Mathematical induction, PHP, invariance, extremal arguments . . . and *Thinking*

J.L.F. King

IMO is '*International Mathematical Olympiad*'.

USAMO is '*United States of America Mathematical Olympiad*'.

HMMT is '*Harvard-MIT Mathematics Tournament*'.

MC is '*Mathcamp*'.

Problems from these and from the Putnam competition, are labeled as such.

Each class has had an Amanuensis, Problem Czar, Royal Scribe, whom I thank. Some were: *Knight Max Redmond, Sir Alexander Widom, Prime Minister James Cherry, Lady Lindsey Grigsby, Nicholas Campo, Bhaskar Mishra.*

What does this mean?

stand	*took*	*to*	*world.*
I	*you*	*throw*	*the*

§Outline

Quantifiers ∀ and ∃ ("for all" and "there exists") are like nitroglycerin, in that one little mis-step leads to the whole thing blowing up in your face.

There is no partial credit when it comes to Explosives and Quantifiers.

–JLF King

Pigeon-Hole Principle (PHP)

1.1: *PHP* How's my hair? *Prove that some two people on Earth have the same # of hairs on their heads.* ◊

Proof. With H the maximum number of head-hairs a person could have, we have $H+1$ PHs: *A box labeled "0", for all the bald folk. A box labeled "1", for all the the 1-haired people ... A box labeled "H", for all the max-hair folk.*

With U denoting the current Earth-popUlation, the PHP says that there is at last one box with at least

$$\left\lceil \frac{U}{H+1} \right\rceil \quad \textit{people in it.}$$

It seems that the max-number of head hairs is about 150,000. Conservatively, take $H+1 := 2\times 10^5$ hairs. As of Oct.2020, the human pop. is estimated at $U := 7.8\times 10^9$. Ratio

$$\frac{7.8 \times 10^9}{2 \times 10^5} = 3.9 \times 10^4.$$

So, *on average*, about $N := 3.9\times 10^4$ people have the same number of head-hairs that you do. In particular, there is *some* number h, where *at least* N people have exactly h head-hairs. ♦

1.2: *PHP* Martian socks. *Marty the Martian is dressing for his date; he'll meet her at the restaurant. [As we all know] Martians have 3 feet. In his sock drawer, jumbled up, are 500 socks; 100 apiece of five colors. He wants to wear matching socks on his date. Alas there is a power failure and he can't see the colors. What is the minimum number of loose socks he can grab, to guarantee he has 3 socks of the same color?* ◊

Proof. With 10 socks, he might have 2 of each color; no matching triple. Marty needs 11 socks.

With $C:=5$ the number of **c**olors [i.e, the # of pigeon-holes], and $D:=3$ the **d**esired number of matching socks, the max-number of socks *without* a monochromatic D-set is $\text{TooFew} := [D-1]C$.

Therefore, the min-# of socks needed is $\text{TooFew}+1$, i.e $[[D-1]C]+1$. ♦

2.1: ?? N-friends Problem. *In each set of $N \geq 2$ people, some two of them have the same number of friends.* (*View friendship as an anti-reflexive, symmetric relation.*) ♢

Solved by: *Jeremy S.*, 2011t. *Caleb S.*, 2014g. *Patrick B. & Isaac K.*, 2017g. *Aerin B. & Jeremy M.*, 2018t. *Riley B.*, 2018t. *Everybody*, 2019t. *Morgan F. & ??*, 2020t. *Chris C.*, 2021g. *Luke C.*, 2021t. *Nate B.*, 2022g. *Alexa M.*, 2022t. *Zhengmao Z., "Bill"*, 2023t. *Melanie R., Sarah B. & Andrey N.*, 2024g.

> *Learn from the mistakes of others. You can't live long enough to make them all yourself.*
> —*Eleanor Roosevelt*

3.1: ?? Points-in-a-square. *In square $\mathbf{C} := [0,1]\times[0,1]$, there are 10 "special" points. Prove that some two of them are no-further-apart than $\sqrt{2}/3$.* ◊

SOLVED BY: *Diego R.*, 2014g. *Yifei L.*, 2017g. *Daniel ?*, 2018t. *Bhaskar M.*, 2019t. *Julia A.*, 2020t. *Bill Z.*, 2021t. *Noah K.*, 2022g. *Aidan H.*, *Noah K.*, 2022g. *Edward G.*, 2022t. *Abhinav P. & Olivia J.*, 2023t. *Rohit D.*, *Luke L.*, 2024g.

Malaphors

It's not rocket surgery.

We'll burn that bridge when we come to it.

You can beat a dead horse, but you can't make him drink.

4.1: ?? $2N$-Subset-Problem. *Let $J_N := [1\,..\,2N]$, where $N\in\mathbb{Z}_+$. If subset $S\subset J_N$ is **big**, i.e has $|S|\geq N+1$, then:*

Appetizer: There exist distinct numbers $x,y \in S$ with $x \perp y$.

Entrée: There exist distinct $u,d \in S$ with $u \mid\bullet\, d$. [Such a (u,d) is a ***divisibility-pair***.] ◊

SOLVED BY: *Hannah P. & Patrick W.*, 2011t. *Zach N.*, 2012t. *Morgan W.*, 2014g. Appetizer: *CJ* [Charles F.], 2017g. Entrée: *Jessie C.*, 2017g. *Anthony M., Joey F. & Kailey S.*, 2018t. App: *Bhaskar M.*, 2019t. *Noam A.*, 2020g. *Junhao Z.*, 2020t. App: *Shi Z.*, 2020t. Ent: *Brandon A.*, 2021g. *Luke C.*, 2021t. App: *Nate B.*, 2022g. Ent: *Alejandro L.*, 2022g. App: *Anneka H.*, 2022h. *Appetizer-by Olivia J.*, 2023t. *Entree-by Faythe Corr*, 2023t. *Sam C.*, 2024g.

4.2: ?? *Generalized $2N$-Subset-Prob.* If $|S| \geq N+2$, must S have at least *two* divisor-pairs? How does the-above result generalize? □

Unhyphenated English pentasyllabic noun.
Hyphenated monosyllabic long paragraph.

5: ?? Monochromatic rectangle (USAMO 1976.1).

a: *Suppose that each cell of a 7×4 chessboard is colored either red or green. Prove, for each such coloring, that the board must contain a rectangle [formed by the horizontal and vertical lines of the board] whose four distinct corner-cells are all of the same color; a **monochromatic rectangle**.*

b: *Exhibit a red-green coloring of the 4×6 board with no monochromatic rectangle.*

c: *Produce an improvement of part (a).* ◊

Solved by: James C. & Caleb S., 2014g. Ken D., 2017g. Alex K., 2018t. Part (b) by Yukai H., Vanessa W., 2020g. Part (a) by Noam A., 2020g. Part (b) by Morgan F., Hani S., 2020t. Part (b) by Alex T., 2021g. Bill Z., 2021t. Part (b) by Nate B., 2022. Diego P., 2022t. Andrey N., 2024g.

> *Measure twice, cut once.* –**Proverb**

6.1: ?? Lattice coloring. *Each point of the lattice quadrant ℕ×ℕ is colored one of 50 colors. Prove that ℕ×ℕ admits a **monochromatic rectangle**. [I.e, the four corner lattice-pts have the same color.]* ◊

Solved by: Yuhan B. & Hao Z., 2019g. Teegan B., Chris P., Caden C., Jessica V., 2020g. Junhao Z., 2020t. Nicholas V.N., Alex T., Max W., 2021g. Andrey N., 2024g.

> *I am always ready to learn although I do not always like being taught.*
> –Winston Churchill

7.1: ?? Triangle Existence. *Sticks of lengths a, b, c can form a* (non-degenerate) *triangle IFF the sum of each two lengths exceeds the third.* [A ***length*** is a posreal.]

*Initially, let "upper bnd" $\mathbf{U} := 32$ and "number of sticks" $N := 13$. A **bag** $\mathcal{B}$ is a multiset of lengths with $|\mathcal{B}|{=}N$, where each length $\ell \in \mathcal{B}$ satisfies $1 \leq \ell < \mathbf{U}$. We say that N-bag $\mathcal{B}$ is **"U-bounded"**.*

a: *Prove that each bag has some 3 sticks which can form a triangle; this, using a simple* PHP *argument.* [*I.e,* prove each 32-bounded 13-bag admits a triangle.]

b: *With the same argument, to what value can we lower N and retain the conclusion?*

c: *Fix posint $N{\geq}3$. There is a largest real $\mathbf{U}_N$ st.: Every $\mathbf{U}_N$-bounded N-bag admits a* (non-degenerate) *triangle. Compute each $\mathbf{U}_N$.* [*Hint:* Note $\mathbf{U}_3 = 2$.] ◊

Solved by: *Justin K.*, 2020t.

Nicholas V.N., Alex T., Max W., Aubrey S. & Haritha K., 2021g.

Ben R., 2021t. *Alexa M.*, 2022t. *Amogh A. and Abhinav P.*, 2023t.

This next problem is similar, although I don't see how to solve it with PHP.

Cute 8.1: ??? Acute triangle (USAMO 2012.1). *A tuple $\vec{\boldsymbol{\ell}} := (\ell_1, \ell_2, \ldots, \ell_N)$ of posreals is **cute** if there are distinct indices i,j,k whose lengths ℓ_i, ℓ_j, ℓ_k form the sides of an acute triangle* [each angle $<90°$]*. An $N{\geq}3$ is **good** if every N-tuple satisfying*

†: $\operatorname{Max}(\ell_1, \ell_2, \ldots, \ell_N) \leq N \cdot \operatorname{Min}(\ell_1, \ell_2, \ldots, \ell_N)$

is cute. Find all good integers. ◊

Rooks

Let 7×7 denote the 7×7 chessboard, viewed as a set of 49 cells. A subset $S \subset$ 7×7 is ***friendly*** if its elements lie in distinct rows, and in distinct columns. [I.e, no rook in S could capture another S-rook.]

9.1: ?? Non-attacking rooks Thm. *Say a subset $\Gamma \subset$ 7×7 is **large** if $|\Gamma| \geq 22$. Then: Each large Γ admits a friendly 4-subset.* ◊

SOLVED BY: *Alisa M.*, 2015g. *Nathan T.*, 2019t. *Jessica V.*, 2020g. *Luke C.*, 2021t. *Mason ??*, 2022g. *Abhinav P.*, 2023t.

