# The Circle Method

## Basic ideas

# 1 The method

Some of the most famous problems in Number Theory are additive problems (Fermat's last theorem, Goldbach conjecture...). It is just asking whether a number can be expressed as a sum of other numbers, all of them belonging to some subsets of integers.

Suppose that we have sequence of integers $0 \le a_1 < a_2 < a_3 < \dots$ and we want to know if a large positive integer $N$ is a sum of $k$ terms of this sequence (repetitions are allowed). We can be even more ambitous and ask about a good (possibly asymptotic) approximation for

$$r_k(N) = \#\{(n_1, n_2, \dots, n_k) \ : \ N = a_{n_1} + a_{n_2} + \cdots + a_{n_k}\}.$$

This is the kind of problems treated by circle method. The starting point is to consider the analytic function $F(z) = \sum z^{a_n}$ and note that

$$r_k(N) = \text{coeff. of } z^N \text{ in } (F(z))^k.$$

We can write it in a fancy way involving a complex integral:

$$r_k(N) = \frac{1}{2\pi i} \int_C (F(z))^k \frac{dz}{z^{N+1}} \tag{1.1}$$

where $C$ is a circle $\{z \in \mathbb{C} \ : \ |z| = r\}$ with $0 < r < 1$. In principle this seems rather unnatural and useless, we can see the circle but not the method. The guidelines for success in this approach come from a general philosophy in Analytic Number Theory: *extract arithmetical information from the singularities*. For instance, the study of the distribution of prime numbers depends heavily on the poles of $\zeta'/\zeta$.

In (1.1) the only singularity, the high order pole at $z = 0$, has been introduced rather artificially and an application of residue theorem simply dismantles the formula recovering the definition of $r_k(N)$. We have to escape from $z = 0$. On the other hand, in the most of the practical examples, the unit circle is the natural boundary of the holomorphic function $F$, and hence it is impossible to push $r$ beyond 1 in search of new singularities. In the circle method one takes $r$ close enough to 1 in order to feel the influence of the "main singularities" on the boundary, but small enough to avoid uncontrolled "interferences".

The circle method appeared firstly in a paper by Hardy and Ramanujan about partitions [3], but it was developed by Hardy and Littlewood (it is sometimes called Hardy-Littlewood method). They introduced the nowadays standard terminology *major arcs* and *minor arcs* referring to a subdivision of $C$. In the former the influence of near singularities leads to a good approximated formula, while in the latter we have to content ourselves with a bound.

In practice the definition of major and minor arcs depends on diophantine approximation properties. This is not so strange, if $z$ tends to 1 radially there is not any cancellation in $F$ and this “big singularity” causes a big major arc. On the other hand, if $z$ tends radially to $e^{2\pi ia/q}$, the size of the singularity, if it exists, depends on the distribution of $a_n$ modulus $q$, but typically one hopes less cancellation and a bigger major arc when $q$ is small (because of lower oscillation). In this scheme, minor arcs correspond to directions far apart from having small denominator slopes.

## 2 Sums of squares

One can ask about the number of representations of a (large) positive integer $N$ as a sum of $k$ squares. By technically reasons (write a simpler final formula) we shall assume that $8|k$ although this is not essential for the method. As square function is not injective, $(-n)^2 = n^2$, we shall forget about $a_n$ giving an *ad hoc* definition

$$r_k(N) = \#\{(n_1, n_2, \dots, n_k) \in \mathbb{Z}^k \ : \ n_1^2 + n_2^2 + \cdots + n_k^2 = N\}.$$

Now (1.1) reads

$$r_k(N) = \frac{1}{2\pi i}\int_C (F(z))^k \frac{dz}{z^{N+1}} \qquad \text{with } \ F(z) = \sum_{n=-\infty}^{\infty} z^{n^2} = 1 + 2\sum_{n=1}^{\infty} z^{n^2}.$$

