Kelly's Workshop

Sophia Xu and Judy Li

November 21, 2024

1 Monday – Common Kitchen Problems

The Watermelon Problem: *What is the maximum amount of pieces we can cut a watermelon into, given only* 17 *slices? What about* n *slices?*

Conjectures (and questions) we considered:

- How can we minimize the number of pieces for n slices?
- To minimize slices, we minimize intersections (no intersections)
- To maximize slices, we maximize intersections

Other NOT as *interesting* things we considered:

- Do we need to cut through the watermelon?
- Do we need to make a straight linear/planar cut?
- Can we move the pieces before we cut them?

We decided that we must have straight cuts and preceded to begin with considering the 2D "pizza" case, 1D "licorice" case and the 0D "jolly rancher" case. We immediately conjectured the following formulas for the jolly rancher:

$$\binom{n}{0},$$

the licorice:

$$\binom{n}{1} + \binom{n}{0},$$

the pizza:

$$\binom{n}{2} + \binom{n}{1} + \binom{n}{0},$$

the watermelon:

$$\binom{n}{3} + \binom{n}{2} + \binom{n}{1} + \binom{n}{0},$$

and for the kth dimensional object where $k \in \mathbb{N}$:

$$\binom{n}{k} + \cdots + \binom{n}{3} + \binom{n}{2} + \binom{n}{1} + \binom{n}{0}.$$

From here, we worked to justify the formulas (specifically the watermelon one) with many different approaches. One approach is outlined as follows by Noah.

Proof. Whenever we cut a watermelon with a plane, the intersection of the plane and the watermelon is a circle. Each of the other planes will be a line which goes through the circle. If none of the lines are parallel (which can be achieved by placing the plane such that it is not parallel to the lines of intersection of any other two planes), then we know by the 2D pizza case that the lines divide the circle into

$$n + 1 + \binom{n}{2}$$

pieces. Thus, we have divided $n + 1 + \binom{n}{2}$ regions in half, so we have added $n + 1 + \binom{n}{2}$ regions to the watermelon. Then, we can show by induction on n that n slices can divide a watermelon into at most

$$1 + n + \binom{n}{2} + \binom{n}{3}$$

pieces. P.I.G.

Induction

Next, we discussed and defined mathematical induction. We noticed that usually textbooks begin induction examples with the sum of all natural numbers and discussed why this is BAD. We decided to start with another example:

Theorem 1 *We can tile any 2^n by 2^n square $\forall n \in \mathbb{N}$ with L-trominos and one 1 by 1 black tile.*

Proof.

Base case: n=0. Here, we have a single black tile.

Inductive hypothesis: It is possible to tile a 2^k by 2^k square with L-trominos and 1 black tile which can be anywhere.

Inductive step: We want to tile a 2^{k+1} by 2^{k+1} suare. We know that the black square can be anywhere-WLOG, assume it is in the top-left corner. We split the square into 4 quadrants and by the inductive assumption, we can tile that quadrant. For the other 3 quadrants, we place an L-tromino in the center-most corner like as shown below in Figure 1. We see that we can split the middle tromino into 3 squares. Now we

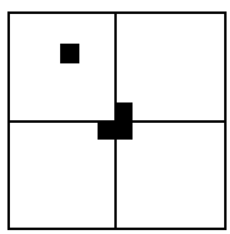

Figure 1: This is cute.

need to prove that we can tile a 2^k by 2^k square with a black square in the corner, however this is proven by the inductive hypothesis. Hence, we are done. P.I.G.

More things we thought about:

- The Tower of Hanoi problem (and a few variants).
- $2n$ people are standing in a field– all different distances apart. Prove that after they all shoot water guns at the person closest to them at the same time, one person is always dry.
- 17 = number of muscles in a horse's ear.
- 17 = number of syllables in a haiku = number of syllables one can say in one breath.

We ended with an activity sorting ourselves into groups (which allowed us to discover the STS conditions (to be later defined on Wednesday.))