Counting in Two Ways (Double counting)

One type of proof counts a (usually finite) set in two different ways. Here is an example:

Eg Mult-is-commutative. *Integer $2 \cdot 3$ equals $3 \cdot 2$.* ◊

Double-count pf. Make a 2×3 array of dots. Counting the # of dots row-wise, gives 2 rows of 3 dots apiece. Counting column-wise yields 3 columns of 2 dots.♦

Now for something more substantial...

10.1: *DC* Fermat's Little Thm. *Fix P prime. For each integer n, difference $n^{\mathsf{P}} - n$ is a multiple of P.* ◊

[See (18a) proving this by Induction.]

Double-count pf. [WLOG $n>0$.] The idea is illustrated by $n=4$. Let S comprise those P-tuples of stones, colored from G,R,O,B, that are *not* monochromatic. Thus $|S| = 4^{\mathsf{P}} - 4$. We now count S a different way.

Connecting the ends of a tuple forms a ***necklace***. Group together those tuples that form identical necklaces, up to rotation. [We are not allowed to turn-over a necklace.] It suffices to show

∗: *Each necklace-group comprises P many tuples.*

For then, $|S| = [\text{\# of necklace-groups}] \cdot \mathsf{P}$.

If a necklace-group comprised only d many tuples, where $d<\mathsf{P}$, then the corresponding necklace is periodic with period d. Hence, *d is a proper divisor of P*. Our P is prime, whence $d = 1$. But that means that the necklace is monochromatic, hence was not in S.♦

11.1: ?? Candy-store identity. *The store has an unlimited supply of 4 types of candy [MMs, lemon-drops, twizzlers, jelly-beans]. From the 4 types, compute the number of ways of picking 5 candies, total.*

*I use $\left[\!\left[\begin{smallmatrix}4\\5\end{smallmatrix}\right]\!\right]$, read as "4 types pick 5", for this number. For $\mathbf{T}\in\mathbb{N}$ and $\mathbf{K}\in\mathbb{Z}$, use $\left[\!\left[\begin{smallmatrix}\mathbf{T}\\\mathbf{K}\end{smallmatrix}\right]\!\right]$ for "**T** types pick **K** (objects)"* ♢

Solved by: *Samantha-S.*, 2017g. *Ken D.*, 2017g. *Daniel Z.*, 2018t. *Hani S.*, 2020t. *Andrew L. & Isabel del-C.*, 2021t. *Ben R.*, 2021t. *Kevin J. & Noah K.*, 2022g. *Edward G.*, 2022t. *Zhengmao Z.*, 2023t. *Ivy Z.*, *Rohit D.*, 2024g.

> *Being a mathematician means never having to comb your hair.*

12.1: ??Scheherazade's Stratagem. *On each of the 1001 nights, as Scheherazade tells a tale to King Tut (yes, I know!) she flips a coin; as does he. But on the final night, Scheherazade has so mesmerized him that he forgets to flip. [She flipped 1001 times; he, only 1000.] She wins if she counted strictly more* HEADS *than he; else, he wins.*

What is Scheherazade's probability of winning? ◊

SOLVED BY: *Justin K. & Matthew C.*, 2020g. (Lively ideas contributed by *Hani S., Junhao Z. & Sydney E.*)

Jeremy G. & Emily Y., 2022g. *Abhinav P.*, 2023t. *Sam C.*, 2024g.

A FLEA AND A FLY IN A FLUE
Were imprisoned, so what could they do?
Said the fly, "let us flee!"
Said the flea, "let us fly!"
So they flew through a flaw in the flue.

–Ogden Nash

13: ??Binomial-product-PoT Lemma. *Consider natnums $N \geq E$. Then*

$$*: \quad \sum_{k \in [E \,..\, N]} \binom{N}{k}\binom{k}{E} \quad = \quad 2^{N-E} \cdot \binom{N}{E}. \qquad \diamond$$

SOLVED BY: *Mike C.*, 2014g. *Ross P.*, 2015g. *Ken D.*, 2017g. *Daniel Z.*, 2018t. *Nathan T.*, 2019t. *Hani S.*, 2020t. *Bill Z.*, 2021t. *Gabriel G.*, 2022t. *Zhengmao Z.*, 2023t. *Sarah] B.*, 2024g.

Combinatorial counting

The CANDY-STORE PROBLEM was an example of using double counting [stars-and-bars], and binomial-coeffs to prove an identity. Here we look at a related counting problem.

Tuples. Below, N, L and each a_j is a natnum. With various restrictions, we count the number of tuples $\vec{\boldsymbol{a}} = (a_1, a_2, \dots, a_L)$ satisfying

$$**: \qquad \left[\sum_{j=1}^{L} a_j\right] = N\,.$$

For *posint*-tuples, use $\mathsf{V}_+(N)$ to count *all* of them, whereas $\mathsf{F}_+(N,L)$ counts those of length exactly L. Finally, use $\mathsf{F}_0(N,L)$ to count all L-tuples of *natnums*. [Symbol V counts Variable-length; F counts Fixed-length.]

These (1,1,1), (1,2), (2,1), (3) are the only posint-tuples summing to 3. So $\mathsf{V}_+(3) = 4$. And $\mathsf{F}_+(3,2) = 2$, as only (1,2), (2,1) have length 2. Allowing natnum entries (0,3), (1,2), (2,1), (3,0), shows that $\mathsf{F}_0(3,2) = 4$.

In contrast, $\mathsf{F}_0(2,3) = 6$, as witnessed by these six tuples: (2,0,0), (0,2,0), (0,0,2), (0,1,1), (1,0,1), (1,1,0). □

14.1: ?? Counting tuples. *Allowing factorials, what are the simplest formulas you can find for*

$$\mathsf{V}_+(N) = ?\,, \quad \mathsf{F}_+(N,L) = ?\,, \quad \mathsf{F}_0(N,L) = ?\,.$$

Can you avoid summations? Is $N{=}0$ a special case?◊

SOLVED BY: *Matthew C. & Sydney E. & Hani S.*, 2020t. *Partial soln by Morgan F.*, 2020t. *Bill Z.*, 2021t.

Inclusion-Exclusion

The InEx pamphlet has a proof of InEx, and several examples, a few of which appear below.

15: *InEx* Counting limited candy. *The store sells jelly-Beans and Chocolate squares and Dates. Mom allows you a total of 20 candies.*

Alas!, the store only has $8\mathcal{B}$ *and* $5\mathcal{C}$ *and* $13\mathcal{D}$*. Stars-and-Bars counts how to pick out of multiset* $\{\infty\mathcal{B}, \infty\mathcal{C}, \infty\mathcal{D}\}$*. The relevant multiset is* $\{8\mathcal{B}, 5\mathcal{C}, 13\mathcal{D}\}$*; so how do we count?* ◊

Candy soln. Let Ω be the set of natnum triples $(\mathcal{B}, \mathcal{C}, \mathcal{D})$ with $\mathcal{B}+\mathcal{C}+\mathcal{D} = 20$. We'll count the "***good***" [$\mathcal{B}\le 8$ & $\mathcal{C}\le 5$ & $\mathcal{D}\le 13$] triples, using Incl-Excl.

Let $A_{\mathcal{B}}$ be the set of natnum-triples that are "***Awful***" because $\mathcal{B} > 8$. Hence,

$$|A_{\mathcal{B}}| \overset{\text{Why?}}{=\!=} \left[\!\!\left[\begin{matrix}3\\ 20-[8+1]\end{matrix}\right]\!\!\right] = \binom{2+11}{2} = 78.$$

So $|A_{\mathcal{C}}| = \left[\!\left[\begin{smallmatrix}3\\ 20-[5+1]\end{smallmatrix}\right]\!\right] = \binom{2+14}{2} = 120$, and $|A_{\mathcal{D}}| = 28$.

For *pairwise* intersections

$$|A_{\mathcal{B}} \cap A_{\mathcal{C}}| \overset{\text{Why?}}{=\!=} \left[\!\!\left[\begin{matrix}3\\ 20-[8+5+2]\end{matrix}\right]\!\!\right] = \binom{2+5}{2} = 21.$$

Also, $|A_{\mathcal{B}} \cap A_{\mathcal{D}}| = \left[\!\left[\begin{smallmatrix}3\\ 20-[8+13+2]\end{smallmatrix}\right]\!\right] = \left[\!\left[\begin{smallmatrix}3\\ \text{negative}\end{smallmatrix}\right]\!\right] \overset{\text{Why?}}{=\!=} 0$, and $|A_{\mathcal{C}} \cap A_{\mathcal{D}}| = \left[\!\left[\begin{smallmatrix}3\\ 20-[5+13+2]\end{smallmatrix}\right]\!\right] = \left[\!\left[\begin{smallmatrix}3\\ 0\end{smallmatrix}\right]\!\right] = 1$.

