

ON THE SERIES FOR THE PARTITION FUNCTION*

BY
D. H. LEHMER

1. **Introduction.** In 1917 Hardy and Ramanujan† gave the following asymptotic formula for the number $p(n)$ of partitions of n ,

$$(1.1) \quad p(n) = \frac{1}{\pi 8^{1/2}} \sum_{k=1}^{[\alpha n^{1/2}]} A_k(n) k^{1/2} \frac{d}{dn} \left(\frac{e^{c\lambda_1/k}}{\lambda_n} \right) + O(n^{-1/4}),$$

where

$$c = \pi(2/3)^{1/2}, \quad \lambda_n = (n - 1/24)^{1/2}, \quad \alpha > 0,$$

and the coefficients $A_k(n)$ are defined by

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

and in general

$$(1.2) \quad A_k(n) = \sum_{(\rho)} \omega_{\rho,k} e^{-2n\rho\pi i/k},$$

where ρ ranges over those numbers which are less than k and prime to k . Here $\omega_{\rho,k}$ are certain $24k$ th roots of unity which arise in the theory of modular functions and are defined by (1.4) and (1.5).

Without knowledge of the behavior of $A_k(n)$ for large values of k other than the obvious fact that

$$(1.3) \quad A_k(n) = O(k)$$

Hardy and Ramanujan were unable to decide several questions about (1.1). For instance, if α is given, (1.1) gives $p(n)$ to within half a unit for all sufficiently large n . Just how large n must be was not discovered. Whether (1.1) would converge if extended to infinity and what is the least number of terms that need be taken were other questions depending on the magnitude of $A_k(n)$.

Quite recently Rademacher‡ has shown that if in (1.1) we replace e^x by $2 \sinh x$ we obtain an infinite series for $p(n)$ (with $\alpha = \infty$) whose convergence follows easily from (1.3). This striking result enables one to estimate the

* Presented to the Society, March 27, 1937; received by the editors March 11, 1937.

† Proceedings of the London Mathematical Society, (2), vol. 17, pp. 75-115.

‡ Proceedings of the London Mathematical Society, (2), vol. 43, pp. 241-254.

difference between $p(n)$ and the first N terms of the series of Hardy and Ramanujan. This estimate, of course, depends on $A_k(n)$ so that information about the general behavior of $A_k(n)$ for large as well as small values of k is important in this connection.

Apart from these questions there is the problem of actually using (1.1) to determine isolated values of $p(n)$ for n large. The task of evaluating $A_k(n)$ from its definition is quite formidable when k is large. Hardy and Ramanujan gave $A_k(n)$ for $k \leq 18$ as sums of cosines, while the actual values of $A_k(n)$ for $k \leq 20$ and all n have been tabulated recently.* The apparent intricacy of $A_k(n)$ would seem definitely to restrict the usefulness of (1.1).

It would therefore seem desirable to make an intensive study of $A_k(n)$. In a recent paper† we have proved that the series (1.1) would diverge if extended to infinity. This result was obtained from a simple estimate of $A_k(n)$, where k is a square of a prime. In this paper we give formulas of $A_k(n)$ as a single term thus eliminating the necessity of any sort of tables of $A_k(n)$. This result enables us to give close estimates for $A_k(n)$, and to answer the questions mentioned above, and makes feasible the application of (1.1) to any number of terms.

The method employed in the present paper depends in part on showing that $A_k(n)$ may be transformed into "generalized Kloosterman sums." These in turn may be evaluated by a slight extension of the results of Salié.‡ The results of this paper were first obtained independently of Kloosterman sums. Considerable space is saved, however, by referring to results already published. Section 2 is devoted to multiplication theorems for $A_k(n)$ which reduce the evaluation of $A_k(n)$ to the case in which k is a prime or a power of a prime.§ In §3 these evaluations are carried out. The final section applies the results of the preceding sections to the Hardy-Ramanujan and Rademacher series.

The quantities $\omega_{\rho,k}$ appearing in the definition (1.2) of $A_k(n)$ are given by

$$(1.4) \quad \omega_{\rho,k} = \left(\frac{-\rho}{k}\right) \exp \left[- \left\{ \frac{1}{4}(k-1) + \frac{1}{12} \left(k - \frac{1}{k} \right) (2\rho + \bar{\rho} - \rho^2 \bar{\rho}) \right\} \pi i \right]$$

if k is odd, and by

* Journal of the London Mathematical Society, vol. 11 (1936), pp. 117-118. Erratum: for $A_{20}(n)$ read $A_{20}(n+5)$.

† Journal of the London Mathematical Society, vol. 12, pp. 171-176.

‡ Mathematisches Zeitschrift, vol. 34 (1931), pp. 91-109.

§ This multiplicative property, discovered empirically, could have been anticipated eight years ago from a result of Estermann: Hamburger Abhandlungen, vol. 7 (1929), p. 91.

$$(1.5) \quad \omega_{\rho, k} = \left(\frac{-k}{\rho} \right) \exp \left[- \left\{ \frac{1}{4} (2 - k\rho - \rho) + \frac{1}{12} \left(k - \frac{1}{k} \right) (2\rho + \bar{\rho} - \rho^2 \bar{\rho}) \right\} \pi i \right]$$

when k is even. Here (a/b) is the symbol of Jacobi and $\rho \bar{\rho} \equiv 1 \pmod{k}$.

If we substitute $\exp \left[\left\{ 1 - (a/b) \right\} (\pi i/2) \right]$ for the symbol (a/b) in (1.4) and (1.5), we obtain after a few simple reductions the following expressions for $A_k(n)$:

$$(1.6) \quad A_k(n) = \sum_{(\rho)} \exp \left[f_n(\rho) \frac{\pi i}{12k} \right] \quad (k \text{ odd}),$$

$$(1.7) \quad A_k(n) = \sum_{(\rho)} \exp \left[g_n(\rho) \frac{\pi i}{12k} \right] \quad (k \text{ even}),$$

where ρ ranges over a complete system of residues prime to k and where the functions f and g are given by

$$(1.8) \quad f_n(\rho) = f_n(\rho, k) = - \left\{ 24n\rho + 6k \left(\frac{-\rho}{k} \right) + 3k(k-3) + (k^2-1)(2\rho + \bar{\rho} - \rho^2 \bar{\rho}) \right\},$$

$$(1.9) \quad g_n(\rho) = g_n(\rho, k) = - \left\{ 24n\rho + 6k \left(\frac{-k}{\rho} \right) - \rho(k+1)(k+2) - (k^2-1)(\rho^2-1)\bar{\rho} \right\}.$$

The number $1 - 24n$ plays the dominant role in what follows and is abbreviated by writing

$$(1.10) \quad \nu = 1 - 24n.$$

From (1.6) and (1.7) it is seen that $f(\rho)$ and $g(\rho)$ need only be determined modulo $24k$. The following fundamental congruences are used many times in the sequel and are set forth here for reference. If k is odd

$$(1.11) \quad f_n(\rho) \equiv \nu\rho + \bar{\rho} \pmod{k \text{ or } 3k}^*$$

according as 3 is prime to k or not.

$$(1.12) \quad f_n(\rho) \equiv 0 \pmod{3}$$

if k is prime to 3.

$$(1.13) \quad f_n(\rho) \equiv 2k \left(\frac{-\rho}{k} \right) + k - 3 \pmod{8}.$$

If $k = 2^\lambda k_1$ where k_1 is odd,

$$(1.14) \quad g_n(\rho) \equiv \nu\rho + \bar{\rho} \pmod{k_1 \text{ or } 3k_1}^*$$

* In these congruences $\bar{\rho}$ stands for $1/\rho \pmod{M}$ where M is the modulus of the congruence.

according as k_1 is prime to 3 or not. If k_1 is prime to 3

$$(1.15) \quad g_n(\rho) \equiv 0 \pmod{3}.$$

For every k_1

$$(1.16) \quad g_n(\rho) \equiv \nu\rho + \bar{p} + 2k\left(\frac{-k}{\rho}\right) + k(k+3)\rho \pmod{2^{\lambda+3}}.*$$

2. Multiplication theorems. We shall derive three theorems for expressing $A_k(n)$ as a product of two A 's whose subscripts are coprime integers whose product is k . This enables us to evaluate $A_k(n)$ for all k when the values of A_q are known, where q runs over all powers of primes.

THEOREM 1. *If k_1 and k_2 are odd coprime integers, then*

$$(2.1) \quad A_{k_1}(n_1)A_{k_2}(n_2) = A_{k_1k_2}(n_3),$$

where $n_3 \equiv k_1^2 n_2 + k_2^2 n_1 - (k_1^2 + k_2^2 - 1)/24 \pmod{k_1k_2}$.

Remark. In case k_1 or k_2 is a multiple of 3, the numerator of the fraction $(k_1^2 + k_2^2 - 1)/24$ is also a multiple of 3 and the fraction becomes of the form $M/8$. In any case, then, the quantity n_3 may be replaced by an integer modulo k_1k_2 .

