1}^{m}\bar{x}_i \pmod{p},$$

then

$$S^{(n)}(h) = \sum_{x=1}^{p-1}\sum_{x_1,\ldots,x_m=1}^{p-1} \varepsilon\Big(\sum_{i=1}^{m} x_i + x\prod_{i=1}^{m}\bar{x}_i\Big) \sum_{x_{m+2},\ldots,x_n=1}^{p-1} \varepsilon\Big(\sum_{i=m+2}^{n} x_i + h\bar{x}\prod_{i=m+2}^{n}\bar{x}_i\Big)$$

which is the theorem, by (1.3).

In order to give a generalization of (1.7) we define the Kronecker symbol modulo p as

$$\delta_a^b = \begin{cases} 1 & \text{if } a \equiv b \pmod{p}, \\ 0 & \text{otherwise}, \end{cases} \tag{2.3}$$

then we can state

THEOREM 2.2. *For* $a \neq 0$,

$$\sum_{h=0}^{p-1} S^{(n)}(h) S^{(n)}(ah) = p^{n+1}\delta_a^{(-1)^{n+1}} - p^n - p^{n-1} - \ldots - p. \tag{2.4}$$

Proof. The theorem is true for $n = 0$, since

$$\sum_{h=0}^{p-1} \varepsilon(h)\varepsilon(ah) = \sum_{h=0}^{p-1} \varepsilon\big(h(1+a)\big) = \delta_a^{-1} p.$$

It has also been proved for $n = 1$ in [4] formula (3.6). Suppose that (2.4) holds for $n-1$, then by Theorem 2.1 with $m = n-1$ we have

$$\begin{aligned}\sum_{h=0}^{p-1} S^{(n)}(h) S^{(n)}(ah) &= \sum_{x,y=1}^{p-1} S^{(n-1)}(x) S^{(n-1)}(y) \sum_{h=0}^{p-1}\varepsilon\big(h(\bar{x}+a\bar{y})\big) \\ &= p\sum_{x=1}^{p-1} S^{(n-1)}(x) S^{(n-1)}(-\bar{a}x) \\ &= p\big[p^n\delta_{-\bar{a}}^{(-1)^n} - p^{n-1} - p^{n-2} - \ldots - p - \big(S^{(n-1)}(0)\big)^2\big] \\ &= p^{n+1}\delta_a^{(-1)^{n+1}} - p^n - p^{n-1} - \ldots - p,\end{aligned}$$

by (1.5), which is the theorem.

As an adjunct to Theorem 2.2 we give

THEOREM 2.3. *For* $n > m$, $a \neq 0$,

$$\begin{aligned}&\sum_{h=0}^{p-1} S^{(n)}(h) S^{(m)}(ah) \\ &\quad = p^{m+1} S^{(n-m-1)}\big((-1)^{m+1}\bar{a}\big) - (-1)^{n-m}(p^m + p^{m-1} + \ldots + p).\end{aligned} \tag{2.5}$$

Proof. By Theorem 2.1,

$$\sum_{h=0}^{p-1} S^{(n)}(h) S^{(m)}(ah) = \sum_{x=1}^{p-1} S^{(n-m-1)}(x) \sum_{h=0}^{p-1} S^{(m)}(h\bar{x}) S^{(m)}(ah).$$

Letting $ah = k$, Theorem 2.2 gives

$$\begin{aligned}&\sum_{h=0}^{p-1} S^{(n)}(h) S^{(m)}(ah) \\ &\quad = \sum_{x=1}^{p-1} S^{(n-m-1)}(x)\,[\delta_{ax}^{(-1)^{m+1}} p^{m+1} - p^m - \ldots - p] \\ &\quad = p^{m+1} S\big((-1)^{m+1}\bar{a}\big) - (p^m + p^{m-1} + \ldots + p)\sum_{x=1}^{p-1} S^{(n-m-1)}(x)\end{aligned}$$

which yields the theorem using (1.5) and (1.6).

The special case of Theorem 2.3 with $m = 0$ might be of interest. This gives

$$\sum_{h=0}^{p-1} S^{(n)}(h)\varepsilon(ah) = pS^{(n-1)}(-\bar{a}). \tag{2.6}$$

This is an inversion of (2.1).

In order to calculate the sums of the cubes of the $S^{(2)}(h)$ without counting the number of solutions of various congruences, as in Carlitz [3], we make use of formula (3.20) of [4] which is as follows:

$$\sum_{h=0}^{p-1} S^{(1)}(h)S^{(1)}(ah)S^{(1)}(bh) = 2p+p^2\chi[(a-b)^2-2(a+b)+1], \tag{2.7}$$

where $\chi(n)$ is the Legendre symbol $\left(\frac{n}{p}\right)$. This gives

THEOREM 2.4.

$$\sum_{h=0}^{p-1}[S^{(2)}(h)]^3 = p(p-2)(p+1)^2-p^3[1+\chi(-3)].$$

Proof. By (2.7)

$$\begin{aligned}\sum_{h=0}^{p-1}[S^{(2)}(h)]^3 &= \sum_{x,y,z=1}^{p-1}\sum_{h=0}^{p-1} S^{(2)}(xh)S^{(2)}(yh)S^{(2)}(zh)\\ &= \sum_{x,y,z=1}^{p-1}\sum_{h=0}^{p-1}\varepsilon\big(h(\bar{x}+\bar{y}+\bar{z})\big)S^{(1)}(x)S^{(1)}(y)S^{(1)}(z)\end{aligned}$$

by (2.1). The sum over h is zero unless $\bar{x}+\bar{y} = -\bar{z}$, in which case it is p. Letting $x = zu$, $y = zv$ this condition becomes $\bar{u} = -(1+\bar{v})$, so that $\bar{x} = -\bar{z}(1+\bar{v})$. Substituting these values after summing over h we obtain

$$\sum_{h=0}^{p-1}[S^{(2)}(h)]^3 = p\sum_{v=1}^{p-2}\sum_{z=1}^{p-1} S(z)S(zv)S\left(\frac{-zv}{1+v}\right).$$

We can now apply (2.7) with $a = v$, $b = -v/(1+v)$, then

$$\chi[(a-b)^2-2(a+b)+1] = \chi(1+v+v^2)^2.$$

Hence

$$\begin{aligned}\sum_{h=0}^{p-1}[S^{(2)}(h)]^3 &= p\sum_{v=1}^{p-2}[2p+p^2\chi^2(1+v+v^2)+1]\\ &= p(p-2)(p+1)^2-p^3[1+\chi(-3)].\end{aligned}$$

3. Hyper-periods. Let $p = ef+1$ and let C_j be the class of integers $h \pmod{p}$ for which $\operatorname{ind} h \equiv j \pmod{e}$. We now consider the problem of summing the hyper-Kloosterman sums over a given residue class C_j. We define

$$\eta_j^{(n)} = \sum_{h\epsilon C_j} S^{(n)}(h) \quad (j = 0, 1, \ldots, e-1). \tag{3.1}$$

Then the usual cyclotomic periods are

$$\eta_j^{(0)} = \eta_j = \sum_{h\epsilon C_j}\varepsilon(h)$$

and the Kloosterman periods studied in [4] are

$$\theta_j = \eta_j^{(1)} = \sum_{h\epsilon C_j} S(h).$$

These hyper-periods enjoy many of the fundamental properties of the cyclotomic periods, which we will consider next.

