An extension of some formulae of Lerch

A. Schinzel

Abstract. A formula of Lerch expressing the sum of fractional parts of $x + a^2m/n$ $(a = 0, \dots, n-1)$ for n odd in terms of class number of binary quadratic forms is extended to the case of arbitrary n.

Let

$$E^*(x) = \begin{cases} x - \frac{1}{2} & \text{if } x \in \mathbb{Z}, \\ [x] & \text{otherwise;} \end{cases}$$

$$\phi(z,d) = \begin{cases} \sqrt{d} \sum\limits_{\nu=1}^{\infty} \left(\frac{\nu}{d}\right) \frac{\cos 2\nu z\pi}{\nu\pi} & \text{if } d \equiv -1 \bmod 4, \\ \sqrt{d} \sum\limits_{\nu=1}^{\infty} \left(\frac{\nu}{d}\right) \frac{\sin 2\nu z\pi}{\nu\pi} & \text{if } d \equiv 1 \bmod 4. \end{cases}$$

Lerch [4], [5] gave the following formula for n odd, $(m,n) = 1$

$$(1) \qquad \sum_{a=0}^{n-1} \left(E^*\left(x + \frac{a^2m}{n}\right) - \left(x + \frac{a^2m}{n}\right)\right) = -\frac{n}{2} + \sum_{n=dd'} \left(\frac{m}{d}\right) \phi\left(d'x, d\right)$$

(see [2], p. 168). As an application he expressed in terms of class numbers of primitive binary quadratic forms the sums $\sum\limits_{a=0}^{n-1} \left\{x + \frac{a^2m}{n}\right\}$ for $x = 0, \frac{1}{2}, \frac{1}{4}$, where $\{\cdot\}$ is the fractional part. Particularly simple and elegant is the formula for $x = 0$, namely

$$(2) \qquad \sum_{a=0}^{n-1} \left\{\frac{a^2m}{n}\right\} = \frac{n-q}{2} - \sum_{\substack{d|n \\ d\equiv 3 \bmod 4}} \left(\frac{m}{d}\right) \frac{2}{w_d} h(-d)$$

Received: November 5, 2001.
1991 *Mathematics Subject Classification:* 11E41, 11L05.
Key words and phrases: binary quadratic forms, class number, Gauss sums.

where q^2 is the greatest square dividing n and $q > 0$, $h(-d)$ is the class number of primitive binary quadratic forms with discriminant $-d$ and w_d is the number of integer solutions of the equation $u^2 + dv^2 = 4$, hence

$$c_d = \frac{2}{w_d} = \begin{cases} 1/3 & \text{if } d = 3, \\ 1/2 & \text{if } d = 4, \\ 1 & \text{otherwise.} \end{cases}$$

Lerch returned to the formula (2) in [6] and proved it by a different method for n odd being the absolute value of a fundamental discriminant. For n even with the same property Lerch obtained ([6], p. 245, formula (41))

$$(3) \qquad \sum_{a=0}^{n-1} \left\{ \frac{a^2 m}{n} \right\} = \frac{1}{2}n - 1 - \sum_{\delta} \left(\frac{-\delta}{m} \right) \left[1 - \left(\frac{2}{\delta} \right) + 2 \left(\frac{4}{\delta} \right) \right] \frac{2}{w_\delta} h(-\delta)$$

where δ runs through divisors of n such that $-\delta$ is a fundamental discriminant.

We shall extend the formulae (1) and (2) to the case of an arbitrary n. For this we need the following notation

$$\phi_1(z,d) = \begin{cases} \sqrt{d} \sum_{\nu=1}^{\infty} \left(\frac{d}{\nu}\right) \frac{\sin 2\nu z \pi}{\nu \pi} & \text{if } d \equiv 0, 1 \bmod 4, \\ 0, & \text{otherwise} \end{cases}$$

$$\phi_{-1}(z,d) = \begin{cases} \sqrt{d} \sum_{\nu=1}^{\infty} \left(\frac{-d}{\nu}\right) \frac{\cos 2\nu z \pi}{\nu \pi} & \text{if } d \equiv 0, -1 \bmod 4 \\ 0, & \text{otherwise.} \end{cases}$$

