A SUM CONNECTED WITH THE SERIES FOR THE PARTITION FUNCTION

ALBERT LEON WHITEMAN

1. Introduction. The famous formula of Rademacher [5] for the number $p(n)$ of partitions of an integer n states that

$$p(n)=\frac{1}{\pi\sqrt{2}}\sum_{k=1}^{\infty} A_k(n)k^{1/2}\frac{d}{dn}\left(\frac{\sinh(K\lambda/k)}{\lambda}\right),$$

where $K=\pi(2/3)^{1/2}$, $\lambda=(n-1/24)^{1/2}$ and the series is absolutely convergent. The coefficients $A_k(n)$ are defined by

$$A_1(n)=1\ ,\quad A_2(n)=(-1)^n\ ,\quad A_3(n)=2\cos\left[\pi(12n-1)/18\right]\ ,$$

and in general

$$A_k(n)=\sum_{(h,k)=1}\omega_{h,k}\exp(-2\pi ihn/k)\ , \tag{1.1}$$

where h ranges over those numbers which are less than k and prime to k. The numbers $\omega_{h,k}$ are certain $24k$th roots of unity which arise in the theory of modular functions and are defined by

$$\omega_{h,k}=\left(\frac{-h}{k}\right)\exp\left[-\left\{\frac{1}{4}(k-1)+\frac{1}{12}\left(k-\frac{1}{k}\right)(2h+\bar{h}-h^2\bar{h})\right\}\pi i\right] \tag{1.2}$$

if k is odd, and by

$$\omega_{h,k}=\left(\frac{-k}{h}\right)\exp\left[-\left\{\frac{1}{4}(2-hk-h)+\frac{1}{12}\left(k-\frac{1}{k}\right)(2h+\bar{h}-h^2\bar{h})\right\}\pi i\right] \tag{1.3}$$

when k is even. Here $(a|b)$ is the symbol of Jacobi and $\bar{h}$ is defined as any solution of the congruence $h\bar{h}\equiv 1 \pmod{k}$.

Because of the intricacy of the numbers $\omega_{h,k}$ the task of evaluating $A_k(n)$ for large k directly from its definition in (1.1) is quite formidable. To surmount this difficulty D. H. Lehmer [3] made an intensive study of the $A_k(n)$. He was able to reduce them to sums studied by H. D. Kloosterman and H. Salié. In the first place he factored the $A_k(n)$ according to the prime number powers contained in k. Secondly, by using Salié's formulas, he evaluated $A_k(n)$ explicitly in the case in which k is a prime or a power of a prime. Both results together provide a method for calculating the $A_k(n)$. It should also be mentioned that another

Received May 10, 1954. This investigation was supported by the Office of Naval Research. The author is indebted to Professor Atle Selberg who kindly communicated to him the hitherto unpublished result given in formula (1.4).

method for evaluating and factorizing $A_k(n)$ based on a different expression for $\omega_{h,k}$ is given in [6] and [7].

Some years ago Atle Selberg proved (but did not publish) the result that $A_k(n)$ may be expressed alternatively in the form

$$A_k(n)=\left(\frac{k}{3}\right)^{1/2} \sum_{(3l^2+l)/2\equiv -n (\bmod k)} (-1)^l \cos\frac{6l+1}{6k}\pi \,, \tag{1.4}$$

where l runs over integers in the range $0\leq l<2k$ which satisfy the summation condition. In this striking formula $A_k(n)$ is expressed as a sum which involves only cosines and which contains considerably fewer terms than (1.1). Selberg's derivation of (1.4) is based upon an investigation of the underlying function $\eta(\tau)$ which plays a fundamental role in the theory of elliptic modular functions. A related investigation has been made by Fischer [1] for the determination of a $24k$th root of unity closely connected with $\omega_{h,k}$.

In §§ 2, 3, 4 of this paper we give a direct proof of the equivalence of the two formulas (1.1) and (1.4) for $A_k(n)$. The method of proof consists in showing that (1.1) is the finite Fourier series expansion of (1.4). In § 5 we show that (1.4) may be transformed in various ways (Theorems 1, 2, 3 and 4) so as to yield formulas which are suitable for the direct computation of $A_k(n)$. These formulas in turn reduce immediately to the formulas of Lehmer in the case in which k is a prime or a power of a prime. Finally in § 6 we show that the theorems in § 5 may be utilized to derive three factorization theorems (Theorems 5, 6 and 7) for the $A_k(n)$. It will be seen that the present approach to the evaluation of $A_k(n)$ makes no use of Kloosterman sums.

2. Finite Fourier series expansion of $A_k(n)$. The connection between the two expressions for $A_k(n)$ given in (1.1) and (1.4) is clear from the viewpoint of finite Fourier series. The function $A_k(n)$ defined by (1.4) is periodic in the variable n with period k. Hence it permits of expansion into a finite Fourier series of the form

$$A_k(n)=\sum_{h=0}^{k-1} \rho_{h,k} \exp\left(-\frac{2\pi ihn}{k}\right). \tag{2.1}$$

We shall prove that the coefficients $\rho_{h,k}$ are determined by the formula

$$\rho_{h,k}=\begin{cases} 0 & ((h,k)>1)\,, \\ \omega_{h,k} & ((h,k)=1)\,, \end{cases} \tag{2.2}$$

where $\omega_{h,k}$ is defined by (1.2) and (1.3). Consequently (2.1) reduces to (1.1).

Inverting (2.1) we obtain first

$$\rho_{h,k}=\frac{1}{k}\sum_{j=0}^{k-1}A_k(j)\exp\left(\frac{2\pi ihj}{k}\right). \tag{2.3}$$

Then substituting from (1.4) into (2.3) we get

$$\begin{aligned}\rho_{h,k}&=\frac{1}{(3k)^{1/2}}\sum_{l(\mathrm{mod}\,2k)}(-1)^l\cos\frac{6l+1}{6k}\pi\exp\left[-\frac{\pi ih}{k}(3l^2+l)\right]\\ &=\frac{\exp(\pi i/6k)}{2(3k)^{1/2}}\sum_{l\,(\mathrm{mod}\,2k)}\exp\left[\frac{\pi i}{k}(-3hl^2+l(k-h+1))\right]\\ &\quad+\frac{\exp(-\pi i/6k)}{2(3k)^{1/2}}\sum_{l\,(\mathrm{mod}\,2k)}\exp\left[\frac{\pi i}{k}(-3hl^2+l\,(k-h-1))\right],\end{aligned} \tag{2.4}$$

where the sums extend over any complete residue system modulo $2k$. In order to prove the first part of (2.2) we require the following lemma.