First of all it follows from the definition (3.1) that

$$\sum_{j=0}^{e-1}\eta_j^{(n)} = (-1)^{n+1}, \tag{3.2}$$

since the sum in (3.2) goes over all non-zero values of h, so that by (1.5) and (1.6) it is $(-1)^{n+1}$.

Next it is well known that [1]

$$e\sum_{i=0}^{e-1}\eta_i\eta_{j+i} = ep\Delta_j^{(p-1)/2}-p+1$$

where

$$\Delta_j^k = \begin{cases} 1 \text{ if } k\equiv j \pmod{e},\\ 0 \text{ otherwise}.\end{cases}$$

More generally Theorem 2.2 leads to the following:

THEOREM 3.1.

$$e\sum_{i=0}^{e-1}\eta_i^{(n)}\eta_{i+j}^{(n)} = ep^{n+1}\Delta_j^{(n+1)(p-1)/2}-p^{n+1}+1.$$

Proof. From the definition (3.1) we have

$$e\sum_{i=0}^{e-1}\eta_i^{(n)}\eta_{j+i}^{(n)} = e\sum_{i=0}^{e-1}\sum_{h\epsilon C_i} S^{(n)}(h)\sum_{k\epsilon C_{i+j}} S^{(n)}(k).$$

Letting $k = ah$, implies a is in class C_j and we can write

$$\begin{aligned}e\sum_{i=0}^{e-1}\eta_i^{(n)}\eta_{j+i}^{(n)} &= e\sum_{a\epsilon C_j}\sum_{h=1}^{p-1} S^{(n)}(h)S^{(n)}(ah)\\ &= e\sum_{a\epsilon C_j}[p^{n+1}\delta_a^{(-1)^{n+1}}-p^n-p^{n-1}-\ldots-p-1]\\ &= ep^{n+1}\Delta_j^{(n+1)(p-1)/2}-ef\frac{p^{n+1}-1}{p-1}\end{aligned}$$

which is the theorem since $ef = p-1$.

Theorem 2.1 leads to its analogue, namely

THEOREM 3.2.

$$\eta_j^{(n)} = \sum_{i=0}^{e-1} \eta_i^{(n-m-1)}\eta_{j-i}^{(m)}.$$

Proof. By Theorem 2.1 we have

$$\eta_j^{(n)} = \sum_{h\in C_j} S^{(n)}(h) = \sum_{x=1}^{p-1}\sum_{h\in C_j} S^{(m)}(\bar{x}h)\, S^{(n-m-1)}(x)$$
$$= \sum_{i=0}^{e-1}\sum_{x\in C_i} S^{(n-m-1)}(x)\,\eta_{j-i}^{(m)} = \sum_{i=0}^{e-1}\eta_i^{(n-m-1)}\eta_{j-i}^{(m)}.$$

Letting $n = 2m+1$ we have a useful corollary

(3.3) $$\eta_j^{(2m+1)} = \sum_{i=0}^{e-1}\eta_i^{(m)}\eta_{j-i}^{(m)}.$$

One of the most fundamental properties of the periods is that the product of any two periods can be written as a linear combination of the periods with integer coefficients. This property is preserved for the hyper-periods. In the cyclotomic case the coefficients are the so-called cyclotomic numbers (i, j) which are the number of solutions of the congruence $x+1 \equiv y \pmod{p}$ where x is in class C_i and y is in class C_j. The classical formula is [1]

(3.4) $$\eta_i\eta_{i+j} = \sum_{k=0}^{e-1}(j, k)\,\eta_{i+k} + f\Delta_j^{(p-1)/2}.$$

Letting

(3.5) $$a_{j,k}^{(0)} = a_{j,k} = (j, k) - f\Delta_j^{(p-1)/2}$$

we can write

(3.6) $$\eta_i\eta_{i+j} = \sum_{k=0}^{e-1} a_{j,k}\,\eta_{i+k}.$$

The corresponding theorem for hyper-periods now reads:

THEOREM 3.3. *The product of any two hyper-periods is a linear combination of the hyper-periods with integer coefficients. More precisely*

(3.7) $$\eta_i^{(n)}\eta_{i+j}^{(n)} = \sum_{k=0}^{e-1} a_{j,k}^{(n)}\eta_{i+k}^{(n)}$$

where

(3.8) $$a_{j,k}^{(n)} = \sum_{\nu,\mu=1}^{e-1} a_{\nu,\mu}^{(n-1)} a_{j-\nu,k-\mu}.$$

Proof. The theorem is true for $n = 0$ by (3.4) and (3.5). We now suppose that it holds for $n-1$ and show that it holds for n. By Theorem 3.2 with $m = 0$ we have

$$\eta_i^{(n)}\eta_{i+j}^{(n)} = \sum_{s=0}^{e-1}\eta_s^{(n-1)}\eta_{i-s}\sum_{t=0}^{e-1}\eta_t^{(n-1)}\eta_{i+j-t}$$
$$= \sum_{s,\nu=0}^{e-1}\eta_s^{(n-1)}\eta_{s+\nu}^{(n-1)}\eta_{i-s}\eta_{i-s+j-\nu}$$
$$= \sum_{s,\nu,\mu=0}^{e-1} a_{\nu,\mu}^{(n-1)}\eta_{s+\mu}^{(n-1)}\sum_{\tau=0}^{e-1} a_{j-\nu,\tau}\eta_{i-s+\tau}$$
$$= \sum_{\nu,\mu,\tau=0}^{e-1} a_{\nu,\mu}^{(n-1)} a_{j-\nu,\tau}\sum_{s=0}^{e-1}\eta_{s+\mu}^{(n-1)}\eta_{i-s+\tau}$$
$$= \sum_{\nu,\mu,\tau=0}^{e-1} a_{\nu,\mu}^{(n-1)} a_{j-\nu,\tau}\eta_{i+\mu+\tau}^{(n)}.$$

The theorem now follows if we let $\mu+\tau = k$.

