Chapter 7

Sums of nine positive cubes via the circle method

The goal of the next 4 lectures is to prove that each large enough positive integer n is the sum of 9 positive integer cubes. The number of all possible representations will be denoted by

$$R(n) := \#\{(x_1, \dots, x_9) \in \mathbb{N}^9 : x_1^3 + \dots + x_9^3 = n\}, \tag{7.1}$$

where $\mathbb{N} = \{1, 2, \dots\}$. We need to show that there exists $n_0 \in \mathbb{N}$ such that

$$n \geqslant n_0 \Rightarrow R(n) > 0.$$

The exact value of n_0 shall not concern us, since a finite computation can provide a list of all integers $9 \leqslant n < n_0$ such that $R(n) = 0$. It is important to note that we will prove the following much stronger statement.

Theorem 7.1. *There exists a positive real constant c such that*

$$\lim_{n \to +\infty} \frac{R(n)}{n^2} = c.$$

The constant c has an explicit value which will be given later in this course. Note that the fact that $c > 0$ guarantees that $R(n)$ remains positive for n large enough.

7.0.1 Heuristics behind Theorem 7.1

Before we embark on the details of the proof let us give some heuristics on why the growth of the number of representations should behave like n^2. Let

$$N := [n^{\frac{1}{3}}]. \tag{7.2}$$

Each integer x_i in (7.1) satisfies $x_i^3 \leqslant n$, hence it lies in the interval $[1, N]$, which has approximately $n^{\frac{1}{3}}$ integers. Therefore there are approximately $(n^{\frac{1}{3}})^9 = n^3$ choices for the integers $x_1, \ldots, x_9$ in (7.1). For those choices the polynomial

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

takes values between 1 and n. If it were true that each such value can be taken with equal probability then the probability that it takes the value n would be $\frac{1}{n}$. Therefore the number of representations $R(n)$ should be approximately the product of all available values (that is n^3) multiplied by this probability (that is $\frac{1}{n}$). This explains why $R(n)$ grows to infinity at a rate of cn^2, for some positive constant c. The method of proof will therefore have to convert the heuristics about the random behavior of the integer values of $x_1^3 + \cdots + x_9^3$ into a legitimate argument. This method was discovered almost a century ago by Hardy, Ramanujan and Littlewood. It is known as the *circle method*. It can be used for a large variety of problems and is of central importance in modern research; we choose to apply it for proving only Theorem 7.1 for matters of illustration.

Literature:

Davenport, H. : *Analytic methods for Diophantine equations and Diophantine inequalities*, Cambridge Mathematical Library, 2005.

Vaughan, R. C. : *The Hardy-Littlewood method*, Cambridge University Press, 1997.

7.1 Setting up the circle method

We will use the notation

$$\mathrm{e}(z) := \mathrm{e}^{2\pi i z},\ z \in \mathbb{R},$$

throughout our lectures. The fact that $\mathrm{e}^{2\pi i} = 1$ shows that this function is periodic with period 1, meaning that $\mathrm{e}(z+1) = \mathrm{e}(z)$. Furthermore, for a non-zero real h the expression

$$\int_0^1 \mathrm{e}(\alpha h) \mathrm{d}\alpha$$

vanishes, because the anti-derivative of $\mathrm{e}(\alpha h)$ is $\frac{\mathrm{e}(\alpha h)}{h}$. Hence the integral equals 1 if $h = 0$ and is otherwise equal to 0. Using this with $h = x_1^3 + \cdots + x_9^3 - n$ shows that $R(n)$ equals

$$\sum_{\substack{x_1,\ldots,x_9\in\mathbb{N}\\1\leqslant x_i\leqslant N}} \int_0^1 \mathrm{e}\left(\alpha\left(x_1^3+\cdots+x_9^3-n\right)\right)\mathrm{d}\alpha = \int_0^1 \prod_{i=1}^{9}\left(\sum_{\substack{x_i\in\mathbb{N}\\1\leqslant x_i\leqslant N}} \mathrm{e}(\alpha x_i^3)\right)\mathrm{e}(-\alpha n)\mathrm{d}\alpha.$$

