5

Waring's problem: the singular series

We now study the singular series:

$$\mathfrak{S}(N) = \sum_{q=1}^{\infty} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} \left(q^{-1}S_{a,q}\right)^s e(-aN/q). \tag{5.1}$$

We shall find that the value of $\mathfrak{S}(N)$ is closely related to the number of solutions of the congruences

$$x_1^k + \cdots + x_s^k \equiv N \pmod{q}$$

for all positive integers q, and indeed $\mathfrak{S}(N) = 0$ if any such congruence is insoluble. This might be expected from the appearance of the asymptotic formula, since then $r(N) = 0$.

We write

$$\mathfrak{S}(N) = \sum_{q=1}^{\infty} A(q), \quad A(q) = \sum_{\substack{a=1 \\ (a,q)=1}}^{q} \left(q^{-1}S_{a,q}\right)^s e(-aN/q). \tag{5.2}$$

Lemma 5.1. *If* $(q_1, q_2) = 1$, *then*

$$A(q_1q_2) = A(q_1)A(q_2). \tag{5.3}$$

Proof. Write

$$f(a,q) = (S_{a,q})^s e(-aN/q).$$

We shall prove that if $(a_1, q_1) = (a_2, q_2) = 1$ and

$$\frac{a}{q} \equiv \frac{a_1}{q_1} + \frac{a_2}{q_2} \pmod{1}, \quad q = q_1q_2, \tag{5.4}$$

then

$$f(a,q) = f(a_1,q_1)f(a_2,q_2). \tag{5.5}$$

This will suffice to give the result, for the relation (5.4) sets up a 1-to-1 correspondence between reduced residue classes $a \pmod q$ and pairs of reduced residue classes $a_1 \pmod{q_1}$ and $a_2 \pmod{q_2}$, whence

$$\sum_{\substack{a=1\\(a,q)=1}}^{q} f(a,q) = \left(\sum_{\substack{a_1=1\\(a_1,q_1)=1}}^{q_1} f(a_1,q_1)\right)\left(\sum_{\substack{a_2=1\\(a_2,q_2)=1}}^{q_2} f(a_2,q_2)\right).$$

To prove (5.5), we use a somewhat similar argument, but with complete sets of residues. Putting

$$\frac{z}{q} \equiv \frac{z_1}{q_1} + \frac{z_2}{q_2} \pmod 1,$$

we have

$$S_{a,q} = \sum_{z=1}^{q} e(az^k/q) = \sum_{z_1=1}^{q_1}\sum_{z_2=1}^{q_2} e\left(\frac{a}{q}q^k\left(\frac{z_1}{q_1}+\frac{z_2}{q_2}\right)^k\right),$$

and since

$$\frac{a}{q}q^k\left(\frac{z_1}{q_1}+\frac{z_2}{q_2}\right)^k \equiv \frac{a_1}{q_1}(q_2z_1)^k + \frac{a_2}{q_2}(q_1z_2)^k \pmod 1,$$

we get

$$\begin{aligned} S_{a,q} &= \sum_{z_1=1}^{q_1} e\left(\frac{a_1}{q_1}(q_2z_1)^k\right)\sum_{z_2=1}^{q_2} e\left(\frac{a_2}{q_2}(q_1z_2)^k\right) \\ &= S_{a_1,q_1}S_{a_2,q_2}. \end{aligned}$$

Since, in addition

$$e\left(-\frac{a}{q}N\right) = e\left(-\frac{a_1}{q_1}N\right)e\left(-\frac{a_2}{q_2}N\right),$$

we obtain (5.5). □

Note. This result of this lemma is in no way dependent on the fact that $S_{a,q}$ is formed with the special polynomial z^k. We could replace z^k

with any polynomial $f(z)$ with integral coefficients, and indeed we could replace $S_{a,q}$ with a multiple exponential sum

$$\sum e\left(\frac{a}{q}f(z_1,\dots,z_n)\right),$$

where each of $z_1,\dots,z_n$ runs through a complete set of residues (mod q). The proof is just the same.

