Алгоритм Евклида для гауссовых чисел. А.Я. Канель (10–11)

Всем хорошо знаком алгоритм Евклида. Даны два числа a, b. Из них выбирается большее, из большего вычитается меньшее и большее заменяется на разность, с новой парой чисел производится та же процедура. С помощью алгоритма Евклида доказываются арифметические свойства чисел и это Вы изучали раньше. Приведем принципиально новые (для большинства школьников) его применения.

В этом пункте используется понятие комплексных чисел.

1. Решите уравнения в целых числах.
(a) $x^2 + 4 = y^3$. (b) $x^2 + 2 = y^n$. (c)* $x^3 + y^3 = z^3$.

Попробуйте порешать их, не читая дальнейшего! Впрочем, у Вас вряд ли получится. Возвращайтесь к этой задаче по мере чтения дальнейшего материала.

При решении уравнения $x^2+4 = y^3$ в целых числах хочется действовать так: $x^2 + 4 = (x + 2i)(x - 2i)$, а дальше при нечетном x оба эти множители взаимно просты, и потому оба кубы. Из этого вытягивается решение. (Случай четного x хитрее: обе скобки могут делиться на $(1 + i)^3$.) Попробуйте довести решение, а затем сравнить с приведенным в конце темы.

Одним словом, хочется наслаждаться дополнительными возможностями при разложении на множители за счет использования *гауссовых чисел*, т.е. чисел вида $a + bi$ с целыми a и b. Однако не все коту масленица — так получается не всегда, но иногда все же получается. Чтобы применять разложение на множители для решения уравнений, нужна *однозначность разложения на простые множители.* Если она имеет место, то мы имеем все те же арифметические удовольствия, что и для целых чисел. Следующая задача показывает удивительный факт: для *арифметических* удовольствий достаточно доказать *геометрический* факт о возможности деления с остатком.

2. Будем называть *простыми* гауссовы числа, не разложимые на (отличные от ± 1 и $\pm i$) множители.

(a) Однозначность разложения на простые множители вытекает из следующего свойства ('аналога основной леммы арифметики').

Факториальность. *Если простое число p делит ab, то p делит a или p делит b.*

(b) Факториальность вытекает из следующего свойства.

Главноидеальность. *Пусть d есть наибольший общий делитель чисел a, b (дайте его определение самостоятельно!). Тогда $ma + nb = d$ для некоторых чисел m, n.*

(c) Главноидеальность обеспечивается возможностью делить с остатком (причем остаток должен быть меньше делителя). Т.е. она вытекает из следующего свойства.

Евклидовость. *Для любых чисел a, b существует такое число k, что* $|a - kb| < |b|$.

Про обычные числа и многочлены вы все знаете. *Докажем евклидовость множества целых гауссовых чисел.* Покажем, как разделить a на

[0]Материал Системы дистанционного обучения математике http://math.olymp.mioo.ru

b. Множество чисел $(p + qi)b$, кратных b, образуют квадратную решетку со стороной $|b|$. Число a попадает в один из образовавшихся квадратиков. Остается воспользоваться геометрическим фактом: *расстояние от точки внутри квадрата до ближайшей вершины строго меньше длины стороны квадрата.*

3. Верна ли евклидовость (и, значит, факториальность!) в множестве чисел вида $a + b\xi$, где ξ есть

(a) $\sqrt{-2}$? (b) $\sqrt{-3}$? (c) $(1 - \sqrt{-3})/2$? (d) $(1 - \sqrt{-5})/2$? (e) $(1 - \sqrt{-7})/2$?

4. Эту задачу проще решать без гауссовых чисел, однако потренируйтесь их применить!

(a) Докажите что простое число вида $4k-1$ не разлагается в сумму двух квадратов, а простое вида $4k + 1$ разлагается одним способом.

(b) Докажите, что существует число, ровно 1024 способами разлагающееся в сумму двух квадратов.

Дополнение.

Следующие две задачи посвящены алгоритму Евклида для вещественных чисел, т.е. цепным дробям.

5. От прямоугольника отрезают квадрат, и с оставшимся прямоугольником производят ту же процедуру. Может ли последовательность отношений сторон у этих прямоугольников быть периодической, если одна из сторон исходного прямоугольника равна 1, а другая равна

(a) $\sqrt{2}$. (b) $(1 + \sqrt{5})/2$. (c) $\sqrt[3]{2}$. (d)* $\sqrt{2005}$.

6.* Пусть α – иррациональное число. Применим к паре $(\alpha, 1)$ алгоритм Евклида. Докажите что получившиеся числа будут величинами наилучших приближений (по недостатку или по избытку) αn к целым.

