Chapter 11

The singular series

Recall that by Theorems 10.3 and 10.4 together provide us the estimate

$$R(n)=\mathfrak{S}(n)\Gamma\left(\frac{4}{3}\right)^9\frac{n^2}{2}+o(n^2), \tag{11.1}$$

where the singular series $\mathfrak{S}(n)$ was defined in Chapter 10 as

$$\mathfrak{S}(n)=\sum_{q=1}^{\infty}\frac{S(q)}{q^9},$$

with

$$S(q)=\sum_{\substack{1\leqslant a\leqslant q\\ \gcd(a,q)=1}}S(q,a)^9\mathrm{e}(-an/q),\quad S(q,a)=\sum_{m=1}^{q}\mathrm{e}(am^3/q).$$

The definition of the Gamma function shows that $\Gamma\left(\frac{4}{3}\right)>0$, hence if we could prove that $\mathfrak{S}(n)>0$ then the main result of our lectures, Theorem 8.1, would be established with

$$c=\frac{\mathfrak{S}(n)}{2}\Gamma\left(\frac{4}{3}\right)^9.$$

Our aim in this chapter is to prove $\mathfrak{S}(n)>0$ and furthermore to provide a conceptual description of $\mathfrak{S}(n)$. Define for each $q\in\mathbb{N}$,

$$M_n(q):=\#\{(x_1,\dots,x_9)\in(\mathbb{Z}\cap[1,q])^9 : x_1^3+\cdots+x_9^3\equiv n(\mathrm{mod}\ q)\},$$

where here and below, the x_i denote integers. For prime powers $q = p^k$ we might guess that for each of the p^{8k} choices for the variables $1 \leqslant x_1, \ldots, x_8 \leqslant p^k$ there exist at most 3 solutions of the cubic equation in the variable x_9,

$$x_1^3 + \cdots + x_9^3 \equiv n(\text{mod } p^k).$$

Hence it is natural to consider the following limit for every prime p,

$$\sigma_p(n) := \lim_{k \to \infty} \frac{M_n(p^k)}{p^{8k}}. \tag{11.2}$$

Theorem 11.1. *The limit* (11.2) *exists and is positive. Furthermore the infinite product* $\prod_p \sigma_p(n)$*, taken over all primes, converges absolutely to the singular series,*

$$\mathfrak{S}(n) = \prod_p \sigma_p(n).$$

The constants $\sigma_p(n)$ are called *p-adic Hardy–Littlewood* densities and, as (11.2) reveals, they are intimately connected to solving the equation

$$x_1^3 + \cdots + x_9^3 = n$$

modulo positive integers q. Of course, if there is some $q \in \mathbb{N}$ such that

$$x_1^3 + \cdots + x_9^3 \equiv n(\text{mod } q)$$

has no solutions for x_i then $R(n) = 0$. One interpretation of Theorem 11.1 is that it provides evidence for the *opposite*; namely that if $x_1^3 + \cdots + x_9^3 = n$ is soluble modulo every q then it can be solved in the integers. This is not true in general, a counterexample is given by

$$4x_1^2 + 25x_2^2 - 5x_3^2 = 1.$$

11.1 Relating $\mathfrak{S}(n)$ to $\sigma_p(n)$.

Lemma 11.2. *Let* q_1, q_2 *be coprime integers and let* $q := q_1 q_2$*. Then for all*

$$a_1 \in \mathbb{Z} \cap [1, q_1], \quad a_2 \in \mathbb{Z} \cap [1, q_2]$$

we have

$$S(q_1, a_1) S(q_2, a_2) = S(q, a),$$

where $a := a_1 q_2 + a_2 q_1$*.*

Proof. As the variable m_1 ranges through all residue classes (mod q_1) in the sum

$$S(q_1, a_1) = \sum_{m_1 (\text{mod } q_1)} \mathrm{e}\left(\frac{a_1 m_1^3}{q_1}\right)$$

we see that, due to the coprimality of q_1, q_2, the integers $m_1 q_2$ also cover all residue classes (mod q_1). Hence we may write

$$S(q_1, a_1) = \sum_{m_1 (\text{mod } q_1)} \mathrm{e}\left(\frac{a_1 (m_1 q_2)^3}{q_1}\right),$$

and the fact that for any positive integer q the function $\mathrm{e}(\frac{\cdot}{q})$ is periodic (mod q), allows us to write

$$S(q_1, a_1) = \sum_{m_1 (\text{mod } q_1)} \mathrm{e}\left(\frac{a_1 (m_1 q_2)^3}{q_1}\right) = \sum_{m_1 (\text{mod } q_1)} \mathrm{e}\left(\frac{a_1 (m_1 q_2 + m_2 q_1)^3}{q_1}\right).$$