Then we have

Theorem. *For m, n coprime positive integers and for all $x \in \mathbb{R}$*

$$\sum_{a=0}^{n-1} \left(E^* \left(x + \frac{a^2 m}{n} \right) - \left(x + \frac{a^2 m}{n} \right) \right) =$$
$$= -\frac{n}{2} + \sum_{n = dd'} \left(\left(\frac{d}{m} \right) \phi_1 (d'x, d) + \left(\frac{-d}{m} \right) \phi_{-1} (d'x, d) \right).$$

Corollary 1. *For m, n coprime positive integers*

$$F(m,n) := \sum_{a=0}^{n-1} \left\{ \frac{a^2 m}{n} \right\} = \frac{n-q}{2} - \sum_{\substack{d \mid n \\ d \equiv 0,3 \bmod 4}} c_d \left(\frac{-d}{m} \right) h(-d)$$

where q^2 is the greatest square dividing $n, q > 0$.

Corollary 2. *For every m prime to n we have $F(m,n) \geq F(1,n)$ with the equality attained if and only if either m is a quadratic residue* mod n, *or $n/(n,2)$ is composed entirely of primes congruent to* 1 mod 4.

Theorem extends formula (1) since for $\varepsilon = \pm 1$,

$$\left(\frac{\varepsilon d}{m}\right) = \left(\frac{m}{d}\right), \ \phi(z,d) = \phi_\varepsilon(z,d) \text{ for } d \equiv \varepsilon \bmod 4.$$

Corollary 1 implies formulae (2) and (3). For (2) this is obvious, for (3) follows from the fact that for δ odd, $-\delta$ being a fundamental discriminant

$$\left(1 - \left(\frac{2}{\delta}\right) + 2\left(\frac{4}{\delta}\right)\right) h(-\delta) = h(-\delta) + h(-4\delta).$$

Before proceeding to a proof of the theorem I thank John Robertson for calling my attention to this circle of problems. The proof is based an

Lemma. *For coprime positive integers m and n*

$$(4) \qquad \varphi(m,n) := \sum_{a=0}^{n-1} e^{2\pi i \frac{ma^2}{n}} = \begin{cases} \left(\frac{n}{m}\right)\sqrt{n} & \text{if } n \equiv 1 \bmod 4, \\ \left(\frac{-n}{m}\right) i\sqrt{n} & \text{if } n \equiv 3 \bmod 4, \\ 0 & \text{if } n \equiv 2 \bmod 4, \\ \left(\left(\frac{n}{m}\right) + \left(\frac{-n}{m}\right) i\right)\sqrt{n} & \text{if } n \equiv 0 \bmod 4 \end{cases}$$

and

$$(5) \qquad \varphi(dm, dn) = d\varphi(m,n).$$

Proof. Formula (4) for $m = 1$ and formula (5) are well known (see [1], p. 151, (17), p. 197, (78), where φ has a slightly different meaning and [3], Satz 211). Also well known are the following formulae

$$(6) \qquad \varphi(m,n) = \left(\frac{m}{n}\right)\varphi(1,n) \text{ for } n \text{ odd (see [1], p. 165, (45))},$$

$$(7) \qquad \varphi(m,n)\varphi(n,m) = \varphi(1,mn) \text{ for } (m,n) = 1 \text{ (ibid., p. 150, (16))}.$$

Now (4) for n odd follows from (6) since for $\varepsilon = \pm 1$,

$$\left(\frac{m}{n}\right) = \left(\frac{\varepsilon n}{m}\right) \text{ for } n \equiv \varepsilon (\bmod 4).$$

For $n \equiv 2 \bmod 4$, m odd we have by (6) and (7)

$$\varphi(m,n)\varphi(n,m) = 0$$

and, since by (6) $\varphi(n,m) \neq 0$, it follows that $\varphi(m,n) = 0$.
For $n \equiv 0 \bmod 4$, m odd we have by (6) and (7)

$$\varphi(m,n) = \frac{\varphi(1,mn)}{\varphi(n,m)} =$$

$$= \frac{(1+i)\sqrt{mn}}{\left(\frac{n}{m}\right) i^{\left(\frac{m-1}{2}\right)^2}\sqrt{m}} = \left(\left(\frac{n}{m}\right) + (-1)^{\frac{m-1}{2}}\left(\frac{n}{m}\right) i\right)\sqrt{n} = \left(\left(\frac{n}{m}\right) + \left(\frac{-n}{m}\right) i\right)\sqrt{n}.$$

