Exercise 1.

Theorem If $\gcd(e, m) = 1$, then for any $a \in (\mathbb{Z}/m\mathbb{Z})^{\times}$, there is a unique solution to $x^e \equiv a \bmod m$ $(x \in \mathbb{Z}/m\mathbb{Z})$ given by $x = a^d$ where d is the mult. inverse of e modulo $\phi(m)$.

---

way to find roots in $\mathbb{Z}/m\mathbb{Z}$ i.e. solve

$x^e = a \mod m$.

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: $\quad 24 = 5 \cdot 4 + 4 \qquad 1 = 5 - 1 \cdot 4$

$5 = 1 \cdot 4 + 1 \qquad = 5 - (24 - 5 \cdot 4)$

Euclidean algorithm + unwind to compute mult. inverse.

$= 5 \cdot 5 - 24$

mult. inverse of 5 mod 24 is 5! $\quad (5 \cdot 5 = 25 = 1 + 24)$.

so $d = 5$. $\quad$ Solution is $x = a^d = 2^5 = \underline{\underline{32}}$

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

$(-3)^3 = -27$
$\equiv 8 \bmod 35$ $\quad (-3)^2$

Exercise 2.

① Recall the order of $g \in G$ is the smallest k s.t.

$$g^k = e.$$

E.g. in $\mathbb{F}_{13}^{\times}$, $\operatorname{ord}(g) = 12 \iff \theta$ is a primitive roots.

② and ⑦ are interesting ← use discrete log to solve some equations.

2 is a primitive root in $\mathbb{F}_{11}$.

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

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

$I(x) = k$ s.t. $2^k = x$.

Turns mult. into addition

2-(2)(c) — $4x^2 \equiv 9 \mod 11$.

$$I(4x^2) = I(9) \text{ in } \mathbb{Z}/10\mathbb{Z}$$

$$I(4) + I(x^2) = I(9) \text{ in } \mathbb{Z}/10\mathbb{Z}$$

$$2\,I(x) = I(9) - I(4) \text{ in } \mathbb{Z}/10\mathbb{Z}.$$

- solve for $I(x)$

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

To do this need discrete log table,

need to write out

a	0	1	2	3	4	5	6	7	8	9
$2^a \bmod 11$	1	2	4	8	5	10	9	7	3	6

$\mathbb{F}_{11}^{\times} \ni x$	1	2	3	4	5	6	7	8	9	10
$\mathbb{Z}/10\mathbb{Z} \ni I(x)$	0	1	8	2	4	9	7	3	6	5

$$2^a \equiv 2^b \mod 11$$

if $a \equiv b \mod 10$

$2 \in \mathbb{F}_{11}^{\times} \leftarrow$ 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 $\mathbb{F}_{11}^{\times}$

by Lagrange because

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

Made with Ziteboard