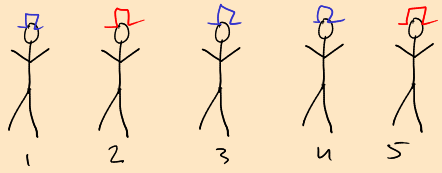
100 prisoners



3 5 1 4 2

There are 100 prisoners. They can all talk to each other and make any plans until I give them hats. Tonight I will put either a red or blue hat on each of their heads, and after that they will not be able to communicate with each other in any way. Everyone can see everyone else's hat and no one can see their own hat.

The next morning, I will call on the prisoners in a random order and ask them to guess the color of their hat. If their guess is correct, then they get to live, otherwise they die. Every prisoner is able to hear the guess as it is shouted aloud.

How many prisoners can definitely make it alive?

What if there are three colors?

What if there are k colors and n prisoners?

Bonus
3 colors ?

sagnick@

$3 \equiv 10 \pmod 7$

$3 \cdot 3^{-1} \equiv 10 \cdot 3^{-1} \equiv 10 \cdot 5 \equiv 50 \equiv 1 \pmod 7$

$3/3 \equiv 1 \neq 10/3 =$

$3 \cdot [3^{-1}] \equiv 1 \pmod 7$ $\quad 3 \cdot 5 = 15 = 2 \cdot 7 + 1$

$3x \equiv 1 \pmod 7$ $\quad 3 \cdot 5 \equiv 1 \pmod 7$

$x \equiv 3^{-1}$ $\quad 3^{-1} \pmod 7 \equiv 5 \pmod 7$

$3x \equiv 1 \pmod 7$

$3 \cdot 5 \equiv 15 \equiv 1 \pmod 7$

Extended GCD algo

$\frac{3}{5} = 3 \cdot 5^{-1}$

$-1 \cdot -1 \equiv 1 \pmod 5$

$4 \equiv -1 \pmod 5$

$(-1)^{-1} \equiv -1 \pmod 5$

$4^{-1} \pmod 5$

$4 \cdot 4 \equiv 16 \equiv 1 \pmod 5$

$4^{-1} \equiv 4 \pmod 5$

$2^{-1} \pmod 5$

$3 \cdot 2 \equiv 6 \equiv 1 \pmod 5$

$2^{-1} \equiv 3 \pmod 5$

"equivalent"
"congruent"

$x \equiv 5 \pmod 7$

$x = k \cdot 7 + 5, \quad k \in \mathbb{Z}$

$3 \equiv 7 \equiv -1 \pmod 4$

$3 = 1 \cdot 4 - 1$

$3^5 \equiv 3 \times 3 \times 3 \times 3 \times 3 \pmod 5$

$\equiv 243 \equiv 3 \pmod 5$

$3^{-5} \equiv (3^{-1})^5 \equiv 2^5 \pmod 5$

$\equiv 2 \pmod 5$

$1 = 1 \cdot 4 - 3$

$7 = 2 \cdot 4 - 1$

$5 \neq 9$

$5 \neq 1$

$5 \equiv 1 \pmod 4$

$9 \equiv 5 \pmod 4$

$5 + 9 \equiv 1 + 5 \equiv 1 + 1 \equiv 2 \pmod 4$

$5 = 1 \cdot 4 + 1$

$1 = 0 \cdot 4 + 1$

$9 = 2 \cdot 4 + 1$

$7 = 1 \cdot 4 + 3$

$5 + 9 = 14$

$(1 \cdot 4 + 1) + (2 \cdot 4 + 1)$

$= 3 \cdot 4 + 2$

$3 \times 1 = 3$

$5 \times 7 = 35$

$(1 \cdot 4 + 1)(1 \cdot 4 + 3)$

$= 1 \cdot 16 + 3 \cdot 4 + 1 \cdot 4 + 3 = 8 \cdot 4 + 3$

CS 70 Discrete Mathematics and Probability Theory
Fall 2021 DIS 3B

1 Party Tricks

You are at a party celebrating your completion of the CS 70 midterm. Show off your modular arithmetic skills and impress your friends by quickly figuring out the last digit(s) of each of the following numbers:

(a) Find the last digit of 11^{3142}.

