THE CIRCLE PROBLEM IN AN ARITHMETIC PROGRESSION

R. A. Smith

(received October 12, 1967)

1. Introduction. In following a suggestion of S. Chowla to apply a method of C. Hooley [3] to obtain an asymptotic formula for the sum $\sum_{n \leq x} r(n)r(n+a)$, where $r(n)$ denotes the number of representations of n as the sum of two squares and a is a positive integer, we have had to obtain non-trivial estimates for the error term in the asymptotic expansion of

$$\sum_{\substack{n \leq x \\ n \equiv b \pmod{k}}} r(n). \tag{1}$$

In this paper, we devote most of our attention to this sum, and in a paper to follow, we shall obtain the asymptotic formula for $\sum_{n \leq x} r(n)r(n+a)$. In fact, Hooley's method allows us to obtain the asymptotic formula for $\sum_{n \leq x} r(pn)r(qn+a)$, where p and q are positive integers. We remark that T. Estermann obtained the asymptotic expansion for this sum in 1932 [1] for $p = q = 1$, using elementary methods.

In this paper, we use a technique used by Estermann [2] to obtain the functional equation of $R(s;e(p/q))$ and its meromorphic part. As an application of our asymptotic formula for (1), we "generalize" a problem of Mordell [4] on the least solution of a quadratic congruence, and slightly improve upon his result.

The author wishes to thank Professor Chowla for his encouragement and suggestions during the development of this paper, and J.H.H. Chalk for bringing Mordell's work to his attention.

2. Definitions and Notation. Throughout this paper, we shall adopt the following conventions. χ is always the non-principal character modulo 4, and $r(n) = \sum_{d \mid n} \chi(d)$. We shall reserve the asterisk to mean: for each ordered pair of positive integers a and q, define a^* and ℓ such that $4a = \ell q + a^*$, where $1 \leq a^* \leq q$. The prime on the summation sign $\sum'$ will be reserved to mean that, in

case the index of summation begins with zero, the zero term is to be deleted if it is not defined; also, if g is defined as a series whose summation index begins at zero, then we shall write g' to mean that a prime appears on the summation sign defining g. For brevity, we shall write $\sum_{h\leq k}$ instead of $\sum_{1\leq h\leq k}$. If q is an integer, we shall write $p(q)$ to mean that p runs through a set of reduced residues modulo q. $a, b, c, d, h, k, \ell, m, n, p, q, u, v, x, y, M, N, Q, R$ are always non-negative integers. B, C, X are positive real numbers and $s = \sigma + it$ is an arbitrary complex number, as usual. Also define $e(s) = e^{2\pi is}$.

Let

$$g(s) = \sum_{n\geq 1} a_n n^{-s}$$

be any Dirichlet series. We define the following related series:

$$g(s;e(h/k)) = \sum_{n\geq 1} a_n e(nh/k)\, n^{-s};$$

$$g(s;b,k) = \sum_{\substack{n\geq 1 \\ n\equiv b \pmod k}} a_n n^{-s};$$

$$g(s,w) = \sum_{n\geq 0} a_{n+1}(n+w)^{-s}, \quad 0<w\leq 1.$$

In particular,

$$\zeta(s) = \sum_{n\geq 1} n^{-s},$$

which is the Riemann Zeta Function;

$$L_\ell(s) = \sum_{n\geq 1} \chi(n-\ell)\, n^{-s},$$

which reduces to the ordinary L-function of the non-principal character modulo 4 if $\ell \equiv 0 \pmod 4$, in which case we write $L(s) = L_0(s)$; and

$$R(s) = \sum_{n\geq 1} r(n)\, n^{-s}.$$

Finally, we shall adopt the following definitions throughout this paper.

(1) Whenever we write $m = 2^u M$, it shall be understood that $(2, M) = 1$.

https://doi.org/10.4153/CMB-1968-019-2 Published online by Cambridge University Press

(2) $\chi^{\circ}(m) = \chi(M)$, where $m = 2^{u}M$.

(3) $$E_m(n) = \begin{cases} 1 & \text{if } m \mid n \\ 0 & \text{if } m \nmid n. \end{cases}$$

(4) $$e_m(n) = \begin{cases} 1 & \text{if } u \leq v \\ 0 & \text{if } u > v, \end{cases}$$

where $m = 2^{u}M$ and $n = 2^{v}N$.

(5) δ_{uv} = Kronecker's Delta.