For the sole *three-fold* intersection

$$|A_{\mathcal{B}} \cap A_{\mathcal{C}} \cap A_{\mathcal{D}}| = \left[\!\!\left[\begin{matrix}3\\ 20-[8+5+13+3]\end{matrix}\right]\!\!\right] = \left[\!\!\left[\begin{matrix}3\\ \text{neg}\end{matrix}\right]\!\!\right] = 0.$$

Since $\left[\!\left[\begin{smallmatrix}3\\ 20\end{smallmatrix}\right]\!\right] = 231$, the number of good triples is

$$\begin{aligned}
&|\Omega| - \Big(|A_{\mathcal{B}}| + |A_{\mathcal{C}}| + |A_{\mathcal{D}}|\Big) \\
&\quad + \Big(|A_{\mathcal{B}} \cap A_{\mathcal{C}}| + |A_{\mathcal{B}} \cap A_{\mathcal{D}}| + |A_{\mathcal{C}} \cap A_{\mathcal{D}}|\Big) \\
&\quad - |A_{\mathcal{B}} \cap A_{\mathcal{C}} \cap A_{\mathcal{D}}| \\
&= 231 - [78+120+28] + [21+0+1] - 0.
\end{aligned}$$

This equals 27. ♦

Doubting Thomas. Here are the 27 good triples:

```
(2 5 13) (3 4 13) (3 5 12) (4 3 13) (4 4 12) (4 5 11)
(5 2 13) (5 3 12) (5 4 11) (5 5 10) (6 1 13) (6 2 12)
(6 3 11) (6 4 10) (6 5  9) (7 0 13) (7 1 12) (7 2 11)
(7 3 10) (7 4  9) (7 5  8) (8 0 12) (8 1 11) (8 2 10)
(8 3  9) (8 4  8) (8 5  7)
```
□

Prelim. Below, sets $\mathfrak{D}$ (Domain) and $\mathfrak{C}$ (Codomain) have cardinalities $\mathsf{D} := |\mathfrak{D}|$ and $\mathsf{C} := |\mathfrak{C}|$; both finite. Thus $\mathfrak{C}^{\mathfrak{D}}$, the set of fncs $\mathfrak{D}\to\mathfrak{C}$, has cardinality C^{D}. Easily:

$$*: \quad [\text{The \# of injections } \mathfrak{D}\to\mathfrak{C}] = [\![\mathsf{C} \downarrow \mathsf{D}]\!].$$

Let's compute $\text{Sur}(\mathsf{D},\mathsf{C})$, the number of *surjections*. □

16a: *InEx* Counting surjective fncs. *With notation from above*

$$\dagger: \quad \text{Sur}(\mathsf{D},\mathsf{C}) = \sum_{k=0}^{\mathsf{C}} [\text{-}1]^k \cdot \binom{\mathsf{C}}{k} \cdot [\mathsf{C} - k]^{\mathsf{D}}. \qquad \lozenge$$

Sur. For point $y \in \mathfrak{C}$, let A_y comprise those functions $h()$ which *Avoid* y; i.e, $\text{Range}(h) \not\ni y$. Thus

$$\ddagger: \quad \mathfrak{C}^{\mathfrak{D}} \smallsetminus \Big[\bigcup_{y\in\mathsf{C}} A_y\Big]$$

is the *set* of surjections.

For $I \subset \mathfrak{C}$, let $\mathbf{A}_I$ comprise those fncs which miss *each* member of I. With $k := {}^{\#}I$, then,

$$\mathbf{A}_I = \{h \in \mathfrak{C}^{\mathfrak{D}} \mid \text{Range}(h) \sqcap I\} \text{ and } |\mathbf{A}_I| = [\mathsf{C} - k]^{\mathsf{D}}.$$

The number of subsets $I \subset \mathfrak{C}$ with ${}^{\#}I = k$ is $\binom{\mathsf{C}}{k}$. Consequently, Inclusion-Exclusion yields (†). ♦

When $\mathsf{D}<\mathsf{C}$. There are *no* surjections, when $\mathsf{D}<\mathsf{C}$. As a (†)-example, $\text{Sur}(2,3)$ equals

$$\binom{3}{0}\cdot 3^2 - \binom{3}{1}\cdot 2^2 + \binom{3}{2}\cdot 1^2 - \binom{3}{3}\cdot 0^2$$
$$= 1\cdot 9 - 3\cdot 4 + 3\cdot 1 - 1\cdot 0 = 9 - 12 + 3,$$

which indeed equals zero. □

[*A Curious Corollary* of Counting sur-fncs.]

16b: A Curious Corollary. *For* $N = 0, 1, 2, \ldots$

$$\pounds_N: \quad N! = \sum_{k=0}^{N} [\text{-}1]^k \cdot \binom{N}{k} \cdot [N - k]^N. \qquad \lozenge$$

Proof. When $|\mathfrak{D}| = |\mathfrak{C}| =: N$, then we can identify $\mathfrak{D}$ with $\mathfrak{C}$ and view each surjection as a permutation. There are $N!$ permutations. And $\text{RhS}(\pounds_N)$ equals RhS(†) when $\mathsf{D} = \mathsf{C} = \mathbb{N}$. ♦

When $|\mathfrak{D}| = |\mathfrak{C}| = 3$. Computing, $\text{Sur}(3,3)$ equals

$$\binom{3}{0}\cdot 3^3 - \binom{3}{1}\cdot 2^3 + \binom{3}{2}\cdot 1^3 - \binom{3}{3}\cdot 0^3$$
$$= 1\cdot 27 - 3\cdot 8 + 3\cdot 1 - 1\cdot 0 = 27 - 24 + 3 = 6,$$

which, happily, equals 3-factorial. □

TwoStirling numbers. For natnums D, C, the number of partitions of a D-set into C many non-void-atoms, is a "***Stirling # of the 2nd kind***", (or ***Stirling partition number***). Here, I'll write it as $\mathcal{S}(\mathsf{D}, \mathsf{C})$.

Were the C many atoms *labeled*, then we could view a partition as a surjective [each atom is non-empty] *function* from the D-set into the label-set. Consequently,

$$\text{16c:} \quad \mathcal{S}(\mathsf{D},\mathsf{C}) = \frac{\text{Sur}(\mathsf{D},\mathsf{C})}{\mathsf{C}!} = \sum_{k=0}^{\mathsf{C}} [\text{-}1]^k \cdot \frac{[\mathsf{C} - k]^{\mathsf{D}}}{k! \cdot [\mathsf{C} - k]!} \underset{(k,n)\in\mathbb{N}\times\mathbb{N}}{=} \sum_{k+n=\mathsf{C}} [\text{-}1]^k \cdot \frac{n^{\mathsf{D}}}{k! \cdot n!}$$

is the nifty formula we obtain. □

17.1: ?? Random digits (USAMO 1972.3). *A random number selector selects one of the nine integers* $1, 2, \ldots, 9$, *and it makes these selections independently and with equal probability. Determine the probability,* D_N, *that after* $N \in \mathbb{N}$ *selections, the product of the* N *numbers selected is divisible by* 10. ◊

SOLVED BY: *Hani S.*, 2020t. *Haritha K. & Alex T.*, 2021g. *Aryaan V.*, 2022t. *Zhengmao Z.*, 2023t. *Rohit D.*, 2024g.

Suggestion. Write $1 = \mathbf{v}+\mathbf{e}+\mathbf{r}$ where, at one selection,

$$\mathbf{v} := [\text{Probability of five}]\,;$$
$$\mathbf{e} := [\text{Probability of an even}] \quad \textit{and}$$

$\mathbf{r}$ is the rest of the probability. Use InEx to compute $1 - D_N$. □

Psychic shop closed due to unforeseen circumstances.

Induction

For the next thm and two lemmas, P is a fixed prime, and $\equiv$ means $\equiv_{\mathsf{P}}$. [See (10.1) for a double-count proof.]

18a: *Ind* Fermat's Little Thm. *Each* $n \in \mathbb{Z}$ *has* $n^{\mathsf{P}} \equiv n$.

Induction pf of (18a). WLOGenerality, $n \geq 0$.

Base case: $0^{\mathsf{P}} = 0 \equiv 0$.

Induction: Fix n st. $n^{\mathsf{P}} \equiv n$. The Prime-binomial lemma 123 gives $\binom{\mathsf{P}}{k} \equiv 0$, for each $k{=}1, 2, \ldots, \mathsf{P}{-}1$. Hence

$$[n{+}1]^{\mathsf{P}} = \sum_{k=0}^{\mathsf{P}} \binom{\mathsf{P}}{k} \cdot n^k \cdot 1^{\mathsf{P}-k} = \overbrace{n^{\mathsf{P}}}^{k=\mathsf{P}} + \overbrace{1}^{k=0} + \sum_{k=1}^{\mathsf{P}-1} \binom{\mathsf{P}}{k} \cdot n^k$$
$$\equiv n^{\mathsf{P}} + 1,$$

by the Binomial thm, Thus $[n{+}1]^{\mathsf{P}} \equiv n + 1$, courtesy the ind.hypothesis. ♦

See (123a) for a related result.

> *How Do You Know When You're Middle Aged?*
> **The Four Warning Signs...**

Fixable inequality? Suppose I ask you to demonstrate the following assertion.

19.1: *Error* (Busted base) Statement A. *For each posint n:*

$$*: \quad 5 \cdot 2^n < 3^n . \quad \diamond$$

You would detect the error and write:

Dear Prof. King:

Something is amiss; assertion $(*)$ fails for $n = 1$, since $5 \cdot 2 \not< 3$. [Inequality $(*)$ also fails for $n{=}2$ and $n{=}3$.] I, Bubba, correct the statement below, and prove my correction.

19.2: Theorem A′. *For each $n \in [4..\infty)$:*

$$\mathsf{P}(n): \quad 5 \cdot 2^n < 3^n . \quad \diamond$$

Proof. Let $L(k) := 5{\cdot}2^k$ and $R(k) := 3^k$.

Base case: Note that

$$L(4) = 5 \cdot 16 = 80 < 81 ,$$

which equals $R(4)$. Hence $\mathsf{P}(4)$.

Induction: Fix an index $n \in [4..\infty)$. [Henceforth, "n" plays the role of a constant.]

Assuming $\mathsf{P}(n)$, my goal is to establish $\mathsf{P}(n{+}1)$. So I want to examine how $L(n{+}1)$ relates to $L(n)$, and ditto for $R()$.

Easily

$$\begin{aligned} L(n{+}1) &\stackrel{\text{def}}{=} 2 \cdot L(n) \\ &< 2 \cdot R(n) , \end{aligned}$$

courtesy $\mathsf{P}(n)$ and that 2 is positive. [Multiplication by a positive number is order-preserving.] Thus

$$\begin{aligned} L(n{+}1) &< 2 \cdot R(n) \\ &< 3 \cdot R(n) , \quad \text{since } R(n) \text{ is positive,} \\ &\stackrel{\text{def}}{=} R(n{+}1) , \end{aligned}$$

as desired. ♦

Autopsy. Of course, your proof used this elementary tool.

19.3: Lemma. *For all reals $\alpha<\beta$, and "multiplier" $M \in \mathbb{R}$: If M is positive, then $\alpha M < \beta M$.* $\diamond$

Exer.: *You used this lemma twice in your proof of* Thm A′; *where are the two occurrences?*

(How Do You Know You're Middle Aged?)

