constant depending upon β, this and similar estimates show that we can construct a subsequence B of A which satisfies, for an infinity of values of x,

(i) $B(n) \sim Cn^{\alpha}(\log n)^{-\beta} \sim CA(n)(\log n)^{-\beta}$,

(ii) $\sum_{b_i \leqslant n} \nu^k(b_i) \sim (1-\beta)^k B(n)(\log\log n)^k$,

as $x \to \infty$ through integral powers of e.

We do this by analogy with the earlier limiting example. Thus, we can find such a subsequence of almost all sequences A. Clearly the set of sequences B has measure zero with respect to the measure induced by the μ_i corresponding to $M(n)$.

References

[1] М. Б. Барбан, *Мультипликативные функции от Σ_R-равнораспределенных последовательностей*, Известия Акад. Наук. Узбек., Серия физ.-мат. наук 6 (1964), pp. 13-19.

[2] T. G. van der Corput, *Une inégalité relative au nombre des diviseurs*, Proc. K. Neder. Akad. van. Wet. Amsterdam 42 (1939), pp. 547-553.

[3] P. Erdös, *On the sum* $\sum_{k=1}^{x} d(f(k))$, J.Lond. Math. Soc. 27 (1952), pp. 7-15.

[4] — *Problems and results in additive number theory*, Colloque sur la théorie des nombres, Bruxelles 1955, pp. 127-137.

[5] P. Erdös and A. Rényi, *Additive properties of random sequences of positive integers*, Acta Arith. 6 (1960), pp. 83-110.

[6] H. Halberstam, *On the distribution of additive number-theoretic functions I-III*, J. Lond. Math. Soc. 30 (1955), pp. 43-53; 31 (1956), pp. 1-14; pp. 15-28.

[7] G. H. Hardy and S. Ramanujan, *The normal number of prime factors of a number n*, Quart. J. Math. 48 (1917), pp. 76-92.

[8] C. Hooley, *On the representation of numbers as the sum of two squares and a prime*, Acta Math. 97 (1957), pp. 189-210.

[9] J. Kubilius, *Probabilistic methods in the theory of numbers*, A. M. S. Translations no. 11, 1964.

[10] A. Kolmogoroff, *Grundbegriffe der Wahrscheinlichkeitsrechnung*, Berlin 1933.

[11] T. Nagell, *Généralisation d'un théorème de Tchebycheff*, Journ. de Math. 8 Série, 4 (1921), pp. 343-356.

[12] K. Prachar, *Primzahlverteilung*, Berlin 1957.

[13] A. Selberg, *Note on a paper of L. G. Sathe*, J. Indian Math. Soc. N. S. 18 (1954), pp. 83-87.

[14] E. C. Titchmarsh, *The theory of the Riemann zeta function*, Oxford 1951.

UNIVERSITY OF NOTTINGHAM

Reçu par la Rédaction le 20. 8. 1966

ACTA ARITHMETICA
XII (1967)

The cyclotomy of Kloosterman sums

by

D. H. and EMMA LEHMER (Berkeley, Calif.)

1. Introduction. Historically the Kloosterman sum arose as a coefficient in the expansion of certain series giving the number of representations of integers by various quadratic forms. Thus it was that questions of the order of magnitude of the Kloosterman sums were uppermost in the minds of writers of the many papers on these sums. In this paper we try to indicate that Kloosterman sums have rather interesting intrinsic properties not depending on their estimated magnitude. In particular we show that there is a complete theory, parallel to the classical theory of cyclotomy, in which the Kloosterman sums now play the role of the roots of unity.

To be more precise some notation will be needed to which we adhere throughout the paper.

Let p be an odd prime and let

$$\varepsilon(\nu) = \exp\{2\pi i\nu/p\}. \tag{1.0}$$

The ordinary Kloosterman sum will be denoted as usual by

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

so that

$$S(0) = \sum_{x=1}^{p-1} \varepsilon(x) = -1. \tag{1.2}$$

In § 3 we investigate sums of products of Kloosterman sums extending the early results of Salié [10]. The methods used here apply equally well to the more general Kloosterman sum

$$S_k(h) = \sum_{x=1}^{p-1} \varepsilon(x+hx^k) \tag{1.3}$$

where k is an integer prime to $p-1$, so that x^k modulo p runs through the numbers $1(1)p-1$ as x does. A still more general sum would be

$$S_{(\sigma)}(h) = \sum_{x=1}^{p-1} \varepsilon\big(x+h\sigma(x)\big)$$

where $\sigma(x)$ is a permutation of the numbers from 1 to $p-1$. For our purposes however we would need to assume that the function σ is odd and multiplicative, modulo p, that is

$$\sigma(x) \equiv -\sigma(-x), \qquad \sigma(x)\sigma(y) \equiv \sigma(xy) \pmod{p}.$$

It is easily shown that for every such permutation σ there is an integer k prime to $p-1$ such that

$$\sigma(x) \equiv x^k \pmod{p} \qquad (x = 1(1)p-1).$$

In fact

$$k \equiv \operatorname{ind}_g \sigma(g) \pmod{p-1}$$

for any primitive root g of p. Thus we have adopted the notation (1.3). The case $k \equiv -1 \equiv p-2 \pmod{p-1}$ gives us the ordinary Kloosterman sum as (1.1). The case $k = 1$ is a degenerate exponential sum

$$S_1(h) = \sum_{x=1}^{p-1} \varepsilon(x\{1+h\}) = -1+p\,\delta_h^{p-1} \tag{1.4}$$

where we use a Kronecker symbol modulo p,

$$\delta_a^b = \begin{cases} 1 & \text{if} \quad a \equiv b \pmod{p}, \\ 0 & \text{if} \quad a \not\equiv b \pmod{p}. \end{cases} \tag{1.5}$$

Salié had already pointed out that the $p-1$ Kloosterman sums $S(h)$, for $h \neq 0$, fall into two classes according to the value of the Legendre symbol

$$\chi(h) = \left(\frac{h}{p}\right)$$

each set being the roots of an irreducible polynomial of degree $(p-1)/2$. This is the beginning of a theory, developed in §§ 4-7, in which the $p-1$ Kloosterman sums fall into e classes according to the value of $\operatorname{ind} h \pmod{e}$, where e is some divisor of $p-1 = ef$.

In § 4 and 5 we develop the basic relations between the $S_k(h)$ and classical cyclotomy that hold for a general k prime to $p-1$. In § 6 we restrict k to be $p-2$ so we are dealing thereafter with the ordinary Kloosterman sum $S(h)$. For this case we have the well known alternative formula

$$S(h) = \sum_{x=0}^{p-1} \chi(x^2-4h)\,\varepsilon(x) \tag{1.6}$$

easily derived from (1.1). This allows us to utilize the so-called *Jacobsthal sums* to investigate sums and sums of squares of Kloosterman sums over eth power residue classes. Finally in § 7 we consider the equations satisfied by such sums. These equations correspond to the so-called *period equations* of cyclotomy. Rather than the usual enumeration of solutions of congruences, the methods employed in what follows depend on the elementary theory of finite Fourier series, as set forth briefly in § 2. This theory is sufficient to obtain as special cases all the previously known properties of $S(h)$ with one exception. This is the theorem

$$\sum_{h=0}^{p-1} \{S(ch^2)\}^3 = \begin{cases} 2p^2\chi(-c)-p(p-2) & \text{if} \quad p = 6n-1, \\ 4pA^2\chi(-c)+p(p+2) & \text{if} \quad p = A^2+3B^2, \end{cases} \tag{1.7}$$

a rather difficult proof of which was discovered by us in 1959 [6]. Another proof by Mordell [9] is equally sophisticated. This theorem is used in § 7.

