Суммы квадратов и целые гауссовы числа

В.СЕНДЕРОВ, А.СПИВАК

«Зачем складывать простые числа? – недоумевал великий физик Ландау. – Простые числа созданы для того, чтобы их умножать, а не складывать!»

ЗАЧЕМ СКЛАДЫВАТЬ КВАДРАТЫ ЦЕЛЫХ ЧИСЕЛ? Почему бы не складывать их кубы или 666-е степени? Вопросы эти весьма серьезны и встают перед каждым, кто начинает изучать математику. Из огромного разнообразия задач не все достойны пристального внимания. Задача о сумме квадратов – в высшей степени достойна. К сожалению для философа, это невозможно объяснить, не рассказав ее решение и не углубившись тем самым в детали.

«Детали» – это критерий того, какие натуральные числа представимы в виде суммы квадратов двух целых чисел. В доказательстве этого критерия будут использованы не только «обычные» целые числа, но и числа комплексные – прекрасный пример применения абстрактной теории к конкретной арифметической задаче! Хотя эта статья содержит лишь малую часть богатейшей теории делимости алгебраических чисел, надеемся, ее очарование никого не оставит равнодушным.

Иллюстрация В.Власова

Суммы квадратов

Если вы внимательно проследите за вычислениями в основном тексте и будете рассматривать упражнения вычислительного характера не только как отнимающие время (неизбежно они обладают этой особенностью), но и как представляющие интерес, доставляющие наслаждение и понимание, то я убежден, что вы сможете оценить как мощь, так и крайнюю простоту теории.

Г.Эдвардс

Таблица сумм квадратов

Рассмотрим таблицу, в верхней строке и левом столбце которой – квадраты целых чисел, а в других клетках – суммы квадратов:

0	1	4	9	16	25	36	49	64	81	100
1	2	5	10	17	26	37	50	65	82	101
4	5	8	13	20	29	40	53	68	85	104
9	10	13	18	25	34	45	58	73	90	109
16	17	20	25	32	41	52	65	80	97	116
25	26	29	34	41	50	61	74	89	106	125
36	37	40	45	52	61	72	85	100	117	136
49	50	53	58	65	74	85	98	113	130	149
64	65	68	73	80	89	100	113	128	145	164
81	82	85	90	97	106	117	130	145	162	181
100	101	104	109	116	125	136	149	164	181	200

Эта таблица позволяет выписать представления: $1 = 1^2 + 0^2$, $2 = 1^2 + 1^2$, $4 = 2^2 + 0^2$, $5 = 2^2 + 1^2$, $8 = 2^2 + 2^2$, $9 = 3^2 + 0^2$, $10 = 3^2 + 1^2$, $13 = 3^2 + 2^2$,... Не вошедшие в таблицу числа первой сотни (3, 6, 7, 11, 12, 14, 15,...) в виде суммы двух квадратов не представимы.

Упражнение 1. Найдите наименьшее число, которое двумя существенно разными (т. е. не получающимися один из другого перестановкой слагаемых) способами представимо в виде суммы двух квадратов а) целых; б) натуральных чисел.

Остатки от деления на 3

Наименьшее натуральное число, не представимое в виде суммы двух квадратов целых чисел,– это 3. Кратные 3 числа 6, 12, 15, 21 тоже не представимы, а вот числа $9 = 3^2 + 0^2$ и $18 = 3^2 + 3^2$ – представимы. Возникает гипотеза: числа, которые кратны 3, но не кратны 9, не представимы в виде суммы двух квадратов. Эта гипотеза верна. Верно даже более сильное утверждение:

Теорема 1. *Если сумма квадратов $x^2 + y^2$ целых чисел x, y кратна 3, то числа x, y тоже кратны 3.*

Доказательство. Выпишем остатки от деления квадратов целых чисел на 3:

Закономерность очевидна: остатки периодически повто-

Квадрат	0	1	4	9	16	25	36	49	64	81	100
Остаток	0	1	1	0	1	1	0	1	1	0	1

ряются, и никаких остатков кроме 0 и 1 не бывает. (Точнее говоря, остаток от деления квадрата целого числа x на 3 равен 0, если x кратно 3, т. е. представимо в виде $x = 3k$, где k – целое число, и остаток равен 1, если x не кратно 3, т. е. представимо в виде $x = 3k \pm 1$. В самом деле, в первом случае $x^2 = 9k^2$ делится на 3 без остатка, а во втором случае $x^2 = 9k^2 \pm 6k + 1$ дает при делении на 3 остаток 1.)

Суммы остатков 0 + 1 и 1 + 1 не кратны 3. Значит, сумма квадратов $x^2 + y^2$ кратна 3 в том и только том случае, когда x и y кратны 3.

Упражнение 2. Докажите, что если сумма квадратов двух целых чисел кратна 3^{1999}, то эта сумма кратна 3^{2000}.

Остатки от деления на 7

Следующее после 3 и 6 не представимое в виде суммы двух квадратов число – это 7. Кратные 7 числа 14, 21, 28, 35, 42, 56, 63 не представимы в виде суммы квадратов. Опять возникает гипотеза: *если сумма квадратов $x^2 + y^2$ кратна 7, то и сами целые числа x, y кратны 7.*

Для доказательства составим таблицу остатков от деления квадратов на 7:

Квадрат	0	1	4	9	16	25	36	49	64	81	100	121	144	169	196
Остаток	0	1	4	2	2	4	1	0	1	4	2	2	4	1	0

Остатки, как видите, периодически повторяются. Поскольку сумма никаких двух из остатков 1, 2, 4 не кратна 7, мы доказали нашу гипотезу.

Упражнения

3. Остаток от деления квадрата целого числа x на 7 равен 0, если $x = 7k$, где k – целое число; равен 1, если $x = 7k \pm 1$; равен 2, если $x = 7k \pm 3$; равен 4, если $x = 7k \pm 2$. Докажите это.

4. Докажите, что если сумма квадратов двух целых чисел кратна 21, то она кратна и 441.

5. а) Какие остатки дают квадраты целых чисел при делении на 11? б) Докажите, что если сумма квадратов двух целых чисел кратна 11, то она кратна 121. в) Докажите, что если сумма квадратов двух целых чисел кратна 1331, то она кратна и 14641.

Остатки от деления на 19

Если простое число p представлено в виде суммы квадратов, $p = x^2 + y^2$, то, очевидно, числа x, y меньше p и потому не могут быть кратны p. Значит, на роль тех чисел p, для которых из делимости суммы квадратов на p следует делимость на p обоих слагаемых, претендуют только числа, не представимые в виде суммы двух квадратов. Любое такое число можно исследовать аналогично числам 3 и 7.

