CS 135

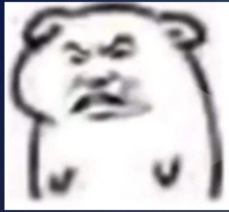
Lab

7

Problem 1

Find the remainder when 7^{2001} is divided by 5.

My calculator tryna solve this:



Problem 1

Given the lemma and use of Fermat's Little Theorem

$a \equiv b \pmod{n}$ and $c \equiv d \pmod{n} \rightarrow ac \equiv bd \pmod{n}$

$7^4 \equiv 1 \pmod{5}$ and $7^4 \equiv 1 \pmod{5} \rightarrow 7^8 \equiv 1 \pmod{5}$

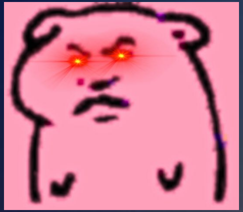
$7^8 \equiv 1 \pmod{5}$ and $7^4 \equiv 1 \pmod{5} \rightarrow 7^{12} \equiv 1 \pmod{5}$ and so on...

Until $7^{2000} \equiv 1 \pmod{5}$

And since $7 \equiv 2 \pmod{5}$ our final answer is $\mathbf{7^{2001} \equiv 2 \pmod{5}}$

Problem 2

What is $4^{100,000} \pmod{19}$ equal to?



Problem 2

$100{,}000 = 5555 * 18 + 10$

$4^{100{,}000} \equiv (4^{18})^{5555} * 4^{10} \pmod{19}$

$\equiv 1^{5555} * 4^{10} \pmod{19}$

$\equiv 4^{8} * 4^{2} \pmod{19}$

$\equiv 5 * -3 \pmod{19}$

$\equiv 4 \pmod{19}$

*want 18 to have FLT work

*use successive squaring to find these numbers mod 19

Problem 3

$x \equiv 3 \pmod{5}$

$x \equiv 1 \pmod{7}$

$x \equiv 6 \pmod{8}$

Find x.

Problem 3

Step 1: Calculate m = 5*7*8 = 280

Step 2: Calculate M_1=56, M_2=40, M_3=35

Step 3: Calculate $y_1 = M_1^{-1} \equiv 1 \pmod 5$

$y_2 = M_2^{-1} \equiv 3 \pmod 7$

$y_3 = M_3^{-1} \equiv 3 \pmod 8$

Step 4: Calculate X = 3*1*56 + 1*3*40 + 6*3*35

= 918 ≡ **78** (mod 280)

Racket Time!