$$\left(\frac{n}{p}\right) \equiv n^{\frac{p-1}{2}} \mod p.$$

Exercise 1 – part (1)

Use this to compute some specific examples.

Example: (a) Use a calculator, or

$n = 2 \qquad p = 31$

$$2^{\frac{31-1}{2}} = 2^{15} \mod 31$$

Can use successive squares

$$15 = 8 + 4 + 2 + 1$$

$$2^{15} = 2^8 2^4 2^2 2^1$$

$2^1 = 2$

$2^2 = 4$

$2^4 = 16$

$2^8 = 256 = 8 \mod 31$

$2^{15} = 2 \cdot 4 \cdot 16 \cdot 8 \mod 31$

$= 2 \cdot 16 \mod 31$

$= 32 \mod 31$

$= 1.$

So $2^{15} = 1 \mod 31$

so $\left(\frac{2}{31}\right) = 1$

so 2 is a square mod 31.

Ex 1 - (2)

Use discrete log with base $g=3$ to find the square roots of 5 in $\mathbb{F}_{19}$.

I discrete log.

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

$$I(x^2) = I(5) \text{ in } \mathbb{Z}/18\mathbb{Z}.$$

$$\longrightarrow 2I(x) = I(5)$$

Careful because 2 is not invertible in $\mathbb{Z}/18\mathbb{Z}$.

$$2I(x) = I(5)$$

$$g^{2I(x)} = 5$$

$$(g^{I(x)})^2 = 5.$$

↖ Solve this in $\mathbb{Z}/18\mathbb{Z}$ then go back by raising g to the power.

Ex 1 - (3).

a) Does $x^2 + 4x + 11 \equiv 0 \mod 43$ have a solution?

$$(x+2)^2 + 7 \equiv 0 \mod 43$$

$$\Leftrightarrow$$

$$(x+2)^2 \equiv -7 \mod 43$$

So there is a solution $\Leftrightarrow -7$ is a square mod 43

$$\Leftrightarrow \left(\frac{-7}{43}\right) = 1.$$

Note: $\left(\frac{-?}{4k+3}\right) = \left(\frac{-1}{4k+3}\right)\left(\frac{?}{4k+3}\right) = -\left(\frac{?}{4k+3}\right)$

In video, we used $\left(\frac{n}{p}\right) \equiv n^{\frac{p-1}{2}} \pmod p$

to show multiplicative of the Legendre symbol

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

Still need to explain $\left(\frac{?}{p}\right) = \{ \ldots -$

and quadratic reciprocity.

Need something new.

Idea: Express square roots using roots of unity and then manipulate that expression.

An nth root of unity in a field $\mathbb{K}$ is a root in $\mathbb{K}$ of $x^n - 1$

i.e. $\zeta \in \mathbb{K}$ is an nth root of unity if $\zeta^n = 1$.

Example: 1 is a nth root of unity for any n

$$1^n = 1$$

$$x^n - 1 = (x-1)(x^{n-1} + x^{n-2} + \cdots + x + 1).$$

- -1 is an nth root of unity when n is even.

$$(-1)^n = 1$$

$$x^2 - 1 = (x-1)(x-(-1))$$
$$= (x-1)(x+1).$$

- Any $a \in \mathbb{F}_p^\times$ is a $(p-1)$st root of unity.

Lagrange: $a^{p-1} = 1$
(Fermat's little theorem).

$$x^{p-1} - 1 = (x-1)(x-2)\dots(x-(p-1)) \mod p.$$

- $\zeta = e^{2\pi i/n}$ ζ is an nth root of unity.

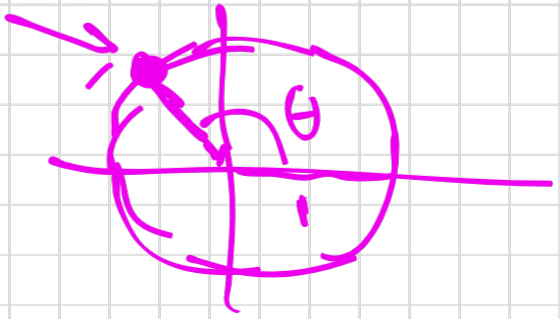
$$\zeta^n = \left(e^{2\pi i/n}\right)^n = e^{2\pi i} = 1$$

Can check w/ Euler's identity: $e^{\theta i} = \cos\theta + i\sin\theta$

(Extra 2π on worksheet - please correct and I'll fix online)

$$e^{2\pi i} = \cos 2\pi + i\sin 2\pi$$
$$= 1 + i0 = 1.$$

Euler's identity: $e^{i\theta}$



An nth root of unity ζ is <u>primitive</u> if $\zeta^d \neq 1$ for any proper divisor $d \mid n$ $d \neq n$.

<u>Example</u>: • 1 is an nth root of unity for all n but is only a primitive first root of unity.

• -1 is a primitive 2nd root of unity

• In part (1) of Ex. 2 show $e^{2\pi i/n}$ is a primitive nth root in $\mathbb{C}$

- $g \in \mathbb{F}_p^\times$ is a primitive root $\iff$ g is a primitive $(p-1)$st root of unity.. (our earlier terminology)

Exercise 2: (2) → (6), (3) → (7), (4) → (8).

$e^{i\theta} = \cos\theta + i\sin\theta$,

(2) $(\zeta_3 - \zeta_3^2)^2$ where $\zeta_3 = e^{2\pi i/3}$ $\quad 1 = \zeta_3^3$ $\quad \zeta_3^4 = \zeta_3^3\zeta_3 = \zeta_3^1$

$= \zeta_3^2 - 2(\zeta_3^3) + \zeta_3^4 = \zeta_3^2 - 2\cdot 1 + \zeta_3$

$= \zeta_3^2 + \zeta_3 - 2$.

$= e^{\frac{4\pi i}{3}} + e^{\frac{2\pi i}{3}} - 2$

$= \cos\frac{4\pi}{3} + i\sin\frac{4\pi}{3} + \cos\frac{2\pi}{3} + i\sin\frac{2\pi}{3} - 2$

$-\frac{1}{2}$ $\qquad$ $-\frac{1}{2}$

$= -1 - 2 = -3$

Part (6)

$\zeta = 2$

$(2^2 - 2)^2 = (2)^2 = 4$

$\equiv -3 \bmod 7$.

$\sin(x) = -\sin(2\pi - x)$