A similar argument shows that

$$S(q_2, a_2) = \sum_{m_2 (\text{mod } q_2)} \mathrm{e}\left(\frac{a_2 (m_1 q_2 + m_2 q_1)^3}{q_2}\right).$$

Thus we are led to

$$S(q_1, a_1) S(q_2, a_2) = \sum_{\substack{m_1 (\text{mod } q_1) \\ m_2 (\text{mod } q_2)}} \mathrm{e}\left(\frac{a_1 (m_1 q_2 + m_2 q_1)^3}{q_1} + \frac{a_2 (m_1 q_2 + m_2 q_1)^3}{q_2}\right),$$

which equals

$$\sum_{\substack{m_1 (\text{mod } q_1) \\ m_2 (\text{mod } q_2)}} \mathrm{e}\left(\frac{(a_1 q_2 + a_2 q_1)(m_1 q_2 + m_2 q_1)^3}{q_1 q_2}\right).$$

We can see that as the variables m_1, m_2 range through all available residue classes (mod q_1) and (mod q_2) respectively, then the variable

$$m := m_1 q_2 + m_2 q_1$$

takes each residue class (mod $q_1 q_2$) once. Therefore the last sum equals

$$\sum_{m (\text{mod } q_1 q_2)} \mathrm{e}\left(\frac{(a_1 q_2 + a_2 q_1) m^3}{q_1 q_2}\right),$$

which concludes our proof. $\square$

Lemma 11.3. *The function $S(q)$ is multiplicative.*

Proof. Let q_1, q_2 be coprime positive integers. Then the sets

$$\{a_1 \in \mathbb{Z} \cap [1, q_1] : \gcd(a_1, q_1) = 1\} \times \{a_2 \in \mathbb{Z} \cap [1, q_2] : \gcd(a_2, q_2) = 1\}$$

and $\{a \in \mathbb{Z} \cap [1, q] : \gcd(a, q) = 1\}$ are in $1-1$ correspondence. This can be seen by mapping $(a_1 (\mathrm{mod}\ q_1), a_2 (\mathrm{mod}\ q_2))$ to $a (\mathrm{mod}\ q)$, where $a := a_1 q_2 + a_2 q_1$. Hence we may write

$$S(q) = \sum_{\substack{1 \leqslant a_1 \leqslant q_1 \\ \gcd(a_1, q_1)=1}} \sum_{\substack{1 \leqslant a_2 \leqslant q_2 \\ \gcd(a_2, q_2)=1}} S(q, a)^9 \mathrm{e}\left(-n \frac{(a_1 q_2 + a_2 q_1)}{q}\right).$$

The identity

$$\mathrm{e}\left(-n \frac{(a_1 q_2 + a_2 q_1)}{q}\right) = \mathrm{e}\left(-n \frac{a_1}{q_1}\right) \mathrm{e}\left(-n \frac{a_2}{q_2}\right)$$

and Lemma 11.2 allows us to deduce

$$S(q) = \left(\sum_{\substack{1 \leqslant a_1 \leqslant q_1 \\ \gcd(a_1, q_1)=1}} S(q_1, a_1)^9 \mathrm{e}\left(-n \frac{a_1}{q_1}\right) \right) \left(\sum_{\substack{1 \leqslant a_2 \leqslant q_2 \\ \gcd(a_2, q_2)=1}} S(q_2, a_2)^9 \mathrm{e}\left(-n \frac{a_2}{q_2}\right) \right),$$

which is sufficient. □

Recall that we have proved in Chapter 10 that $\mathfrak{S}(n)$ is an absolutely convergent series, a fact which, when combined with Lemma 11.3 shows that the Euler product of $\mathfrak{S}(n)$ is

$$\mathfrak{S}(n) = \prod_p \left(1 + \sum_{m=1}^{\infty} \frac{S(p^m)}{p^{9m}}\right) \tag{11.3}$$

and furthermore that for each prime p,

$$\lim_{k \to +\infty} \left(1 + \sum_{m=1}^{k} \frac{S(p^m)}{p^{9m}}\right) \quad \text{exists.} \tag{11.4}$$

