Лагранж і його теоерма про чотири квадрати

Ярослав Ківва

Київський національний університет імені Тараса Шевченка

16 лютого 2019 р.

Жозеф Луї Лагранж: 1

Жозеф Луї Лагранж (1736–1813) народився в Туріні, а помер і похований в Парижі. В його жилах текла французька та італійська кров, і тому обидві нації можуть пишатися чоловіком, який (за словами Талейрана) зробив своїм генієм честь всьому людству.

Жозеф Луї Лагранж: 2

За своїми науковими поглядами Лагранж відрізнявся від свого старшого великого сучасника – Леонарда Ейлера. Ейлер протягом свого життя розв'зував і розв'язав величезну, небачену, ні з чим не порівнянну кількість окремих, конкретних задач, і у більшості своїй кожну задачу він розв'язував своїм, особливим, особливим, індивідуальним прийомом.

Лагранж же намагався відшукати загальні закономірності у різнорідних явищ, знайти потаємні зв'язки між окремими об'єктами, розкрити єдність здавалося б непоєднуваного. Але при всьому при тому йому належить також і безліч чудових конкретних результатів. Про один з них – про подання натуральних чисел у вигляді суми чотирьох квадратів – і буде зараз розказано.

Жозеф Луї Лагранж: 3

Лагранж залишився у вдячній пам'яті людства як світла, благородна особистість. Ось як характеризує його Фур'є: "Лагранж був настільки ж філософ, наскільки математик. Він довів це своїм життям, помірністю бажань земних благ, глибокою відданістю загальним інтересам людства, шляхетною простотою своїх звичок, височиною душі і глибокої справедливістю в оцінці праці своїх сучасників."

А тепер перейдемо до формулювання і доведення теореми Лагранжа.

Теорема: формулювання і перша лема

Теорема. Кожне натуральне число є сумою чотирьох квадратів цілих чисел:

$$\mathbb{N} = \left\{ a_1^2 + a_2^2 + a_3^2 + a_4^2 \middle| a_1, a_2, a_3, a_4 \in \mathbb{Z} \right\} \stackrel{\text{def}}{=} S.$$

Лема. Множина чисел що можуть бути подані у вигляді суми чотирьох квадратів замкнута відносно множення, тобто добуток чисел, що подаються у вигляді суми чотирьох квадратів, подається у вигляді суми чотирьох квадратів: $a, b \in S \implies a \cdot b \in S$.

Доведення леми:

$$\begin{aligned}
(a_1^2 + a_2^2 + a_3^2 + a_4^2) \cdot (b_1^2 + b_2^2 + b_3^2 + b_4^2) = \\
= (a_1 b_1 + a_2 b_2 + a_3 b_3 + a_4 b_4)^2 + \\
+ (-a_1 b_2 + a_2 b_1 - a_3 b_4 + a_4 b_3)^2 + \\
+ (-a_1 b_3 + a_3 b_1 - a_4 b_2 + a_2 b_4)^2 + \\
+ (-a_1 b_4 + a_4 b_1 - a_2 b_3 + a_3 b_2)^2.
\end{aligned}$$

Друга лема: формулювання і початок доведення

Лема. Для довільного непарного простого знайдеться кратне йому менше за його квадрат що подається у вигляді суми трьох квадратів:

$$\forall p \in \mathbb{P} \setminus \{2\} : \exists n \in \{1, \dots, p-1\}, a, b, c \in \mathbb{Z} : a^2 + b^2 + c^2 = np.$$

Доведення леми: Розглянемо дві множини лишків із $\mathbb{Z}_p$:

$$K = \left\{ 0^2, 1^2, 2^2, \dots, \left(\frac{p-1}{2} \right)^2 \right\},$$

$$L = \left\{ -1 - 0^2, -1 - 1^2, -1 - 2^2, \dots, -1 - \left(\frac{p-1}{2} \right)^2 \right\}.$$

Зрозуміло, що в кожній з цих множин всі лишки різні. Справді,

$$k_1^2 \overset{p}{\equiv} k_2^2 \vee -1 - k_1^2 \overset{p}{\equiv} -1 - k_2^2 \implies k_1^2 \overset{p}{\equiv} k_2^2 \implies k_1^2 - k_2^2 \overset{p}{\equiv} 0 \implies$$

$$\implies (k_1 + k_2) \cdot (k_1 - k_2) \overset{p}{\equiv} 0 \implies k_1 + k_2 \overset{p}{\equiv} 0 \vee k_1 - k_2 \overset{p}{\equiv} 0.$$

Друга лема: завершення доведення

Жодне з цього неможливо бо $0 \le k_1 \ne k_2 \le \frac{p-1}{2}$, а тому $0 < k_1 + k_2 < p - 1$ та $k_1 - k_2 \ne 0$ і $|k_1 - k_2| < \frac{p-1}{2}$.

