Lecture 18: Modular exponentiation and division

Last time:

- Let \([a] + [b] := [a + b]\). Then \(+\) is well-defined
- Let \([a] \cdot [b] := [a \cdot b]\). Then \(\cdot\) is well-defined

Example: What is \([2059482] \cdot [31756]\) (working mod 5)?

\[
\begin{align*}
\end{align*}
\]
Modular exponentiation

Last time:

- Let \([a] + [b] := [a + b]\). Then + is well-defined
- Let \([a] \cdot [b] := [a \cdot b]\). Then \(\cdot\) is well-defined

**Question:** How would you define \([a]^{[b]}\)? Check whether it’s well-defined. Consider \([2]^{[3]} \pmod{5}\).

A. Making progress
B. Done: well-defined
C. Done: not well-defined
D. I have a question
E. I’m stuck
Units and division

Question: How many units does \( \mathbb{Z} \) have?

1. 0
2. 1
3. 2
4. infinitely many
5. unsure/what's a unit?

\[
\begin{align*}
(1,1) & = 1. \\
1 & = 1^{-1}.
\end{align*}
\]

\(-1\) is a unit
\((-1).(-1) = 1\)
\((-1)^{-1} = -1\)

Only units of \( \mathbb{Z} \) for any other \( a \in \mathbb{Z} \),
\( \frac{1}{a} \notin \mathbb{Z} \).

\[
\begin{align*}
\left( \frac{1}{2} \right) \cdot 2 & = 5 \cdot \frac{1}{2} \\
\frac{1}{2} & = \text{the} \ x < \frac{1}{2}
\end{align*}
\]

\[
\frac{2}{3} \text{ is the multiplicative inverse of } 2.
\]

\[
\left( \frac{3}{2} \right)^{-1} = \left( \frac{2}{3} \right)
\]

\[
\text{Denoted, unless } p \neq 0.
\]

Note: units of \( \mathbb{Q} \) (rationals) are:

- everything but 0.

\[
\frac{p}{q} \text{ is defined, unless } p = 0.
\]

Def.: \( y \) is a multiplicative inverse of \( x \)
if \( x \cdot y = 1 \) we would write \( y = x^{-1} \)

Def.: A unit of a set \( X \) is an element \( x \in X \) with an inverse \( y \in X \)
Units of $\mathbb{Z}_m$

Definitions/notation:

- $\mathbb{Z}_m^*$ is the set of units of $\mathbb{Z}_m$.
- The *totient of $m$,* (written $\varphi(m)$) is the number of units of $\mathbb{Z}_m$.
- $\varphi$ is sometimes called "Euler's phi function".
- Representatives of units of $m$ are sometimes called *totatives of $m$.*

\[
\begin{align*}
\mathbb{Z}_5^* &= \{ [1], [2], [3], [4] \} \\
\varphi(5) &= 4
\end{align*}
\]

If

\[
\begin{align*}
[12] &= [23].
\end{align*}
\]
Example: \( \sqrt{\text{gcd}(1,5)} = 1 \), \( \sqrt{\text{gcd}(3,5)} = 1 \), \( \sqrt{\text{gcd}(2,5)} = 1 \), \( \sqrt{\text{gcd}(4,5)} = 5 \)

Units of \( \mathbb{Z}_m \)

How many units are in \( \mathbb{Z}_m \)? What are they?

**Claim:** \([a]_m\) is a unit of \( \mathbb{Z}_m \) if and only if \( \text{gcd}(a, m) = 1 \).

**Proof:** Suppose \( \text{gcd}(a, m) = 1 \). We will show \([a]_m\) is a unit. The other direction is left as an exercise.

If \( \text{gcd}(a, m) = 1 \), then we can write

\[
\text{gcd}(a, m) = 1 = s \cdot a + tm
\]

for some \( s \neq 0 \).

(Bézout coefficients)

 \((\text{mod } m)\) we have

\[
\begin{align*}
[a] & = [sa + tm] \\
& = [s][a] + [tm] \\
& = [s][a] + [0] \\
& = [s][a] + [0] \\
& = [s][a]
\end{align*}
\]

So \([s] = [a]^{-1}\) \(\text{mod } m\).

So \([a]_m\) is a unit \(\text{mod } m\).
Finding $\varphi(m)$

- $[a]_m$ is a unit of $\mathbb{Z}_m$ if and only if $\gcd(a, m) = 1$
- $\gcd(a, m) = 1$ means $a$ and $m$ are relatively prime: they share no common factors (other than 1).
- $\varphi(m)$ is the number of units of $\mathbb{Z}_m$

**Question:** What are the units of $\mathbb{Z}_p$ if $p$ is prime? What is $\varphi(p)$?

A: I know! I have an idea.

B: unsure.

$\mathbb{Z}_p = \{[1], [2], [3], \ldots, [p-1]\}$

all units: $\gcd(a, p) = 1$ since $p$ prime.

$p-1$ units, $\varphi(p) = p-1$. 

$p - 1$ units, $\varphi(p) = p - 1$. 
Finding $\varphi(m)$

- $[a]_m$ is a unit of $\mathbb{Z}_m$ if and only if $\gcd(a, m) = 1$
- $\gcd(a, m) = 1$ means $a$ and $m$ are relatively prime: they share no common factors (other than 1).
- $\varphi(m)$ is the number of units of $\mathbb{Z}_m$

**Question:** What are the units of $\mathbb{Z}_{pq}$ if $p$ and $q$ are different primes? What is $\varphi(pq)$?

*(next time)*