Lemma 11.4. *For each prime p and $k \in \mathbb{N}$ we have*

$$1 + \sum_{m=1}^{k} \frac{S(p^m)}{p^{9m}} = \frac{M_n(p^k)}{p^{8k}}.$$

Proof. We begin by detecting solutions x_i of the equation

$$x_1^3 + \cdots + x_9^3 \equiv n (\text{mod } p^k)$$

using certain exponential functions. To this end observe that for each integer x we have

$$\frac{1}{p^k} \sum_{\alpha=1}^{p^k} \mathrm{e}\left(\alpha \frac{x}{p^k} \right) = \begin{cases} 1 & \text{if } x \equiv 0 (\text{mod } p^k), \\ 0 & \text{otherwise.} \end{cases}$$

Thus writing

$$M_n(p^k) = \sum_{1 \leqslant x_1, \dots, x_9 \leqslant p^k} a_n(x_1, \dots x_9) \text{ with } a_n(x_1, \dots x_9) = \begin{cases} 1 \text{ if } x_1^3 + \cdots + x_9^3 - n \equiv 0 (\text{mod } p^k), \\ 0 \text{ otherwise} \end{cases}$$

and inverting the order of summation, we see that $M_n(p^k)$ equals

$$\frac{1}{p^k} \sum_{\alpha=1}^{p^k} \sum_{1 \leqslant x_1, \dots, x_9 \leqslant p^k} \mathrm{e}\left(\alpha \frac{(x_1^3 + \cdots + x_9^3 - n)}{p^k} \right) = \frac{1}{p^k} \sum_{\alpha=1}^{p^k} S(p^k, \alpha)^9 \mathrm{e}(-\alpha n / p^k).$$

Let $\nu_p(\alpha) := t$ where t is the integer such that p^t divides α but p^{t+1} does not divide α. Then each integer α in the last sum can be factorised uniquely as $\alpha = p^{k-m} a$, where $m := k - \nu_p(\alpha)$ and a is coprime to p. Note that $1 \leqslant \alpha \leqslant p^k$, hence the only possible values for m and a are

$$0 \leqslant m \leqslant k, \quad 1 \leqslant a \leqslant p^m.$$

Note that the identity $\alpha = p^{k-m} a$ implies that

$$S(p^k, \alpha) = \sum_{1 \leqslant x \leqslant p^k} \mathrm{e}\left(\frac{a x^3}{p^m} \right) = p^{k-m} S(p^m, a),$$

hence we obtain that $\sum_{\alpha=1}^{p^k} S(p^k, \alpha)^9 \mathrm{e}(-\alpha n / p^k)$ is equal to

$$p^{9k} \sum_{m=0}^{k} p^{-9m} \sum_{\substack{1 \leqslant a \leqslant p^m \\ \gcd(a, p^m) = 1}} S(p^m, a)^9 \mathrm{e}\left(-a n / p^m \right) = p^{9k} \sum_{m=0}^{k} p^{-9m} S(p^m).$$

This is sufficient for our lemma. $\square$

Combining (11.4) and Lemma 11.4 shows that the limit (11.2), that defines $\sigma_p(n)$. exists. In addition, Lemma 11.4 and (11.3) show that

$$\mathfrak{S}(n) = \prod_p \sigma_p(n),$$

hence the only remaining part regarding the verification of Theorem 11.1 is the positivity of each $\sigma_p(n)$. This is the aim of the last section.

Remark 11.5. The absolute convergence of the series defining $\mathfrak{S}(n)$ guarantees that the infinite product in Theorem 11.1 is absolutely convergent. As such, it has a strictly positive value if and only if each of the p-adic factors is strictly positive. Therefore the positivity of each $\sigma_p(n)$ guarantees that the constant c in Theorem 8.1 does not vanish, which, in turn, implies that for all large enough integers n the function $R(n)$ is positive, i.e. there exists at least one representation of n as a sum of exactly 9 positive integer cubes.