LEMMA 1. *Let a, b, c denote integers and let the highest common divisor d of h and k be greater than* 1. *If $d\nmid c$, then*

$$\sum_{l\,(\mathrm{mod}\,2k)}\exp\left[\frac{\pi i}{k}(ahl^2+bhl+cl)\right]=0\,. \tag{2.5}$$

Proof. We put $h=dh'$, $k=dk'$. Then the summation condition $l(\mathrm{mod}\,2k)$ is equivalent to the double summation condition $0\leqq r\leqq 2k'-1$, $l\equiv r(\mathrm{mod}\,2k')$, $0\leqq l<2k$. For each fixed value of r we put $l=r+2jk'$, $0\leqq j\leqq d-1$. The sum in (2.5) may now be written in the form

$$\sum_{r=0}^{2k'-1}\exp\left[\frac{\pi ih'}{k'}(ar^2+br)\right]\sum_{j=0}^{d-1}\exp\left[\frac{\pi ic}{k}(r+2jk')\right]. \tag{2.6}$$

Since $2\pi icjk'/k=2\pi icj/d$ and $d\nmid c$ it follows at once that the inner sum in the right member of (2.6) is equal to zero for each value of r. This proves the lemma.

Applying the lemma with $a=-3$, $b=-1$ and $c=k\pm 1$ to (2.4) we deduce from (2.5) that $\rho_{h,k}=0$ when $(h,k)>1$.

Turning to the proof of the second part of (2.2) we now assume that $(h,k)=1$. We proceed to complete the square in the two sums in the last member of (2.4). For this purpose it is convenient to assume that the solution $\bar{h}$ of the congruence $h\bar{h}\equiv 1\,(\mathrm{mod}\,k)$ is selected so that $(h\bar{h}-1)/k$ is even when k is even. We shall see later that this assumption entails no loss in generality. From the assumption it follows also that $\exp[\pi il(h\bar{h}-1)(k\pm 1)/k]=1$. The two sums in the last member of (2.4) may now be written in the form

$$(2.7)\qquad \sum_{l\,(\mathrm{mod}\,2k)} \exp\left[\frac{\pi i}{k}(-3hl^2+l(k-h\pm 1))\right]\exp\left[\frac{\pi i l}{k}(h\bar{h}-1)(k\pm 1)\right],$$

which reduces after simplification to

$$(2.8)\qquad \exp\left[\frac{\pi i h}{12k}(1-\bar{h}k\mp\bar{h})^2\right]\sum_{l\,(\mathrm{mod}\,2k)}\exp\left[-\frac{\pi i h}{12k}(6l+(1-\bar{h}k\mp\bar{h}))^2\right].$$

It is therefore natural to introduce the sum

$$(2.9)\qquad H_{h,k}(\gamma)=\frac{1}{2}\sum_{j\,(\mathrm{mod}\,2k)}\exp\left[\frac{\pi i h}{12k}(6j+\gamma)^2\right]$$

for integers h, k and γ with $k>0$. This sum has already been employed by Fischer in his paper cited in the introduction. Combining the results in (2.4), (2.7) and (2.8) we obtain a formula for $\rho_{h,k}$ which is given in the following lemma.

LEMMA 2. *For $(h,k)=1$ let the solution $\bar{h}$ of the congruence $h\bar{h}\equiv 1 \pmod{k}$ be selected so that $(h\bar{h}-1)/k$ is even when k is even. Then the finite Fourier coefficient $\rho_{h,k}$ defined in* (2.1) *has the value*

$$(2.10)\qquad \rho_{h,k}=\frac{1}{(3k)^{1/2}}\left\{\exp\left[\frac{\pi i}{12k}(2+h\alpha^2)\right]H_{-h,k}(\alpha)\right.$$
$$\left.+\exp\left[\frac{\pi i}{12k}(2+h\beta^2)\right]H_{-h,k}(\beta)\right\},$$

where $H_{h,k}(\gamma)$ is defined by (2.9) *and α, β are defined by*

$$(2.11)\qquad \alpha=1-\bar{h}k-\bar{h}\,,\qquad \beta=1-\bar{h}k+\bar{h}\,.$$

Next we must evaluate $H_{h,k}(\gamma)$. This is accomplished in the following section.

3. **The sum $H_{h,k}(\gamma)$.** It is evident that the sum $H_{h,k}(\gamma)$ is closely related to the classical Gauss sum defined by

$$(3.1)\qquad G_{h,k}=\sum_{j\,(\mathrm{mod}\,k)}\exp\left(\frac{2\pi i h j^2}{k}\right).$$

Indeed we shall make use of the following formulas which are taken from Fischer's paper [1, § 3].

If k is odd and $3|k$, then

$$(3.2)\qquad H_{h,k}(1)=0,\ H_{h,k}(3)=\exp\left(\frac{3}{4}\pi i h k\right)G_{2h,3k}\,.$$

If k is odd and $3 \nmid k$, then

$$(3.3)\qquad H_{h,k}(1)=\exp\left(\frac{4}{3}\pi ihk\right)H_{h,k}(3)\ ,$$

$$(3.4)\qquad H_{h,k}(3)=\left(\frac{k}{3}\right)\exp \pi i\left(\frac{k-1}{2}+\frac{3hk}{4}\right)G_{2h,k}\ .$$

If $k=2^\lambda k_1$, $\lambda \geqq 1$, k_1 odd and $3|k$, then

$$(3.5)\qquad H_{h,k}(2)=0,\qquad H_{h,k}(0)=2^{\lambda/2}\left(\frac{2}{h}\right)^\lambda \exp\left(\frac{3}{4}\pi ihk_1\right)G_{2h,3k_1}\ .$$

If $k=2^\lambda k_1$, $\lambda \geqq 1$, k_1 odd and $3 \nmid k$, then

$$(3.6)\qquad H_{h,k}(2)=\exp\left(\frac{4}{3}\pi ihk\right)H_{h,k}(0)\ ,$$

$$(3.7)\qquad H_{h,k}(0)=\left(\frac{k}{3}\right)2^{\lambda/2}\left(\frac{2}{h}\right)^\lambda \exp \pi i\left(\frac{k_1-1}{2}+\frac{3hk_1}{4}\right)G_{2h,k_1}\ .$$

We note also the easily established relations

$$(3.8)\qquad H_{h,k}(\gamma)=H_{h,k}(-\gamma)=H_{h,k}(\gamma+6n)\ ,$$

which are valid for any integer n.

For $G_{h,k}$ defined in (3.1) we shall require the following well-known formulas which may be found, for example, in [4, Chapter 5].

$$(3.9)\qquad G_{h,k}=\left(\frac{h}{k}\right)G_{1,k}\qquad (k \text{ odd}).$$

$$(3.10)\qquad G_{1,k}=k^{1/2}i^{((k-1)/2)^2}\qquad (k \text{ odd}).$$

$$(3.11)\qquad G_{h,2^\lambda}=\begin{cases}0 & (h \text{ odd},\ \lambda=1),\\ 2^{(\lambda+1)/2}\left(\dfrac{2}{h}\right)^{\lambda+1}e^{\pi ih/4} & (h \text{ odd},\ \lambda \geqq 2).\end{cases}$$

We also recall the formulas $(-1|k)=(-1)^{(k-1)/2}$ and $(2|k)=(-1)^{(k^2-1)/8}$ which are valid for k odd.