Proof. We consider first the product

$$(2.2) \quad A_{k_1}(n_1)A_{k_2}(n_2) = \sum_{(\rho_1)} \sum_{(\rho_2)} \exp \left[\{ k_2 f_{n_1}(\rho_1, k_1) + k_1 f_{n_2}(\rho_2, k_2) \} \frac{\pi i}{12k_1k_2} \right],$$

where ρ_1 and ρ_2 range over the numbers less than and prime to k_1 and k_2 respectively. For each value of these summation indices we define ρ_3 by the system of congruences

$$(2.3) \quad \rho_3 \equiv \rho_1/k_2 \pmod{k_1},$$

$$(2.4) \quad \rho_3 \equiv \rho_2/k_1 \pmod{k_2}.$$

It is clear that as ρ_1 and ρ_2 range over their respective values the numbers ρ_3 modulo k_1k_2 run over the numbers $< k_1k_2$ and prime to k_1k_2 so that

$$(2.5) \quad A_{k_1k_2}(n_3) = \sum_{(\rho_3)} \exp \left[f_{n_3}(\rho_3, k_1k_2) \frac{\pi i}{12k_1k_2} \right].$$

We show that every term of (2.2) is equal to the corresponding term of (2.5), where the correspondence is determined by (2.3) and (2.4) and n_3 is defined by (2.1). This amounts to showing that

* See footnote on p. 273.

$$(2.6) \quad D_1 = f_{n_1}(\rho_3, k_1 k_2) - \{k_2 f_{n_1}(\rho_1, k_1) + k_1 f_{n_1}(\rho_2, k_2)\} \equiv 0 \pmod{24k_1 k_2}.$$

In the first place if neither k_1 nor k_2 is divisible by 3, then it follows from (1.12) that

$$D_1 \equiv 0 \pmod{3}.$$

On the other hand we may suppose from symmetry that k_2 is divisible by 3 if not both k_1 and k_2 are prime to 3. Therefore let $k = 3k_2$ or k_2 according as 3 does or does not divide $k_1 k_2$. Our task is then to show that

$$D_1 \equiv 0 \pmod{8kk_1}.$$

We consider first the modulus k_1 . By (1.11) we have

$$D_1 \equiv \nu_3 \rho_3 + \bar{\rho}_3 - k_2(\nu_1 \rho_1 + \bar{\rho}_1) \pmod{k_1},$$

where

$$(2.7) \quad \nu_3 = 1 - 24n_3 = k_2^2 \nu_1 + k_1^2 \nu_2.$$

Hence in view of (2.3) we have

$$\nu_3 \rho_3 + \bar{\rho}_3 \equiv k_2 \nu_1 \rho_1 + k_2 \bar{\rho}_1 \pmod{k_1},$$

so that

$$D_1 \equiv 0 \pmod{k_1}.$$

If $k = k_2$, the same argument shows that $D_1 \equiv 0 \pmod{k}$. In case $k = 3k_2$ we note that $f_{n_1}(\rho_1, k_1) \equiv 0 \pmod{3}$ so that

$$D_1 \equiv f_{n_1}(\rho_3, k_1 k_2) - k_1 f_{n_1}(\rho_2, k_2) \equiv \nu_3 \rho_3 + \bar{\rho}_3 - k_1(\nu_2 \rho_2 + \bar{\rho}_2) \pmod{k},$$

but from (2.7) $\nu_3 \equiv k_1^2 \nu_2 \pmod{k}$, so that

$$D_1 \equiv k_1(k_1 \rho_3 - \rho_2) \left(\nu_2 - \frac{1}{k_1 \rho_2 \rho_3} \right) \pmod{k}.$$

By (2.4) the second factor is a multiple of k_2 while the third factor is a multiple of 3 since $\nu_2 \equiv 1 \pmod{3}$, and $k_1 \rho_2 \rho_3 \equiv \rho_2^2 \pmod{k_2}$ so that $k_1 \rho_2 \rho_3 \equiv 1 \pmod{3}$. Hence

$$D_1 \equiv 0 \pmod{kk_1}.$$

There remains to show that $D_1 \equiv 0 \pmod{8}$. By (1.13) we have

$$(2.8) \quad \begin{aligned} D_1 &\equiv 2k_1 k_2 \left(\frac{-\rho_3}{k_1 k_2} \right) + k_1 k_2 - 3 \\ &\quad - \left\{ 2k_1 k_2 \left[\left(\frac{-\rho_1}{k_1} \right) + \left(\frac{-\rho_2}{k_2} \right) \right] + 2k_1 k_2 - 3k_1 - 3k_2 \right\} \pmod{8}, \end{aligned}$$

while, by (2.3) and (2.4),

$$(2.9) \quad \begin{aligned} \left(\frac{-\rho_3}{k_1 k_2}\right) &= \left(\frac{-\rho_3}{k_1}\right) \left(\frac{-\rho_3}{k_2}\right) = \left(\frac{-\rho_1}{k_1}\right) \left(\frac{k_2}{k_1}\right) \left(\frac{-\rho_2}{k_2}\right) \left(\frac{k_1}{k_2}\right) \\ &= \left(\frac{-\rho_1}{k_1}\right) \left(\frac{-\rho_2}{k_2}\right) (-1)^{(k_1-1)(k_2-1)/4}. \end{aligned}$$

We now separate two cases according as k_1 and k_2 are both of the form $4x-1$ or not. In the affirmative case we have

$$\left(\frac{-\rho_3}{k_1 k_2}\right) = - \left(\frac{\rho_1}{k_1}\right) \left(\frac{\rho_2}{k_2}\right), \text{ and } k_1 k_2 \equiv 1 \pmod{4},$$

so that (2.8) becomes

$$\begin{aligned} D_1 &\equiv 2 \left\{ -1 + \left(\frac{\rho_1}{k_1}\right) + \left(\frac{\rho_2}{k_2}\right) - \left(\frac{\rho_1}{k_1}\right) \left(\frac{\rho_2}{k_2}\right) \right\} + (k_1 + 3)(k_2 + 3) + 4 \\ &\equiv -2 \left\{ 1 - \left(\frac{\rho_1}{k_1}\right) \right\} \left\{ 1 - \left(\frac{\rho_2}{k_2}\right) \right\} + 4 + 4 \equiv 0 \pmod{8}. \end{aligned}$$

In case not both k_1 and k_2 are of the form $4x-1$ we have from (2.9)

$$\left(\frac{\rho_3}{k_1 k_2}\right) = \left(\frac{-\rho_1}{k_1}\right) \left(\frac{-\rho_2}{k_2}\right)$$

and

$$\begin{aligned} D_1 &\equiv 2k_1 k_2 \left\{ -1 - \left(\frac{-\rho_1}{k_1}\right) - \left(\frac{-\rho_2}{k_2}\right) + \left(\frac{-\rho_1}{k_1}\right) \left(\frac{-\rho_2}{k_2}\right) + 2 \right\} \\ &\quad - 4k_1 k_2 + (k_1 + 3)(k_2 + 3) + 4 \\ &\equiv 2k_1 k_2 \left\{ 1 - \left(\frac{-\rho_1}{k_1}\right) \right\} \left\{ 1 - \left(\frac{-\rho_2}{k_2}\right) \right\} \\ &\quad - 4(k_1 k_2 - 1) + (k_1 + 3)(k_2 + 3) \equiv (k_1 + 3)(k_2 + 3) \\ &\equiv 0 \pmod{8}, \end{aligned}$$

since at least one factor is a multiple of 4.

This completes the proof of Theorem 1.

THEOREM 2. *Let k be odd and λ be an integer > 1 , then*

$$A_k(n_1)A_{2^\lambda}(n_2) = (-1)^{2^{\lambda-2}} A_{2^\lambda k}(n_3),$$

where

$$(2.10) \quad n_3 \equiv k^2 n_2 + 2^{2\lambda} n_1 - (k^2 - 1 + 2^{2\lambda})/24 \pmod{2^\lambda k}.$$

Proof. Since

$$(-1)^{2^{\lambda-2}} = \exp(3 \cdot 2^{2\lambda} k \pi i / 12 \cdot 2^\lambda k),$$

we have to show that the product

$$(2.11) \quad A_k(n_1) A_{2^\lambda}(n_2) = \sum_{(\rho_1)} \sum_{(\rho_2)} \exp \left[\left\{ 2^\lambda f_{n_1}(\rho_1, k) + k g_{n_2}(\rho_2, 2^\lambda) \right\} \pi i / 12 \cdot 2^\lambda k \right]$$

is equal to

$$(2.12) \quad (-1)^{2^{\lambda-2}} A_{2^\lambda k}(n_3) = \sum_{(\rho_3)} \exp \left[\left\{ g_{n_3}(\rho_3, 2^\lambda k) + 3 \cdot 2^{2\lambda} k \right\} \pi i / 12 \cdot 2^\lambda k \right].$$

In fact we show that, provided ρ_3 is related to ρ_1 and ρ_2 by means of the system

$$(2.13) \quad \rho_3 \equiv \rho_1 / 2^\lambda \pmod{k},$$

$$(2.14) \quad \rho_3 \equiv \rho_2 / k \pmod{2^\lambda},$$

then the corresponding terms of (2.11) and (2.12) are equal. To this effect we consider the difference

$$D_2 = g_{n_3}(\rho_3, 2^\lambda k) + 3 \cdot 2^{2\lambda} k - [2^\lambda f_{n_1}(\rho_1, k) + k g_{n_2}(\rho_2, 2^\lambda)]$$

and prove that it is divisible by $24 \cdot 2^\lambda k$.