Например, пусть $p = 19$. Составим таблицу остатков от деления квадратов на 19:

Квадрат	0	1	4	9	16	25	36
Остаток	0	1	4	9	16	6	17
Квадрат	49	64	81	100	121	144	169
Остаток	11	7	5	5	7	11	17
Квадрат	196	225	256	289	324		
Остаток	6	16	9	4	1		

В верхней строке – квадраты чисел 0, 1,..., 18. (Другие квадраты можно не рассматривать, поскольку любое целое число x можно представить в виде $x = 19q + r$, где q – целое, $0 \le r \le 18$, и при этом число $x^2 = 19^2 q^2 +$

$+38qr + r^2$ дает при делении на 19 такой же остаток, как и r^2.)

В нижней строке таблицы один раз присутствует число 0 и по два раза – числа 1, 4, 5, 6, 7, 9, 11, 16 и 17. Ненулевые остатки от деления квадратов целых чисел на простое число $p > 2$ называют *квадратичными вычетами* по модулю p. Все другие ненулевые остатки – *квадратичные невычеты* (при $p = 19$ это 2, 3, 8, 10, 12, 13, 14, 15 и 18).

Поскольку сумма никаких двух из чисел 1, 4, 5, 6, 7, 9, 11, 16 и 17 не кратна 19, приходим к выводу: сумма квадратов двух целых чисел кратна 19 в том и только том случае, когда слагаемые кратны 19.

Упражнение 6. Если p – простое число, $p > 2$, то существует $(p-1)/2$ квадратичных вычетов и ровно столько же квадратичных невычетов по модулю p. Докажите это.

Свойство простых чисел, не являющихся суммами двух квадратов

Как относиться к трудностям? В области неведомого надо рассматривать трудности как скрытый клад! Обычно: чем труднее, тем полезнее. Не так ценно, если трудности возникают от твоей борьбы с самим собой. Но когда трудности исходят от увеличившегося сопротивления предмета – это прекрасно!!

А.И.Солженицын

Чем больше по величине простое число p, тем больше квадратичных вычетов по модулю p. Поэтому пора менять метод исследования: если мы не желаем погрязнуть в нескончаемых вычислениях, то должны каким-то одним общим рассуждением охватить числа 3, 7, 11, 19 и многие другие простые числа.

Пока не вполне ясно, что это за числа и чем они отличаются от чисел 2, 5, 13, 17,... Впрочем, одно отличие очевидно: числа 3, 7, 11, 19 не представимы, а числа 2, 5, 13, 17 представимы в виде суммы квадратов двух целых чисел. Кроме того, простые числа $p = 3, 7, 11, 19$ обладают, как мы уже доказали, тем свойством, что если сумма квадратов целых чисел кратна p, то каждое из слагаемых кратно p. Продолжив (довольно утомительные, если не использовать компьютер) вычисления, можно доказать это свойство для $p = 23, 31, 43, 47, 59, 67, 71, 79, 83, 87$. Осечки ни разу не будет:

Теорема 2. *Если простое число p не представимо в виде суммы двух квадратов и если сумма квадратов $x^2 + y^2$ кратна p, то каждое из целых чисел x, y кратно p.*

Мы получим эту теорему как одно из следствий теории целых гауссовых чисел. Поскольку это не так уж просто, давайте отвлечемся на некоторое время от теоремы 2 и обратим внимание на другое свойство рассматриваемых простых чисел 3, 7, 11,..., 83, 87: *при делении на 4 они дают остаток 3.*

Числа вида $4n + 3$

В виде суммы двух квадратов не представимы не только простые числа, которые при делении на 4 дают остаток 3, но и вообще все числа 3, 7, 11, 15, 19, 23, 27,...:

Теорема 3. *Всякое представимое в виде суммы квадратов двух целых чисел нечетное число при делении на 4 дает остаток 1, а не 3.*

Доказательство. Из двух квадратов, сумма которых нечетна, обязательно один четен, а другой нечетен. Квадрат четного числа нацело делится на 4, а квадрат нечетного числа при делении на 4 дает остаток 1 (проверьте!).

Упражнение. 7 а) Квадрат нечетного числа дает остаток 1 не только при делении на 4, но даже при делении на 8. Докажите это. б) Решите в целых числах уравнение $x^2 + y^2 + z^2 = 8n - 1$. в) Никакое число вида $4^m(8n+7)$, где m, n – целые неотрицательные числа, не представимо в виде суммы квадратов трех целых чисел. Докажите это.

Произведение сумм квадратов

Мы уже нашли несколько признаков непредставимости числа в виде суммы двух квадратов. Не менее важны признаки представимости. Начнем с того, что если $n = x^2 + y^2$, то

$$(x+y)^2 + (x-y)^2 = x^2 + 2xy + y^2 + x^2 - 2xy + y^2 = 2\left(x^2 + y^2\right) = 2n.$$

Значит, вместе с каждым представимым числом n представимо и число $2n$. Далее,

$$(2x+y)^2 + (x-2y)^2 = 4x^2 + 4xy + y^2 + x^2 - 4xy + 4y^2 = 5\left(x^2 + y^2\right) = 5n.$$

Легко проверить и формулы

$$(2x+3y)^2 + (3x-2y)^2 = 13n,$$

$$(4x+y)^2 + (x-4y)^2 = 17n.$$

Все они являются частными случаями общей формулы, которая представляет произведение сумм двух квадратов в виде суммы двух квадратов. Чтобы получить ее, раскроем скобки

$$\left(a^2 + b^2\right)\left(x^2 + y^2\right) = a^2x^2 + b^2x^2 + a^2y^2 + b^2y^2,$$

прибавим и отнимем $2abxy$ и изменим порядок слагаемых:

$$\left(a^2 + b^2\right)\left(x^2 + y^2\right) = a^2x^2 + 2axby + b^2y^2 + b^2x^2 - 2bxay + a^2y^2 = (ax+by)^2 + (bx-ay)^2. \quad (1)$$

Упражнение 8. Докажите, что

а) если четное число n есть сумма квадратов двух целых чисел, то и число $n/2$ представимо в виде суммы квадратов двух целых чисел;

б)* если кратное 5 число n есть сумма квадратов двух целых чисел, то число $n/5$ тоже представимо в таком виде;

в)* если $13k = x^2 + y^2$, где k, x, y – целые числа, то хотя бы одна из формул $k = \left(\frac{3x+2y}{13}\right)^2 + \left(\frac{2x-3y}{13}\right)^2$ и $k = \left(\frac{3x-2y}{13}\right)^2 + \left(\frac{2x+3y}{13}\right)^2$ представляет k в виде суммы квадратов целых чисел.

Теорема Ферма–Эйлера

Поскольку мы научились представлять произведение сумм двух квадратов в виде суммы двух квадратов, очень важно выяснить, какие простые числа представимы в виде суммы двух квадратов целых чисел, а какие не представимы. Числа вида $4n + 3$, как утверждает теорема 3, не представимы. Поэтому рассмотрим простые числа, которые при делении на 4 дают остаток 1. Это: $5 = 2^2 +$

$+1^2$, $13 = 3^2 + 2^2$, $17 = 4^2 + 1^2$, $29 = 5^2 + 2^2$, $37 = 6^2 + 1^2$, $41 = 5^2 + 4^2$, $53 = 7^2 + 2^2$,…

Теорема 4. *Любое простое число p, которое при делении на 4 дает остаток 1, представимо в виде суммы квадратов двух натуральных чисел.*

Мы приведем доказательство, состоящее из следующих двух лемм.

