6

The singular series continued

We now prove the result mentioned in connection with the Corollary to Lemma 3.1, namely that

$$|S_{a,q}| \ll q^{1-1/k}. \tag{6.1}$$

This implies that

$$|A(q)| \ll q^{1-s/k},$$

from which it follows that the singular series is absolutely convergent if $s \geq 2k+1$. Also (5.8) of Chapter 5 and the Corollary to Lemma 5.2, both hold under the same condition.

Lemma 6.1. *If* $a \not\equiv 0 \pmod{p}$ *and* $\delta = (k, p-1)$ *then*

$$|S_{a,p}| \leq (\delta - 1)p^{1/2}. \tag{6.2}$$

Proof. Since $x^k \equiv m \pmod{p}$ has the same number of solutions as $x^\delta \equiv m \pmod{p}$, we have

$$S_{a,p} = \sum_x e\left(\frac{a}{p}x^\delta\right).$$

Let χ be a primitive character (mod p) of order δ. Then the number of solutions of $x^\delta \equiv t \pmod{p}$ is

$$1 + \chi(t) + \cdots + \chi^{\delta-1}(t).$$

Hence

$$S_{a.p} = \sum_t \left\{1 + \chi(t) + \cdots + \chi^{\delta-1}(t)\right\} e\left(\frac{a}{p}t\right), \tag{6.3}$$

where here (and elsewhere in this proof) summations are over a complete set of residues modulo p. The sum arising from the term 1 in the bracket is 0, since $a \not\equiv 0 \pmod{p}$.

If ψ is any non-principal character (mod p), the sum

$$T(\psi) = \sum_t \psi(t) e\left(\frac{at}{p}\right)$$

is called a Gauss sum, to commemorate the important part played by such sums in Gauss's work on cyclotomy. We can easily prove that $|T(\psi)| = p^{1/2}$, as follows. We have

$$|T(\psi)|^2 = \sum_t \sum_u \psi(t)\overline{\psi}(u) e\left(\frac{a}{p}(t-u)\right).$$

Here we can omit $u = 0$, since $\psi(0) = 0$. Changing the variable from t to v, where $t \equiv vu \pmod{p}$, we obtain

$$|T(\psi)|^2 = \sum_v \sum_{u \neq 0} \psi(v) e\left(\frac{au}{p}(v-1)\right).$$

The inner sum is $p-1$ if $v = 1$ and is $-\psi(v)$ otherwise. Hence

$$|T(\psi)|^2 = p\psi(1) - \sum_v \psi(v) = p.$$

This is the result stated earlier. Using this in (6.3) for $\psi = \chi, \ldots, \chi^{\delta-1}$ we obtain (6.2). □

Note. (6.2) remains valid if $p = 2$ (so that $\delta = 1$), but is then trivial since $a = 1$ and $S_{1,2} = 1 + e^{i\pi} = 0$.

Lemma 6.2. *Suppose $a \not\equiv 0 \pmod{p}$ and $p \nmid k$. Then, for $1 < \nu \leq k$,*

$$S_{a,p^\nu} = p^{\nu-1}, \tag{6.4}$$

and for $\nu > k$,

$$S_{a,p^\nu} = p^{k-1} S_{a,p^{\nu-k}}. \tag{6.5}$$

Proof. In the definition

$$S_{a,p^\nu} = \sum_{x=0}^{p^\nu - 1} e\left(\frac{a}{p^\nu} x^k\right),$$

we put $x = p^{\nu-1}y + z$ where $0 \leq y < p$, $0 \leq z < p^{\nu-1}$. Then

$$x^k \equiv z^k + kp^{\nu-1} z^{k-1} y \pmod{p^\nu},$$

since $2(\nu-1) \geq \nu$. Hence

$$S_{a,p^\nu} = \sum_{z=0}^{p^{\nu-1}-1} \sum_{y=0}^{p-1} e\left(\frac{az^k}{p^\nu} + \frac{akz^{k-1}y}{p}\right).$$

Since $ak \not\equiv 0 \pmod{p}$, the inner sum is 0 unless $z \equiv 0 \pmod{p}$ in which case it is p. Hence, if $z = pw$

$$S_{a,p^\nu} = p \sum_{w=0}^{p^{\nu-2}-1} e\left(\frac{aw^k}{p^{\nu-k}}\right).$$

If $\nu \leq k$, all the terms in the last sum are 1, and we get $S_{a,p^\nu} = p^{\nu-1}$. If $\nu > k$, the general term is a periodic function of w with period $p^{\nu-k}$, whence

$$S_{a,p^\nu} = pp^{k-2} S_{a,p^{\nu-k}}.$$

This proves the two results. (Note again that p may be 2.) □

Lemma 6.3. *The second result of Lemma 6.2 holds also when $p \mid k$.*

Proof. Put $k = p^\tau k_0$, as earlier, and note that since $\nu > k$ we have

$$\nu > p^\tau k_0 \geq 2^\tau \geq \tau + 1,$$

whence $\nu \geq \tau + 2$. Indeed, $k \geq \tau + 2$, since $k \geq 6$ if $\tau = 1$.

