Наш семинар: математические сюжеты

Неравенства С. Н. Бернштейна для тригонометрических многочленов

С. Б. Гашков, С. В. Кравцев

§ 1. Введение

Сначала сформулируем несколько задач.

Первая из них предлагалась на LXXVII Московской математической олимпиаде (2014 г., 11 класс, 2-й день, задача 2).

Задача 1. Найдите все такие a и b, что $|a| + |b| \geqslant 2/\sqrt{3}$ и при всех x выполнено неравенство $|a \sin x + b \sin 2x| \leqslant 1$.

Первоначальная формулировка была такова:

Задача 2. Доказать, что если при всех x выполнено неравенство

$$|b_1 \sin x + b_2 \sin 2x| \leqslant 1,$$

где b_i — постоянные коэффициенты, то $|b_1| + |b_2| \leqslant 2/\sqrt{3}$, причём равенство возможно, лишь когда $|b_1| = 4/\sqrt{27}$, $|b_2| = 2/\sqrt{27}$.

Задача 3. Если для многочлена $t(x) = b_1 \sin x + b_2 \sin 2x + b_3 \sin 3x$ выполняются неравенства

$$\left|t\left(\tfrac{2\pi}{7}\right)\right| = \left|b_1 \sin\frac{2\pi}{7} + b_2 \sin\frac{4\pi}{7} + b_3 \sin\frac{6\pi}{7}\right| \leqslant 1,$$
$$\left|t\left(\tfrac{4\pi}{7}\right)\right| = \left|b_1 \sin\frac{4\pi}{7} - b_2 \sin\frac{\pi}{7} - b_3 \sin\frac{5\pi}{7}\right| \leqslant 1,$$
$$\left|t\left(\tfrac{6\pi}{7}\right)\right| = \left|b_1 \sin\frac{6\pi}{7} - b_2 \sin\frac{5\pi}{7} + b_3 \sin\frac{4\pi}{7}\right| \leqslant 1,$$

то выполняется неравенство

$$|b_1| + |b_2| + |b_3| \leqslant \frac{6}{\sqrt{7}}.$$

Задача 4. Проверить, что многочлен

$$\frac{2\sqrt{7}}{7}\sin x + \frac{2\sqrt{7}}{7}\sin 2x - \frac{2\sqrt{7}}{7}\sin 3x$$

удовлетворяет неравенствам из предыдущей задачи и тем самым неравенство $|b_1| + |b_2| + |b_3| \leqslant 6/\sqrt{7}$ нельзя улучшить.

Можно добавить ещё несколько подобных задач, но ограничимся этими. Рекомендуем вам, прежде чем читать дальше, попробовать решить хотя бы одну из них.

Пусть n — простое число. Напомним следующее определение (и обозначение):

$\left(\frac{k}{n}\right) = 1$, если k равно остатку от деления квадрата некоторого целого числа на n;

$\left(\frac{k}{n}\right) = 0$, если k делится на n;

$\left(\frac{k}{n}\right) = -1$ в оставшихся случаях.

Так определённая величина $\left(\frac{k}{n}\right)$ называется *символом Лежандра*; числа k, для которых он равен 1, называются *квадратичными вычетами по модулю n*, а числа, для которых он равен -1, — *квадратичными невычетами по модулю n*.

Далее будут доказаны следующие замечательные (и незаслуженно мало известные) неравенства для суммы модулей коэффициентов тригонометрических многочленов, частные случаи которых были сформулированы выше.

Академик АН СССР Сергей Натанович Бернштейн (1880–1968)

Теорема 1 (С. Н. Бернштейн). *Пусть нечётный действительный тригонометрический многочлен*

$$t_n(x) = \sum_{k=1}^{n} b_k \sin kx$$

удовлетворяет неравенствам

$$\left| t_n\left(\frac{2\pi k}{2n+1}\right)\right| \leqslant 1, \quad k = 1, \ldots, n. \qquad (*)$$

Тогда

$$\sum_{k=1}^{n} |b_k| \leqslant \sqrt{2n+1} - \frac{1}{\sqrt{2n+1}}.$$

Неравенство обращается в равенство при нечётных n, *для которых* $p = 2n+1$ — *простое, и*

$$b_k = \frac{2}{\sqrt{2n+1}}\left(\frac{k}{2n+1}\right), \quad k = 1, \ldots, n.$$

Пусть чётный действительный тригонометрический многочлен

$$t_n(x) = \sum_{k=1}^{n} a_k \cos kx$$

удовлетворяет условию $t_n(0) = 0$ *и неравенствам* $(*)$. *Тогда*

$$\sum_{k=1}^{n} |a_k| \leqslant \sqrt{2n+1} - \frac{1}{\sqrt{2n+1}}.$$

Неравенство обращается в равенство при чётных n, *для которых* $p = 2n+1$ — *простое, и*

$$a_k = \frac{2}{\sqrt{2n+1}}\left(\frac{k}{2n+1}\right), \quad k = 1, \ldots, n.$$

Эти неравенства (а также ряд других) были найдены С. Н. Бернштейном чуть больше ста лет назад (см. [1]), причём в их доказательстве неожиданно оказались задействованы не самые тривиальные теоретико-числовые факты.