1: *You don't understand what on earth the young peasants are talking about.*

20: *Ind* ∞ly-many-Primes Thm (Euclid). *There are ∞ly many primes.* ♢

Pf. Given primes $p_1, \ldots, p_N$ (not-nec. distinct), we construct a new prime. Let $Q := [p_1 \cdot p_2 \cdot \ldots \cdot p_N]$; this Q is at least 1. [Even for $N=0$; the void-product is 1.]

Now add 1; let $R := Q + 1$. Necessarily, $R \perp Q$. Thus R is coprime to *each* p_j. Moreover, $R \geq 2$, so R has *at least one* prime factor (which might be R itself). And each of these prime factors is new. ♦

Algorithm. Becoming precise, at each stage let the new prime, call it p_{n+1}, be the *smallest* prime-factor of R_n. Then we will generate the Euclid–Mullin sequence, which is A000945 in OEIS.

Let's compute the beginning of the sequence. [Looking into the future: $1807 = \mathbf{13} \cdot 139$; $23479 = \mathbf{53} \cdot 443$.]

Primes_n	Q_n	R_n	p_{n+1}
$\{\}$	1	2	2
$\{2\}$	2	3	3
$\{2,3\}$	6	7	7
$\{2,3,7\}$	42	43	43
$\{2,3,7,43\}$	1806	1807	13
$\{2,3,7,43,13\}$	23478	23479	53
$\{2,3,7,43,13,53\}$	?	? + 1	??

(Exercise: Write down the rest of the table...) □

20a: Joke (Hendrik Lenstra). *There are ∞ly many composite numbers.* ♢

Proof. To obtain a new composite number, multiply together the first N composite numbers, then *don't* add 1. ♦

(How Do You Know You're Middle Aged?)

2: *You struggle to read Chaucer in weak candlelight.*

21.1: *Valid?* All horses have the same color.

Prelim. For $n \in \mathbb{N}$, we will use induction to prove

P_n: *Each collection of n horses is monochromatic* (Mcr). □

Poof. Base case: The emptyset is Mcr, hence (P_0). [Alternatively, we could start with (P_1), as singletons are Mcr.]

Induction: Our goal is to show that if each n-set of horses is monochromatic, then each $[n+1]$-set is too. Let's illustrate the idea with $n = 50$:

Take an arbitrary collection, $\mathcal{C}$, of 51 horses. Gently lead one of the horses, say, *Abby*, out of the corral, then close the gate, leaving 50 horses in the corral. [*Abby* is comfortably munching Kentucky bluegrass in the field.] Using (P_{50}), the 50-set in the corral is necessarily monochromatic say, brown. Now lead *Abby* back in the corral, but take *Bert-the-horse* out to the Kentucky bluegrass. Appealing to (P_{50}) again, the 50 horses currently in the corral must also be a monochromatic collection, hence also brown. Now bring *Bert-the-horse* back in, reforming collection $\mathcal{C}$, an all-brown 51-set of horses. The argument was applies to an *arbitrary* starting collection, $\mathcal{C}$, so our proof is complete. ♦

(How Do You Know You're Middle Aged?)

3: *You grumble that the Crusaders look younger every single year!*

22.1: *Ind* General Triangle-Inequality. *For each natnum N, and sequence $s_1, \ldots, s_N$ of complex numbers, this inequality holds:*

$$Q_N: \qquad \left|\sum_{j=1}^{N} s_j\right| \leq \sum_{j=1}^{N} |s_j| . \qquad \lozenge$$

Remark. Looking ahead, our tool will be (Q_2). □

22.2: Weak Tri-Ineq. *For all complex numbers α,β:*

$$*: \qquad |\alpha + \beta| \leq |\alpha| + |\beta| . \qquad \lozenge$$

Rem. For α,β real, this follows by a case-by-case argument [Both negative? Mixed sign?] For complexes, this takes a bit of development of the complex plane. □

Proof of Gen. Tri-Ineq. We use the vacuous base-case.

Base case: Evidently (Q_0), since $0 \leq 0$. [And (Q_1), since $|s_1| \leq |s_1|$. However, we don't need this argument, since the induction gets the same result.]

Induction: Fix a natnum N, and sequence $s_1, \ldots, s_N, s_{N+1}$. Assuming (Q_N), our goal is to establish (Q_{N+1}).

Applying (22.2∗) with $\alpha := \sum_{j=1}^{N} s_j$ and $\beta := s_{N+1}$, gives

$$\left|\sum_{j=1}^{N+1} s_j\right| \leq |\alpha| + |\beta| .$$

And (Q_N) yields $|\alpha| \leq \sum_{j=1}^{N} |s_j|$. Adding these gives

$$\left|\sum_{j=1}^{N+1} s_j\right| \leq \left[\sum_{j=1}^{N} |s_j|\right] + |\beta| ,$$

which equals $\text{RhS}(Q_{N+1})$, as was sought. ♦

(How Do You Know You're Middle Aged?)

4: *And you constantly worry about testing positive for Black Death...*

Prelim lemmas, sqrt-harmonic sum

By looking ahead in our induction proof, we may find a result that we wish to prove as a separate lemma.

23.1: *Ind* Recip-Squareroot thm. *For each $N \in \mathbb{Z}_+$,*

$$\dagger: \qquad 1 + \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{3}} + \ldots + \frac{1}{\sqrt{N}} \quad < \quad 2\sqrt{N}\,. \qquad \diamondsuit$$

Hmmm [Bubba thinks to her/him-self]*: After playing with* (†) *for a bit, I realize I need a little inequality involving square-roots. Let me state and prove that separately, to be nice to those reading my proof.*

23.2: Lemma. *For each real $x \geq 1$, we have that*

$$*: \qquad \frac{1}{\sqrt{x}} \quad < \quad 2[\sqrt{x} - \sqrt{x-1}]\,.$$

(*We needed $x \geq 1$ for $\sqrt{x-1}$ to make sense in $\mathbb{R}$.*) ◊

Proof of (23.2). Since $\sqrt{x} > 0$, our (∗) is implied by

$$1 \quad \overset{?}{<} \quad 2[x - \sqrt{x^2 - x}\,]\,,$$

hence by $2\sqrt{x^2 - x} \overset{?}{<} 2x - 1$. *Both sides are non-negative*, so this follows from the squared-version,

$$4[x^2 - x] \overset{?}{<} 4x^2 - 4x + 1\,.$$

And this last is trivially true. ♦

Proof of Recip-Squareroot thm. Let L_N and R_N denote the left/right-hand sides of (23.1†).

Base case. Since $L_1 = 1 < 2 = R_1$, we can start [♡1]our induction at $N{=}2$.

Induction: ISTEstablish, for each $N \in [2\,..\,\infty)$, that $L_N - L_{N-1} < R_N - R_{N-1}$, i.e, that

$$\ddagger: \qquad \frac{1}{\sqrt{N}} \quad \overset{?}{<} \quad 2[\sqrt{N} - \sqrt{N-1}]\,.$$

Happily, this is implied by Lemma 23.2. ♦

[♡1]Actually, *in a sense* we could use $N{=}0$ as our base case. True, $L_0 = 0 = R_0$, so we do not have the strict inequality of (†). But as (‡) is strict, we would obtain (†) for $N = 1, 2, \ldots$.

Après-proof. In developing our induction argument, at (‡) we realized we needed another result. Not only is it clearer to split the result out to a separate lemma, but we got a *slightly stronger* result, since (23.2) holds for reals, not just integers. □

23.3: *Alternative.* We can sharpen (23.1), using calculus. For an arbitrary decreasing fnc $f\colon \mathbb{R}_+ \to \mathbb{R}_+$ and integer $N \in [2\,..\,\infty)$, a picture easily shows[♡2] that

$$¥: \qquad \sum_{j=2}^{N} f(j) \quad < \quad \int_1^N f(x) \cdot \mathrm{d}x\,.$$

Applying this with $f(x) := 1/\sqrt{x}$ yields that

$$L_N - 1 \quad < \quad 2x^{1/2}\Big|_{x=1}^{x=N} \; = \; 2[\sqrt{N} - \sqrt{1}]\,.$$

Adding 1 to each side yields $L_N < [2\sqrt{N}] - 1$, for $N = 2, 3, 4, \ldots$. □

> *Precaution is called the Mother of Wisdom;*
> *the father was never known.*
> *That should prove to you, at at glance,*
> *that even Precaution once took a chance.*
>
> *–Paul von der Porten, translated from the German by his son, Arnold von der Porten.*

[♡2]Specifically: The inequality in (¥) is strict *unless* f is *the* step-function which mimics the summation.

Defn. For numbers, recall that A^{B^C} means $A^{[B^C]}$.

The n^{th} ***Fermat number*** is $F_n := 2^{2^n} + 1$. E.g $F_0 = 3$ and $F_3 = 1 + 2^{2^3} = 1 + 2^8 = 257$. □

24: ?? Coprime Fermat. *For each pair $K < N$ of natnums, Fermat numbers F_K and F_N are coprime. (Coro: There are infinitely many prime numbers. [How does this follow?])* ◊

Hint. How is $G_n := F_n - 2$ related to F_n? □

Caveat: The Wikipedia page has a proof.

Solved by: *2013t & 2015g classes, on a takehome.*

Patrick T., 2018t. *Hani S.*, 2020t. *Joseph M.*, 2021g.

The Stalled-Induction ditty

...Ninety-nine bottles of beer on the wall.
Ninety-nine bottles of beer.
And if no bottles should happen to fall...

We now discuss a sequence like the Fibonacci sequence.