2 Tuesday – A Review of Third Grade

We posed the question, 'Why does the principle of mathematical induction (PMI) work?' To answer this, we tried to explain what natural numbers are:
G. Peano's axioms for $\mathbb{N}$:

1. $0 \in \mathbb{N}$
2. Denote the successor of n by $S(n)$. If $x \in \mathbb{N}$, then $S(x) \in \mathbb{N}$
3. If $S(x) = S(y)$, then $x = y$
4. $\forall x \in \mathbb{N}$, $S(x) \neq 0$
5. If A is a set of natural numbers and $0 \in A, x \in A \Rightarrow S(x) \in A$, then $A = \mathbb{N}$

Principle of the least natural number: (PLNN, a.k.a. 'the Well Ordering Principle' in some far away land)
If $A \subset \mathbb{N}$ and A is not the empty set ϕ, then A has a least member.
We will later use PLNN to prove PMI, but PLNN can be used to prove many other theorems as well, e.g.,:

Theorem 2 *Every natural number greater than 1 can be factored into primes.*

We then delved into number theory.
Third Grade Theorem *If* $A, B \in \mathbb{Z}, A > 0, B \geq 0$, *then* $\exists Q, R \in \mathbb{Z}$ *such that* $B = AQ + R, 0 \leq R < A$
Euclidean Algorithm To find the g.c.d. of $A, B \in \mathbb{N}$, we carry out the Euclidean Algorithm:

$$\begin{aligned}
B &= AQ_1 + R_1, \quad 0 \leq R_1 < A \\
A &= R_1Q_2 + R_2, \quad 0 \leq R_2 < R_1 \\
R_1 &= R_2Q_3 + R_3, \quad 0 \leq R_3 < R_2 \\
&\vdots \\
R_{n-3} &= R_{n-2}Q_{n-1} + R_{n-1} \\
R_{n-2} &= R_{n-1}Q_n + 0
\end{aligned}$$

As $k|A, B \Rightarrow k|A, R_1 \Rightarrow k|R_1, R_2 \Rightarrow ..., \Rightarrow k|R_{n-2}, R_{n-1} \Rightarrow k|R_{n-1}, 0$,
We have

$$\begin{aligned}
g.c.d.(A, B) &= g.c.d.(R_{n-1}, 0) \\
&= R_{n-1}
\end{aligned}$$

3 Wednesday – Fundamentals and Functional relationships

3.1 Fundamental Theorem of Arithmetic (FTofA)

Theorem 3 *The prime factorization of* $N \in \mathbb{N}$: $N = p_1^{e_1} p_2^{e_2} \cdot\cdot p_k^{e_k}$, *where* p_j*'s are prime, is unique up to order.*

Proof. Assume for the sake of contradiction that the FTofA is false. Then we have

$$N = \prod_{j=1}^{k} p_j^{e_j} = \prod_{l=1}^{m} q_l^{f_l}.$$

The proof will be completed and proved on θ in class.
Useful Lemma

Theorem 4 *$\exists x, y \in \mathbb{Z}$ such that $(a, b) = ax + by$.*

Proof. Let
$$S_{a,b} := \{ax + by : x, y \in \mathbb{Z}\}.$$
If $d|a$ and $d|b$, then we have that $d|s$ for all $s \in S_{a,b}$. We know that $S_{a,b}$ contains positive members, so by PLNN, $S_{a,b}$ has a least positive member – call it $g \in S_{a,b}$. We know that there exists x_0 and y_0 such that

$$g = ax_0 + by_0$$

and there exists q, r such that
$$a = gq + r$$
where $q \in \mathbb{N}$ and $0 \leq r < g$. Now

$$r = a - gp = a - (ax_0 + by_0)q = a(1 - x_0q) + b(-y_0q) \in S_{a,b}.$$

So, $r \in S_{a,b}$ if r is positive, but $r < g$, so r cannot be positive and must be 0. This means $g|a$, and similarly $g|b$, so we have a contradiction.

3.2 Relations and Functions

A relation, $\lozenge$, is called a **STS relation** if:

1. Selfish: $A \lozenge A$
2. Transitive: $(A \lozenge B$ and $B \lozenge C) \Rightarrow A \lozenge C$
3. Symmetric: $A \lozenge B \Rightarrow B \lozenge A$

Examples include set membership in disjoint sets (”in the same set as”) and congruence of shapes in geometry.