The coefficients $a_{j,k}$ have some of the properties of the cyclotomic numbers, such as

$$(j, k) = (e-j, k-j).$$

Hence also

(3.9) $$a_{j,k} = a_{e-j,k-j}$$

since $(p-1)/2$ is congruent to either 0 or $e/2$ modulo e. Similarly

(3.10) $$a_{j,k}^{(n)} = a_{e-j,k-j}^{(n)}.$$

To prove this assume that (3.10) holds for $n-1$. Then by (3.8)

$$a_{j,k}^{(n)} = \sum_{\nu,\mu=0}^{e-1} a_{\nu,\mu}^{(n-1)} a_{j-\nu,k-\mu} = \sum_{\nu,\mu=0}^{e-1} a_{e-\nu,\mu-\nu}^{(n-1)} a_{\nu-j,k-\mu-j+\nu}$$
$$= \sum_{s,t=0}^{e-1} a_{s,t}^{(n-1)} a_{e-s-j,k-t-j} = a_{e-j,k-j}^{(n)}.$$

Another property of the cyclotomic numbers is

$$\sum_{k=0}^{e-1}(j, k) = f - \Delta_j^{(p-1)/2}, \qquad \sum_{j=0}^{e-1}(j, k) = f - \Delta_k^0.$$

This makes

(3.11) $$\sum_{k=0}^{e-1} a_{j,k} = f - p\Delta_j^{(p-1)/2}, \qquad \sum_{j=0}^{e-1} a_{j,k} = -\Delta_k^0.$$

More generally, if we sum (3.7) over i we obtain by (3.2) and by Theorem 3.1 that

$$e\sum_{k=0}^{e-1} a_{j,k}^{(n)} = (-1)^{n+1}\left[ep^{n+1}\Delta_j^{(n+1)(p-1)/2} - p^{n+1}+1\right]. \tag{3.12}$$

In Theorem 6.1 of [4] we have shown that $\eta_j^{(1)}$ can be written as a linear combination of the classical η's with integer coefficients, which are closely related to the Jacobsthal character sums defined by

$$\varphi_e(h) = \sum_{x=1}^{p-1}\chi(x)\chi(x^e+h) \tag{3.13}$$

and

$$\psi_e(h) = \sum_{x=1}^{p-1}\chi(x^e+h). \tag{3.14}$$

More generally we can state the following theorem:

THEOREM 3.4. *The hyper-periods are linear combinations of the periods with integer coefficients. In fact*

$$\eta_j^{(n)} = \sum_{k=0}^{e-1} c_{j,k}^{(n)}\eta_k \tag{3.15}$$

where

$$c_{j,\nu}^{(n)} = \sum_{i=0}^{e-1}\sum_{k=0}^{e-1} a_{j-k-i,\nu-k}\, c_{i,k}^{(n-1)}$$

with

$$c_{j,\nu}^{(1)} = \begin{cases} \dfrac{1}{e}\varphi_e(-4g^{j-2\nu}), & e \text{ odd},\\[2mm] \dfrac{1}{e}\psi_e(-4g^{j-2\nu}) - f(-1)^{j+(p-1)/2}, & e \text{ even}, \end{cases} \tag{3.16}$$

and the $a_{i,j}$ are defined by (3.5).

Proof. For $n = 1$ this becomes Theorem 6.1 of [4]. We next assume the theorem to be true for $n-1$, then by Theorem 3.2 with $m = 0$,

$$\eta_j^{(n)} = \sum_{i=0}^{e-1}\eta_i^{(n-1)}\eta_{j-i} = \sum_{k=0}^{e-1}\sum_{i=0}^{e-1} c_{i,k}^{(n-1)}\eta_k\eta_{k+(j-k-i)}$$
$$= \sum_{k=0}^{e-1}\sum_{i=0}^{e-1} c_{i,k}^{(n-1)}\sum_{s=0}^{e-1} a_{j-k-i,s}\,\eta_{k+s}$$

by Theorem 3.3 with $n = 0$. Letting $k+s = \nu$ we have

$$\eta_j^{(n)} = \sum_{\nu=0}^{e-1}\eta_\nu\sum_{i,k=0}^{e-1} a_{j-k-i,\nu-k}\, c_{i,k}^{(n-1)} = \sum_{\nu=0}^{e-1} c_{j,\nu}^{(n)}\eta_\nu$$

which completes the proof of the theorem.

We next prove a few properties of the coefficients $c_{j,k}^{(n)}$. Summing (3.15) over j we have by (3.2)

$$\sum_{j=0}^{e-1}\eta_j^{(n)} = (-1)^{n+1} = \sum_{k=0}^{e-1}\eta_k\sum_{j=0}^{e-1} c_{j,k}^{(n)}.$$

Hence, since the η's are linearly independent, we have

$$\sum_{j=0}^{e-1} c_{j,k}^{(n)} = (-1)^n \qquad (k = 0, 1, \ldots, e-1). \tag{3.17}$$

In what follows we shall need the following lemma:

LEMMA 3.1. *If in the expression for $\eta_j^{(n)}$ we replace ε by ε^σ, with $\sigma \not\equiv 0 \pmod p$, then $\eta_j^{(n)}$ becomes $\eta_{j+(n+1)s}^{(n)}$ where $s \equiv \operatorname{ind}\sigma \pmod e$.*

Proof. By (1.3) and (3.1) the expression for $\eta_j^{(n)}$ becomes

$$\sum_x\sum_{h\in C_j}\varepsilon\Big(\sigma\sum_{i=0}^{e-1}x_i + h\sigma\prod_{i=0}^{e-1}\bar{x}_i\Big) = \sum_y\sum_{h\in C_j}\varepsilon\Big(\sum_{i=0}^{e-1}y_i + \sigma^{n+1}h\prod_{i=0}^{e-1}\bar{y}_i\Big)$$

with $y_i = \sigma x_i$. But this is $\eta_{j+(n+1)s}^{(n)}$.

Applying the lemma to Theorem 3.4 with $n = 0$ as well as n, we have

$$\eta_{j+(n+1)s}^{(n)} = \sum_{k=0}^{e-1} c_{j,k}^{(n)}\eta_{k+s} = \sum_{k=0}^{e-1} c_{j+(n+1)s,k}^{(n)}\eta_k.$$

Since the classical periods are linearly independent we can identify coefficients of $\eta_{\nu+s}$ and obtain the property

$$c_{j,\nu}^{(n)} = c_{j+(n+1)s,\nu+s}^{(n)} \qquad (s = 0, 1, \ldots, e-1). \tag{3.18}$$

This leads to a refinement of Theorem 3.4 as follows:

THEOREM 3.5. *Let $\delta = (n+1, e)$ and let $e = \delta e'$, $n+1 = \delta m$, so that $(m, e') = 1$. Let η_i' be the hyperperiods of order e', then*

$$\eta_{j+m\delta s}^{(n)} = \sum_{k=0}^{e'-1} c_{j,k}^{(n)}\eta_{k+s}' \qquad (s = 0, 1, \ldots, e'-1). \tag{3.19}$$

Proof. Letting $s = te'$ in (3.18) for $t = 1, 2, \ldots, \delta-1$ we have

$$c_{j,\nu}^{(n)} = c_{j,\nu+te'}^{(n)} \qquad (t = 1, 2, \ldots, \delta-1).$$

Substituting this into (3.15) gives

$$\eta_j^{(n)} = \sum_{k=0}^{e'-1} c_{j,k}^{(n)} \sum_{t=0}^{\delta-1} \eta_{k+te'} = \sum_{k=0}^{e'-1} c_{j,k}^{(n)} \eta'_k. \tag{3.20}$$

Applying the lemma to this expression the theorem follows.

It follows from (3.18) and (3.17) that

$$\sum_{k=0}^{e-1} c_{j,k}^{(n)} = (-1)^n \quad \text{if} \quad (n+1, e) = 1. \tag{3.21}$$

In particular if $e' = 1$, $\eta'_0 = -1$ and we have:

$$\eta_j^{(n)} = -c_{j,0}^{(n)} \quad (j = 0, 1, \ldots, e-1) \tag{3.22}$$

is an integer, if e divides $(n+1)$.