Using (3.9) and (3.10) we may deduce from (3.2) and (3.4) that

$$(3.12)\qquad H_{h,k}(3)=\left(\frac{h}{k}\right)\left(\frac{h}{3}\right)\exp\left[\frac{\pi i}{4}(3hk-3k+1)\right](3k)^{1/2}\qquad (k \text{ odd},\ 3|k),$$

$$(3.13)\qquad H_{h,k}(3)=\left(\frac{h}{k}\right)\left(\frac{k}{3}\right)\exp\left[\frac{\pi i}{4}(3hk+k-1)\right]k^{1/2}\qquad (k \text{ odd},\ 3 \nmid k).$$

Using (3.9), (3.10) and (3.11) and the law of quadratic reciprocity for the Jacobi symbol we find after some manipulation that the formulas for

$H_{h,k}(0)$ in (3.5) and (3.7) reduce to

$$(3.14)\qquad H_{-h,k}(0)=\left(\frac{-k}{h}\right)\left(\frac{h}{3}\right)\exp\left[\frac{\pi i}{4}(3h+4)\right](3k)^{1/2}\quad (h>0,\ k \text{ even},\ 3|k),$$

$$(3.15)\qquad H_{-h,k}(0)=\left(\frac{-k}{h}\right)\left(\frac{k}{3}\right)\exp\left[\frac{\pi i}{4}(-h-2)\right]k^{1/2}\quad (h>0,\ k \text{ even},\ 3\nmid k).$$

4. Proof of Selberg's formula (1.4). In order to prove the second part of (2.2) we shall show that $\omega_{h,k}$ is equal to the right member of (2.10) when $(h,k)=1$. It is convenient to write the expressions for $\omega_{h,k}$ in (1.2) and (1.3) in the form

$$(4.1)\qquad \omega_{h,k}=\begin{cases}\left(\frac{-h}{k}\right)\exp\left[\frac{\pi i}{12k}f(h,k)\right] & (k \text{ odd}),\\[2ex] \left(\frac{-k}{h}\right)\exp\left[\frac{\pi i}{12k}f(h,k)\right] & (k \text{ even}),\end{cases}$$

where

$$(4.2)\qquad f(h,k)=\begin{cases}-[3k(k-1)+(k^2-1)(2h+\bar h-h^2\bar h)] & (k \text{ odd}),\\ -[6k-h(k+1)(k+2)-(k^2-1)(h^2-1)\bar h] & (k \text{ even}).\end{cases}$$

We divide the discussion into two principal cases.

Case 1. *k divisible by* 3. Then $3\nmid h$ and $h\equiv\bar h \pmod 3$. If k is odd, then $\alpha\equiv 3$ or $-1 \pmod 6$ and $\beta\equiv -1$ or $3 \pmod 6$ according as $h\equiv 1$ or $-1 \pmod 3$. If k is even, then $\alpha\equiv 0$ or $2 \pmod 6$ and $\beta\equiv 2$ or $0 \pmod 6$ according as $h\equiv 1$ or $-1 \pmod 3$.

If $h\equiv 1 \pmod 3$ we see by (3.2), (3.5) and (3.8) that $H_{-h,k}(\beta)=0$ and hence (2.10) reduces to

$$(4.3)\qquad \rho_{h,k}=\frac{1}{(3k)^{1/2}}\exp\left[\frac{\pi i}{12k}(2+h\alpha^2)\right]H_{-h,k}(\alpha)\ .$$

To show that the right member of (4.3) reduces to $\omega_{h,k}$ we replace $H_{-h,k}(\alpha)$ by its value as given in (3.12) or (3.14). The factor $(3k)^{1/2}$ in the denominator of $\rho_{h,k}$ is thereby cancelled. Comparing the result after simplification with (4.1) we find that it suffices to prove that

$$(4.4)\qquad f(h,k)\equiv\begin{cases}2-9k-9(h+1)k^2+h\alpha^2 \pmod{24k} & (k \text{ odd}),\\[1ex] 2-12k+9hk+h\alpha^2 \pmod{24k} & (k \text{ even}),\end{cases}$$

where $f(h,k)$ is defined by (4.2). If k is odd it is easily seen that both members of (4.4) are $\equiv 3k-3 \pmod 8$. With respect to the modulus $3k$ the congruence (4.4) reduces after some manipulation to the easily verified congruence $(h+\bar{h}-2)(h\bar{h}-1)\equiv 0 \pmod{3k}$. If k is even (and hence divisible by 6) the congruence (4.4) reduces to $(h+\bar{h}-2)(h\bar{h}-1)\equiv 0 \pmod{24k}$. The last congruence follows from the hypothesis of Lemma 2. For we have $h\bar{h}\equiv 1 \pmod{2k}$ and hence $h\equiv\bar{h} \pmod{12}$. Since $h\equiv 1$ or $7 \pmod{12}$ we deduce that $h+\bar{h}\equiv 2 \pmod{12}$.

If $h\equiv -1 \pmod 3$ we have to replace in (4.3) $2+h\alpha^2$ by $-2+h\beta^2$ and $H_{-h,k}(\alpha)$ by $H_{-h,k}(\beta)$. If k is odd the right member of (4.4) becomes $-2+3k-9(h+1)k^2+h\beta^2$, and if k is even the right member becomes $-2+h\beta^2+9hk$. We may complete the proof in Case 1 by an argument similar to the one used when $h\equiv 1 \pmod 3$.

Case 2. *k not divisible by* 3. If $k\equiv 1 \pmod 6$, then $\beta\equiv 1 \pmod 6$. Furthermore $\bar{h}\equiv 0$ or $1 \pmod 3$ implies $\alpha\equiv \pm 1 \pmod 6$, and $\bar{h}\equiv -1 \pmod 3$ implies $\alpha\equiv 3 \pmod 6$. If $k\equiv -1 \pmod 6$, then $\alpha\equiv 1 \pmod 6$. Moreover $\bar{h}\equiv 0$ or $-1 \pmod 3$ implies $\beta\equiv\pm 1 \pmod 6$, and $\bar{h}\equiv 1 \pmod 3$ implies $\beta\equiv 3 \pmod 6$. If $k\equiv 2 \pmod 6$, then $\alpha\equiv -2 \pmod 6$. Furthermore $\bar{h}\equiv 0$ or $-1 \pmod 3$ implies $\beta\equiv \pm 2 \pmod 6$, and $\bar{h}\equiv 1 \pmod 3$ implies $\beta\equiv 0 \pmod 6$. Finally if $k\equiv -2 \pmod 6$, then $\beta\equiv -2 \pmod 6$. Moreover $\bar{h}\equiv 0$ or $1 \pmod 3$ implies $\alpha\equiv\pm 2 \pmod 6$, and $\bar{h}\equiv -1 \pmod 3$ implies $\alpha\equiv 0 \pmod 6$.