Lemma 5.2. *If $s \geq 2^k + 1$, we have*

$$\mathfrak{S}(N) = \prod_p \chi(p), \tag{5.6}$$

where

$$\chi(p) = 1 + \sum_{\nu=1}^{\infty} A(p^\nu). \tag{5.7}$$

Also

$$|\chi(p) - 1| \ll p^{-1-\delta} \tag{5.8}$$

for some fixed $\delta > 0$.

Proof. It follows from Lemma 5.1 that if $q = p_1^{\nu_1} p_2^{\nu_2} \cdots$ then

$$A(q) = A\left(p_1^{\nu_1}\right) A\left(p_2^{\nu_2}\right) \cdots .$$

Hence

$$\mathfrak{S}(N) = \sum_{q=1}^{\infty} A(q) = \prod_p \left\{ \sum_{\nu=0}^{\infty} A(p^\nu) \right\} = \prod_p \chi(p),$$

and this is justified by the convergence of $\sum |A(q)|$, which was proved in the preceding chapter.

We already had the estimate

$$|A(q)| \ll q^{-1-1/K+\varepsilon} \ll q^{-1-\delta},$$

and this implies

$$|\chi(p) - 1| \ll \sum_{\nu=1}^{\infty} p^{-\nu(1+\delta)} \ll p^{-1-\delta},$$

which is (5.8). □

Corollary. *If $s \geq 2^k + 1$ there exists $p_0 = p_0(k)$ such that*

$$\frac{1}{2} \leq \prod_{p > p_0} \chi(p) \leq \frac{3}{2}.$$

This follows at once from (5.8), since we can take δ to depend on k only. Again, we shall see that the result holds if $s \geq 2k + 1$.

Definition. Let $M(q)$ denote the number of solutions of the congruence

$$x_1^k + \cdots + x_s^k \equiv N \pmod{q},$$

with $0 < x_1, \ldots, x_s \leq q$.

Lemma 5.3. *We have*

$$1 + \sum_{\nu=1}^{n} A(p^\nu) = M(p^n)/p^{n(s-1)}, \tag{5.9}$$

and consequently

$$\chi(p) = \lim_{n \to \infty} M(p^n)/p^{n(s-1)}. \tag{5.10}$$

Proof. We can express $M(q)$ in terms of exponential sums by a procedure which can be regarded as an arithmetical analogue of that used to express $r(N)$ as an integral in (2.7). We have

$$M(q) = q^{-1} \sum_{t=1}^{q} \sum_{x_1=1}^{q} \cdots \sum_{x_s=1}^{q} e\left(\frac{t}{q}\left(x_1^k + \cdots + x_s^k - N\right)\right),$$

since the sum over t gives q if the congruence is satisfied and 0 otherwise. We collect together those values of t which have the same highest common factor with q. If this highest common factor is denoted by q/q_1, the values of t in question are uq/q_1, where $1 \leq u \leq q_1$ and $(u, q_1) = 1$. Hence

$$M(q) = q^{-1} \sum_{q_1 | q} \sum_{\substack{u=1 \\ (u, q_1) = 1}}^{q_1} \sum_{x_1=1}^{q} \cdots \sum_{x_s=1}^{q} e\left(\frac{u}{q_1}\left(x_1^k + \cdots + x_s^k - N\right)\right).$$

Now

$$\sum_{x=1}^{q} e\left(\frac{u}{q_1} x^k\right) = \frac{q}{q_1} \sum_{x=1}^{q_1} e\left(\frac{u}{q_1} x^k\right) = \frac{q}{q_1} S_{u, q_1}.$$

Thus

$$M(q) = q^{-1} \sum_{q_1 | q} \sum_{\substack{u=1 \\ (u,\, q_1)=1}}^{q_1} \left(\frac{q}{q_1}\right)^s (S_{u,q_1})^s e\left(-\frac{uN}{q_1}\right)$$
$$= q^{s-1} \sum_{q_1 | q} A(q_1).$$

This formula, when $q = p^n$, becomes (5.9), and (5.10) follows from it. □

Note. For each particular N, the series on the left of (5.9) terminates, and therefore (5.10) is true without the limiting operation for all sufficiently large n. However the point at which the series terminates depends on N, as well as on k and p.