§ 2. Квадратичный закон взаимности

Напомним некоторые понятия. Если m — целое и $n > 1$ — натуральное число, то существуют единственные целые числа k и $0 \leqslant l < n$, для которых выполняется равенство $m = k \cdot n + l$. Число l в этом равенстве называется *остатком от деления* m на n.

Два целых числа a, b называются *сравнимыми по модулю натурального числа* $n > 1$ (что обозначается как $a \equiv b \pmod{n}$), если при делении на n они дают одинаковые остатки. Если все сравнимые между собой целые числа объединить в одно подмножество множества целых чисел, то получится n таких подмножеств, соответствующих остаткам $0, 1, 2, \ldots, n-1$. Перечислим несколько свойств *сравнений*.

Задача 5. Докажите, что если $a \equiv b \pmod{n}$ и $c \equiv d \pmod{n}$, то $a + c \equiv b + d \pmod{n}$, $a - c \equiv b - d \pmod{n}$, $ac \equiv bd \pmod{n}$.

Указание. Эти свойства вытекают из равенств

$$
\begin{aligned}
(b+d)-(a+c) &= (b-a)+(d-c),\\
(b-d)-(a-c) &= (b-a)-(d-c),\\
b\cdot d-a\cdot c &= (b-a)d+(d-c)a.
\end{aligned}
$$

Тем самым сравнимость чисел не нарушится, если к одному из них прибавить число, сравнимое с 0 по заданному модулю, а также если оба сравнимых числа умножить на одно и то же целое число или возвести их в одинаковую натуральную степень.

Из перечисленных свойств следует, что сравнение остаётся верным, если какое-либо его слагаемое перенести из одной части сравнения в другую с изменением знака на противоположный или если возвести обе части сравнения в одинаковую степень.

Задача 6. Докажите, что если $a_i \equiv b_i \pmod{n}$, $i = 0, 1, \ldots, m$, и $x \equiv y \pmod{n}$, то

$$a_m x^m + a_{m-1}x^{m-1} + \ldots + a_0 \equiv b_m y^m + b_{m-1}y^{m-1} + \ldots + b_0 \pmod{n}.$$

Указание. Применить предыдущую задачу.

Справедлива

Теорема 2 (квадратичный закон взаимности Эйлера — Гаусса). *Для простых чисел $p, q > 2$ справедливо тождество*

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}.$$

Иными словами, если хотя бы одно из чисел p, q при делении на 4 даёт остаток 1, то число p является квадратом по модулю числа q в точности тогда, когда число q является квадратом по модулю числа p. Если же оба числа p, q при делении на 4 дают остаток 3, то число p является квадратом по модулю числа q в точности тогда, когда число q не является квадратом по модулю числа p. В ходе доказательства понадобится несколько лемм, в которых везде a обозначает целое число, а p — простое число.

Лемма 1 (малая теорема Ферма). $a^p \equiv a \pmod{p}$.

Доказательство. Заметим, что[1] биномиальные коэффициенты

$$\binom{p}{k} = \frac{p(p-1)(p-2)\cdot\ldots\cdot(p-k+1)}{1\cdot 2\cdot 3\cdot\ldots\cdot k}, \quad k = 1, 2, \ldots, p-1,$$

[1] Биномиальные коэффициенты обозначаются также C_n^k.

делятся на p, поскольку множитель p в числителе дроби не может сократиться со знаменателем. Если теперь m, n — целые числа, то из предыдущего наблюдения и формулы бинома следует, что каждое слагаемое в правой части разложения

$$(m+n)^p - m^p - n^p = \binom{p}{1} m^{p-1} n^1 + \binom{p}{2} m^{p-2} n^2 + \ldots + \binom{p}{p-1} m^1 n^{p-1}$$

делится на p, поэтому и левая часть равенства делится на p. Точно так же делится на p число $(l+m+n)^p - l^p - m^p - n^p$, если l, m, n — целые числа. Чтобы убедиться в этом, достаточно применить предыдущее наблюдение к правой части записи

$$(l+m+n)^p - l^p - m^p - n^p = \\ = \big(((l+m)+n)^p - (l+m)^p - n^p\big) + ((l+m)^p - l^p - m^p).$$

Рассуждая аналогично, приходим к выводу, что выражение

$$\left(\sum_{i=1}^{n} a_i\right)^p - \sum_{i=1}^{n} a_i^p$$

всегда делится на p.

Утверждение леммы получается теперь, если взять в последнем сравнении все слагаемые равными 1, а n — равным a. □

Следствие 1. *Если p не делит a, то после деления сравнения $a^p \equiv a \pmod{p}$ на a получится верное сравнение $a^{p-1} \equiv 1 \pmod{p}$, поскольку из условия $a \cdot (a^{p-1} - 1) = k \cdot p$ вытекает, что простое число p делит именно $a^{p-1} - 1$.*

Часто малую теорему Ферма формулируют так, как в этом следствии.

Сравнения вида

$$a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0 \equiv 0 \pmod{p}, \quad a_n \neq 0,$$

называют *сравнениями степени n*.