We now return to the value of $\rho_{h,k}$ in (2.10). In order to evaluate $H_{-h,k}(\alpha)$ and $H_{-h,k}(\beta)$ it suffices to use formulas (3.3) and (3.13) when k is odd and formulas (3.6) and (3.15) when k is even. Unlike the corresponding situation in the proof of Case 1 the factor $\sqrt{3}$ appearing in the denominator of $\rho_{h,k}$ is not immediately cancelled. Accordingly we need a device for separating the factor $\sqrt{3}$ from the numerator of $\rho_{h,k}$. To accomplish this we shall require the following congruences. If $k\equiv 1$ or $-2 \pmod 6$, then

$$(4.5)\qquad 4k-4-h(\alpha^2-\beta^2)\equiv\begin{cases}0 \pmod{24k} & (\bar{h}\equiv 0 \text{ or } 1 \pmod 3),\\ 16hk \pmod{24k} & (\bar{h}\equiv -1 \pmod 3).\end{cases}$$

If $k\equiv -1$ or $2 \pmod 6$, then

$$(4.6)\qquad -4k-4-h(\alpha^2-\beta^2)\equiv\begin{cases}0 \pmod{24k} & (\bar{h}\equiv 0 \text{ or } -1 \pmod 3),\\ 16hk \pmod{24k} & (\bar{h}\equiv 1 \pmod 3).\end{cases}$$

To prove (4.5) and (4.6) we first note that the definition of α and β in (2.11) implies $\alpha^2-\beta^2=-4\bar{h}(1-\bar{h}k)$. It is now an easy matter to verify the various cases which arise. When k is even we again make use of the assumption that $h\bar{h}\equiv 1 \pmod{2k}$.

Turning to the case when $k\equiv 1$ or $-2 \pmod 6$ we utilize congruence

(4.5) in the following manner. Employing (3.3), (3.6) and (3.8) we first make in (2.10) the substitution $H_{-h,k}(\beta)=H_{-h,k}(\alpha)$ when $\bar{h}\equiv 0$ or $1 \pmod 3$ and $H_{-h,k}(\beta)=\exp(-4\pi i hk/3)H_{-h,k}(\alpha)$ when $\bar{h}\equiv -1 \pmod 3$. Next we multiply and divide the numerator of $\rho_{h,k}$ by $\exp[\pi i(2k-2-h\alpha^2)/12k]$ and then apply the congruence (4.5). It is not difficult to verify that we introduce in this way the factor $e^{\pi i/6}+e^{-\pi i/6}=\sqrt{3}$. In general the expression for $\rho_{h,k}$ in (2.10) now reduces to

$$\rho_{h,k}=\frac{1}{k^{1/2}}\exp\left[-\frac{\pi i}{12k}(2k-2-h\alpha^2)\right]H_{-h,k}(\alpha)\,. \tag{4.7}$$

The value of $H_{-h,k}(\alpha)$ is given in (3.3) and (3.13) when $k\equiv 1 \pmod 6$ and is given in (3.6) and (3.15) when $k\equiv -2 \pmod 6$. We have to prove that the right member of (4.7) is equal to $\omega_{h,k}$.

Suppose first that $\bar{h}\equiv 0$ or $1 \pmod 3$. Proceeding as in the proof of Case 1 we find that it suffices to prove that

$$f(h,k)\equiv\begin{cases}2-5k-(h-3)k^2+h\alpha^2 \pmod{24k} & (k\equiv 1 \pmod 6)),\\ 2-(3h+8)k-16hk^2+h\alpha^2 \pmod{24k} & (k\equiv -2 \pmod 6)).\end{cases} \tag{4.8}$$

Both members of the first congruence in (4.8) are $\equiv 0 \pmod 3$ and $3k-3 \pmod 8$. With respect to the modulus k the congruence reduces to $(h+\bar{h}-2)(h\bar{h}-1)\equiv 0 \pmod k$. Both members of the second congruence are $\equiv 0 \pmod 3$. With respect to the modulus $8k$ the second congruence reduces to the congruence $(h+\bar{h}-2)(h\bar{h}-1)\equiv 0 \pmod{8k}$. To prove the last congruence we note that h is odd when k is even. Hence $h\bar{h}\equiv 1 \pmod{2k}$ implies $h+\bar{h}-2\equiv 0 \pmod 4$.

Suppose next that $\bar{h}\equiv -1 \pmod 3$. The discussion is similar to that used when $\bar{h}\equiv 0$ or $1 \pmod 3$. In this case, however, it is necessary to replace $(h-3)k^2$ in the first congruence of (4.8) by $(9h-3)k^2$ and to omit the term $-16hk^2$ in the second congruence.

Finally we turn to the case when $k\equiv -1$ or $2 \pmod 6$. The argument now proceeds along the same lines as in the case $k\equiv 1$ or $-2 \pmod 6$. It turns out in this case, however, that the expression for $\rho_{h,k}$ given in (4.7) must be modified by replacing $\exp[-\pi i(2k-2-h\alpha^2)/12k]$ by $\exp[-\pi i(-2k-2-h\alpha^2)/12k]$.

In conclusion we summarize the results established in this section. When $(h,k)=1$ we have proved that $\rho_{h,k}$ is equal to the right member of (1.2) if k is odd and is equal to the right member of (1.3) if k is even. In the proof the assumption was made that $(h\bar{h}-1)/k$ is even when k is even. We now point out that this assumption does not lead to a loss of generality in the final result. For it is easy to verify that the right member of (1.3) is independent of the choice of $\bar{h}$.

5. Evaluation of $A_k(n)$. Lehmer [3] has evaluated the sum $A_k(n)$ in the case when k is a power of a prime. In the present section we derive from (1.4) formulas for $A_k(n)$ which are valid for arbitrary k, and which reduce immediately to Lehmer's formulas when k is replaced by a power of a prime. Four cases present themselves quite naturally according as the greatest common divisor of k and 6 is 1, 2, 3 or 6. First it is convenient to note that when k is odd we may write (1.4) in the form

$$A_k(n)=2\left(\frac{k}{3}\right)^{1/2}\sum_{(6l+1)^2\equiv v \pmod{24k}}(-1)^l\cos\frac{6l+1}{6k}\pi\,, \tag{5.1}$$

where we have put $v=1-24n$, and where now l runs over integers in the range $0\leqq l<k$ which satisfy the summation condition.

