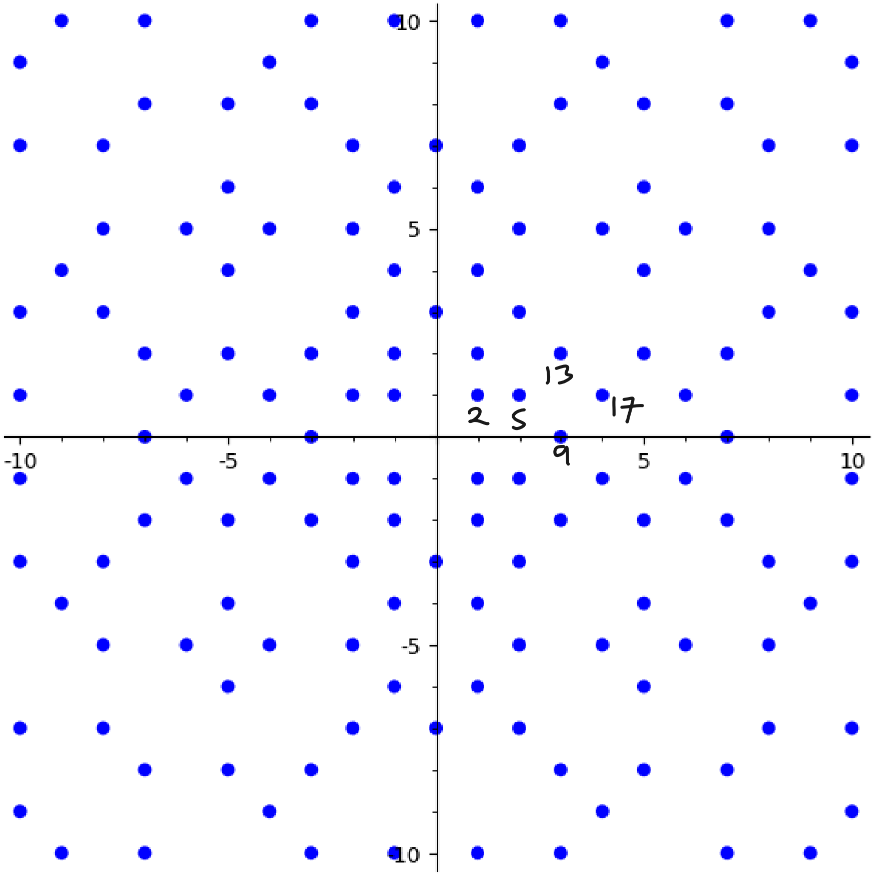
Eisenstein and other quadratic integers


```
R.<i> = GaussianIntegers()
n = 10
primes = [a+b*i for a in range(-n,n+1) for b in range(-n,n+1) \
if (a+b*i).is_prime()]
list_plot(primes, aspect_ratio=1, size=40, figsize=[6,6])
```



Reminder about the Gaussian integers

Theorem Up to units $\{\pm 1, \pm i\}$, the primes in $\mathbb{Z}[i]$ are:

- $1+i$ $\qquad (1+i)^2 = 2$
- $a+bi$ $\qquad a^2+b^2 = p,\ p \equiv 1 \pmod 4$
- p $\qquad p \equiv 3 \pmod 4$

Moreover, unique factorization holds.