A change of variable $z \mapsto e^{2\pi iz}$ leads to a famous $\theta$-function

$$r_k(N) = \int_L \theta^k(z) e^{-2N\pi iz}\, dz \qquad \text{with } \ \theta(z) = \sum_{n=-\infty}^{\infty} e^{2\pi in^2 z} \tag{2.1}$$

and $L$ the horizontal segment $\{0 \le \Re z < 1,\ \Im z = y\}$ where $r = e^{-2\pi y}$. We shall choose $y = 1/N$. This is the natural choice because it constitutes a penalty for the terms with $n^2 > N$ which are negligible in order to represent $N$ as a sum of squares.

A fundamental property of $\theta^k$ is that it is automorphic. This means a kind of invariance by certain (Fuchsian) group of fractional linear transformations. Namely

$$\theta^k\left(\frac{az+b}{4cz+d}\right) = (4cz+d)^{k/2}\theta^k(z)$$

when $a, b, c, d \in \mathbb{Z}$ and $ad - 4bc = 1$. It allows to pass the information from some arcs to others. In fact, it can be proved that it is enough to study the arcs close to 0, 1/2 and 1/4 (for the *cognoscenti*, these are the inequivalent cusps). Without entering into details, it turns out that if $a/q$ is an irreducible fraction it holds

$$\theta^k(z) \sim (qz-a)^{-k/2} \text{ if } 4|q, \quad \theta^k(z) \sim (2(qz-a))^{-k/2} \text{ if } 2\not| q \text{ and } \theta(z) \approx 0 \text{ otherwise,}$$

as $qz - a \to 0$ with $\Im(qz-a)^{-1} \to -\infty$. If $0 \le a < q \le \sqrt{N}$, this is the case for $z = a/q + (u+i)/N$ with $u/N = o\big((q\sqrt{N})^{-1}\big)$ when $N \to \infty$. Hence for $N$ large, the contribution to the integral in (2.1) of this "arc" when $4|q$ is asymptotically equal to

$$\frac{1}{N}\int_{-\sqrt{N}/q}^{\sqrt{N}/q} \big(\frac{qu}{N} + \frac{qi}{N}\big)^{-k/2} e^{-2\pi i aN/q} e^{-2\pi i(u+i)}\, du$$
$$= q^{-k/2} N^{k/2-1} e^{-2\pi i aN/q} \int_{-\sqrt{N}/q}^{\sqrt{N}/q} (u+i)^{-k/2} e^{-2\pi i(u+i)}\, du.$$

If $q$ is small enough in comparison with $\sqrt{N}$ this is $\sim C_k q^{-k/2} N^{k/2-1} e^{-2\pi i aN/q}$, otherwise the contribution is small and we can consider that we are dealing with a minor arc. Taking into account also the case $2\not| q$, and adding all the contributions, it follows

$$r_k(N) \sim C_k N^{k/2-1} \sum_{q=1}^{\infty} \sum_{\substack{a=0 \\ (a,q)=1}}^{q} \epsilon_q q^{-k/2} e^{-2\pi i aN/q} \qquad \text{with} \quad \epsilon_q = \begin{cases} 1 & \text{if } 4|q \\ 2^{-k/2} & \text{if } 2\not| q \\ 0 & \text{otherwise} \end{cases}$$

Some tricky (elementary but not easy) manipulations[*] allow to simplify enormously the summation. The final result is

$$r_k(N) \sim A_k N^{k/2-1} \sum_{d|N} (-1)^{N+N/d} d^{1-k/2}.$$

The value of $A_k$ can be explicitly computed in terms of the $k/2$-th Bernoulli number.

# 3 Sums of primes

One of the most impressive approaches to Goldbach conjecture is Vinogradov's theorem asserting that every large enough odd integer is a sum of three primes.

[*] See the appendix

This is one of the highlights of the circle method and, although the details are rather involved, it is possible to sketch the proof according to the main lines mentioned before.