Besides the notation $\bar{x}$ defined in (1.1) we shall find it convenient to use x' defined by

$$xx' \equiv 1 \pmod{p-1}. \tag{1.8}$$

The sum $S_k(h)$ was noticed by Davenport [2] in 1933 but was dismissed by him with the remark that $S_k(h)$ for k prime to $p-1$ is essentially the same as $S(h)$ as far as obtaining estimates of magnitude is concerned. We hope to convince the reader that $S_k(h)$ has an important role to play. As evidence we point to Theorems 4.1, 4.2 and 5.1. However there is no denying the fact that the ordinary Kloosterman sum $S(h)$ plays the leading role. This appears to be due to the fact that

$$x(1+x^k) \equiv 1+x \pmod{p}$$

holds only for $k \equiv -1\big(\operatorname{mod}(p-1)\big)$.

From the definition of $S_k(h)$ in (1.1) it follows that

$$\sum_{h=0}^{p-1} S_k(h) = \sum_{x=1}^{p-1} \varepsilon(x) \sum_{h=0}^{p-1} \varepsilon(hx^k) = 0 \tag{1.9}$$

holds for all k prime to $p-1$.

2. General finite Fourier series identities. As Whiteman [13] has pointed out, it is advantageous to employ the inversion and Parseval relations of finite Fourier series to the study of exponential sums. For our purposes we need only simple (i.e., not multiple) Fourier series but we need a more general Parseval relation than that usually referred to (see Schoenberg [11]).

Let m be a positive integer and let

$$\zeta = \exp\{2\pi i/m\}. \tag{2.1}$$

Any real or complex-valued numerical function $F(i)$ defined for $i = 0(1)m-1$ and periodic of period m has as its generator

$$G(\zeta^\nu) = \sum_{i=0}^{m-1} F(i)\zeta^{\nu i} \quad (\nu = 0(1)m-1). \tag{2.2}$$

The inversion formula

$$F(i) = m^{-1}\sum_{\mu=0}^{m-1} G(\zeta^\mu)\zeta^{-\mu i} \tag{2.3}$$

follows at once from the orthogonality relation

$$\sum_{i=0}^{m-1} \zeta^{\nu i}\zeta^{-\mu i} = \begin{cases} m & \mu \equiv \nu(\operatorname{mod} m), \\ 0 & \text{otherwise.}\end{cases} \tag{2.4}$$

The general Parseval relation for two functions F_1 and F_2 and their generators G_1 and G_2 is

$$\sum_{i=0}^{m-1} F_1(i)F_2(ai+b) = m^{-1}\sum_{\mu=0}^{m-1} G_2(\zeta^{-\mu})G_1(\zeta^{a\mu})\zeta^{b\mu}. \tag{2.5}$$

This formula is a trivial consequence of (2.2) and (2.3) in case $a \equiv 0(\operatorname{mod} m)$. Otherwise it follows from (2.3) and (2.4).

In the traditional case of $a = 1$ and $F(i)$ real, (2.5) reduces to the familiar Parseval identity

$$\sum_{i=0}^{m-1} F(i)F(i+b) = m^{-1}\sum_{\mu=0}^{m-1} |G(\zeta^\mu)|^2\zeta^{\mu b}. \tag{2.6}$$

Another case, $a = -1$, gives the convolution type formula

$$\sum_{i=0}^{m-1} F(i)F(b-i) = m^{-1}\sum_{\mu=0}^{m-1} \{G(\zeta^\mu)\}^2\zeta^{-b\mu}. \tag{2.7}$$

3. Various applications to Kloosterman sums. In this section for the application of § 2 we set $m = p$, so that in the notation of (1.0)

$$\zeta^\nu = \varepsilon(\nu). \tag{3.0}$$

If we set

$$G(\varepsilon(\mu)) = \begin{cases} p\varepsilon(-\mu^{k'}) & \mu \not\equiv 0(\operatorname{mod} p), \\ 0 & \mu \equiv 0(\operatorname{mod} p),\end{cases} \tag{3.1}$$

where $kk' \equiv 1(\operatorname{mod} p-1)$, then (2.3) becomes, for $i = h$,

$$F(h) = \sum_{\mu=1}^{p-1} \varepsilon\{-\mu^{k'}-\mu h\} = \sum_{x=1}^{p-1} \varepsilon(x+x^k h) = S_k(h), \tag{3.2}$$

using the substitution $x \equiv -\mu^{k'}(\operatorname{mod} p)$. Thus (3.1) is the generator of the general Kloosterman sum $S_k(h)$.

THEOREM 1. *Let a and b be integers, $a \not\equiv 0(\operatorname{mod} p)$; then*

$$\sum_{i=0}^{p-1} S_k(i)S_k(ai+b) = pS_k\big(b(1-a^{k'})^{-k}\big)+p^2\delta_b^0\delta_1^a. \tag{3.3}$$

Proof. Substituting (3.2) into (2.5) and using (3.1) gives us

$$\sum_{i=0}^{p-1} S_k(i)S_k(ai+b) = p\sum_{\mu=1}^{p-1} \varepsilon\big(\mu^{k'}-(\mu a)^{k'}+\mu b\big) \tag{3.4}$$
$$= p\sum_{x=1}^{p-1} \varepsilon(x-xa^{k'}+bx^k).$$

In case $a \not\equiv 1(\operatorname{mod} p)$ we set

$$(1-a^{k'})x \equiv y(\operatorname{mod} p)$$

so that the last sum becomes

$$\sum_{y=1}^{p-1} \varepsilon\big(y+b(1-a^{k'})^{-k}y^k\big) = S_k\big(b(1-a^{k'})^{-k}\big).$$

To complete the proof we let $a \equiv 1(\operatorname{mod} p)$. Then (3.4) becomes

$$\sum_{i=1}^{p-1} S_k(i)S_k(i+b) = p\sum_{\mu=1}^{p-1} \varepsilon(\mu b) = p\{-1+p\delta_b^0\}.$$

For the classical Kloosterman sum $S(i) = S_{-1}(i)$, Theorem 1 gives the following interesting special cases

$$\sum_{i=0}^{p-1} S(i)S(ai+b) = pS\big(b(1-\bar{a})\big)+p^2\delta_b^0\delta_a^1, \tag{3.5}$$

$$\sum_{i=0}^{p-1} S(i)S(ai) = -p+\delta_a^1 p^2, \qquad \sum_{i=0}^{p-1} S(i)S(i+b) = -p+\delta_b^0 p^2. \tag{3.6}$$

For $a \equiv 1(\operatorname{mod} p)$, (3.6) give the result of Salié [10]

$$\sum_{i=0}^{p-1} S^2(i) = p^2-p. \tag{3.7}$$

Another special case of (3.5) is the formula

$$\sum_{i=0}^{p-1} S(i)S(b-i) = pS(2b) \tag{3.8}$$

which becomes the convolution

$$\sum_{i=0}^{p-1} S(i)S(p-i) = -p \tag{3.9}$$

when $b \equiv 0 \pmod{p}$. This is also a special case of (3.6).

