Основы кругового метода в теории чисел.

Максим Александрович Королёв

26 июля 2021 г.

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

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

где мы фиксируем интересующее нас множество 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 $x_i \geqslant 0$.

Чтобы понять, как работает круговой метод, попробуем для примера доказать, что всякое целое число представимо в виде суммы 10 кубов.

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

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

Следовательно

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

где $[*]$ — скобка Айверсона.

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

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

где

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

Теорема же Лагранжа на таком языке будет записана как

$$J(N) := \int_0^1 S_2^4(\alpha) e^{-2\pi \alpha N} d\alpha > 0.$$

А тернарная теорема Гольдбаха на таком языке имеет вид

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

где

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

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*

$$\left| \alpha - \frac{a}{q} \right| \leqslant \frac{1}{q\tau}.$$

Доказательство. Возьмём $n = [\tau] + 1$. Рассмотрим $\alpha_j := \{j\alpha\}$ для $j \in [1; n]$, $\alpha_0 := 0$, а $\alpha_{n+1} := 1$. Тогда

$$0 = \alpha_{i_0} \leqslant \alpha_{i_1} \leqslant \cdots \leqslant \alpha_{i_n} \leqslant \alpha_{i_{n+1}} = 1$$

— разбиение $[0; 1]$, где $(i_k)_{k=0}^n$ — некоторая перестановка $(0; 1; \ldots; n+1)$. Понятно, что $i_0 = 0$, $i_{n+1} = n + 1$. Тогда по принципу Дирихле 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

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

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

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

Определим a и q так, что
$$\frac{a}{q} := \frac{[k\alpha] - [m\alpha]}{k - m}.$$
Тогда $q \mid k - m$, и, следовательно, $q \leqslant k - m$.
$$0 \leqslant \alpha - \frac{a}{q} \leqslant \frac{1}{(n+1)(k-m)} \leqslant \frac{1}{\tau q}.$$

Случай $1 \leqslant k \leqslant m \leqslant n$ рассматривается в точности также, только вместо $k - m$ надо рассматривать $m - k$.

Случай $k = 0$ может выполниться, только если $\alpha_m = 0$ (а в таком случае $\alpha m \in \mathbb{Z}$, следовательно достаточно взять $a := \alpha m$, $q := m$). Аналогично (но уже строго) не может выполниться случай $m = n + 1$.

Пусть $m = 0$. Тогда $k \in [1; n]$, а значит
$$0 \leqslant k\alpha - [k\alpha] \leqslant \frac{1}{n+1}$$
$$0 \leqslant \alpha - \frac{[k\alpha]}{k} \leqslant \frac{1}{k(n+1)}$$
Определим a и q так, что
$$\frac{a}{q} := \frac{[k\alpha]}{k}.$$
Тогда $q \mid k$, и, следовательно, $q \leqslant k$.
$$0 \leqslant \alpha - \frac{a}{q} \leqslant \frac{1}{k(n+1)} \leqslant \frac{1}{q\tau}.$$

Пусть $k = n + 1$. Тогда $m \in [1; n]$, а значит
$$0 \leqslant 1 - m\alpha + [m\alpha] \leqslant \frac{1}{n+1}$$
$$0 \leqslant \frac{1 - [m\alpha]}{m} - \alpha \leqslant \frac{1}{(n+1)m}$$

Определим a и q так, что
$$\frac{a}{q} := \frac{1 - [m\alpha]}{m}.$$
Тогда $q \mid m$, и, следовательно, $q \leqslant m$.
$$-\frac{1}{q\tau} \leqslant -\frac{1}{(n+1)m} \leqslant \alpha - \frac{a}{q} \leqslant 0.$$

$\square$

Замечание 2. Такая дробь $\frac{a}{q}$ называется *рациональным приближением* 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
$$E(a, q) := \left(\frac{a}{q} - \frac{1}{q\tau}; \frac{a}{q} + \frac{1}{q\tau}\right).$$
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

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

— всё остальное. Полуинтервал $(-1/\tau; 1 - 1/\tau]$ был выбран, так как всякий интервал в нём лежит. Действительно, так как $q \leqslant Q \leqslant \tau/2$,

$$\frac{a}{q} - \frac{1}{q\tau} \geqslant \frac{0}{1} - \frac{1}{1 \cdot \tau} = -\frac{1}{\tau}$$
$$\frac{a}{q} + \frac{1}{q\tau} \leqslant \frac{q-1}{q} + \frac{1}{q\tau} = 1 - \frac{\tau - 1}{q\tau} \leqslant 1 - \frac{1}{\tau} + \frac{\tau}{\tau^2} - \frac{2\tau - 2}{\tau^2} = 1 - \frac{1}{\tau} - \frac{\tau - 2}{\tau^2} < 1 - \frac{1}{\tau}.$$