In this case $\{a_n\}$ is the sequence of prime numbers and we want to approximate $r_3(N)$ for $N$ large and odd. Therefore (1.1) reads

$$r_3(N) = \frac{1}{2\pi i}\int_C (F(z))^3 \frac{dz}{z^{N+1}} \qquad \text{with } \ F(z) = \sum_p z^p.$$

In this case $F$ has not automorphic properties and Vinogradov considered that it is useless to preserve the whole series for $F$. We do not lose anything truncating $F$ to $p \le N$ and pushing $C$ to the unit circle. With a change of variable $z = e^{2\pi i x}$ we obtain a Fourier series version of the previous formula:

$$r_3(N) = \int_{-1/2}^{1/2} (S(x))^3 e^{-2\pi i N x}\, dx \qquad \text{with } \ S(x) = \sum_{p\le N} e^{2\pi i p x}.$$

Instead of studying the radial behavior of $F$, we have to face with the trigonometrical sum $S(x)$. It is a completely equivalent procedure but technically simpler.

Using prime number theorem, we have $S(0) \sim N/\log N$. If $x$ is smaller than $1/N$ then we have a similar approximation because $e^{2\pi i p x}$ does not oscillate (use Taylor expansion). And it seems that for $x$ a little greater, the oscillation should cause some cancellation. In fact, using prime number theorem with error term and partial summation, it is not difficult to get an asymptotic formula reflecting this behavior in a "major arc" $I_0$ slighty greater that $[-1/N, 1/N]$. So we have

$$\int_{I_0} (S(x))^3 e^{-2\pi i N x}\, dx \sim C\frac{1}{N}\left(\frac{N}{\log N}\right)^3 = C\frac{N^2}{\log^3 N}.$$

In fact, it holds $C = 1/2$.

In the same way, if $a/q$ is an irreducible fraction,

$$S(a/q) = e^{2\pi i/q} \sum_{\substack{p\le N\\ q|ap-1}} 1 + e^{4\pi i/q} \sum_{\substack{p\le N\\ q|ap-2}} 1 + e^{6\pi i/q} \sum_{\substack{p\le N\\ q|ap-3}} 1 + \dots$$

And we need an asymptotic formula for the number of primes in the arithmetic progression $qn + c$. If $c$ and $q$ are not coprime, of course there are finitely many. On the other hand, there are $\phi(q)$ values of $c \in [1, q]$ which are coprime with $q$, and prime number theorem for arithmetic progressions asserts that prime numbers are equidistributed in the corresponding $\phi(q)$ progressions. Hence

$$S(a/q) \sim \frac{N}{\phi(q)\log N} \sum_{\substack{c=0\\(c,q)=1}}^{q} e^{2\pi ic/q}$$

(if the sum does not vanish). Reasoning as before, we can find a “major arc” $I_{a/q}$ around $a/q$ slighty greater than $[a/q-1/N, a/q+1/N]$.

The problem is that the error term in prime number theorem for arithmetic progressions is rather unknown when $q$ varies, and we are forced to take $q$ very small in comparison with $N$ (something like a logarithm). This causes minor arcs to be really large and Vinogradov had to use very involved arguments to obtain acceptable non trivial bounds on them. If we skip this big problem and we consider only major arcs contribution, we get:

$$r_3(N) \sim \frac{1}{2}\frac{N^2}{\log^3 N}\sum_{q=1}^{\infty}\sum_{\substack{a=0\\(a,q)=1}}^{q}\left(\frac{1}{\phi(q)}\sum_{\substack{c=0\\(c,q)=1}}^{q} e^{2\pi ic/q}\right)^3 e^{-2\pi iNa/q}.$$

Again, with very tricky but elementary arguments, the sum can be evaluated explictly, giving

$$r_3(N) \sim \frac{1}{2}\frac{N^2}{\log^3 N}\prod_{p|N}\left(1-\frac{1}{(p-1)^2}\right)\prod_{p\nmid N}\left(1+\frac{1}{(p-1)^3}\right).$$

Note that for $N$ even, the first product vanishes ruinning the asymptotic formula.