Next, if we let $a = \exp(2\pi i/e)$, then the generalized Gauss sum, or Lagrange's resolvant, is given by [1]

$$\tau(a^\nu) = \sum_{i=0}^{e-1} \eta_i a^{i\nu}. \tag{3.23}$$

The corresponding hyper-Gauss sum defined by

$$\tau^{(n)}(a^\nu) = \sum_{i=0}^{e-1} \eta_i^{(n)} a^{i\nu} \tag{3.24}$$

turns out to be the $(n+1)^{\mathrm{st}}$ power of the Gauss sum, namely

THEOREM 3.6.

$$\tau^{(n)}(a^\nu) = \big(\tau(a^\nu)\big)^{n+1}.$$

Proof. The theorem is true for $n = 0$ by (3.23). Suppose that it is true for $n-1$. Then from the definition (3.24) and by Theorem 3.2 with $m = 0$ we have

$$\begin{aligned}\tau^{(n)}(a^\nu) &= \sum_{j=0}^{e-1} \eta_j^{(n)} a^{j\nu} = \sum_{i,j=0}^{e-1} \eta_i^{(n-1)} \eta_{j-i} a^{\nu j} \\ &= \sum_{i=0}^{e-1} \eta_i^{(n-1)} a^{i\nu} \sum_{j=0}^{e-1} \eta_{j-i} a^{(j-i)\nu} \\ &= \tau^{(n-1)}(a^\nu)\tau(a^\nu) = \big(\tau(a^\nu)\big)^{n+1}\end{aligned}$$

which proves the theorem.

As a corollary we have

$$\tau^{(n)}(a^\nu)\tau^{(n)}(a^{-\nu}) = (-1)^{\nu f(n+1)} p^{n+1} \quad (\nu \not\equiv 0 \pmod{e}). \tag{3.25}$$

This follows from the well known relation

$$\tau(a^\nu)\tau(a^{-\nu}) = (-1)^{\nu f} p \quad (\nu \not\equiv 0 \pmod{e}).$$

4. Hyper-period equations. It is well known that the classical periods satisfy a monic irreducible equation of degree e with integer coefficients and that this equation is abelian.

It follows from Theorem 3.3 that the equation satisfied by the hyper-periods is also abelian, but not necessarily irreducible. In fact we have the following theorem.

THEOREM 4.1. *Let $\delta = (n+1, e)$ so that $e = \delta e'$ and $n+1 = \delta m$ with $(e', m) = 1$. Then the hyper-periods*

$$\eta_{j+\delta\nu}^{(n)} \quad (\nu = 0, 1, \ldots, e'-1) \tag{4.1}$$

satisfy δ irreducible monic equations of degree e' with integer coefficients, one for each $j = 0, 1, \ldots, \delta-1$.

Proof. By Theorem 3.5 the hyper-periods (4.1) with j fixed satisfy an equation of degree e' with integer coefficients, since all the symmetric functions of the hyper-periods in (4.1) can be expressed in terms of the symmetric functions of the η'_i, which are integers. Suppose now that any fixed hyper-period of the set (4.1) say $\eta_{j+\delta k}^{(n)}$ satisfies an irreducible equation $f(x)$ of degree less than or equal to e'. Then $f(\eta_{j+\delta k}^{(n)})$ can be written as a linear combination of η'_i with integer coefficients

$$f(\eta_{j+\delta k}^{(n)}) = \sum_{i=0}^{e'-1} A_i \eta'_i. \tag{4.2}$$

Since $f(\eta_{j+\delta k}^{(n)}) = 0$, all the coefficients $A_i = 0$. Applying Lemma 4.1 to (4.2) we obtain

$$f(\eta_{j+\delta(k+ms)}^{(n)}) = \sum_{i=0}^{e'-1} A_i \eta'_{i+s} = 0.$$

But since $(m, e') = 1$ it follows that $k+ms$ goes through a complete residue system modulo e'. Hence all the hyper-periods in the set (4.1) satisfy $f(x) = 0$. Thus the degree of $f(x)$ is indeed e' and the theorem follows.

As a special case of this theorem with $e = p-1$ we have

THEOREM 4.2. *The hyper-Kloosterman sums $S^{(n)}(h)$ with* ind $h \equiv j \pmod{\delta}$ *satisfy an irreducible equation of degree $(p-1)/\delta$, where $\delta = (p-1, n+1)$ for every $j = 0, 1, \ldots, \delta-1$.*

In particular for $n = 1$, $\delta = 2$ the Kloosterman sums $S(h)$ for $h \neq 0$ satisfy one of two irreducible equations of degree $(p-1)/2$ according as h is a quadratic residue or non residue of p. This was noted by Salié [7].

As an illustration of Theorem 4.2 for $p = 7$ we have the following equations:

n	Hyper-Period Equations
0	$x^6+x^5+x^4+x^3+x^2+x+1 = 0$
1	$(x^3+3x^2-4x-13)(x^3-4x^2-4x+8) = 0$
2	$(x^2-2x+8)(x^2-9x+36)(x^2+12x+99) = 0$
3	$(x^3-25x^2+192x-419)(x^3+24x^2-592x-8896) = 0$
4	$x^6+x^5+1401x^4-240589x^3+2261981x^2+115236171x+4199299651 = 0$
5	$(x+246)(x-6)(x+36)(x-69)(x-174)(x-34) = 0$
6	$x^6+x^5+68629x^4+65441167x^3-11911884179x^2-3634387286753x+ +631587847585633 = 0$

We now define $x_i^{(n)}$ by

$$x_i^{(n)} = e\eta_i^{(n)}+(-1)^n, \tag{4.3}$$

then by (3.2)

$$\sum_{i=0}^{e-1} x_i^{(n)} = 0. \tag{4.4}$$

Theorem 3.2 can now be restated in terms of the x's to read

$$ex_j^{(n)} = \sum_{i=0}^{e-1} x_i^{(n-m-1)} x_{j-i}^{(m)}. \tag{4.5}$$

Squaring (4.3) we have after summing over i

$$\sum_{i=0}^{e-1} (x_i^{(n)})^2 = e^2 \sum_{i=0}^{e-1} (\eta_i^{(n)})^2 + 2e(-1)^n \sum_{i=0}^{e-1} \eta_i^{(n)} + e.$$

Hence by Theorem 3.1 with $j = 0$ we have

$$\sum_{i=0}^{e-1} (x_i^{(n)})^2 = \begin{cases} -ep^{n+1} & \text{if } n \text{ is even and } f \text{ odd}, \\ e(e-1)p^{n+1} & \text{otherwise}. \end{cases} \tag{4.6}$$

Thus the hyper-period equations whose roots are x_i begin

$$\begin{aligned} &x^e + \frac{e}{2} p^{n+1} x^{e-2} + \ldots \quad && \text{if } n \text{ is even and } f \text{ odd}, \\ &x^e - \binom{e}{2} p^{n+1} x^{e-2} + \ldots && \text{otherwise}. \end{aligned} \tag{4.7}$$

