

10/14/2026

Thm (Primes in $\mathbb{Z}[i]$). Let $\pi \in \mathbb{Z}[i]$ be prime.

1. $\pi = \pm 1 \pm i \mid 2$.

$$\begin{array}{c} \parallel \\ \sqrt{d} \quad (d = -1) \end{array}$$

$$\left(\frac{-1}{p}\right) = -1$$

2. $\pi = p \equiv 3 \pmod{4}$ or one of its associates

3. $\pi = x + yi \mid p$ with $x, y \neq 0$, where $p \equiv 1 \pmod{4}$.

$$\left(\frac{-1}{p}\right) = 1$$

In fact,

$$N(\pi) = \pi \bar{\pi} = x^2 + y^2 = p.$$

If π is such a prime divisor of p , there are

8 prime divisors of p in total:

$$\pm \pi, \pm i\pi, \pm \bar{\pi}, \pm i\bar{\pi}.$$

So there are exactly 8 ways of writing $p = x^2 + y^2$.

Similar things hold in $\mathbb{Z}[\sqrt{2}]$

$$\text{If } p > 2, \quad \begin{cases} 1, & p \equiv \pm 1 \pmod{8} \\ -1, & p \equiv \pm 3 \pmod{8} \end{cases}$$

$$\left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right) \left(\frac{2}{p}\right)$$

$$\begin{cases} 1, & p \equiv 1 \pmod{4} \\ -1, & p \equiv -1 \pmod{4} \end{cases} = \begin{cases} 1, & p \equiv 1 \pmod{8} \\ 1, & p \equiv -3 \pmod{8} \\ -1, & p \equiv 3 \pmod{8} \\ -1, & p \equiv -1 \pmod{8} \end{cases}$$

$$= \begin{cases} 1, & p \equiv 1, 3 \pmod{8}, \\ -1, & p \equiv -1, -3 \pmod{8}. \end{cases}$$

If $p = 2$ and $\pi | 2$, then we expect
 $\lambda + \gamma\sqrt{2}$

$$N(\pi) = \lambda^2 + 2\gamma^2 = 2 \Rightarrow (\lambda, \gamma) = (0, \pm 1) \Rightarrow \pi = \pm\sqrt{2}.$$

Thm (Primes in $\mathbb{Z}[\sqrt{-2}]$) Let $\pi \in \mathbb{Z}[\sqrt{-2}]$ be prime.

1. $\pi = \pm\sqrt{2} \mid 2$.

2. $\pi = p \equiv -1, -3 \pmod{8}$ or one of its associates

3. $\pi = x + y\sqrt{-2} \mid p$ with $x, y \neq 0$, where $p \equiv 1, 3 \pmod{8}$. In fact,

$$N(\pi) = \pi \bar{\pi} = x^2 + 2y^2 = p.$$

If π is such a prime divisor of p , there are

4 prime divisors of p in total:

$$\pi, -\pi, \bar{\pi}, -\bar{\pi}.$$

sum of 3 squares.
↑

$$x^2 + y^2 + y^2$$

So there are exactly 4 ways of writing $p = \boxed{x^2 + 2y^2}$.

What about $\mathbb{Z}[\sqrt{2}]$?

If $p > 2$,

$$\left(\frac{2}{p}\right) = \begin{cases} 1, & p \equiv \pm 1 \pmod{8} \\ -1, & p \equiv \pm 3 \pmod{8} \end{cases}$$

If $p = 2$ and $\pi = x + y\sqrt{2} \mid p$, we expect

$$|N(\pi)| = |x^2 - 2y^2| = 2 \Rightarrow (x, y) = (\pm 2, \pm 1),$$

$$(0, \pm 1),$$

$$(\pm 4, \pm 3),$$

Are there any more solutions?

Thm (Primes in $\mathbb{Z}[\sqrt{2}]$) Let $\pi \in \mathbb{Z}[\sqrt{2}]$ be prime.

1. $\pi \mid 2$ with $|N(\pi)| = 2$.

2. $\pi = p \equiv \pm 3 \pmod{8}$ or one of its associates

3. $\pi = x + y\sqrt{2} \mid p$ with $x, y \neq 0$, where $p \equiv \pm 1 \pmod{8}$.

In fact,

$$|N(\pi)| = |\pi \bar{\pi}| = |x^2 - 2y^2| = p.$$

If π is such a prime divisor of p , there are

? prime divisors of p in total.

So there are exactly ? ways of writing $p = |x^2 - 2y^2|$.

Q: What are the units in $\mathbb{Z}[\sqrt{2}]$?

This amounts to solving

$$|N(\alpha)| = |N(x + y\sqrt{2})| = |x^2 - 2y^2| = 1.$$



$$x^2 - 2y^2 = 1$$

(positive Pell's equation)

$$x^2 - 2y^2 = -1$$

(negative Pell's equation)

More generally, for $d > 1$ not a square,

$$x^2 - dy^2 = 1$$

(positive Pell's equation)

$$x^2 - dy^2 = -1$$

(negative Pell's equation)

$$x^2 - 2y^2 = 1$$

$$(x, y) = (\pm 1, 0) \rightarrow \pm 1$$

$$(\pm 3, \pm 2) \rightarrow \pm 3 \pm 2\sqrt{2}$$

$$x^2 - 2y^2 = -1 \quad \begin{matrix} \uparrow \\ \pm 1 \pm \sqrt{2} \end{matrix}$$

$$(x, y) = (\pm 1, \pm 1)$$

$$(\pm 7, \pm 5)$$

$$\downarrow \\ \pm 7 \pm 5\sqrt{2}$$

$$(1 + \sqrt{2})^2 = 1^2 + (\sqrt{2})^2 + 2 \cdot 1 \cdot \sqrt{2} = 3 + 2\sqrt{2}$$

Conjecture: Maybe $\pm \epsilon_0 = \pm 1 \pm \sqrt{2}$ generates everything.

$$(1 + \sqrt{2})^3 = (1 + \sqrt{2})^2 (1 + \sqrt{2}) = (3 + 2\sqrt{2})(1 + \sqrt{2})$$

$$= 7 + 5\sqrt{2}$$

We will prove

Thm. The units in $\mathbb{Z}[\sqrt{2}]$ are

$$\pm \epsilon_0^n = \pm (1 + \sqrt{2})^n, \quad n \in \mathbb{Z}.$$

Equivalently, the set of units under multiplication is

an abelian group generated by -1 and ϵ_0 .