ACTA ARITHMETICA
VI (1960)

On the cubes of Kloosterman sums

by

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

Let p be a prime >3 and let $\chi(s)$ be the quadratic character of s modulo p. The p Kloosterman sums

$$S(\lambda, p) = S(\lambda) = \sum_{h=1}^{p-1} \varepsilon^{h+\lambda\bar{h}} \qquad (\lambda = 0(1)\, p-1),$$

where $\varepsilon = \exp\{2\pi i/p\}$ and

$$h\bar{h} \equiv 1 (\mathrm{mod}\, p),$$

are of two main types according as $\chi(\lambda) = +1$ or -1. Following Salié [1], we write

$$f(\varepsilon) = S(1), \qquad g(\varepsilon) = S(N_0)$$

where $\chi(N_0) = -1$. The functions

$$f(\varepsilon^\nu) = f(\varepsilon^{-\nu}) \quad \text{and} \quad g(\varepsilon^\nu) = g(\varepsilon^{-\nu}) \qquad (\nu = 0(1)p-1)$$

constitute the Kloosterman Sums twice over. This includes the degenerate cases

$$f(\varepsilon^0) = g(\varepsilon^0) = S(0) = -1.$$

Therefore if we write

$$\sum_{\nu=0}^{p-1} \{f(\varepsilon^\nu)\}^n = \sigma_n, \qquad \sum_{\nu=0}^{p-1} \{g(\varepsilon^\nu)\}^n = \sigma_n'$$

we have

$$\sigma_n + \sigma_n' = 2 \sum_{\lambda=0}^{p-1} \{S(\lambda)\}^n.$$

Salié gave the following results

$$\sigma_1 = -\sigma_1' = \chi(-1)p, \qquad \sigma_2 = p^2 - 2p, \qquad \sigma_2' = p^2,$$
$$\sigma_3 + \sigma_3' = 2(\chi(-3)p^2 + 2p). \tag{1}$$

In this paper we prove

THEOREM 1.

$$\sigma_3 = \begin{cases} p^2\{2\chi(-1)-1\}+2p & \text{if} \quad p = 6n-1, \\ p^2+2p\{1+2\chi(-1)A^2\} & \text{if} \quad p = 6n+1 = A^2+3B^2, \end{cases} \tag{2}$$

$$\sigma_3' = \begin{cases} -p^2\{1+2\chi(-1)\}+2p & \text{if} \quad p = 6n-1, \\ p^2+2p\{1-2\chi(-1)A^2\} & \text{if} \quad p = 6n+1 = A^2+3B^2. \end{cases} \tag{3}$$

These results were discovered empirically by an inspection of numerical results in 1952. After repeatedly unsuccessful attempts over the intervening years, a proof of these formulas was completed in 1959. It was seen at the outset that Theorem 1 would follow from

LEMMA 1.

$$\sum_{x=1}^{p-1}\sum_{y=1}^{p-1}\chi(x+\bar{y}+1)\chi(\bar{x}+y+1) = \begin{cases} 2p & \text{if} \quad p = 6n-1, \\ 4A^2 & \text{if} \quad p = 6n+1 = A^2+3B^2 \end{cases}$$

and it was Lemma 1 which proved to be the real difficulty.

In what follows we use the Kronecker symbol modulo p

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

It will be convenient to refer to three other lemmas.

LEMMA 2.

$$\sum_{\nu=0}^{p-1}\varepsilon^{k\nu^2} = \chi(k)\sqrt{p}\,i^{[(p-1)/2]^2}+p\delta_0^k,$$

$$\sum_{\nu=0}^{p-1}\chi(\nu)\varepsilon^{k\nu} = \chi(k)\sqrt{p}\,i^{[(p-1)/2]^2}.$$

LEMMA 3.

$$\sum_{\nu=0}^{p-1}\chi(\nu+n)\chi(\nu+m) = -1+p\delta_m^n.$$

Lemma 2 is the well-known Gauss sum in two guises (see for example [2]). Lemma 3 is a familiar result of E. Jacobsthal [3].