For $e = 2$ the equation becomes

$$x^2 - (\chi(-1)p)^{n+1} = 0$$

so that

$$x_i^{(n)} = \pm p^{(n+1)/2} \quad (i = 0, 1). \tag{4.8}$$

The determination of the sign in (4.8) corresponds to the famous problem of the sign of the Gauss sum for $n = 0$. Fortunately formula (4.5) enables us to prove that this determination holds for all n:

THEOREM 4.3. *For* $e = 2$

$$x_0^{(n)} = (\chi(-1)\,p)^{(n+1)/2}, \qquad x_1^{(n)} = -(\chi(-1)p)^{(n+1)/2}.$$

Proof. Since $x_0 + x_1 = 0$ by (4.4) it suffices to prove the first statement of the theorem. For $n = 0$ that statement is

$$x_0 = \sqrt{\chi(-1)p} = \sum_{h=0}^{p-1} \varepsilon(h^2) \tag{4.9}$$

which is the well known formula for the Gauss sum. Many proofs of (4.9) are available, the most recent elementary proof being that of Mordell [6]. To complete the proof by induction it suffices to show that

$$x_0^{(n)} = (x_0)^{n+1}. \tag{4.10}$$

Suppose that (4.10) holds for $n-1$, so that $x_0^{(n-1)} = (x_0)^n$. Using (4.5) with $e = 2$, $m = j = 0$ we have

$$2x_0^{(n)} = x_0^{(n-1)} x_0 + x_1^{(n-1)} x_1 = 2x_0^{(n-1)} x_0 = 2(x_0)^{n+1}.$$

This completes the induction.

For $e = 3$ it was known to Gauss that the x_i satisfy the irreducible cubic equation

$$x^3 - 3px - pL = 0 \tag{4.11}$$

where

$$4p = L^2 + 27M^2, \qquad L \equiv 1 \pmod 3, \tag{4.12}$$

whose roots are given by (see for example [5])

$$2\sqrt{p}\cos\varphi, \qquad 2\sqrt{p}\cos(\varphi + 2\pi/3), \qquad 2\sqrt{p}\cos(\varphi - 2\pi/3) \tag{4.13}$$

where

$$\cos 3\varphi = L/(2\sqrt{p}). \tag{4.14}$$

Of the three essentially different values of φ satisfying (4.14) we choose that one for which

$$x_0 = 2\sqrt{p}\cos\varphi.$$

Then with an appropriate choice of sign

$$x_1 = 2\sqrt{p}\cos(\varphi \pm 2\pi/3) \quad \text{and} \quad x_2 = 2\sqrt{p}\cos(\varphi \mp 2\pi/3).$$

THEOREM 4.4. *For $e = 3$, let*

$$x_0 = 2\sqrt{p}\cos\varphi, \quad x_1 = 2\sqrt{p}\cos(\varphi + a), \quad x_2 = 2\sqrt{p}\cos(\varphi - a)$$

where $a = \pm 2\pi/3$. Then

$$x_0^{(n)} = 2p^{(n+1)/2}\cos(n+1)\varphi,$$
$$x_1^{(n)} = 2p^{(n+1)/2}\cos[(n+1)\varphi + a],$$
$$x_2^{(n)} = 2p^{(n+1)/2}\cos[(n+1)\varphi - a].$$

Proof. The theorem is true for $n = 0$ by hypothesis. Suppose that it holds for $n-1$, then by (4.5) we have

$$\begin{aligned} 3x_0^{(n)} &= x_0^{(n-1)}x_0 + x_1^{(n-1)}x_2 + x_2^{(n-1)}x_1 \\ &= 2p^{(n+1)/2}\{2\cos n\varphi\cos\varphi + 2\cos(n\varphi + a)\cos(\varphi - a) + \\ &\qquad + 2\cos(n\varphi - a)\cos(\varphi + a)\} \\ &= 2p^{(n+1)/2}\{3\cos(n+1)\varphi + \cos(n-1)\varphi + \cos[(n-1)\varphi - a] + \\ &\qquad + \cos[(n-1)\varphi + a]\} \end{aligned}$$

so that

$$x_0^{(n)} = 2p^{(n+1)/2}\cos(n+1)\varphi$$

which completes the induction for $x_0^{(n)}$. The other two cases of $x_1^{(n)}$ and $x_2^{(n)}$ follow in the same way.

By (4.7) the hyper-period equation for x_i is of the form

$$x^3 - 3p^{n+1}x - p^{n+1}V_{n+1} = 0$$

where

$$\begin{aligned} p^{n+1}V_{n+1} &= x_0^{(n)}x_1^{(n)}x_2^{(n)} \\ &= 8p^{3(n+1)/2}\cos(n+1)\varphi\cos[(n+1)\varphi + a]\cos[(n+1)\varphi - a] \end{aligned}$$

or

$$\begin{aligned} V_{n+1} &= 4p^{(n+1)/2}\cos(n+1)\varphi\left[\cos 2(n+1)\varphi - \frac{1}{2}\right] \\ &= 2p^{(n+1)/2}\cos 3(n+1)\varphi. \end{aligned}$$

Using the recurrence

$$\cos 3(n+1)\varphi = 2\cos 3\varphi\cos 3n\varphi - \cos 3(n-1)\varphi$$

and (4.14), we obtain the following theorem.

THEOREM 4.5. *The hyper-period equation for $e = 3$ is*

$$x^3 - 3p^{n+1}x - p^{n+1}V_{n+1} = 0, \tag{4.15}$$

where

$$V_0 = 2, \quad V_1 = L, \quad V_{n+1} = LV_n - pV_{n-1}.$$

To the Lucas function V_n corresponds the function U_n given by

$$U_0 = 0, \quad U_1 = 1, \quad U_{n+1} = LU_n - pU_{n-1}.$$

These functions are related by

$$V_n^2 + 27M^2U_n^2 = 4p^n \tag{4.16}$$

in view of (4.12). This enables us to give a simple formula for the discriminant of (4.15).

THEOREM 4.6. *The discriminant of the cubic hyper-period equation is*

$$D_n = [27p^{n+1}MU_{n+1}]^2.$$

Proof.

$$\begin{aligned} D_n &= 4(3p^{n+1})^3 - 27(p^{n+1}V_{n+1})^2 \\ &= 27p^{2(n+1)}[4p^{n+1} - V_{n+1}] = 27^2p^{2(n+1)}M^2U_{n+1}^2 \end{aligned}$$

by (4.16).

By Theorem 4.1 the $x_i^{(3t-1)}$ are integers. By Theorem 4.4 these integers are

$$x_0^{(3t-1)} = p^tV_{3t}, \quad x_1^{(3t-1)} = -p^t(V_{3t} + 9MU_{3t})/2,$$
$$x_2^{(3t-1)} = -p^t(V_{3t} - 9MU_{3t})/2.$$

As t varies the three roots satisfy the recurring series

$$x_i^{(3t+2)} = pLx_i^{(3t-1)} - p^3x_i^{(3t-4)},$$

the initial conditions being

$$x_0^{(-1)} = 2, \quad x_1^{(-1)} = -1, \quad x_2^{(-1)} = -1,$$
$$x_0^{(2)} = pL, \quad x_1^{(2)} = -(L+9M)p/2, \quad x_2^{(2)} = -(L-9M)p/2.$$

By Theorem 4.1, the roots $x_i^{(n)}$ satisfy an irreducible cubic equation if $n \neq 3t-1$. An independent proof of this follows from Eisenstein's criterion and its extension (see for example [2]). For $e = 4$, the classical period equation was first given by Lebesgue [1] in factored form and can be written

$$\{x^2 - 2\sqrt{p}x + [1-2\chi(2)]p + 2a\sqrt{p}\}\{x^2 + 2\sqrt{p}x + [1-2\chi(2)]p - 2a\sqrt{p}\} = 0$$

where

$$p = a^2 + b^2, \quad a \equiv 1 \pmod 4)$$

and where the first factor has the roots x_0 and x_2 and the second factor x_1 and x_3.