(6) $$c_q(b) = \sum_{p(q)} e(-pb/q),$$

which is the Ramanujan Sum.

(7) $$c_q(b;\chi) = \sum_{p(q)} \chi(p)\, e(-pb/q).$$

(8) $$h_q(b) = \sum_{n \leq q} \chi(n)\, e(nb/q).$$

(9) $$H_k(b) = \sum_{q \mid k} \chi(q)\, c_q(b)\, q^{-1}.$$

(10) $$\tilde{H}_k(b) = [1 + \chi^{\circ}(b)\, e_{4b}(k)]\, H_k(b).$$

3. Some Lemmas. We now give three lemmas which will be needed in the development of this paper. We omit the proofs, since standard arguments give the results.

LEMMA 1. Let $q = 2^{n}Q$, $n \geq 2$, and $p = 2^{m}P$. Then

$$h_q(p) = (1/2)i\, q\, \chi^{\circ}(pq)\, E_Q(p)\, \delta_{n-m,2}.$$

LEMMA 2. Under the assumption of Lemma 1,

$$c_q(p;\chi) = -i\, 2^{n-1}\, \chi^{\circ}(pq)\, \delta_{n-m,2}\, c_Q(p).$$

LEMMA 3. If

$$g(s) = \sum_{n \geq 1} a_n n^{-s},$$

https://doi.org/10.4153/CMB-1968-019-2 Published online by Cambridge University Press

then

(i) $$g(s;e(h/k)) = \sum_{a \le k} e(ah/k)\, g(s;a,k);$$

(ii) $$g(s;b,k) = k^{-1} \sum_{a \le k} e(-ab/k)\, g(s;e(a/k));$$

(iii) $$g(s;b,k) = k^{-1} \sum_{q \mid k} \sum_{p(q)} e(-bp/q)\, g(s;e(p/q)).$$

4. The Functional Equation of $R(s;e(p/q))$.

THEOREM 1. For $\sigma < 0$ and $1 \le h \le k$,

$$L(s;e(h/k)) = (1/2)(\pi/2)^{s-1}\Gamma(1-s)\,[e(s/4)\,L'_{-\ell-1}(1-s;1-h^*/k) + e(-s/4)\,L_{\ell}(1-s;h^*/k)].$$

Proof. This follows directly from the functional equation of

$$\sum_{n \ge 0}{}' e(nx)\,(n+y)^{-s}$$

(see [5], pages 269 and 280). Here, x and y need not be integers.

THEOREM 2. If $(p,q) = 1$ with $1 \le p \le q$ and $p\bar{p} \equiv 1 \pmod q$, and if $\sigma > 1$, then

(i) $$R(s;e(p/q)) = \sum_{a,b \le q} e(abp/q)\,\zeta(s;a,q)\,L(s;b,q);$$

(ii) $$R(s;e(p/q)) = q^{-1} \sum_{a,b \le q} e(-ab\bar{p}/q)\,\zeta(s;e(a/q))\,L(s;e(b/q)).$$

Proof. (i) follows immediately from the definition of the left side. To prove (ii), apply Lemma 3(ii) to each term on the right side of (i), which gives:

$$R(s;e(p/q)) = q^{-2} \sum_{c,d \le q} \zeta(s;e(c/q))\,L(s;e(d/q)) \sum_{a,b \le q} e((abp-ac-bd)/q).$$

But the inner sum has value $q\,e(-cd\bar{p}/q)$, from which the result follows.

THEOREM 3. If $(p,q) = 1$ with $1 \le p \le q$ and $p\bar{p} \equiv 1 \pmod q$, and if $\sigma < 0$, then we have the following functional equation:

https://doi.org/10.4153/CMB-1968-019-2 Published online by Cambridge University Press

$$R(s;e(p/q)) = K_q(s)\chi(q)R(1-s;e(-\bar{4}\bar{p}/q)) \text{ if } q \equiv 1 \pmod 2 \text{ and } 4\bar{4} \equiv 1 \pmod q;$$

$$= 2^s K_q(s) R(1-s;e(\bar{p}R/q);\chi) \text{ if } q = 2Q \text{ and } 2R = Q - 1;$$

$$= -2iK_q(s)\chi(p)R(1-s;e(-\bar{p}/q)) \text{ if } q \equiv 0 \pmod 4,$$

where

$$R(s;e(p/q);\chi) = \sum_{n\geq 1} \chi(n) r(n) e(p/q) n^{-s}$$

and

$$K_q(s) = \pi^{2s-2} q^{1-2s} \Gamma^2(1-s) \sin \pi s.$$

Proof. Theorem 2(ii), together with Theorem 1 and the functional equation of $\zeta(s;e(b/q))$ (see [5], page 269), gives the following functional equation:

$$(2) \qquad R(s;e(p/q)) = K_q(s) q^{s-1} \sum_{a,\, b \leq q} e(-ab\bar{p}/q) L_\ell(1-s;a^*/q)\zeta(1-s;b,q)$$

where $4a = \ell q + a^*$ with $1 \leq a^* \leq q$.