The proof of Lemma 1 leads us to consider a double sum

$$\psi_e(a) = \sum_{t=1}^{p-1}\sum_{u=1}^{p-1}\chi(t^e+au)\chi(t^e+au^2) \tag{4}$$

which has properties similar to a single sum of Jacobsthal. Two properties are given by

LEMMA 4. *Let* $p = 1+ef$, $e = 2\mu-1$. *Then*

$$\sum_{a=1}^{p-1}\psi_e(a) = p-1, \tag{5}$$

$$\sum_{a=1}^{p-1}\{\psi_e(a)\}^2 = (p-1)[(e-1)p^2+1]. \tag{6}$$

We begin with a proof of Lemma 4. The first part is easy. In (4) we eliminate the letter u in favor of z defined by

$$u \equiv \bar{a}t^{\mu-1}z \pmod p$$

so that we have

$$\psi_e(a) = \sum_{t=1}^{p-1}\sum_{z=1}^{p-1}\chi(t^{\mu-1})\chi(t^\mu+z)\chi(t+\bar{a}z^2). \tag{7}$$

Noting that

$$\sum_{a=1}^{p-1}\chi(t+\bar{a}z^2) = -\chi(t)$$

we obtain

$$\sum_{a=1}^{p-1}\psi_e(a) = -\sum_{t=1}^{p-1}\sum_{z=1}^{p-1}\chi(t^{\mu-1})\chi(t^\mu+z)\chi(t) = \sum_{t=1}^{p-1}\chi(t^{2\mu}) = p-1.$$

To prove (6) we again use (7) and write

$$\sum_{a=1}^{p-1}\{\psi_e(a)\}^2 = \sum_{x,u,z,v=1}^{p-1}\chi(xu)^{\mu-1}\chi(x^\mu+z)\chi(u^\mu+v)\sum_{a=1}^{p-1}(a+xz^{-2})\chi(a+uv^{-2}).$$

By Lemma 3 the inner sum is

$$-1+p\delta_{(z/v)^2}^{x/u}-\chi(xu).$$

Eliminating x and z in favor of s and t defined by

$$x \equiv us, \qquad z \equiv vt \pmod p$$

we find

$$\sum_{a=1}^{p-1}\{\psi_e(a)\}^2 = \sum_{s,t=1}^{p-1}[-\chi(ts^{\mu-1})-\chi(ts^\mu)+p\chi(ts^{\mu-1})\delta_{t^2}^{s^2}]\times$$
$$\times\sum_{u,v=1}^{p-1}\chi(v+u^\mu)\chi(v+\bar{t}(us)^\mu).$$

Again, by Lemma 3 the inner sum is

$$\{-1+p\delta_t^{s^\mu}-\chi(ts^\mu)\}(p-1).$$

Substituting this into our sum we find

$$\begin{aligned}(p-1)^{-1}\sum_{a=1}^{p-1}\{\psi_e(a)\}^2 = \sum_{s,t=1}^{p-1}\{[\chi(ts^{\mu-1})+\chi(ts^\mu)][1+\chi(ts^\mu)]\\ -p[\chi(s)+\chi(ts^{\mu-1})]\,\delta_{t^2}^s\\ -p[\chi(ts^{\mu-1})+\chi(ts^\mu)]\delta_t^{s^\mu}\}+p^2\sum_{s,t=1}^{p-1}\delta_t^{s^\mu}\delta_{t^2}^s.\end{aligned}$$

This last sum is seen to be

$$\sum_{s^{2\mu-1}\equiv 1} 1 = 2\mu-1 = e.$$

Hence

$$\begin{aligned}(p-1)^{-1}\sum_{a=1}^{p-1}\{\psi_e(a)\}^2 &= \sum_{s,t=1}^{p-1}[\chi(ts^{\mu-1})+\chi(s)+\chi(ts^\mu)+1]\\ &\quad -p\sum_{t=1}^{p-1}[\chi(t)+\chi(t^2)]\\ &\quad -p\sum_{s=1}^{p-1}[\chi(s)+\chi(s^2)]+ep^2\\ &= (p-1)^2-2p(p-1)+ep^2 = (e-1)p^2+1.\end{aligned}$$

This completes the proof of Lemma 4.