Але тоді у цих множинах сумарно $p + 1$ лишок, а отже є два однакових, причому вони з різних множин, тобто

$$\exists k, l : k^2 \overset{p}{\equiv} -1 - l^2,$$

тобто $np = k^2 + l^2 + 1^2$, (майже) отримали що хотіли.

Лишилося помітити, що $k, l \le \frac{p-1}{2} < \frac{p}{2}$, тому

$$k^2 + l^2 + 1 \le \left(\frac{p}{2}\right)^2 + \left(\frac{p}{2}\right)^2 + 1 = \frac{p^2}{2} + 1 < p^2,$$

тобто $n < p$.

Третя лема: формулювання і початок доведення

Лема. Довільне просте число подається у вигляді суми чотирьох квадратів.

Доведення леми: для $p = 2$ маємо $2 = 1^2 + 1^2 + 0^2 + 0^2$, для $p > 2$ за другою лемою $np \in S$ для якогось натурального $n < p$. Розглянемо найменше n для якого $np \in S$. Якщо воно парне, то $np = n_1^2 + n_2^2 + n_3^2 + n_4^2$, де, без обмеження загальності, $n_1 \equiv n_2 \pmod 2$, $n_3 \equiv n_4 \pmod 2$. Це так, бо серед n_1, n_2, n_3, n_4 парна кількість парних чисел. Тоді $\frac{n_1+n_2}{2}, \frac{n_1-n_2}{2}, \frac{n_3+n_4}{2}, \frac{n_3-n_4}{2} \in \mathbb{Z}$, причому

$$\left(\frac{n_1+n_2}{2}\right)^2 + \left(\frac{n_1-n_2}{2}\right)^2 + \left(\frac{n_3+n_4}{2}\right)^2 + \left(\frac{n_3-n_4}{2}\right)^2 =$$
$$= \frac{n_1^2+n_2^2+n_3^2+n_4^2}{2} = \frac{n}{2} \cdot p,$$

суперечність з мінімальністю n.

Третя лема: продовження доведення

Якщо тепер n непарне, то запишемо $n_i = q_i n + k_i$ для $i = \overline{1..4}$, причому так, щоб $|k_i| < \frac{n}{2}$, тобто майже ділимо n_i із залишком на n. Тоді

$$np = n_1^2 + n_2^2 + n_3^2 + n_4^2 = ln + k_1^2 + k_2^2 + k_3^2 + k_4^2,$$

де l – якесь ціле число. Як наслідок,

$$k_1^2 + k_2^2 + k_3^2 + k_4^2 = kn,$$

де k – невід'ємне ціле число. Якщо $k = 0$, то всі $k_i = 0$, і тоді

$$np = n_1^2 + n_2^2 + n_3^2 + n_4^2 = n^2 l,$$

де l – натуральне, тобто $p = nl$, $n < p$, а це означає, що $n = 1$. Припустимо тепер що $k \geq 1$.

Третя лема: завершення доведення

Якщо $k \geq 1$, то з леми 1 можемо записати

$$(n_1^2 + n_2^2 + n_3^2 + n_4^2) \cdot (k_1^2 + k_2^2 + k_3^2 + k_4^2) = l_1^2 + l_2^2 + l_3^2 + l_4^2,$$

де

$$l_i = \pm_{i_1} n_1 k_{i_1} \pm_{i_2} n_2 k_{i_2} \pm_{i_3} n_3 k_{i_3} \pm_{i_4} n_4 k_{i_4}.$$

За визначенням, $n_i \equiv k_i \pmod{n}$, тому $l_i \equiv 0 \pmod{n}$, тобто $\frac{l_i}{n} \in \mathbb{Z}$, тому

$$(np) \cdot (kn) = l_1^2 + l_2^2 + l_3^2 + l_4^2,$$

звідки остаточно

$$kp = \left(\frac{l_1}{n}\right)^2 + \left(\frac{l_2}{n}\right)^2 + \left(\frac{l_3}{n}\right)^2 + \left(\frac{l_4}{n}\right)^2,$$

суперечність з мінімальністю n.

Теорема: завершення доведення

Щойно доведене $\mathbb{P} \subset S$ укупі з

$$a, b \in S \implies a \cdot b \in S$$

дає нам

$$\mathbb{N} \setminus \{0, 1\} \subset S.$$

Нарешті

$$0 = 0^2 + 0^2 + 0^2 + 0^2,$$
$$1 = 1^2 + 0^2 + 0^2 + 0^2,$$

що завершує доведення.