Letting for any $\alpha \in \mathbb{R}$,

$$f(\alpha) := \mathrm{e}(\alpha\cdot 1^3) + \mathrm{e}(\alpha\cdot 2^3) + \cdots + \mathrm{e}(\alpha N^3) = \sum_{m=1}^{N} \mathrm{e}(\alpha m^3) \tag{7.3}$$

where as always $N = [n^{1/3}]$, we have proved that

$$R(n) = \int_0^1 f(\alpha)^9 \mathrm{e}(-\alpha n)\mathrm{d}\alpha.$$

Note that the function $f(\alpha)$ also has period 1, therefore we could replace the interval of integration $[0, 1]$ by any interval $\mathcal{U}$ of length 1. It will be convenient to use the interval

$$\mathcal{U} := \left[\frac{1}{n^{1-\frac{1}{300}}}, 1 + \frac{1}{n^{1-\frac{1}{300}}}\right],$$

thus leading to

$$R(n) = \int_{\mathcal{U}} f(\alpha)^9 \mathrm{e}(-\alpha n)\mathrm{d}\alpha. \tag{7.4}$$

This identity is the starting point of the circle method. Its name comes from the fact that the function of n given by $\mathrm{e}(-\alpha n), \alpha \in [0, 1]$, takes values in the unit circle of the complex numbers.

7.1.1 Major and minor arcs

One way to think of $f(\alpha)$ is to consider what happens if one had the simpler function

$$f_1(\alpha) := \mathrm{e}(\alpha\cdot 1) + \mathrm{e}(\alpha\cdot 2) + \cdots + \mathrm{e}(\alpha N) = \sum_{m=1}^{N} \mathrm{e}(\alpha m).$$

If α is an integer then this function equals N and otherwise it has the value

$$\mathrm{e}(\alpha)\frac{\mathrm{e}(\alpha N)-1}{\mathrm{e}(\alpha)-1}=\frac{\mathrm{e}(\alpha(N+1))-\mathrm{e}(\alpha)}{\mathrm{e}(\alpha)-1}.$$

Observe that the denominator is a continuous function, hence it becomes almost zero when α is almost an integer. This means that f_1 takes larger values when α is close to being an integer. A similar phenomenon persists for the slightly more complicated function $f(\alpha)$, only this time the function $f(\alpha)$ takes larger values when α is close to a rational with small denominator, e.g. $\frac{1}{1}$, $\frac{1}{2}$, $\frac{1}{3}, \frac{2}{3}$, $\frac{1}{4}, \frac{3}{4}$, etc. This fact is not obvious but it will become clear in the next lectures. With this in mind we observe that the main contribution in the definite integral (7.4) will come when α is close to some $\frac{a}{q}$ for coprime positive integers a and q. We denote one such interval as follows,

$$\mathfrak{M}(a,q):=\left\{\alpha\in\mathcal{U}:\left|\alpha-\frac{a}{q}\right|\leqslant\frac{1}{n^{1-\frac{1}{300}}}\right\},\ a,q\in\mathbb{N}:\gcd(a,q)=1. \tag{7.5}$$

These intervals are usually called *major arcs*; when $\alpha\in\mathfrak{M}(a,q)$ the function $\mathrm{e}(\alpha)$ takes values in an arc of the unit circle of the complex plane. We can now introduce the union of all major arcs around rationals with small denominator,

$$\mathfrak{M}:=\bigcup_{1\leqslant q\leqslant n^{1/300}}\ \bigcup_{\substack{1\leqslant a\leqslant q-1\\ \gcd(a,q)=1}}\mathfrak{M}(a,q). \tag{7.6}$$

What remains of the interval $\mathcal{U}$ will be called *minor arcs* and will be denoted by

$$\mathfrak{m}:=\mathcal{U}\setminus\mathfrak{M}. \tag{7.7}$$

Observe that two different major arcs in (7.6) have empty intersection. Indeed, for $a/q\neq a'/q'$ the integer $aq'-a'q$ is not zero, hence $|aq'-a'q|\geqslant 1$. This means that

$$\left|\frac{a}{q}-\frac{a'}{q'}\right|=\frac{|aq'-a'q|}{qq'}\geqslant\frac{1}{qq'}\geqslant\frac{1}{n^{\frac{2}{300}}}>\frac{4}{n^{1-\frac{1}{300}}},$$

where in the last inequality we used that n is sufficiently large. Hence the distance of the centres of the intervals $\mathfrak{M}(a,q)$ and $\mathfrak{M}(a',q')$ is greater than the sum of their lengths, therefore they are disjoint.