Is is clear that the values $\psi_e(a)$ $(a = 1\ (1)\ p-1)$ are not all distinct. In fact we see from (4) that

$$\psi_e(aw^e) = \psi_e(a), \qquad w \not\equiv 0 \pmod p.$$

Thus the $p-1$ ψ's fall into e sets of f equal values. If g is a primitive root of p, the distinct ψ's may be represented by

$$\psi_e(1), \psi_e(g), \psi_e(g^2), \ldots, \psi_e(g^{e-1})$$

and Lemma 4 can be restated in the form

$$\sum_{\nu=0}^{e-1}\psi_e(g^\nu) = e, \tag{8}$$

$$\sum_{\nu=0}^{e-1}\{\psi_e(g^\nu)\}^2 = e[(e-1)p^2+1]. \tag{9}$$

In the sum over t in (4), t^e takes on each of its values e times. Hence every ψ is a multiple of e.

It can be seen, furthermore, that

$$\psi_e(1) \text{ is odd},$$

$$\psi_e(g^h) \text{ is even} \qquad (1 \leqslant h < e).$$

In fact, in considering the terms of (4) that vanish, we see that both factors of a term of $\psi_e(a)$ can vanish simultaneously only when $u = 1$ and when

$$t^e \equiv (-1)^e a \pmod p,$$

that is, only when a is congruent to an e-th power $(\mathrm{mod}\, p)$. Thus $\psi_e(1)$ is of different parity from the other representative ψ's. Since e is odd, the only possibility in view of (8) is that $\psi_e(1)$ is odd.

We now prove Lemma 1. Let Ω denote the sum in question and let Λ be the set of lattice points (x, y) for which

$$0 < x < p-1, \qquad 0 < y < p-1, \qquad y \neq p-x-1.$$

Thus Λ consists of $(p-2)(p-3)$ points. Let

$$\Omega' = \sum_{(x,y)\subset\Lambda}\chi(x+\bar{y}+1)\chi(\bar{x}+y+1);$$

then

$$\begin{aligned}\Omega' &= \Omega-\sum_{x=1}^{p-1}\chi(x)\chi(\bar{x})-\sum_{y=1}^{p-1}\chi(y)\chi(\bar{y})\\ &\quad +\chi^2(-1)-\sum_{x=1}^{p-2}\chi\big(x+1-\overline{(x+1)}\big)\chi(\bar{x}-x)\\ &= \Omega-2(p-1)+1-\chi(-1)\sum_{x=1}^{p-2}\chi(x+2)\chi(x-1).\end{aligned}$$

By Lemma 3 we have

$$\Omega' = \Omega-2p+3+\chi(-1)+2\chi(2). \tag{10}$$

Under the transformation

$$x \equiv \frac{t(t+u)}{u-t^2}, \qquad y \equiv \frac{t(t+1)}{u-t^2} \pmod p$$

with its unique inverse

$$t \equiv \frac{x}{1+y}, \qquad u \equiv \frac{x(x+1)}{y(y+1)} \pmod p$$

the set Λ is mapped into a set Λ' given by

$$0 < t < p-1, \quad 0 < u < p, \quad u \not\equiv t^2 (\mathrm{mod}\, p), \quad u \neq p-t$$

moreover

$$\chi(x+\bar{y}+1)\chi(\bar{x}+y+1) = \chi\left(\frac{(t^3+u)(t+u)}{t(u-t^2)(t+1)}\right)\chi\left(\frac{(t^3+u^2)(t+1)}{t(t+u)(u-t^2)}\right)$$