# 4 Appendix

The key observation to simplify the formulas obtained by circle method in the previous examples, is that the *Ramanujan sum*

$$c_q(-N) = \sum_{\substack{a=0\\(a,q)=1}}^{q} e^{-2\pi iaN/q}$$

is multiplicative in $q$, *i.e.* $c_{q_1}(-N) \cdot c_{q_2}(-N) = c_{q_1 q_2}(-N)$ if $q_1$ and $q_2$ are coprimes. This is a simple consequence of chinese remainder theorem. For each prime number $p$, let $l$ be a non-negative integer such that $p^l | N$ and $p^{l+1} \not| N$. The following elementary properties allow to evaluate $c_q(-N)$:

$$0 < l < m \Rightarrow c_{p^m}(-N) = p^l c_{p^{m-l}}(-N/p^l),\ 0 < m \leq l \Rightarrow c_{p^m}(-N) = p^m - p^{m-1}$$
$$0 = l < m \ \Rightarrow\ c_p(-N) = -1, \quad c_{p^{m+1}}(-N) = 0.$$

Hence for any multiplicative arithmetical function $f$, under suitable convergence conditions,

$$\sum_{q=1}^{\infty} f(q) c_q(-N) = \prod_p \left(1 + f(p)c_p(-N) + f(p^2)c_{p^2}(-N) + \dots\right) = \prod_p \mathcal{F}_p$$

and $\mathcal{F}_p$ is actually a finite sum.

For instance, in the case of the sum of squares, we can take $f(q) = 2^{k/2}\epsilon_q q^{-k/2}$. Then for $p \neq 2$

$$\begin{aligned} \mathcal{F}_p &= 1 + p^{-k/2}(p-1) + (p^2)^{-k/2}(p^2 - p) + \dots + (p^l)^{-k/2}(p^l - p^{l-1}) - (p^{l+1})^{-k/2} p^l \\ &= (1 - p^{-k/2})\left(1 + p^{1-k/2} + p^{2(1-k/2)} + \dots + p^{l(1-k/2)}\right). \end{aligned}$$

Similar manipulations lead, for $p = 2$, to

$$\mathcal{F}_2 = 1 + 2^{1-k/2} + 2^{2(1-k/2)} + \dots + 2^{l(1-k/2)} - 2 \cdot 2^{l(1-k/2)}.$$

Then the product $\prod \mathcal{F}_p$ is, up to a factor only depending on $k$, the sum of the $1 - k/2$ powers of the divisors of $N$, substracting twice the divisors containing a maximal power of 2. Note that $N + N/d$ is even if and only if $d$ is even and contains this maximal power, and the closed form $\sum_{d|N}(-1)^{N+N/d} d^{1-k/2}$ follows.

The case of sums of three primes is much easier. The multiplicative function is $f(q) = c_q^3(1)/\phi^3(q)$, hence $\mathcal{F}_p = 1 - c_p(-N)/(p-1)^3$, which is $1 - (p-1)^{-2}$ if $p|N$, and $1 + (p-1)^{-3}$ if $p \not| N$.

# Bibliography

[1] H. Davenport. *Multiplicative number theory*, 2nd ed., revised by Hugh L. Montgomery. Graduate texts in mathematics 74. Springer Verlag, 1980.

[2] W.J. Ellison, M. Mendès-France. *Les nombres premiers*. Hermann, 1975.

[3] G.H. Hardy, S. Ramanujan. Asymptotic formulae in combinatory analysis. *Proc. London Math. Soc.* (2) **17** (1918), 75-115.

[4] R.C. Vaughan. *The Hardy-Littlewood method*. Cambridge tracts in Mathematics 80. Cambridge University Press, 1981.