Case 1. *k odd and not divisible by* 3. In order that solutions exist of the congruence $x^2\equiv v \pmod k$ it is, of course, necessary that v be a quadratic residue of every prime factor of k. We now set up a one-to-one correspondence between the roots of the congruence $(6l+1)^2\equiv v \pmod{24k}$, $0\leqq l<k$, and the roots of the congruence $(24m)^2\equiv v \pmod k$. This correspondence is effected by means of the congruence $6l+1\equiv 24m \pmod k$, which associates each solution l of the first congruence with a unique solution m of the second. Conversely, to distinct solutions of the second congruence correspond distinct solutions of the first. We put also $6l'+1\equiv -24m \pmod k$, $0\leqq l'<k$. Thus if $k\equiv 1 \pmod 6$, then $l'=(k-1)/3-l$ when $0\leqq l\leqq(k-1)/3$ and $l'=(4k-1)/3-l$ when $(k-1)/3<l<k$. But if $k\equiv -1 \pmod 6$, then $l'=(2k-1)/3-l$ when $0\leqq l\leqq(2k-1)/3$ and $l'=(5k-1)/3-l$ when $(2k-1)/3<l<k$. As l runs over the integers which satisfy the summation condition of (5.1) so does l'. In the sum (5.1) we now pair off each l with the corresponding l'. Then we have the identity

$$\begin{aligned}\cos\frac{6l(k+1)+1}{6k}\pi+\cos\frac{6l'(k+1)+1}{6k}\pi \\ =2\cos\frac{3(l+l')(k+1)+1}{6k}\pi\cos\frac{(l-l')(k+1)}{2k}\pi\,.\end{aligned} \tag{5.2}$$

Consider the first cosine factor in the right member of (5.2). Since $3(l+l')(k+1)+1\equiv\pm k$ or $\pm 5k \pmod{12k}$ we see that this factor equals $\pm\cos(\pi/6)$ or $\pm\sqrt{3}/2$. More precisely if $k\equiv 1 \pmod 6$, then this factor equals $-\sqrt{3}/2$ unless $k\equiv 1 \pmod{12}$ and $0\leqq l\leqq(k-1)/3$, but if $k\equiv -1$

(mod 6), then it equals $+\sqrt{3}/2$ unless $k\equiv 5 \pmod{12}$ and $(2k-1)/3<l<k$. As for the second cosine factor we note that $(l-l')(k+1)/4$ is an integer when $k\equiv 3 \pmod 4$. It is also an integer when $k\equiv 1 \pmod{12}$, $0\leqq l\leqq (k-1)/3$ and when $k\equiv 5 \pmod{12}$, $(2k-1)/3<l<k$. Otherwise $(k+l-l')(k+1)/4$ is an integer. Since $l-l'\equiv 8m \pmod k$ it is clear that the integer under consideration $\equiv 2m \pmod k$. It follows that when $(l-l')(k+1)/4$ is an integer the second cosine factor equals $\cos(4\pi m/k)$. Otherwise the second cosine factor equals $-\cos(4\pi m/k)$. Collecting these results we find in general that the right member of (5.2) reduces to $(3|k)\sqrt{3}\cos(4\pi m/k)$, where we note that $(3|k)=\pm 1$ according as $k\equiv\pm 1 \pmod{12}$ or $k\equiv\pm 5 \pmod{12}$. Thus we have proved the following theorem.

THEOREM 1. *If k is odd and not divisible by 3, then*

$$A_k(n)=\left(\frac{3}{k}\right)k^{1/2}\sum_{(24m)^2\equiv v \pmod k}\cos\frac{4\pi m}{k}, \tag{5.3}$$

where m runs through integers (mod k) *satisfying the summation condition.*

Specializing to the case when k is a power of a prime we may prove the following result due to Lehmer [3, Theorem 5].

COROLLARY 1. *If $k=p^\lambda$ and $v=1-24n$, where p is a prime greater than 3, then*

$$A_k(n)=\begin{cases} 0 & (v \text{ a nonresidue of } k \text{ and prime to } k),\\ 2(3|k)k^{1/2}\cos(4\pi m/k) & (v\equiv(24m)^2 \pmod k \text{ and prime to } k),\\ (3|k)k^{1/2} & (v\equiv 0 \pmod p \text{ and } \lambda=1),\\ 0 & (v\equiv 0 \pmod p \text{ and } \lambda>1). \end{cases} \tag{5.4}$$

Proof. By the condition in the first part of (5.4) we mean that no solution exists of the congruence $x^2\equiv v \pmod k$. The sum in (5.3) is therefore vacuous, and the result in (5.4) follows at once. The second result in (5.4) also follows immediately from (5.3) and the fact that in this case the congruence $(24m)^2\equiv v \pmod k$ has exactly two solutions. To prove the third part of the corollary we note that the congruence $(24m)^2\equiv 0 \pmod p$ has the unique solution $m\equiv 0 \pmod p$. The result in (5.3) now reduces immediately to the result in (5.4). Finally we consider the proof of the last result of the corollary. When $v\equiv 0 \pmod p$ and $\lambda>1$ we first seek the solutions of the congruence $x^2\equiv v \pmod k$. Put $v=p^\mu b$, where $0<\mu<\lambda$ and $b\not\equiv 0 \pmod p$. In order that solutions of the given congruence exist it is necessary and sufficient that μ be even, and b be a quadratic residue of p. Each solution x may then be written in the form $x=p^{\mu/2}c$, where $c^2\equiv b \pmod{p^{\lambda-\mu}}$. For any such solution x we now solve the congruence $24m\equiv x \pmod{k}$ for a unique value of m. Then the numbers $m+jp^{\lambda-\mu/2}$, $0\leqq j<p^{\mu/2}$ are incongruent solutions $(\operatorname{mod} k)$ of the congruence $(24m)^2\equiv v \pmod{k}$. The contribution of these numbers to the sum in (5.3) is given by

$$\cos\frac{4\pi m}{k}\sum_{j=0}^{p^{\frac{\mu}{2}}-1}\cos\frac{4\pi j}{p^{\mu/2}}-\sin\frac{4\pi m}{k}\sum_{j=0}^{p^{\frac{\mu}{2}}-1}\sin\frac{4\pi j}{p^{\mu/2}}\,,$$

and both of the last two sums equal zero. This completes the proof of the corollary in all cases.

Case 2. *k odd and divisible by* 3. Let m run over the solutions of the congruence $(8m)^2\equiv v \pmod{3k}$. With each pair of solutions m, $3k-m$ we associate the unique solution l of the congruence $6l+1\equiv\pm 8m$ (mod $3k$), $0\leqq l<k$, where the coefficient of $8m$ is selected to be $+1$ or -1 according as $m\equiv -1$ or $+1 \pmod{3}$. Then each l determined in this manner satisfies the congruence $(6l+1)^2\equiv v \pmod{24k}$, $0\leqq l<k$. On the other hand each l satisfying the last congruence determines a pair of solutions m, $3k-m$ of the first congruence. It follows that l runs twice over integers satisfying the summation condition in (5.1). Consider next a pair of solutions m, $3k-m$ for which $m\equiv -1 \pmod{3}$. Then the corresponding l satisfies the equation $8m=6l+1+3jk$ for some integer j. The summand in (5.1) may now be written in the form $(-1)^l\cos[(j\pi)/2-(4\pi m)/3k]$. If l is even, then $j\equiv k \pmod{4}$; if l is odd, then $j\equiv -k$ (mod 4). Since $(m|3)=-1$ the summand under consideration reduces to $-(-1|k)(m/3)\sin(4\pi m/3k)$. We may show similarly that we get the same result if the pair m, $3k-m$ is such that $m\equiv 1 \pmod{3}$. Accordingly we may state the following theorem.