Лемма 1. *Для любого простого числа $p = 4n + 1$, где $n \in \boldsymbol{N}$, существует такое целое число m, что $m^2 + 1$ кратно p.*

Лемма 2. *Любой простой делитель p числа $m^2 + 1$, где m – целое, представим в виде суммы квадратов двух натуральных чисел.*

Упражнение 9. Пользуясь формулой (1), объясните, почему в лемме 2 слова «любой простой» можно заменить на «любой натуральный».

Лемму 1 мы выведем из теоремы Вильсона (1741–1793), лемму 2 – из теории делимости целых гауссовых чисел. Но сначала сформулируем ответ на один важный вопрос.

Какие натуральные числа – суммы двух квадратов?

По теоремам 3 и 4, простое число $p > 2$ не представимо в виде суммы двух квадратов, если оно имеет вид $p = 4k + 3$, и представимо – если $p = 4k + 1$, где k – целое. Вспомнив формулу (1) и применив (еще не доказанную нами) теорему 2, получаем следующий элегантный критерий: *натуральное число представимо в виде суммы квадратов двух целых чисел тогда и только тогда, когда в его разложение на простые множители любой простой множитель вида $4k + 3$ входит в четной степени.*

Этот критерий впервые был сформулирован голландцем Альбером Жираром (1595–1632) в следующем виде: натуральное число представимо в виде суммы двух квадратов тогда и только тогда, когда оно является или квадратом, или числом 2, или простым числом, которое на 1 больше, чем некоторое кратное 4, или произведением нескольких вышеперечисленных чисел. Скорее всего, Жирар опирался лишь на изучение таблиц и не претендовал на то, что может доказать необходимость и достаточность своих условий.

Упражнения

10. Докажите, что 15 не представимо в виде суммы квадратов двух рациональных чисел. (Этот факт упомянут в «Арифметике» древнегреческого математика Диофанта.)

11. Выведите из критерия представимости числа в виде суммы двух квадратов, что если сумма квадратов $x^2 + y^2$ целых чисел кратна p^{2s-1}, где s – натуральное число, p – простое число, которое при делении на 4 дает остаток 3, то числа x и y кратны p^s.

12. Докажите, что существует бесконечно много натуральных чисел, которые дают остаток 1 при делении на 4, но не представимы в виде суммы квадратов двух целых чисел.

13. а) Для любого делителя d числа $n^2 + 1$, где $n \in \boldsymbol{N}$, существует бесконечно много таких $m \in \boldsymbol{N}$, что $m^2 + 1$ кратно d. Докажите это. б) Сколько существует натуральных чисел $n < 1000$, для которых $n^2 + 1$ кратно 65?

14. Из леммы 2 и теоремы 3 выведите, что число вида $n^2 + 1$, где $n \in \boldsymbol{N}$, не имеет ни одного делителя вида $4k - 1$, где $k \in \boldsymbol{N}$.

15. Докажите, что если x, y, z – целые числа и $4xy - x - y = z^2$, то $x \ge 0$ и $y \ge 0$. (Это упражнение придумал Л. Эйлер.)

16. а) Никакое число вида $m^2 + 1$ не кратно никакому числу вида $n^2 - 1$, где m, n – целые числа, $n > 1$. Докажите это. б) Решите в целых числах уравнение $x^2y^2 = x^2 + y^2 + z^2$.

Доказательство леммы 1

В качестве числа m в лемме 1 годится $m = (2n)!$, т. е. произведение первых $2n$ натуральных чисел. Чтобы это увидеть, рассмотрим число

$$(p-1)! = 1 \cdot 2 \cdot \ldots \cdot (2n-1) \cdot (2n) \times \times (2n+1) \cdot (2n+2) \cdot \ldots \cdot (4n-1) \cdot (4n) = = 1 \cdot 2 \cdot \ldots \cdot (2n-1) \cdot (2n) \cdot (p-2n) \times \times \big(p-(2n-1)\big) \cdot \ldots \cdot (p-2) \cdot (p-1).$$

Оно дает при делении на p такой же остаток, как и число

$$1 \cdot 2 \cdot \ldots \cdot (2n-1) \cdot (2n) \cdot (-1)^{2n} \cdot (2n) \cdot (2n-1) \cdot \ldots \cdot 2 \cdot 1 = m^2.$$

Значит, $m^2 + 1$ при делении на p дает такой же остаток, как и число $(p - 1)! + 1$. Последнее число кратно p по теореме Вильсона, которая впервые была сформулирована англичанином Эдуардом Варингом (1734–1798), а доказана французом Жозефом Луи Лагранжем (1736–1813).

Теорема Вильсона. *Для любого простого числа p сумма $(p - 1)! + 1$ кратна p. (Другими словами, произведение $1 \cdot 2 \cdot \ldots \cdot (p - 1)$ дает остаток $(p - 1)$ при делении на p.)*

Доказательство этой теоремы можно узнать, например, из статьи А. Егорова и А. Котовой «Необыкновенные арифметики» (Приложение к журналу «Квант» № 2 за 1994 год).

Итак, мы вывели лемму 1 из теоремы Вильсона. Идея доказательства леммы 2 – разложение на множители $m^2 + 1 = (m + i)(m - i)$. Что такое i и что делать дальше, вы узнаете, когда познакомитесь с комплексными числами.

Упражнения

17. Докажите, что числа а) $97! \cdot 1901! - 1$; б) $98! \cdot 1900! + 1$ кратны 1999. *Указание.* 1999 – простое число.

18. Если p – простое число, $p > 2$, $m = ((p - 1)/2)!$, то $m^2 \equiv (-1)^{(p+1)/2} \pmod p$, т.е. остаток от деления на p числа m^2 равен 1, если $p = 4n + 3$, и равен $p - 1$, если $p = 4n + 1$. Докажите это.

19. Докажите, что а) если составное число $n > 4$, то $(n - 1)!$ кратно n; б) если $(n - 1)! + 1$ кратно n, где $n > 1$ – натуральное число, то n – простое.

Комплексные числа

Что нам стоит дом построить?
Нарисуем – будем жить!

Что такое комплексное число?