By (7.4) we have therefore proved the important identity

$$R(n)=\int_{\mathfrak{M}}f(\alpha)^9\mathrm{e}(-\alpha n)\mathrm{d}\alpha+\int_{\mathfrak{m}}f(\alpha)^9\mathrm{e}(-\alpha n)\mathrm{d}\alpha. \tag{7.8}$$

We will show that the integral over the major arcs $\mathfrak{M}$ will make a contribution of size n^2, while the contribution from the minor arcs $\mathfrak{m}$ will be significantly smaller. Therefore the integral over the major arcs should be thought of as a main term and the integral over the minor arcs as the error term. Specifically, we shall prove in the next lectures that there exists a positive constant $c > 0$ such that

$$\lim_{n\to+\infty} \frac{\int_{\mathfrak{M}} f(\alpha)^9 \mathrm{e}(-\alpha n)\mathrm{d}\alpha}{n^2} = c \tag{7.9}$$

and

$$\lim_{n\to+\infty} \frac{\int_{\mathfrak{m}} f(\alpha)^9 \mathrm{e}(-\alpha n)\mathrm{d}\alpha}{n^2} = 0. \tag{7.10}$$

These two limit statements are clearly sufficient for the validity of Theorem 7.1.

7.2 Weyl's inequality

Note that for each $\beta \in \mathbb{R}$ we have $|\mathrm{e}(\beta)| = 1$ and hence for all $\alpha \in \mathbb{R}$ we see that the triangle inequality yields

$$|f(\alpha)| = \Big|\sum_{m=1}^{N} \mathrm{e}(\alpha m^3)\Big| \leqslant \sum_{m=1}^{N} |\mathrm{e}(\alpha m^3)| = N \leqslant n^{\frac{1}{3}}.$$

This is the trivial bound for $|f(\alpha)|$ and in order to prove (7.10) we will need to find a better bound whenever α is not close to a rational number. For such α the function $\mathrm{e}(\alpha m^3)$ oscillates around the unit circle quite often, therefore we expect some cancellation among the values $\mathrm{e}(\alpha m^3)$ for $m = 1, \ldots, N$.

Before stating the precise lemma, due to Weyl, let us prepare its proof. For any $\alpha \in \mathbb{R}$ we have

$$|f(\alpha)|^2 = f(\alpha)\overline{f(\alpha)} = \left(\sum_{m_1=1}^{N} \mathrm{e}(\alpha m_1^3)\right)\overline{\left(\sum_{m_2=1}^{N} \mathrm{e}(\alpha m_2^3)\right)} = \sum_{m_2=1}^{N}\left(\sum_{m_1=1}^{N} \mathrm{e}(\alpha(m_1^3 - m_2^3))\right).$$

In the inner sum we make the change of variables $m_1 \mapsto h_1$ given by $m_1 = h_1 + m_2$. The condition $1 \leqslant m_1 \leqslant N$ is equivalent to $1 - m_2 \leqslant h_1 \leqslant N - m_2$, therefore we arrive at the expression

$$\sum_{m_2=1}^{N} \sum_{h_1=1-m_2}^{N-m_2} \mathrm{e}(\alpha((h_1+m_2)^3 - m_2^3)).$$

Note that the variable h_1 takes values in the interval $[1-N, N-1]$ and that

$$(h_1+m_2)^3 - m_2^3 = h_1^3 + 3h_1(h_1 m_2 + m_2^2).$$

Inverting the order of summation in the last sum we produce the equality

$$|f(\alpha)|^2 = \sum_{|h_1|<N} \mathrm{e}(\alpha h_1^3) \sum_{m_2\in[1,N]\cap[1-h_1,N-h_1]} \mathrm{e}(\alpha 3h_1(h_1 m_2 + m_2^2))$$

and the triangle inequality shows that

$$|f(\alpha)|^2 \leqslant \sum_{|h_1|<N} |S_{h_1}|,$$

where we define

$$S_h := \sum_{m_2\in[1,N]\cap[1-h,N-h]} \mathrm{e}(3\alpha h(hm_2 + m_2^2)). \tag{7.11}$$

Therefore we have $|f(\alpha)|^4 \leqslant (\sum_{|h_1|<N} |S_{h_1}|)^2$ and we can combine this with the following special form of Cauchy's inequality [1]

$$\left(\sum_{|h_1|<N} |S_{h_1}|\right)^2 = \left(\sum_{|h_1|<N} 1\cdot|S_{h_1}|\right)^2 \leqslant \left(\sum_{|h_1|<N} 1^2\right)\left(\sum_{|h_1|<N} |S_{h_1}|^2\right) \leqslant 2N\left(\sum_{|h_1|<N} |S_{h_1}|^2\right)$$

to obtain

$$|f(\alpha)|^4 \leqslant 2N \sum_{|h_1|<N} |S_{h_1}|^2. \tag{7.12}$$

This is called a *differencing process* owing to the fact that the sum $f(\alpha)$ involves the cubic polynomial x_1^3 but the sum S_{h_1} involves the quadratic polynomial $m_2^2 + h_1 m_2$.