Consider first the modulus 3 if k is not divisible by 3. Then by (1.12) and (1.15) each term of D_2 is a multiple of 3. Next consider D_2 modulo k or $3k$ according as 3 is prime to k or not. Referring to (1.11) and (1.14) we find that

$$D_2 \equiv \nu_3 \rho_3 + \bar{p}_3 - 2^\lambda (\nu_1 \rho_1 + \bar{p}_1) \pmod{k \text{ or } 3k}.$$

But $\nu_3 = 1 - 24n_3 \equiv 2^{2\lambda} - 24 \cdot 2^{2\lambda} n_1 \equiv 2^{2\lambda} \nu_1 \pmod{k \text{ or } 3k}$, so that

$$D_2 \equiv 2^\lambda (2^\lambda \rho_3 - \rho_1) \left(\nu_1 - \frac{1}{2^\lambda \rho_1 \rho_3} \right) \pmod{k \text{ or } 3k}.$$

The second factor is a multiple of k by (2.13) and, in case 3 divides k , the third factor is also a multiple of 3. Hence

$$D_2 \equiv 0 \pmod{3k}.$$

We must now show that $D_2 \equiv 0 \pmod{2^{\lambda+3}}$. Using (1.13) and (1.16) we have

$$\begin{aligned} D_2 &\equiv \nu_3 \rho_3 + 2^{\lambda+1} k \left(\frac{-2^\lambda k}{\rho_3} \right) + 2^{2\lambda} \rho_3 + 3 \cdot 2^\lambda k \rho_3 + \bar{p}_3 + 3 \cdot 2^{2\lambda} k \\ &\quad - 2^{\lambda+1} k \left(\frac{-\rho_1}{k} \right) - 2^\lambda k + 3 \cdot 2^\lambda \\ &\quad - \left\{ k \nu_2 \rho_2 + 2^{\lambda+1} \left(\frac{-2^\lambda}{\rho_2} \right) k + 2^{2\lambda} k \rho_2 + 3 \cdot 2^\lambda k \rho_2 + k \bar{p}_2 \right\} \pmod{2^{\lambda+3}}. \end{aligned}$$

But since $\nu_3 \equiv k^2\nu_2 + 2^{2\lambda} \pmod{2^{\lambda+3}}$ we obtain on collecting terms

$$(2.15) \quad \begin{aligned} D_2 \equiv & (k\rho_3 - \rho_2) \left(k\nu_2 + 2^{2\lambda}k - \frac{1}{\rho_2\rho_3} \right) + 2^{2\lambda}\rho_3 - 2^\lambda 3k(\rho_2 - \rho_3) + 3 \cdot 2^{2\lambda}k \\ & - 2^\lambda(k-3) + 2^{\lambda+1}k \left[\left(\frac{-2^\lambda k}{\rho_3} \right) - \left(\frac{-\rho_1}{k} \right) - \left(\frac{-2^\lambda}{\rho_2} \right) \right] \pmod{2^{\lambda+3}}. \end{aligned}$$

Consider for the moment the Jacobi symbols. We will show that the quantity

$$Q = \left(\frac{-2^\lambda k}{\rho_3} \right) - \left(\frac{-\rho_1}{k} \right) - \left(\frac{-2^\lambda}{\rho_2} \right) \equiv -(-1)^{(k-1)(\rho_3-1)/4} \pmod{4}.$$

We consider separately the cases λ even and λ odd.

If λ is even, we have by (2.14), $\rho_2 \equiv \rho_3 k \pmod{4}$, and

$$\left(\frac{-2^\lambda k}{\rho_3} \right) = \left(\frac{-1}{\rho_3} \right) \left(\frac{k}{\rho_3} \right), \quad \left(\frac{-2^\lambda}{\rho_2} \right) = \left(\frac{-1}{\rho_2} \right) = \left(\frac{-1}{\rho_3} \right) \left(\frac{-1}{k} \right).$$

By (2.13)

$$\left(\frac{-\rho_1}{k} \right) = \left(\frac{-2^\lambda}{k} \right) \left(\frac{\rho_3}{k} \right) = \left(\frac{-1}{k} \right) \left(\frac{\rho_3}{k} \right).$$

Hence

$$\begin{aligned} Q &= \left(\frac{-1}{\rho_3} \right) \left(\frac{k}{\rho_3} \right) - \left(\frac{-1}{k} \right) \left(\frac{\rho_3}{k} \right) - \left(\frac{-1}{\rho_3} \right) \left(\frac{-1}{k} \right) \\ &= \left\{ \left(\frac{k}{\rho_3} \right) - \left(\frac{-1}{k} \right) \right\} \left\{ \left(\frac{-1}{\rho_3} \right) + \left(\frac{\rho_3}{k} \right) \right\} - \left(\frac{k}{\rho_3} \right) \left(\frac{\rho_3}{k} \right) \\ &\equiv -(-1)^{(k-1)(\rho_3-1)/4} \pmod{4}. \end{aligned}$$

If λ is odd, we have $\lambda > 2$, and $\rho_2 \equiv \rho_3 k \pmod{8}$ so that

$$\left(\frac{-2^\lambda k}{\rho_3} \right) = \left(\frac{-2}{\rho_3} \right) \left(\frac{k}{\rho_3} \right), \quad \left(\frac{-2^\lambda}{\rho_2} \right) = \left(\frac{-2}{\rho_3} \right) \left(\frac{-2}{k} \right)$$

and

$$\left(\frac{-\rho_1}{k} \right) = \left(\frac{-2}{k} \right) \left(\frac{\rho_3}{k} \right).$$

Hence, in this case,

$$\begin{aligned} Q &= \left\{ \left(\frac{k}{\rho_3} \right) - \left(\frac{-2}{k} \right) \right\} \left\{ \left(\frac{-2}{\rho_3} \right) + \left(\frac{\rho_3}{k} \right) \right\} - \left(\frac{\rho_3}{k} \right) \left(\frac{k}{\rho_3} \right) \\ &\equiv -(-1)^{(k-1)(\rho_3-1)/4} \pmod{4}. \end{aligned}$$

With this result we return to (2.15). We note first that on account of (2.14) we have

$$(2.16) \quad k\rho_3 - \rho_2 = 2^\lambda h,$$

so that the factor

$$\left(k\nu_2 + 2^{2\lambda}k - \frac{1}{\rho_2\rho_3} \right)$$

of (2.15) may be considered modulo 8 only. Since $\nu_2 \equiv 1 \pmod{8}$ we find that by (2.16) the first term of (2.15) is congruent to

$$\rho_3 h^2 \cdot 2^{2\lambda} \pmod{2^{\lambda+3}}.$$

Hence the first four terms of (2.15) become congruent to

$$\begin{aligned} 2^{2\lambda} [\rho_3(h^2 + 1) + 3k(h + 1)] - 3 \cdot 2^\lambda k\rho_3(k - 1) \\ \equiv -3 \cdot 2^\lambda k\rho_3(k - 1) \equiv 3 \cdot 2^\lambda \rho_3(k - 1) \pmod{2^{\lambda+3}}, \end{aligned}$$

since the quantity in square brackets is even and $2\lambda + 1 \geq \lambda + 3$. Hence we have

$$\begin{aligned} D_2 &\equiv 2^\lambda [3\rho_3(k - 1) - (k - 3) + 2kQ] \\ &\equiv 2^\lambda [3\rho_3k - 3\rho_3 - k + 3 - 2k \cdot (-1)^{(k-1)(\rho_3-1)/4}] \pmod{2^{\lambda+3}}. \end{aligned}$$

But the quantity in brackets is divisible by 8. In fact if both k and ρ_3 are of the form $4x - 1$ it becomes

$$(3\rho_3 + 1)(k - 1) + 4 \equiv 0 \pmod{8}.$$

In the opposite case we have

$$3(k - 1)(\rho_3 - 1) \equiv 0 \pmod{8}.$$

Hence in both cases D_2 is divisible by $2^{\lambda+3}$. This completes the proof of the theorem.

