Euclidean algorithm in $\mathbb{Z}$, $\mathbb{F}_p[x]$, $\mathbb{Z}[i]$

* All the same <u>once you know how to divide</u>

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

(just long division).

Division in <u>$\mathbb{F}_p[x]$</u>: If a, b in $\mathbb{F}_p[x]$ (a nonzero) 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 $N(r) < N(a)$.

$(|r| < |a|)$.

To compute q and r

1. Compute $\frac{b}{a} = x + yi$ in $\mathbb{C}$.

$N(x+yi) = x^2 + y^2$
$= |x+iy|^2$.

2. Round x and y to the nearest integers to get

$q = x_0 + y_0 i$.

$r = b - qa$.

<u>Example</u>: $b = 2 + 5i$ $a = 1 + i$.

$$\frac{b}{a} = \frac{2+5i}{1+i} = \frac{(2+5i)(1-i)}{(1+i)(1-i)} = \frac{7+3i}{2}$$

$$= \frac{7}{2} + \frac{3}{2}i$$

$$q = 4+2i$$

$$r = 2+5i - (4+2i)(1+i)$$

$$r = 2+5i - (2+6i)$$

$$= -i.$$

$$\underbrace{(2+5i)}_{b} = \underbrace{(4+2i)}_{q}\underbrace{(1+i)}_{a} + \underbrace{(-i)}_{r}$$

Euclidean algorithm stops when you get zero as a remainder

The gcd is the last non-zero remainder.

In $\mathbb{F}_3(x)$ can't tell difference between $x+1$ and $2(x+1)$ in terms of what they divide.

(gcd only well-defined up to a unit; any one of them is ok)

QR and the Legendre symbol.

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

(First factor n, separate out terms, then simplify them using q.r.).

$$\left(\frac{5}{39}\right) = \left(\frac{5}{3}\right)\left(\frac{5}{13}\right)$$

$$= \left(\frac{2}{3}\right)\left(\frac{13}{5}\right)$$

$$= \left(\frac{2}{3}\right)\left(\frac{3}{5}\right)$$

$$= \left(\frac{2}{3}\right)\left(\frac{5}{3}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{3}\right)$$

$$= 1$$

So 5 is a square mod 39.

Other big thing to know: $\left(\frac{k}{p}\right)$ p an odd prime

$$\left(\frac{k}{p}\right) = k^{\frac{p-1}{2}} \bmod p.$$

Week 10 - Ex 1.2 — Use the discrete log w/ base $g=3$ to find the square roots of 5 in $\mathbb{F}_{19}$.

$I: \mathbb{F}_{19}^\times \to \mathbb{Z}/18\mathbb{Z}$

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

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

$t^2 = 5 \qquad t \in \mathbb{F}_{19}^\times$

$2\,I(t) = I(5)$ in $\mathbb{Z}/18\mathbb{Z}$ ← solve this equation in $\mathbb{Z}/18\mathbb{Z}$ for $I(t)$

Use CRT solve in $\mathbb{Z}/9\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z}$

$t = g^{I(t)}$.

Exercise 2 on Week 10 roots of unity.

This will not show up in Exercise 3 of the final.

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

In a field K an nth root of unity is an element $\alpha \in K$ s.t. $\alpha^n = 1$.

It's a primitive nth root if n is
the smallest power that gives 1.
(suffices check only powers dividing n)

---

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

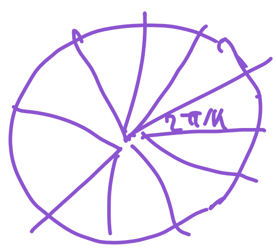
$$\left(e^{2\pi i/n}\right)^n = e^{2\pi i} = \cos(2\pi) + i\sin(2\pi) = 1$$

so it $\underline{\text{is}}$ an nth root of unity.

Take $0 < k < n$

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

this is $1 \iff \cos(2\pi k/n) = 1 \iff 2\pi k/n$
$\sin(2\pi k/n) = 0$. is an integral multiple of 2π.



Because $0 < k < n$

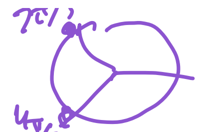
$$0 < \frac{2\pi k}{n} < 2\pi$$

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

so $e^{2\pi i k/n} \neq 1$.

(2). $\zeta_3 = e^{2\pi i/3}$

verify $(\zeta_3 - \zeta_3^2)^2 = -3$.



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

$\cos(4\pi/3) = -\frac{1}{2}$ $\quad \sin(4\pi/3) = -\frac{\sqrt{3}}{2}$

$$\zeta_3 = e^{2\pi i/3} = \cos 2\pi/3 + i \sin 2\pi/3 = -\tfrac{1}{2} + i\tfrac{\sqrt{3}}{2}$$

$$\zeta_3^2 = e^{4\pi i/3} = \cos 4\pi/3 + i \sin 4\pi/3 = -\tfrac{1}{2} - i\tfrac{\sqrt{3}}{2}.$$

$$\zeta_3 - \zeta_3^2 = i\sqrt{3}$$

square $\rightsquigarrow -3$.

<u>Ex 4</u> Sums of 2 squares and Gaussian primes

know decent

Know the form of Gaussian primes.

<u>Ex 5</u> <u>Pell's equations</u>

Understand idea of using multiplicativity of norm to get new solutions