Another application of § 2 arises from (1.6) which can be written

$$S(ci^2) = p^{-1}\sum_{\mu=0}^{p-1} p\chi(\mu^2 i^2 - 4ci^2)\,\varepsilon(-\mu i).$$

From this we see by (2.3) that

$$G\big(\varepsilon(\mu)\big) = p\chi(\mu^2 - 4c)$$

is the generator of $F(i) = S(ci^2)$. By (2.2) we have inversely

$$\sum_{i=0}^{p-1} S(ci^2)\,\varepsilon(\mu i) = p\chi(\mu^2 - 4c). \tag{3.10}$$

Putting $\mu = 0$ gives

$$\sum_{i=0}^{p-1} S(ci^2) = p\chi(-c), \tag{3.11}$$

a result of Salié [10]. Using (2.5) with $a = 1$ gives, for $c \not\equiv 0 \pmod{p}$,

$$\sum_{i=0}^{p-1} S(ci^2)\,S\big(c(i+b)^2\big) = p\sum_{\mu=0}^{p-1} \varepsilon(b\mu)\,\chi^2(\mu^2 - 4c)$$
$$= \delta_0^b p^2 - p\big(1+\chi(c)\big)\cos(4\pi bm/p)$$

where m is a solution, if any, of the congruence

$$x^2 \equiv c \pmod{p}.$$

The important case of $b = 0$ gives Salié's result [10]

$$\sum_{i=0}^{p-1} S^2(ci^2) = p^2 - p\big(1+\chi(c)\big). \tag{3.12}$$

We consider next the determination of the generator of

$$F(i) = S(i)S(ai), \qquad a \not\equiv 0 \pmod{p},$$

that is

$$G\big(\varepsilon(\nu)\big) = \sum_{i=0}^{p-1} S(i)S(ai)\,\varepsilon(i\nu).$$

If $\nu \equiv 0 \pmod{p}$ we have

$$G(1) = \sum_{i=0}^{p-1} S(i)S(ai) = -p + p^2\delta_a^1 \tag{3.13}$$

by (3.6). For $\nu \not\equiv 0 \pmod{p}$ we have

$$G\big(\varepsilon(\nu)\big) = \sum_{x=1}^{p-1}\sum_{y=1}^{p-1} \varepsilon(x+y)\sum_{i=0}^{p-1} \varepsilon(i\{\bar{x} + a\bar{y} + \nu\})$$
$$= p\sum_{\bar{x}+a\bar{y}\equiv-\nu} \varepsilon(x+y).$$

If we set $y = -\nu xs$ the condition of summation becomes

$$x \equiv -\bar{\nu}(1 - a\bar{s}\bar{\nu}) \pmod{p}.$$

Since $x \not\equiv 0 \pmod{p}$, we must have $s \not\equiv a\bar{\nu} \pmod{p}$. Furthermore,

$$x + y = x(1 - s\nu) \equiv -\bar{\nu}(1-s\nu)(1-a\bar{s}\bar{\nu}) \equiv -\bar{\nu}(1+a) + s + a\bar{\nu}^2\bar{s} \pmod{p}.$$

Hence

$$G\big(\varepsilon(\nu)\big) = p\varepsilon\{-\bar{\nu}(1+a)\}\sum_{s\not\equiv a\nu} \varepsilon(s + a\bar{\nu}^2\bar{s})$$
$$= p\varepsilon\{-\bar{\nu}(1+a)\}[S(a\bar{\nu}^2) - \varepsilon\{\bar{\nu}(1+a)\}],$$

or finally

$$G\big(\varepsilon(\nu)\big) = p[\varepsilon\{-\bar{\nu}(1+a)\}S(a\bar{\nu}^2) - 1]. \tag{3.14}$$

Applying (2.3), we have by (3.13) and (3.14)

$$F(i) = S(i)S(ai) = p^{-1}\Big[G(1) + \sum_{\mu=1}^{p-1} G\big(\varepsilon(\mu)\big)\varepsilon(-\mu i)\Big]$$
$$= -1 + p\delta_a^1 + \sum_{\mu=1}^{p-1} \varepsilon\big(-\bar{\mu}(1+a) - \mu i\big)S(a\bar{\mu}^2) - \sum_{\mu=1}^{p-1} \varepsilon(-\mu i).$$

Letting $\bar{\mu} = -i\nu$ we have

$$S(i)S(ai) = p\delta_a^1 + \sum_{\nu=1}^{p-1} \varepsilon\big((1+a)i\nu + \bar{\nu}\big)S(ai^2\nu^2). \tag{3.15}$$

This formula for the product of any two Kloosterman sums was first given by Davenport [2] in the more symmetrical form $(ai = j)$

$$S(i)S(j) = p\delta_i^j + \sum_{\nu=1}^{p-1} \varepsilon\big((i+j)\nu + \bar{\nu}\big)S(ij\nu^2). \tag{3.16}$$

The possibility of obtaining (3.16) by the inversion (2.3) was pointed out by Whiteman [13].

We now apply (2.6) with $b = 0$ to our current choice of F. By (3.13) and (3.14) we have

$$(3.17)\qquad \sum_{i=0}^{p-1} S^2(i)S^2(ai) = p^{-1}\sum_{\nu=0}^{p-1} G\big(\varepsilon(\nu)\big)G\big(\varepsilon(-\nu)\big)$$

$$= p\Big\{(p\delta_a^1-1)^2+\sum_{\nu=1}^{p-1} S^2(a\bar{\nu}^2)-2\sum_{\nu=1}^{p-1}\varepsilon(\{1+a\}\bar{\nu})S(a\bar{\nu}^2)+p-1\Big\}.$$

The first of the two sums on the right is equal to

$$p^2-\big(1+\chi(a)\big)p-1$$

by (3.12). The second sum on replacing $\bar{\nu}$ by i and using (3.10) becomes

$$\sum_{i=0}^{p-1}\varepsilon\{(1+a)i\}S(ai^2)+1 = p\chi\big((1+a)^2-4a\big)+1$$

$$= p\chi^2(a-1)+1 = p+1-p\delta_a^1.$$

Substituting these values for the two sums into (3.17) and simplifying we have

$$(3.18)\qquad \sum_{i=0}^{p-1} S^2(i)S^2(ai) = p^3(1+\delta_a^1)-p^2\{2+\chi(a)\}-3p.$$

For $a = 1$ we get the result of Salié [10]

$$(3.19)\qquad \sum_{i=0}^{p-1} S^4(i) = 2p^3-3p^2-3p.$$

As an application of (2.5) in which $F_1 \neq F_2$ we consider the sum

$$\sum_{i=0}^{p-1} S(i)S(ai)S(ci)\qquad (ac\not\equiv 0\,(\mathrm{mod}\,p)).$$

For this we set

$$F_1(i) = S(i)S(ai),\qquad F_2(i) = S(ci).$$

The generator G_1 of F_1 is given by (3.13) and (3.14). That of F_2, by (3.1), is

$$G_2\big(\varepsilon(\mu)\big) = \begin{cases} p\varepsilon(-\bar{\mu}) & \mu\not\equiv 0\,(\mathrm{mod}\,p),\\ 0 & \mu\equiv 0\,(\mathrm{mod}\,p).\end{cases}$$

Applying (2.5) (with $a = c$ and $b = 0$) we have by (3.10)

$$\sum_{i=0}^{p-1} S(i)S(ai)S(ci) = p\Big[-\sum_{\mu=1}^{p-1}\varepsilon(\bar{\mu})+\sum_{\mu=1}^{p-1}\varepsilon\{\bar{\mu}-\bar{\mu}\bar{c}(1+a)\}S(a\bar{c}^2\bar{\mu}^2)\Big]$$

$$= p+p\sum_{i=1}^{p-1}\varepsilon\big(i\{1-\bar{c}(1+a)\}\big)S(a\bar{c}^2i^2)$$

$$= p+p\Big[p\chi\big[\big(1-\bar{c}(1+a)\big)^2-4a\bar{c}^2\big]+1\Big]$$

$$= 2p+p^2\chi[(c-1-a)^2-4a]$$

or

$$(3.20)\qquad \sum_{i=0}^{p-1} S(i)S(ai)S(ci) = 2p+p^2\chi[(a-c)^2-2(a+c)+1],$$

a form which exhibits the symmetry in a and c.