The Eisenstein integers

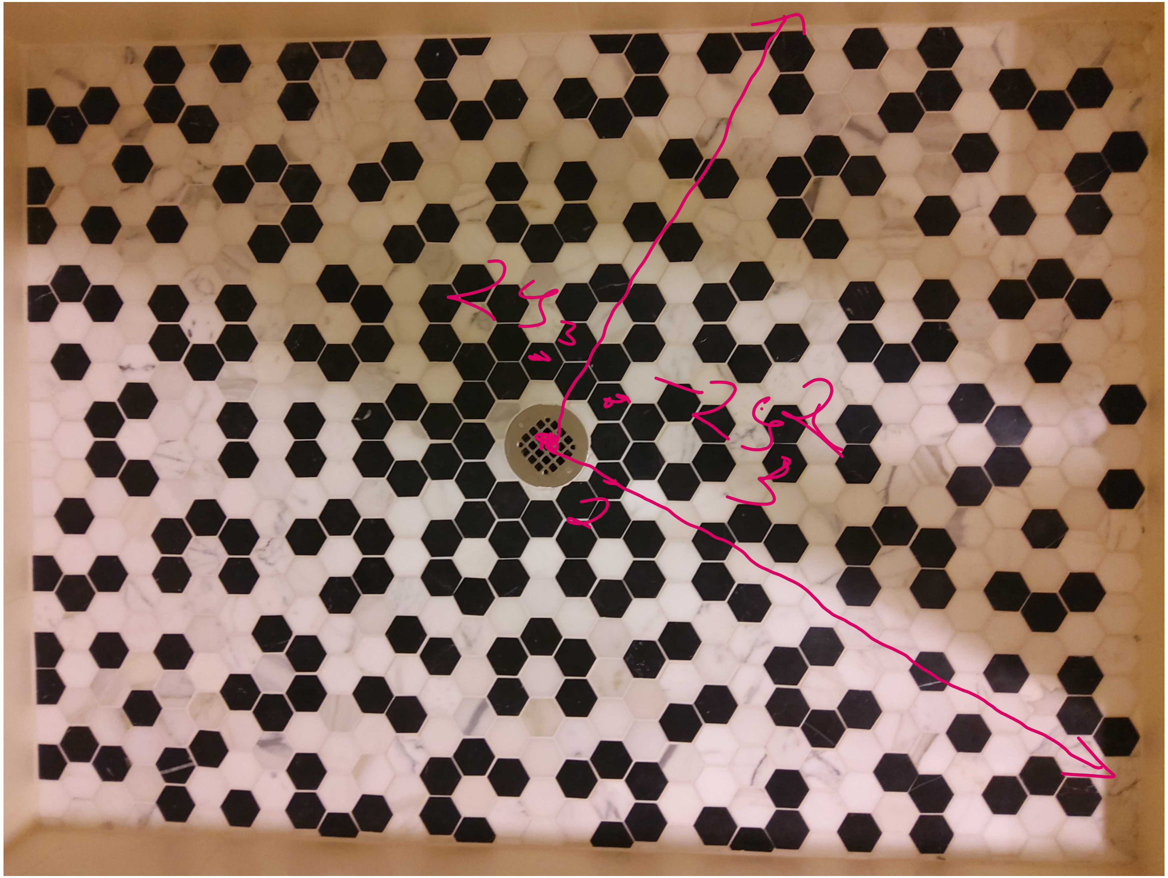
$$\zeta_3^2 = -1 - \zeta_3$$

$$\mathbb{Z}[\zeta_3] = \{a + b\zeta_3 + \cancel{c\zeta_3^2} : a, b, \cancel{c} \in \mathbb{Z}\}$$

minpoly is $x^2 + x + 1$

$$\zeta_3 = \frac{-1 + \sqrt{3}i}{2}$$

fraction field is $\mathbb{Q}(\zeta_3) = \mathbb{Q}(\sqrt{-3})$



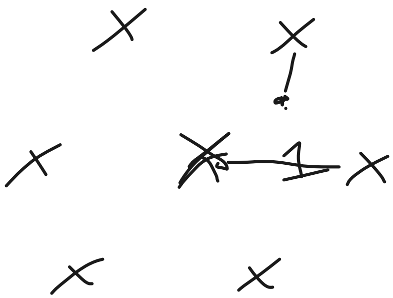
The Eisenstein integers are a Euclidean domain

For any $a, b \in \mathbb{Z}[\zeta_3]$ $b \neq 0$

$\exists\, q, r \in \mathbb{Z}[\zeta_3]$ with $a = qb + r$

$|r| < |b|$.

$$\frac{a}{b} = q + \frac{r}{b}$$ again, set q by rounding $\frac{a}{b}$.



Primes in the Eisenstein integers

Theorem Up to units $\{\pm 1, \pm \zeta_3, \pm \zeta_3^2\}$

The primes in $\mathbb{Z}[\zeta_3]$ are

- $1-\zeta_3$ $\qquad |1-\zeta_3|^2 = 3$
- $a+b\zeta_3$ $\qquad = (1-\zeta_3)(1-\zeta_3^2)$
  $|a+b\zeta_3|^2 = p \quad p \equiv 1 \pmod 3$
- p $\qquad p \equiv 2 \pmod 3$

