Основы кругового метода в теории чисел.

Максим Александрович Королёв

23 июля 2021 г.

Мы будем задаваться вопросом вида когда и сколькими способами некоторое целое число N раскладывается в сумму

$$N = a_1 + \dots + a_k, \qquad a_i \in A.$$

Пример 1. Теорема Лагранжа о разложимости числа в сумму 4 квадратов есть частный случай для $k = 4$, $A = \{a^2\}_{a\in\mathbb{Z}}$.

Утверждение 1 (проблема Варинга, доказана)**.** *Для всякого $n > 1$ есть константа $k = k(n)$, что всякое натуральное N представимо в виде*

$$N = x_1^n + \dots + x_k^n,$$

где $x_i \geqslant 0$.

Определение 1. Для всякого целого m определим

$$\delta(m) := \int_0^1 e^{2\pi i m\alpha} d\alpha.$$

Замечание 1. $\delta(0) = 1$. Если $m \neq 0$, то

$$\delta(m) = \left.\frac{e^{2\pi i\alpha m}}{2\pi i m}\right|_0^1 = 0.$$

Следовательно

$$\delta(m) = [m = 0].$$

Пусть $I(N)$ — число решений уравнения

$$N = x_1^3 + \dots + x_10^3.$$

Рассмотрим случайный вектор $x = (x_1, \dots, x_10)$ и обозначим

$$m = x_1^3 + \dots x_10^3 - N.$$

Следовательно $\delta(m) = 1$ тогда и только тогда, когда x — корень. Понятно, что $x_i \leqslant \sqrt[3]{N} =: P$. Следовательно

$$\begin{aligned} I(N) &= \sum_{0\leqslant x_1,\dots,x_10\leqslant P} \delta(x_1^3 + \dots x_10^3 - N) \\ &= \sum_{\vec{x}} \int_0^1 e^{2\pi i\alpha(x_1^3+\dots+x_10^3-N)} d\alpha \\ &= \int_0^1 \prod_{j=1}^{10} \sum_{0\leqslant x_j\leqslant P} e^{2\pi i\alpha x_j^3} \cdot e^{-2\pi i\alpha N} d\alpha \\ &= \int_0^1 S_3^{10}(\alpha) e^{-2\pi i\alpha N} d\alpha. \end{aligned}$$

$J(N)$ — частное решение уравнения Лагранжа.

$$J(N) = \int_0^1 S_2^4(\alpha) e^{-2\pi\alpha N} d\alpha.$$

Имеем, что $J(N) > 0$ для всякого $N \geqslant 1$. Также получаем, что

$$J(N) = \int_0^1 W^3(\alpha) e^{-2\pi\alpha N} d\alpha,$$

где

$$W(\alpha) = \sum_{p \leqslant N} e^{2\pi\alpha p}.$$

Теорема 2. *Пусть есть $\tau > 1$. Тогда для всякого $\alpha \in [0;1]$ существуют целые $0 \leqslant a \leqslant q$, что* $\mathrm{GCD}(a,q) = 1$, $1 \leqslant q \leqslant \tau$, *что*

$$|\alpha - \frac{p}{q}| \leqslant \frac{1}{q\tau}.$$

Доказательство. Рассмотрим $\alpha_j := \{j\alpha\}$. Возьмём $n = [\tau] + 1$. Тогда

$$0 = \alpha_0 \leqslant \alpha_1 \leqslant \cdots \leqslant \alpha_n \leqslant \alpha_{n+1} = 1$$

— разбиение $[0;1]$. Тогда существуют k и m, что

$$0 \leqslant \alpha_k - \alpha_m \leqslant \frac{1}{n+1}.$$

Пусть $1 \leqslant m \leqslant k \leqslant n$. Тогда

$$0 \leqslant k\alpha - [k\alpha] - m\alpha + [m\alpha] \leqslant \frac{1}{n+1}$$
$$0 \leqslant \alpha(k-m) - ([k\alpha] - [m\alpha]) \leqslant \frac{1}{n+1}$$
$$0 \leqslant \alpha - \frac{[k\alpha] - [m\alpha]}{k-m} \leqslant \frac{1}{(n+1)(k-m)}$$

Пусть

$$\frac{a}{q} := \frac{[k\alpha] - [m\alpha]}{k-m}.$$

Тогда

$$0 \leqslant \alpha - \frac{a}{q} \leqslant \frac{1}{(n+1)(k-m)} \leqslant \frac{1}{\tau q}.$$

□

Замечание 2. Такая дробь $\frac{a}{q}$ называется *рациональным приближением (к) α порядка τ.*

Замечание 3. Если $\frac{a}{q}$ — рациональное приближение порядка τ, то $\alpha = \frac{a}{q} + \frac{\theta}{q\tau}$, где $|\theta| \leqslant 1$.

Замечание 4. Пусть

$$E(a,q) := (\frac{a}{q} - \frac{1}{q\tau}; \frac{a}{q} + \frac{1}{q\tau}).$$

Тогда $\frac{a}{q}$ будет приближением порядка τ тогда и только тогда, когда $\alpha \in E(a,q)$.

Теперь пусть $\tau = 6P^2 = 6N$. Берём $Q \in (1; \frac{\tau}{2})$ (конкретное значение будет позже). Отрезок $[0;1]$ покрыт объединением

$$\bigcup_{1\leqslant q\leqslant \tau} \bigcup_{\substack{a=0 \\ (a,q)=1}}^{q} E(a,q).$$

Пусть E_1 — объединение интервалов $E(a,q)$ с $q \leqslant Q$, а

$$E_2 := (\frac{-1}{\tau}; 1-\frac{1}{\tau}] \setminus E_1$$

— всё остальное.

Теорема 3. *E_1 состоит из непересекающихся интервалов.*

Доказательство. Предположим противное. Пусть есть точки $\frac{a_1}{q_1}$ и $\frac{a_2}{q_2}$, отрезки которых перекрываются. Следовательно

$$\begin{gathered} 0 < \frac{a_2}{q_2} - \frac{a_1}{q_1} < \frac{1}{q_1\tau} + \frac{1}{q_2\tau} \\ 0 < \frac{a_2q_1 - a_1q_2}{q_1q_2} < \frac{q_1+q_2}{q_1q_2\tau} \\ \tau < q_1 + q_1 \leqslant 2Q \end{gathered}$$

□

$$I(N) = \int_{E_1} + \int_{E_2} = I_1(N) + I_2(N)$$

— *интегралы по большим и малым дугам.*

Тригонометрические суммы:

$$S_1(\alpha) := \sum_{x=0}^{P} e^{2\pi i\alpha x}.$$

Если α целое, то $S_1 = P+1$, иначе

$$S_1(\alpha) = \frac{e^{2\pi i\alpha(P+1)} - 1}{e^{2\pi i\alpha} - 1}.$$

Таким образом

$$|S_1(\alpha)| \leqslant \frac{2}{|e^{\pi i\alpha}(e^{\pi i\alpha} - e^{-\pi i\alpha})|} = \frac{1}{\sin(\pi\alpha)} = \frac{1}{\sin(\pi\|\alpha\|)} \leqslant \frac{1}{2\|\alpha\|},$$

где

$$\|\alpha\| := \min_{n\in\mathbb{Z}}(|\alpha - n|).$$