By (4.5) we have

$$4x_0^{(1)} = x_0^2 + x_2^2 + 2x_1x_3 = 4p - 2x_0x_2 + 2x_1x_3 = 4p - 8a\sqrt{p}$$

so that

$$x_0^{(1)} = \sqrt{p}(\sqrt{p} - 2a) \quad \text{and} \quad x_2^{(1)} = \sqrt{p}(\sqrt{p} + 2a)$$

while x_1 and x_3 are $-\sqrt{p}(\sqrt{p} \pm 2b)$.

Letting $-a/\sqrt{p} = \cos\gamma$ we can choose γ so that

$$\begin{aligned} x_0^{(1)} &= p(1+2\cos\gamma), & x_1^{(1)} &= -p(1+2\sin\gamma), \\ x_2^{(1)} &= p(1-2\cos\gamma), & x_3^{(1)} &= -p(1-2\sin\gamma). \end{aligned} \tag{4.17}$$

In general, we have for n odd the following theorem.

THEOREM 4.7. *For* $e = 4$

$$\begin{aligned} x_0^{(2t-1)} &= p^t(1+2\cos t\gamma), & x_2^{(2t-1)} &= p^t(1-2\cos t\gamma), \\ x_1^{(2t-1)} &= -p^t(1+2\sin t\gamma), & x_3^{(2t-1)} &= -p^t(1-2\sin t\gamma) \end{aligned}$$

where

$$\cos\gamma = -a/\sqrt{p}. \tag{4.18}$$

Proof. By (4.17) the theorem is true for $x_i^{(1)}$. Assume that it holds for $x_i^{(2t-1)}$, then by (4.5) we have

$$\begin{aligned} 4x_0^{(2t+1)} &= x_0^{(2t-1)}x_0^{(1)} + x_1^{(2t-1)}x_3^{(1)} + x_2^{(2t-1)}x_2^{(1)} + x_3^{(2t-1)}x_1^{(1)} \\ &= p^{t+1}[(1+2\cos t\gamma)(1+2\cos\gamma) + (1+2\sin t\gamma)(1-2\sin\gamma) + \\ &\quad + (1-2\cos t\gamma)(1-2\cos\gamma) + (1-2\sin t\gamma)(1+2\sin\gamma)] \end{aligned}$$

or

$$\begin{aligned} x_0^{(2t+1)} &= p^{t+1}[1 + 2\cos t\gamma\cos\gamma - 2\sin t\gamma\sin\gamma] \\ &= p^{t+1}[1 + 2\cos(n+1)\gamma]. \end{aligned}$$

This completes the induction for x_0. The remaining three cases are similarly disposed of and the theorem follows.

The following inequalities on the roots are an obvious consequence of the theorem:

$$-p^t < x_0^{(2t-1)}, \quad x_2^{(2t-1)} < 3p^t, \quad -3p^t < x_1^{(2t-1)}, \quad x_3^{(2t-1)} < p^t.$$

It also follows from the theorem that

$$x_0^{(2t-1)} + x_2^{(2t-1)} = 2p^t, \quad x_1^{(2t-1)} + x_3^{(2t-1)} = -2p \tag{4.19}$$

while

$$\begin{aligned} x_0^{(2t-1)}x_2^{(2t-1)} &= p^{2t}(1-4\cos^2 t\gamma), \\ x_1^{(2t-1)}x_3^{(2t-1)} &= p^{2t}(1-4\sin^2 t\gamma). \end{aligned} \tag{4.20}$$

We can now give a general form of the quartic hyperperiod equation for n odd as a product of two quadratics as follows:

THEOREM 4.8. *The hyper-period equation for* $e = 4$ *and* $n = 2t-1$ *can be written as*

$$[x^2 - 2p^tx - p^t(p^t + W_t)][x^2 + 2p^tx - p^t(p^t - W_t)] = 0$$

where

$$W_0 = 2, \quad W_1 = 4a^2 - 2p, \quad W_{n+1} = W_1W_n - p^2W_{n-1}.$$

Proof. Let

$$W_t = 2p^t\cos 2t\gamma$$

where γ is defined by (4.18), then it can be easily verified that W_n satisfies the initial conditions and recurrence stated in the theorem. Therefore by (4.20)

$$x_0^{(2t-1)}x_2^{(2t-1)} = -p^t(p^t + W_t), \quad x_1^{(2t-1)}x_3^{(2t-1)} = -p^t(p^t - W_t)$$

and the theorem follows using (4.19).

5. Congruence properties of the hyper-periods. In this section we shall assume that e is prime to $n+1$. Then by Theorem 4.1 the hyper-periods satisfy an irreducible equation

$$F_e^{(n)}(z) = \prod_{i=0}^{e-1}(z - \eta_i^{(n)}) = 0$$

of degree e with integer coefficients.

We first consider the divisibility properties of the hyper-periods with respect to the prime p itself. We let

$$\varepsilon = \exp(2\pi i/p) = \varepsilon(1) \tag{5.1}$$

then the prime p can be written in the cyclotomic field $R(\varepsilon)$ as

$$p = \prod_{\nu=1}^{p-1}(1-\varepsilon^\nu). \tag{5.2}$$

We first prove the following lemma.

LEMMA 5.1. *There exist integers $X_i^{(n)}$ in the cyclotomic field $R(\varepsilon)$ such that*

$$e^n x_i^{(n)} = (1-\varepsilon)^{n+1} X_i^{(n)}. \tag{5.3}$$

Proof. First of all for $n=0$ we have

$$x_i = e\eta_i + 1 = e\sum_{h\epsilon C_i} \varepsilon(h) - \sum_{x=1}^{p-1} \varepsilon(x).$$

This can be written as

$$x_i = \sum_{h\epsilon C_i} \sum_{\nu=1}^{e-1} [\varepsilon(h) - \varepsilon(g^\nu h)]$$

so that $1-\varepsilon$ can be seen to be a factor of each of the differences $[\varepsilon(h) - \varepsilon(g^\nu h)]$. Hence the lemma is true for $n=0$. Next assume the lemma to hold for $n-1$. Substituting the expression for $x_i^{(n-1)}$ and x_{j-i} into (4.5) with $m=0$, we obtain

$$e^n x_i^{(n)} = (1-\varepsilon)^{n+1} \sum X_i^{(n-1)} X_{j-i} = (1-\varepsilon)^{n+1} X_i^{(n+1)}$$

which is the lemma.