Лемма 2. *Любое сравнение $a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0 \equiv 0 \pmod{p}$ равносильно некоторому сравнению степени не выше $p-1$.*

Доказательство. Разделим многочлен $q(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0$ на двучлен $x^p - x$, в результате получим $q(x) = (x^p - x) f(x) + r(x)$, причём степень остатка $r(x)$ не превосходит $p-1$. По малой теореме Ферма верно сравнение $x^p - x \equiv 0 \pmod{p}$, поэтому исходное сравнение равносильно сравнению $r(x) \equiv 0 \pmod{p}$. □

Лемма 3. *Если сравнение* $a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0 \equiv 0 \pmod p$ *степени* n *имеет более* n *различных решений, то все коэффициенты* $a_n, a_{n-1}, \ldots, a_0$ *кратны* p (*и тогда сравнение тривиально, т. е. все целые числа являются его решениями*).

Доказательство. Если рассматриваемое сравнение имеет по меньшей мере $n+1$ различное решение $x_1, x_2, \ldots, x_{n+1}$, $0 \leqslant x_i < p$, то многочлен

$$q(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0$$

можно записать в виде

$$\begin{aligned} q(x) = b_n&(x-x_1)(x-x_2)\ldots(x-x_{n-2})(x-x_{n-1})(x-x_n) + \\ &+ b_{n-1}(x-x_1)(x-x_2)\ldots(x-x_{n-2})(x-x_{n-1}) + \\ &+ b_{n-2}(x-x_1)(x-x_2)\ldots(x-x_{n-2}) + \ldots + b_1(x-x_1) + b_0. \end{aligned}$$

В самом деле, достаточно положить $b_n = a_n$, затем взять коэффициент b_{n-1} равным коэффициенту при x^{n-1} в разности

$$q(x) - a_n(x-x_1)(x-x_2)\ldots(x-x_{n-2})(x-x_{n-1})(x-x_n),$$

после чего взять коэффициент b_{n-2} равным коэффициенту при x^{n-2} в разности

$$\begin{aligned} q(x) - a_n(x-x_1)(x-x_2)\ldots(x-x_{n-2})(x-x_{n-1})(x-x_n) - \\ - b_{n-1}(x-x_1)(x-x_2)\ldots(x-x_{n-2})(x-x_{n-1}) \end{aligned}$$

и т. д. Но тогда $0 \equiv q(x_1) = b_0 \pmod p$, т. е. p делит b_0,

$$0 \equiv q(x_2) = b_0 + b_1(x_2 - x_1) \equiv b_1(x_2 - x_1) \pmod p,$$

и тогда p делит b_1, поскольку $0 < |x_2 - x_1| < p$. Последовательно подставляя далее $x = x_3, x_4, \ldots, x_{n-1}$, убеждаемся, что все коэффициенты b_i, $i = 1, 2, \ldots, n$, делятся на p, но тогда и все коэффициенты многочлена $q(x)$ делятся на p, поскольку они являются суммами произведений чисел b_i, $i = 1, 2, \ldots, n$, и целых чисел. □

Следствие 2. *Всякое нетривиальное*[2)] *сравнение по модулю простого числа* p *равносильно сравнению степени не выше* $p-1$ *и имеет не более чем* $p-1$ *решение.*

Доказательство. Это непосредственно вытекает из лемм 2 и 3. □

[2)] То есть сравнение, для которого не все целые числа являются решениями.

Лемма 4 (критерий Эйлера). *Если $p>2$ — простое и a не кратно p, то*

$$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod p.$$

Доказательство. Согласно малой теореме Ферма $a^{p-1} \equiv 1 \pmod p$, что можно также переписать в виде

$$(a^{\frac{p-1}{2}} - 1) \cdot (a^{\frac{p-1}{2}} + 1) \equiv 0 \pmod p.$$

Разность сомножителей в левой части последнего сравнения равна 2, поэтому только один из них делится на $p > 2$. Рассмотрим первый из двух возможных случаев: число a является квадратичным вычетом по модулю p, т. е. сравнение $a \equiv x^2 \pmod p$ имеет решение. Тогда то же самое решение имеет и сравнение $a^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1 \pmod p$, которое получается из предыдущего сравнения почленным возведением в степень $\dfrac{p-1}{2}$ и применением малой теоремы Ферма. Осталось заметить, что сравнение $a^{\frac{p-1}{2}} \equiv 1 \pmod p$ согласно следствию 10 не может иметь более $\dfrac{p-1}{2}$ решений, т. е. множество решений этого сравнения исчерпывается квадратичными вычетами. Тем самым все квадратичные невычеты удовлетворяют сравнению $a^{\frac{p-1}{2}} \equiv -1 \pmod p$. □

Следующие две задачи пригодятся в дальнейшем.

Задача 7 (Эйлер — Лежандр). Доказать для простого числа n тождества

$$\left(\frac{k}{n}\right)\left(\frac{m}{n}\right) = \left(\frac{km}{n}\right), \quad \left(\frac{k}{n}\right)^2 = 1, \quad \left(\frac{k}{n}\right)\left(\frac{n-k}{n}\right) = \left(\frac{n-1}{n}\right).$$

Указание. Применить критерий Эйлера.

Задача 8 (Эйлер — Лежандр). Доказать для простого числа n вида $4l+3$ тождество

$$\left(\frac{k}{n}\right) = -\left(\frac{n-k}{n}\right),$$

а для простого числа n вида $4l+1$ доказать тождество

$$\left(\frac{k}{n}\right) = \left(\frac{n-k}{n}\right).$$

Указание. Применить критерий Эйлера.