Definition. For each prime p, let p^τ be the highest power of p dividing k, and put $k = p^\tau k_0$. Define γ by

$$\gamma = \begin{cases} \tau + 1 & \text{if} \quad p > 2, \\ \tau + 2 & \text{if} \quad p = 2. \end{cases} \tag{5.11}$$

Of course, γ depends on both p and k.

Lemma 5.4. *If the congruence* $y^k \equiv m \pmod{p^\gamma}$ *is soluble where* $m \not\equiv 0 \pmod{p}$*, then the congruence* $x^k \equiv m \pmod{p^\nu}$ *is soluble for every* $\nu > \gamma$.

Proof. *Suppose* $p > 2$. The relatively prime residue classes (mod p^ν) form a cyclic group of order $\phi(p^\nu) = p^{\nu-1}(p-1)$, being represented by the powers of a primitive root g to the modulus p^ν. If $\nu > \gamma$, then g is necessarily also a primitive root to the modulus p^γ.

Write

$$m \equiv g^\mu, \quad y \equiv g^\eta, \quad x \equiv g^\xi \pmod{p^\nu}.$$

Then the hypothesis that $y^k \equiv m \pmod{p^\gamma}$ is equivalent to

$$k\eta \equiv \mu \pmod{p^{\gamma-1}(p-1)}.$$

Since $k = p^\tau k_0$ and $\tau = \gamma - 1$, it follows that μ is divisible by $p^{\gamma-1}$ and also by $(k_0, p-1)$. But now we can find ξ to satisfy

$$k\xi \equiv \mu \pmod{p^{\nu-1}(p-1)},$$

since μ is divisible by the highest common factor of k and $p^{\nu-1}(p-1)$. The last congruence is equivalent to $x^k \equiv m \pmod{p^\nu}$.

Suppose $p = 2$. First, if $\tau = 0$, so that k is odd, there is no problem. For as x runs through a reduced set of residues to the modulus 2^ν then so does x^k, and the congruence $x^k \equiv m \pmod{2^\nu}$ is soluble for any odd m without any hypothesis.

Now suppose $\tau \geq 1$. Since $k = 2^\tau k_0$ is even, we have $x^k \equiv 1 \pmod 4$ for all x. Those residue classes $(\mathrm{mod}\ 2^\nu)$ that are $\equiv 1 \pmod 4$ constitute a cyclic group of order $2^{\nu-2}$, and it is well known that 5 is a generating element, i.e. a primitive root. As before, write

$$m \equiv 5^\mu, \quad y \equiv 5^\eta, \quad x \equiv 5^\xi \pmod{2^\nu}.$$

Then the hypothesis is equivalent to

$$k\eta \equiv \mu \pmod{2^{\gamma-2}}.$$

Since $k = 2^\tau k_0$ and $\tau = \gamma - 2$, it follows that μ is divisible by 2^τ. Hence there exists ξ such that

$$k\xi \equiv \mu \pmod{2^{\nu-2}},$$

which implies that $x^k \equiv m \pmod{2^\nu}$. This completes the proof of Lemma 5.4. □

