Lecture 18: Modular exponentiation

So far:

- We can add, subtract, multiply and (sometimes) divide modular numbers.
- All operations well-defined
- Operations behave "like" corresponding operations on regular numbers

New implementation of familiar interface:

- Can solve equations
- Can construct higher-level objects out of modular numbers (e.g. polynomials, vectors and matrices, even geometry)

Modular numbers are useful:

- Questions about divisibility ($m \mid a$ means $[a]_m = [0]_m$)
- "Summarizing" data (checksums, hashes)
- Performing operations (encryption)

Today: exponentiation, logs, and kth roots.

A bit more practice with units/finding $\varphi(m)$:

Last time: if p is prime, $\varphi(p) = p - 1$ (recall $\varphi(p)$ is number of units)

Proof sketch: List $\mathbb{Z}_p$, cross out non-units (only [0]), count what's left.

Question: If p, q different primes, what is $\varphi(pq)$?

Proof sketch: List $\mathbb{Z}_{pq}$, cross out non-units, count what's left

$$\mathbb{Z}_{pq} = \left\{ \begin{array}{llll} [0], & [1], & [2], & \dots & [p-1] \\ [p], & [p+1], & [p+2], & \dots & [2p-1] \\ [2p], & [2p+1], & [2p+2] & \dots & [3p-1] \\ \vdots & \vdots & & \ddots & \\ [(q-1)p], & [(q-1)p+1], & \dots & \dots & [qp-1] \end{array} \right\}$$

A bit more practice with units/finding $\varphi(m)$:

Last time: if p is prime, $\varphi(p) = p - 1$ (recall $\varphi(p)$ is number of units)

Proof sketch: List $\mathbb{Z}_p$, cross out non-units (only [0]), count what's left.

Question: If p, q different primes, what is $\varphi(pq)$?

Fact: $[a]_{pq}$ is a unit iff no factors in common w/ pq

Proof sketch: List $\mathbb{Z}_{pq}$, cross out non-units, count what's left

$$\mathbb{Z}_{pq} = \left\{ \begin{array}{llll} [0], & [1], & [2], & \dots \quad [p-1] \\ [p], & [p+1], & [p+2], & \dots \quad [2p-1] \\ [2p], & [2p+1], & [2p+2] & \dots \quad [3p-1] \\ \vdots & \vdots & & \ddots \\ [(q-1)p], & [(q-1)p+1], & \dots & \dots \quad [qp-1] \end{array} \right\}$$

What are the non-units?

A. progress B. I have some C. I have a question D. I'm stuck

non-units: q multiples of p.
p multiples of q.
(double counted 0)

p, q are prime: everything else is a unit.

Total # units: pq elts
$-q$ mults of p
$-p$ " " q
$+1$ (double counted 0)

$$\varphi(pq) = pq - q - p + 1$$
$$= (p-1)(q-1). \quad \text{[algebra]}$$

Euler's theorem

Claim (Euler's theorem): If $[a]_m$ is a unit, then $[a]_m^{[b]_{\varphi(m)}} := [a^b]_m$ is well-defined

$\varphi(5) = 4$

$[2^8] = [2]_5^{[8]_{\varphi(5)}=4} \pmod 5$

$= [2]_5^{[0]} = [2^0]_5 = [1]$

$[2^8] = [256]_5 = [1]$ ✓

Euler's theorem

Claim (Euler's theorem): If $[a]_m$ is a unit, then $[a]_m^{[b]_{\varphi(m)}} := [a^b]_m$ is well-defined

Proof: We'll use the following fact (proved on next slide):

- Claim (Euler's theorem v2): If $[a]_m$ is a unit, then $[a]_m^{\varphi(m)} = [1]$

$[a]^n = [a][a][a]\cdots[a]$ (n times.)

Choose an arbitrary unit $[a]_m = [a']_m$ and $[b]_{\varphi(m)} = [b']_{\varphi(m)}$.

