Гауссовы числа 4.04, пара 1

Наша цель — решить следующую задачу:
Простое число вида $4k+1$ представляется в виде суммы 2 квадратов.

Для ее решения мы будем пользоваться целыми гауссовыми числами (обозначение: $\mathbb{Z}[i]$), т. е. комплексными числами, у которых действительная и мнимая части обе целые. С этими числами можно обращаться как с обычными целыми числами. В частности, для них верен аналог теоремы о разложении на простые множители.

Целое гауссово число a называется *обратимым*, если единицу можно представить в виде $ab = 1$ для некоторого целого гауссова b (иными словами, все числа из $\mathbb{Z}[i]$ делятся на a.

Упр 1. Какие целые гауссовы числа обратимы?

Число a называется *простым*, если оно не обратимо, а для любого разложения на множители $a = bc$ либо b, либо c обратимо.

В решении задачи нам поможет следующий факт, доказательство которого является нашей ближайшей целью:

а) любое число раскладывается в произведение простых.

б) это разложение единственно с точностью до перестановки сомножителей и до домножения каждого из них на обратимый.

Доказательство является некоторым обобщением обычной теоремы о существовании и единственности разложения на простые. Как и прежде, мы будем пользоваться возможностью деления с остатком. Для этого сначала нужно научиться как-то сравнивать целые гауссовы числа. Введем на них норму $n\colon \mathbb{Z}[i] \to \mathbb{N} \cup \{0\}$, которая определяется так: $n(a+bi) = a^2 + b^2$.

1. (Геометрическая интерпретация)

а) Пусть дан квадрат $ABCD$ и точка K внутри него. Доказать, что хотя бы одно из расстояний AK, BK, CK, DK строго меньше стороны квадрата.

б) Доказать, что в $\mathbb{Z}[i]$ возможно деление с остатком: для любых двух целых гауссовых a и b ($b \neq 0$) существуют такие q и r, что $a = bq + r$ и $n(r) < n(b)$.

2*. Повторить рассуждение задачи 1 алгебраическими методами (можно пользоваться без доказательства известными нам фактами из обычной теории чисел, например возможностью деления с остатком, принципом Архимеда, ...)

Далее, в задачах 5–9 под словом "число" следует понимать именно целое гауссово число.

Наибольшим общим делителем чисел $a \neq 0$ и $b \neq 0$ называется их общий делитель с наибольшей нормой.

5. Доказать, что НОД существует и единственен с точностью до домножения на обратимые.
Указание: повторить для нашего случая алгоритм Евклида.

6. Доказать "лемму о линейном разложении НОД": пусть d — НОД $a \neq 0$ и $b \neq 0$. Тогда существуют такие u и v, что $d = au + bv$.

Число a называется *простым*, если оно не обратимо, а для любого разложения на множители $a = bc$ либо b, либо c обратимо.

7. Доказать "лемму о сокращении": пусть ab делится на c (т. е. существует такое k, что $ab = kc$), и a и c *взаимно просты* (т. е. не имеют общих делителей, отличных от обратимых). Тогда b делится на c.

8. Доказать, что любые 2 простых либо взаимно просты, либо отличаются на обратимый множитель.

9. Докажите теорему о разложении на простые для $\mathbb{Z}[i]$.

Теперь применим наши познания к практике. Для начала разберемся, какими вообще могут быть простые целые гауссовы числа.

10. Доказать, что норма простого гауссова числа есть степень (натурального) простого числа. Чему может быть равен показатель этой степени?

11. Теория чисел учит, что если $p = 4k+1$ — натуральное простое число, то существуют такие натуральные a и b, что $a^2 + b^2$ делится на p, а если p — простое натуральное число вида $4k+3$, то таких a и b не существует. Этот факт предполагается известным, но при желании можно его доказать. (Это доказывается существенно другими методами, чем рассмотренные выше.) Используя этот факт, решить задачу, сформулированную в начале.

12. Опишите все простые гауссовы числа (в терминах натуральных простых чисел).

13. (Совсем "практическая" задача) Найти все натуральные числа a и b, такие что $a^2 + 4 = b^3$.