25.1: *Ind* Two-term recurrence. *Sequence* $\vec{b} := (b_0, b_1, b_2, \ldots)$ *starts with* $b_0 := -1$ *and* $b_1 := 2$. *Moreover, for each integer* $n \geq 2$,

†: $$b_n \quad := \quad 5b_{n-1} - 6b_{n-2}\,.$$

Prove, for each natnum k, *that*[♡3]

‡: $$b_k \quad = \quad [4\cdot 3^k] - [5\cdot 2^k]\,. \qquad \Diamond$$

Preliminaries. Define $\mathbf{f}{:}\,\mathbb{N}\to\mathbb{Z}$ by

‡‡: $$\mathbf{f}(k) \quad := \quad [4{\cdot}3^k] - [5{\cdot}2^k]\,.$$

Before starting work, do I even *believe* the outlandish assertion of the thm? From (†) I can compute

$$b_2 \overset{\text{def}}{=} 5{\cdot}2 - 6{\cdot}[-1] = 10+6 = 16\,.$$

And $\mathbf{f}(2)$ equals $[4{\cdot}9] - [5{\cdot}4] = 36 - 20$, which indeed equals 16. Also,

$$b_3 \overset{\text{def}}{=} 5{\cdot}16 - 6{\cdot}[2] = 80 - 12 = 68\,.$$

And $\mathbf{f}(3)$ equals $[4{\cdot}27]-[5{\cdot}8] = 108-40$, which –wow!– also equals 68. So now I [Bubba Student] think the stmt is plausible, and I am willing to work on it. □

Observation. When k is large, the value 3^k swamps 2^k. So a corollary of Two-term is that $\vec{b}$ grows like $k\mapsto 3^k$, in the sense that ratio $[b_k/[4{\cdot}3^k]] \to 1$, as $k\nearrow\infty$.

And that is not obvious from the recursive *definition* of $\vec{b}$, in (†). □

Proof of Two-term. Since (†) needs the *two* previous values in $\vec{b}$ in order to determine the next, we'll need to check two base cases.

Base cases: Firstly [or should I say "Zerothly"?],

$$\mathbf{f}(0) = [4{\cdot}1] - [5{\cdot}1] = -1 \overset{\text{Hooray!}}{=\!=} b_0\,.$$

And secondly ["firstly"?],

$$\mathbf{f}(1) = [4{\cdot}3] - [5{\cdot}2] = 12 - 10 = 2 \overset{\text{note}}{=\!=} b_1\,,$$

as was needed.

Induction: We just need to show that fnc $\mathbf{f}()$ behaves like (†). So say that a fnc $g{:}\,\mathbb{N}\to\mathbb{Z}$ is ***good*** if

∗: $$\forall k\in\mathbb{N}: \quad g(k{+}2) = 5g(k{+}1) - 6g(k)\,.$$

Restated, our goal is to show that $\mathbf{f}$ is good.

We can, of course, show goodness directly, but let's "look ahead", and see if we can shorten our work.

We glance at (‡‡) and note that $\mathbf{f}$ is built from two simpler fncs, namely

$$H(k) := 3^k \quad\text{and}\quad W(k) := 2^k\,.$$

["H" is for tHree, and "W" is for tWo.] Our beloved $\mathbf{f}$ is simply the linear combination

$$\mathbf{f}() \quad = \quad 4{\cdot}H() - 5{\cdot}W()\,.$$

Evidently, if a fnc $g()$ is good, then for α an arbitrary real, the product $\alpha g()$ is also good; this follows from (∗) since mult distributes-over addition.

Moreover, the *sum* of two good fncs is good; this, since addition is associative and commutative. So we've established:

∗∗: *Linear combinations of good functions are good.*

Hence our task has simplified to the following.

Goal: Fnc $H()$ is good, and so is $W()$. Letting $Y := 3$, in order to show $H()$ good, we covet

$$\forall k\in\mathbb{N}: \quad Y^{k+2} = 5Y^{k+1} - 6Y^k\,.$$

But this is implied by establishing

$$Y^2 \overset{?}{=} 5Y - 6\,,$$

simply by multiplying by Y^k. And this nice quadratic equality (we *could* just compute that 9 equals $[5{\cdot}3] - 6$, but let's take an approach that illustrates how the problem was created) is the same as saying that $Y{=}3$ is a root of polynomial

$$P(x) \quad := \quad x^2 - 5x + 6\,.$$

Similarly, showing $W()$ good is equivalent to showing that $P(2) = 0$. So we could simply check that both $P(3)$ and $P(2)$ are each zero. Or note that

$$P(x) \quad = \quad [x-3]\cdot[x-2]\,;$$

i.e, we simply factor the $P()$ polynomial. *Elegant!* ♦

[♡3] Do you see why (†) uses ":=", but (‡) uses the "=" relation?

Autopsy. Indeed, to *create* the problem, Prof. K simply started with the factored poly $[x-3]\cdot[x-2]$, then multiplied to get x^2-5x+6. This gave him the coeffs for (†).

The Upshot?: We learn a lot about a subject/technique by *creating* problems with that technique. So I encourage you to create and post induction problems, and to post solns to others' posted problems.

We adults tend to learn by synthesis, more than by analysis. [Or at least, we retain more.] □

25.2: Exercise. *For distinct reals α,β, define a sequence $\vec{\boldsymbol{b}}$ by (25.1†) together with $b_0 := \alpha$ and $b_1 := \beta$. Derive formulas for numbers $\mathsf{H}_{\alpha,\beta}$ and $\mathsf{W}_{\alpha,\beta}$ so that:*

25.3: $\forall k \in \mathbb{N}$: $$b_k = \left[\mathsf{H}_{\alpha,\beta}\cdot 3^k\right] - \left[\mathsf{W}_{\alpha,\beta}\cdot 2^k\right].$$ ◊

26.1: ?? Favorite-Toy Problem (HMMT2013.7). *There is a set* $\mathbf{K}$ *of* n *kids, and a set* Ω *of* n *toys. Each child has a (strict) preference ordering on the toys. A* ***distribution*** *of the toys, is a bijection* $f\colon\mathbf{K}\hookrightarrow\!\!\!\rightarrow\Omega$; *it indicates that child* $\mathbf{c}$ *gets toy* $f(\mathbf{c})$. *A distribution is* ***disappointing*** *if no child gets his favorite toy.*

Distribution h ***dominates*** f, *written* $h \succcurlyeq f$, *if each child likes his* h*-toy at least as much as his* f*-toy.* [*Further, say "*h ***exceeds*** f*", written* $h \succ f$, *if* $h \succcurlyeq f$ *and* $h \neq f$.] The goal is to prove:

‡[n]: *Suppose* f *is a disappointing* n*-distribution. Then there exists an* h *with* $h \succ f$. ◊

Solved by:

> *Tarantulas tarantulas*
> *Everybody loves tarantulas*
> *If there's just fuzz where your hamster was*
> *It's probably because of tarantulas*
>
> –chorus of "The Tarantula Song" –Bryant Oden

27: ?? Modsum-zero Problem. *Given a posint V (initial Value), define a sequence $\vec{\boldsymbol{b}}$ by $b_1 := V$ and, for each $n \in [2 .. \infty)$, let b_n be the unique value in $[0 .. n)$ for which sum*

$$S_n \quad := \quad b_1 + b_2 + \ldots + b_n$$

is divisible by n. Prove that $\vec{\boldsymbol{b}}$ is eventually-constant.

E.g.

b_n:	31	1	1	3	4	2	0	6	6 ⋯
n:	1	2	3	4	5	6	7	8	9 ⋯

◊

SOLVED BY: *Alex K., Christopher P., Reid O.*, 2012g. *Bhaskar M.*, 2019t. *Bill Z.*, 2021t. *Amogh A.*, 2023t.

28.1: ??? Difference-divider (USAMO 1998.4). *Each $N \geq 2$ admits a set $\mathcal{S}$ of N integers such that $[s - \widehat{s}]^2$ divides product $s \cdot \widehat{s}$, for each distinct $s, \widehat{s} \in \mathcal{S}$.* ◊

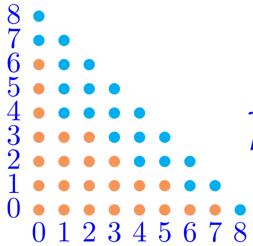
Thoughts. The $N \geq 2$ restriction is irrelevant; the result vacuously holds for $N = 0,1$.

Temporarily remove squaring, seeking just that each difference $s - \widehat{s}$ divides $s \cdot \widehat{s}$. A soln might generalize to squares.

For $\mathcal{S}$ comprising posints $s_1 < s_2 < \cdots < s_N$, what simple condition forces $s_\ell - s_k$ to divide $s_k s_\ell$, whenever $N > \ell > k \geq 1$?

Fabricate $\{s_j\}_1^N$ to iteratively satisfy the condition. Try both going up from s_1, and going down from s_N □

Visual **29.1: ??** Blue trails (IMO 2002.1). *Fix posint N. Let Δ be the set of all natnum-pairs (x,y) st. $x+y<N$. Each element of Δ is colored pink or blue, so that if (x,y) is pink and $x' \leq x$ and $y' \leq y$, then (x',y') is also pink.*



An example of pink-blue Δ for $N=9$.

“Happy trails” (to you)

An **X-*trail*** *is an N-set of blue points in Δ of form*

$$\Big\{(0,y_0),(1,y_1),(2,y_2),\ldots,(N-1,y_{N-1})\Big\};$$

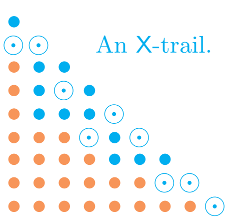
one blue point per-column of Δ.

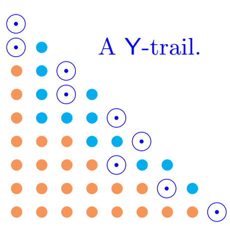
A **Y-*trail*** *is also an N-set of blue pts, but has form $\{(x_0,0),(x_1,1),\ldots,(x_{N-1},N-1)\}$; one blue per-row.*

Prove $|\mathbb{X}|=|\mathbb{Y}|$; equal numbers of X and Y trails. ♢

A better proof? While the PList has an induction proof, a more elegant demonstation would be to produce a natural bijection $\mathbb{X} \hookrightarrow\!\!\!\!\rightarrow \mathbb{Y}$. I don't have one, but perhaps an ES [Energetic Student] can find one? □

Hint. These two examples...





show that an X-trail need not be a Y-trail.

This legal coloring of a *square* board, has one X-trail, but *no* Y-trails. Board-shape matters... □

30: ??Coloring subsets (USAMO 2002.1). *An element of*

$$J := \{1, 2, 3, \ldots, 2002\}$$

is a ***token***. *A set-of-tokens is a* ***blip***. *A* ***"coloring*** *over* J***"*** *is a map,* $\mathcal{C}$*, which assigns to each blip either* ***green*** *or* ***red*** *such that*

†: *The union of each two red blips is red, and the union of each two green blips is green.*

Let $\mathsf{R}(\mathcal{C})$ *denote the number of red blips. Prove:*

‡: $\forall n \in [0 \,..\, 2^{2002}]$, *there exists an* n***-coloring***, $\mathcal{C}$*, i.e, a coloring with* $\mathsf{R}(\mathcal{C}) = n$. ◊

Solved by: I think this was solved by former student.