THEOREM 2. *If k is odd and divisible by* 3, *then*

$$A_k(n)=-\left(\frac{-1}{k}\right)\left(\frac{k}{3}\right)^{1/2}\sum_{(8m)^2\equiv v\ (\operatorname{mod} 3k)}\left(\frac{m}{3}\right)\sin\frac{4\pi m}{3k}\,,\tag{5.5}$$

where m runs through integers (mod $3k$) *satisfying the summation condition.*

When $k=3^\lambda$ the congruence $(8m)^2\equiv v \pmod{3k}$ has precisely two solutions. Therefore an immediate consequence of Theorem 2 is the following corollary [3, Theorem 6].

COROLLARY 2. *If $k=3^\lambda$, then*

$$A_k(n)=2(-1)^{\lambda+1}(m|3)(k/3)^{1/2}\sin(4\pi m/3k)\,,$$

where m is an integer such that $(8m)^2\equiv 1-24n \pmod{3k}$.

We now return to the sum (1.4) in the case when k is even. In this case $A_k(n)$ may be written in the form

$$A_k(n)=\frac{1}{2}\left(\frac{k}{3}\right)^{1/2}\sum_{(6l+1)^2\equiv v\ (\mathrm{mod}\ 24k)}(-1)^l\cos\frac{6l+1}{6k}\pi\ , \tag{5.6}$$

where now l runs over integers in the range $0\leqq l<4k$ which satisfy the summation condition.

Case 3. *k even and not divisible by* 3. The congruence $6l+1\equiv 3m\ (\mathrm{mod}\ 8k)$ establishes a one-to-one correspondence between integers l, $0\leqq l<4k$, and odd integers m, $0\leqq m<8k$. For any such l which satisfies the congruence $(6l+1)^2\equiv v\ (\mathrm{mod}\ 24k)$, the corresponding m satisfies the congruence $(3m)^2\equiv v\ (\mathrm{mod}\ 8k)$. Conversely, to distinct solutions of the second congruence correspond distinct solutions of the first. We put also

$$6l'+1\equiv -3m\ (\mathrm{mod}\ 8k)\ , \qquad 0\leqq l'<4k.$$

Thus if $k\equiv 1\ (\mathrm{mod}\ 3)$, then $l'=(4k-1)/3-l$ when $0\leqq l\leqq(4k-1)/3$ and $l'=(16k-1)/3-l$ if $(4k-1)/3<l<4k$. But if $k\equiv -1\ (\mathrm{mod}\ 3)$, then $l'=(8k-1)/3-l$ when $0\leqq l\leqq(8k-1)/3$ and $l'=(20k-1)/3-l$ when $(8k-1)/3<l'<4k$. In the sum (5.6) we now pair off each l with the corresponding l'. We note that in any event $l+l'$ is odd, and we employ the identity

$$\cos\frac{6l+1}{6k}\pi-\cos\frac{6l'+1}{6k}\pi=-2\sin\frac{3(l+l')+1}{6k}\pi\sin\frac{l-l'}{2k}\pi\ . \tag{5.7}$$

If $k\equiv 1\ (\mathrm{mod}\ 3)$, then $3(l+l')+1=4k$ or $16k$; if $k\equiv -1\ (\mathrm{mod}\ 3)$, then $3(l+l')+1=8k$ or $20k$. The first sine factor in the right member of (5.7) is therefore $\pm\sqrt{3}/2$ according as $k\equiv\pm 1\ (\mathrm{mod}\ 3)$. From the congruence $l-l'\equiv m\ (\mathrm{mod}\ 4k)$ it follows that the second sine factor in (5.7) is equal to $\sin(4\pi m/8k)$. Also the congruence $6l+1\equiv 3m\ (\mathrm{mod}\ 8k)$ implies that l is odd or even according as $m\equiv\pm 1\ (\mathrm{mod}\ 4)$. Hence we have the equation $-(-1)^l=(-1|m)$. Our results may be combined in the following theorem:

THEOREM 3. *If k is even and not divisible by* 3, *then*

$$A_k(n)=\frac{1}{4}\left(\frac{k}{3}\right)k^{1/2}\sum_{(3m)^2\equiv v\ (\mathrm{mod}\ 8k)}\left(\frac{-1}{m}\right)\sin\frac{4\pi m}{8k}\ , \tag{5.8}$$

where m runs through integers $(\mathrm{mod}\ 8k)$ *satisfying the summation condition.*

If $k=2^\lambda$ the congruence $(3m)^2\equiv v\ (\mathrm{mod}\ 8k)$ has exactly four roots. If m is one such root, then the four roots are given by $\pm m$ and $\pm m+4k$. We may therefore state the following corollary [3, Theorem 7] of Theorem 3.

COROLLARY 3. *If* $k=2^\lambda$, $\lambda \geqq 0$, *then*

$$A_k(n)=(-1)^\lambda\left(\frac{-1}{m}\right)k^{1/2}\sin(4\pi m/8k),$$

where m *is an integer such that* $(3m)^2\equiv 1-24n \pmod{8k}$.

Case 4. *k even and divisible by* 3. Let m run over the roots of the congruence $m^2\equiv v \pmod{24k}$. Each such m determines a unique solution l of the congruence $6l+1\equiv \pm m \pmod{24k}$, $0\leqq l<4k$, where the coefficient of m is ± 1 according as $m\equiv \pm 1 \pmod 6$. The numbers l obtained in this way are solutions of the congruence $(6l+1)^2\equiv v \pmod{24k}$, $0\leqq l<4k$. Conversely each solution l of the last congruence determines a pair of solutions m, $24k-m$ of the first congruence. As a result the numbers l run twice over the integers which satisfy the summation condition in (5.6). Suppose first that a solution m is such that $m\equiv 1 \pmod 6$. Then the equation $6l+1=m+24jk$ (for some integer j) implies that l is even or odd according as $m\equiv 1$ or $7 \pmod{12}$. Consequently we have $(-1)^l=(3|m)$. The summand in (5.6) may now be written in the form $(3|m)\cos(4\pi m/24k)$. In a similar manner we may derive the last result when $m\equiv -1 \pmod 6$. Thus we have established the following theorem:

THEOREM 4. *If k is even and divisible by* 3, *then*

$$A_k(n)=\frac{1}{4}\left(\frac{k}{3}\right)^{1/2}\sum_{m^2\equiv v \pmod{24k}}\left(\frac{3}{m}\right)\cos\frac{4\pi m}{24k}, \tag{5.9}$$

where m runs through integers $\pmod{24k}$ *satisfying the summation condition.*

6. Factorization of the $A_k(n)$. The theorems of the preceding section open a new approach to the factorization of the $A_k(n)$. Alternative approaches have previously been given by Lehmer [3] and Rademacher and Whiteman [6]. In what follows we shall derive three theorems for expressing $A_k(n)$ as a product of two A's whose subscripts are relatively prime integers whose product is k. It should be pointed out that our theorems and Lehmer's theorems overlap to a certain extent. Lehmer's Theorem 1 is included in our Theorem 5. His Theorem 2 follows from our Theorems 5 and 6. His Theorem 4 is equivalent to our Theorem 7.