THEOREM 3. *Let k be an odd integer, then*

$$(2.17) \quad A_k(n) = A_{2k}(4n + (k^2 - 1)/8).$$

Proof. Since

$$(2.18) \quad A_{2k}(n_1) = \sum_{(\rho_1)} \exp \left[g_{n_1}(\rho_1, 2k) \frac{\pi i}{24k} \right],$$

while

$$(2.19) \quad A_k(n) = \sum_{(\rho_2)} \exp \left[2f_n(\rho_2, k) \frac{\pi i}{24k} \right],$$

where for brevity we take n_1 for $4n + (k^2 - 1)/8$, it suffices to show that a correspondence may be set up between ρ_1 and ρ_2 so that corresponding terms of (2.18) and (2.19) are equal. We show that the correspondence is simply

$$(2.20) \quad \rho_1 \equiv \rho_2/2 \pmod{k}.$$

To this effect we define D_3 by

$$(2.21) \quad D_3 = 2f_n(\rho_2, k) - g_{n_1}(\rho_1, 2k)$$

and show that $D_3 \equiv 0 \pmod{48k}$.

We first show that D_3 is divisible by $3k$. In case 3 is prime to k , the fact that $D_3 \equiv 0 \pmod{k}$ is an immediate consequence of (1.12) and (1.15). In case 3 divides k we use (1.11) and (1.14). In either case

$$D_3 \equiv 2\nu\rho_2 + 2\bar{p}_2 - \nu_1\rho_1 - \bar{p}_1 \pmod{k \text{ or } 3k}.$$

But

$$(2.22) \quad \nu_1 = 1 - 24n_1 = 1 - 96n - 3(k^2 - 1) \equiv 4(1 - 24n) \equiv 4\nu \pmod{3k}.$$

So that

$$D_3 \equiv (\rho_2 - 2\rho_1) \left(2\nu - \frac{1}{\rho_1\rho_2} \right) \pmod{k \text{ or } 3k}.$$

By (2.20) the first factor is divisible by k while in case $3|k$, the second factor contains 3 by (2.20), since $\nu \equiv 1 \pmod{3}$. Hence $D_3 \equiv 0 \pmod{3k}$.

We must now show that D_3 is divisible by 16. Using (1.13) and (1.16) in (2.21) we find

$$D_3 \equiv 4k \left(\frac{-\rho_2}{k} \right) + 2k - 6 - \nu_1\rho_1 - 4k \left(\frac{-2k}{\rho_1} \right) - 4\rho_1 - 6k\rho_1 - \bar{p}_1 \pmod{16}.$$

In view of (2.20) and (2.22) we may substitute for ρ_2 and ν_1 and obtain

$$D_3 \equiv 4 \left\{ k \left[\left(\frac{-2\rho_1}{k} \right) - \left(\frac{-2k}{\rho_1} \right) \right] + 2 \frac{(k-3)(k\rho_1+1)}{4} + 2\bar{p}_1 \frac{k^2\rho_1^2-1}{8} + 2 \right\} \pmod{16}.$$

Considering the quantity inside the braces modulo 4 and replacing all odd factors of even numbers by unity we obtain

$$D_3 \equiv 4 \left\{ \left(\frac{-2\rho_1}{k} \right) - \left(\frac{-2k}{\rho_1} \right) + 1 - (-1)^{(\rho_1+1)(k+1)/4} + 1 - \left(\frac{2}{k\rho_1} \right) + 2 \right\}$$

$$\begin{aligned}
&\equiv 4 \left\{ \left(\frac{-2}{k} \right) - \left(\frac{-2}{\rho_1} \right) (-1)^{(\rho_1-1)(k-1)/4} \right. \\
&\quad \left. + (-1)^{(\rho_1-1)(k-1)/4} \left(\frac{-1}{k\rho_1} \right) - \left(\frac{2}{k\rho_1} \right) \right\} \\
&\equiv 4 \left\{ \left(\frac{-2}{k} \right) - \left(\frac{-2}{\rho_1} \right) + \left(\frac{-1}{k\rho_1} \right) - \left(\frac{2}{k\rho_1} \right) \right\} \\
&\equiv 4 \left\{ \left(\frac{-1}{k} \right) - \left(\frac{2}{\rho_1} \right) \right\} \left\{ \left(\frac{-1}{\rho_1} \right) + \left(\frac{2}{k} \right) \right\} \equiv 0 \pmod{16}.
\end{aligned}$$

This proves Theorem 3.

Another form of Theorem 3, which exhibits it as a multiplication theorem, is

THEOREM 4. *If k is odd, then*

$$(2.23) \quad A_2(n_1)A_k(n_2) = A_{2k}(n_3)$$

where

$$n_3 \equiv 4n_2 + kn_1 + (k^2 - 1)/8 \pmod{2k}.$$

This follows easily from the following

LEMMA 1. *If k and n are arbitrary integers*

$$A_{2k}(n) = -A_{2k}(n+k).$$

Proof. This is an immediate consequence of applying the identity

$$e^{-2n\rho\pi i/2k} = -e^{-2(n+k)\rho\pi i/2k}$$

where ρ is odd, to the definition (1.2) of $A_k(n)$.

To prove Theorem 4 we need only to observe that if we apply Lemma 1 n_1 times with $n = 4n_2 + (k^2 - 1)/8$, we obtain from Theorem 3

$$A_{2k}\left(4n_2 + kn_1 + \frac{k^2 - 1}{8}\right) = (-1)^{n_1}A_k(n_2) = A_2(n_1)A_k(n_2).$$

Another form of Theorem 3 states that if k is odd,

$$A_{2k}(n) = (-1)^n \left(\frac{2}{k} \right) A_k \left(\frac{8n+1}{32} \right).$$

This follows readily from Theorem 4.

Theorems 1, 2, and 4 may be used to express $A_k(n)$ in terms of A 's whose subscripts are powers of primes dividing k . This is illustrated in the following examples.

Example I. Express $A_{35}(23)$ in terms of A_5 and A_7 . By (2.1), $n_3 = 23 \equiv 25n_2 + 49n_1 - 73/24 \pmod{35}$. This gives two congruences

$$49n_1 \equiv 0 \pmod{5}$$

and

$$25n_2 \equiv 3 \pmod{7}.$$

Hence $n_1 \equiv 0 \pmod{5}$ and $n_2 \equiv 6 \pmod{7}$. Therefore

$$A_{35}(23) = A_5(0)A_7(6).$$

Example II. Express $A_{30}(17)$ in terms of A_2 , A_3 , and A_5 . By Theorem 4 with $k=15$ we have

$$n_3 = 17 \equiv 4n_2 + 15n_1 + 28 \pmod{30},$$

whence

$$n_2 \equiv 1 \pmod{15},$$

$$n_1 \equiv 1 \pmod{2},$$

so that

$$A_{30}(17) = A_2(1)A_{15}(1).$$

Applying Theorem 1 to $A_{15}(1)$ as in Example I, we find

$$A_{15}(1) = A_3(2)A_5(2),$$

whence

$$A_{30}(17) = A_2(1)A_3(2)A_5(2).$$

Example III. Express $A_{36}(13)$ in terms of A_4 and A_9 . By Theorem 2, $A_{36}(13) = -A_9(n_1)A_4(n_2)$, where $13 \equiv 81n_2 + 16n_1 - 4$, so that

$$n_1 \equiv 5 \pmod{9},$$

$$n_2 \equiv 1 \pmod{4}$$

and we have

$$A_{36}(13) = -A_4(1)A_9(5).$$

3. The evaluation of $A_q(n)$. From the results of the preceding section it is clear that questions concerning the actual value of $A_k(n)$ or merely the order of magnitude of $A_k(n)$ may be reduced to the corresponding questions about $A_q(n)$, where q is a power of a prime. Three cases present themselves quite naturally, namely those in which (I) $q = p^\alpha$, where p is a prime > 3 and $\alpha \geq 1$, (II) q is a power of 3, (III) q is a power of 2. In all cases the number $A_q(n)$ may be expressed in terms of generalized Kloosterman sums of the type

$$\sum_{(s)} \chi(s) e^{2\pi i(a\bar{s} + \bar{s})/q},$$

where χ is a quadratic character, and $s\bar{s} \equiv 1 \pmod{q}$.

The problem of evaluating these sums has been solved in case q is a prime by Salié. In case q is a power of an odd prime the sums may be easily evaluated if use is made of Salié's discussion (§§2, 3) of the original Kloosterman sum. In fact the introduction of the character has no influence on the argument until the very last stage where it results in changing some of the cosines to sines or vice versa. We give therefore without further comment the following lemmas.

