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).

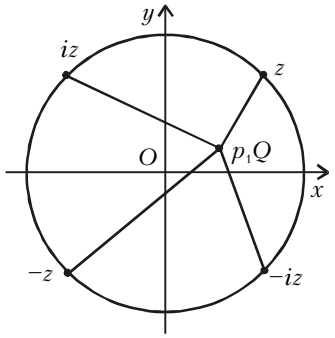

Рис. 6

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.