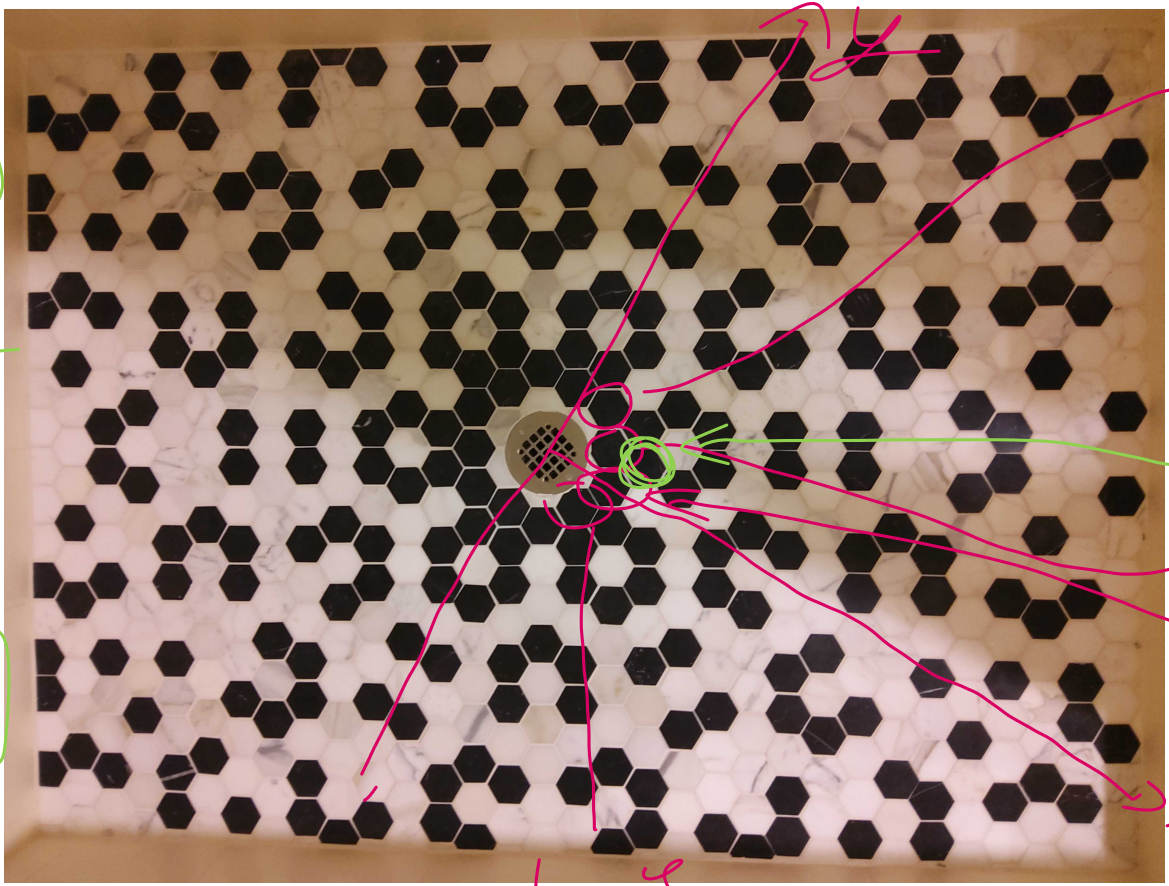
$(2-y_3^2)(2-y_3)$

$= 4-2y_3$

$-2y_3^2$

$+1$

$= 7$



$Z[y_3]$

Integers in other quadratic fields

D squarefree integer $\neq 1$

$\mathbb{Q}(\sqrt{D})$ is a number field and

$$\mathbb{Q}(\sqrt{D}) \cap \overline{\mathbb{Z}} = \begin{cases} \mathbb{Z}[\sqrt{D}] & D \not\equiv 1 \pmod 4 \\ \mathbb{Z}\left[\frac{1+\sqrt{D}}{2}\right] & D \equiv 1 \pmod 4 \end{cases}$$

Proof: look at minimal polynomials.

Euclidean vs. PID vs. UFD

If $\mathbb{Q}(\sqrt{D}) \cap \overline{\mathbb{Z}}$ is Euclidean, then it is a principal ideal domain and a unique factorization domain

Otherwise could still be a PID $\Rightarrow$ UFD

In this case UFD $\Rightarrow$ PID.

Imaginary quadratic fields $D<0$

Only a few cases where $\mathbb{Q}(\sqrt{D}) \cap \overline{\mathbb{Z}}$ is Euclidean,

and only 9 cases where it is a PID:

$$D = -1, -2, -3, -7, -11, -19, -43, -67, -163$$

Conjectured by Gauss,

proved by Heegner, Baker, Stark

Real quadratic fields $D>0$

Arithmetic statistics

Again only finitely many Euclidean but conjecture (Cohen-Lenstra)

infinitely many which are PID's and we can predict the percentage

CE 600 CE 1100 CE 1600

Thm Brahmagupta, Bhāskara, Fermat, Pell

$\exists\ \infty$ many $a,b\in\mathbb{Z}$ s.t. $a^2-b^2D=1$

$\Longrightarrow a+b\sqrt{D}$ is a unit in $\mathbb{Z}[\sqrt{D}]$

A failure of unique factorization

in $\mathbb{Z}[\sqrt{-5}]$ $\quad (1+\sqrt{-5})(1-\sqrt{-5})$

$$= 6 = 2 \cdot 3$$

all of 2, 3, $1+\sqrt{-5}$, $1-\sqrt{-5}$ are irreducible.