LEMMA* 2. *Let $q = p^\alpha$, where p is an odd prime. Then if s runs over the numbers less than and prime to q , the sum*

$$\sum_{(s)} \left(\frac{s}{q}\right) e^{2\pi i(a\bar{s} + \bar{s})/q} = \begin{cases} 0 & \text{if } a \text{ is a non-residue of } q \text{ prime to } q, \\ i^{((q-1)/2)^2} 2q^{1/2} \cos \frac{4\pi\theta}{q} & \text{if } a \equiv \theta^2 \pmod{q}, a \text{ prime to } q, \\ 0 & \text{if } a \text{ is divisible by } p \text{ and } \alpha > 1, \\ i^{((q-1)/2)^2} q^{1/2} & \text{if } a \text{ is divisible by } p \text{ and } \alpha = 1. \end{cases}$$

LEMMA 3. *If $q = 3^\alpha$, $\alpha > 1$ and if $a \equiv 1 \pmod{3}$, then*

$$\sum_{(s)} \left(\frac{s}{3^{\alpha-1}}\right) e^{2\pi i(a\bar{s} + \bar{s})/q} = i^{((q-1)/2)^2+1} \left(\frac{\theta}{3}\right) 2q^{1/2} \sin \frac{4\pi\theta}{q},$$

where $\theta^2 \equiv a \pmod{q}$.

To apply these lemmas to the evaluation of $A_q(n)$ where q is odd we separate two cases.

Case I. $q = p^\alpha$, where p is a prime > 3 . Returning to the definition (1.8) of $f_n(\rho)$, we have from congruences (1.12) and (1.13)

$$f_n(\rho) \equiv 0 \pmod{3}$$

and

$$f_n(\rho) \equiv q - 3 + 2q \left(\frac{-\rho}{q}\right) \pmod{8}.$$

If $q \equiv 1 \pmod{4}$, $q - 3 \equiv -2q(2/q) \pmod{8}$. Hence $f_n(\rho)$ is an even or odd multiple of 12 according as $(2\rho/q) = +1$, or -1 . If $(2\rho/q) = +1$ we may write

$$f_n(\rho) \equiv 24t(\rho) \pmod{24q},$$

while, if $(2\rho/q) = -1$,

* Cf. Salié, loc. cit., equations (54) and (57), p. 102, in case q is a prime. For q a power of a prime compare (32) and (33), p. 97.

$$f_n(\rho) \equiv 24t(\rho) + 12q \pmod{24q},$$

where, in both cases,

$$(3.1) \quad t \equiv t(\rho) \equiv f_n(\rho)/24 \equiv (\nu\rho + \bar{\rho})/24 \pmod{q}$$

by (1.11). Hence for a given ρ we get a term of (1.6) of the form $e^{2\pi i t/q}$ or $e^{2\pi i t/q} e^{\pi i}$, so that if $q \equiv 1 \pmod{4}$,

$$A_q(n) = \sum_{(\rho)} \left(\frac{2\rho}{q} \right) e^{2\pi i t/q},$$

where t is defined by (3.1).

If $q \equiv -1 \pmod{4}$, $f_n(\rho) \equiv 0 \pmod{3}$ and

$$f_n(\rho) \equiv -6q \left(\frac{2\rho}{q} \right) \pmod{8}.$$

Hence, in this case,

$$f_n(\rho) = 24t - 6q \left(\frac{2\rho}{q} \right) \pmod{24q},$$

where t is given by (3.1) and the typical term of (1.6) is, in this case,

$$e^{2\pi i t/q} \exp \left[- \left(\frac{2\rho}{q} \right) \frac{\pi i}{2} \right] = -i \left(\frac{2\rho}{q} \right) e^{2\pi i t/q}.$$

So that whether $q \equiv +1$ or $-1 \pmod{4}$, we have

$$(3.2) \quad A_q(n) = (-i)^{((q-1)/2)^2} \sum_{(\rho)} \left(\frac{2\rho}{q} \right) e^{2\pi i t/q}, \text{ where } t \equiv (\nu\rho + \bar{\rho})/24 \pmod{q}.$$

In order to apply Lemma 2 to (3.2) we set $24\rho \equiv s \pmod{q}$, so that

$$t \equiv \frac{\nu}{24^2} s + \bar{s} \pmod{q}$$

and

$$\left(\frac{2\rho}{q} \right) = \left(\frac{3s}{q} \right) = \left(\frac{3}{q} \right) \left(\frac{s}{q} \right).$$

With this change in notation (3.2) becomes

$$A_q(n) = (-i)^{((q-1)/2)^2} \left(\frac{3}{q} \right) \sum_{(s)} \left(\frac{s}{q} \right) e^{2\pi i (as + \bar{s})/q}, \text{ where } a \equiv \nu/24^2 \pmod{q}.$$

Applying Lemma 2, we obtain

THEOREM 5. If $q = p^\alpha$, p a prime > 3 , $\alpha \geq 1$ and $\nu = 1 - 24n$, then

$$A_q(n) = \begin{cases} 0 & \text{if } \nu \text{ is non-residue* of } q, \text{ prime to } q, \\ 2 \left(\frac{3}{q} \right) q^{1/2} \cos \frac{4\pi m}{q} & \text{if } \nu \equiv (24m)^2 \pmod{q}, \text{ prime to } q, \\ 0 & \text{if } \nu \equiv 0 \pmod{p} \text{ and } \alpha > 1, \\ \left(\frac{3}{q} \right) q^{1/2} & \text{if } \nu \equiv 0 \pmod{p} \text{ and } \alpha = 1. \end{cases}$$

Case II. $q = 3^\beta$, $\beta \geq 1$. First let β be even. Then from (1.11) and (1.13) we have

$$f_n(\rho) \equiv 8t(\rho) \pmod{3^{\beta+1}}.$$

$$(3.3) \quad t = t(\rho) \equiv (\nu\rho + \bar{\rho})/8 \pmod{3^{\beta+1}},$$

so that $\exp [f_n(\rho)\pi i/12q] = e^{2\pi i t/3^{\beta+1}}$.

If β is odd, then

$$f_n(\rho) \equiv 8t - 6q \left(\frac{2\rho}{q} \right) \pmod{8 \cdot 3^{\beta+1}}.$$

Hence in this case

$$\exp [f_n(\rho)\pi i/12q] = -i \left(\frac{2\rho}{q} \right) e^{2\pi i t/3^{\beta+1}},$$

where t is given again by (3.3). Hence in both cases we have

$$(3.4) \quad A_q(n) = (-i)^{((q-1)/2)^2} \sum_{(\rho)} \left(\frac{2\rho}{q} \right) e^{2\pi i t(\rho)/3^{\beta+1}},$$

where ρ runs over the numbers prime to 3 and less than 3^β . Since $t(\rho + 3^\beta) \equiv t(\rho) \pmod{3^{\beta+1}}$, if $\bar{\rho}$ is replaced by $\bar{\rho} - 3^\beta \bar{\rho}^2$ we may let ρ run up to $3^{\beta+1}$ in (3.4) and obtain $3A_q(n)$. At the same time we replace ρ by $s/8 \pmod{3^{\beta+1}}$, so that

$$t(\rho) \equiv \frac{\nu}{8^2} s + \bar{s} \pmod{3^{\beta+1}}$$

and $(2\rho/q) = (s/q)$. Hence (3.4) becomes

$$A_q(n) = \frac{1}{3} (-i)^{((q-1)/2)^2} \sum_{(s)} \left(\frac{s}{q} \right) e^{2\pi i (s + \bar{s})/3^{\beta+1}},$$

* This condition should not be confused with $(\nu/q) = -1$. We mean that no solution exists of the congruence $x^2 \equiv \nu \pmod{q}$.

where $a \equiv \nu/8^2 \pmod{3^{\beta+1}}$. Since $\nu \equiv 1 \pmod{3}$, we may apply Lemma 3 with $\alpha = \beta + 1$ and obtain the following:

THEOREM 6. *Let $\nu = 1 - 24n$, then*

$$A_3^\beta(n) = (-1)^{\beta+1} \left(\frac{m}{3}\right) \frac{2}{3^{1/2}} (3^\beta)^{1/2} \sin \frac{4\pi m}{3^{\beta+1}},$$

where $(8m)^2 \equiv \nu \pmod{3^{\beta+1}}$.

Case III. $q = 2^\lambda$. In this case we shall evaluate $A_q(n)$ directly without passing to a generalized Kloosterman sum, since the introduction of the appropriate quadratic character into Salé's discussion of the corresponding Kloosterman sum cannot be accomplished without considerable reconstruction. The method of proof is similar to that used by Salé and Estermann.

THEOREM 7. *If $\lambda \geq 0$,*

$$A_2^\lambda(n) = (-1)^\lambda \left(\frac{-1}{m}\right) (2^\lambda)^{1/2} \sin \frac{4\pi m}{2^{\lambda+3}},$$

where m is an integer $\equiv \nu^{1/2}/3 \pmod{2^{\lambda+3}}$.