Lemma 5.5. *If the congruence*

$$x_1^k + \cdots + x_s^k \equiv N \pmod{p^\gamma}$$

has a solution with $x_1, \ldots, x_s$ *not all divisible by* p, *then*

$$\chi(p) > 0.$$

Proof. Suppose $a_1^k + \cdots + a_s^k \equiv N \pmod{p^\gamma}$ and $a_1 \not\equiv 0 \pmod p$. We can obtain many solutions of $x_1^k + \cdots + x_s^k \equiv N \pmod{p^\nu}$ for $\nu > \gamma$ by the following construction. We choose $x_2, \ldots, x_s$ arbitrarily, subject to

$$x_j \equiv a_j \pmod{p^\gamma}, \quad 0 < x_j \leq p^\nu.$$

These choices are possible in $p^{(\nu-\gamma)(s-1)}$ ways. Then choose x_1 to satisfy

$$x_1^k \equiv N - x_2^k - \cdots - x_s^k \pmod{p^\nu};$$

this is possible by Lemma 5.4 because the expression on the right is

$\equiv a_1^k \pmod{p^\nu}$ and $a_1 \not\equiv 0 \pmod{p}$. Thus, in the notation introduced earlier, we have

$$M(p^\nu) \geq p^{(\nu-\gamma)(s-1)} = C_p p^{\nu(s-1)},$$

where $C_p = p^{-\gamma(s-1)} > 0$. By (5.10) of Lemma 5.3, this implies $\chi(p) > 0$. □

Lemma 5.6. *If $s \geq 2k$ (k odd) or $s \geq 4k$ (k even), then $\chi(p) > 0$ for all primes p and all N.*

Proof. By Lemma 5.5 it suffices to prove that the congruence

$$x_1^k + \cdots + x_s^k \equiv N \pmod{p^\gamma} \tag{5.12}$$

is soluble with $x_1, \ldots, x_s$ not all divisible by p. If $N \not\equiv 0 \pmod{p}$, the latter requirement is necessarily satisfied. If $N \equiv 0 \pmod{p}$, it will suffice to solve the congruence

$$x_1^k + \cdots + x_{s-1}^k + 1^k \equiv N \pmod{p^\gamma}.$$

Hence (replacing $s-1$ by s) we see that it suffices to prove the solubility of (5.12) when $N \not\equiv 0 \pmod{p}$ for $s \geq 2k-1$ (k odd) or $s \geq 4k-1$ (k even).

Suppose $p > 2$. We consider all N satisfying

$$0 < N < p^\gamma, \quad N \not\equiv 0 \pmod{p},$$

their number being $\phi(p^\gamma) = p^{\gamma-1}(p-1)$. Let $s(N)$ denote the least s for which (5.12) is soluble. If $N \equiv z^k N' \pmod{p^\gamma}$, then obviously $s(N) = s(N')$. Hence if we distribute the numbers N into classes according to the value of $s(N)$, the number in each class is at least equal to the number of distinct values assumed by z^k when $z \not\equiv 0 \pmod{p}$. By putting $z \equiv g^\zeta \pmod{p^\gamma}$, where g is a primitive root $\pmod{p^\gamma}$, and $a \equiv g^\alpha \pmod{p^\gamma}$, one easily sees that the congruence $z^k \equiv a \pmod{p^\gamma}$ is soluble if and only if α is divisible by $p^\tau \delta$ where $\delta = (k, p-1)$. Since $\tau = \gamma - 1$, the number of distinct values for $\alpha \pmod{p^{\gamma-1}(p-1)}$, which is also the number of distinct values for $a \pmod{p^\gamma}$, is

$$\frac{p^{\gamma-1}(p-1)}{p^{\gamma-1}\delta} = \frac{p-1}{\delta} = r,$$

say. Hence each class of values of N includes at least r elements.

Let us enumerate first all N for which $s(N) = 1$:

$$N_1^{(1)} < N_2^{(1)} < \cdots < N_{r_1}^{(1)}, \quad \text{where } r_1 \geq r.$$

Then we enumerate all N for which $s(N) = 2$:

$$N_1^{(2)} < N_2^{(2)} < \cdots < N_{r_2}^{(2)}, \quad \text{where } r_2 \geq r,$$

and so on. Some of these sets may be empty, but we shall prove that two consecutive sets cannot be empty.