Defn. For each natural number M, let $J_M := [1 \,..\, M]$.

Use ***TAP*** for "3-*term arithmetic progression*"; a triple $(\boldsymbol{\tau}, \boldsymbol{\tau}+G, \boldsymbol{\tau}+2G)$ of numbers, with $G > 0$. □

31.1: ?? 3Term integer AP (precursor of USAMO 1980.2). *Compute $f(M)$, the number of TAPs in J_M.* ♢

[*Suggestion:* Inclusion-exclusion. Induction.]

SOLVED BY: *Daniel Z.*, 2018t. *Daniel S.*, 2019t. *Atharva P.*, 2019t.

31.2: ?? 3Term real AP (USAMO 1980.2). *Determine $g(M)$, the maximum number of three-term arithmetic progressions which can be chosen from a sequence of M real numbers [which we'll call **tokens**]*

$$*: \qquad \boldsymbol{\tau}_1 < \boldsymbol{\tau}_2 < \cdots < \boldsymbol{\tau}_M .$$

[I.e, $g(M)$ is the max taken over all M-sequences of tokens.] ♢

[*Suggestion:* Induction.]

SOLVED BY: *Atharva P.*, 2019t.

32: ?? Stable-table Conundrum (USAMO 2005.4). *Legs L_1, L_2, L_3, L_4 of a square table each have length n, where $n \in \mathbb{N}$. For how many ordered 4-tuples (k_1, k_2, k_3, k_4) of natnums can we cut a piece of length k_i from the end of leg L_i, and still have a stable table? Let A_n denote this number.* (*The table is **stable** if it can be placed so that all four of the leg-ends touch the floor. Note that a cut leg of length 0 is permitted.*) ♢

A stable table need not be level.

SOLVED BY: *Cameo L. & Diego R.*, 2014g. *Ken D.*, 2017g.

New 33.1: ??? Sealed-set (USAMO 2004.2). *Consider posint N and $\mathbb{Z}$-tuple $\vec{\alpha} = (\alpha_1, \ldots, \alpha_N)$ with $\text{GCD}(\vec{\alpha}) = 1$. A set $\Omega \subset \mathbb{Z}$ owns each α_j, and satisfies:*

i: $\forall i, j$ (*not nec. distinct*): $\alpha_i - \alpha_j \in \Omega$.

ii: $\forall x, y \in \Omega$: If $x + y \in \Omega$ then $x - y \in \Omega$.

Prove that $\Omega = \mathbb{Z}$. ◊

Solved by: (No one, so far.)

Defn. A (finite or infinite) sequence $\vec{n} = (n_1, n_2, \ldots)$ of *posints* is ***cute*** if, for each j, product $n_j n_{j+1}$ is divisible by sum $n_j + n_{j+1}$, □

34.1: ?? Cute sequences (USAMO 2002.5). *For* $\mathbf{a}, \mathbf{b} \geq 3$, *prove there exists a cute-sequence* $\vec{n} = (n_1, n_2, \ldots, n_K)$ *with* $n_1 = \mathbf{a}$ *and* $n_K = \mathbf{b}$. ◊

Solved by: *Hani S.*, 2021t.

Induction, abstractly

Seeking to prove some proposition P on $\mathbb{N}$, ***weak induction*** and ***strong induction*** are

$$\text{WEAK:}\quad \forall n \in \mathbb{Z}_+: \qquad \mathsf{P}_{n-1} \Rightarrow \mathsf{P}_n\,;$$
$$\text{STRONG:}\quad \forall n \in \mathbb{N}: \quad [\mathsf{P}_0 \wedge \mathsf{P}_1 \wedge \ldots \wedge \mathsf{P}_{n-1}] \Rightarrow \mathsf{P}_n\,.$$

Strong-ind says: *If all the descendants of n are* P*, then so is n.* *In principle*, strong-ind has no base case. Note, however, that $n=0$ has no descendants, so sometimes P_0 needs to be treated separately.

Strong-ind can be converted to weak-ind at the expense of adjoining a quantifier to the proposition. Let

$$\mathsf{Q}_n := \Big[\forall k < n\colon \quad \mathsf{P}_k \text{ holds}\Big]\,.$$

Then weak-ind for Q is the same as strong-ind for P.

General induction. This takes place on a *well-founded* [each non-void subset has a minimal element] poset $(\Omega, \prec)$. For $\beta \in \Omega$, the "***descendants*** of β" comprise the set

$$\Omega^{\prec\beta} := \{\omega \in \Omega \mid \omega \prec \beta\}\,.$$

To prove that all of Ω is, say, blue, ISTEstablish:

†: $\forall\beta\in\Omega$: *If each descendant of β is blue, then β is blue.*

To see that this is strong-induction on Ω, FTSOContradiction suppose the CEX set [*the set of non-blue elts*] is non-void. Since Ω is well-founded, CEX has a minimal element; call it *Mindy*. Since *Mindy* is *minimal non-blue*, all of its descendants *are* blue. But this contradicts (†). [Possibly *Mindy* has no descendants; fine.]

Say that α is a "***child*** of β" if $\alpha \prec \beta$ and there is *no* elt ω with $\alpha \prec \omega \prec \beta$. Suppose your poset has each elt β satisfying:

∗: *Each descendant of β is less-equal some child of β.*

Then proving Ω blue can be done by weak-induction:

‡: $\forall\beta\in\Omega$: *If each child of β is blue, then β is blue.*

[In practice, one might have a separate "base case" argument, showing that all the "childless" Ω-minima are blue.]

Notation. Induction on a poset Ω more complicated than $(\mathbb{N}, <)$ is called ***transfinite induction***. Typically, transfinite induction is done on a totally-ordered [i.e, ***well-ordered***] set.

Infinite descent. Induction by Infinite descent is when, initially, you don't know well-founded set to induct on. But you discover it while exploring properties of the problem.

Infinite descent

I describe Proof by infinite descent as *"Induction, when you don't know what you are inducting on."*

P∞↓ [Proof by infinite descent] starts with "For the sake of ※, suppose…" In the process of manipulating the parts in problem, you discover something get smaller, in a context where it can't get smaller forever; thus, ※. [By "smaller", here, I mean that a quantity moves in some direction, where that direction is eventually blocked.] Here is an example.

Golden ratio. Break a stick into a long piece, length L, and a short piece, S. Suppose we have that ratios $\frac{\text{Total len}}{\text{long}}$ and $\frac{\text{long}}{\text{short}}$ are equal, i.e $\frac{L+S}{L} = \frac{L}{S}$. The common ratio is called the ***golden ratio***, $\boldsymbol{\lambda}$. [For future reference: A ***golden rectangle*** is a $W \times H$ rectangle where $\frac{\text{long side}}{\text{short side}}$ is $\boldsymbol{\lambda}$.] □

36: ∞↓ The Irrationality of Gold. *Golden $\boldsymbol{\lambda}$ is irrational.* (*The Menendez Proposition*) ◊

Proof by ∞↓. FTSOC, suppose there exist positive *integers* $T>L$ with $\frac{T}{L} = \boldsymbol{\lambda}$. From the defining property of $\boldsymbol{\lambda}$, letting $S := T-L$ gives this new pair $L>S$ of posints, whose $\frac{L}{S}$ ratio is golden. Hence we can (supposedly) descend in the positive integers *ad infinitum*, getting golden-ratio pairs; ※. (contradiction) ♦

Alt. Making $S = 1$, relation $\frac{L+1}{L} = \frac{L}{1}$ says that $\boldsymbol{\lambda}$ is the positive root of $g(x) := x^2 - x - 1$, so $\boldsymbol{\lambda} = \frac{1+\sqrt{5}}{2}$.

Hence irrationality of $\boldsymbol{\lambda}$ is equivalent to irrationality of $\sqrt{5}$. However, proof of the latter seems to need higher-powered stuff like the uniqueness of factoring-into-primes, whereas the above ∞↓ argument used *nothing*. (Discussion? Objection?) □

The downloaded movie got 3.1415 stars. It's a $\boldsymbol{\pi}$-rated movie…

–*transmitted by Ruth King*

37.1: ∞↓ Root-flipping example (IMO1988.6). *A posint integer R is **nice** if there exist posints b, c such that ratio*

$$*: \quad \frac{b^2+c^2}{bc+1} = R.$$

Then each nice R is a perfect square. ♢

NB. Allowing R negative ruins the perfect-square conclusion. E.g $\frac{[-1]^2+3^2}{[-1\cdot 3]+1} = \frac{10}{-2} = -5$. □

The below proof is from Wikipedia's Vieta jumping.

Root flipping. FTSOC, fix a non-square nice R. Among all *posint*-pairs (b,c) satisfying $(*)$, pick a pair *minimizing* sum $b+c$, and call it (B,C). WLOG, $\mathsf{B} \geq \mathsf{C}$.

Our contradiction shall be to produce a

$$\dagger: \quad \text{Posint } \beta < \mathsf{B} \text{ such that } \frac{\beta^2+\mathsf{C}^2}{\beta\mathsf{C}+1} = R.$$

Polynomial. Numbers, x, that satisfy $\frac{x^2+\mathsf{C}^2}{x\mathsf{C}+1} = R$, are the roots of quadratic

$$f(x) := x^2 - \mathsf{C}Rx + [\mathsf{C}^2 - R] = x^2 - \mathcal{S}x + \mathcal{P},$$

where $\mathcal{S}$ is the **s**um of the f-roots, and $\mathcal{P}$ is their **p**roduct. Our $\mathcal{P} \neq 0$, since R is not a square.

The *other* f-root, $\beta := \mathcal{S} - \mathsf{B}$, is an *integer*, since $\mathcal{S}$ and B are.