Прежде чем сформулировать следующую лемму, введём необходимые дополнительные обозначения. Ранее уже говорилось, что если все целые числа, сравнимые между собой по модулю фиксированного числа n, объединить в одно подмножество множества целых чисел, то получится n таких подмножеств, соответствующих остаткам $0, 1, 2, \ldots, n-1$. Заметим, что эти остатки мы считали обозначениями получающихся подмножеств. Понятно, что можно ввести и иные обозначения для подмножеств чисел, сравнимых между собой по фиксированному модулю. Достаточно просто выбрать по одному числу из каждого такого подмножества и назначить выбранные числа обозначениями подмножеств. Выбранные числа образуют набор, который называется *полной системой вычетов по модулю* n.

Например, для сравнения по простому модулю $p > 2$ удобно выбрать в качестве набора обозначений классов сравнимых чисел набор

$$\left\{-\frac{p-1}{2}, -\frac{p-3}{2}, \ldots, -1, 0, 1, \ldots, \frac{p-3}{2}, \frac{p-1}{2}\right\}.$$

Такой выбор интересен тем, что из каждого подмножества был выбран его элемент, имеющий наименьшую абсолютную величину в этом подмножестве. Набор вычетов с указанным свойством называют набором *абсолютно наименьших вычетов*.

Обозначим символом Ω положительную часть этого набора:

$$\Omega = \left\{1, 2, \ldots, \frac{p-3}{2}, \frac{p-1}{2}\right\}.$$

Для произведения целого числа a и каждого $s \in \Omega$ найдём его абсолютно наименьший вычет по модулю p: $a \cdot s \equiv t_s \pmod{p}$, после чего положим $\varepsilon_s = 1$, если $t_s > 0$, и $\varepsilon_s = -1$, если $t_s < 0$. Будем также считать, что $t_s = \varepsilon_s \cdot r_s$, $r_s > 0$.

Если из полной системы вычетов по некоторому модулю n удалить все вычеты, которые имеют общий делитель, больший 1, с модулем сравнения, то оставшийся набор взаимно простых с модулем вычетов называется *приведённой системой вычетов*.

Число элементов в приведённой системе вычетов по модулю n равно количеству тех натуральных чисел из набора $1, 2, \ldots, n-1$, которые взаимно просты с n. Это число обозначается символом $\varphi(n)$, а φ называется *функцией Эйлера*. Из определения приведённой системы вычетов следует, что любые $\varphi(n)$ попарно не сравнимых по модулю n и взаимно простых с этим модулем целых чисел образуют приведённую систему вычетов по модулю n.

Лемма 5. *Если целое число a взаимно просто с модулем n и переменная x пробегает приведённую систему вычетов по модулю n, то произведение $a \cdot x$ также пробегает приведённую систему вычетов по этому модулю.*

Доказательство. Поскольку различные значения переменной x попарно несравнимы и взаимно просты, как и число a, с модулем, то и числа

ax будут попарно несравнимы и взаимно просты с модулем. Осталось заметить, что таких чисел ровно $\varphi(n)$. $\square$

Лемма 6 (лемма Гаусса). *Если $p > 2$ — простое, то* $\left(\frac{a}{p}\right) = \prod_{s\in\Omega} \varepsilon_s$.

Доказательство. Согласно лемме 5 множество чисел $\{\pm a\cdot s \mid s\in\Omega\}$ является приведённой системой вычетов по модулю p. Соответствующие абсолютно наименьшие вычеты составляют набор

$$\{\pm\varepsilon_s r_s \mid s\in\Omega\} = \bigl\{-\varepsilon_1 r_1, \varepsilon_1 r_1, -\varepsilon_2 r_2, \varepsilon_2 r_2, -\varepsilon_3 r_3, \ldots, -\varepsilon_{\frac{p-1}{2}} r_{\frac{p-1}{2}}, \varepsilon_{\frac{p-1}{2}} r_{\frac{p-1}{2}}\bigr\}.$$

Подмножество положительных вычетов из последнего набора, т. е. множество $\{r_1, r_2, \ldots, r_{\frac{p-1}{2}}\}$, совпадает с множеством чисел $1, 2, \ldots, \frac{p-1}{2}$, т. е. со множеством Ω. Перемножим теперь сравнения

$$a\cdot 1 \equiv \varepsilon_1 r_1 \pmod p, \quad a\cdot 2\equiv \varepsilon_2 r_2 \pmod p, \quad \ldots,$$
$$a\cdot\frac{p-1}{2} \equiv \varepsilon_{\frac{p-1}{2}} r_{\frac{p-1}{2}} \pmod p$$

и разделим обе части сравнения-произведения на число

$$1\cdot 2\cdot\ldots\cdot\frac{p-1}{2} = r_1 r_2\cdot\ldots\cdot r_{\frac{p-1}{2}}.$$

Получаем сравнение $a^{\frac{p-1}{2}} \equiv \varepsilon_1\varepsilon_2\ldots\varepsilon_{\frac{p-1}{2}} \pmod p$. Остаётся применить критерий Эйлера. $\square$

Лемма 7 (лемма Эйзенштейна). *Для каждого нечётного натурального числа $2n+1$ справедливо тождество*

$$\frac{\sin((2n+1)x)}{\sin x} = (-4)^n \prod_{1\leqslant k\leqslant n}\Bigl(\sin^2 x - \sin^2\frac{2\pi k}{2n+1}\Bigr).$$