Новые числа в математике вводят, когда старых оказывается недостаточно. Изобретение целых чисел, т. е. расширение множества $\boldsymbol{N} = \{1, 2, 3,\ldots\}$ натуральных чисел до множества $\boldsymbol{Z} = \{\ldots, -2, -1, 0, 1, 2,\ldots\}$, дает возможность решить, например, уравнение $x + 7 = 5$. Построив еще более широкое множество $\boldsymbol{Q} = \{\frac{m}{n} \mid m \in \boldsymbol{Z}, n \in \boldsymbol{N}\}$ рациональных чисел, мы получаем возможность решать уравнения вроде $3x = 8$. Желание измерить диагональ единичного квадрата (или, что то же, решить уравнение $x^2 = 2$) приводит к очередному расширению множества

чисел до множества $Q[\sqrt{2}]$ чисел вида $a + b\sqrt{2}$, где a, $b \in \boldsymbol{Q}$. Нет никаких сомнений, что сумма, разность и произведение чисел вида $a + b\sqrt{2}$ – число такого же вида. С делением тоже все в порядке:

$$\frac{1+\sqrt{2}}{3-2\sqrt{2}} = \frac{\left(1+\sqrt{2}\right)\left(3+2\sqrt{2}\right)}{\left(3-2\sqrt{2}\right)\left(3+2\sqrt{2}\right)} = 7+5\sqrt{2},$$

$$\frac{2-5\sqrt{2}}{3+\sqrt{2}} = \frac{\left(2-5\sqrt{2}\right)\left(3-\sqrt{2}\right)}{\left(3+\sqrt{2}\right)\left(3-\sqrt{2}\right)} = \frac{16-17\sqrt{2}}{7}.$$

Видите, как просто? В общем виде это выглядит так:

$$\frac{a+b\sqrt{2}}{c+d\sqrt{2}} = \frac{\left(a+b\sqrt{2}\right)\left(c-d\sqrt{2}\right)}{\left(c+d\sqrt{2}\right)\left(c-d\sqrt{2}\right)} = \frac{ac-2bd+(bc-ad)\sqrt{2}}{c^2-2d^2}.$$

Для алгебраических вычислений важно, что квадрат числа $\sqrt{2}$ равен 2. Комплексные числа мы получим, введя в рассмотрение число i, квадрат которого равен -1. Может показаться, что «такого не бывает», ведь уравнение $x^2 + 1 = 0$ не имеет решений не только в рациональных, но и в вещественных числах. Однако число $\sqrt{2}$, заметьте, тоже «не существовало» до тех пор, пока мы рассматривали только рациональные числа.

Итак, рассмотрим выражения вида $a + bi$, где a, b – вещественные числа. Эти выражения мы и будем называть *комплексными числами*. Сумму и произведение *определим* естественными формулами

$$(a+bi)+(c+di) = (a+c)+(b+d)i,$$

$$(a+bi)\cdot(c+di) = (ac-bd)+(ad+bc)i.$$

Последняя формула, быть может, нуждается в комментарии:

$$(a+bi)\cdot(c+di) = ac + adi + bci + bdi^2 =$$

$$= ac + adi + + bci - bd.$$

Это именно комментарий, а не доказательство, поскольку пользоваться обычными правилами раскрытия скобок можно только после того, как даны определения сложения и умножения комплексных чисел и проверены эти «обычные правила», т. е. формулы $z_1 + z_2 = z_2 + z_1$ (переместительный закон, или коммутативность сложения), $z_1 z_2 = z_2 z_1$ (коммутативность умножения), $(z_1 + z_2) + z_3 = z_1 + (z_2 + z_3)$ (сочетательный закон, или ассоциативность сложения), $(z_1 z_2) z_3 = z_1 (z_2 z_3)$ (ассоциативность умножения), $(z_1 + z_2) z_3 = z_1 z_3 + z_2 z_3$ (распределительный закон, или дистрибутивность).

Упражнения

20. Выполните эту проверку.

21. Докажите, что а) для любого комплексного числа z существует и определено единственным образом такое число w, что $z + w = 0 + 0i$; б) для любого отличного от числа $0 + 0i$ комплексного числа z существует и определено единственным образом такое число w, что $zw = 1 + 0i$.

в) Научитесь делить комплексные числа, т.е. для вещественных чисел a, b, c, d найдите, при условии $c^2 + d^2 \neq 0$, такие вещественные числа x и y, что $a + bi = (c + di)(x + yi)$. (Не удивляйтесь, что последняя формула записана без знака деления: если бы он был, то все равно пришлось бы дать определение частного $(a + bi)/(c + di)$ комплексных чисел. А самый разумный способ сделать это – назвать частным u/v, где $v \neq 0$, такое число w, что $u = vw$.)

22. Вычислите: а) i^3; б) i^4; в) i^{1999}; г) $1 + i + i^2 + \ldots + i^{10} + i^{11}$; д) $(1+i)^{12}$; е) $\left(i^{34}+i^{39}\right)\Big/\left(i^{41}+i^{44}\right)$.

Геометрическая интерпретация

Формулы сложения и умножения комплексных чисел позволяют отождествить комплексное число $a + 0i$ с вещественным числом a. Поэтому в дальнейшем мы будем писать не $a + 0i$, а попросту a.

Расширение множества $\boldsymbol{R}$ вещественных чисел до множества $\boldsymbol{C}$ комплексных чисел можно пояснить геометрически. Отождествим ось абсцисс координатной плоскости с вещественной осью (т.е. множеством всех вещественных чисел); единичный вектор (1; 0) оси абсцисс обозначим просто 1, а единичный вектор (0; 1) оси ординат обозначим через i (рис.1). Произвольный вектор $z = (x; y)$ плоскости можно теперь записать в виде $z = x(1; 0) + y(0; 1) = x + yi$. Принято вещественные числа x и y называть *вещественной и мнимой частями* комплексного числа z. Обозначения: $x = \mathrm{Re}\, z$, $y = \mathrm{Im}\, z$. Сложение комплексных чисел –это обычное сложение векторов. А умножение определяется, как мы уже видели, более «хитрой» формулой.

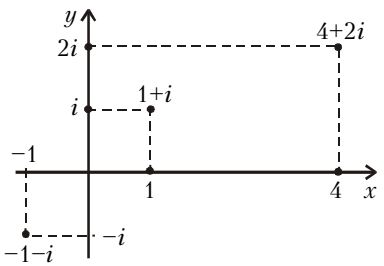

Рис. 1

Модуль комплексного числа

Определение. *Модулем (абсолютной величиной) числа $z = a + bi$ называют расстояние $|z| = \sqrt{a^2 + b^2}$ от начала координат до точки $(a; b)$.*

Теорема 5. *Модуль произведения комплексных чисел равен произведению их модулей:*

$$\left|(a+bi)(x+yi)\right| = |a+bi|\cdot|x+yi|.$$

Доказательство. Воспользуемся формулой (1):

$$\left|(a+bi)(x+yi)\right| = \left|(ax-by)+(ay+bx)i\right| =$$

$$= \sqrt{(ax-by)^2+(ay+bx)^2} = \sqrt{\left(a^2+b^2\right)\left(x^2+y^2\right)} =$$

$$= |a+bi|\cdot|x+iy|.$$

Упражнения

23. Научитесь извлекать квадратный корень из комплексного числа, т. е. для вещественных чисел a, b найдите такие пары $(x; y)$ вещественных чисел, что $(x + iy)^2 = a + bi$.