Case 1. For q odd,

$$L_\ell(1-s;a^*/q) = q^{1-s}\chi(q)\, L(1-s;4a,q),$$

so that, by (2), we have

$$R(s;e(p/q)) = K_q(s)\chi(q) \sum_{a,\, b \leq q} e(-ab\bar{4}\bar{p}/q)\, L(1-s;a,q)\zeta(1-s;b,q).$$

Now compare this result with Theorem 2(i).

Case 2. For $q = 2Q$, Q odd,

$$L_\ell(1-s;a^*/q) = \chi(Q)\, Q^{1-s}\, L_{2a}(1-s;2a,Q),$$

so that, by (2), we have

$$R(s;e(p/q)) = K_q(s)2^{s-1}\chi(Q) \sum_{a,\, b \leq q} e(-ab\bar{p}/q)\, L_{2a}(1-s;2a,Q)\zeta(1-s;b,q)$$

$$= K_q(s)2^{s-1}\chi(Q) \sum_{a \leq q} L_{2a}(1-s;2a,Q)\zeta(1-s;e(-a\bar{p}/q))$$

$$= K_q(s)2^{s-1}\chi(Q) \sum_{n\geq 1} n^{s-1} \Sigma_n,$$

https://doi.org/10.4153/CMB-1968-019-2 Published online by Cambridge University Press

where

$$\Sigma_n = \sum_{a \le q} e(-an\bar{p}/q)\, L_{2a}(1-s;2a,Q).$$

Now split the last sum into two parts, the first part with $1 \le a \le Q$ and $Q+1 \le a \le 2Q$ for the second part. In the second sum, replace a by $Q+a$, and note that

$$L_{2a}(1-s;2a,Q) = (-1)^a L(1-s;2a,Q)$$

and

$$1 - (-1)^n = 2\chi^2(n).$$

Then

$$\Sigma_n = 2\chi^2(n) \sum_{a \le Q} e(-an\bar{p}/q)\,(-1)^a L(1-s;2a,Q)$$

$$= 2\chi^2(n) \sum_{a \le Q} e(an\bar{p}R/Q)\, L(1-s;2a,Q),$$

since $(-1)^a = e(-an\bar{p}/2)$ for n odd, and $2R = Q-1$, where R is an integer. Hence

$$\Sigma_n = 2\chi^2(n)\chi(Q)L(1-s;e(n\bar{p}R/q)),$$

so that

$$R(a;e(p/q)) = 2^s K_q(s) \sum_{n \ge 1} \chi^2(n)\, n^{s-1} L(1-s;e(n\bar{p}R/q)),$$

from which the result follows.

Case 3. For $q \equiv 0 \pmod 4$,

$$L(s;b,q) = \chi(b)\zeta(s;b,q),$$

so that, by Theorem 2(i), we have

$$(3)\quad R(s;e(p/q)) = \sum_{a,b \le q} e(abp/q)\chi(b)\zeta(s;a,q)\zeta(s;b,q)$$

$$(4)\quad = q^{-1}\chi(p) \sum_{a,b \le q} \chi(a)\, e(-ab\bar{p}/q)\zeta(s;e(a/q))\zeta(s;e(b/q)).$$

In (3), we apply the functional equation of $\zeta(s;w)$, and after expanding, we replace a by $q-a$ and b by $q-b$ in the appropriate sums, noting

https://doi.org/10.4153/CMB-1968-019-2 Published online by Cambridge University Press

that in replacing b by q-b, $\chi(b)$ becomes $-\chi(b)$. Consequently, two of the sums cancel and we are left with

$$R(s;e(p/q)) = -i q^{-1} K_q(s) \sum_{a,\, b \le q} e(ab\bar{p}/q)\chi(a)\zeta(1-s;e(a/q))\zeta(1-s;e(b/q)).$$

The result follows upon comparing this with (4).