(b) Find the last digit of 9^{9999}.

$3^4 \equiv 1 \pmod{10}$

$11^{56} \equiv 6 \pmod{10}$

$11^{3142} \equiv 1^{3142} \pmod{10}$

$11 \times 11 \times 11 \cdots \equiv 1 \times 1 \times 1 \cdots \pmod{10}$

9^{9999}

$9^{9999} \equiv -1 \pmod{10}$

$\equiv -1 \pmod{10}$

$\equiv 9 \pmod{10}$

$0, \ldots, (10-1)$

$9^2 \equiv 81 \equiv 1 \pmod{10}$

$9^{9999} = (9^2)^{4999} \times 9 = 1^{4999} \times 9 \equiv 9 \pmod{10}$

2 Modular Potpourri

$a^{(x^y)} \neq (a^x)^y = a^{x \cdot y}$

(a) Evaluate $4^{96} \pmod 5$.

$4^{96} \pmod 5$

$4 \equiv -1 \pmod 5$

$4^{96} \equiv 4 \times 4 \times \cdots \times 4 \equiv \underbrace{(-1) \times (-1) \times \cdots \times (-1)}_{96 \text{ times}} \equiv 1 \pmod 5$

$4 \equiv 4 \pmod 5$

$16 \equiv 4^2 \equiv 1 \pmod 5$

$4^{96} \equiv (4^2)^{48} \equiv 1^{48} \pmod 5$

(b) Prove or Disprove: There exists some $x \in \mathbb{Z}$ such that $x \equiv 3 \pmod{16}$ and $x \equiv 4 \pmod 6$.

$x \equiv 3 \pmod{16} \Rightarrow x = k \cdot 16 + 3 = 8k \cdot 2 + 2 + 1 = (8k+1) \cdot 2 + 1 \Rightarrow x \equiv 1 \pmod 2$

$3 = 1 \cdot 2 + 1$

$x \equiv 4 \pmod 6 \Rightarrow x = \ell \cdot 6 + 4 = (3\ell + 2) \cdot 2 + 0 \Rightarrow x \equiv 0 \pmod 2$

$0 \not\equiv 1 \pmod 2$

contradiction!

$16k + 3 = 6\ell + 4$

$\Rightarrow \underbrace{16k - 6\ell}_{\text{even}} = \underbrace{1}_{\text{odd}}$

(c) Prove or Disprove: $2x \equiv 4 \pmod{12} \iff x \equiv 2 \pmod{12}$.

$\Rightarrow$

$\Leftarrow$

3 Fibonacci GCD

The Fibonacci sequence is given by $F_n = F_{n-1} + F_{n-2}$, where $F_0 = 0$ and $F_1 = 1$. Prove that, for all $n \geq 1$, $\gcd(F_n, F_{n-1}) = 1$.

4 Modular Inverses

Recall the definition of inverses from lecture: let $a, m \in \mathbb{Z}$ and $m > 0$; if $x \in \mathbb{Z}$ satisfies $ax \equiv 1 \pmod{m}$, then we say x is an **inverse of** a **modulo** m.

Now, we will investigate the existence and uniqueness of inverses.

(a) Is 3 an inverse of 5 modulo 10?

(b) Is 3 an inverse of 5 modulo 14?

(c) Is each $3 + 14n$ where $n \in \mathbb{Z}$ an inverse of 5 modulo 14?

(d) Does 4 have inverse modulo 8?

(e) Suppose $x, x' \in \mathbb{Z}$ are both inverses of a modulo m. Is it possible that $x \not\equiv x' \pmod{m}$?