Proof. For brevity define u and v by

$$u = \left\lfloor \frac{\lambda}{2} \right\rfloor + 2, \quad v = \left\lfloor \frac{\lambda + 1}{2} \right\rfloor - 2$$

so that $\lambda = u + v$. The numbers ρ which are less than 2^λ and odd may be represented by

$$\rho = \tau + 2^u h \quad \begin{cases} \tau = 1, 3, 5, \dots, 2^u - 1, \\ h = 0, 1, 2, \dots, 2^v - 1. \end{cases}$$

Hence $A_2^\lambda(n)$ may be written as a double sum

$$(3.5) \quad A_2^\lambda(n) = \sum_{(\tau)} \sum_{h=0}^{2^v-1} \exp [g_n(\tau + 2^u h) \pi i / 12 \cdot 2^\lambda].$$

For $h_1 \neq h_2$ we consider the difference

$$\Delta_\tau = g_n(\tau + 2^u h_1) - g_n(\tau + 2^u h_2).$$

By (1.15), $\Delta_\tau \equiv 0 \pmod{3}$. Assuming that $\lambda > 4$ so that $u > 3$, and $2u \geq \lambda + 3$ we find from (1.16) that

$$(3.6) \quad \Delta_\tau \equiv 2^u (h_1 - h_2) \left\{ \nu - \frac{1}{\tau^2} \right\} \pmod{2^{\lambda+3}}.$$

Since

$$(3.7) \quad \nu \equiv \bar{\nu} \equiv 1 \pmod{8},$$

it follows that ν is a quadratic residue of $2^{\lambda+3}$. In view of (3.6), $\Delta_\tau \equiv 0 \pmod{2^{u+3}}$ for all τ . We proceed to arrange the values of τ into sets according to the highest power of 2 dividing $\tau^2 - \bar{\nu}$.

If $\tau^2 \not\equiv \bar{\nu} \pmod{2^4}$, τ will be said to belong to set 1. For such a τ , $\Delta_\tau \equiv 0 \pmod{2^{u+3}}$ for all pairs (h_1, h_2) , but since each $h < 2^v$, $h_1 - h_2$ is never divisible by 2^v , that is, $\Delta_\tau \not\equiv 0 \pmod{2^{\lambda+3}}$. This means that those terms of (3.5) for which τ belongs to set 1 correspond to g 's of the form

$$g_n(\tau + 2^u h) = c_\tau + 3M_{\tau, h} 2^{u+3} \pmod{24 \cdot 2^\lambda},$$

where $M_{\tau, h}$ runs with h over the numbers $0, 1, 2, \dots, 2^v - 1$ in some order. Hence the contribution to (3.5) from any member τ of set 1 is

$$\exp \left[\frac{c_\tau \pi i}{12 \cdot 2^\lambda} \right] \sum_{h=0}^{2^v-1} \exp \frac{2\pi i h}{2^v} = 0.$$

Hence we need only consider those τ 's which do not belong to set 1. For such numbers $\tau^2 \equiv \bar{\nu} \pmod{2^4}$. For any $h_1 < 2^{v-1}$ there exists an $h_2 = h_1 + 2^{v-1}$ such that $(h_1 - h_2) \equiv 0 \pmod{2^{v-1}}$ and the corresponding difference Δ_τ is divisible by $3 \cdot 2^u \cdot 2^{v-1} \cdot 2^4 = 24 \cdot 2^\lambda$. Since the corresponding terms of (3.5) make precisely the same contribution to $A_{2^\lambda}(n)$ we may contract (3.5) to read

$$(3.8) \quad A_{2^\lambda}(n) = 2 \sum_{(\tau)} \sum_{h=0}^{2^{v-1}-1} \exp [g_n(\tau + 2^u h) \pi i / 12 \cdot 2^\lambda],$$

where now the outer sum extends over the values of τ for which

$$\tau^2 \equiv \bar{\nu} \pmod{2^4}.$$

If $\tau^2 \not\equiv \bar{\nu} \pmod{2^5}$, τ will be said to belong to set 2. For such a τ , $\Delta_\tau \equiv 0 \pmod{2^{u+4}}$, but $\Delta_\tau \not\equiv 0 \pmod{2^{\lambda+3}}$, since now $h_1 - h_2$ is never divisible by 2^{v-1} . This means that the terms of (3.8) belonging to a fixed number τ of set 2 contribute nothing to $A_{2^\lambda}(n)$. We may therefore ignore all τ 's but those for which $\tau^2 \equiv \bar{\nu} \pmod{2^5}$. Moreover if for any such τ , $h_2 = h_1 + 2^{v-2}$ the corresponding Δ_τ will be divisible by $3 \cdot 2^u \cdot 2^{v-2} \cdot 2^5 = 24 \cdot 2^\lambda$ so that the corresponding contributions to (3.8) are identical. Hence

$$A_{2^\lambda}(n) = 2^2 \sum_{(\tau)} \sum_{h=0}^{2^{v-2}-1} \exp [g_n(\tau + 2^u h) \pi i / 12 \cdot 2^\lambda],$$

where now $\tau^2 \equiv \bar{\nu} \pmod{2^5}$. Repeating the argument we may reduce the terms of the inner sum to a single term corresponding to $h=0$ and obtain

$$(3.9) \quad A_{2^\lambda}(n) = 2^v \sum_{(\tau)} \exp [g_n(\tau) \pi i / 12 \cdot 2^\lambda],$$

where

$$(3.10) \quad \tau^2 \equiv \bar{\nu} \pmod{2^{v+3}}.$$

At this point we separate two cases according to the parity of λ . If λ is odd, $u = v + 3$, and since τ is chosen from the odd numbers $< 2^u = 2^{v+3}$ the congruence (3.10) has four solutions

$$\tau \equiv \pm \gamma, \quad \pm (\gamma + 2^{v+2}) \pmod{2^{v+3}}$$

where $\gamma^2 \equiv \bar{\nu} \pmod{2^{\lambda+3}}$. If we consider the difference

$$D_1 = g_n(\gamma + 2^{v+2}) - g_n(\gamma),$$

we find by (1.15) that $D_1 \equiv 0 \pmod{3}$, while by (1.16)

$$\begin{aligned} D_1 &\equiv 2^{v+2} \left\{ \nu - \frac{1}{\gamma(\gamma + 2^{v+2})} \right\} \\ &\equiv 2^{v+2} \{ \nu \gamma^2 - 1 + \nu \gamma 2^{v+2} \} (\gamma^2 + 2^{v+2} \gamma)^{-1} \pmod{2^{\lambda+3}}. \end{aligned}$$

Since $\nu \gamma^2 - 1 \equiv 0 \pmod{2^{v+2}}$ the last factor may be taken modulo $2^{\lambda+3-2v-4} = 4$, and is $\equiv 1 \pmod{4}$ since $v \geq 0$. Hence

$$D_1 \equiv 2^{\lambda+1} \bar{\gamma} \pmod{2^{\lambda+3}},$$

and

$$g_n(\gamma + 2^{v+2}) \equiv g_n(\gamma) + 3c2^{\lambda+1} \pmod{24 \cdot 2^\lambda}$$

where c is an integer $\equiv 1/3\gamma \equiv -\gamma \pmod{4}$. Since $g(\rho) = -g(-\rho) \pmod{24 \cdot 2^\lambda}$, (3.9) becomes

$$\begin{aligned} A_2^\lambda(n) &= 2^{v+1} \{ \cos [g_n(\gamma)\pi/12 \cdot 2^\lambda] + \cos [g_n(\gamma)\pi/12 \cdot 2^\lambda - \gamma\pi/2] \} \\ &= 2^{v+2} \cos \frac{\pi\gamma}{4} \cos [g_n(\gamma)\pi/12 \cdot 2^\lambda - \gamma\pi/4]. \end{aligned}$$

But $v+2 = (\lambda+1)/2$ and $\cos \pi\gamma/4 = (2/\gamma)(1/2^{1/2})$, so that we have

$$(3.11) \quad A_2^\lambda(n) = \left(\frac{2}{\gamma} \right) (2^{\lambda/2}) \cos [g_n(\gamma)\pi/12 \cdot 2^\lambda - \pi\gamma/4].$$

Before proceeding further we take up the case of λ even. In this case $u = v + 4$. Since $\tau < 2^u = 2^{v+4}$ there are 8 values of τ which are needed in (3.9). These are

$$\tau \equiv \pm (\gamma + j2^{v+2}) \pmod{2^{v+3}} \quad (j = 0, 1, 2, \text{ and } 3).$$

Now if

$$D_2 = g_n(\gamma + j2^{v+2}) - g_n(\gamma),$$

then $D_2 \equiv 0 \pmod{3}$ and

$$\begin{aligned} D_2 &\equiv j2^{v+2} \left\{ \nu - \frac{1}{\gamma(\gamma + j2^{v+2})} \right\} \\ &\equiv \tilde{\gamma} j^2 2^{2v+4} \equiv 9\gamma j^2 2^\lambda \pmod{2^{\lambda+3}}. \end{aligned}$$