THEOREM 5. *If* $k=k_1k_2$, $(k_1,k_2)=1$, *and if furthermore* $8|k$ *in case k is even, then*

$$A_k(n)=A_{k_1}(n_1)A_{k_2}(n_2), \tag{6.1}$$

where n_1 *and* n_2 *are determined by the congruences*

$$(6.2)\qquad \begin{aligned} k_2^2 d_2 e n_1 &\equiv d_2 e n + (k_2^2-1)/d_1 \pmod{k_1}\ , \\ k_1^2 d_1 e n_2 &\equiv d_1 e n + (k_1^2-1)/d_2 \pmod{k_2}\ , \end{aligned}$$

respectively, and where d_1, d_2, e *are defined by*

$$(6.3)\qquad d_1=(24, k_1),\ d_2=(24, k_2),\ 24=d_1d_2e\ .$$

Proof. The assumption $8|k$ when k is even enables us to write the summation conditions of Theorems 1, 2, 3 and 4 in the general form

$$(6.4)\qquad (24m/d)^2 \equiv v \pmod{dk}\ ,$$

where $d=(24, k)$. Let n_1, n_2 be two integers to be determined explicitly later on. We wish to establish the equation (6.1) where, for brevity, we write $A_k(n)=\sum_m$, $A_{k_1}(n_1)=\sum_{m_1}$, $A_{k_2}(n_2)=\sum_{m_2}$. The summation indices m_1, m_2 run over the solutions of the two congruences

$$(6.5)\qquad \begin{aligned} (24m_1/d_1)^2 &\equiv v_1 \pmod{d_1k_1}\ , \\ (24m_2/d_2)^2 &\equiv v_2 \pmod{d_2k_2}\ , \end{aligned}$$

respectively, where $v_1=1-24n_1$, $v_2=1-24n_2$, and d_1, d_2 are defined in (6.3). We note also that $d=d_1d_2$. For each pair of summation indices m_1, m_2 we now define numbers m, m' by means of the congruences

$$(6.6)\qquad \begin{aligned} m\ &\equiv d_1k_1m_2 + d_2k_2m_1 \pmod{d_1d_2k}\ , \\ m' &\equiv d_1k_1m_2 - d_2k_2m_1 \pmod{d_1d_2k}\ . \end{aligned}$$

Our object is to select v_1, v_2 in (6.5) so that m or m' runs over the solutions of the congruence (6.4). It is clear that (6.4) has no solutions if there exists an odd prime factor p of dk for which $(v|p)=-1$. Otherwise it follows from a well-konwn result [2, vol. 1, Satz 88] that if s denotes the number of odd prime divisors of dk, then the number of solutions of (6.4) is 2^s when k is odd and 2^{s+2} when k is even. Substituting from (6.6) into (6.4) and applying (6.5) we get

$$(6.7)\qquad (24m/d)^2 \equiv (24m'/d)^2 \equiv k_1^2v_2 + k_2^2v_1 \pmod{dk}\ .$$

In order to make (6.7) equivalent to (6.4) we need to select v_1, v_2 so that the congruence $v \equiv k_1^2v_2 + k_2^2v_1 \pmod{d_1d_2k}$ is satisfied. For this purpose we define v_1, v_2 by means of the pair of congruences

$$(6.8)\qquad \begin{aligned} k_2^2v_1 &\equiv v \pmod{d_1k_1}\ , \\ k_1^2v_2 &\equiv v \pmod{d_2k_2}\ . \end{aligned}$$

With this choice of v_1, v_2 we see that the number of solutions of (6.4) is the product of the number of solutions of the first congruence in (6.5) multiplied by the number of solutions of the second. Moreover this number is precisely the number of incongruent integers m or m' defined by (6.6).

The pair of congruences (6.8) is equivalent to the pair of congruences (6.2) in the hypothesis of Theorem 5. In order to prove (6.1) we find it convenient to divide the discussion into the following five cases. Case 1. $d_1=d_2=1$. Case 2. $d_1=1$, $d_2=3$. Case 3. $d_1=1$, $d_2=8$. Case 4. $d_1=3$, $d_2=8$. Case 5. $d_1=1$, $d_2=24$. The argument proceeds along the same lines in each of these cases. To illustrate the method we give the proof in Case 4. In this case the value of $A_{k_1}(n_1)$ is given by Theorem 2, and the value of $A_{k_2}(n_2)$ is given by Theorem 3. By (5.5) and (5.8) the product $A_{k_1}(n_1)A_{k_2}(n_2)$ may be put in the form

$$A_{k_1}(n_1)A_{k_2}(n_2) = -\frac{1}{4}\left(\frac{-1}{k_1}\right)\left(\frac{k_2}{3}\right)\left(\frac{k_1k_2}{3}\right)^{1/2} \sum_{m_1,m_2} \left(\frac{m_1}{3}\right)\left(\frac{-1}{m_2}\right) \sin\frac{4\pi m_1}{3k_1} \sin\frac{4\pi m_2}{8k_2}, \tag{6.9}$$

where the respective ranges of m_1 and m_2 are given by the solutions of the congruences $(8m_1)^2 \equiv v_1 \pmod{3k_1}$ and $(3m_2)^2 \equiv v_2 \pmod{8k_2}$. On the other hand the value of $A_k(n)$ is given by Theorem 4. In the sum (5.9) we now pair off each $m \equiv 3k_1m_2+8k_2m_1 \pmod{24k}$ as defined in (6.6) with the corresponding $m' \equiv 3k_1m_2-8k_2m_1 \pmod{24k}$. Since $(3|m)=(-1|3k_1m_2)(8k_2m_1|3)$ and $(3|m')=(-1|3k_1m_2)(-8k_2m_1|3)$ it follows that $(3|m)(3|m')=-1$. Hence we get

$$A_k(n)=\frac{1}{8}\left(\frac{k}{3}\right)^{1/2} \sum_m \left(\frac{3}{m}\right)\left(\cos\frac{4\pi m}{24k} - \cos\frac{4\pi m'}{24k}\right), \tag{6.10}$$

where m runs over the incongruent solutions of the congruence $m^2 \equiv v \pmod{24k}$. To complete the proof we show that every term of (6.9) is equal to the corresponding term of (6.10). This follows at once from the trigonometric identity

$$\cos\frac{4\pi m}{24k} - \cos\frac{4\pi m'}{24k} = -2\sin\frac{4\pi m_1}{3k_1}\sin\frac{4\pi m_2}{8k_2} \tag{6.11}$$

and the number theoretic identity $(3|m)=(-1|k_1)(k_2|3)(m_1|3)(-1|m_2)$. The remainder of the proof may be completed in a similar fashion.