4 θ – Introducing...

We began with the following theorem:

Theorem 5 *$\sqrt[n]{k}$ is rational iff k is an nth power.*

Proof. We assume for the sake of contradiction that $\sqrt[n]{k}$ is rational when k is not an nth power. We call this rational number $\frac{a}{b}$ for some $a, b \in \mathbb{Z}$. Hence, we have that

$$\sqrt[n]{k} = \left(\frac{a}{b}\right).$$

So,
$$k = \frac{a^n}{b^n},$$
which means that
$$kb^n = a^n.$$
By the Fundamental Theorem of Arithmetic, $kb^n = a^n$ have the same prime factorization, so they must both have an exponent of p^{rn} where p is a prime that divides a. By similar reasoning, b^n has an exponents of p^{sn} for some $r, s \in \mathbb{N}$. Hence, k must have all primes to the nth power.

Next, we discovered and proved a Theorem and a relating Corollary.

Theorem 6 *If $a|bc$ and $(a, b) = 1$, then $a|c$.*

Corollary: If p is a prime and $p|ab$, then $p|a$ or $p|b$.
Proof of Corollary.
If p does not divide a, then $(p, a) = 1$, so by the theorem, $p|b$.

Proof of Theorem:
By the Useful Lemma, $\exists x, y$ such that $ax + by = 1$. Thus we know that

$$acx + bcy = c.$$

We know that $a|acx$ and from the hypothesis, we know that $a|bcy$. Hence, $a|c$, as desired. P.I.G.

Then, we proved the Fundamental Theorem of Arithmetic which states that the prime factorization of a number must be unique. We changed topics to have a thoughtful discussion on the fundamental (which turned out to be the only) moves to transform a square and ended a nice long θ with a discussion on relations and functions.

5 Friday – ... the Transformers

5.1 Modular arithmetic: (Or Enfield calculations?)

We proved the following results:

1. $\exists y \in \mathbb{Z}$ such that $xy \equiv 1 \pmod{m}$ iff $(x, m) = 1$
2. $ax \equiv b \pmod{m}$,, where $a, b \in \mathbb{Z}$ has integer solutions for x iff $(a, m) = 1$

Wilson's Theorem (the theorem that was neither suggested nor proved by Wilson) $(n-1)! \equiv n-1 \pmod{n}$ *for all primes* n.
Sketch of Proof.
Consider $16! \equiv 16 \pmod 17$.
Each of the 14 components of 16! except 1 and 16 can be paired up with its own multiplicative inverse, so $(p-1)! = 16 \pmod 17$.
This is because 16 and 1 are the only two positive integers less than 17 which are their own multiplicative inverses, proven below:
If x is its own multiplicative inverse, then $x \cdot x \equiv 1 \pmod{p} \implies x^2 - 1 \equiv 0 \pmod{p}$.
Thus, $p \mid (x-1)(x+1) \implies p \mid x-1$ or $p \mid x+1$, i.e., $x \equiv 1, -1 \pmod{p}$.

5.2 Transformers:

What is a transformer? A transformer consists of a set S and operation $\circ : S \times S \to S$, such that:

1. Existence of 'do-nothing' element: $\exists i \in S \; \forall s \in S$ such that $i \circ s = s \circ i = s$
2. Existence of an inverse: $\forall s \in S, \exists t \in S$ s.t. $s \circ t = t \circ s = i$
3. Assosciativity: $\forall s, u, v \in S$, $(s \circ u) \circ v = s \circ (u \circ v)$.

$x \in S$ is **powerful** if $\forall y \in S$, $\exists n \in \mathbb{N}$ s.t. $x^n = y$.
It should be noted that $\circ$ maps S to itself. I.e., for $s_1, s_2, s_3 \in S$, $(s_1, s_2) \mapsto s_3$.
An example of a transformer in the mods is $(\mathbb{Z}/n\mathbb{Z}, +)$, while $(\mathbb{Z}/n\mathbb{Z}, \cdot)$ isn't unless n is prime. Other groups (sorry, I meant transformers) in the mods may be found at Enfield.