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

$$0 < \frac{a_2}{q_2} - \frac{a_1}{q_1} < \frac{1}{q_1\tau} + \frac{1}{q_2\tau}$$
$$0 < \frac{a_2q_1 - a_1q_2}{q_1q_2} < \frac{q_1 + q_2}{q_1q_2\tau}$$
$$\frac{1}{q_1q_2} < \frac{q_1 + q_2}{q_1q_2\tau}$$

(так как $a_2q_1 - a_1q_2$ — целое, неотрицательное и неравное 0, так как $\mathrm{GCD}(a_1, q_1) = \mathrm{GCD}(a_2, q_2) = 1$)

$$\tau < q_1 + q_1 \leqslant 2Q$$

□

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

— *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

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

— расстояние от α до ближайшего целого, так как для $t \in [0; 1/2]$ верно $\sin(\pi t) \geqslant 2t$. Таким образом

$$|S_1(\alpha)| \leqslant \min\left(P+1, \frac{1}{2\|\alpha\|}\right)$$

Теперь давайте оценим $I_2(N)$. Квадратичная сумма:

$$S_2(\alpha, \beta) = \sum_{0\leqslant x\leqslant P} e^{2\pi i(\alpha x^2 + \beta x)}.$$

Тогда

$$|S_2|^2 = \overline{S}_2 \cdot S_2 = \sum_{0\leqslant x\leqslant P} e^{-2\pi i(\alpha x^2+\beta x)} \sum_{0\leqslant y\leqslant P} e^{2\pi i(\alpha y^2+\beta y)} = \sum_{0\leqslant x,y\leqslant P} e^{2\pi i(\alpha(y^2-x^2)+\beta(y-x))}$$

Фиксируя x и делая замену $h := y - x \in [-x; P-x]$, получаем, что

$$|S_2|^2 = \sum_{0\leqslant x\leqslant P}\ \sum_{-x\leqslant h\leqslant P-x} e^{2\pi i(\alpha h^2+\beta h)} \cdot e^{2\pi i\cdot 2\alpha hx}$$

Пусть $x_1 := \max(0, -h)$, $y_1 := \min(P, P-h)$. Тогда

$$\begin{aligned}|S_2|^2 &= \sum_{|h|\leqslant P} e^{2\pi i(\alpha h^2+\beta h)} \sum_{x_1\leqslant x\leqslant y_1} e^{2\pi i\cdot 2\alpha hx}\\ &\leqslant \sum_{|h|\leqslant P} \min\left(P+1, \frac{1}{2\|2\alpha h\|}\right)\end{aligned}$$

(так как $|e^{2\pi i(\alpha h^2+\beta h)}| = 1$, а внутренння сумма содержит не более $P+1$ члена с модулем 1, поэтому $\leqslant P+1$, а также по аналогии с S_1 не более $1/(2\|2\alpha h\|)$)

$$\begin{aligned}&\leqslant P+1+2\sum_{1\leqslant h\leqslant P} \min\left(P+1, \frac{1}{2\|2\alpha h\|}\right)\\ &\leqslant P+1+2\sum_{1\leqslant h\leqslant P} \min\left(P+1, \frac{1}{\|2\alpha h\|}\right)\end{aligned}$$

(так как больше — не меньше)

$$\leqslant P+1+2\sum_{1\leqslant h\leqslant 2P} \min\left(P+1, \frac{1}{\|\alpha h\|}\right)$$

(вообще произошла замена $h := 2h$, и поэтому стоило бы писать, что новое h чётно, но мы не будем, так как это добавит нечётные члены, которые не уменьшат сумму)

Определение 2. Знак Виноградова — если $|A| \leqslant c \cdot B$, то

$$A \ll B.$$

Если $c = c(\alpha, \beta, \dots)$, то

$$A \ll_{\alpha,\beta,\dots} B.$$

Лемма 4 (неравенство Гёльдера)**.** *Пусть даны* $a_m \geqslant 0$*. Тогда*

$$\left(\sum_{m=1}^{M} a_m\right)^k \leqslant M^{k-1}\sum_{m=1}^{M} a_m^k.$$

Следствие 4.1. *Если* $M, k = \mathrm{const}$*, то*

$$\left(\sum_{m=1}^{M} a_m\right)^k \ll \sum_{m=1}^{M} a_m^k.$$

Кубическая сумма:

$$S_3(\alpha) = \sum_{0\leqslant x\leqslant P} e^{2\pi i\alpha x^3}.$$

Тогда по аналогии с S_2

$$|S_3|^2 = \sum_{0\leqslant x\leqslant P}\ \sum_{-x\leqslant h_1\leqslant P-x} e^{2\pi i\alpha((x+h_1)^3-x^3)} = \sum_{|h_1|\leqslant P} e^{2\pi i\alpha h_1^3}\sum_{x_1\leqslant x\leqslant y_1} e^{2\pi i\cdot 3\alpha h_1(x^2+xh_1)}$$

$$\leqslant \sum_{|h_1|\leqslant P}\left|\sum_{x_1\leqslant x\leqslant y_1} e^{2\pi i\cdot 3\alpha h_1(x^2+xh_1)}\right| \leqslant P+1+2\sum_{1\leqslant|h_1|\leqslant P}\left|\sum_{x_1\leqslant x\leqslant y_1} e^{2\pi i\cdot 3\alpha h_1(x^2+xh_1)}\right|$$

Таким образом

$$|S_3|^4 \ll P^2 + \left(\sum_{1\leqslant|h_1|\leqslant P}\left|\sum_{x_1\leqslant x\leqslant y_1} e^{2\pi i\cdot 3\alpha h_1(x^2+xh_1)}\right|\right)^2$$

(так как банально представили как $(|S_3|^2)^2$ и использовали неравенство Гёльдера для $k = 2$, $M = 3$: $(A+B)^2 \ll A^2 + B^2$)

$$\ll P^2 + P\sum_{1\leqslant|h_1|\leqslant P}\left|\sum_{x} e^{2\pi i\cdot 3\alpha h_1(x^2+xh_1)}\right|^2$$

(так как ещё банальнее использовали неравенство Гёльдера для $k = 2$, $M \sim P$, где a_i — это модули внутренних сумм)

$$\ll P^2 + P\sum_{1\leqslant|h_1|\leqslant P}\left|S_2(3\alpha h_1, 3\alpha h_1^2)\right|^2$$

$$\ll P^2 + P\sum_{1\leqslant|h_1|\leqslant P}\left(P + \sum_{1\leqslant h_2\leqslant 2P}\min\left(P, \frac{1}{\|3\alpha h_1 h_2\|}\right)\right)$$

$$\ll P^3 + P\sum_{1\leqslant|h_1|\leqslant P}\ \sum_{1\leqslant h_2\leqslant 2P}\min\left(P, \frac{1}{\|3\alpha h_1 h_2\|}\right)$$

$$\ll P^3 + 2P\sum_{1\leqslant h_1\leqslant P}\ \sum_{1\leqslant h_2\leqslant 2P}\min\left(P, \frac{1}{\|3\alpha h_1 h_2\|}\right)$$

$$\ll P^3 + P\sum_{1\leqslant h_1\leqslant 3P}\ \sum_{1\leqslant h_2\leqslant 2P}\min\left(P, \frac{1}{\|\alpha h_1 h_2\|}\right)$$

$$\ll P^3 + P\sum_{1\leqslant n\leqslant 6P^2}\tau(n)\min\left(P, \frac{1}{\|\alpha n\|}\right)$$

(где $n = h_1h_2 \in [1; 6P^2]$, а $\tau(n)$ — количество делителей n, а значит и оценка сверху на количество пар $(h_1; h_2)$ с произведением n)

$$\ll P^3 + P^{1+\varepsilon} \sum_{1 \leqslant n \leqslant 6P^2} \min\left(P, \frac{1}{\|\alpha n\|}\right)$$

(так как $\forall \varepsilon > 0\ \exists c = c(\varepsilon)\colon \forall n \in \mathbb{N} \quad \tau(n) \leqslant c(\varepsilon) n^{\varepsilon} \ll n^{\varepsilon}$).

Теорема 5. *Пусть $m \in \mathbb{Z}$, $T \geqslant 1$, $\alpha = \frac{a}{q} + \frac{\theta}{q^2}$, $|\theta| \leqslant 1$, $\mathrm{GCD}(a, q) = 1$, $q \geqslant 6$,*

$$W = \sum_{m - \frac{q}{2} < n \leqslant m + \frac{q}{2}} \min\left(T, \frac{1}{\|\alpha n\|}\right).$$

Тогда $W \leqslant 4T + 2q\ln(q)$.