5. The Meromorphic Part of $R(s;b,k)$.

THEOREM 4. *$L(s;c,q)$ is analytic in the entire finite plane if $q \not\equiv 0 \pmod 4$. If $q \equiv 0 \pmod 4$, then $L(s;c,q) = \chi(c)\,\zeta(s;c,q)$, and so has a simple pole at $s = 1$ if c is odd, and is identically zero if c is even.*

Proof. The second part of the Theorem is obvious. For $q \not\equiv 0 \pmod 4$, $L(s;b,q)$ is essentially the difference of two ζ-functions of the form $\zeta(s;w)$, each of which has the meromorphic part $(s-1)^{-1}$, so that the difference of two such functions is analytic everywhere in the s-plane.

THEOREM 5. *If $q \not\equiv 0 \pmod 4$ and $(p,q) = 1$, then $R(s;e(p/q))$ has the same meromorphic part as*

$$q^{1-2s}\chi(q)\zeta(s)\,L(s).$$

Proof. From Theorem 2(i),

$$R(s;e(p/q)) - \zeta(s;q,q) \sum_{a,\, c \le q} e(acp/q)\, L(s;c,q)$$

$$= \sum_{a,\, c \le q} e(acp/q)\,[\zeta(s;a,q) - \zeta(s;q,q)]\, L(s;c,q).$$

Since $\zeta(s;a,q) - \zeta(s;q,q)$ is analytic in the entire s-plane, and also $L(s;c,q)$ by Theorem 4, then $R(s;e(p/q))$ has the same meromorphic part as:

$$\zeta(s;q,q) \sum_{a,\, c \le q} e(acp/q)\, L(s;c,q)$$

$$= q^{1-s}\zeta(s)\, L(s;q,q),$$

from which the result follows.

THEOREM 6. *If $q \equiv 0 \pmod 4$ and $(p,q) = 1$, then $R(s;e(p/q))$ has the same meromorphic part as:*

$$i\chi(p)\,(q/2)^{1-2s}\zeta(s)\,L(s).$$

https://doi.org/10.4153/CMB-1968-019-2 Published online by Cambridge University Press

Proof. From Theorems 2(i) and 4,

$$R(s;e(p/q)) = \sum_{a,\, c \le q} \chi(c)\, e(acp/q)[\zeta(s;q,q) - Z(s;a,q)][\zeta(s;q,q) - Z(s;c,q)],$$

where

$$Z(s;a,q) = \zeta(s;q,q) - \zeta(s;a,q),$$

which is analytic everywhere. Therefore

$$R(s;e(p/q)) = q^{-2s}\zeta^2(s)\Sigma_1 - q^{-s}\zeta(s)\,\Sigma_2 + \Sigma_3, \tag{5}$$

where

$$\Sigma_1 = \sum_{a,\, c \le q} \chi(c)\, e(acp/q),$$

$$\Sigma_2 = \sum_{a,\, c \le q} \chi(c)\, e(acp/q)[Z(s;a,q) + Z(s;c,q)],$$

and

$$\Sigma_3 = \sum_{a,\, c \le q} \chi(c)\, e(acp/q)\, Z(s;a,q)\, Z(s;c,q).$$

One easily shows that $\Sigma_1 = q\chi(q) = 0$. Since both Σ_2 and Σ_3 are analytic, the only possible singularity of $R(s;e(p/q))$ must arise from the second term of (5) so that we only need to evaluate Σ_2.

$$\Sigma_2 = -\sum_{a,\, c \le q} \chi(c)\, e(acp/q)\,[\zeta(s;c,q) + \zeta(s;a,q)]$$

$$= -q\chi(q)\,\zeta(s;q,q) - \sum_{a,\, c \le q} \chi(c) \sum_{m \ge 1} e(mcp/q)\, m^{-s}$$

using Lemma 3(i),

$$= -\sum_{m \ge 1} h_q(mp)\, m^{-s}$$

$$= -\sum_{m \ge 1} (1/2)i\, q\, \chi^{\circ}(pqm)\, E_Q(mp)\, \delta_{u-v,\,2}\, m^{-s}$$

by Lemma 1, where $q = 2^u Q$, $u \ge 2$, and for each $m \ge 1$, we write $m = 2^v M$,

$$= -i\, 2^{2s-1}\, q^{1-s}\, \chi(p)\, L(s).$$

https://doi.org/10.4153/CMB-1968-019-2 Published online by Cambridge University Press

THEOREM 7. R(s;b, k) has the same meromorphic part as:

$$k^{-1}\zeta(s)L(s)\,[1+\chi^{o}(b)\,e_{4b}(k)\,(2^{\nu+1})^{2-2s}]\sum_{q|k}\chi(q)c_q(b)\,q^{1-2s},$$

where $b = 2^{\nu}M$.