Доказательство. Заметим, что

$$\sin((2n+1)x) = \operatorname{Im}((e^{ix})^{2n+1}) = \operatorname{Im}((\cos x + i\sin x)^{2n+1}).$$

Если в правой части этого равенства воспользоваться формулой бинома Ньютона, то мнимая единица появится только в тех слагаемых, которые будут содержать множитель $i\sin x$ в нечётной степени, и тогда множитель $\cos x$ будет присутствовать в таких слагаемых непременно в чётной степени, поскольку сумма степеней этих двух множителей всегда равна нечётному числу $2n+1$. Используя тождество $\cos^2 x = 1-\sin^2 x$, получаем, что левая часть доказываемого тождества — это многочлен степени n от функции $\sin^2 x$. Числа $\frac{2\pi k}{2n+1}$, $k = 1, 2, \ldots, n$, обращают левую часть тождества в 0, и их количество совпадает со степенью левой части как многочлена от $\sin^2 x$. Поэтому нулями многочлена в левой части доказываемого тождества являются числа $\sin^2 \dfrac{2\pi k}{2n+1}$, $k = 1, 2, \ldots, n$, и только они. Осталось проверить, что множитель перед произведением в правой части тождества выбран правильно. Для этого достаточно найти старший коэффициент многочлена относительно $\sin^2 x$ в левой его части. Старший коэффициент в правой части доказываемого тождества, очевидно, равен $(-4)^n$.

Чтобы не смешивать обозначения, положим $\sin x = t$. Многочлен в левой части перепишется в виде

$$\sum_{k=0}^{n}(-1)^k\binom{2n+1}{2k+1}t^{2k}(1-t^2)^{n-k}.$$

Его коэффициент при t^{2n} будет равен

$$(-1)^n\sum_{k=0}^{n}\binom{2n+1}{2k+1} = (-1)^n 2^{2n} = (-4)^n,$$

потому что в силу формулы бинома

$$\sum_{k=0}^{n}\binom{2n+1}{2k+1} - \sum_{k=0}^{n}\binom{2n+1}{2k} = (1-1)^{2n+1} = 0,$$

$$\sum_{k=0}^{2n+1}\binom{2n+1}{k} = (1+1)^{2n+1} = 2^{2n+1}. \qquad \square$$

Изложенное ниже доказательство[3] закона взаимности содержится, например, в [2, с. 20–21].

По лемме 6 для двух простых чисел $p, q > 2$ справедливо тождество

$$\left(\frac{q}{p}\right) = \prod_{s\in\Omega}\varepsilon_s.$$

Используя обозначения из доказательства этой леммы, имеем $q\cdot s = \varepsilon_s r_s$, поэтому, используя нечётность синуса, получаем

$$\sin\frac{2\pi qs}{p} = \varepsilon_s \sin\frac{2\pi r_s}{p}.$$

Перемножая эти равенства для всех индексов s, имеем (с учётом биективности отображения $s \to r_s$)

$$\left(\frac{q}{p}\right) = \prod_{s\in\Omega}\varepsilon_s = \prod_{s\in\Omega}\left(\frac{\sin(2\pi qs/p)}{\sin(2\pi s/p)}\right).$$

[3] Оно принадлежит ученику Гаусса Эйзенштейну.

Применяя лемму 7 к сомножителям правой части последнего тождества (для $2n+1=q$), получаем

$$\left(\frac{q}{p}\right)=\prod_{s\in\Omega}(-4)^{\frac{q-1}{2}}\prod_{1\leqslant k\leqslant\frac{q-1}{2}}\left(\sin^2\frac{2\pi s}{p}-\sin^2\frac{2\pi k}{q}\right)=$$
$$=(-4)^{\frac{(q-1)(p-1)}{4}}\prod_{1\leqslant k\leqslant\frac{q-1}{2},\, s\in\Omega}\left(\sin^2\frac{2\pi s}{p}-\sin^2\frac{2\pi k}{q}\right).$$

Меняя числа q и p ролями, точно так же получаем

$$\left(\frac{q}{p}\right)=(-4)^{\frac{(q-1)(p-1)}{4}}\prod_{1\leqslant k\leqslant\frac{q-1}{2},\, s\in\Omega}\left(\sin^2\frac{2\pi k}{q}-\sin^2\frac{2\pi s}{p}\right).$$

Осталось заметить, что соответствующие множители в правых частях двух последних тождеств противоположны по знаку, причём число этих множителей равно $\dfrac{(q-1)(p-1)}{4}$, поэтому

$$\left(\frac{q}{p}\right)=\left(\frac{p}{q}\right)(-1)^{\frac{(q-1)(p-1)}{4}},$$

что и завершает доказательство. □

Для доказательства неравенств С. Н. Бернштейна понадобится несколько тригонометрических тождеств.