For $c = a$ we get the special case

$$(3.21)\qquad \sum_{i=0}^{p-1} S(i)S^2(ai) = 2p+p^2\chi(1-4a),$$

which, for $a = 1$, gives the result of Salié [10]

$$(3.22)\qquad \sum_{i=0}^{p-1} S^3(i) = 2p+p^2\chi(-3).$$

In order that the sum in (3.20) be exactly $2p$ we must have

$$(c-1-a)^2\equiv 4a\,(\mathrm{mod}\,p),$$

so that $\chi(a) = 1$. Letting $a\equiv s^2\,(\mathrm{mod}\,p)$ we have

$$(c-1-s^2) = \pm 2s\qquad\text{or}\qquad c = (s\pm 1)^2$$

Hence if $s\pm 1\not\equiv 0\,(\mathrm{mod}\,p)$ we have

$$(3.23)\qquad \sum_{i=0}^{p-1} S(i)S(s^2i)S\big((s\pm 1)^2i\big) = 2p.$$

For $p = 6n+1$, examples of this are provided by s and $(1+s)$ being solutions of $x^2+x+1\equiv 0\,(\mathrm{mod}\,p)$ and for $p = 10n+1$, we can take for s and $1-s$ the Fibonacci roots of $x^2-x-1\equiv 0\,(\mathrm{mod}\,p)$.

4. Sums over *e*th power residue classes. In (3.11) and (3.12) we are in effect summing the Kloosterman sums and their squares over the set of quadratic residues or non-residues of p. More generally we consider now the problem of summing over eth power residue and non-residue classes, where e is some divisor of $p-1 = ef$. For this purpose we need the following basic facts from the theory of cyclotomy ([1], [2], [3]).

It will be convenient to introduce a Kronecker symbol mod e as

$$\Delta_a^b = \begin{cases} 1 & \text{if} \quad a \equiv b \pmod{e}, \\ 0 & \text{if} \quad a \not\equiv b \pmod{e}. \end{cases} \tag{4.0}$$

Let g be a fixed primitive root of the odd prime $p = ef+1$ and let C_i be the class of all f incongruent x's for which

$$\operatorname{ind}_g(x) \equiv i \pmod{e} \qquad (i = 0(1)e-1).$$

The so-called *cyclotomic periods* η_i are defined by

$$\eta_i = \sum_{h \epsilon C_i} \varepsilon(h) \qquad (i = 0(1)e-1). \tag{4.1}$$

It is easily seen that

$$\sum_{i=0}^{e-1} \eta_i = \sum_{h \neq 0} \varepsilon(h) = -1. \tag{4.2}$$

The generator of the η's is the Lagrange resolvent

$$\tau(\alpha^\nu) = \sum_{i=0}^{e-1} \eta_i \alpha^{i\nu}, \tag{4.3}$$

where $\alpha = \exp(2\pi i/e)$, so that by (4.2)

$$\tau(1) = -1. \tag{4.4}$$

By inversion (2.3)

$$\eta_i = e^{-1} \sum_{\nu=0}^{e-1} \tau(\alpha^\nu) \alpha^{-i\nu}. \tag{4.5}$$

A well-known property of this resolvent is ([1], p. 87)

$$\tau(\alpha^\nu)\tau(\alpha^{-\nu}) = \begin{cases} (-1)^{\nu f} p & \text{if} \quad \nu \not\equiv 0 \pmod{e}, \\ 1 & \text{if} \quad \nu \equiv 0 \pmod{e}. \end{cases} \tag{4.6}$$

Similarly we define the corresponding Kloosterman periods and resolvent by

$$\theta_i^{(k)} = \sum_{h \epsilon C_i} S_k(h) \qquad (i = 0(1)e-1) \tag{4.7}$$

and

$$T_k(\alpha^\nu) = \sum_{i=0}^{e-1} \theta_i^{(k)} \alpha^{i\nu}. \tag{4.8}$$

In case $k = -1$ we write

$$\theta_i^{(-1)} = \theta_i \quad \text{and} \quad T_{-1}(\alpha^\nu) = T(\alpha^\nu).$$

By inversion we have

$$\theta_i^{(k)} = e^{-1} \sum_{\nu=0}^{e-1} T_k(\alpha^\nu) \alpha^{-i\nu}. \tag{4.9}$$

A connection between the $\theta_j^{(k)}$ and the η_i is given by

THEOREM 4.1.

$$\theta_j^{(k)} = \sum_{i=0}^{e-1} \eta_i \eta_{ki+j}. \tag{4.10}$$

Proof. By definitions (4.7) and (1.3)

$$\theta_j^{(k)} = \sum_{x=1}^{p-1} \varepsilon(x) \sum_{h \epsilon C_j} \varepsilon(x^k h) = \sum_{i=0}^{e-1} \sum_{x \epsilon C_i} \varepsilon(x) \sum_{h \epsilon C_j} \varepsilon(x^k h) = \sum_{i=0}^{e-1} \sum_{x \epsilon C_i} \varepsilon(x) \sum_{y \epsilon C_{ki+j}} \varepsilon(y),$$

since $\operatorname{ind} y = \operatorname{ind}_g(x^k h) \equiv ki+j \pmod{e}$.

The theorem now follows from (4.1).

For the Kloosterman sums we have simply

$$\theta_j = \sum_{i=0}^{e-1} \eta_i \eta_{j-i}. \tag{4.11}$$

In the degenerate case $k = 1$ we have by (4.7) and (1.4)

$$\theta_j^{(1)} = \sum_{h \epsilon C_j} (-1 + p\delta_h^{-1}).$$

Theorem 4.1 gives in this case

$$\sum_{i=0}^{e-1} \eta_i \eta_{i+j} = -f + p\Delta_j^{(p-1)/2}, \tag{4.12}$$

a well-known identity of cyclotomy ([3], p. 395). The two kinds of resolvents are related by

THEOREM 4.2.

$$T_k(\alpha^\nu) = \tau(\alpha^\nu)\tau(\alpha^{-k\nu}). \tag{4.13}$$

Proof. Applying (2.5) with $m = e$, $F_1(i) = F_2(i) = \eta_i$, $a = k$, $b = j$ so that $G_1(\alpha^\nu) = G_2(\alpha^\nu) = \tau(\alpha^\nu)$, we find

$$\sum_{i=0}^{e-1} \eta_i \eta_{ki+j} = e^{-1} \sum_{\nu=0}^{e-1} \tau(\alpha^\nu)\tau(\alpha^{-k\nu})\alpha^{-j\nu} = \theta_j^{(k)}$$

by (4.10). But $T_k(\alpha^\nu)$ is the generator of $\theta_j^{(k)}$. Hence the theorem.

For $k = -1$ we have the simple result

$$T(\alpha^\nu) = \tau^2(\alpha^\nu). \tag{4.14}$$

As another example by (4.6)

$$T_1(\alpha^\nu) = \begin{cases} (-1)^{\nu f} p & \text{if} \quad \nu \not\equiv 0 \pmod{e}, \\ 1 & \text{if} \quad \nu \equiv 0 \pmod{e}. \end{cases}$$

The analogue of (4.6) is

THEOREM 4.3.

$$T_k(\alpha^\nu)T_k(\alpha^{-\nu}) = \begin{cases} p^2 & \textit{if} \quad \nu \not\equiv 0 \pmod{e}, \\ 1 & \textit{if} \quad \nu \equiv 0 \pmod{e}. \end{cases} \tag{4.15}$$

Proof. This follows from (4.6) and (4.13) and the fact that k is odd.