$$= \chi(t^3+u)\chi(t^3+u^2).$$

Hence

$$\begin{aligned}\Omega' &= \sum_{(t,u)\subset\Lambda'} \chi(t^3+u)\chi(t^3+u^2) \\ &= \sum_{t=1}^{p-1}\sum_{u=1}^{p-1} \chi(t^3+u)\chi(t^3+u^2) - \sum_{u=1}^{p-1}\chi(u-1)\chi(u^2-1) \\ &\quad - \sum_{t=1}^{p-2}\chi(t^3-t)\chi(t^3+t^2) - \sum_{t=1}^{p-2}\chi(t^3+t^2)\chi(t^3+t^4) \\ &= \psi_3(1)+2+2\chi(2)+\chi(-1)\end{aligned}$$

in which we have used Lemma 3. Therefore in view of (10)

$$\Omega = 2p-1+\psi_3(1). \tag{11}$$

Suppose first that $p = 6n-1$. Then as t ranges over a complete residue system so also does t^3 and so, by Lemma 3,

$$\begin{aligned}\psi_3(1) &= \sum_{u=1}^{p-1}\sum_{t=1}^{p-1}\chi(t^3+u)\chi(t^3+u^2) = \sum_{u=1}^{p-1}\sum_{t=1}^{p-1}\chi(t+u)\chi(t+u^2) \\ &= \sum_{u=1}^{p-1}\{-1+p\delta_u^{u^2}-\chi(u^3)\} = -p+1+p = 1.\end{aligned}$$

Hence in this case $\Omega = 2p$, in accordance with Lemma 1. It remains to consider the case $p = 6n+1 = A^2+3B^2$ and to determine $\psi_3(1)$. For brevity we write

$$\psi_3(1) = a, \quad \psi_3(g) = b, \quad \psi_3(g^2) = c.$$

By (8) and (9)

$$a+b+c = 3, \quad a^2+b^2+c^2 = 3(2p^2+1).$$

Hence

$$\begin{aligned}2bc &= (a+b+c)^2-(a^2+b^2+c^2)-2a(b+c) \\ &= 9-6p^2-3-2a(3-a) = 6(1-p^2)+2a^2-6a\end{aligned}$$

and

$$b^2+c^2 = 6p^2+3-a^2.$$

Subtracting we find

$$(b-c)^2 = 12p^2-3(a-1)^2$$

or

$$p^2 = [(a-1)/2]^2+3[(b-c)/6]^2$$

where the numbers in the square brackets are integers by the general remarks made following the proof of Lemma 4. But

$$p^2 = (2A^2-p)^2+3(2AB)^2$$

is the essentially unique representation of p^2 by the form x^2+3y^2. Hence

$$a-1 = \pm 2(2A^2-p).$$

The upper sign must be taken since a is a multiple of 3. Therefore

$$a = \psi_3(1) = 1+4A^2-2p.$$

Substituting this into (11) gives $\Omega = 4A^2$. This completes the proof of Lemma 1.

It remains to prove Theorem 1. Using Lemma 2, we can write

$$\begin{aligned}\sigma_3 &= \sum_{\nu=0}^{p-1}\{f(\varepsilon^\nu)\}^3 = \sum_{x,y,z=1}^{p-1}\varepsilon^{x+y+z}\sum_{\nu=0}^{p-1}\varepsilon^{(\bar{x}+\bar{y}+\bar{z})\nu^2} \\ &= \sqrt{p}\,i^{[(p-1)/2]^2}\sum_{x,y,z=1}^{p-1}\chi(\bar{x}+\bar{y}+\bar{z})\varepsilon^{x+y+z} \\ &\quad + p\sum_{x,y,z=1}^{p-1}\delta_0^{\bar{x}+\bar{y}+\bar{z}}\varepsilon^{x+y+z} \\ &= \sqrt{p}\,i^{[(p-1)/2]^2}\sum_{u,v,z=1}^{p-1}\chi(\bar{u}+\bar{v}+1)\chi(\bar{z})\varepsilon^{(u+v+1)z} \\ &\quad + p\sum_{\substack{u,v,z=1 \\ \bar{u}+\bar{v}+1\equiv 0\,(\mathrm{mod}\,p)}}^{p-1}\varepsilon^{(u+v+1)z} - p\sum_{\bar{u}+\bar{v}+1\equiv 0} 1.\end{aligned}$$

