

① Fast Mod Exp

② Factoring

```
# Calc  $\text{base}^{\text{exp}} \% \text{mod}$ 
def modexp(base, exp, mod):
    ans = 1
    for i in range(exp):
        ans = (ans * base) % mod
    return ans
```

REG EXPO

If $\text{exp} = 10^{35}$
 then this will
 take forever.

if exp is even

just calculate $\text{tmp} = \text{base}^{\text{exp}/2} \% \text{mod}$
 return $(\text{tmp} * \text{tmp}) \% \text{mod}$

$$17^{100} \Rightarrow (17^{50})^2$$

Run time $\log_2 \text{exp}$ SLOW FACTORING

BRUTE FORCE - TRY EACH #

```
for (i = 2; i <= n; i++)
    if (n % i == 0)
        WHOO!
```

RUNTIME
 $\sqrt{n}$

10/25/19 @

FERMAT FACTORING

assume n is odd product of 2 primes. $n = pq$

$$n = 13 \times 17$$

↑ ↑

$$x^2 - y^2 = (x+y)(x-y)$$

~~$$(15+2)^2 - (15-2)^2$$~~

$$15^2 - 2^2 = (15+2)(15-2)$$

$$x^2 - y^2 = n$$

$$15^2 - y^2 = 221$$

$$225 - 221 = y^2$$

$$4 = y^2$$

$$2 = y$$

$$y^2 = x^2 - n$$

$$n = 221$$

thus $x > \sqrt{221}$, $x \geq 15$
 $x > \sqrt{n}$

$$\sqrt{2923} \approx 54.06$$

$$x \geq 55$$

x	$x^2 - n$	$n = 2923$	square?
55	102		x
56	213		x
57	326		x
58	441		✓ 21^2

$$2923 = 58^2 - 21^2$$

$$= (58+21)(58-21)$$

$$= \boxed{79 \times 37}$$

LOOK UP POLLARD-RHO
 FACTORING (Clt & NOTES)