Euclidean algorithm in \( \mathbb{Z} \), \( \mathbb{Z}[x] \), \( \mathbb{Z}[i] \)

* All the same once you know how to divide

Division in \( \mathbb{Z} \): If \( a, b \) in \( \mathbb{Z} \), \( b = qa + r \) with \( 0 \leq r < |a| \)

[just long division].

Division in \( \mathbb{F}_p[x] \): If \( a, b \) in \( \mathbb{F}_p[x] \) then

\( b = qa + r \) where \( \deg r < \deg a \).

[just polynomial long division].

Division in \( \mathbb{Z}[i] \): If \( a, b \) in \( \mathbb{Z}[i] \)

then \( b = qa + r \) where \( N(r) < N(a) \).

To compute \( q \) and \( r \) \( (|r| < |a|) \),

1. Compute \( \frac{b}{a} = x + yi \) in \( \mathbb{C} \). \( N(x + yi) = x^2 + y^2 \)
2. Round \( x \) and \( y \) to the nearest integers to get \( q = x_0 + y_0 i \).

\( r = b - qa \).

Example: \( b = 2 + 3i \), \( a = 1 + i \).
\[
\frac{b}{\lambda} = \frac{2 + 5i}{1 + i} = \frac{(2 + 5i)(1 - i)}{(1 + i)(1 - i)} = \frac{7 + 3i}{2} = \frac{7}{2} + \frac{3}{2}i
\]

\[q = 4 + 2i\]

\[r = 2 + 5i - (4 + 2i)(1 + i)\]

\[r = 2 + 5i - (2 + 6i)\]

\[r = -i\]

\[\overline{(2 + 5i)} = (4 + 2i)(1 + i) + (-i)\]

Euclidean algorithm stops when you get zero as a remainder.

The \(\text{gcd}\) is the last non-zero remainder.

In \(\text{Eq} \ (6)\), can't tell difference between \(x + 1\) and \(2(x + 1)\) in terms of what \(\text{Eq} \ (6)\) divide.

\(\text{gcd}\) only well-defined up to a unit if any one of them is ok.
QR and the Legendre symbol.

1. \( \left( \frac{m}{n} \right) \) ← compute using the rules.

(First factor \( \chi \), separate out terms, then simplify them using q.r.):

\[
\left( \frac{5}{3q} \right) = \left( \frac{5}{3} \right) \left( \frac{5}{13} \right) = \left( \frac{2}{3} \right) \left( \frac{13}{5} \right)
\]

\[
= \left( \frac{2}{3} \right) \left( \frac{3'}{5} \right) = \left( \frac{2}{3} \right) \left( \frac{2}{5} \right) = 1
\]

So \( S \) is a square mod 79.

Offer this hint to know: \( \left( \frac{K}{p} \right) \) \( p \) an odd prime

\[
\left( \frac{K^a}{p} \right) = K^{\frac{p-1}{2}} \text{ mod } p.
\]
Week 10 - Ex 1.2 — Use the discrete log w/ base $g^3$ to find the square roots of $5$ in $\mathbb{F}_{19}$.

$I: \mathbb{F}_{19}^x \to \mathbb{Z}/19\mathbb{Z}$

send $y \in \mathbb{F}_{19}^x$ to the power $x$ s.t. $g^x = y$.

Looking for square roots of $5$ in $\mathbb{F}_{19}$

$t^2 = 5 + \in \mathbb{F}_{19}^x$

$2 \cdot I(\cdot) = I(5)$ — solve this equation in $\mathbb{Z}/19\mathbb{Z}$

$\sqrt{5} = I(\cdot)$

Use CRT to solve in $\mathbb{Z}/19\mathbb{Z}$ and $\mathbb{Z}/19\mathbb{Z}$.

Exercise 2 on Week 10 root of unity

This will not show up in Exercise 3.

But it may still show up in T/F questions.

In a field $K$, an nth root of unity is an element $\omega \in K$ s.t. $\omega^n = 1$. 
It's a primitive nth root if $n$ is the smallest power that gives $1$ (sufficient check only your dividing $n$).

(1) Show $e^{2\pi i/n}$ is a primitive nth root of unit $e^{2\pi i}$.

$(e^{2\pi i/n})^n = e^{2\pi i} = \cos(2\pi) + i\sin(2\pi) = 1$

so it is an nth root of unit $e^{2\pi i}$.

Take $0 < k < n$

$(e^{2\pi i/n})^k = e^{2\pi ik/n} = \cos(2\pi k/n) + i\sin(2\pi k/n)$

thus $k < 1 \implies \cos(2\pi k/n) < 1 \implies 2\pi k/n < \pi$, $\sin(2\pi k/n) = 0$, and $\frac{\pi}{n}$ radians of $2\pi$.

Because $0 < k < n$

$0 < \frac{2\pi k}{n} < \pi$

so $\cos(2\pi k/n) \neq 1$.

$\therefore e^{2\pi ik/n} \neq 1$. 

\[\]
(2). $z_3 = e^{2\pi i / 3}$

Verify $\left(z_3 - \overline{z}_3\right)^2 = -3$.

$\cos(\theta) = -\frac{1}{2}, \quad \sin(\theta) = \frac{\sqrt{3}}{2}$

$3_3 = e^{2\pi i / 3} = \cos \frac{2\pi}{3} + i \sin \frac{2\pi}{3} = -\frac{1}{2} + i \frac{\sqrt{3}}{2}$

$z_3 = e^{4\pi i / 3} = \cos \frac{4\pi}{3} + i \sin \frac{4\pi}{3} = -\frac{1}{2} - i \frac{\sqrt{3}}{2}$

$z_3 - \overline{z}_3 = i \sqrt{3}$

$\Rightarrow -3$. 

Ex 4 Sum of 2 squares and Gaussian rings
Know the form of Gaussian primes.

Ex 5 Pell's equations
Understand idea of using multiplicativity of norm to get new solutions.