Задача 9. Докажите, что при $l<m$ справедливы тождества

$$\sum_{k=1}^{m}\sin\left(x+\frac{2\pi kl}{m}\right)=0=\sum_{k=1}^{m}\cos\left(x+\frac{2\pi kl}{m}\right).$$

Указание. Сумма векторов, выходящих из начала координат в точки на единичной окружности, образующие правильный n-угольник, равна нулю. Чтобы доказать этот факт, достаточно повернуть плоскость с изображёнными на ней векторами против часовой стрелки на угол $2\pi/m$. Если сумма рассматриваемых векторов ненулевая, то она тоже должна была бы повернуться на этот угол. С другой стороны, при таком повороте каждый вектор превратился в соседний вектор, т. е. набор векторов не изменился и сумма измениться не должна. Осталось заметить, что

$$\sum_{k=1}^{m}\cos\left(x+\frac{2\pi kl}{m}\right)+\sum_{k=1}^{m}i\sin\left(x+\frac{2\pi kl}{m}\right)=\sum_{k=1}^{m}e^{i(x+2\pi kl/m)},$$

а последняя сумма геометрически изображается как раз как сумма векторов, выходящих из начала координат в точки на единичной окружности, образующие правильный n-угольник.

Задача 10. Докажите, что при $l < m/2$ выполняются тождества

$$\sum_{k=1}^{m} \sin\Bigl(x + 2\frac{\pi kl}{m}\Bigr) \cos\Bigl(y + \frac{2\pi ks}{m}\Bigr) = 0 = \sum_{k=1}^{m} \sin\Bigl(x + \frac{2\pi kl}{m}\Bigr) \sin\Bigl(y + \frac{2\pi ks}{m}\Bigr),$$

$$\sum_{k=1}^{m} \cos\Bigl(x + \frac{2\pi kl}{m}\Bigr) \cos\Bigl(y + \frac{2\pi ks}{m}\Bigr) = 0,$$

$$\sum_{k=1}^{m} \cos^2\Bigl(x + \frac{2\pi kl}{m}\Bigr) = \frac{m}{2} = \sum_{k=1}^{m} \sin^2\Bigl(x + \frac{2\pi kl}{m}\Bigr).$$

Указание. Достаточно выразить каждое слагаемое вида

$$\cos(x + la)\sin(y + sa), \quad \cos(x + la)\cos(y + sa), \quad \sin(x + la)\sin(y + sa)$$

в виде линейной комбинации синусов или косинусов от $x + y + (l + s)a$ и $x - y + (l - s)a$, а каждый квадрат — через косинус двойного угла, и применить тождества задачи 9.

Задача 11. Докажите, что для каждого действительного тригонометрического многочлена

$$t_n(x) = \frac{a_0}{2} + \sum_{k=1}^{n} (a_k \cos kx + b_k \sin kx)$$

при $m > 2n$, $l \leqslant n$ справедливы тождества

$$\frac{1}{m} \sum_{k=1}^{m} t_n^2\Bigl(x + \frac{2\pi k}{m}\Bigr) = \frac{a_0^2}{4} + \sum_{k=1}^{n} \frac{a_k^2 + b_k^2}{2},$$

$$a_l = \frac{2}{m} \sum_{k=1}^{m} t_n\Bigl(\frac{2k\pi}{m}\Bigr) \cos\frac{2kl\pi}{m}, \quad b_l = \frac{2}{m} \sum_{k=1}^{m} t_n\Bigl(\frac{2k\pi}{m}\Bigr) \sin\frac{2kl\pi}{m}.$$

Указание. Применить тождества задачи 10.

Задача 12. Докажите, что при каждом натуральном $m \leqslant 2n$ справедливы тождества

$$\sum_{k=1}^{n} \cos\frac{2mk\pi}{2n+1} = -\frac{1}{2},$$

$$\sum_{k=1}^{n} \sin^2\frac{mk\pi}{2n+1} = \frac{2n+1}{4}, \quad \sum_{k=1}^{n} \cos^2\frac{mk\pi}{2n+1} = \frac{2n-1}{4}.$$

Указание. Первое из этих тождеств следует из второй строки тождеств в задаче 10 при $x = y = s = 0$, остальные два тождества следуют из первого, если применить формулы двойного угла.

Далее понадобится замечательное тригонометрическое тождество:

Теорема 3 (Гаусс). *При простом* $n = 4m+1$ *и* $l = 1, \ldots, n-1$

$$\sum_{k=1}^{n-1} \left(\frac{k}{n}\right) \cos\frac{2kl\pi}{n} = \pm\sqrt{n}, \quad \sum_{k=1}^{n-1} \left(\frac{k}{n}\right) \sin\frac{2kl\pi}{n} = 0.$$

При простом $n = 4m+3$ *и* $l = 1, \ldots, n-1$

$$\sum_{k=1}^{n-1} \left(\frac{k}{n}\right) \sin\frac{2kl\pi}{n} = \pm\sqrt{n}, \quad \sum_{k=1}^{n-1} \left(\frac{k}{n}\right) \cos\frac{2kl\pi}{n} = 0.$$

На самом деле Гаусс доказал более сильное утверждение: в правой части левых равенств можно заменить $\pm\sqrt{n}$ на $\sqrt{n}\left(\frac{l}{n}\right)$. Но доказательство сложно, а нас устроит более слабое утверждение.

Сначала докажем вспомогательные тождества, тоже найденные Гауссом.