Proof of Theorem. We have, following [5] (see also [3], Satz 216)

$$E^*(x) = x - \frac{1}{2} + \sum_{\nu=1}^{\infty} \frac{\sin 2\nu x\pi}{\nu\pi}.$$

Hence

$$\begin{aligned}
S := \sum_{a=0}^{n-1}\left(E^*\left(x+\frac{a^2m}{n}\right)-\left(x+\frac{a^2m}{n}\right)\right) &= -\frac{n}{2}+\sum_{a=0}^{n-1}\sum_{\nu=1}^{\infty}\frac{\sin 2\nu\left(x+\frac{a^2m}{n}\right)\pi}{\nu\pi} \\
&= -\frac{n}{2}+\sum_{\nu=1}^{\infty}\sum_{a=0}^{n-1}\frac{\sin 2\nu x\pi\cos 2\nu\pi a^2m/n+\cos 2\nu x\pi \sin 2\nu\pi a^2 m/n}{\nu\pi} \\
&= -\frac{n}{2}+\sum_{\nu'=1}^{\infty}\left(\frac{\sin 2\nu' x\pi}{\nu'\pi}\Re\varphi(m\nu',n)+\frac{\cos 2\nu' x\pi}{\nu'\pi}\Im\varphi(m\nu',n)\right)
\end{aligned}$$

and by Lemma, putting $(n,\nu') = d'$, $n = d'd$, $n' = d'\nu$

$$\begin{aligned}
S &= -\frac{n}{2}+\sum_{d\mid n}\sum_{\substack{\nu=1\\(\nu,d)=1}}^{\infty}\left(\frac{\sin 2\nu d' x\pi}{\nu d'\pi}d'\Re\varphi(m\nu,d)+\frac{\cos 2\nu d' x\pi}{\nu d'\pi}d'\Im\varphi(m\nu,d)\right) \\
&= -\frac{n}{2}+\sum_{\substack{d\mid n\\ d\equiv 0,1 \bmod 4}}\sum_{\nu=1}^{\infty}\frac{\sin 2\nu d' x\pi}{\nu\pi}\left(\frac{d}{m\nu}\right)\sqrt{d} \\
&\quad+\sum_{\substack{d\mid n\\ d\equiv 0,-1 \bmod 4}}\sum_{\nu=1}^{\infty}\frac{\cos 2\nu d' x\pi}{\nu\pi}\left(\frac{-d}{m\nu}\right)\sqrt{d} \\
&= -\frac{n}{2}+\sum_{d\mid n}\left(\left(\frac{d}{m}\right)\phi_1(d'x,d)+\left(\frac{-d}{m}\right)\phi_{-1}(d'x,d)\right).
\end{aligned}$$

Proof of Corollary 1. Using Theorem for $x = 0$ we obtain

$$\sum_{a=0}^{n-1}\left(E^*\left(\frac{a^2m}{n}\right)-\frac{a^2m}{n}\right) = -\frac{n}{2}+\sum_{d\mid n}\left(\left(\frac{d}{m}\right)\phi_1(0,d)+\left(\frac{-d}{m}\right)\phi_{-1}(0,d)\right).$$

However

$$\left\{\frac{a^2m}{n}\right\} = \begin{cases}\frac{a^2m}{n}-E^*\left(\frac{a^2m}{n}\right)-\frac{1}{2} & \text{if } a^2\equiv 0 \bmod n,\\ \frac{a^2m}{n}-E^*\left(\frac{a^2m}{n}\right) & \text{otherwise;}\end{cases}$$

$$\phi_1(0,d) = 0,$$

$$\phi_{-1}(0,d) = \begin{cases}\sqrt{d}\sum_{\nu=1}^{\infty}\frac{1}{\nu\pi}\left(\frac{-d}{\nu}\right) = c_d h(-d) \text{ if } d\equiv 0,3 \bmod 4,\\ 0, \text{otherwise}\end{cases}$$

(for the last formula see [3], Satz 209). Hence

$$\sum_{a=0}^{n-1}\left\{\frac{a^2m}{n}\right\}=\frac{n}{2}-\frac{1}{2}\sum_{\substack{a=0\\ n\mid a^2}}^{n-1}1-\sum_{\substack{d\mid n\\ d\equiv 0,3 \bmod 4}}\left(\frac{-d}{m}\right)c_d h(-d).$$

