Fall Break Donut Session

Theory Club officers

October 14, 2022

1 Number Theory

1.1 An Inductive Proof of Fermat's Little Theorem

As a refresher, Fermat's Little Theorem (FLT) states that for any prime p and integer a, $a^p \equiv a \pmod{p}$.

In an proof by induction, we seek to show a statement is true for all integers k. We do this by first showing that the statement is true for $k = 1$ as a base case. We then show that when assuming a statement is true for k, it must be true for $k + 1$.

1. What is the base case for FLT and why is it true?
2. To help with the inductive step (part 3), it is helpful to first show that p divides $\binom{p}{n}$ when $1 \leq n \leq p - 1$. Prove this.
3. Now assume, $k^p \equiv k \pmod{p}$ for some integer k and prime p.
   Show $(k + 1)^p \equiv k + 1 \pmod{p}$

   Hint: Try applying the Binomial Theorem to expand the left side of the congruence

1.2 Bezout's Lemma and Multiplicative Inverses

For integers a and b, let $d = \gcd(a, b)$. Bezout's Lemma states that there exists integers x and y such that $ax + by = d$.

Bezout's Lemma is helpful in demonstrating a variety of results in number theory, including the existence of multiplicative inverses. Let's try proving it!

1. Let us first fix the values of a and b. Consider the following set:

   $S = \{n > 0 : n = ax + by \text{ for some } x, y \in \mathbb{Z}\}$

   To show that S has a smallest element, first prove that S is non-empty.

2. Let s_0 represent the smallest element of S. Show that d divides s_0.

3. Show that s_0 divides a.

   Hint: By the Division Algorithm, $a = s_0q + r$ for a quotient q and remainder r where $r < s_0$. Try writing r as a linear combination of a and b. Why would this show that $r = 0$?

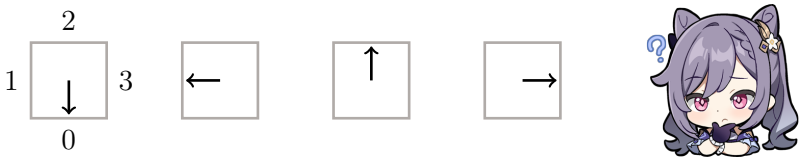
4. The same method from part 3 can be used to show s_0 divides b. Why does this imply that $s_0 \leq d$?

5. Apply the results from parts 2 and 4 to show that $s_0 = d$. Why does this prove Bezout's Lemma?

6. Use Bezout's Lemma to prove that if a is coprime to n, then a must have a multiplicative inverse under mod n. In other words, show that there exists a^{-1} such that $aa^{-1} \equiv 1 \pmod{n}$.

1.3 Number theory meets linear algebra in Genshin Impact.

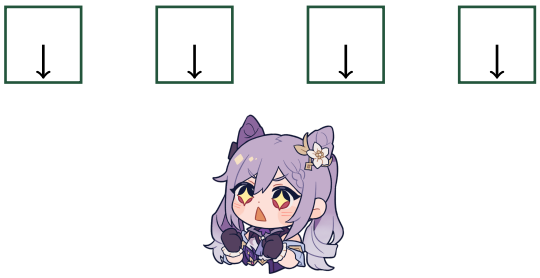
Suppose there are four blocks arranged in a straight line. Each block has an orientation that is fixed to the four cardinal directions. When the player hits a block, it and its adjacent neighbors rotate 90 degrees clockwise. The situation is pictured below.



In order to denote the state, we arbitrarily number the orientations and then read the orientations of the blocks from left to right. For example, the state pictured above corresponds to a representation of $(0, 1, 2, 3)$.

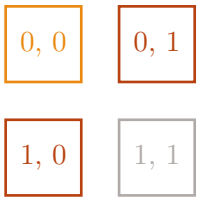
If, for example, the player hit the second block from the left, this would change to

The state is now $(1, 2, 3, 3)$. The goal is to align all the blocks in the least number of moves, that is, to end on the state of $(0, 0, 0, 0)$.



Give a closed-form expression for the blocks to hit given the starting state.