The analogue of (4.12) is

THEOREM 4.4.

$$\sum_{i=0}^{e-1} \theta_i^{(k)} \theta_{i+j}^{(k)} = -f(p+1) + p^2 \Delta_j^0. \tag{4.16}$$

Proof. Applying (2.5) we get

$$\sum_{i=0}^{e-1} \theta_i^{(k)} \theta_{i+j}^{(k)} = e^{-1} \sum_{\nu=0}^{e-1} T_k(\alpha^\nu) T_k(\alpha^{-\nu}) \alpha^{j\nu}.$$

By Theorem 4.3 the right-hand side becomes

$$e^{-1}\Big[1 + p^2 \sum_{\nu=1}^{e-1} \alpha^{j\nu}\Big] = e^{-1}[1 - p^2 + ep^2 \Delta_j^0].$$

The theorem now follows from the fact that $p = ef + 1$.

Combining the θ's with the η's we have

THEOREM 4.5.

$$\sum_{i=0}^{e-1} \theta_i^{(k)} \eta_{i+b} = \begin{cases} f + p\eta_{k'b} & \textit{if } f \textit{ is even}, \\ f + p\eta_{k'b+e/2} & \textit{if } f \textit{ is odd}; \end{cases} \tag{4.17}$$

$$\sum_{i=0}^{e-1} \theta_i^{(k)} \eta_{b-k'i} = \begin{cases} f + p\eta_{bk} & \textit{if } f \textit{ is even}, \\ f + p\eta_{bk+e/2} & \textit{if } f \textit{ is odd}. \end{cases} \tag{4.18}$$

Proof. Choosing $F_1(i) = \theta_i^{(k)}$ and $F_2(i) = \eta_i$ we obtain from (2.5)

$$\begin{aligned} \sum_{i=0}^{e-1} \theta_i^{(k)} \eta_{ai+b} &= e^{-1}\Big[T_k(1)\tau(1) + \sum_{\mu=1}^{e-1} \tau(\alpha^{-\mu}) T_k(\alpha^{a\mu}) \alpha^{b\mu}\Big] \\ &= e^{-1}\Big[-1 + \sum_{\mu=1}^{e-1} \tau(\alpha^{-\mu})\tau(\alpha^{-ka\mu})\tau(\alpha^{a\mu})\alpha^{b\mu}\Big]. \end{aligned} \tag{4.19}$$

The two values $a = 1$ and $a = -k$ permit the use of (4.6). Furthermore $(-1)^f = \alpha^{(p-1)/2}$. Setting $a = 1$, (4.19) becomes

$$\begin{aligned} \sum_{i=0}^{e-1} \theta_i^{(k)} \eta_{i+b} &= e^{-1}\Big[-1 + p \sum_{\mu=1}^{e-1} \tau(\alpha^{-k\mu}) \alpha^{\mu(b+(p-1)/2)}\Big] \\ &= e^{-1}\Big[-1 + p \sum_{\nu=0}^{e-1} \tau(\alpha^\nu) \alpha^{-\nu k'(b+(p-1)/2)} + p\Big]. \end{aligned}$$

By (4.5) we have

$$\sum_{i=0}^{e-1} \theta_i^{(k)} \eta_{i+b} = f + p\eta_h$$

where

$$h = k'\big(b + (p-1)/2\big) \equiv \begin{cases} k'b & \text{if} \quad f \text{ is even}, \\ k'b + e/2 & \text{if} \quad f \text{ is odd}. \end{cases}$$

(4.18) follows in the same way by setting $a = -k'$.

5. Connection with Jacobi's function.

The function

$$\begin{aligned} R_n(\alpha^\nu) &= \begin{cases} \displaystyle\sum_{s=1}^{p-2} \alpha^{\nu\{\operatorname{ind} s - (n+1)\operatorname{ind}(1+s)\}} & \nu \not\equiv 0 \pmod{e} \\ -1 & \nu \equiv 0 \pmod{e} \end{cases} \\ &= \sum_{i=0}^{e-1} b(i, n)\alpha^{i\nu} \end{aligned} \tag{5.1}$$

where

$$\sum_{i=0}^{e-1} b(i, n) = -1$$

is due to Jacobi and its properties are treated in [1], [3], [4] and [7]. It is connected with τ by the fundamental identity

$$R_n(\alpha^\nu)\tau(\alpha^{(n+1)\nu}) = \tau(\alpha^\nu)\tau(\alpha^{n\nu}) \begin{bmatrix} n\nu \not\equiv 0 \pmod{e} \\ (n+1)\nu \not\equiv 0 \pmod{e} \end{bmatrix} \tag{5.2}$$

which also holds when $\nu = 0$. Another property we shall need is

$$R_1(a^\nu)R_1(a^{-\nu}) = \begin{cases} p & \text{if} \quad 2\nu \not\equiv 0 \pmod{e}, \\ 1 & \text{if} \quad 2\nu \equiv 0 \pmod{e}. \end{cases} \tag{5.3}$$

This follows from (4.6) and (5.2) with $n = 1$.

By inversion of (5.1)

$$b(i, n) = e^{-1} \sum_{\nu=0}^{e-1} R_n(a^\nu) a^{-i\nu}. \tag{5.4}$$

A well-known property of the periods η_i is that the product of any two of them is linear combination of the η's with integer coefficients. By Theorem 4.1 it follows that $\theta_j^{(k)}$ is also a linear combination of the η's with integer coefficients. More than mere existence can be proved about these coefficients. If e is a prime we have

THEOREM 5.1. *Let e be a prime and let $k \neq 1$. Then*

$$\theta_j^{(k)} = \sum_{i=0}^{e-1} b\big(j+i(k-1), -k\big)\eta_i,$$

where the b's are coefficients of the Jacobi function (5.1).

Proof. If in (5.2) we set $n = -k$ and use Theorem 4.2 we have

$$T_k(a^\nu) = \tau(a^{\nu(1-k)}) R_{-k}(a^\nu) \qquad (\nu = 0(1)e-1),$$

since e is a prime.

We now use (2.5) with (4.8), (5.1) and (4.3) to obtain the theorem.

6. Kloosterman sums and Jacobsthal sums.

In what follows we restrict ourselves to the case of $k = -1$, the classical Kloosterman sum $S(h)$. The Jacobsthal sums ψ and φ are defined as follows [5]

$$\psi_e(h) = \sum_{x=1}^{p-1} \chi(x^e + h), \tag{6.1}$$

$$\varphi_e(h) = \sum_{x=1}^{p-1} \chi(x)\chi(x^e + h). \tag{6.2}$$

These are related to the function $R_1(a^\nu)$ as follows [7]

$$R_1(a^\nu) = \begin{cases} (-1)^f e^{-1} \sum_{i=0}^{e-1} \psi_e(4g^i) a^{i\nu} & \text{if } e \text{ is even}, \\ e^{-1} \sum_{i=0}^{e-1} \varphi_e(4g^i) a^{i\nu} & \text{if } e \text{ is odd}. \end{cases} \tag{6.3}$$

Other properties of the Jacobsthal sums are [7]

$$\psi_e(0) = \frac{p-1}{2}\big(1+(-1)^e\big), \tag{6.4}$$

$$\psi_e(ny^{2e}) = \psi_e(n), \tag{6.5}$$

$$\psi_e(\bar{h}) = \begin{cases} \chi(h)\psi_e(h) & \text{if } e \text{ is even}, \\ \chi(h)\varphi_e(h) & \text{if } e \text{ is odd}. \end{cases} \tag{6.6}$$

For the expansion of θ_j as a linear combination of the η_i we have, for the general e, the following counterpart of Theorem 5.1.