It remains to notice that $n \mid a^2$, if and only if $\frac{n}{q} \mid a$, hence

$$\sum_{\substack{a=0\\ n\mid a^2}}^{n-1}1=q.$$

Remark. It is possible to prove Corollary 1 by the method of [6], but the proof is longer. It is also possible to evaluate the sum $\sum_{a=0}^{n-1}\left\{x+\frac{a^2m}{n}\right\}$ in terms of class numbers for $x=\frac{1}{2}$ or $\frac{1}{4}$ and arbitrary n, but the formulae are more complicated. We give without proof the formula for $x=\frac{1}{2}$ to be compared with that quoted in [2], p. 168

$$\sum_{a=0}^{n-1}\left\{\frac{1}{2}+\frac{a^2m}{n}\right\}=\frac{n}{2}-\frac{q}{4}\left(1+(-1)^{n/q^2}\right)+$$
$$+\sum_{\substack{n=dd'\\ d\equiv 0,3 \bmod 4\\ d'\equiv 1 \bmod 2}}\left(\frac{-d}{m}\right)c_d\left(1-\left(\frac{-d}{2}\right)\right)h(-d)-\sum_{\substack{n=dd'\\ d\equiv 0,3 \bmod 4\\ d'\equiv 0 \bmod 2}}\left(\frac{-d}{m}\right)c_d h(-d)$$

and the formula for $x=\frac{1}{4}$ and $n\equiv 2 \bmod 4$,

$$\sum_{a=0}^{n-1}\left\{\frac{1}{4}+\frac{a^2m}{n}\right\}=\frac{n}{2}+2\sum_{\substack{d\mid n\\ d\equiv 3 \bmod 8}}\left(\frac{-d}{m}\right)c_d h(-d),$$

which is simpler than that for $n\equiv 1 \bmod 2$ quoted in [2], p. 158, formula (2).

Proof of Corollary 2. It is clear that $F(m,n)\geq F(1,n)$, that the condition for the equality is sufficient and that $F(m,n)=F(1,n)$ implies $\left(\frac{-d}{m}\right)=1$ for all divisors d of n congruent to 0 or 3 mod 4. Assume that $F(m,n)=F(1,n)$ and suppose first that $n\not\equiv 0 \bmod 4$. Then for every prime factor q of n, $q\equiv 3 \bmod 4$, we have $\left(\frac{-q}{m}\right)=1$, hence $\left(\frac{m}{q}\right)=1$ and if there is at least one such q_0, then for every prime factor p of $n, p\equiv 1 \bmod 4$ $\left(\frac{-pq_0}{m}\right)=1$ implies $\left(\frac{p}{m}\right)=1$, hence $\left(\frac{m}{p}\right)=1$ and m is a quadratic residue mod n. Suppose now that $n\equiv 4\,(\mathrm{mod}\ 8)$. Then $\left(\frac{-4}{m}\right)=1$ implies $m\equiv 1 \bmod 4$ and for every odd prime factor p of n, $\left(\frac{-4p}{m}\right)=1$ implies $\left(\frac{m}{p}\right)=1$, hence m is a quadratic residue mod n. Suppose finally that $n\equiv 0\,(\mathrm{mod}\ 8)$. Then $\left(\frac{-4}{m}\right)=\left(\frac{-8}{m}\right)=1$ implies $m\equiv 1 \bmod 8$ and for every odd prime factor p of n, $\left(\frac{-4p}{m}\right)=1$ implies $\left(\frac{m}{p}\right)=1$, hence m is again a quadratic residue mod n.

References

[1] P. Bachmann, *Die analytische Zahlentheorie*, Leipzig 1894.

[2] L.E. Dickson, *History of the theory of numbers*, vol. 3, reprint Chelsea 1952.

[3] E. Landau, *Vorlesungen über Zahlentheorie. Aus der elementaren Zahlentheorie*, reprint Chelsea 1950.

[4] M. Lerch, *O součtu celych etc.* (Czech), Rozpravy česke akademie 7 (1898), No 7.

[5] M. Lerch, *Sur quelques applications des sommes de Gauss*, Annali Mat. Pura Appl. 11 (1905), 79–91.

[6] M. Lerch, *Essais sur le calcul du nombre des classes de formes quadratiques binaires aux coefficients entiers II*, Acta Math. 30 (1906), 203–293.