Число αn называется *наилучшим приближением* если при всех $1 \le m < n$ расстояние от αn до ближайшего целого меньше расстояния αm до ближайшего целого. Аналогично определяются наилучшие приближения *по недостатку* и *по избытку.*

Решения и указания.

Зачетные задачи: 1b, 2abc, 3abcd, 4ab.

1. (a) (Р. Девятов) Ответ. $x = \pm 2$, $y = 2$ и $x = \pm 11$, $y = 5$.

Перейдем к целым гауссовым и получим уравнение: $(x+2i)(x-2i) = y^3$.

Целое гауссово число называется *точным кубом*, если оно равно b^3 для некоторого целого гауссова b. Заметим, что "обратимые" числа $\pm 1, \pm i$ все являются точными кубами. Поэтому точным кубом является любое целое гауссово число, представимое в виде ωa^3, где a — целое гауссово число и ω — одно из "обратимых" чисел $\pm 1, \pm i$. Поэтому мы будем называть точными кубами числа такого вида.

Два целых гауссовых числа a и b называются *ассоциированными*, если $a = \omega b$, где ω — одно из "обратимых" чисел $\pm 1, \pm i$.

Лемма. *Оба числа $x + 2i$ и $x - 2i$ являются точными кубами.*

Доказательство. Будем использовать единственность разложения на простые гауссовы множители с точностью до умножения на "обратимые" числа $\pm 1, \pm i$. Пусть $d = GCD(x+2i, x-2i)$. Тогда $x+2i-(x-2i) = 4i = -i(1+i)^4$ делится на d. Т. к. $1+i$ простое, то d — степень числа $1+i$, причем не более, чем четвертая.

Заметим, что разложение на простые целые гауссовы для числа $x-2i$ отличается от разложения $x+2i$ заменой всех простых множителей на сопряженные.

Т. к. $1+i = i(1-i)$, то степени, в которых $1+i$ входит в разложение чисел $x+2i$ и $x-2i$ на множители, одинаковы. Обозначим их через k. Тогда y^3 делится на $1+i$ во вдвое большей степени $2k$. Т. к. $2k$ делится на 3, то и k делится на 3. Т. к. d — степень $(1+i)$, причем не более чем четвертая, то $x+2i$ либо не делится на $1+i$, либо делится на $(1+i)^3$.

Если $x+2i$ не делится на $1+i$, то $x+2i$ и $x-2i$ взаимно просты. Т. к. их произведение $(x+2i)(x-2i)$ является точным кубом, то сами числа $x+2i$ и $x-2i$ в этом случае являются точными кубами.

Если $x+2i = a(1+i)^3$ для некоторого целого гауссова a, то и $x-2i = b(1+i)^3$ для некоторого целого гаусоова b. Тогда $y^3 = ab(1+i)^6$, т. е. y^3 делится на $(1+i)^6$. Значит, y делится на $(1+i)^2$. Поэтому $ab = (\frac{y}{(1+i)^2})^3$, т. е. ab является точным кубом. Но a и b взаимно просты, поэтому сами являются точными кубами. А значит и $x+2i = a(1+i)^3$ и $x-2i = b(1+i)^3$ являются точными кубами. $\square$

Продолжение решения. Пусть

$$x+2i = (c+di)^3 = c^3 + 3c^2di + 3cd^2i^2 + d^3i^3 = c^3 - 3cd^2 + (3c^2d - d^3)i.$$

Приравняем мнимые части: $2 = 3c^2d - d^3$ и $2 = d(3c^2 - d^2)$. Это равенство обычных целых чисел, поэтому можно разобрать только 2 случая: $d = \pm 2$ и $d = \pm 1$.

Случай 1. $d = \pm 1$. Тогда $3c^2 - 1 = \pm 2$, т. е. $3c^2 = -1$ или 3. Но -1 оно равняться не может, значит $c = \pm 1$, $c + di = 1 + i$ или ассоциировано с ним, $x + 2i = 2 + 2i$ или ассоциировано с ним, откуда $x = \pm 2$, $y = 2$.

Случай 2. $d = \pm 2$. Тогда $3c^2 - 2 = \pm 1$, т. е. $3c^2 = 1$ или 3. Но 1 оно равняться не может, значит $c = \pm 1$, $c + di = 2 + i$ или ассоциировано с ним, $x + 2i = 11 + 2i$ или ассоциировано с ним, откуда $x = \pm 11$, $y = 5$.

1 (b). Используйте 3a.

1 (c). Используйте 3c.

1–3. См. книгу М. М. Постникова, 'Теорема Ферма: введение в теорию алгебраических чисел', §4.

5, 6. См. книгу В. И. Арнольда "Цепные дроби".