Is $\beta \overset{?}{>} 0$: Ratio $\frac{\beta^2+\mathsf{C}^2}{\beta\mathsf{C}+1}$ is positive, so $\beta\mathsf{C}+1$ is positive; thus $\beta\mathsf{C} \geq 0$. But $\beta \neq 0$, since product $\mathcal{P} \neq 0$. Hence $\beta > 0$. Conclusion: β is a positive integer.

Is $\beta \overset{?}{<} \mathsf{B}$: Note $\beta\mathsf{B} = \mathsf{C}^2 - R \overset{\text{note}}{<} \mathsf{C}^2 \leq \mathsf{B}^2$, since $\mathsf{B} \geq \mathsf{C} \geq 0$. Thus $\beta < \frac{\mathsf{B}^2}{\mathsf{B}} = \mathsf{B}$, yielding (†). ※ ♦

Addenum. Let $\langle b, c \mid R\rangle$ mean $(*)$ where $\boxed{b \geq c}$ and R are three posints.

37.2: Obs. *TFAEquivalent:* ①: $\langle b,c \mid R\rangle = \langle 1,1 \mid 1\rangle$. ②: $b = c$. ③: $c = 1$ (or $b=1$). ④: $R = 1$. ♢

Proof of ②⇒③. Since $[c^2+1]R = 2c^2$, our $R \bullet c^2$, so $R \geq c^2$. Thus $0 = [c^2+1]R - 2c^2 \geq c^4 + c^2 - 2c^2$, which is non-neg. Hence all are zero and thus $c = 1$. ♦

Pf ③⇒④. We have $b^2+1 = [b+1]R$, so $R \equiv_b 1$. Thus $b^2+1 = [b+1][mb+1]$ for some natnum m, whence $b^2 = mb^2 + [m+1]$. So $m = 0$ and thus $R = 1$. ♦

Proof of ④⇒①. We have $b^2+c^2 \overset{\text{by ④}}{=\!=} bc+1 \leq b^2+1$. Thus $c^2 \leq 1$, so $c = 1$. Hence $b^2+1 = b+1$, so $b^2 = b$, whence $b = 1$. ♦

Families. Fixing R, when $\langle b,c \mid R\rangle$ minimizes $b+c$ [or just b] then our ∞↓ proved $R \overset{\text{must}}{=\!=} c^2$. Thus $(*)$ gives $b = c^3$. Hence

$$\langle \overbrace{n^3}^{b}, \overbrace{n}^{c} \mid \overbrace{n^2}^{R} \rangle$$

is an ∞ soln-family.

Another ∞-family is

$$\langle \overbrace{n^5 - n}^{b}, \overbrace{n^3}^{c} \mid \overbrace{n^2}^{R} \rangle.$$

An example of both is $n=2$. Note that $2^5 - 2 = 30$. So...

$$\frac{30^2+8^2}{[30\cdot 8]+1} = \frac{964}{241} = 4 \quad \textit{and}$$

$$\frac{8^2+2^2}{[8\cdot 2]+1} = \frac{68}{17} = 4.$$

38: ??*bcq-bc* Problem (USAMO 1976.3). *Determine all integral solutions of*

$$\dagger_0: \quad b^2 + c^2 + q^2 \quad = \quad b^2 \cdot c^2 .$$

[*Hint: ∞↓, after preparation.*] ♢

SOLVED BY: *Lizzie [Donna] N-C.*, 2017g.

Alex T. & Allan D. & Isabel D. & Max W., 2021g. *Bill Z.*, 2021t. *Aryaan V.*, 2022t. *Abhinav P.*, 2023t.

39: ??Football Prob. (*Research possibility: Tug-of-war*). *A tuple* $\vec{\boldsymbol{w}} = (w_1, w_2, \ldots, w_{23})$ *represents the* [*real number*] *weights of football players. Tuple* $\vec{\boldsymbol{w}}$ *is a* ***football tuple*** *if: No matter whom is chosen as referee, there exists a partitioning of the remaining players into two equal-cardinality, equal total-weight teams.*

Prove that the only football tuples are the constant tuples. [*Hint: First consider integer weights and use ∞↓.*] ♢

SOLVED BY: *Forrest K.* (*for integral weights*), 2013t. *Junhao Z.* (*for integral weights*), 2021t.

40.1: ?? Coalescing Robots. *Consider an $K{\times}L$ chessboard, which we'll think of as the $K{\cdot}L$ many rooms of a building. Initially, the walls are all the edges of rooms. Remove some of the interior walls, so the building is **connected**; it is possible to walk from any room to any other room. Call a connected building a **house**.*

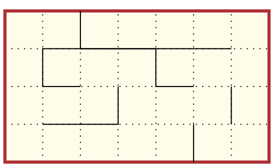
Put a robot mouse in each room. You can radio commands N,E,S,W *[North, East, South, West] to all the robots. If you radio* N*, then each robot with a room to his north* and *no wall between, rolls to that room; otherwise, he doesn't move. [Now, some rooms might contain two robots; a room can hold any number of robots.]*

*A house is **coalesceable** if there exists a finite instruction sequence [e.g* NNES…WWN*] after which all $K{\cdot}L$ robots are in a single room.*

Prove that every (finite; foreshadowing) house is coalesceable. [Hint: Create a Lemma *which, used repeatedly, proves coalescence. Now use $\infty\downarrow$ to establish the* Lemma*.]* ♢

Solved by: *Isaac K.*, 2017g. *Nathan T.*, 2019t. *Atharva P.*, 2019t. *Ben R.*, 2021t. *Nate B.*, 2022g. *Faythe C.* (The essential Idea), 2023g.

Example:
A 7×4 house.



40.2: *Ans.* Each (K, L) is good.

Tool: In a house, define the ***distance*** between two rooms A, B as the length of a minimum length walking-path [which need not be unique] between them. For example, $\text{Dist}(A, A) = 0$ and, for $A = (3, 5)$ and $B = (3, 6)$: *If there is no wall between these rooms, then* $\text{Dist}(A, B) = 1$, *else* $\text{Dist}(A, B) \geq 2$. □

40.3: *Defn.* Consider two robots (i.e, rooms) A,B in a house $\mathbf{H}$. Their ***Pair-coalescence Time***, $\text{PT}_{\mathbf{H}}(A, B)$, is the *minimum* time it takes to coalesce A with B. For a finite house, it makes sense to define the ***worst-case pair-coalescence-time***,

$$\widehat{\text{PT}}_{\mathbf{H}} := \text{Max}\{\text{PT}_{\mathbf{H}}(A, B) \mid A,B \in \mathbf{H}\}. \quad \textit{So}$$

$$\widehat{K{\times}L} := \text{Max}\{\widehat{\text{PT}}_{\mathbf{H}} \mid \mathbf{H} \text{ a } K{\times}L \text{ house}\} \quad \textit{is}$$

the worst-case over all houses with a given footprint. □

Every $\mathbf{H}$ has $\widehat{\text{PT}}_{\mathbf{H}} \geq [K{-}1] + [L{-}1]$, since that many horizontal+vertical commands are need to unite antipodal corners. In a house with a single path visiting every room, its end rooms are distance $\text{Area}(\mathbf{H}){-}1$ apart. So the minimum time to coalesce those two robots is at least

$$\underbrace{\left\lceil \frac{KL-1}{2} \right\rceil \overset{\text{hence}}{\leq} \widehat{K{\times}L}}_{\substack{\textit{Where is the 2 from?} \\ \textit{Is it necessary?}}}.$$

40.4: ?? Pair-coalescence Time. *What are interesting upper and lower bounds for $\widehat{K{\times}L}$?* ♢

40.5: *MinCW.* (CW = ***Coalescence-Word***.) For a finite house $\mathbf{H}$, use $\text{AT}_{\mathbf{H}}$ for the *minimum* time to coalesce *All* the robots into a single room. [There may be several CWs of this min-length.] □

40.6: ?? House-coalescence Time. By defn, $\text{AT}_{\mathbf{H}} \geq \widehat{\text{PT}}_{\mathbf{H}}$. *Is there an interesting IFF condition for equality? Are there houses where $\text{AT}_{\mathbf{H}} \geq 10 + \widehat{\text{PT}}_{\mathbf{H}}$? Where $\text{AT}_{\mathbf{H}} \geq 10{\cdot}\widehat{\text{PT}}_{\mathbf{H}}$? What is a nt–upper-bound for $\text{AT}_{\mathbf{H}}$?* ♢

40.7: *Defn.* For a N,E,S,W-word π, let $B{\cdot}\pi$ be the room where π would bring a robot from room B. Say that rooms A,B are ***exchangeable*** if $\exists\pi$ st. $A{\cdot}\pi = B$ and $B{\cdot}\pi = A$. House $\mathbf{H}$ is ***universally exchangeable*** if *every* pair A,B is exchangeable. □

40.8: ?? Exchangeable Robots. *Which $K{\times}L$ admit a house with an exchangeable pair $A{\neq}B$? Which $K{\times}L$ admit a universally exchangeable house?* ♢

Solved by: *Mason H.* gave an example of an exchangeable-pair, 2022g.

[Questions await. Solve ho', don't be shmo; get on the Go!]

40.9: *Defn.* A tuple $\vec{\mathcal{A}} := (A_1, \ldots, A_k)$ is ***full*** if the k rooms are distinct. A building [finite or infinite] is ***k-transitive*** if for every two k-tuples $\vec{\mathcal{A}}$ and $\vec{\mathcal{B}}$, each full, there exists a word π st. for every j: $A_j{\cdot}\pi = B_j$.

So "1-transitive" is a synonym for "connected". If a house is 2-transitive then it is certainly universally exchangeable.

A house is ***weakly k-transitive*** if for each two k-sets of rooms, there exists a word carrying one k-set to the other.

A k-***attractor*** is a k-set $\mathcal{A}=\{A_1,\ldots,A_k\}$ to which *every* k-set can be carried. [So "∃ a 1-*attractor*" is a synonym for "*house is coalesceable*".] □

What's a 1 "L" la-ma?	A Tibetan monk.
What's a 2 "L" la-ma?	A South Amerian pack-animal.
What's a 3 "L" la-ma?	A Fire...

