# CIS 3362 10/13/25

## Fast Modular Exponentiation

Fermets Thm if $\gcd(a,p)=1$, $p \in$ Prime
$a, p \in \mathbb{Z}^+$, then $a^{p-1} \equiv 1 \pmod{p}$

Eder's Thm $a, n \in \mathbb{Z}^+$ if $\gcd(a,n)=1$, then
$a^{\phi(n)} \equiv 1 \pmod{n}$

Fundament Necessary task:
Given base b, exp e, mod MOD
Calculate the remainder when $b^e$ is divided by MOD.

exp, e, could be very large

DEFAULT CODE:

```
ans = 1
for (i=0; i<e; i++)
    ans = (ans * b) o/o MOD;
```

→ $< MOD^2$ (limits time for each mult)

Run-time $O(e *$ time of mult/mod$)$

↑ could be large $10^{100}$ or more!

$b^e$ and e is even, $b^e = b^{e/2} \times b^{e/2}$

$2^{12} = (2^6) \times (2^6)$

$b^e \bmod MOD$ is same as

$$\left(\left(b^{e/2} \bmod MOD\right) \times \left(b^{e/2} \bmod MOD\right)\right) \bmod MOD$$

SAME  mod ≠ 1

```
mymodpow(int b, int e, int mod) {
    if (e==0) return 1;
    if (e%2==0) {
        int tmp=mymodpow(b, e/2, mod);
        return (tmp*tmp)%mod;
    }
    return (b*mymodpow(b,e-1,mod))%mod;
}
```

$b^e = b^{e-1} \times b^1$

$e \to e-1 \to \frac{e-1}{2} \to \frac{e-1}{2}-1 \to \frac{\frac{e-1}{2}-1}{2}$

every 2 steps guaranteed to divide exponent by 2.

# rec calls $\leq 2*k$, where $\frac{e}{2^k} = 1$  $2^k = e$

$k = \log_2 e$ ↑ exponent!

# steps $\leq 2 * \log_2$ exponent

if $e = 10^{100}$  # steps $\sim 600 = 6 \times 10^2$

Python

import math

pow(b, e, m) returns

$b^e \bmod m$ efficiently!

(b**e)%m too slow!

↳ first very big slow!

Java

modPow uses BigInteger

import java.math.*;

# Miller-Rabin Prime Test

If $p$ is prime for all $a$, $\gcd(a,p)=1$,

$a^{p-1} \equiv 1 \pmod{p}$ Fermat's Thm

If composite, it's "usually not true"

## Simple Fermat Prime Test (n)

1. Pick random $a \in [1, n-2]$.
2. Calculate $a^{n-1} \bmod n$
3. If ans $\neq 1$ return composite
   else return "is probably prime"

## Easy Improvement

Repeat Simple Fermat Test 50 times with different values (randomly chosen) of $a$.

if ANY answer composite, return this and stop.

if all 50 give ans "is prob prime" ~~ans~~ return "IS PROBABLY PRIME"

* SPECIAL COMPOSITE #S CALLED CARMICHAEL #S, such that for all $a$, $\gcd(a,n)=1$, $a^{n-1} \equiv 1 \pmod{n}$

if you ever pick $a$, such that $\gcd(a, n) \neq 1$, immediate answer comp.

↳ $a^{any} \not\equiv 1 \mod n$