24. Решите в комплексных числах уравнения: а) $z^2 - 2z + 1 = i$; б) $z^2 - 5z + 7 = i$; в) $z^2 + 10 + 2i = (4 + i)z$.

Сопряженные числа

Уравнение $z^2 = -1$ имеет два корня: i и $-i$. Поскольку при вычислениях используется именно равенство $i^2 = -1$, возникает идея заменить i на $-i$. Верное равенство при одновременной замене всех входящих в него символов i на $-i$ останется верным!

Точная реализация этой идеи такова: два комплексных числа, действительные части которых равны, а мнимые части равны по абсолютной величине и противоположны по знаку, называют сопряженными. Число, сопряженное

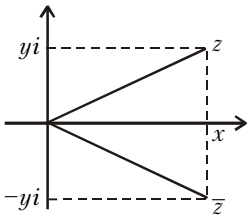

Рис. 2

с $z = x + yi$, обозначают $\overline{z} = x - yi$ (рис.2). Геометрический смысл перехода от числа к сопряженному – симметрия относительно оси абсцисс. Легко проверить тождества

$$\overline{u+v} = \overline{u} + \overline{v},\ \overline{u \cdot v} = \overline{u} \cdot \overline{v},$$

которые как раз и позволяют заменять в формулах все числа на сопряженные.

Между прочим, $|z|^2 = x^2 + y^2 = (x + iy)(x - iy) = z\overline{z}$. Это позволяет очень изящно доказать теорему 5:

$$|uv|^2 = (uv)\overline{uv} = uv\overline{uv} = (u\overline{u})(v\overline{v}) = |u|^2 \cdot |v|^2.$$

Формула (1) не потребовалась! Точнее, формула (1) – это по сути и есть формула $|uv|^2 = |u|^2 \cdot |v|^2$.

Целые гауссовы числа

Определения

Комплексное число $a + bi$ называют *целым гауссовым*, если a и b – целые числа. Сумма, разность и произведение целых гауссовых чисел – целые гауссовы числа, так что множество $\boldsymbol{Z}[i]$ целых гауссовых чисел является, как говорят алгебраисты, кольцом.

Определение. *Целое гауссово число u кратно целому гауссову числу v, если существует такое целое гауссово число w, что $u = vw$.*

Отметив на плоскости целые гауссовы числа, мы получим решетку (рис.3). Интересно, что числа, кратные данному числу z, тоже образуют решетку (рис.4).

На рисунке 5 синим цветом выделены кратные числа $2 + i$, а красным — кратные числа $2 - i$. Давайте спросим себя, какие целые гауссовы числа являются кратными и числа $2 + i$, и числа $2 - i$ одновременно. Ответ очевиден: пересечение множеств «синих» и «красных» чисел состоит из чисел, кратных 5. Другими словами, наименьшее общее кратное чисел $2 + i$ и $2 - i$ равно 5.

Произведение $(a + bi)(a - bi) = a^2 + b^2$ комплексного числа $z = a + bi$ и сопряженного с ним числа $\overline{z} = a - bi$ является числом вещественным. Поэтому для любого ненулевого целого гауссова числа z существует кратное ему натуральное число $z\overline{z} = a^2 + b^2$.

Теорема 6. *Если числа a и b взаимно просты, то наименьшим натуральным числом n, которое кратно числу $a + bi$, является именно число $a^2 + b^2$.*

Доказательство. Поскольку

$$\frac{n}{a+bi} = \frac{n(a-bi)}{(a+bi)(a-bi)} = \frac{na}{a^2+b^2} - \frac{nb}{a^2+b^2}\,i,$$

натуральное число n кратно числу $a + bi$ только в тех случаях, когда числа na и nb кратны $a^2 + b^2$. Поскольку числа a и b взаимно просты, это бывает только когда n кратно $a^2 + b^2$.

Упражнения

25. При каком условии на целые числа a и b частное $(a + bi)/(1 + i)$ является целым гауссовым числом?

26. Изобразите на плоскости числа, кратные числу а) $1 + 3i$; б) $1 - 3i$. в) Какие целые гауссовы числа являются кратными и числа $1 + 3i$, и числа $1 - 3i$ одновременно?

27. Докажите, что если целое вещественное число n кратно ненулевому целому гауссову числу $a + bi$, то n кратно числу $(a^2 + b^2)/\text{НОД}(a, b)$.

Делители единицы

Очевидно,

$$1 = 1 \cdot 1 = i \cdot (-i) = (-1) \cdot (-1) = (-i) \cdot i.$$

Других способов разложить 1 в произведение двух целых гауссовых чисел нет:

Теорема 7. *В $\boldsymbol{Z}[i]$ нет делителей единицы, кроме чисел 1, i, -1 и $-i$. (Другими словами, целое гауссово число $a + bi$ является делителем единицы в том и только том случае, когда $a^2 + b^2 = 1$.)*

Доказательство. Если $1 = uv$, где u, $v \in \boldsymbol{Z}[i]$, то $1 = |u| \cdot |v|$. Поскольку модуль ненулевого целого гауссова числа не меньше 1, имеем $|u| = |v| = 1$, откуда и следует утверждение теоремы.

Ассоциированные числа

Числа u и v называют *ассоциированными*, если они кратны друг другу, т.е. u кратно v и v кратно u. Всякое целое гауссово число z можно представить в виде произведения

$$z = 1 \cdot z = i(-iz) = (-1)(-z) = (-i)(iz),$$

первый множитель которого – делитель единицы, а второй – ассоциирован с числом z. Столь же очевидно, что если целое гауссово число w кратно числу z, то делителями числа w являются также и числа $-z$, iz, $-iz$. Поэтому, рассматривая разложения на множители, можно «не различать» ассоциированные числа.

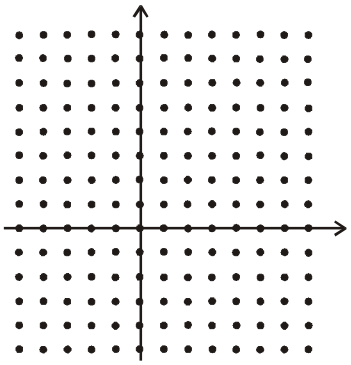

Рис. 3

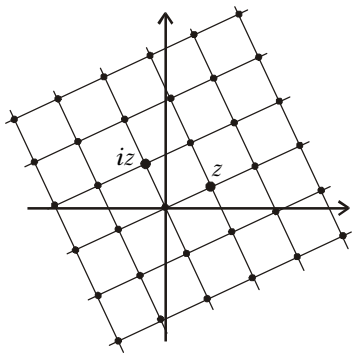

Рис. 4

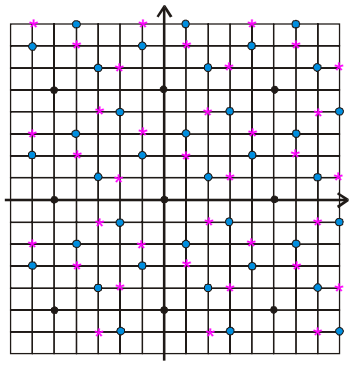

Рис. 5

Упражнения

28. Для комплексного числа $z = 2 + i$ отметьте на комплексной плоскости числа iz, $-z$, $-iz$.