THEOREM 5.1. *If $(e, n+1) = 1$, the product*

$$P_k^{(n)} = \prod_{i=0}^{e-1} (\eta_i^{(n)} - \eta_{i+k}^{(n)}) = e^{-e} \prod_{i=0}^{e-1} (x_i^{(n)} - x_{(i+k)}^{n})$$

is a rational integer divisible by p^{n+1}.

Proof. Applying Lemma 3.1 to (5.3) we have

$$e^n [x_{i+(n+1)s}^{(n)} - x_{i+(n+1)s+k}^{(n)}] = (1-\varepsilon^\sigma)^{n+1} [X_{i+(n+1)s}^{(n)} - X_{i+(n+1)s+k}^{(n)}].$$

Since $n+1$ is prime to e, the product $P_k^{(n)}$ remains invariant when ε is replaced by ε^σ and is therefore an integer. Moreover

$$e^{(n+1)e} P_k^{(n)} = \prod_{\sigma=1}^{e-1} (1-\varepsilon^\sigma)^{n+1} \prod_{i=1}^{e-1} (X_i^{(n)} - X_{i+k}^{(n)})$$

is divisible by p^{n+1} by (5.2).

A similar argument shows that every symmetric function of the x's is divisible by p^{n+1}. In particular

$$\prod_{i=0}^{e-1} x_i^{(n)} \equiv 0 \pmod{p^{n+1}}. \tag{5.3'}$$

We recall the usual definition of congruences involving the classical periods, with respect to a prime modulus q.

DEFINITION. *We say that $N \equiv M \pmod q$, where*

$$N = \sum_{i=0}^{e-1} n_i \eta_i \quad \text{and} \quad M = \sum_{i=0}^{e-1} m_i \eta_i$$

if and only if

$$n_i \equiv m_i \pmod q \quad (i = 0, 1, \ldots, e-1).$$

LEMMA 5.2. *If $r \equiv \operatorname{ind} q \pmod e$, then*

$$[\eta_i^{(n)}]^p \equiv (-1)^n f \pmod p, \quad [\eta_i^{(n)}]^q \equiv \eta_{i+(n+1)r}^{(n)} \pmod q \quad (q \neq p).$$

Proof. The lemma is well known for $n=0$ and follows easily from the fact that the qth power binomial coefficients are divisible by q. For $n>0$ and $q \neq p$, we have, by Theorem 3.4,

$$[\eta_i^{(n)}]^q = \Big[\sum_{k=0}^{e-1} c_{i,k}^{(n)} \eta_k\Big]^q \equiv \sum_{k=0}^{e-1} c_{i,k}^{(n)} \eta_k^q \equiv \sum_{k=0}^{e-1} c_{i,k}^{(n)} \eta_{k+r} \pmod q.$$

But by (3.18), with $s=r$ we have

$$c_{i,k}^{(n)} = c_{i+(n+1)r,k+r}^{(n)}.$$

Hence

$$[\eta_i^{(n)}]^q \equiv \sum_{\nu=0}^{e-1} c_{i+(n+1)r,\nu}^{(n)} \eta_\nu = \eta_{i+(n+1)r}^{(n)} \pmod q.$$

The second statement of the lemma follows in the same way.

LEMMA 5.3. *All the hyper-periods $\eta_i^{(n)}$ are incongruent modulo a prime $q \neq p$.*

Proof. Suppose that some two hyper-periods were congruent, say

$$\eta_i^{(n)} \equiv \eta_j^{(n)} \pmod q \quad (i \neq j).$$

Then it follows from Lemma 3.1 that

$$\eta_{i+(n+1)s}^{(n)} \equiv \eta_{j+(n+1)s}^{(n)} \pmod q \quad \text{for} \quad s = 0, 1, \ldots, e-1.$$

Since $n+1$ is prime to e this makes all the hyper-periods congruent modulo q. By (3.2) their sum is $(-1)^n$ and hence we would have

$$e\eta_i^{(n)} \equiv (-1)^n \pmod q \quad (i = 0, 1, \ldots, e-1)$$

so that

$$x_i^{(n)} = e\eta_i^{(n)} + (-1)^{n+1} \equiv 0 \pmod q \quad (i = 0, 1, \ldots, e-1).$$

But Theorem 3.1 for odd e and $j \neq 0$ can be written

$$\sum_{i=0}^{e-1} x_i^{(n)} x_{i+j}^{(n)} = -ep^{n+1}$$

so that q^2 divides ep^{n+1}. This contradicts the assumption $q \neq p$ and the lemma follows.

We are now in a position to prove the following theorem:

THEOREM 5.2. *If $(n+1, e) = 1$, the discriminant D_n of the hyper-period equation is divisible by $p^{(e-1)(n+1)}$, and only by those primes $q \neq p$ which are e-th power residues of p, where e is a prime.*

Proof. The absolute value of the discriminant can be written

$$|D_n| = \prod_{k=1}^{e-1} P_k^{(n)}.$$

Hence by Theorem 5.1 the discriminant is divisible by $p^{(e-1)(n+1)}$.

Suppose that contrary to the statement of the theorem some $P_k^{(n)}$ contains a prime factor q which is not an eth power residue. Then $\operatorname{ind} q = r$ is prime to e. By Lemma 5.2 with $i = 0$ and $i = k$

$$(\eta_0^{(n)} - \eta_k^{(n)})^q \equiv \eta_{(n+1)r}^{(n)} - \eta_{(n+1)r+k}^{(n)} (\operatorname{mod} q).$$

Iterating this expression we get

$$(\eta_0^{(n)} - \eta_k^{(n)})^{q^t} \equiv \eta_{(n+1)rt}^{(n)} - \eta_{(n+1)rt+k}^{(n)} (\operatorname{mod} q).$$

Multiplying these congruences together for all $t < e$ gives

$$\prod_{t=0}^{e-1} (\eta_0^{(n)} - \eta_k^{(n)})^{q^t} = (\eta_0^{(n)} - \eta_k^{(n)})^{(q^e-1)/(q-1)} \equiv \prod_{i=0}^{e-1} (\eta_i^{(n)} - \eta_{i+k}^{(n)}) \equiv P_k^{(n)}.$$

Since q divides $P_k^{(n)}$ by assumption it must also divide $(\eta_0^{(n)} - \eta_k^{(n)})^{q^e}$ but by Lemma 5.2

$$(\eta_0^{(n)} - \eta_k^{(n)})^{q^e} \equiv \eta_0^{(n)} - \eta_k^{(n)} (\operatorname{mod} q),$$

so that q would have to divide $(\eta_0^{(n)} - \eta_k^{(n)})$, but all the η's are incongruent modulo q by Lemma 5.3. Hence our assumption that r is prime to e is false and q is an eth power residue. This completes the proof of the theorem.

THEOREM 5.3. *Let e be a prime not dividing $n+1$ and let $q \neq p$ be any prime; then the congruence*

$$F_e^{(n)}(z) \equiv 0 (\operatorname{mod} q) \tag{5.4}$$

has e solutions or none, according as q is or is not an e-th power residue of p.