THEOREM 6.1.

$$\theta_j = \begin{cases} e^{-1} \sum_{i=0}^{e-1} \psi_e(-4g^{j-2i})\eta_i + (-1)^{j+(p-1)/2} f & \textit{if } e \textit{ is even}, \\ e_{-1} \sum_{i=0}^{e-1} \varphi_e(-4g^{j-2i})\eta_i & \textit{if } e \textit{ is odd}. \end{cases} \tag{6.7}$$

Proof. By (1.6) we have

$$\theta_j = \sum_{h \in C_j} S(h) = \sum_{x=0}^{p-1} \varepsilon(x) \sum_{h \in C_j} \chi(x^2 - 4h). \tag{6.8}$$

Putting

$$h = g^{j+et}$$

and letting $t = 0(1)p-2$ we get the class C_j repeated e times over and the inner sum becomes

$$e^{-1}\chi(-1) \sum_{t=0}^{p-1} \chi(g^j)\chi(g^{te} - \bar{4}g^{-j}x^2) = (-1)^{j+(p-1)/2} e^{-1} \psi_e(-\bar{4}p^{-j}x^2).$$

Returning with this result to (6.8) and setting, for $x \neq 0$,

$$x = g^{i+es} \qquad (i = 0(1)e-1, \ s = 0(1)f-1)$$

we obtain from (6.5)

$$\begin{aligned} \theta_j &= (-1)^{j+(p-1)/2} e^{-1} \Big[\psi_e(0) + \sum_{i=0}^{e-1} \psi_e(-\bar{4}g^{2i-j}) \sum_{x \in C_i} \varepsilon(x)\Big] \\ &= (-1)^{j+(p-1)/2} e^{-1} \Big[\frac{p-1}{2}\big(1+(-1)^e\big) + \sum_{i=0}^{e-1} \eta_i \psi_e(-\bar{4}g^{2i-j})\Big]. \end{aligned}$$

To get (6.7) it is convenient to separate the two cases, e even and e odd, and use (6.6) to reciprocate the argument of $\psi_e(-\bar{4}g^{2i-j})$.

We consider next the two sums

$$\Omega_j = \sum_{i\epsilon C_j} S^2(i), \tag{6.9}$$

$$\Omega'_j = \sum_{i\epsilon C_j} S(i)S(-i) \tag{6.10}$$

for which we have by (3.7) and (3.9)

$$\sum_{j=0}^{c-1}\Omega_j = p^2-p-1, \qquad \sum_{j=0}^{e-1}\Omega'_j = -p-1. \tag{6.11}$$

THEOREM 6.2.

$$\Omega_j = \begin{cases} e^{-1}\sum_{i=0}^{e-1}\varphi_e(-4g^{-i})\,\theta_{i+j}+pf & \text{if } e \text{ is odd,} \\ e^{-1}\sum_{i=0}^{e-1}\psi_e(-4g^{-i})\,\theta_{i+j}+pf & \text{if } e \text{ is even,} \end{cases} \tag{6.12}$$

$$\Omega'_j = e^{-1}\sum_{i=0}^{e-1}\psi_{2e}(4g^{-2i})\,\theta_{i+j}-f.$$

Proof. For the proofs it is convenient to use the following lemma which is to be contrasted with (3.15).

LEMMA. *For* $a \neq 0$

$$S(i)S(ai) = p\delta_a^1+\sum_{m=0}^{p-1}\chi\big((1+a-m)^2-4a\big)S(mi). \tag{6.13}$$

Proof. By definition (1.1),

$$S(i)S(ai) = \sum_{x,y=1}^{p-1}\varepsilon[x+y+i(\bar{x}+a\bar{y})].$$

Letting $y = sx$ and then $t = x(1+s)$ for $s \not\equiv p-1$ we have

$$\begin{aligned} S(i)S(ai) &= \sum_{x,s=1}^{p-1}\varepsilon[x(1+s)+i\bar{x}(1+a\bar{s})] \\ &= \sum_{x=1}^{p-1}\varepsilon\big((1-a)i\bar{x}\big)+\sum_{s=1}^{p-2}\sum_{t=1}^{p-1}\varepsilon\big(t+\bar{t}(1+s)(1+a\bar{s})i\big) \\ &= -1+p\delta_a^1+\sum_{s=1}^{p-2}S[(1+s)(1+a\bar{s})i] \\ &= p\delta_a^1+\sum_{s=1}^{p-1}S[(1+s)(1+a\bar{s})i]. \end{aligned}$$

Now if we ask for each $m = 0(1)p-1$ how many solutions s are there of the congruence

$$(1+s)(1+a\bar{s}) \equiv m \pmod{p};$$

we find that the number is

$$1+\chi[(1+a-m)^2-4a].$$

Therefore

$$S(i)S(ai) = p\delta_a^1+\sum_{m=0}^{p-1}S(mi)+\sum_{m=0}^{p-1}\chi\big((1+a-m)^2-4a\big)S(mi).$$

The lemma is therefore a consequence of (1.9).

To prove the Theorem we use the lemma to write, (taking $m = 0$ separately)

$$\begin{aligned} \sum_{i\epsilon C_j} S(i)S(ai) &= pf\delta_1^a+\sum_{m=1}^{p-1}\chi[(1+a-m)^2-4a]\,\theta_{j+\operatorname{ind} m}-f\chi^2(1-a) \\ &= f[(p+1)\delta_a^1-1]+\sum_{i=0}^{e-1}\theta_{j+i}\sum_{m\epsilon C_i}\chi[(1+a-m)^2-4a]. \end{aligned} \tag{6.14}$$

The inner sum can be evaluated in terms of Jacobsthal sums in the two cases $a = \pm 1$. In the first case we have with $m = g^{i+et}$ and $t = 0(1)p-2$

$$\begin{aligned} \sum_{m\epsilon C_i}\chi(m)\chi(m-4) &= e^{-1}\sum_{t=0}^{p-2}\chi(g^{i+et})\chi(g^{i+et}-4) \\ &= e^{-1}\sum_{t=0}^{p-2}\chi(g^{et})\chi(g^{et}-4g^{-i}) \\ &= e^{-1}\sum_{y=1}^{p-1}\chi(y^e)\chi(y^e-4g^{-i}) \\ &= \begin{cases} e^{-1}\psi_e(-4g^{-i}) & \text{if } e \text{ is even,} \\ e^{-1}\varphi_e(-4g^{-i}) & \text{if } e \text{ is odd.} \end{cases} \end{aligned}$$

The formula (6.11) now follows at once from (6.14). In case $a = -1$ the inner sum of (6.14) now becomes

$$\begin{aligned} \sum_{m\epsilon C_i}\chi(m^2+4) &= e^{-1}\sum_{t=0}^{p-2}\chi(g^{2i})\chi(g^{2et}+4g^{-2i}) \\ &= e^{-1}\sum_{y=1}^{p-1}\chi(y^{2e}+4g^{-2i}) = e^{-1}\psi_{2e}(4g^{-2i}). \end{aligned}$$

Formula (6.12) now follows at once from (6.14).

Next we find the generator of the Ω_j.