29. Ассоциированные с числом z числа – это в точности числа вида εz, где ε – делитель единицы. Докажите это.

30. Докажите, что а) числа $1 + i$ и $1 - i$ ассоциированы; б) числа $a + bi$ и $a - bi$ ассоциированы в том и только том случае, когда выполнено хотя бы одно из условий: $a = 0$, $b = 0$, $a = b$, $a = -b$.

Доказательство теоремы Ферма–Эйлера

Доказательство леммы 2

Вернемся к лемме 2, от которой мы надолго отвлеклись, чтобы придать смысл разложению $m^2 + 1 = (m + i)(m - i)$. Числу p не кратен ни один из множителей $m + i$ и $m - i$, но кратно произведение $m^2 + 1$. Что это значит? Как может произведение быть кратно p, если ни один из множителей не кратен p? Неужели арифметика гауссовых чисел настолько своеобычна, что в ней нет никаких привычных нам законов? Например, мы привыкли к тому, что разложение натурального числа на простые множители единственно с точностью до порядка множителей. Вдруг основная теорема арифметики неверна для $\boldsymbol{Z}[i]$?

Оказывается, все не так плохо. Разложение на простые множители в $\boldsymbol{Z}[i]$ единственно в том же смысле, в каком оно единственно для обычных целых чисел (мы докажем это в разделе «Основная теорема арифметики»). А кажущееся противоречие устраняется тем, что простое число p может перестать быть простым при расширении $\boldsymbol{Z}$ до $\boldsymbol{Z}[i]$. Например, $2 = (1 + i)(1 - i)$ и $5 = (1 + 2i)(1 - 2i)$. Вообще, $p = (a + bi)(a - bi)$ для всякого числа $p = a^2 + b^2$.

Итак, разрешим себе пофантазировать: вообразим, что мы уже доказали теорему о единственности разложения целых гауссовых чисел на простые множители, и докажем лемму 2. Делитель p числа $(m + i)(m - i)$ не может быть простым гауссовым числом. Значит,

$$p = (a + bi)(c + di),$$

где целые гауссовы числа $(a + bi)$ и $(c + di)$ – не делители единицы. Поскольку модуль произведения равен произведению модулей, имеем

$$p = \sqrt{a^2 + b^2}\,\sqrt{c^2 + d^2},$$

т. е. $p^2 = \left(a^2 + b^2\right)\left(c^2 + d^2\right)$, откуда $p = a^2 + b^2 = c^2 + d^2$. Лемма 2, а заодно и теорема 4 доказаны.

Разложение простого числа на простые множители

Заголовок этого подраздела мог бы удивить, если бы выше мы не разлагали уже простые натуральные числа на простые гауссовы множители. Какие же простые натуральные числа останутся простыми во множестве целых гауссовых чисел, а какие станут составными? И как устроены разложения «новых составных» чисел?

Теорема 8. *Всякое простое натуральное число вида $p = 4n + 3$ является простым в $\boldsymbol{Z}[i]$; число 2 ассоциировано с квадратом простого гауссова числа $1+ i$; всякое простое натуральное число вида $p = 4n + 1$ разлагается на два сопряженных множителя: $p = (a + bi)(a - bi)$, причем множители $a + bi$ и $a - bi$ – простые гауссовы числа.*

Доказательство. Если число $p = 4n + 3$ представлено в виде произведения двух целых гауссовых чисел $p = (a + bi)(c + di)$, то

$$|p| = |a + bi| \cdot |c + di|,$$

откуда $p^2 = \left(a^2 + b^2\right)\left(c^2 + d^2\right)$. Значит, либо один из множителей $\left(a^2 + b^2\right)$ и $\left(c^2 + d^2\right)$ равен 1, а другой равен p^2, либо $p = a^2 + b^2 = c^2 + d^2$. В первом случае ясно, что число p было представлено в виде произведения делителя единицы и ассоциированного с p числа. Второй случай невозможен в силу теоремы 3.

С числом 2 дело обстоит еще проще: $2 = -i(1 + i)^2$. Впрочем, мы должны объяснить, почему число $1 + i$ простое.

Лемма 3. *Простое натуральное число p нельзя представить в виде произведения более чем двух целых гауссовых чисел, не являющихся делителями единицы. (Другими словами, если p ассоциировано с произведением двух не являющихся делителями единицы целых гауссовых чисел, то эти числа – простые.)*

Доказательство леммы 3. Если $p = (a + bi)(c + di)(e + fi)$, то

$$|p| = |a + bi| \cdot |c + di| \cdot |e + fi|,$$

откуда $p^2 = \left(a^2 + b^2\right)\left(c^2 + d^2\right)\left(e^2 + f^2\right)$. Квадрат простого числа никак не может быть произведением трех отличных от 1 натуральных чисел. Лемма 3 и теорема 8 доказаны.

Упражнения

31. Изобразите на комплексной плоскости все числа, на которые нацело делится число $5 - i$.

32. Сколько среди делителей числа а) $3 - 11i$; б) $6 + 12i$ таких, у которых и вещественная, и мнимая части положительны?

33. Разложите на простые гауссовы множители числа а) 16; б) 1001; в) $47 + i$.

Доказательство теоремы 2

Помните, мы обещали получить теорему 2 как одно из следствий теории целых гауссовых чисел? Настало время это сделать. Пусть простое число p не представимо в виде суммы двух квадратов и сумма квадратов $x^2 + y^2$ кратна p. Из теоремы 8 следует, что всякое простое натуральное число p либо является простым гауссовым числом, либо представимо в виде суммы квадратов двух целых чисел. Значит, в рассматриваемой ситуации p – простое гауссово число. Поскольку произведение $(x + iy)(x - iy) = x^2 + y^2$ кратно p, хотя бы один из сомножителей кратен p. Это в точности означает, что x и y кратны p. Теорема 2 доказана.

Количество представлений

Единственность представления простого числа в виде суммы двух квадратов

По теореме Ферма–Эйлера любое простое число p, которое при делении на 4 дает остаток 1, представимо в виде суммы двух квадратов. Давайте докажем, что такое представление единственно с точностью до порядка слагаемых.

Теорема 9. *Никакое простое число не может быть представлено в виде суммы квадратов двух целых чисел существенно разными (т. е. не получающимися один из другого перестановкой слагаемых) способами.*

Доказательство. Если бы простое число p имело два существенно разных представления, $p = a^2 + b^2 = c^2 + d^2$, то разложения $p = (a + bi)(a - bi) = (c + di)(c - di)$ противоречили бы теореме 8.

Упражнение 34 (М1288*). Докажите, что число $1000009 = 235^2 + 972^2$ составное.