We perform this process once more to obtain linear polynomials, which are easier to handle. We have

$$|S_{h_1}|^2 = \sum_{m_2,m_3\in[1,N]\cap[1-h_1,N-h_1]} \mathrm{e}(3\alpha h_1(h_1 m_2 + m_2^2 - h_1 m_3 - m_3^2))$$

---

[1] The general Cauchy's inequality is $\big(\sum_{i=1}^{k} x_i y_i\big)^2 \leqslant \big(\sum_{i=1}^{k} x_i^2\big)\big(\sum_{i=1}^{k} y_i^2\big)$ for $x_i, y_i \in \mathbb{R}$.

and the change of variables $m_2 \mapsto h_2$, where $m_2 = m_3 + h_2$ makes the last sum equal to

$$\sum_{|h_2|<N} \mathrm{e}(3\alpha h_1^2 h_2 + 3\alpha h_1 h_2^2) \sum_{m_3 \in \mathcal{I}_{h_1,h_2}} \mathrm{e}(6\alpha h_1 h_2 m_3),$$

where $\mathcal{I}_{h_1,h_2} \subset [1, N]$ is the intersection of 4 intervals, namely,

$$\mathcal{I}_{h_1,h_2} := [1, N] \cap [1 - h_1, N - h_1] \cap [1 - h_2, N - h_2] \cap [1 - h_1 - h_2, N - h_1 - h_2].$$

Thus, $\mathcal{I}_{h_1,h_2}$ is a closed subinterval of $[1, N]$ with integer boundaries. By the triangle inequality we get

$$|S_{h_1}|^2 \leqslant \sum_{|h_2|<N} \Big| \sum_{m_3 \in \mathcal{I}_{h_1,h_2}} \mathrm{e}(6\alpha h_1 h_2 m_3) \Big|,$$

which, when combined with (7.12), yields

$$|f(\alpha)|^4 \leqslant 2N \sum_{|h_1|<N} \sum_{|h_2|<N} \Big| \sum_{m_3 \in \mathcal{I}_{h_1,h_2}} \mathrm{e}(6\alpha h_1 h_2 m_3) \Big|.$$

If $h_1 = 0$ then each term in the sum equals 1 and the fact that $\mathcal{I}_{h_1,h_2} \subset [1, N]$ shows that the contribution to $|f(\alpha)|^4$ is $\leqslant (2N)^2 N$, while the same holds for the contribution of h_2 with $h_2 = 0$. We have thus obtained

$$|f(\alpha)|^4 \leqslant 8N^3 + 2N \sum_{0<|h_1|<N} \sum_{0<|h_2|<N} \Big| \sum_{m_3 \in \mathcal{I}_{h_1,h_2}} \mathrm{e}(6\alpha h_1 h_2 m_3) \Big|. \tag{7.13}$$

We need an estimate for the sum over m_3. We use the following lemma.

Lemma 7.2. *For a real number θ, let $\|\theta\|$ denote the distance to the nearest integer. Then, for each $\theta \in \mathbb{R}$ and each pair of integers a, b with $1 \leqslant a \leqslant b \leqslant N$, we have*

$$\Big| \sum_{m \in [a,b]} \mathrm{e}(\theta m) \Big| \ll \min \Big\{ N, \frac{1}{\|\theta\|} \Big\}.$$

Proof. The periodicity of $\mathrm{e}(z)$ allows us to assume that θ is a real number in $(-\frac{1}{2}, \frac{1}{2}]$, hence $\|\theta\| = |\theta|$. If $\theta = 0$ then

$$\Big| \sum_{m \in [a,b]} \mathrm{e}(\theta m) \Big| \leqslant N$$

and our bound is valid. Otherwise, we have

$$\Big|\sum_{m\in[a,b]} \mathrm{e}(\theta m)\Big| = \Big|\mathrm{e}(a\theta)\sum_{m\in[0,b-a]} \mathrm{e}(\theta m)\Big| = \Big|\frac{\mathrm{e}(\theta(b-a+1))-1}{\mathrm{e}(\theta)-1}\Big| \leqslant \frac{2}{|\mathrm{e}(\theta)-1|}.$$

Moreover, for $|\theta| < \frac{1}{2}$, we have

$$|\mathrm{e}(\theta)-1| = |\mathrm{e}(\theta/2)||\mathrm{e}(\theta/2)-\mathrm{e}(-\theta/2)| = 2|\sin(\pi\theta)| \gg |\theta|,$$

which concludes our proof. □

Applying the above lemma with $[a,b] = \mathcal{I}_{h_1,h_2}$, $\theta = 6\alpha h_1 h_2$ and substituting the resulting bound into (7.13) we obtain

$$|f(\alpha)|^4 \leqslant 8N^3 + 2N \sum_{0<|h_1|<N}\sum_{0<|h_2|<N} \min\Big\{N, \frac{1}{\|\alpha\cdot 6h_1h_2\|}\Big\}.$$