Задача 13. При простом n и $l = 1, \ldots, n$

$$\sum_{k=1}^{n-1} \left(\frac{k}{n}\right) \cos\frac{2kl\pi}{n} = \left(\frac{l}{n}\right) \sum_{k=1}^{n-1} \left(\frac{k}{n}\right) \cos\frac{2k\pi}{n},$$
$$\sum_{k=1}^{n-1} \left(\frac{k}{n}\right) \sin\frac{2kl\pi}{n} = \left(\frac{l}{n}\right) \sum_{k=1}^{n-1} \left(\frac{k}{n}\right) \sin\frac{2k\pi}{n}.$$

Указание. При l, кратном n, обе части формул нулевые, так как $\left(\frac{l}{n}\right) = 0$ и $\sum_{k=1}^{n-1}\left(\frac{k}{n}\right) = 0$. Если l не кратно n, то

$$\left(\frac{l}{n}\right) \sum_{k=1}^{n-1} \left(\frac{k}{n}\right) \cos\frac{2kl\pi}{n} = \sum_{k=1}^{n-1} \left(\frac{kl}{n}\right) \cos\frac{2kl\pi}{n} = \sum_{k=1}^{n-1} \left(\frac{k}{n}\right) \cos\frac{2k\pi}{n},$$

потому что остатки от деления kl на n при $k = 1, \ldots, n-1$ пробегают все числа от 1 до $n-1$ по одному разу. Для синуса доказательство аналогично.

Теперь всё готово для доказательства теоремы Гаусса. Удобно использовать комплексное обозначение $e^{i\varphi} = \cos\varphi + i\sin\varphi$ и тождества доказывать одновременно (равенство нулю в них легко проверить непосредственно). Эти тождества можно записать в компактном виде:

$$\sum_{k=1}^{n-1} \left(\frac{k}{n}\right) e^{2kl\pi i/n} = \pm\sqrt{n} \quad \text{при } n = 4m+1$$

и

$$\sum_{k=1}^{n-1}\left(\frac{k}{n}\right)e^{2kl\pi i/n}=\pm i\sqrt{n}\quad\text{при } n=4m+3,$$

или, в общем случае,

$$\left(\sum_{k=1}^{n-1}\left(\frac{k}{n}\right)e^{2kl\pi i/n}\right)^2=n(-1)^{(n-1)/2}.$$

Далее будем использовать обозначение

$$g_l=\sum_{k=1}^{n-1}\left(\frac{k}{n}\right)e^{2kl\pi i/n}.$$

Из доказанных тригонометрических тождеств следует, что $g_0=g_n=0$ и при $0<l<n$

$$g_l^2=\left(\sum_{k=1}^{n-1}\left(\frac{k}{n}\right)e^{2kl\pi i/n}\right)^2=:g^2=\left(\sum_{k=1}^{n-1}\left(\frac{k}{n}\right)e^{2k\pi i/n}\right)^2.$$

Вычислим двумя способами сумму $\sum_{l=1}^{n}g_lg_{n-l}$. С одной стороны, согласно задаче 7,

$$g_lg_{n-l}=\left(\frac{l}{n}\right)\left(\frac{n-l}{n}\right)g^2=\left(\frac{n-1}{n}\right)g^2,\quad g_0=g_n=0,$$

поэтому сумма равна $(n-1)(-1/n)g^2$. С другой стороны, непосредственно после раскрытия скобок имеем

$$g_lg_{n-l}=\sum_{k=1}^{n-1}\left(\frac{k}{n}\right)e^{2kl\pi i/n}\sum_{m=1}^{n-1}\left(\frac{m}{n}\right)e^{2m(n-l)\pi i/n}=\sum_{k,m=1}^{n-1}\left(\frac{k}{n}\right)\left(\frac{m}{n}\right)e^{2(k-m)l\pi i/n},$$

откуда

$$(n-1)\left(\frac{n-1}{n}\right)g^2=\sum_{l=1}^{n}g_lg_{n-l}=\sum_{k,m=1}^{n-1}\left(\frac{k}{n}\right)\left(\frac{m}{n}\right)=$$

$$=\sum_{l=1}^{n}e^{2(k-m)l\pi i/n}=\sum_{k=1}^{n-1}\left(\frac{k}{n}\right)^2n=\sum_{k=1}^{n-1}n=n(n-1),$$

и теорема Гаусса доказана. □

Задача 14. Докажите, что для любого набора действительных чисел $(b_1,b_2,\ldots,b_n)$ справедливо неравенство Коши:

$$|b_1|+|b_2|+\ldots+|b_n|\leqslant\sqrt{n(b_1^2+b_2^2+\ldots+b_n^2)}.$$

Это неравенство обращается в равенство тогда и только тогда, когда все числа $|b_i|$ равны.

Наконец мы можем доказать теорему С. Н. Бернштейна (см. с. 88). Напомним её формулировку.