11.2 Positivity of the p-adic densities.

For primes p define the quantity

$$\gamma_p := \begin{cases} 2 & \text{if } p = 2, 3, \\ 1 & \text{if } p > 3. \end{cases}$$

Lemma 11.6. *For each prime p, every element in $\mathbb{Z}/p^{\gamma_p}\mathbb{Z}$ is the sum of at most* 9 *cubes of elements of $\mathbb{Z}/p^{\gamma_p}\mathbb{Z}$, at least one of which is coprime to p.*

Proof. The statement is obvious when $p = 2$ or 3, since one can add 1^3 several times. Assume that $p > 3$, so that $\gamma_p = 1$. We have that $0(\text{mod} p)$ equals $1^3 + (-1)^3(\text{mod} p)$, hence it is sufficient to prove that each element of $(\mathbb{Z}/p\mathbb{Z})^* := (\mathbb{Z}/p\mathbb{Z}) \setminus \{0\}$ is a sum of at most 9 cubes. We know that this set forms a cyclic group under multiplication. Pick a generator g and consider the subgroup

$$\Gamma_p := \{g^{3m}(\text{mod} p) : m \in \mathbb{N}\},$$

which has order

$$\frac{p-1}{\gcd(p-1, 3)}.$$

If $p \equiv 2 (\text{mod } 3)$ then $\Gamma_p = (\mathbb{Z}/p\mathbb{Z})^*$, hence our lemma holds. In the remaining case, $p \equiv 1 (\text{mod } 3)$, the set Γ_p has $(p-1)/3$ elements. Let $C_1 := \Gamma_p$ and for each $m \in \mathbb{N}$ with $m \geqslant 2$ denote by C_m the elements of $(\mathbb{Z}/p\mathbb{Z})^*$ that are a sum of m elements of Γ_m but not a sum of $m-1$ elements of Γ_m. Fix $j \geqslant 1$ and consider the minimum element $x \in (\mathbb{Z}/p\mathbb{Z})^*$ that is not in any of $C_1, C_2, \ldots, C_j$. Then $x-1$ or $x-2$ is also in $(\mathbb{Z}/p\mathbb{Z})^*$ and must therefore be a sum of at most j cubes. Owing to $x = (x-1) + 1^3$ and $x = (x-2) + 1^3 + 1^3$, we see that $x \in C_{j+1}$ or $x \in C_{j+2}$. Applying this for $j = 1$ and $j = 3$ we infer that at least 3 of $C_1, \ldots, C_5$ must be non-empty. Also note that for each j we have $\Gamma_p C_j \subset C_j$, hence if C_j is not empty then it must contain at least $\#\Gamma_p = \frac{p-1}{3}$ elements. Assume that

$$(\mathbb{Z}/p\mathbb{Z})^* \neq \cup_{i=1}^5 C_i.$$

Then

$$p - 1 > \sum_{j=1}^{5} \#C_j = \sum_{\substack{1 \leqslant j \leqslant 5 \\ \#C_j \neq 0}} \#C_j \geqslant \frac{p-1}{3} \sum_{\substack{1 \leqslant j \leqslant 5 \\ \#C_j \neq 0}} 1 \geqslant p - 1,$$

which is a contradiction. This proves that each element of $x \in (\mathbb{Z}/p\mathbb{Z})^*$ is a sum of at most 5 cubes, all of which are coprime to p. $\square$

We deduce that for each $n \in \mathbb{N}$ and prime p, there is at least one solution of

$$x_1^3 + \cdots + x_9^3 \equiv n \ (\text{mod } p^{\gamma_p})$$

with $p \nmid x_j$ for some j. For each $i \neq j$ and $k > \gamma_p$ there are $p^{k-\gamma_p}$ elements $y_i (\text{mod } p^k)$ with $y_i \equiv x_i (\text{mod } p^{\gamma_p})$. For any of those $(p^{k-\gamma_p})^8$ choices we note that

$$n - \sum_{i \neq j} y_i^3 \equiv n - \sum_{i \neq j} x_i^3 \equiv x_j^3 (\text{mod } p),$$

hence

$$\mu := n - \sum_{i \neq j} y_i^3$$

is an integer coprime to p for which the equation $x^3 \equiv \mu (\text{mod } p)$ has a solution. Hensel's lemma allows us to lift this solution to a solution $(\text{mod } p^k)$, thereby giving rise to a solution of

$$\sum_{i=1}^{9} x_i^3 \equiv n \ (\text{mod } p^k).$$

This implies that $M_n(p^k) \geqslant (p^{k-\gamma_p})^8$, hence $\sigma_p(n) \geqslant p^{-8\gamma_p} > 0$, thus concluding the proof of Theorem 11.1. $\square$