

10/16/2026

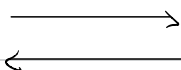
$$x^2 - dy^2 = 1$$

(positive Pell's equation)

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

(negative Pell's equation)

units $\varepsilon = x + y\sqrt{d}$



in $\mathbb{Z}[\sqrt{d}]$

Solutions (x, y) to

Pell's equations $x^2 - dy^2 = \pm 1$.

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

$$\pm \varepsilon_0^n = \pm (1 + \sqrt{2})^n, \quad n \in \mathbb{Z}.$$

Equivalently, the set of units under multiplication is

an abelian group generated by -1 and ε_0 .

Note : $\underbrace{(1+\sqrt{2})}_{\varepsilon_0} \underbrace{(-1+\sqrt{2})}_{\varepsilon_0^{-1}} = -1^2 + (\sqrt{2})^2 = 1$

$\hookrightarrow \varepsilon_0^{-1} = \frac{1}{1+\sqrt{2}} = \sqrt{2}-1 \in \mathbb{Z}[\sqrt{2}]$

$\parallel$

$$\frac{-1+\sqrt{2}}{\underbrace{(1+\sqrt{2})(-1+\sqrt{2})}_1} = -1+\sqrt{2}$$

$\varepsilon_0 = 1+\sqrt{2}$ satisfies $N(\alpha) = 1^2 - 2 \cdot 1^2 = -1$

$N(\varepsilon_0^n) = (N(\varepsilon_0))^n = (-1)^n, \quad n \geq 0.$

$N(\varepsilon_0^{-n}) = (N(\varepsilon_0^{-1}))^n = (N(-1+\sqrt{2}))^n = (-1)^n, \quad n \geq 0.$

$\hookrightarrow \pm \varepsilon_0^n \ (n \in \mathbb{Z})$ are units in $\mathbb{Z}[\sqrt{2}]$.

pf. Already verified that $\pm \epsilon_0^n$ ($n \in \mathbb{Z}$) are units.

Step 1. Show ϵ_0 is the least unit > 1 .

Assume $1 < \epsilon = x + y\sqrt{2} < \epsilon_0 = 1 + \sqrt{2}$ is a unit.

①

So

$$|N(\epsilon)| = |x^2 - 2y^2| = 1.$$

$$\epsilon \bar{\epsilon} = (x + y\sqrt{2})(x - y\sqrt{2})$$

Thus

$$|x - y\sqrt{2}| = \frac{1}{|x + y\sqrt{2}|} < 1. \Rightarrow \underline{-1 < x - y\sqrt{2} < 1.}$$

②

$$\textcircled{1} + \textcircled{2} : 0 < 2x < 2 + \sqrt{2} \Rightarrow 0 < x < 1 + \frac{\sqrt{2}}{2} < 2.$$

So $x = 1$. But $x^2 - 2y^2 = \pm 1$. So $y = 0, \pm 1$.

Since $1 < \epsilon = x + y\sqrt{2} < 1 + \sqrt{2}$, impossible.

Hence no unit lies in $(1, \epsilon_0)$.

Step 2 Show that any unit is one of $\pm \epsilon_0^n$ ($n \in \mathbb{Z}$).

Let ϵ be a unit. If $\epsilon < 0$, we argue for $-\epsilon > 0$.

If $0 < \epsilon < 1$, then we argue for the unit $\epsilon^{-1} > 1$.

So may assume $\epsilon \geq 1$.



$\exists n \geq 0$ s.t. $\epsilon_0^n \leq \epsilon < \epsilon_0^{n+1}$.

Then the unit $\varepsilon \varepsilon_0^{-n}$ lies in $[1, \varepsilon_0)$.

Step 1 shows that there is no unit in $(1, \varepsilon_0)$.

$$\text{So } \varepsilon \varepsilon_0^{-n} = 1, \text{ i.e., } \varepsilon = \varepsilon_0^n.$$



If $\varepsilon_n = \pm \varepsilon_0^n = x_n + y_n \sqrt{2}$, where $x_n, y_n \in \mathbb{Z}$, then

$$x_n^2 - 2y_n^2 = N(\pm \varepsilon_n) = (N(\varepsilon_0))^n = (-1)^n.$$

So even values of n gives all $x, y \in \mathbb{Z}$ satisfying

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

and odd values of n gives all $x, y \in \mathbb{Z}$ satisfying

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

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

1. $\pi \mid 2$ with $|N(\pi)| = 2$: $\pm \epsilon_0^n \sqrt{2}$ ($n \in \mathbb{Z}$).

2. $\pi = p \equiv \pm 3 \pmod{8}$ or one of $\pm \epsilon_0^n p$ ($n \in \mathbb{Z}$).

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:

$$\pm \epsilon_0^n \pi, \pm \epsilon_0^n \bar{\pi}.$$

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

Ex. Find all units and classify all the primes in $\mathbb{Z}[\sqrt{3}]$.

Note: $x^2 - 3y^2 = -1$ has no solutions.

1. $x^2 + 1 = 3y^2$: $e_3(3y^2) = 1 + e_3(y^2) = 1 + 2e_3(y)$ is odd, so $3y^2 \neq \square + \square$, but $x^2 + 1$ is. So

$x^2 - 3y^2 = -1$ has no integer solutions.

(Or just mod 3: $x^2 \equiv -1 \pmod{3}$, impossible).

2. $x^2 - 3y^2 = 1$ has a solution $\epsilon_0 = 2 + \sqrt{3}$.

Show ϵ_0 is the least unit > 1 and every unit is one of $\pm \epsilon_0^n$ ($n \in \mathbb{Z}$).

More generally, $x^2 - dy^2 = -1$ may not have a solution, but $x^2 - dy^2 = 1$ always have a solution

$\epsilon_0 = x_0 + y_0\sqrt{d}$, the least unit > 1 .

fundamental unit: every unit in $\mathbb{Z}[\sqrt{d}]$

is one of $\pm \epsilon_0^n$, when $x^2 - dy^2 = -1$ has no solutions.

If $x^2 - dy^2 = -1$ has a solution $\epsilon'_0 > 1$, the least

unit > 1 , then every unit is one of $\pm (\epsilon'_0)^n$.