Summing over z we find

$$\sigma_3 = p\chi(-1)\Omega + p^2\sum_{\substack{\bar{u}+\bar{v}+1\equiv 0 \\ u+v+1\equiv 0}} 1 - p\sum_{\bar{u}+\bar{v}+1\equiv 0} 1.$$

The conditions in the first sum imply

$$u^2+u+1 \equiv v^2+v+1 \equiv 0 \ (\mathrm{mod}\, p)$$

and so the number of solutions is $1+\chi(-3)$. In the second sum there is exactly one u for each $v \neq p-1$. Hence the sum is $p-2$. Therefore we have

$$\sigma_3 = \chi(-1)p\Omega + p^2\big(1+\chi(-3)\big) - p(p-2) = p^2\chi(-3) + p\{2+\chi(-1)\Omega\}.$$

Separating the cases $p = 6n \pm 1$ and substituting from Lemma 1 we have (2). (3) now follows from (1). This completes the proof of Theorem 1.

References

[1] H. Salié, *Über die Kloostermanschen Summen $S(u, v; q)$*, 1936, Math. Zeit. 34 (1932), p. 91-109.

[2] E. Landau, *Vorlesungen über Zahlentheorie*, Leipzig 1927, V. 1, p. 153.

[3] E. Jacobsthal, *Anwendungen einer Formel aus der Theorie der quadratischen Reste*, Dissertation (Berlin 1906), or see Pacific Journal of Math. 6 (1956), p. 491-499.

Reçu par la Rédaction le 10. 8. 1959

ACTA ARITHMETICA
VI (1960)

On new "explicit formulas" in prime number theory II

by

S. Knapowski (Poznań)

1. The first part of this paper has been concerned with new explicit formulas for

$$\psi_0(x) = \frac{\psi(x-0)+\psi(x+0)}{2}, \quad \text{where} \quad \psi(x) = \sum_{n\leqslant x}\Lambda(n) \equiv \sum_{p^m\leqslant x}\log p,$$

depending upon the zeros of the partial sums $U_N(s) = \sum_{n\leqslant N} 1/n^s$ of the zeta-series. The following formula has been established ([2], Theorem):

$$\psi_0(x) = \frac{\log N!}{N} - \sum_{\varrho}\frac{x^\varrho}{\varrho}, \tag{1.1}$$

$\varrho = \beta + i\gamma$ running through the zeros of $U_N(s)$, $2 \leqslant x \leqslant N$, and N being sufficiently large. In the particular case of $N = [e^x]$ we have obtained

$$\psi_0(x) = x - \sum_{|\gamma|\leqslant x^{16},\, \beta\geqslant -1}\frac{x^\varrho}{\varrho} + O(\log x). \tag{1.2}$$

It seems to be worth while to generalise (1.1), (1.2) and find similar formulas depending upon the zeros of other Dirichlet-polynomials approximating to $\zeta(s)$. The most interesting case is that of the Riesz means

$$R_N(s) = \sum_{n\leqslant N}\Big(1-\frac{\log n}{\log N}\Big)n^{-s}, \qquad s = \sigma + it,$$

considering that they converge to $\zeta(s)$ in the closed half-plane $\sigma \geqslant 1$, $s \neq 1$ (see [3] and [4]). We are now going to study that case. We shall, in fact, find some analogies with (1.1), (1.2) and at the same time touch on the distribution of zeros of $R_N(s)$. It seems plausible that $R_N(s)$ do not vanish in the whole half-plane $\sigma \geqslant 1$. Yet, for the time being, we are only able to determine a certain portion of this half-plane which is free of the zeros of $R_N(s)$. We may note in passing that the regions announced