We modify the previous proof by putting

$$x = p^{\nu-\tau-1}y + z, \quad 0 \leq y < p^{\tau+1}, \quad 0 \leq z < p^{\nu-\tau-1}.$$

We shall prove that

$$x^k \equiv z^k + kp^{\nu-\tau-1}z^{k-1}y \pmod{p}. \tag{6.6}$$

Assuming this, the proof can be completed as before. For then

$$S_{a,p^\nu} = \sum_{z=0}^{p^{\nu-\tau-1}-1} \sum_{y=0}^{p^{\tau+1}-1} e\left(\frac{az^k}{p^\nu} - \frac{ak_0z^{k-1}y}{p}\right),$$

and again the inner sum is 0 unless $z \equiv 0 \pmod{p}$, whence

$$\begin{aligned} S_{a,p^\nu} &= p^{\tau+1} \sum_{w=0}^{p^{\nu-\tau-2}-1} e\left(\frac{aw^k}{p^{\nu-k}}\right) \\ &= p^{\tau+1}p^{k-\tau-2}S_{a,p^{\nu-k}}. \end{aligned}$$

This proves (6.5). It remains to prove the congruence (6.6). It will suffice to prove that

$$(z + p^{\nu-\tau-1}y)^{p^\tau} \equiv z^{p^\tau} + p^{\nu-1}z^{p^\tau-1}y \pmod{p^\nu}$$

since the further operation of raising both sides to the power k_0 presents no difficulty. Putting $\nu - \tau - 1 = \lambda$, we have to prove that

$$(z + p^\lambda y)^{p^\tau} \equiv z^{p^\tau} + p^{\lambda+\tau}z^{p^\tau-1}y \pmod{p^{\lambda+\tau+1}}. \tag{6.7}$$

This is not quite as immediate as it might appear, because not all the binomial coefficients in the expansion of $(A + B)^{p^\tau}$ are divisible by p^τ. However, we can prove the result in stages (or in other words by induction on τ). We prove first that

$$(z + p^\lambda y)^p \equiv z^p + p^{\lambda+1}z^{p-1}y \pmod{p^{\lambda+2}} \tag{6.8}$$

provided $\lambda \geq 1$ (if $p > 2$) or $\lambda \geq 2$ (if $p = 2$). The only term which needs examination in the binomial expansion is the last; for this we need $\lambda p \geq \lambda + 2$, and this is true if $\lambda \geq 1$ when $p > 2$, or if $\lambda \geq 2$ when $p = 2$.

Finally (6.7) follows by repetition from (6.8); at the next stage we obtain

$$\begin{aligned}(z + p^\lambda y)^{p^2} &= (z^p + p^{\lambda+1}z^{p-1}y_1)^p \\ &\equiv z^{p^2} + p^{\lambda+2}z^{p^2-1}y_1 \pmod{p^{\lambda+3}} \\ &\equiv z^{p^2} + p^{\lambda+2}z^{p^2-1}y \pmod{p^{\lambda+3}},\end{aligned}$$

where $y_1 \equiv y \pmod{p}$, and we have applied (6.8) with $\lambda + 1$ in place of λ. The argument continues, and gives (6.7).

The conditions on λ are satisfied when $\lambda = \nu - \tau - 1$. We have already seen that $\nu - \tau - 1 \geq 1$, and if $p = 2$ we have $\nu \geq k + 1 \geq \tau + 3$, as noted earlier. Thus the proof is complete. □

Lemma 6.4. $|S_{a,q}| \ll q^{1-1/k}$ *for* $(a, q) = 1$.

