Conjecture A:

$4 = 2+2$
$6 = 3+3$
$8 = 3+5$
$10 = 3+7 = 5+5$
$12 = 7+5$
$14 = 7+7 = 11+3$

testConjectureA[n] — returns True if n is the sum of two primes, False otherwise

Prime[i]

MODULAR ARITHMETIC

$23 \pmod 7$ means the remainder when you divide 23 by 7.

$23 \equiv 2 \pmod 7$

$\equiv$ is congruent to

example: $134 \equiv 4 \pmod 5$

Our Goal: compute $b^e \pmod m$ when b, e, m are huge — say, 30 digits each

b — base
e — exponent
m — modulus

If b, e have 30 digits (10^{30}) each, how big is b^e?

b^2 — about 60 digits
b^3 — about 90 digits
b^4 — about 120 digits
⋮
b^e — about 30e digits
$\sim 10^{31}$ digits

500 × 500 = 250000

computer RAM: 8 GB
~ 8 billion bytes
$\sim 10^{10}$ bytes

Way too big to store in memory.

REPEATED SQUARING

example: 3^{32}

$3^2 = 9$

$3^4 = (3^2)^2 = 9^2 = 81$

$3^8 = 81^2 = 6561$

$3^{16} = 6561^2 = 43,046,721$

$3^{32} = 43046721^2 = 1,853,020,188,851,841$

$3^{32} \pmod 7$

$3^2 = 9 \equiv 2 \pmod 7$

$3^4 \equiv 2^2 = 4 \pmod 7$

$3^8 \equiv 4^2 = 16 \equiv 2 \pmod 7$

$3^{16} \equiv 2^2 = 4 \pmod 7$

$3^{32} \equiv 4^2 = 16 \equiv 2 \pmod 7$

$$3^{32} \equiv 2 \pmod 7$$

How would I compute $3^{26} \pmod 7$?

$$3^{26} = 3^{16+8+2} = 3^{16} \cdot 3^8 \cdot 3^2 \equiv 4 \cdot 2 \cdot 2 = 16 \equiv 2 \pmod 7$$

Binary representation of 26:

$$26_{ten} = 1\,1\,0\,1\,0_{two}$$

tens, ones; sixteens, eights, fours, twos, ones

$26 \pmod 2 \equiv 0$

$\frac{26}{2} = 13 \pmod 2 \equiv 1$

$\lfloor \frac{13}{2} \rfloor = 6 \pmod 2 \equiv 0$

$\frac{6}{2} = 3 \pmod 2 \equiv 1$

$\lfloor \frac{3}{2} \rfloor = 1 \pmod 2 = 1$

$\lfloor \frac{1}{2} \rfloor = 0$ DONE.