Therefore

$$g_n(\gamma + j2^{v+2}) \equiv g_n(\gamma) + 9\gamma j^2 2^\lambda \pmod{3 \cdot 2^{\lambda+3}},$$

so that if

$$F(j) = \exp [g_n(\gamma + j2^{v+2})\pi i / 12 \cdot 2^\lambda] = \exp [g_n(\gamma)\pi i / 12 \cdot 2^\lambda] e^{3\gamma j^2 \pi i / 4},$$

then $F(0) = -F(2)$ and $F(1) = F(3)$, and (3.9) becomes

$$\begin{aligned} A_2^\lambda(n) &= 2^{v+2} \cos [g_n(\gamma)\pi / 12 \cdot 2^\lambda + 3\gamma\pi / 4] \\ &= - (2^{\lambda/2}) \cos [g_n(\gamma)\pi / 12 \cdot 2^\lambda - \gamma\pi / 4]. \end{aligned}$$

In view of (3.11) we may combine the results for even and odd by writing

$$(3.12) \quad A_2^\lambda(n) = (-1)^{\lambda+1} \left(\frac{2^\lambda}{\gamma} \right) (2^{\lambda/2}) \cos [g_n(\gamma)\pi / 12 \cdot 2^\lambda - \gamma\pi / 4].$$

To evaluate this cosine we refer once more to (1.15) and (1.16) and write $g_n(\gamma) \equiv 0 \pmod{3}$ and

$$g_n(\gamma) \equiv \nu\gamma + \tilde{\gamma} - 6 \cdot 2^\lambda \left(\frac{-2^\lambda}{\gamma} \right) + 3\gamma 2^\lambda \pmod{2^{\lambda+3}},$$

so that if we define the integer m by

$$m \equiv (\nu\gamma + \tilde{\gamma}) / 6 \equiv \nu^{1/2} / 3 \pmod{2^{\lambda+3}},$$

we have

$$\begin{aligned} \cos [g_n(\gamma)\pi / 12 \cdot 2^\lambda - \gamma\pi / 4] &= \cos \left\{ \frac{4\pi m}{2^{\lambda+3}} - \left(\frac{-2^\lambda}{\gamma} \right) \frac{\pi}{2} \right\} \\ &= \left(\frac{-2^\lambda}{\gamma} \right) \sin \frac{4\pi m}{2^{\lambda+3}}. \end{aligned}$$

Hence substituting into (3.12) we have

$$A_2^\lambda(n) = (-1)^{\lambda+1} \left(\frac{-1}{\gamma} \right) (2^{\lambda/2}) \sin \frac{4\pi m}{2^{\lambda+3}},$$

where m is an integer $\equiv \nu^{1/2} / 3 \pmod{2^{\lambda+3}}$. But

$$\left(\frac{-1}{\gamma} \right) = \left(\frac{-1}{3} \right) \left(\frac{-1}{m} \right) = - \left(\frac{-1}{m} \right),$$

so the theorem follows, when $\lambda > 4$.

As a matter of fact the theorem is true when $\lambda \leq 4$. This may be verified by merely consulting the tables of $A_k(n)$.

The following corollary, which is a consequence of Theorems 1, 2, 3, and 5, is especially useful in applying series (1.1). The proof, which involves the separation of three cases, is left to the reader.

COROLLARY. *If k is divisible by the prime p and if $A_p(n) = 0$, then $A_k(n) = 0$.*

4. Estimates and remainders. In this section we apply the preceding results to the discussion of the order of magnitude of $A_k(n)$ and to the estimation of the errors committed by taking only the first N terms of the Hardy-Ramanujan and Rademacher series.

THEOREM 8. *Let ω be the number of distinct odd prime factors of k . Then*

$$|A_k(n)| < 2^\omega k^{1/2}.$$

Proof. Let

$$k = 2^\lambda p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_\omega^{\alpha_\omega}$$

be the decomposition of k into its prime factors. By §2, there exists a set $(n_0, n_1, n_2, \dots, n_\omega)$ such that

$$(4.1) \quad A_k(n) = A_{2^\lambda}(n_0) A_{p_1^{\alpha_1}}(n_1) \cdots A_{p_\omega^{\alpha_\omega}}(n_\omega).$$

By theorem 7

$$|A_{2^\lambda}(n_0)| < 2^{\lambda/2},$$

while by Theorems 5 and 6

$$|A_{p^\alpha}(n)| < 2p^{\alpha/2}.$$

Hence the theorem follows from (4.1).

Since, for every $\epsilon > 0$

$$2^{\omega(k)} = O(k^\epsilon),$$

we have as an immediate consequence

$$(4.2) \quad A_k(n) = O(k^{1/2+\epsilon}).$$

Using this result it is possible to prove the following:

THEOREM 9. *Let w be any number greater than $2\pi(2/3)^{1/2} = 5.130 \dots$, then for all sufficiently large n , $p(n)$ is the nearest integer to the first $[wn^{1/2}/\log n]$ terms of the Hardy-Ramanujan series.*

This theorem is similar to a result of Hardy and Ramanujan* based on

* Loc. cit., pp. 107-108, §6.3.

$A_k(n) = O(k)$ in which w is replaced by $4\pi(2/3)^{1/2}$, and may be proved in the same way. However it is possible to prove somewhat more than (4.2).

THEOREM 10. *For every $\epsilon > 0$ there exists a K such that for all n and for all $k > K$*

$$|A_k(n)| < k^{1/2 + (1+\epsilon)\log 2 / \log \log k}.$$

Proof. This follows easily from a theorem of Wigert* to the effect that for every ϵ there exists a K such that if $k > K$

$$\tau(k) < 2^{(1+\epsilon)\log k / \log \log k},$$

where $\tau(k)$ is the number of divisors of k , and from the trivial inequality

$$2^{\omega(k)} \leq \tau(k).$$

In contrast to this theorem we prove:

THEOREM 11. *For every $\epsilon > 0$ there exist infinitely many values of n and k for which*

$$|A_k(n)| > .11367 k^{1/2 + (1-\epsilon)\log 2 / \log \log k}.$$

Proof. Let p be a prime > 3 and let n_p be an integer $\equiv -35/24 \pmod{p}$. Then

$$\nu_p = 1 - 24n_p \equiv 6^2 \pmod{p}.$$

Applying Theorem 5 with $q=p$ and $n=n_p$ we find $m \equiv (p^2-1)/4 \pmod{p}$ and

$$(4.3) \quad |A_p(n_p)| = 2p^{1/2} \left| \cos \frac{(p^2-1)\pi}{p} \right| = 2p^{1/2} \cos \frac{\pi}{p} > 2p^{1/2} \left(1 - \frac{\pi^2}{2p^2} \right).$$

Let p_j denote the j th prime ≥ 2 . By Theorem 1 there exists an n such that

$$A_k(n) = A_2(0)A_3(0)A_5(n_5) \cdots A_{p_t}(n_{p_t}),$$

where $k = 2 \cdot 3 \cdot 5 \cdot 7 \cdots p_t$ and where t will be determined later. Applying (4.3) we find

$$\begin{aligned} |A_k(n)| &> \frac{A_3(0)}{6^{1/2}} k^{1/2} 2^{t-2} \prod_{j=3}^t \left(1 - \frac{\pi^2}{2p_j^2} \right) \\ &> \frac{A_3(0)}{6^{1/2}} k^{1/2} 2^{t-2} \frac{\prod_{j=1}^{\infty} (1 - \pi^2/2(2j-1)^2)}{(1 - \pi^2/2)(1 - \pi^2/18)(1 - \pi^2/162)} \\ &> .12044 k^{1/2} \cdot 2^t \left| \cos (\pi^2/8^{1/2}) \right| \\ (4.4) \quad |A_k(n)| &> .11367 k^{1/2} \cdot 2^t. \end{aligned}$$

* Archiv för Matematik, Astronomi, och Fysik, vol. 3 (1906-1907), no. 18. See also Landau Handbuch, vol. 1, p. 220.

As to the factor 2^t , we have by the prime number theorem

$$\log 2^t = t \cdot \log 2 = \pi(p_t) \log 2 \sim p_t \log 2 / \log p_t.$$

But

$$p_t \sim \sum_{i=1}^t \log p_i = \log k.$$

Hence

$$\log 2^t \sim \frac{\log 2 \log k}{\log \log k}.$$

Therefore if $\epsilon > 0$ is given

$$\log 2^t > \frac{(1 - \epsilon) \log 2 \log k}{\log \log k}$$

for all sufficiently large values of t and k . In other words there are infinitely many k 's for which

$$2^t > k^{(1-\epsilon) \log 2 / \log \log k}.$$

From this and (4.4) the theorem follows at once.