Proof. Put $T(a, q) = q^{-1+1/k}S_{a,q}$. We have to prove that $T(a, q)$ is bounded independently of q. If $q = p_1^{\nu_1}p_2^{\nu_2}\cdots$, then by the multiplicative property of $S_{a,q}$ in the proof of Lemma 5.1, we have

$$T(a, q) = T(a_1, p_1^{\nu_1})T(a_2, p_2^{\nu_2})\cdots,$$

for suitable $a_1, a_2, \ldots$, each of which is relatively prime to the corresponding p^ν. By the second part of Lemma 6.2 and Lemma 6.3, we have

$$T(a, p^\nu) = T(a, p^{\nu-k})$$

for $\nu > k$, so we can suppose all v_i are $\leq k$.

By Lemma 6.1,

$$T(a,p) \leq kp^{1/2}p^{-(1-1/k)} \leq kp^{-1/6}$$

and by the first part of Lemma 6.2,

$$T(a,p^\nu) = p^{\nu-1}p^{-\nu(1-1/k)} \leq 1 \quad \text{for } 1 < \nu \leq k.$$

Hence $T(a,p^\nu) \leq 1$ except possibly if $\nu = 1$ and $p \leq k^6$. Hence

$$T(a,q) \leq \prod_{p \leq k^6} (kp^{-1/6}),$$

and the number on the right is independent of q. □

Theorem 6.1. *The singular series* $\mathfrak{S}(N)$ *and the product* $\prod_p \chi(p)$ *are absolutely convergent if* $s \geq 2k+1$ *and*

$$\mathfrak{S}(N) \geq C_1(k,s) > 0$$

if $s \geq 2k+1$ *(k odd) or* $s \geq 4k$ *(k even).*

Proof. The absolute convergence follows as before, using Lemma 6.4 in place of the Corollary to Lemma 3.1, and the final assertion follows from Lemma 5.6 and the Corollary to Lemma 5.2. □

Theorem 6.1 shows that there would be no difficulty in improving on the condition $s \geq 2^k + 1$ for the validity of the asymptotic formula, as far as the singular series alone is concerned (except when $k = 4$). The crux of the difficulty is with the minor arcs, and not with the singular series.

Note. Hardy and Littlewood proved that the singular series, in the form $\sum_{q=1}^{\infty} A(q)$, is absolutely convergent for $s \geq 4$, and the same applies to the product form. The essential idea is to make sure of the cancellation which occurs in the summation over a in

$$\sum_{\substack{a=1 \\ (a,q)=1}}^{q} (q^{-1}S_{a,q})^s e\left(\frac{-Na}{q}\right).$$

The absolute convergence is, however, no longer uniform in N. If the absolute value of $q^{-1}S_{a,q}$ is taken, the condition $s \geq 2k+1$ of Theorem 6.1 is best possible.

It is an interesting question how the sum $\mathfrak{S}(N)$ of the singular series fluctuates with N. Each factor $\chi(p)$ depends mainly on the residue class (mod p^γ) to which N belongs. The factors which fluctuate most as N varies are those for which p divides k, but those for which $p-1$ has a large factor in common with k may also fluctuate appreciably.

In their early papers, Hardy and Littlewood worked mainly with the definition of $\mathfrak{S}(N)$ in terms of the exponential sums $S_{a,q}$, rather than with the expression in terms of congruences (mod p^ν). In P.N. II [38] they had to prove that $\mathfrak{S}(N)$ has a positive lower bound in the case $k=4$, $s=21$. The factors $\chi(p)$ which fluctuate most as N varies are in this case $\chi(2)$ and $\chi(5)$; the product of all the others does not differ appreciably from 1. They found that $\chi(5)$ varies between about 0.7 and 1.3. But $\chi(2)$ varies by a factor of about 200. Hardy and Littlewood showed that (in the particular case mentioned)

$$\begin{aligned}\chi(2) \quad = \quad & 1 - 1.3307 \cos\frac{(2N-5)\pi}{16} + 0.415 \cos\frac{(6N+1)\pi}{16} \\ & -0.3793 \cos\frac{(2N+3)\pi}{8} + \varepsilon(N),\end{aligned}$$

where $|\varepsilon(N)| < 0.002$. It can be verified that $\chi(2)$ becomes very small (but still positive) when $N \equiv 2$ or $3 \pmod{16}$. It is relatively large when $N \equiv 10$ or $11 \pmod{16}$. These results correspond to the fact that $x^4 \equiv 0$ or $1 \pmod{16}$, and that consequently the choices for $x_1, \ldots, x_{21}$ in $x_1^4 + \cdots + x_{21}^4 \equiv N \pmod{16}$ are much more restricted in the one case than in the other.