Proof. Let $\operatorname{ind} q \equiv r (\operatorname{mod} e)$. Substituting $z = \eta_i^{(n)}$ into Lagrange's identical congruence

$$z - z^q \equiv z(1-z)(2-z)\ldots(q-1-z) \ (\operatorname{mod} q)$$

we obtain by Lemma 5.2

$$\eta_i^{(n)} - \eta_{i+(n+1)r}^{(n)} = \eta_i^{(n)}(1-\eta_i^{(n)})\ldots(q-1-\eta_i^{(n)}).$$

Multiplying these congruences together for $i = 0, 1, \ldots, e-1$ we obtain

$$P_{(n+1)r}^{(n)} \equiv F_e^{(n)}(0) F_e^{(n)}(1) \ldots F_e^{(n)}(q-1) \ (\operatorname{mod} q). \tag{5.5}$$

If $r \equiv 0 (\operatorname{mod} e)$ so that q is an eth power residue of p, then $P_{(n+1)r}$ vanishes and so the congruence (5.4) has a solution. Since the equation $F_e(z) = 0$ is abelian, the congruence has e solutions since it has one solution. These roots are not necessarily incongruent.

Next suppose that $r \not\equiv 0 (\operatorname{mod} e)$ and that (5.4) has a solution modulo q. Then by (5.5) q would divide the discriminant D_n of $F_e(z)$. This contradicts Theorem 5.2.

As a corollary, we can state the following theorem:

THEOREM 5.4. *Let e be a prime not dividing $n+1$ and let N be an arbitrary integer; then the prime factors of $F_e(N)$ are either p or e-th power residues of p.*

As to the divisibility by p, it can be seen from Lemma 5.2 that

$$F_e(z) \equiv \big(z - (-1)^n f\big)^e (\operatorname{mod} p)$$

so that $(-1)^n f$ is a root of multiplicity e.

As an example of the above for $e = 5$, $p = 11$, $n = 1$

$$F_5(z) = z^5 - z^4 - 48z^3 - 63z^2 + 91z - 23$$

we have

$$D = 11^8 \cdot 67^2,$$

$$F_5(z) \equiv (z+2)^5 \ (\operatorname{mod} 11),$$

$$F_5(z) \equiv z(z-7)(z-11)(z-12)(z-17) \ (\operatorname{mod} 23),$$

$$F_5(z) \equiv (z-1)(z-6)(z-14)(z-31)(z-35) \ (\operatorname{mod} 43),$$

$$F_5(z) \equiv (z-12)(z-18)^2(z-26)(z-61) \ (\operatorname{mod} 67).$$

If we apply Theorems 5.2 and 5.4 to the cubic hyper-period equations and their discriminants given explicitly by Theorems 4.5 and 4.6, we obtain an interesting result about the prime factors of the terms of some rather special Lucas sequences as follows.

THEOREM 5.5. *Let $4p = L^2+27M^2$, let p be a prime and let $L \equiv 1 \pmod 3$, let*

$$V_0 = 2, \quad V_1 = L, \quad V_{n+1} = LV_n - pV_{n-1},$$

$$U_0 = 0, \quad U_1 = 1, \quad U_{n+1} = LU_n - pU_{n-1},$$

then the divisors of U_n and V_n for $n \not\equiv 0 \pmod 3$ are cubic residues of p.

In particular, for $p = 7$, $L = 1$, the terms of the series

$$0, 1, 1, -6, -13, 29, 120, -83, -923, -342, 6119, 8513, \ldots,$$

$$U_{n+1} = U_n - 7U_{n-1}$$

which are odd have divisors of the form $14k \pm 1$ exclusively.

A similar theorem can be obtained by applying Theorem 5.2 to $P_2^{(n)}$ for $e = 4$, namely

THEOREM 5.6. *Let $p = a^2+b^2$ be a prime, let*

$$W_0 = 1, \quad W_1 = 4a^2 - p, \quad W_{n+1} = (4a^2-2p)W_n - p^2 W_{n-1},$$

then all the divisors of W_n are quadratic residues of p.

For example for $p = 5$ all the divisors of the series

$$1, -1, -19, 139, -359, -1321, 16901, -68381, -12239, \ldots,$$

$$U_{n+1} = -6U_n - 25U_{n-1}$$

are of the form $10n \pm 1$.

For $e = 5$ we may use the relation (3.25) to get

$$\tau^{(n)}(\alpha)\tau^{(n)}(\alpha^4) = \tau^{(n)}(\alpha^2)\tau^{(n)}(\alpha^3).$$

This with Theorem 3.6 and an identity from the theory of the quintic equation apparently first given by Young [8] leads to

$$\tau^{5(n+1)}(\alpha) + \tau^{5(n+1)}(\alpha^2) + \tau^{5(n+1)}(\alpha^3) + \tau^{5(n+1)}(\alpha^4) = x_0^{(n)} x_1^{(n)} x_2^{(n)} x_3^{(n)} x_4^{(n)}.$$

Hence the constant terms of the hyper-period equations for $e = 5$ form a recurring series of the fourth order whose scale of relation is the quartic equation satisfied by the $\tau(\alpha^\nu)$. By Theorem 5.4, all the divisors of the terms of such a series, whose subscripts are not divisible by 5 are either p itself or quintic residues of p.

For example for $p = 11$ we tabulate the series whose recurrence is

$$V_{n+4} = -(89V_{n+3} + 3861V_{n+2} + 118459V_{n+1} + 1771561V_n)$$

n	V_n
0	4
1	−89
2	199
3	$-29459 = 89 \cdot 331$
4	5310119
5	$-224763804 = 2^2 \cdot 3^2 \cdot 29 \cdot 41 \cdot 59 \cdot 89$
6	$2638752139 = 199 \cdot 241 \cdot 55021$
7	$56121135751 = 89 \cdot 630574559$
8	$2035092641759 = 1759 \cdot 1156960001$
9	$-312208100506919 = 89^2 \cdot 331 \cdot 119079269$
10	$8606264257237604 = 2^2 \cdot 19^2 \cdot 199 \cdot 2081 \cdot 3581 \cdot 4019$

The prime factors of V_n are seen to be of the form $22k \pm 1$ except for $n = 5$ and 10.

References

[1] P. Bachmann, *Die Lehre von der Kreistheilung*, Leipzig 1872.
[2] G. Birkhoff and S. MacLane, *Survey of modern algebra*, p. 78, ex. 5.
[3] L. Carlitz, *Multiple Exponential Sums*, Pacific Journ. Math. 15 (1965), pp. 757-765.
[4] D. H. and Emma Lehmer, *The cyclotomy of Kloosterman sums*, Acta Arith. 12 (1967), pp. 385-407.
[5] G. B. Matthews, *Theory of Numbers*, p. 223.
[6] L. J. Mordell, *The sign of the Gaussian sum*, Illinois Journ. Math. 6 (1962), pp. 177-180.
[7] H. Salié, *Über die Kloostermanschen Summen $S(u, v; q)$*, Math. Zeitschr. 34 (1932), pp. 91-109.
[8] G. P. Young, *Resolution of a solvable equation of the fifth degree*, Amer. Journ. Math. 6 (1883), pp. 106-107.

Reçu par la Rédaction le 27. 5. 1967