The preceding theorem enables us to decompose $A_k(n)$ for composite k if k is odd or divisible by 2^3. We now consider the cases in which k is even but is not divisible by 2^3.

THEOREM 6. *If $k=4k_1$ with k_1 odd, then*

$$A_k(n) = -A_{k_1}(n_1)A_4(n_2)\ , \tag{6.12}$$

where n_1 and n_2 are determined by the congruences

$$\begin{aligned} 128n_1 &\equiv 8n+5 \pmod{k_1}\ , \\ k_1^2 n_2 &\equiv n-2-(k_1^2-1)/8 \pmod 4\ , \end{aligned} \tag{6.13}$$

respectively.

Proof. Since k is divisible by 4 but not by 8 the summation conditions of Theorems 3 and 4 may now be written in the general form

$$(24m/\delta)^2 \equiv v \pmod{\delta k}\ , \tag{6.14}$$

where δ is defined by the equation $\delta=(2k, 24)$. Proceeding as in the proof of Theorem 5 we have in place of (6.5) the pair of congruences

$$\begin{aligned} (24m_1/d_1)^2 &\equiv v_1 \pmod{d_1 k_1}\ , \\ (3m_2)^2 &\equiv v_2 \pmod{8k_2}\ , \end{aligned} \tag{6.15}$$

respectively, where d_1 is defined by (6.3) as before, and where we now put $k_2=4$. Unlike the situation in the proof of Theorem 5 the analogue of the pair of congruences (6.6) does not here lead to the analogue of congruence (6.7). Accordingly we modify our former argument as follows. For each pair of summation indices m_1, m_2 we define numbers m, m' by means of the congruences

$$\begin{aligned} m &\equiv d_1k_1(m_2+2k_2)+8k_2m_1 \pmod{\delta k}\ , \\ m' &\equiv d_1k_1(m_2+2k_2)-8k_2m_1 \pmod{\delta k}\ . \end{aligned} \tag{6.16}$$

Then we may verify that $(24m/\delta)^2 \equiv (24m'/\delta)^2 \equiv k_1^2 v_2 + k_2^2 v_1 \pmod{\delta k}$. In order to make this congruence equivalent to the congruence (6.14) we now define v_1, v_2 by means of the pair of congruences

$$\begin{aligned} k_2^2 v_1 &\equiv v \pmod{d_1k_1}\ , \\ k_1^2 v_2 + k_2^2 &\equiv v \pmod{8k_2}\ . \end{aligned} \tag{6.17}$$

Exactly as in the proof of Theorem 5 it follows that the numbers m or m' defined in (6.16) run through the entire set of incongruent solutions of (6.14). Moreover the number of solutions of (6.14) is the product of the numbers of solutions of the two congruences in (6.15).

The pair of congruences (6.17) is equivalent to the pair of congruences (6.13) in the hypothesis of Theorem 6. In order to prove (6.12) we need to consider the two cases $d_1=1$ and $d_1=3$. We now indicate the proof in the case $d_1=3$. The argument is step by step similar to the argument given in the proof of Case 4 of Theorem 5. It is necessary, however, to replace the factor $\sin(4\pi m_2/8k_2)$ in the right member of (6.11) by the factor $\sin(\pi+4\pi m_2/8k_2)$. This change accounts for the presence of the minus sign in the factorization formula (6.12). This completes the proof of Theorem 6. We conclude with the following theorem.

THEOREM 7. *If $k=2k_1$ with k_1 odd, then*

$$A_k(n)=A_{k_1}(n_1)A_2(n_2)\ , \tag{6.18}$$

where n_1 and n_2 are the respective solutions of the congruences

$$\begin{aligned} 32n_1 &\equiv 8n+1 \pmod{k_1}\ , \\ n_2 &\equiv n-(k_1^2-1)/8 \pmod 2\ . \end{aligned} \tag{6.19}$$

Proof. Since the proof of this theorem is very much like the proof of Theorem 5, it will suffice to sketch it briefly. The summation conditions in Theorems 3 and 4 are now expressed by the congruence $(24m/D)^2\equiv v \pmod{Dk}$, where $D=(4k,24)$. The second congruence in (6.5) is replaced by $(3m_2)^2\equiv v_2 \pmod{8k_2}$, where this time we take $k_2=2$. The pair of congruences (6.6) is replaced by the pair $m\equiv d_1k_1m_2+8k_2m_1 \pmod{Dk}$, $m'\equiv d_1k_1m_2-8k_2m_1 \pmod{Dk}$. These two congruences, in turn, lead to the congruence $(24m/D)^2\equiv(24m'/D)^2\equiv k_2^2v_1+k_1^2(v_2-4) \pmod{Dk}$. In order to reduce the right member of the last congruence to $v \pmod{Dk}$ it suffices to define v_1, v_2 by means of the pair of congruences

$$\begin{aligned} k_2^2v_1 &\equiv v \pmod{d_1k_1}\ , \\ k_1^2v_2 &\equiv v \pmod{8k_2}\ . \end{aligned} \tag{6.20}$$

Finally the two congruences (6.20) are equivalent respectively to the two congruences (6.19) in the hypothesis of the theorem. It is convenient to treat separately the two cases $d_1=1$, $d_1=3$. Then the rest of the proof goes through without difficulty.

REFERENCES

1. W. Fischer, *On Dedekind's function $\eta(\tau)$*, Pacific J. Math., **1** (1951), 82–95.
2. E. Landau, *Vorlesungen über Zahlentheorie*, S. Hirzel, Leipzig, 1927.
3. D. H. Lehmer, *On the series for the partition function*, Trans. Amer. Math., Soc., **43** (1938), 271–295.
4. T. Nagell, *Introduction to number theory*, John Wiley and Sons, New York, 1951.

5. H. Rademacher, *On the partition function* $p(n)$, Proc. London Math. Soc. (2), **43** (1937), 241–254.
6. H. Rademacher and A. L. Whiteman, *Theorems on Dedekind sums*, Amer. J. Math., **63** (1941), 377–407.
7. A. L. Whiteman, *A sum connected with the partition function,* Bull. Amer. Math. Soc., **53** (1947), 598–603.

THE INSTITUTE FOR ADVANCED STUDY AND
UNIVERSITY OF SOUTHERN CALIFORNIA