Целые гауссовы числа позволяют решать многие задачи, сформулированные в терминах натуральных чисел, но иногда их недостаточно. Например, условие задачи 14 (см. ниже) очень похоже на условие задачи 13, но решить ее полностью аналогично, пользуясь целыми гауссовыми числами, не получается. Но помогает более сильное обобщение понятия натурального число — общее алгебраическое понятие кольца.

Немного общей теории:

Множество A называется *ассоциативным коммутативным кольцом с единицей без делителей нуля* (далее — просто кольцом), если в нем есть 2 операции, сложение и умноженние, при этом выполнено следующее:
$(a+b)+c=a+(b+c)$
$0+a=a+0=0$
Для любого элемента существует обратный по сложению $a+(-a)=0$
$a+b=b+a$
$a(b+c)=ab+ac$
$ac+bc=(a+b)c$
$(ab)c=a(bc)$
$1\cdot a=a$
$ab=ba$
если $ab=0$, то $a=0$ или $b=0$
$1\neq 0$

Упр 2. 0 единственен, 1 единственна, $0a=0$.

Упр 3. Если $ac=bc$, то $a=b$.

Элемент a кольца называется *обратимым*, если найдется такое b, что $ab=1$. При этом b называют обратным к a.

Упр 4. Произведение обратимых элементов обратимо, обратный к обратимому элементу также обратим.

3*. *Нормой* элемента кольца называют такую функцию $n\colon A\to\mathbb{N}\cup\{0\}$, что $n(ab)=n(a)n(b)$. Кольцо с данной нормой называют *евклидовым*, если там есть "деление с остатком": для любых 2 элементов a и b ($b\neq 0$) существуют такие q и r, что $a=bq+r$ и $n(r)<n(b)$. Доказать, что:

а) $n(a)=0\Leftrightarrow a=0$

б) $n(a)=1\Leftrightarrow a$ обратим

4*. (задача в сторону)

Можно предъявлять более слабые требования к норме, а именно: если $a\neq 0$, то $n(ab)\geq n(b)$. Определение евклидовости можно оставить без изменений. Тогда

а) $a=0\Leftrightarrow n(a)$ — минимальный элемент множества значений n.

б) a обратим $\Leftrightarrow n(a)$ — минимальный элемент множества значений n на $A\setminus\{0\}$.

в) Если для некоторого b выполнено $n(ab)=n(b)$, то a обратим. Обратно, если a обратим, то $n(ab)=(b)$ для любого b.

Упр 5. Проверьте, что все утверждения задач 5–9 выполнены для произвольного евклидова кольца (только слово "число" следует теперь понимать как "элемент кольца").

Теперь мы можем сказать, что целые гауссовы числа с нормой, определенной выше, являются евклидовым кольцом. Далее все кольца в задачах подразумеваются евклидовыми.

Как мы уже говорили, решить задачу 14 полностью аналогично задаче 13, пользуясь только целыми гауссовыми числами, не получается. Поэтому полезно рассмотреть другое кольцо, а именно числа вида $a+\sqrt{2}bi$ с нормой a^2+2b^2. Доказательство возможности деления с остатком полностью аналогично.

14. Найти все натуральные числа a и b, такие что $a^2+2=b^3$.

15*. Будет ли евклидовым кольцом множестов чисел вида $a+b\sqrt{2}$, где a и b — целые, с нормой $n(a+b\sqrt{2})=|a^2-2b^2|$?

Не все кольца, в которых выполнена теорема о существовании и единственности разложения на простые, являются евклидовыми. Например, многочлены от одной переменной с коэффициентами в $\mathbb{Q}$, $\mathbb{R}$ или $\mathbb{C}$ образуют евклидово кольцо (т. е. мы доказали для них теорему о разложении на неприводимые множители), а с коэффициентами в $\mathbb{Z}$ — нет. Тем не менее, для них единственность разложения имеет место, что объясняет возникновение следующей задачи. Дело в том, что иногда бывает удобно пользоваться не самим разложением на простые множители, а утверженими задач 7 и 8.

16*. Пусть про кольцо известно только то, что было сказано в начале, евклидовости нет. Но пусть выполнена теорема о существовании и единственности разложения на простые множители. Докажите в этих предположениях:

а) задачу 7

б) задачу 8

17. Докажите, что в кольце чисел вида $a + \sqrt{3}bi$ теорема о существовании и единственности разложения на простые не верна.