Делимость комплексных чисел

! Кольцо $\mathbb{Z}[\mathfrak{i}] = \{a + b\mathfrak{i}, a, b \in \mathbb{Z}\}$ называется *кольцом гауссовых чисел.* Те его элементы, которые нельзя представить в виде произведения двух необратимых, называются *простыми.*

! Число $z \in \mathbb{Z}[\mathfrak{i}]$ *делится* на число $w \in \mathbb{Z}[\mathfrak{i}]$, если существует $t \in \mathbb{Z}[\mathfrak{i}]$ такое, что $z = wt$. Запись стандартная: $z \vdots w$ (либо $w|z$).

1. Опишите все пары чисел z, w такие, что одновременно $z|w$ и $w|z$.

2. Докажите, что если $|z|^2 \in \mathbb{P}$, то z – простой элемент $\mathbb{Z}[\mathfrak{i}]$.

? Какие из чисел $1+\mathfrak{i}$, 2, $2 \pm \mathfrak{i}$, 3, $3 \pm \mathfrak{i}$, $3 \pm 2\mathfrak{i}$, $4 \pm \mathfrak{i}$, $4 \pm 3\mathfrak{i}$, 5, $5 \pm \mathfrak{i}$, $5 \pm 2\mathfrak{i}$, $6 \pm \mathfrak{i}$, $5 \pm 4\mathfrak{i}$, 7 являются простыми в $\mathbb{Z}[\mathfrak{i}]$?

3. **Деление с остатком.**

   Докажите, что для любых $n, m \in \mathbb{Z}[\mathfrak{i}]$ $(m \neq 0)$ найдутся $q, r \in \mathbb{Z}[\mathfrak{i}]$ такие, что

$$n = mq + r \quad \text{и} \quad |r| < |m|.$$

4. Найдите $(4 + 19\mathfrak{i}, -6 + 17\mathfrak{i})$ в $\mathbb{Z}[\mathfrak{i}]$. Представьте числа $4 + 19\mathfrak{i}$ и $-6 + 17\mathfrak{i}$ в виде произведения простых. Единственно ли это представление?

5. **Линейное представление НОДа.**

   Докажите, что для любых $n, m \in \mathbb{Z}[\mathfrak{i}]$ найдутся $s, t \in \mathbb{Z}[\mathfrak{i}]$ такие, что

$$sn + tm = (n, m)\ .$$

6. **Единственность разложения.**

   Докажите, что любой $w \in \mathbb{Z}[\mathfrak{i}]$ единственным образом (с точностью до перестановки и умножения на обратимые) представляется в виде произведения простых элементов.

7. Решите в целых числах (т.е. в $\mathbb{Z}$) уравнение

$$x^3 - y^2 = 4.$$

8. Докажите, что простое $q \equiv_4 3$ является простым и в $\mathbb{Z}[\mathfrak{i}]$.

!! **Теорема Ферма-Эйлера.**

Простое $p \equiv_4 1$ можно представить в виде суммы двух квадратов.

В связи с этим в $\mathbb{Z}[\mathfrak{i}]$ такое p не является простым.

Делимость комплексных чисел

! Кольцо $\mathbb{Z}[\mathfrak{i}] = \{a + b\mathfrak{i}, a, b \in \mathbb{Z}\}$ называется *кольцом гауссовых чисел.* Те его элементы, которые нельзя представить в виде произведения двух необратимых, называются *простыми.*

! Число $z \in \mathbb{Z}[\mathfrak{i}]$ *делится* на число $w \in \mathbb{Z}[\mathfrak{i}]$, если существует $t \in \mathbb{Z}[\mathfrak{i}]$ такое, что $z = wt$. Запись стандартная: $z \vdots w$ (либо $w|z$).

1. Опишите все пары чисел z, w такие, что одновременно $z|w$ и $w|z$.

2. Докажите, что если $|z|^2 \in \mathbb{P}$, то z – простой элемент $\mathbb{Z}[\mathfrak{i}]$.

? Какие из чисел $1+\mathfrak{i}$, 2, $2 \pm \mathfrak{i}$, 3, $3 \pm \mathfrak{i}$, $3 \pm 2\mathfrak{i}$, $4 \pm \mathfrak{i}$, $4 \pm 3\mathfrak{i}$, 5, $5 \pm \mathfrak{i}$, $5 \pm 2\mathfrak{i}$, $6 \pm \mathfrak{i}$, $5 \pm 4\mathfrak{i}$, 7 являются простыми в $\mathbb{Z}[\mathfrak{i}]$?

3. **Деление с остатком.**

   Докажите, что для любых $n, m \in \mathbb{Z}[\mathfrak{i}]$ $(m \neq 0)$ найдутся $q, r \in \mathbb{Z}[\mathfrak{i}]$ такие, что
   $$n = mq + r \quad \text{и} \quad |r| < |m|.$$

4. Найдите $(4 + 19\mathfrak{i}, -6 + 17\mathfrak{i})$ в $\mathbb{Z}[\mathfrak{i}]$. Представьте числа $4 + 19\mathfrak{i}$ и $-6 + 17\mathfrak{i}$ в виде произведения простых. Единственно ли это представление?

5. **Линейное представление НОДа.**

   Докажите, что для любых $n, m \in \mathbb{Z}[\mathfrak{i}]$ найдутся $s, t \in \mathbb{Z}[\mathfrak{i}]$ такие, что
   $$sn + tm = (n, m)\ .$$

6. **Единственность разложения.**

   Докажите, что любой $w \in \mathbb{Z}[\mathfrak{i}]$ единственным образом (с точностью до перестановки и умножения на обратимые) представляется в виде произведения простых элементов.

7. Решите в целых числах (т.е. в $\mathbb{Z}$) уравнение
   $$x^3 - y^2 = 4.$$

8. Докажите, что простое $q \equiv_4 3$ является простым и в $\mathbb{Z}[\mathfrak{i}]$.

!! **Теорема Ферма-Эйлера.**

Простое $p \equiv_4 1$ можно представить в виде суммы двух квадратов.

В связи с этим в $\mathbb{Z}[\mathfrak{i}]$ такое p не является простым.