Теорема. *Пусть нечётный действительный тригонометрический многочлен*

$$t_n(x) = \sum_{k=1}^{n} b_k \sin kx$$

удовлетворяет неравенствам

$$\left| t_n\left(\frac{2\pi k}{2n+1}\right) \right| \leqslant 1, \quad k = 1, \ldots, n. \tag{$*$}$$

Тогда

$$\sum_{k=1}^{n} |b_k| \leqslant \sqrt{2n+1} - \frac{1}{\sqrt{2n+1}}.$$

Неравенство обращается в равенство при нечётных n, для которых $p = 2n+1$ — простое, и

$$b_k = \frac{2}{\sqrt{2n+1}} \left(\frac{k}{2n+1}\right), \quad k = 1, \ldots, n.$$

Пусть чётный действительный тригонометрический многочлен

$$t_n(x) = \sum_{k=1}^{n} a_k \cos kx$$

удовлетворяет условию $t_n(0) = 0$ и неравенствам $(*)$. Тогда

$$\sum_{k=1}^{n} |a_k| \leqslant \sqrt{2n+1} - \frac{1}{\sqrt{2n+1}}.$$

Неравенство обращается в равенство при чётных n, для которых $p = 2n+1$ — простое, и

$$a_k = \frac{2}{\sqrt{2n+1}} \left(\frac{k}{2n+1}\right), \quad k = 1, \ldots, n.$$

Доказательство теоремы 1. Рассмотрим случай нечётного многочлена. Воспользуемся тождеством из задачи 11, в котором выберем $x = 0$, $m = 2n+1 > 2n$, и тогда

$$\sum_{k=1}^{2n+1} t_n^2\left(\frac{2k\pi}{2n+1}\right) = \frac{2n+1}{2} \sum_{k=1}^{n} b_k^2.$$

Заметим, что середина отрезка $\left[\frac{2k\pi}{2n+1}, \frac{2(2n+1-k)\pi}{2n+1}\right]$ находится в точке π, поэтому

$$t_n\Big(\frac{2k\pi}{2n+1}\Big) = -t_n\Big(\frac{2(2n+1-k)\pi}{2n+1}\Big)$$

в силу тождества $t_n(x) = -t_n(2\pi - x)$, справедливого для всех нечётных тригонометрических многочленов. Таким образом, верхнюю границу индекса суммирования в левой части написанного выше равенства можно понизить до n, если одновременно вдвое уменьшить его правую часть (слагаемое при $k = 2n+1$ равно нулю). Следовательно, имеем

$$\sum_{k=1}^{n} t_n\Big(\frac{2k\pi}{2n+1}\Big)^2 = \frac{2n+1}{4}\sum_{k=1}^{n} b_k^2.$$

С другой стороны, из условия теоремы следует, что все слагаемые левой части последнего равенства не превосходят единицы, поэтому их сумма не превосходит числа слагаемых. Тем самым доказано неравенство

$$\sum_{k=1}^{n} b_k^2 \leqslant \frac{4n}{2n+1}.$$

Чтобы получить выписанную в условии теоремы оценку для суммы модулей коэффициентов, воспользуемся неравенством Коши:

$$\sum_{k=1}^{n} |b_k| \leqslant \sqrt{n\sum_{k=1}^{n} b_k^2} \leqslant \sqrt{\frac{4n}{2n+1}}\sqrt{n} = \sqrt{2n+1} - \frac{1}{\sqrt{2n+1}},$$

и неравенство теоремы в случае нечётного тригонометрического многочлена доказано. Конечно, всё изящество этого результата проявится лишь тогда, когда мы докажем, что полученная оценка — точная, т. е. её уже не удастся улучшить, если рассматривать всё множество нечётных тригонометрических многочленов, удовлетворяющих условиям теоремы. Для этого понадобятся тождества Гаусса.

Сначала заметим, что для коэффициентов, удовлетворяющих условию

$$|b_k| = \frac{2}{\sqrt{2n+1}}, \quad k = 1, \ldots, n,$$

неравенство теоремы превращается в равенство. Остаётся для каждого числа n из множества, указанного в теореме, предъявить нечётный тригонометрический многочлен порядка n, коэффициенты которого удовлетворяют этому условию, а его значения — условию

$$\left|t_n\Big(\frac{2\pi k}{2n+1}\Big)\right| \leqslant 1, \quad k = 1, \ldots, n,$$

что и доказывает неулучшаемость полученных неравенств. И действительно, при простом $p = 2n + 1 = 4m + 3$ и

$$b_k = \frac{2}{\sqrt{2n+1}}\left(\frac{k}{2n+1}\right), \quad k = 1, \ldots, n,$$

из теоремы Гаусса получаем:

$$\sum_{k=1}^{n}\left(\frac{k}{2n+1}\right)\sin\left(\frac{2kl\pi}{2n+1}\right) = \pm\sqrt{\frac{2n+1}{4}};$$

отсюда для любого $l = 1, \ldots, n$

$$t_n\left(\frac{2l\pi}{n}\right) = \sum_{k=1}^{n} b_k \sin\left(\frac{2kl\pi}{2n+1}\right) = \frac{2}{\sqrt{2n+1}}\sum_{k=1}^{n}\left(\frac{k}{2n+1}\right)\sin\left(\frac{2kl\pi}{2n+1}\right) = \pm 1,$$

что и требовалось доказать. □

Чётный случай аналогичен, и мы предлагаем читателю разобрать его самостоятельно, по аналогии с доказательством для нечётного тригонометрического многочлена.

Список литературы

[1] *Bernstein Serge.* Sur certaines fonctions périodiques qui s'écartent le moins possible de zéro // Сообщ. Харьковского математ. об-ва. Сер. 2. Т. 14. 1914. С. 145–152.

[2] *Серр Ж.-П.* Курс арифметики. М.: Мир, 1972.

Сергей Борисович Гашков, мехмат МГУ
`sbgashkov@gmail.com`

Сергей Владимирович Кравцев, мехмат МГУ
`svkrav@gmail.com`