

Fast Modular Exponentiation

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

Euler'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) % MOD; // (limits time)
                        // for each
                        // mult
```

Run-time $O(e \times \text{time of mult(mod)})$

↑ could be large 10^{100} or more!

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

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

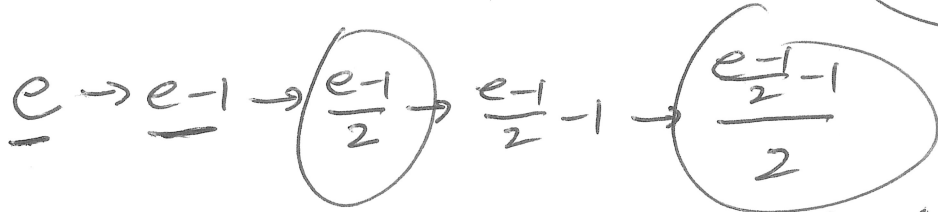
$b^e \pmod{\text{MOD}}$ is same as

$$\left(\underbrace{(b^{e/2} \pmod{\text{MOD}})} \times \underbrace{(b^{e/2} \pmod{\text{MOD}})} \right) \pmod{\text{MOD}}$$

SAME $\pmod{\neq 1}$

```
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;  
}
```

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



Every 2 steps guaranteed to divide exponent by 2.

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

steps $\leq 2 * \log_2 \text{exponent}$

$k = \log_{2^{\uparrow}} e$
exponent!

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

Python

```
import math
```

`pow(b, e, m)` returns

$b^e \pmod m$ 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 , $\gcd(a, p) = 1$,

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

If composite, it's "usually not true"

Simple Fermat Prime Test (n)

1. Pick random $a \in [2, n-1]$.
2. Calculate $a^{n-1} \pmod{n}$
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
 $\gcd(a, n) \neq 1$, ~~imp~~ immediate answer comp.

$$\hookrightarrow a^{\text{any}} \not\equiv 1 \pmod n$$