For each h_1, h_2 as above, the integer $h = 6h_1h_2$ satisfies $0 < |h| < 6N^2$. Furthermore, there are at most $4\tau(\frac{h}{6}) \leqslant 4\tau(h)$ such decompositions, where $\tau(k)$ denotes the number of positive divisors of k. This leads to the bound

$$|f(\alpha)|^4 \leqslant 8N^3 + 8N \sum_{0<|h|<6N^2} \tau(h)\min\Big\{N, \frac{1}{\|\alpha h\|}\Big\}.$$

Using $\tau(h) = O_\epsilon(h^\epsilon)$ for each $\epsilon > 0$ (exercise 2.7), we arrive at

$$|f(\alpha)|^4 \ll_\epsilon N^3 + N^{1+\epsilon} \sum_{0<h<6N^2} \min\Big\{N, \frac{1}{\|\alpha h\|}\Big\}. \tag{7.14}$$

Theorem 7.3 (Weyl's inequality)**.** *Assume that there are coprime positive integers a, q with $n^{\frac{1}{300}} \leqslant q \leqslant n^{1-\frac{1}{300}}$ such that the real number α satisfies*

$$\Big|\alpha - \frac{a}{q}\Big| \leqslant \frac{1}{q^2}.$$

Then we have

$$\big|f(\alpha)\big| \ll_\epsilon n^{\frac{1}{3}-\frac{1}{2000}}.$$

If q is closer to 1 than in the statement above, then α is relatively close to an integer. Thus, each term $\mathrm{e}(\alpha m^3)$ in the definition (7.3) of $f(\alpha)$ may be close to 1. This means that $f(\alpha)$ could take a value close to $N \asymp n^{\frac{1}{3}}$ and then the conclusion of the lemma would not be valid.

Proof. Recall that $N = [n^{1/3}]$. In light of (7.2) and (7.14) it is sufficient to prove that

$$\sum_{0<h<6N^2} \min\left\{N, \frac{1}{\|\alpha h\|}\right\} \ll n^{1-\frac{1}{400}}. \tag{7.15}$$

We may now partition the sum over h into blocks of q consecutive integers; the number of such blocks is at most

$$\frac{6N^2}{q} + 1.$$

The sum over any of these blocks will be

$$\sum_{m=0}^{q-1} \min\left\{N, \frac{1}{\|\alpha(h_1+m)\|}\right\},$$

where h_1 is the least integer of the block. Since we assumed $\left|\alpha - \frac{a}{q}\right| \leqslant \frac{1}{q^2}$ and we have $m < q$, we obtain that

$$\alpha(h_1+m) = \alpha h_1 + \frac{am}{q} + O\left(\frac{m}{q^2}\right) = \alpha h_1 + \frac{am}{q} + O\left(\frac{1}{q}\right).$$

The coprimality of a and q guarantees that as m ranges through the interval $[0, q-1]$, the integer am will assume each value (mod q) once. We make the substitution $r \equiv am (\bmod\ q)$. Then, the last sum becomes

$$\sum_{r=0}^{q-1} \min\left\{N, \frac{1}{\|(r+b)/q + O(1/q)\|}\right\},$$

where b is the integer closest to $\alpha q h_1$, which is independent of r. If the least residue of $r+b$ (mod q), which we call s, satisfies $s = O(1)$ then

$$\left\|\frac{s}{q} + O\left(\frac{1}{q}\right)\right\| = O\left(\frac{1}{q}\right),$$

in which case we bound the minimum by N. In all other cases we will have

$$\left\|\frac{s}{q} + O\left(\frac{1}{q}\right)\right\| \gg \frac{s}{q}.$$

Therefore the sum over m is

$$\ll N + \sum_{s=1}^{q-1} \frac{q}{s} \ll N + q \log q,$$

where we have used $\displaystyle\sum_{s=1}^{q-1} \frac{1}{s} \leqslant 1 + \log q$. Recalling the bound for the number of blocks, the sum in (7.14) becomes

$$\ll \left(\frac{N^2}{q} + 1 \right) (N + q \log q) \ll \frac{N^3}{q} + N^2 \log q + N + q \log q.$$

The inequalities $N \leqslant n^{\frac{1}{3}}$ and $n^{\frac{1}{300}} \leqslant q \leqslant n^{1-\frac{1}{300}}$ allow us to bound this by

$$\ll n^{1-\frac{1}{300}} \log n$$

which proves (7.15). □