Можно обойтись в доказательстве теоремы 9 и без комплексных чисел. Предположим, что простое число p двумя существенно разными (т. е. отличающимися не только порядком слагаемых) способами разложено в сумму квадратов натуральных чисел:

$$p = a^2 + b^2 = c^2 + d^2.$$

Тогда $a^2 \equiv -b^2$ и $c^2 \equiv -d^2 \pmod p$. Следовательно, $a^2c^2 \equiv \equiv \left(-b^2\right)\left(-d^2\right) \pmod p$, т. е. число $a^2c^2 - b^2d^2$ кратно p. (Если рассуждения со сравнениями по модулю p непривычны и потому подозрительны, вы можете получить то же самое, рассматривая тождество $a^2c^2 - b^2d^2 = a^2\left(c^2 + d^2\right) - \left(a^2 + b^2\right)d^2$.)

Поскольку число p простое, из делимости произведения $(ac + bd)(ac - bd)$ на p следует, что один из множителей кратен p. Если число $ac + bd$ кратно p, то воспользуемся формулой (1):

$$p^2 = (ac + bd)^2 + (ad - bc)^2.$$

Если $ad - bc \neq 0$, то противоречие очевидно, ибо первое слагаемое $(ac + bd)^2$ кратно p^2 и потому не меньше p^2. Если же $ad - bc = 0$, то $ad = bc$. Поскольку как числа a и b, так и числа c и d взаимно просты, имеем $a = c$ и $d = b$.

Случай, когда $ac - bd$ кратно p, можно рассмотреть аналогично, воспользовавшись формулой $p^2 = (ac - bd)^2 + (ad + bc)^2$.

Упражнение 35. Представьте число $1000009 = 235^2 + 972^2$ в виде произведения двух отличных от 1 натуральных чисел.

Итак, простое число нельзя двумя существенно разными способами представить в виде суммы квадратов двух натуральных чисел. Число, единственным образом представимое в виде суммы квадратов двух натуральных чисел, не всегда является простым: $10 = 1^2 + 3^2$, $25 = 3^2 + 4^2$. Легко сформулировать условия, при которых число имеет единственное представление в виде суммы двух квадратов. Но давайте не будем тратить на это свои силы, а ответим на более общий вопрос.

Сколькими способами число можно представить в виде суммы двух квадратов?

В III веке нашей эры греческий математик Диофант не только знал, что число 65 представимо двумя способами, но и объяснял это тем, что 65 является произведением чисел 13 и 5, каждое из которых – сумма двух квадратов. Комплексных чисел Диофант не знал, иначе он непременно выписал бы разложения $5 = (2 + i)(2 - i)$, $13 = (3 + 2i)(3 - 2i)$ и продолжил бы свои объяснения следующим образом:

$$65 = (2 + i)(3 + 2i) \cdot (2 - i)(3 - 2i) = (4 + 7i) \cdot (4 - 7i) =$$
$$= 4^2 + 7^2 = (2 + i)(3 - 2i) \cdot (2 - i)(3 + 2i) =$$
$$= (8 - i) \cdot (8 + i) = 8^2 + 1^2.$$

Понимаете? По-разному группируя множители, получили два разных разложения!

Следующий пример – число 25. Тот, кто решил упражнение 1, знает, что 25 – наименьшее число, двумя способами представимое в виде суммы квадратов двух целых чисел. Оба эти разложения легко получить, по-разному группируя множители:

$$25 = (2 + i)^2 \cdot (2 - i)^2 = (3 + 4i) \cdot (3 - 4i) = 3^2 + 4^2 =$$
$$= (2 + i)(2 - i) \cdot (2 + i)(2 - i) = 5 \cdot 5 = 5^2 + 0^2.$$

Последний пример – число 5746. Как мы хорошо знаем, всякому представлению $5746 = a^2 + b^2$ соответствует разложение $5746 = (a + bi)(a - bi)$ на сопряженные множители. Поэтому разложим рассматриваемое число сначала на простые натуральные, а затем и на простые гауссовы множители:

$$5746 = 2 \cdot 13^2 \cdot 17 =$$
$$= (1 + i)(1 - i)(3 + 2i)^2 (3 - 2i)^2 (4 + i)(4 - i).$$

Теперь мы должны из нескольких этих множителей составить $a + bi$, да так, чтобы произведение остальных множителей равнялось $a - bi$. Это нетрудно сделать:

$$a + bi = (1 + i)(3 + 2i)^2 (4 + i) = -45 + 61i,$$
$$a - bi = (1 - i)(3 - 2i)^2 (4 - i) = -45 - 61i.$$

При этом, разумеется, $45^2 + 61^2 = 2025 + 3721 = 5746$. Легко найти и еще два варианта:

$$a + bi = (1 + i)(3 + 2i)(3 - 2i)(4 + i) = 39 + 65i$$

или

$$a + bi = (1 + i)(3 - 2i)^2 (4 + i) = 75 - 11i.$$

Они приводят к представлениям $39^2 + 65^2 = 1521 + 4225 = 5746$ и $75^2 + 11^2 = 5625 + 121 = 5746$. Никаких других представлений нет (попытайтесь их придумать – и довольно скоро поймете причину этого).

Аналогично можно найти число представлений в виде суммы двух квадратов любого натурального числа $n = 2^a p_1^{a_1} \ldots p_r^{a_r} Q$, где $p_1, \ldots, p_r$ – попарно различные простые числа, каждое из которых дает остаток 1 при делении на 4, Q – число, не имеющее простых делителей кроме тех, которые дают остаток 3 при делении на 4. А именно, если Q не является точным квадратом, то n не представимо в виде суммы двух квадратов; если же Q – точный квадрат, то, применив необходимое число раз теорему 2, получаем: количество представлений числа n в виде суммы двух квадратов равно количеству представлений числа $m = 2^a p_1^{a_1} \ldots p_r^{a_r}$ в виде суммы двух квадратов. Формулу для этого количества нашел немец Петер Густав Лежен Дирихле (1805–1859).

Теорема 10. *Количество представлений числа m в виде суммы квадратов двух целых чисел равно $[(a_1 + 1) \cdot \ldots \ldots \cdot (a_r + 1) + 1)/2]$. (Если число сомножителей равно 0, то произведение считается равным 1. Представления, отличающиеся порядком слагаемых, не различаются.)*

Надеемся, доказательство не представит непреодолимой трудности. Если трудности возникли – не огорчайтесь, а перечитайте статью заново (и так много раз – до тех пор, пока не поймете, почему формула Дирихле верна).

Упражнения

36. При каком наименьшем радиусе окружности с центром в начале координат на ней лежат ровно а) 4 целочисленные точки; б) 8 точек; в) 12; г) 16?

37. а) Сколько решений в натуральных числах $x < y$ имеет уравнение $x^2 + y^2 = 5^n$, где n – данное натуральное число? б) Докажите, что для всякого натурального n существует бесконечно много окружностей с центрами в начале координат, на каждой из которых лежат ровно $4n$ точек с целыми координатами.