THEOREM 6.3. *The generator of Ω_j is*

$$\sum_{j=0}^{e-1}\Omega_j\alpha^{\nu j}=\begin{cases}(-1)^{f(1+\nu)}R_1(\alpha^\nu)T(\alpha^\nu) & \nu\not\equiv 0(\operatorname{mod} e),\\ p^2-p-1 & \nu\equiv 0(\operatorname{mod} e).\end{cases}\tag{6.15}$$

Proof. In case $\nu\equiv 0$ the result follows at once from (6.9) and (3.7). Suppose now that $\nu\not\equiv 0$. Then (6.12) can be written

$$\Omega_j=e^{-1}\sum_{i=0}^{e-1}H(-4g^i)\,\theta_{j-i}+pf$$

where H is φ_e or ψ_e according as e is odd or even. Since $-1\equiv g^{ef/2}(\operatorname{mod} p)$, we have

$$\sum_{j=0}^{e-1}\Omega_j\alpha^{\nu j}=e^{-1}\sum_{i,j=0}^{e-1}H(4g^{i+ef/2})\,\theta_{j-i}\,\alpha^{\nu(j-i)}\,\alpha^{\nu(i+ef/2)}\,\alpha^{-ef\nu/2}+pf\sum_{j=0}^{e-1}\alpha^{\nu j}.$$

Summing first over $j-i$ and then over $i+ef/2$ we have by (4.8) and (6.3)

$$\sum_{j=0}^{e-1}\Omega_j\alpha^{\nu j}=(-1)^fR_1(\alpha^\nu)T(\alpha^\nu)\alpha^{-ef\nu/2}=(-1)^{f(1+\nu)}R_1(\alpha^\nu)T(\alpha^\nu).$$

We are now in a position to prove

THEOREM 6.4.

$$\sum_{i=0}^{e-1}\Omega_i\Omega_{i+j}=(f+\Delta_j^0)p^3-f(p+1)(2p+1)-\begin{cases}(-1)^jfp^2 & \textit{if } e \textit{ is even},\\ 0 & \textit{if } e \textit{ is odd}.\end{cases}\tag{6.16}$$

Proof. We use the Parseval identity (2.5) with $a=1$, $b=j$, $m=e$, and we use Theorem 6.3. This gives us

$$e\sum_{i=0}^{e-1}\Omega_i\Omega_{i+j}=(p^2-p-1)^2+\sum_{\mu=1}^{e-1}R_1(\alpha^{-\mu})R_1(\alpha^\mu)T(\alpha^\mu)T(\alpha^{-\mu})\alpha^{j\mu}.\tag{6.17}$$

Using (4.15) and (5.3) the sum on the right becomes

$$p^2\sum_{\mu=1}^{e-1}\big(p-(p-1)\Delta_{2\mu}^e\big)\alpha^{j\mu}=p^3(-1+e\Delta_j^0)-\begin{cases}(-1)^jefp^2 & \text{if } e \text{ is even},\\ 0 & \text{if } e \text{ is odd}.\end{cases}$$

Substituting this into (6.17) and simplifying gives (6.16).

7. Period equations.

The equation satisfied by the e quantities η_i is known as the period equation. It is an irreducible monic abelian equation with integer coefficients. Similarly the quantities $\theta_i^{(k)}$ and Ω_i satisfy equations of degree e with properties similar to those of the classical period equation.

If we let

$$\begin{aligned}x_i&=e\eta_i+1,\\ y_i^{(k)}&=e\theta_i^{(k)}-1,\\ z_i&=e\Omega_i-p^2+p+1,\end{aligned}$$

then

$$\sum_{i=0}^{e-1}x_i=\sum_{i=0}^{e-1}y_i^{(k)}=\sum_{i=0}^{e-1}z_i=0,\tag{7.1}$$

so that the equations satisfied by x's, y's and z's are reduced. By (4.12), (4.16), and (6.16),

$$\sum x_i^2=e^2\sum\eta_i^2-e=\begin{cases}pe(e-1) & \text{if } f \text{ is even},\\ -pe & \text{if } f \text{ is odd},\end{cases}\tag{7.2}$$

$$\sum\{y_i^{(k)}\}^2=e^2\sum\{\theta_i^{(k)}\}^2-e=p^2e(e-1),\tag{7.3}$$

$$\sum z_i^2=e^2\sum\Omega_i^2-e(p^2+p-1)=\begin{cases}p^3e(e-1) & e \text{ odd},\\ p^3e(e-2)+p^2e & e \text{ even}.\end{cases}\tag{7.4}$$

If e is odd the three equations satisfied by the x's, $y^{(k)}$'s and z's are strikingly similar to begin with. In fact they begin, by (7.2), (7.3), (7.4)

$$\left.\begin{aligned}&x^e-\binom{e}{2}px^{e-2}+\ldots=0, &&(7.5)\\ &y^e-\binom{e}{2}p^2y^{e-2}+\ldots=0, &&(7.6)\\ &z^e-\binom{e}{2}p^3z^{e-2}+\ldots=0. &&(7.7)\end{aligned}\right\}\quad(e \text{ is odd})$$

When e is even the equations in y and z split into two equations of degree $e/2$ with integer coefficients.

For special values of e, more coefficients of the period equations of $y_i^{(-1)}=y_j$ are known in the following cases.

Case I: $e=p-1$. From the previous discussion we known the sums of nth powers of the $S(i)$ for $n=0(1)4$. Hence the equation (corresponding to $x^p-1=0$) satisfied by all the Kloosterman sums $S(i)$, including $S(0)=-1$ begins

$$y^p-\binom{p}{2}y^{p-2}-\frac{p}{3}(p\chi(-3)+2)y^{p-3}+\tfrac{1}{8}p(p-3)(p^2-3p-2)y^{p-4}+\ldots=0$$

If we remove the factor $y-S(0)=y+1$, the quotient is not irreducible in the rational field but is the product of two polynomials of degree $(p-1)/2$ with integral coefficients. Namely

$$Q_0(y)=\prod_{\chi(i)=1}\big(y-S(i)\big)$$

and

$$Q_1(y) = \prod_{\chi(i)=-1} \big(y-S(i)\big).$$

The first four coefficients of each of these factors are easily derived from (3.11), (3.12) and (1.7). We have

$$\begin{aligned} Q_0(y) = y^{(p-1)/2} &- \tfrac{1}{2}\big(p\chi(-1)+1\big)y^{(p-3)/2} - \tfrac{1}{8}\{p^2-2p\big(2+\chi(-1)\big)-3\}\, y^{(p-5)/2} + \\ &+ \tfrac{1}{48}[5p^3\chi(-1)+p^2\{8\chi(3)-8\chi(-3)-20\chi(-1)+3\} - \\ &\qquad -p\{16A^2\{\chi(-1)+\chi(3)\}+9\chi(-1)+28\}]\, y^{(p-7)/2}+\ldots, \end{aligned}$$

$$\begin{aligned} Q_1(y) = y^{(p-1)/2} &+ \tfrac{1}{2}\{p\chi(-1)-1\}y^{(p-3)/2} - \tfrac{1}{8}\{p^2+2p\chi(-1)-3\}\, y^{(p-5)/2} + \\ &+ \tfrac{1}{48}[-5p^3\chi(-1)-p^2\{8\chi(3)+8\chi(-3)+\chi(-1)-3\} + \\ &\qquad +p\{16A^2\{\chi(-1)+\chi(3)\}+9\chi(-1)-16\}]\, y^{(p-7)/2}+\ldots \end{aligned}$$

where $p = A^2+3B^2$, if possible.