- since multiplication is well defined, we have $[a^n] = [a'^n]$ for any n.
- since $[b]_{\varphi(m)} = [b']_{\varphi(m)}$ we have $b = b' + k\varphi(m)$ for some k.

We want to show $[a^b]_m = [a'^{b'}]_m$. We have:

$$
\begin{aligned}
[a^b] &= [a'^b] && \text{multiplication well defined} \\
&= [a'^{b'+k\varphi(m)}] && \text{Since } b = b' + km \\
&= [a'^{b'}\, a'^{k\varphi(m)}] && \text{Algebra} \\
&= [a'^{b'}][a'^{\varphi(m)}]^k && \text{Definition} \\
&= [a'^{b'}][1]^k = [a'^{b'}] && \text{Euler's v2}
\end{aligned}
$$

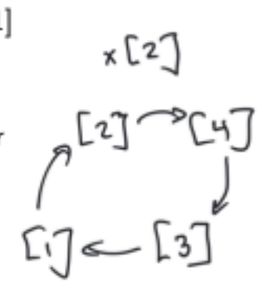
$[a^{\varphi(m)k}] = [(a^{\varphi(m)})^k]$

Euler's theorem version 2:

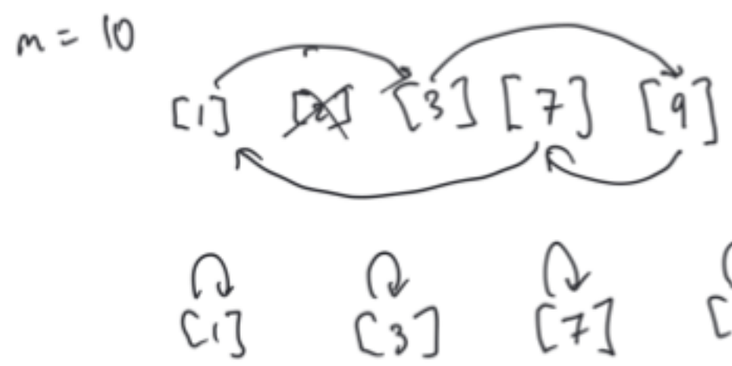
Claim (also Euler's theorem): If $[a]_m$ is a unit, then $[a]_m^{\varphi(m)} = [1]$

Exercise to understand proof:

- Pick m (e.g. $m = 5, 7, 10, 12, 15$) different from your neighbor
- List $\mathbb{Z}_m^*$
- Pick $[a]_m \in \mathbb{Z}_m^*$
- Draw an edge from each unit $[b]$ to $[a][b]$.
- Compare your picture to neighbor's; what are the patterns?



A. progress B. I've got a picture C. I have a question D. I'm stuck



insights / patterns: units will break up into loops, all loops same size (for a given a & m).

General proof: choose arb. $[a]_m$ a unit.
Consider $\mathbb{Z}_m^*$, draw a picture of multiplication by $[a]$.

all units. $\{$ $[1] \to [a] \to [a^2] \to [a^3] \to \cdots$
$[b] \to [ba] \to [ba^2] \to \cdots$

Can't happen:

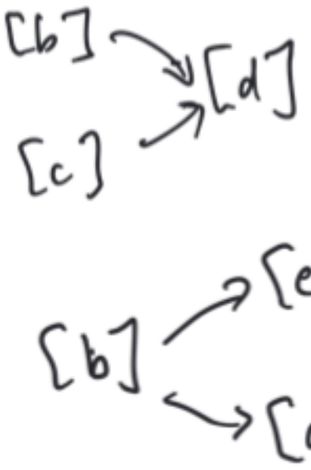
unit $\to$ non-unit.

$[b]$ $[ab]$ has inverse $[a]^{-1}[b]^{-1}$.

$[b]$ unit s. $[b]^{-1}$ exists
$[a]$ unit so $[a]^{-1}$ exists

$[a][b][a]^{-1}[b]^{-1} = [1]$.

Can't happen:



$[1] \to [a] \to [a^2] \to \cdots$ (forever)