38. Рассмотрим окружность с центром в начале координат радиуса $\sqrt{2^a p_1^{a_1} \dots p_r^{a_r}}$, где $p_1, \dots, p_r$ – попарно различные простые числа, каждое из которых дает остаток 1 при делении на 4. Сколько на этой окружности точек с целыми координатами?

39*. Может ли так быть, что натуральное число n не представимо в виде суммы двух квадратов а) целых; б) натуральных; в) взаимно простых чисел, а число n^{1999} представимо в таком виде?

40*. Какие числа единственным с точностью до перестановки слагаемых образом представимы в виде суммы квадратов двух а) целых неотрицательных; б) натуральных; в) взаимно простых чисел?

41. Если число $n > 2$ представимо в виде суммы квадратов двух взаимно простых чисел, то число таких представлений равно 2^{s-1}, где s – количество простых делителей n, имеющих вид $4k + 1$. Докажите это.

42*. Количество точек с целыми координатами на окружности радиуса $\sqrt{n}$ с центром в начале координат (т. е. количество решений в целых числах уравнения $x^2 + y^2 = n$) равно учетверенной разности между количеством натуральных делителей числа n, которые имеют вид $4k + 1$, и количеством натуральных делителей вида $4k + 3$. Докажите это.

Приложение

Основная теорема арифметики

Прежде чем доказывать единственность разложения целого гауссова числа на простые множители, напомним, что для «обычных» натуральных чисел единственность разложения на простые натуральные множители вовсе не очевидна. Наиболее известны два доказательства. Одно из них изложено в «Началах» Евклида (III век до н. э.), а другое придумал немец Эрнст Цермело (1871–1953). Мы рассмотрим доказательство Цермело (сразу для целых гауссовых чисел).

Теорема 11. *Разложение на простые множители в* $\boldsymbol{Z[i]}$ *единственно (с точностью до перестановки множителей и ассоциированности).*

Доказательство. Тот факт, что любое ненулевое целое гауссово число можно представить в виде произведения простых гауссовых чисел, очевиден: разлагаем, пока можно, а когда перестанет разлагаться, то все уже разложилось! (Любитель абсолютной строгости то же самое оформит следующим образом. Предположим, что не все целые гауссовы числа имеют разложения на простые гауссовы множители. Рассмотрим такое число z с *наименьшим* модулем. Если z – делитель единицы или простое число, то оно в разложении не нуждалось. А если z представимо в виде произведения $z = uv$ целых гауссовых чисел, где $|u| < |z|$ и $|v| < |z|$, то числа u и v имеют разложения на простые множители. Объединив их, мы как раз получаем разложение числа z.)

Намного труднее и интереснее доказательство единственности разложения. Предположим, что некоторое целое гауссово число z двумя существенно разными способами представлено в виде произведения простых гауссовых чисел:

$$z = p_1 p_2 \dots p_r = q_1 q_2 \dots q_s. \qquad (2)$$

Можно считать, что z – *наименьшее* по абсолютной величине из чисел, обладающих разными разложениями на простые гауссовы множители. Тогда ни одно из чисел $p_1, \dots, p_r$ не ассоциировано ни с одним из чисел $q_1, q_2, \dots, q_s$ (в противном случае мы сократили бы обе части равенства (2) на общий множитель, получив меньшее по модулю число).

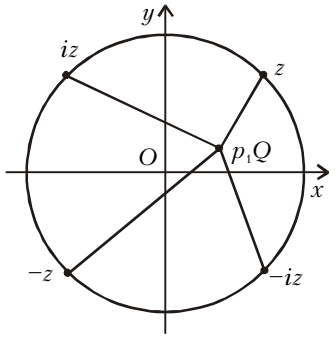

Рис. 6

Обозначим $P = p_2 \dots p_r$ и $Q = q_2 \dots q_s$. Тогда $z = p_1 P = q_1 Q$. Не ограничивая общности, можно считать, что $|p_1| \le |q_1|$. При этом $|P| \ge |Q|$ и, значит, $|p_1 Q| \le |z|$. Рассмотрим число $w = \varepsilon z - p_1 Q$, где ε – такой делитель единицы, что $|w| < |z|$. (Почему такой делитель единицы ε можно выбрать, ясно из рисунка 6. В самом деле, числа z, iz, $-z$ и $-iz$ – вершины квадрата. Точка $p_1 Q$ расположена внутри описанного круга этого квадрата. Весь описанный круг можно покрыть четырьмя кругами с центрами в вершинах квадрата, радиусы которых равны половине диагонали квадрата. Значит, хотя бы одна из вершин квадрата расположена к точке $p_1 Q$ ближе, чем на расстояние $|z|$.) Число w может быть разложено на множители двумя способами:

$$w = \varepsilon z - p_1 Q = p_1(\varepsilon P - Q) = (\varepsilon q_1 - p_1) q_2 \dots q_s.$$

Поскольку $|w| < |z|$, для числа w должна иметь место единственность разложения на простые гауссовы множители. Значит, хотя бы один из множителей $\varepsilon q_1 - p_1, q_2, \dots, q_s$ должен быть кратен простому числу p_1. Если число $\varepsilon q_1 - p_1$ кратно p_1, то q_1 кратно p_1, откуда следует, поскольку q_1 – простое гауссово число, что числа p_1 и q_1 ассоциированы, что невозможно. Еще очевиднее противоречие в случае, когда кратен числу p_1 один из множителей $q_2, \dots, q_s$.

Доказательство Лагранжа леммы 2

Могло сложиться впечатление, что обойтись в доказательстве леммы 2 без комплексных чисел невозможно. Тем не менее, Лагранж придумал следующее удивительно короткое рассуждение.

Рассмотрим все такие пары $(r; s)$ целых чисел, что $0 \le r, s < \sqrt{p}$, и для каждой пары рассмотрим остаток от деления числа $r + ms$ на p. Поскольку количество таких пар равно $\left(\left[\sqrt{p}\right] + 1\right)^2 > p$, среди них обязаны найтись такие две пары $(r_1; s_1)$ и $(r_2; s_2)$, что остатки от деления на p чисел $r_1 + ms_1$ и $r_2 + ms_2$ равны. При этом число $r + ms$, где $r = r_1 - r_2$ и $s = s_1 - s_2$, кратно p. Поэтому число

$$r^2 + s^2 = r^2 - m^2 s^2 + (m^2 + 1)s^2 = (r + ms)(r - ms) + (m^2 + 1)s^2$$

тоже кратно p. Заметим, что $0 < r^2 + s^2 < p + p = 2p$. Единственным кратным p числом, которое больше 0, но меньше $2p$, является само число p. Значит, $r^2 + s^2 = p$, что и требовалось.

Замечание. В статье В.Тихомирова «Теорема Ферма – Эйлера о двух квадратах» («Квант» №10 за 1991 год), помимо доказательства Лагранжа, приведены еще два доказательства теоремы Ферма – Эйлера.