What is the solution to the initial state of $(0, 1, 2, 3)$ depicted above? Do the same but if the blocks are in a *torus*, that is, we also consider the first and last block adjacent. Do the same, but if the blocks are arranged in a 2×2 grid instead of a 1×4 line,



where blocks are considered adjacent if their indices in the grid are within 1 in ℓ_1 norm, that is, block (i_1, j_1) is adjacent to block (i_2, j_2) if $|i_1 - i_2| + |j_1 - j_2| \leq 1$. Can you generalize to a grid of $m \times n$? To hypercubes? To different notions of adjacency?

1.4 Möbius inversion.

1. We say a function is *arithmetic* if it is defined on the positive integers.

   Let f and g be two arithmetic functions. Define their *Dirichlet product* by

   $$(f \cdot g)(n) \coloneqq \sum_{d|n} f(d)g(n/d)$$

   where $\sum_{d|n}$ means summing over all integers d that divide n and let

   $$e(n) \coloneqq \begin{cases} 1 & n = 1 \\ 0 & n > 1 \end{cases}$$

   We say that g is the *Dirichlet inverse* of f if $f \cdot g = g \cdot f = e$. Show an arithmetic function f has an inverse if and only if $f(1) \neq 0$.

2. Define the *summatory function* F of an arithmetic function f as

   $$F(n) = \sum_{d|n} f(d)$$

   Let μ be the *Möbius function*, that is, the arithmetic function that satisfies

   $$f(n) = \sum_{d|n} F(d)\mu(n/d)$$

   for any arithmetic function f. Compute the Dirichlet inverse of μ.

   (*Hint: it is not necessary to get a closed form for μ!*)

3. Let $\phi(n)$ be defined as the arithmetic function that counts the number of positive numbers relatively prime to n, not exceeding n. We say two numbers are *relatively prime* if they do not share a common divisor, that is, m, n are relatively prime if and only if $\gcd(m, n) = 1$. The function $\phi(n)$ is known as *Euler's totient function.*

   The first 12 values of $\phi(n)$ are shown below.

n	1	2	3	4	5	6	7	8	9	10	11	12
$\phi(n)$	1	1	2	2	4	2	6	4	6	4	10	4

   Show that the summatory function $\Phi(n)$ of $\phi(n)$ is n, that is,

   $$\Phi(n) \coloneqq \sum_{d|n} \phi(d) = n$$

2 Probability

2.1 Worth a Gamble?

You're playing the following game: on a table is a pile of money, initially containing a single dollar. On every turn, you have two options. The first option is to take the money on the table, ending the game. The second option is to roll a die. If you roll a 6, all the money on the table disappears and the game ends. Otherwise, a dollar gets added to the pile of money on the table and the game continues. What's the optimal strategy and EV for this game?

2.2 Coins and a Grid

You're playing a game where you try to throw a coin of radius R onto a table lined with a grid where each cell is $D \times D$. The goal is to get as close to the middle of a grid cell as you can. Specifically, your payout in dollars is the distance from the coin to the grid – if the coin overlaps the grid, you get \$0. Assuming you aren't very good at this game, and you can guarantee your coin lands on the table and grid, but have no control over where in a cell it lands, what's your expected value from this game in terms of R and D?

2.3 Ho-kago Tea Time (HTT).

Flip an unbiased coin until you see the sequence `HTT` at any point.

For example, a series of coin flips might look like

`HTHHTHTHTT`

Here, it took 10 flips until the sequence was seen.

How many coins do you expect to flip until you see the sequence?

Is the answer different for the sequence `HTH`? `HHH`?

Give a closed-form expression for the number of flips until you see n heads in row.

Give an algorithm to compute the expected number of flips for any sequence.

Can you extend your algorithm to biased coins? Can you get a linear time algorithm?

3 Rowhammer

Rowhammer is a phenomenon affecting DRAM cells. DRAM is organized in terms of rows, and data is accessed by *activating* rows. Rowhammer occurs when an *aggressor* row is activated enough so that bits in adjacent *victim* rows are flipped. We characterize DRAM modules by their Rowhammer threshold T_{RH}. To prevent Rowhammer, defenses must perform mitigations before a victim row is afflicted by T_{RH} activations from an aggressor row.

We discuss the functionality of PARA (CAL 2014). PARA mitigates Rowhammer by performing a reset on adjacent rows (which is non-destructive). On a row activation, PARA performs a Rowhammer mitigation on adjacent rows with probability p. Given

a Rowhammer threshold of T_{RH}, what should p be to avoid Rowhammer flips from occurring with probability $1 - \epsilon$?