In the subsequent discussion however we need an estimate of $A_k(n)$ for all values of k and n . The one we shall use is given by the following:

THEOREM 12. *For all n and k*

$$(4.5) \quad |A_k(n)| < 2k^{5/6}.$$

Proof. Let $\omega(k)$ denote as before the number of odd prime factors of k and let P_j be the product of the first j odd primes. The number k being given, there exists a j such that

$$P_j \leq k < P_{j+1}.$$

This means that

$$(4.6) \quad \omega(k) \leq j.$$

Suppose for the moment that $k \geq 105 = P_8$. Then since $P_{j+1} > k$, we have $j \geq 3$. Hence

$$k \geq P_j \geq 3 \cdot 5 \cdot 7 \cdot 11^{j-3}$$

or

$$j \leq .96026 \log_{10} k + 1.05914.$$

Therefore in view of (4.6)

$$2^{\omega(k)} \leq 2^j < 2.0836 k^{.28907} < 2k^{1/3}$$

since $k > 3$. It follows by Theorem 8 that

$$|A_k(n)| < 2k^{5/6} \text{ for } k \geq 105.$$

If $15 \leq k < 105$, then $2^{\omega(k)} \leq 4 < 2 \cdot (15)^{1/3}$ and $|A_k(n)| < 2(15)^{1/3} \cdot k^{1/2} \leq 2k^{5/6}$. For $1 \leq k < 15$, $2^{\omega(k)} \leq 2$ so that $|A_k(n)| < 2k^{1/2} < 2k^{5/6}$. Hence the inequality (4.5) holds for all k .

It is clear that an infinite number of inequalities similar to (4.5) but with smaller powers ($> 1/2$) of k may be established in the same way (for example $|A_k(n)| < 3k^{3/4}$), but only at the expense of larger constant coefficients.

We now consider the remainder of Rademacher's convergent series for $p(n)$.

$$(4.7) \quad p(n) = \frac{1}{\pi 2^{1/2}} \sum_{k=1}^{\infty} A_k(n) k^{1/2} \frac{d}{dn} \left(\frac{\sinh(c\lambda_n/k)}{\lambda_n} \right),$$

where

$$c = \pi(2/3)^{1/2}, \quad \lambda_n = (n - 1/24)^{1/2}.$$

Introducing the notation

$$(4.8) \quad c\lambda_n = \mu_n = \mu = \frac{\pi}{6} (24n - 1)^{1/2},$$

$$(4.9) \quad A_k(n) = A_k^*(n) k^{1/2},$$

we may write (4.7) in the form

$$(4.10) \quad p(n) = \frac{12^{1/2}}{24n - 1} \sum_{k=1}^N A_k^*(n) \left\{ \left(1 - \frac{k}{\mu}\right) e^{\mu/k} + \left(1 + \frac{k}{\mu}\right) e^{-\mu/k} \right\} + R_N(n),$$

where the remainder $R_N(n)$ may be written after expanding the exponentials and collecting

$$(4.11) \quad R_N(n) = \frac{4(12)^{1/2}}{24n - 1} \sum_{k=N+1}^{\infty} A_k^*(n) \sum_{j=1}^{\infty} \frac{j(\mu/k)^{2j}}{(2j+1)!},$$

By Theorem 12

$$(4.12) \quad |A_k^*(n)| < 2k^{1/3}.$$

Therefore if we eliminate n from (4.11) by means of (4.8) we obtain

$$\begin{aligned} |R_N(n)| &< \frac{4\pi^{23/2}}{9\mu^2} \sum_{k=N+1}^{\infty} k^{1/3} \sum_{j=1}^{\infty} \frac{j(\mu/k)^{2j}}{(2j+1)!} \\ &< \frac{4\pi^{23/2}}{9\mu^2} \int_N^{\infty} \sum_{j=1}^{\infty} \frac{j(\mu/x)^{2j} x^{1/3}}{(2j+1)!} dx. \end{aligned}$$

Setting $\mu/x = t$ and defining r by

$$r = \mu/N,$$

we obtain on eliminating x

$$\begin{aligned} |R_N(n)| &< \frac{4\pi^{2/3}}{9\mu^{2/3}} \int_0^r \sum_{j=1}^{\infty} \frac{j t^{2j-7/3}}{(2j+1)!} dt \\ (4.13) \quad &< \frac{N^{-2/3}\pi^2}{3^{1/2}} \sum_{j=0}^{\infty} \frac{r^{2j}}{(2j+3)(3j+1)(2j+1)!} \\ &< \frac{N^{-2/3}\pi^2}{3^{1/2}} \left\{ \frac{1}{3} + \sum_{j=1}^{\infty} \frac{r^{2j}}{(2j+3)!} \right\}. \end{aligned}$$

So that

$$(4.14) \quad |R_N(n)| < \frac{N^{-2/3}\pi^2}{3^{1/2}} \left\{ \frac{\sinh r}{r^3} + \frac{1}{6} - \frac{1}{r^2} \right\} = N^{-2/3}F(r).$$

We give a few values of $F(r)$ for typical values of r .

r	$F(r)$	r	$F(r)$
1.0	1.9480	3.5	2.6831
1.5	2.0122	4.0	3.0233
2.0	2.1085	4.5	3.4825
2.5	2.2444	5.0	4.1044
3.0	2.4308	5.5	4.9515

To illustrate the use of (4.14) we give the following examples.

I. Find the maximum error committed by using only 18 terms of the Rademacher series for $p(599)$. Here we have $\mu_{599} = 62.777$ and $r = \mu/18 = 3.4876$. Hence $F(r) = 2.720$ so that $|R_{18}(599)| < .396$. Actually $\dagger R = .00027$.

II. Find $R_{21}(721)$. Here $\mu = 68.8746$, $\mu/21 = r = 3.2797$. $F(r) = 2.596$, and $|R_{21}(721)| < .341$. Actually $\dagger R = .00041$.

We now consider the difference $d_N(n)$ between the sums of the N first terms of Rademacher series and that of Hardy and Ramanujan. That is, in view of (4.10),

$$d_N(n) = \frac{12^{1/2}}{24n-1} \sum_{k=1}^N A_k^*(n) \left(1 + \frac{k}{\mu}\right) e^{-\mu/k}.$$

Using (4.12) we find

$$|d_N(n)| < \frac{48^{1/2}}{24n-1} \left\{ \int_0^N x^{1/3} \left(1 + \frac{x}{\mu}\right) e^{-\mu/x} dx + N^{1/3} \left(1 + \frac{N}{\mu}\right) e^{-\mu/N} \right\}.$$

Since $e^{-\mu/x} < x/\mu$ we find, on writing $r = \lambda/N$ and $24n-1 = (6\mu/\pi)^2$,

\dagger Journal of the London Mathematical Society, vol. 11 (1936), pp. 115-116.

$$(4.15) \quad |d_N(n)| < \frac{\pi^2}{3^{1/2}\mu} \frac{r+1}{r^2} \left\{ \frac{\mu^{1/3}}{7r^{4/3}} + \frac{r^{1/3}}{3\mu} \right\}.$$

This estimate, crude though it is, shows that, for typical calculations of $p(n)$, $d_N(n)$ is sensibly zero.

We are now in a position to answer the question: When is the Hardy-Ramanujan series applicable? This may be answered in a number of ways of which the following is an example.

THEOREM 13. *If only $2n^{1/2}/3$ terms of the Hardy-Ramanujan series (1.1) be taken, the resulting sum will differ from $p(n)$ by less than $1/2$, provided $n > 600$.†*

Proof. If $N = 2n^{1/2}/3$, then

$$(4.16) \quad r = \frac{\mu}{N} = \frac{2\mu}{3n^{1/2}} = \frac{\pi}{9} \frac{(24n-1)^{1/2}}{n^{1/2}} < 3.847.$$

Since $n > 600$, $N = \frac{2}{3}n^{1/2} > 16$, and $\mu > \pi/6(24n)^{1/2} > 62.832$.

$$|R_N(n)| < F(3.847)16^{-2/3} < .46.$$

Now since the right member of (4.15) is a decreasing function of μ , we obtain

$$|d_N(n)| < .0031.$$

Hence the sum of the first N terms of the Hardy-Ramanujan series differs from $p(n)$ by an amount which is less than

$$|R_N(n)| + |d_N(n)| < .46 + .0031 < 1/2$$

in absolute value.

The factor $2/3$ of Theorem 13 may be made smaller by allowing the lower limit of n to increase. For example if we wish to take only $n^{1/2}/2$ terms of the series we may do so provided $n > 3600$. By making a general argument we may easily prove the following:

THEOREM 14. *Let $\delta > 1$ and let $c = \pi(2/3)^{1/2} = 2.565 \dots$. Then $p(n)$ is the nearest integer to the sum of the first $n^{1/2}/\delta$ terms of the Hardy-Ramanujan series provided*

$$n > \frac{27^{1/2}c^6}{\delta^2} \left\{ \frac{\sinh(c\delta)}{c^3\delta^3} + \frac{1}{6} \right\}^3 = O(e^{3c\delta}\delta^{-11}).$$

† The tables of $p(n)$ for $n \leq 600$ have been published by Gupta, Proceedings of the London Mathematical Society, (2), vol. 39 (1935), pp. 148-149; vol. 42, pp. 546-549.