Exercise 1.

Theorem. If \( \gcd(c, m) = 1 \), then for any \( \alpha \in \mathbb{Z}/n\mathbb{Z} \), there is a unique solution \( x \) to \( x^e \equiv a \pmod{m} \) \( (x \in \mathbb{Z}/m\mathbb{Z}) \) given by \( x = a^d \)

where \( d \) is the multiplicative inverse of \( e \) modulo \( \phi(m) \).

This way to find roots in \( \mathbb{Z}/n\mathbb{Z} \) is called...
$x^e \equiv a \mod m$.

Part (1)-(4) Exercise 1.

Example: $x^5 \equiv 2 \mod 35 \quad e = 5 \quad a = 2 \quad m = 35$

$\phi(m) = \phi(35) = \phi(5)\phi(7) = 24$

$\gcd(5, 24) = 1$ so the theorem applies.

Need to compute $d$: $24 = 5 \cdot 4 + 4 \quad 1 = 5 - 1 \cdot 4$

Euclidean algorithm to compute mult. inverse.

mult. inverse of $5 \mod 24$ is $5!$

so $d = 5$. Solution is $x = a^d = 2^5 = 32$

Can check: $32^5 = (-3)^5 = 8 \cdot 9 = 72 \equiv 2 \mod 35$
Exercise 2.

1. Recall the order of \( g \in G \) is the smallest \( k \) s.t.
\[
g^k = e.
\]
E.g., in \( \mathbb{F}_3^* \), \( \text{ord}(g) = 12 \) \( \Rightarrow \) \( \theta \)
is a primitive root.

2. and \( \cdots \) are interesting — use discrete by
to solve some equations.
$2$ is a primitive root in $\mathbb{F}_{11}$.

Discrete log base $2$ in $\mathbb{F}_{11}$

$$\mathbb{F}_{11} \xrightarrow{I} \mathbb{Z}/10\mathbb{Z}$$

$I(x) = y \iff 2^y = x$.

Turns mult. into addition

$$2 \cdot (2^2 \cdot c) \implies \forall x^2 \equiv a \mod 11.$$

$$I(y \cdot x^2) = I(a) \text{ in } \mathbb{Z}/10\mathbb{Z}$$

$$I(y) + I(x^2) = I(a) \text{ in } \mathbb{Z}/10\mathbb{Z}$$

$$2 \cdot I(x) = I(a) - I(4) \text{ in } \mathbb{Z}/10\mathbb{Z}.$$

- Solve for $I(x)$
To discretely need to write out

\[ x = 2 \text{ I}(x) \]

\[ a \rightarrow 0 1 2 3 4 5 6 7 8 9 \]

\[ 2^a \mod 11 = 1 2 4 9 \]

\[ F_{11}^x = x \rightarrow 1 2 3 4 5 6 7 8 9 10 \]

\[ \mathbb{Z}/10\mathbb{Z} \rightarrow \text{I}(x) \rightarrow 0 1 8 2 4 9 7 3 6 5 \]

\[ 2^a = 2^5 \mod 11 \]

if \( a \in \mathbb{Z} \mod 11 \)
$z \in \mathbb{F}_{11}^x \subseteq \text{group of order 10}$

$b = 10q + a$

$2^b = 2^{10q} \cdot 2^a \mod 11$

$= (2^{10})^q \cdot 2^a \mod 11$

$= 1^q \cdot 2^a \mod 11$

$= 2^a \mod 11$

$2^{10} = 1 \in \mathbb{F}_{11}^x$

by Lagrange

$|\mathbb{F}_{11}^x| = 10$

because