Proof. From Lemma 3(iii) and Theorems 5 and 6, R(s;b, k) has the same meromorphic part as:

$$k^{-1}\zeta(s)\,L(s)\,[\sum_{\substack{q|k\\ 4\nmid q}}\chi(q)\,q^{1-2s}\,c_q(b)+i\sum_{\substack{q|k\\ 4|q}}(q/2)^{1-2s}\,c_q(b;\chi)].$$

To complete the proof, use Lemma 2.

6. The Sum $\sum_{\substack{n\le X\\ n\equiv b(\mathrm{mod}\,k)}} r(n)$. Finally, we state the main results of this paper. We shall not give the proofs of Theorems 8 and 9, since the arguments run parallel to those given in Hooley's paper [3]. As in Hooley's paper, our results depend upon Weil's estimates for the Kloosterman sum.

THEOREM 8. If $k = O(X^{2/3})$ and $0 < \beta < 1/3$, then

$$\sum_{\substack{n\le X\\ n\equiv b(\mathrm{mod}\,k)}}(X-n)^2\,r(n) = \frac{\pi}{12}\tilde{H}_k(b)\frac{X^3}{k}+O(X^{2+\beta}k^{(1/2)(1-3\beta)}(b,k)^{(1/2)}d(k)).$$

Remark. In applying Theorem 8 to $\Sigma r(n)r(n+a)$, we want $\beta = 0$, in which case the error term becomes

$$O(X^2k^{-1/2}\log(k+1)\,(b,k)^{1/2}\,d(k)).$$

To obtain this result, we proceed as in [3], except that in estimating $J_q^{(1)}$ we move the line of integration to $\sigma = 0$ instead of to $\sigma = \beta$, noting that we must be careful at the origin.

THEOREM 9. Under the hypothesis of Theorem 8,

$$\sum_{\substack{n\le X\\ n\equiv b(\mathrm{mod}\,k)}} r(n) = \frac{\pi}{4}\tilde{H}_k(b)\frac{X}{k}+O(X^{(2/3)+\beta}k^{-(1/2)(1+3\beta)}(b,k)^{(1/2)}d(k)).$$

https://doi.org/10.4153/CMB-1968-019-2 Published online by Cambridge University Press

7. A Problem of Mordell. In [4], Mordell proved that if p is a prime, then there exist non-negative integers $x, y \leq B p^{3/4} \log p$ (B is a positive absolute constant) such that

$$ax^2 + by^2 \equiv c \pmod{p},$$

provided $abc \not\equiv 0 \pmod{p}$.

In Theorem 9, let $X = Bk^{3/2}$, where B is a suitable positive constant. Then it follows that if k is odd and contains only a bounded number of factors, then there exist non-negative integers $x, y \leq B_1 k^{3/4}$, not both zero, such that

$$x^2 + y^2 \equiv b \pmod{k}, \tag{6}$$

provided $(b, k) = 1$, say. This follows since, under the conditions on k, and for some positive constant $C < 1$, we have

$$\tilde{H}_k(b) = H_k(b) = \prod_{p \mid k} \left(1 - \frac{\chi(p)}{p}\right) > C.$$

(6) is slightly sharper than Mordell's result when $a = b = 1$ and $k = p$. To lower the exponent in (6) below 3/4 would be of great interest, but seems very difficult.

REFERENCES

1. T. Estermann, An asymptotic formula in the theory of numbers, Proc. London Math. Soc. (2) 34 (1932) 280-292.

2. _____, On the representations of a number as the sum of two products, Proc. London Math. Soc. (2) 31 (1930) 123-133.

3. C. Hooley, An asymptotic formula in the theory of numbers, Proc. London. Math. Soc. (3) 7 (1957) 396-413.

4. L. J. Mordell, On the number of solutions in incomplete residue sets of quadratic congruences, Arch. der Math. 8(1957) 153-157.

5. Whittaker and Watson, Modern Analysis (4th edition, London, Cambridge, 1958).

University of Toronto