Consider the least $N' \not\equiv 0 \pmod{p}$ which is not in any of the first $j-1$ sets. Then either $N'-1$ or $N'-2$ is $\not\equiv 0 \pmod{p}$, and being less than N' it must be in one of the first $j-1$ sets. Representing N' as

$$(N'-1) + 1^k \qquad \text{or} \qquad (N'-2) + 1^k + 1^k,$$

we deduce that $s(N') \leq j+1$. Hence the sets for which $s(N) = j$, $s(N) = j+1$ cannot both be empty.

Suppose the last set in the enumeration is that for which $s(N) = m$. Then at least $\frac{1}{2}(m-1)$ of the first $m-1$ sets are not empty, and also the mth set is not empty, making at least $\frac{1}{2}(m+1)$ non-empty sets. Since each set contains at least r numbers, we have

$$\tfrac{1}{2}(m+1)r \leq \phi(p^\gamma) = p^{\gamma-1}(p-1),$$

whence

$$\begin{aligned}(m+1) \leq \frac{2p^{\gamma-1}(p-1)}{r} &= 2p^{\gamma-1}\delta \\ &= 2p^\tau(k_0, p-1) \leq 2k.\end{aligned}$$

Hence $m \leq 2k-1$, whence $s(N) \leq 2k-1$ for all N. Thus for $p > 2$, the congruence (5.12) is soluble for $s \geq 2k-1$.

Suppose $p = 2$. If $\tau = 0$, that is if k is odd, the congruence (5.12) is soluble for $N \not\equiv 0 \pmod{p}$ when $s = 1$, as was remarked in the proof of Lemma 5.4. This proves the conclusion of Lemma 5.6 since then the only significant restriction on s comes from the primes $p > 2$.

Now suppose $\tau \geq 1$, so that k is even. We can suppose without loss of generality that $0 < N < 2^\gamma$, since N is now odd. By taking all the x_j in (5.12) to be 0 or 1, we can certainly solve the congruence if $s \geq 2^\gamma - 1$. Now

$$2^\gamma - 1 = 2^{\tau+2} - 1 \leq 4k - 1.$$

Hence it suffices if $s \geq 4k-1$, and this proves the conclusion of Lemma 5.6 in the case when k is even. □

Note. Although the final argument might, at first sight, seem to be a crude one, we have in fact lost nothing if $k = 2^\tau$ and $\tau \geq 2$. For then

$x^{2^\tau} \equiv 1 \pmod{2^{\tau+2}}$ if x is odd, and $x^{2^\tau} \equiv 0 \pmod{2^{\tau+2}}$ if x is even, so the values of x^k are in this case simply 0 and 1.

Hardy and Littlewood defined $\Gamma(k)$ to be the least value of s such that the congruence (5.12) is soluble with $x_1, \ldots, x_s$ not all divisible by p, for all p and all N. In this notation, Lemma 5.6 states that $\Gamma(k) \leq 2k$ when k is odd and $\Gamma(k) \leq 4k$ when k is even. Hardy and Littlewood made a very detailed study of $\Gamma(k)$ in P.N.VIII [41].[1] In particular they determined all types of k for which $\Gamma(k) > k$. The first few values of $\Gamma(k)$ are

k	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$\Gamma(k)$	4	16	5	9	4	32	13	12	11	16	6	14	15	64

Theorem 5.1. *If* $s \geq 2^k + 1$ *then*

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

for all N.

Proof. The result follows from Lemma 5.6 and the Corollary to Lemma 5.2, since $2^k + 1 \geq 2k$ (k odd) and $2^k + 1 \geq 4k$ (k even, $k > 2$). □

Theorem 5.1 is a necessary supplement to Theorem 4.1, in that it shows that the main term in the asymptotic formula is $\gg N^{s/k-1}$, and that consequently, $r(N) \to \infty$ as $N \to \infty$.

In the present chapter I have followed for the most part Vinogradov's exposition [93, Chapter 2].[2] This is somewhat simpler than the original exposition of Hardy and Littlewood.

[1] See also Chowla [14].
[2] The case $p = 2$ of our Lemma 5.4 is inadvertently omitted by Vinogradov.