Conjugates:
If $A = L^{-1}BL$ for some L, then A and B are both conjugate.
Let $\approx$ represent the relation "is conjugate to". We showed that $\approx$ is a STS relation.

5.3 Permutations

Let S_n be the set of permutations of a n element list.
An example of a permutation, $\sigma \in S_7$:

$$\begin{array}{ccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 2 & 7 & 4 & 3 & 6 & 1 & 5 \end{array}$$

This can be represented by **disjoint cycle notation**: $\sigma = (1,\ 2,\ 7,\ 5,\ 6)(3,\ 4) = (4,\ 3)(7,\ 5,\ 6,\ 1,\ 2)$.
We noted that the order in which we compose 2 different permutations matters.
A brain break for the reader:
Futurama Theorem states that there is a brain-swapping machine which can swap 2 people's brains, but only once. After some group of people's brains were swapped, 2 mathematicians enter. The brains of the mathematicians follow the rules of the machine. Can everyone get their own brain back after a series of swaps?

6 Saturday – Animal Theory

We were given a set of many different animals (graphs) and determined what the qualifications were for an animal to be a gira~~ffe~~ph. We ended with the following set of ideas:

- Number of pieces = walkability.
- No homecoming cycles (cannot go "home" without turning back).
- Number of points = number of lines +1.
- Every line must end with an endpoint

From these observations, we came up with Noah ~~and Derek~~'s Theorem, which was named after the person who FIRST presented the theorem to the workshop.

Then we discussed Sophia and Judy's genius proof of Fermat's Little Theorem which was greatly **inspired** by Wilson's Theorem.

Theorem 7 *$a^p \equiv 1 \pmod p$ for prime values of p and $a \in \mathbb{N}$.*

Proof. We begin by salvaging the proof. We claim that the theorem is only possible if $(a, p) = 1$. To prove this, we use a proof by contradiction (call this proof by contradiction "Proof (a)". Because p is prime, $(a, p) = 1$ or $(a, p) = p$. We assume that $(a, p) \neq 1$ by our hypothesis in our proof by contradiction. Thus,

$$a = pk$$

for $k \in \mathbb{N}$. Plugging this into the theorem, we have that

$$(pk)^{p-1} \equiv 1 \pmod p,$$

however, $pk \equiv 0 \pmod p$, so we have a contradiction. Therefore, $(a, p) = 1$. From here, we note that

$$(p-1)!a^{p-1} \equiv a(1) \cdot a(2) \cdot a(3) \cdots a(p-1) \pmod p.$$

We want to prove that when we take the mods of each of the terms, we get distinct values, in other words, the resulting values after taking $\pmod p$ map in a one-to-one correspondence with the set $1, 2, \cdots p-1$. To do this, we use another proof by contradiction (call this "Proof (b)".) We assume two values in our set of products have congruent values after taking $\pmod{p}$. Suppose for some m and n that are in the interval $[1, p-1]$,

$$ma \equiv na \pmod{p}.$$

Then,

$$a(m-n) \equiv 0 \pmod{p}.$$

We then proved that $m - n$ cannot be congruent to $0 \pmod{p}$, proof is left to reader for length reasons. So, as p is prime, then $p|a$, which is a contradiction.

So, we proved that each term in our product has a distinct modulo, so multiplying our product, we have

$$(p-1)!a^{p-1} \equiv (p-1)! \pmod{p}.$$

Because the set $1, 2, \cdots p-1$ has multiplicative inverses, we can divide both sides by $(p-1)!$, and get the desired. P.I.not.G.

Ok. There's a problem. We know that the proof works, but the proof by contradictions are not necessary. Proof (a) and Proof (b) are examples of what is called a "useless contradiction." In class, we proceeded to reprove the two proofs without using contradictions and then learned about strategies to determine whether or not the contradiction statement is truly necessary. With these modifications, P.I.very.G.

To end the first week of first (and last) $7 \cdot 17 \cdot 17$ Summer Studies, we continued Friday's conversation about the properties of sub-transformers.