НА ПОДСТУПАХ К РОЖДЕСТВЕНСКОЙ ТЕОРЕМЕ ФЕРМА (РТФ)

ТЕОРЕМА ВИЛЬСОНА

Приступаем к реализации нашего плана, заявленного на прошлом уроке. Первой ступенью в доказательстве утверждения шага №1

$p = 4k + 1$ — простое число $\Rightarrow \ \exists\, c \in \mathbb{N}$ такое, что $c^2 + 1 \vdots p$ является следующая теорема:

ТЕОРЕМА ВИЛЬСОНА

Для любого простого числа p
$(p - 1)! + 1 \vdots p$.

Доказательство $(p - 1)! = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p - 1)$.

Для любого остатка а по модулю p существует остаток b по модулю p такой, что $ab \equiv 1(\mathrm{mod}\ p)$.

Например, для остатка 2 это остаток $\dfrac{p+1}{2}$.

При их перемножении получаем $p + 1$.

Если есть такой остаток , что $a \cdot a \equiv 1(\mathrm{mod}\ p)$,
тогда $a^2 - 1 = (a - 1)(a + 1) \vdots p$,
следовательно, либо $a \equiv 1(\mathrm{mod}\ p)$, либо $a \equiv -1(\mathrm{mod}\ p)$,
то есть $a = 1$ или $p - 1$.

Таким образом, все остатки от 2 до $p - 2$ разбиваются на пары, останется только 1 и $p - 1$. А значит,

$(p - 1)! \equiv (p - 1)(\mathrm{mod}\ p) \equiv -1(\mathrm{mod}\ p) \Rightarrow$
$(p - 1)! + 1 \vdots p$.

Доказано.

2-Я СТУПЕНЬ ДОКАЗАТЕЛЬСТВА $c^2 + 1 \vdots p$

Итак, $(p - 1)! + 1 \vdots p$.

Если $p = 4k + 1$,
то $(4k)! + 1 \vdots p$.

Распишем:

$(4k)! = 1 \cdot 2 \cdot \ldots \cdot 2k(2k + 1)(2k + 2) \ldots 4k$.

Заметим, что т. к. $p = 4k + 1$,
$2k + 1 \equiv -2k(\mathrm{mod}\ p)$,
$2k + 2 \equiv -2k + 1(\mathrm{mod}\ p) = -(2k - 1)(\mathrm{mod}\ p)$ и т. д.

Таким образом, вторая половина произведения равна первой, домноженной на $(-1)^{2k} = 1$.

Отсюда $(p - 1)! + 1 \equiv (2k)!^2 + 1(\mathrm{mod}\ p) \Rightarrow$
при $c = (2k)! \quad c^2 + 1 \vdots p$.

Доказано.

СТРОИМ ТЕОРИЮ ДЕЛИМОСТИ В ГАУССОВЫХ ЧИСЛАХ

Во множестве целых чисел $\mathbb{Z}$ определено понятие деления с остатком. На основе этого понятия выводилось, что $\forall a, b \in \mathbb{Z}$ множество общих делителей a и b совпадает с множеством делителей некоторого числа, которое является $\text{НОД}(a, b)$ и представляется в виде $\text{НОД}(a, b) = am + bn$.

Далее, мы выводили, что если $\text{НОД}(a, c) = 1$ и при этом $ab \vdots c$, то тогда $b \vdots c$.

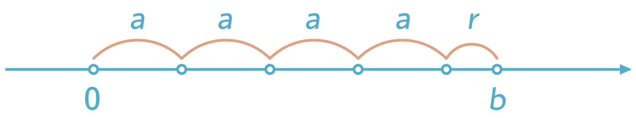
Далее мы выводили, что если p — простое, то из того, что a и b не делятся на р следует, что ab тоже не делится на p.

Наша цель: повторить эту цепочку в гауссовых числах. Мы разберемся, как выглядит деление с остатком в $\mathbb{Z}[i]$, и выясним, что НОД в $\mathbb{Z}[i]$ определяется с точностью до ассоциированности (домножения на обратимый).

В результате мы докажем рождественскую теорему Ферма. А потом займемся основной теоремой арифметики в $\mathbb{Z}[i]$ и ее основными следствиями.

ДЕЛЕНИЕ С ОСТАТКОМ В ГАУССОВЫХ ЧИСЛАХ

В $\mathbb{Z}$:



Чтобы разделить с остатком b на a, откладываем на отрезке длины b отрезок длины a столько раз, что оставшийся отрезок будет иметь длину $r < a$.

В гауссовых числах мы не можем ввести отношение «<>» между числами. Нужно другое понимание.

Например, поделим $7 + i$ на $3 + 2i$.
Можно убедиться, что нацело поделить не удастся:

$$\frac{7+i}{3+2i} = \frac{(7+i)(3-2i)}{(3+2i)(3-2i)} = \frac{23-11i}{13}$$

Или предположить, что существует делитель $7 + i = (3 + 2i)(a + bi)$ и получить, что $a + bi$ не является гауссовым.

АЛГЕБРАИЧЕСКИЙ МЕТОД ДЕЛЕНИЯ С ОСТАТКОМ:

Будем искать неполное частное такое, что его вещественная и мнимая часть будут ближайшими целыми к результату (не дальше, чем на $\frac{1}{2}$). Тогда остаток будет иметь модуль меньше 1:

$$\frac{7+i}{3+2i} = \frac{23}{13} - \frac{11}{13}i = 2 - \frac{3}{13} - i + \frac{2i}{13} =$$

$$= 2 - i + \left(-\frac{3}{13} + \frac{2i}{13}\right)$$

Таким образом,

$$\frac{\overset{\in\mathbb{Z}[i]}{z}}{\underset{\in\mathbb{Z}[i]}{w}} = \overset{\in\mathbb{Z}[i]}{s} + (x+yi),\ \text{где } x + yi \text{ такое, что } x, y \leq \frac{1}{2}.$$

Тогда $\mathrm{N}(x+yi) = \sqrt{x^2 + y^2} \leq \sqrt{\frac{1}{4} + \frac{1}{4}} < 1$

Отсюда $z = sw + w(x + yi)$, где число $w(x + yi)$ обязано быть гауссовым, причем его модуль $< |w|$.

Итак, деление с остатком в гауссовых числах возможно.