Доказательство. Пусть $n = m + x$, $-\frac{q}{2} < x \leqslant \frac{q}{2}$. Тогда

$$\alpha n = \alpha(m + x) = \alpha x + \alpha m = \left(\frac{a}{q} + \frac{\theta}{q^2}\right) x + \alpha m$$
$$= \frac{ax}{q} + \alpha m + \frac{\theta x}{q^2} = \frac{ax + \alpha q m}{q} + \frac{\theta x}{q^2} = \frac{ax + b + \theta_1}{q} + \frac{\theta x}{q^2} = \frac{ax + b}{q} + r_x,$$

где b — ближайшее целое к $\alpha q m$, тогда $\alpha q m = b + \theta_1$, где $|\theta_1| \leqslant \frac{1}{2}$. При этом

$$r_x = \frac{\theta_1}{q} + \frac{\theta x}{q^2}.$$

Вспоминая, что $|\theta_1| \leqslant \frac{1}{2}$, $|\theta| \leqslant 1$, $|x| \leqslant \frac{q}{2}$, имеем, что

$$|r_x| \leqslant \left|\frac{\theta_1}{q}\right| + \left|\frac{\theta x}{q^2}\right| \leqslant \frac{1}{2q} + \frac{q/2}{q^2} = \frac{1}{q}.$$

Определим y как остаток $ax + b$ взятый с полуинтервала $(-\frac{q}{2}; \frac{q}{2}]$. Заметим, что так как x пробегает все остатки по модулю q единожды, а $\mathrm{GCD}(a, q) = 1$, то так же пробегает все остатки и $ax + b \equiv y$, быть может, в другом порядке. Также мы имеем

$$\|\alpha n\| = \left\|\frac{y}{q} + \rho_y\right\|, \qquad \text{где } \rho_y := r_x.$$

Поскольку $|\rho_y| = |r_x| \leqslant 1/q$, то есть ровно не более одного остатка y по модулю q, что

$$\left|\frac{y}{q} + \rho_y\right| \geqslant \frac{1}{2}.$$

Таким образом оценим в сумме значение для этого остатка, а также для остальных остатков, как T сверху. Для остальных y будет верно, что

$$\left|\frac{y}{q} + \rho_y\right| \leqslant \frac{1}{2},$$

т.е. 0 — ближайшее значение к $\frac{y}{q}+\rho_y$, а значит

$$\|\alpha n\| = \left\|\frac{y}{q}+\rho_y\right\| = \left|\frac{y}{q}+\rho_y\right| \geqslant \left|\frac{y}{q}\right| - |\rho_y| \geqslant \frac{|y|}{q} - \frac{1}{q} = \frac{|y|-1}{q}.$$

Поскольку $|y|-1$ принимает неприятные значения при $y \in \{0; 1; -1\}$, то оценим и соответствующие им члены суммы тоже как T сверху; остальные члены оценим сверху как

$$\leqslant \frac{1}{\|\alpha n\|} \frac{q}{|y|-1}.$$

Таким образом получаем, что

$$\begin{aligned} W &\leqslant 4T + \sum_{\substack{y \in (-\frac{q}{2}; \frac{q}{2}] \\ y \neq 0, 1, -1, \pm\lfloor \frac{q}{2} \rfloor}} \frac{q}{|y|-1} \\ &\leqslant 4T + 2q \sum_{y=2}^{\lfloor \frac{q}{2} \rfloor} \frac{1}{y-1} \\ &= 4T + 2q \sum_{y=1}^{\lfloor \frac{q}{2} \rfloor - 1} \frac{1}{y} \\ &\leqslant 4T + 2q\left(1 + \ln\left(\left\lfloor \frac{q}{2} \right\rfloor - 1\right)\right) \\ &\leqslant 4T + 2q\ln(q) + 2q(1 - \ln(2)) \end{aligned}$$

[получилось хуже, мы не понимаем почему, но нам и такого хватит]. $\square$

Так мы получаем

$$|S_3|^4 \ll P^3 + P^{1+\varepsilon}\left(\frac{6P^2}{q} + 1\right)(4P + 2q\ln(q) + 2q(1-\ln(2)))$$

(так как мы разбили отрезок $[1; 6P^2]$ на отрезки длины q и применили теорему к каждому из них)

$$\begin{aligned} &\ll P^3 + P^{1+\varepsilon}\left(\frac{P^3}{q} + P^2\ln(q) + q\ln(q)\right) \\ &\ll P^{1+\varepsilon}\left(\frac{P^3}{4} + P^2\ln(q) + q\ln(q)\right) \\ &= P^{4+\varepsilon}\left(\frac{1}{4} + \frac{\ln(q)}{P} + \frac{q\ln(q)}{P^2}\right). \end{aligned}$$