Case II. $e = (p-1)/2$. In this case we have

$$\theta_i = S(g^i)+S(-g^i), \qquad i = 0(1)(p-3)/2.$$

The equation satisfied by these θ's corresponds to Sylvester's cyclotomic polynomial of the second kind [12]. Formulas (3.21) (with $a = -1$) and (3.22) enable us to find one more term in the equation (7.6) as follows

$$\begin{aligned} y^{(p-1)/2} - \frac{p^2(p-1)(p-3)}{8}\, y^{(p-5)/2} - \\ - \frac{p^2(p-1)}{24}\{[\chi(-3)+3\chi(5)](p-1)^2+2p+6\}\, y^{(p-7)/2}+\ldots \end{aligned}$$

Case III. $e = 2$. In this case we may use (7.1), (7.3) and (7.4) to obtain the quadratic period equations

$$y^2-p^2 = 0,$$
$$z^2-p^2 = 0.$$

These results are obvious consequences of the more explicit statements

(7.8) $$y_0 = \chi(-1)p, \quad y_1 = -\chi(-1)p,$$

(7.9) $$z_0 = -p, \quad z_1 = p$$

that follow from (3.11), (3.12) and the definitions of y_i and z_i. The corresponding cyclotomic period equation is, of course,

$$x^2-\chi(-1)p = 0$$

and (7.8) and (7.9) correspond to the determination of the sign of the Gauss sum

$$\sum_{i=0}^{p-1} \varepsilon(ci^2) = \sqrt{p\chi(-1)}\,\chi(c).$$

Case IV. $e = 3$. The three period equations (7.5), (7.6) and (7.7) in this case involve the integer defined unambiguously by the quadratic partition of $4p$,

$$4p = L^2+27M^2 \qquad (L \equiv 1 \pmod 3).$$

They are

(7.10) $$x^3-3px-pL = 0,$$

(7.11) $$y^3-3p^2y-p^2(L^2-2p) = 0,$$

(7.12) $$z^3-3p^3z-p^2(L^5-5pL^3+5p^2L) = 0.$$

In the constant terms of these three equations one recognizes the Chebyshev polynomials

$$C_n(t) = 2\cos(n\arccos t/2)$$

for $n = 1, 2,$ and 5. Hence if we define

$$\gamma = \arccos(\tfrac{1}{2}L/\sqrt{p})$$

the roots of these three equations are

$$x_1 = 2\sqrt{p}\cos\frac{\gamma}{3}, \qquad x_2 = 2\sqrt{p}\cos\frac{\gamma+2\pi}{3}, \qquad x_3 = 2\sqrt{p}\cos\frac{\gamma+4\pi}{3},$$

$$y_1 = 2p\cos\frac{2\gamma}{3}, \qquad y_2 = 2p\cos\frac{2\gamma+2\pi}{3}, \qquad y_3 = 2p\cos\frac{2\gamma+4\pi}{3},$$

$$z_1 = 2p^{3/2}\cos\frac{5\gamma}{3}, \qquad z_2 = 2p^{3/2}\cos\frac{5\gamma+2\pi}{3}, \qquad z_3 = 2p^{3/2}\cos\frac{5\gamma+4\pi}{3}.$$

The discriminants of (7.10), (7.11), and (7.12) are

$$(27pM)^2, \qquad (27p^2LM)^2, \qquad [27p^2M(p^2-3pL^2+L^4)]^2,$$

respectively.

Case V. $e = 4$. The three period equations, in this case involve the integers a, b in the quadratic partition of p

$$p = a^2+b^2 \qquad (a \equiv 1 \pmod 4).$$

In the classical case ([1], p. 230) it is customary to write the quartic polynomial, in Lebesgue's form, as a product of two quadratics with coefficients in the field $k(\sqrt{p})$, namely

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

In the case of y_i and z_i the two quadratics have rational integral coefficients and are in fact

$$[y^2-2py+p^2-4pa^2][y^2+2py+p^2-4pb^2] = 0$$

and

$$[z^2+2pz-4p^3+p^2+16pa^2b^2][z^2-2pz+p^2-16pa^2b^2] = 0.$$

Actually solving for the y's and z's we find

$$y_0, y_2 = p\pm 2a\sqrt{p}, \qquad y_1, y_3 = -p\pm 2b\sqrt{p},$$
$$z_0, z_2 = -p\pm 2(a^2-b^2)\sqrt{p}, \quad z_1, z_3 = p\pm 4ab\sqrt{p}.$$

The discriminants of the x's, y's and z's are

$$2^{14}p^3b^6 \text{ if } p = 8n+1 \quad \text{or} \quad 2^{14}p^3b^2(3p+a^2)^2 \text{ if } p = 8n+5,$$
$$\{2^{10}p^3a^3b^3\}^2,$$

and

$$\{2^9p^3ab(a^2-b^2)[p^2(p-1)^2-16a^2b^2(a^2-b^2)^2]\}^2,$$

respectively.

Case VI. $e = 5$. Here we encounter for the first time the sums $S_k(h$ which are different from $S(h)$ and nondegenerate, namely $S_3(h)$. These sums, and their squares, lead to reduced "period equations" of degree 5 differing from the equations corresponding to $S(h)$ and their squares

Both pairs of equations, like the classical equation for the five η_i, have coefficients which depend on a certain quaternary quadratic partition of $16p$ [8]. Instead of finding these coefficients for a general prime $p = 5n+1$, we give as an example the five equations for $p = 11$. We also define a parallel of (6.9),

$$\Omega_j^{(3)} = \sum_{i\epsilon C_j}\{S_3(i)\}^2, \qquad z_i^{(3)} = 5\Omega_i^{(3)}-109.$$

The five equations have discriminants D and coefficients as given in the following table.

Roots	$D\cdot 5^{-20}$	Coefficients					
x_i	11^4	1	0	-110	-55	$+2310$	$+979$
y_i	$11^8\cdot 67^2$	1	0	-1210	-11495	$+37510$	-24079
$y_i^{(3)}$	11^{12}	1	0	-1210	$+18755$	-53240	-145079
z_i	$11^8\cdot 23^2\cdot 1123^2\cdot 9439^2$	1	0	-13310	$+17545$	$+26379210$	$+174094679$
$z_i^{(3)}$	$11^{12}\cdot 23^2\cdot 43^2\cdot 263^2$	1	0	-19360	-508805	$+68892560$	$+2078701229$

In conclusion we wish to point out that the classical results concerning the period equation considered as a congruence modulo an arbitrary prime also have their counterparts for the above period equations. These will be the subject of another paper.

References

[1] Paul Bachman, *Die Lehre von der Kreistheilung*, Leipzig 1872.

[2] H. Davenport, *On certain exponential sums*, J. Reine Angew. Math. 169 (1933), pp. 158-176.

[3] L. E. Dickson, *Cyclotomy, Higher Congruences and Waring's Problem*, Amer. J. Math. 57 (1935), pp. 391-424.

[4] — *Cyclotomy and Trinomial Congruences*, Trans. Amer. Math. Soc. 37 (1935), pp. 363-380.

[5] E. Jacobsthal, *Anwendungen einer Formal aus der Theorie der Quadratischen Reste*, Dissertation, Berlin 1906.

[6] D. H. and Emma Lehmer, *On the cubes of Kloosterman sums*, Acta Arith. 6 (1960), pp. 15-22.

[7] Emma Lehmer, *On Jacobi Functions*, Pacific J. Math. 10 (1960), pp. 887-893.

[8] — *The quintic character of* 2 *and* 3, Duke Math. J. 18 (1951), pp. 11-18.

[9] L. J. Mordell, *On Lehmer's congruence associated with cubes of Kloosterman's sums*, J. London Math. Soc. 36 (1961), pp. 335-339.

[10] H. Salié, *Über die Kloostermanschen Summen* $S(u, v; q)$, Math. Zeit. 34 (1932), pp. 91-109.

[11] I. J. Schoenberg, *The finite Fourier series and elementary geometry*, Amer. Math. Monthly 57 (1950), pp. 390-404.

[12] J. J. Sylvester, *On certain ternary cubic-form equations*, Amer. J. Math. 2, pp. 366-368; *Collected Papers*, v. 3, p. 325.

[13] A. L. Whiteman, *Finite Fourier series and cyclotomy*, Nat. Acad. Sci. Proc. 37 (1951), pp. 373-378.

[14] — *Cyclotomy and Jacobsthal sums*, Amer. J. Math. 74 (1952), pp. 88-89.

UNIVERSITY OF CALIFORNIA
Berkeley, California

Reçu par la Rédaction le 26. 8. 1966