Infinite houses

40.10: ?? Word-of-Doom. [***doomed***='non-coalesceable', and ***coal***='coalesceable'.] *Does there exist a* (necessarily ∞) *house, rooms* A, B and word ε [ε for "error"] *s.t:*

> *Pair* (A, B) *is coalesceable, but*
> *pair* $(A{\cdot}\varepsilon,\ B{\cdot}\varepsilon)$ *is doomed?*

Does there exist an ∞*-house with* ∞*ly many coal-pairs, and* ∞*ly many doomed-pairs?* ◊

40.11: ?? Robots in Infinity-House. *With all of* $\mathbb{Z}\times\mathbb{Z}$ *being rooms, with each room having at least 2 walls, produce a pair-coalescable house.* ◊

40.12: ?? Questions/Challenges. *Is every finite house 2-transitive? How about weakly? Produce an* ∞*-house which is 2-transitive. Can you make one which is 3-transitive?* ◊

Iterative/Algorithmic

Iteration can be viewed as a kind of induction. T.fol are "programmable" problems.

41.1: ??Wizard-cards (USAMO 2016.6). *Fix integers* $\mathsf{N}, L \geq 2$. *Cards are labeled* $\mathsf{c}_1, \mathsf{c}_2, \ldots, \mathsf{c}_\mathsf{N}$, *and the deck has* *two* *copies of each. The Wizard shuffles the* $2\mathsf{N}$ *cards and lays them face-down in a row, in places*

$$1,\ 2,\ 3,\ \ldots,\ 2\mathsf{N}{-}2,\ 2\mathsf{N}{-}1,\ 2\mathsf{N}\,.$$

On your turn, you point at L *places.* [*So* $\binom{2\mathsf{N}}{L}$ *possibilities.*] *Wiz turns those cards face-up,* *in place*. *If some two of the revealed-cards match, you have won! Else, you look away, and Wiz returns those cards, face-down, to the* L *places, but permuted in any way he wishes.* [*I.e, you now know the* **set** *of cards in those* L *places, but not their order.*] *Now it is your turn again.*

The game is ***winnable*** *if there exists a posint* $T{=}T_{\mathsf{N},L}$ *and strategy, that is guaranteed to win in at most* T *moves, regardless of Wiz's play.*

Which (N, L) *pairs are winnable?* ◊

Solved by: *Junhao Z.*, 2021t.

42.1: ??? Thirteen coin problem. *Thirteen coins, labeled $1, 2, \ldots, 13$, have standard-weight, except one of them* ***might*** *be heavier or lighter than std-weight (or they could all weigh the same). You also have a std-weight coin, W.*

Available is a scales-of-justice (SOJ) balance. Putting some coins on the left-pan and on the right, either SOJ balances, or tilts left or tilts right.

Using no more than three weighings, determine the coin-situation. ◊

Solved by: ?

42.2: ??? SOJ conundrum. *Consider std-weight coin W, and mystery coins $1, 2, 3, \ldots, \mathbf{C}-1, \mathbf{C}$ which have std-weight* <u>except</u> *one coin* ***might*** *be heavier or lighter.*

Maximize **C** *st. N many clever SOJ weighings can determine the coin-situation.* ◊

The four-year-old niece of a mathematician was playing a game in which she was the conductor on a train and her mother was a passenger.
"Wait a minute," said Nancy, "we have to get some paper to make tickets." "Oh," said her mother, who had probably had a long day, "do we really need them? After all, it's only a pretend game with pretend tickets." "No Mommy, you're wrong," replied Nancy; "they're pretend tickets, but it's a ***real*** game."

–transmitted by *David Gale*

Well-ordered set

See BoP or SaP or Wikipedia for definitions of: total-order, partial-order (both strict and lax), well-ordered set, well-founded poset.

Dictionary-order. Alphabet $\boldsymbol{A} = \{\mathtt{a}, \mathtt{b}, \ldots \mathtt{z}\}$ has $\mathtt{a} \lessdot \mathtt{b} \lessdot \mathtt{c} \lessdot \ldots$ ordering. A ***word*** $\mathbf{w} = w_1 w_2 w_3 \ldots w_L$ has some finite length, L, with each $w_j \in \boldsymbol{A}$.

Let $\boldsymbol{A}^\star$ be the set of *all* words. Define a strict total-order $\prec$ on $\boldsymbol{A}^\star$ by

$$u_1 u_2 u_3 \ldots u_K \prec w_1 w_2 w_3 \ldots w_L$$

IFF *Either*: $K < L$ *and* $u_1 u_2 \ldots u_K = w_1 w_2 \ldots w_K$, [i.e, $\mathbf{u}$ is an ***initial-segment*** of $\mathbf{w}$] *OR:* Words $\mathbf{u}$ and $\mathbf{w}$ disagree at some index *and*, letting $d \leq \text{Min}(K, L)$ be the *smallest* disagreement-index, that $u_d \lessdot w_d$. □

43.1: **???** Dictionary-order conundrum.
Is $(\boldsymbol{A}^\star, \prec)$ *a well-order?*
Is $(\boldsymbol{A}^\star, \succ)$ *a well-order?* ♢

Solved by: ?

44: **???** Well-founded conundrum. *For binrel* $\prec$ *on set* Ω, *define* $\alpha \succ \beta$ *by* $\beta \prec \alpha$.

i: *Suppose both* $(\Omega, \prec)$ *and* $(\Omega, \succ)$ *are strict well-orders. Prove that* Ω *is finite.*

ii: *Weaken* $(\Omega, \prec)$ *and* $(\Omega, \succ)$ *to strict well-founded partial-orders. Prove or give CEX to statement "Set* Ω *is finite."* ♢

Solved by: ?

Snowclones

To X or not to X.

X is the new Y.

In space, no one can hear you X.

It's the mother of all X.

Y-ing while X.

If Eskimos have n words for snow, X surely have m words for Y. [Wikipedia: In 2003, an article in The Economist stated, *"If Eskimos have dozens of words for snow, Germans have as many for bureaucracy."*]

The number you have reached is imaginary. Please rotate your phone 90 degrees and dial again.
–David Grabiner

Complex numbers

The algebraic structure of $\mathbb{R}$ can be consistently extended to a larger field, by adjoining a sqroot of negative 1. This is conventionally[♡4] called $\mathbf{i}$, so $\mathbf{i}^2 = -1 = [-\mathbf{i}]^2$. Extending $\mathbb{R}$ by $\mathbf{i}$ produces field

$$\mathbb{C} := \{x\mathbf{1} + y\mathbf{i} \mid \textit{where } x \textit{ and } y \textit{ are real}\}.$$

[I've written $x\mathbf{1} + y\mathbf{i}$ to emphasize that the additive structure of $\mathbb{C}$ is that of a 2-dimensional $\mathbb{R}$-vectorspace, with basis vectors $\mathbf{1}$ and $\mathbf{i}$. In practice, we write $2+3\mathbf{i}$, not $2\cdot\mathbf{1}+3\mathbf{i}$.]

A geometric picture of $\mathbb{C}$, with the ***real axis*** horizontal, and the ***imaginary axis*** vertical, is called the ***Argand plane*** or the ***complex plane***.

Write ***real-part*** and ***imaginary-part*** extractors as, e.g, for $z := 2 - 3\mathbf{i}$, give

$$\operatorname{Re}(z) = 2 \quad \textit{and} \quad \operatorname{Im}(z) = -3$$

since $z = 2\cdot 1 + [-3]\cdot\mathbf{i}$. The ***absolute-value*** or ***modulus*** of z is its distance to the origin; so

$$|z| = \sqrt{\operatorname{Re}(z)^2 + \operatorname{Im}(z)^2}.$$

[Here, $|2 - 3\mathbf{i}| = \sqrt{4+9} = \sqrt{13}$.] The ***complex conjugate*** of this z is $\overline{z} = 2 + 3\mathbf{i}$. For a general $\omega = x + y\mathbf{i}$ with $x,y \in \mathbb{R}$, observe that

$$\operatorname{Re}(\omega) := x = \tfrac{\omega+\overline{\omega}}{2}, \quad \operatorname{Im}(\omega) := y = \tfrac{\omega-\overline{\omega}}{2\mathbf{i}};$$
$$\overline{\omega} = \operatorname{Re}(\omega) - \operatorname{Im}(\omega)\mathbf{i};$$
$$|\omega|^2 \overset{\text{Pythag. thm}}{=\!=\!=} x^2 + y^2 = \omega\overline{\omega}.$$

(Complex-)conjugation $\omega \mapsto \overline{\omega}$ is an *involution* of $\mathbb{C}$, since $\overline{\overline{\omega}} = \omega$. For complex polynomial $f(z) = \sum_{j=0}^{N} \mathbf{c}_j z^j$, define $\overline{f}(z) := \sum_{j=0}^{N} \overline{\mathbf{c}_j}\, z^j$, its ***conjugate polynomial***. Thus

$$\overline{f(z)} = \overline{f}(\overline{z}),$$

since $\overline{\mu+\nu} = \overline{\mu} + \overline{\nu}$ and $\overline{\mu\nu} = \overline{\mu}\cdot\overline{\nu}$ for $\mu,\nu \in \mathbb{C}$.

Multiplying complex numbers corresponds to multiplying their moduli and adding their angles.

To write a quotient $\frac{\nu}{\alpha}$ in std $x + \mathbf{i}y$ form, note

$$\frac{\nu}{\alpha} = \frac{\nu\overline{\alpha}}{\alpha\overline{\alpha}} = \nu\overline{\alpha}/|\alpha|^2$$

So write $\nu\overline{\alpha}$ in std form, then divide by real $|\alpha|^2$.

See W: Complex number and W: Argand plane for arithmetic with complex numbers.

See Appendix (F) for further $\mathbb{C}$ information.

[♡4] Electrical engineers use $\mathbf{j}$ rather than $\mathbf{i}$, as "i" is used to represent current/amperage in EE. Also, while boldface $\mathbf{i}$ is a sqroot of −1, we still have non-boldface i as a variable. E.g, we *could* [but wouldn't] write $7\mathbf{i} + \sum_{i=3}^{4} i^2 \overset{\text{note}}{=\!=} 7\mathbf{i} + 3^2 + 4^2$.

45.1: **SV** Buried Treasure Problem [BTP]. *Floating in the ocean you spy a bottle containing a pirate's map to fabulous treasure. You sell your possessions, purchase a robot-crewed ocean-catamaran, and sail to the island, discovering it is a* vast *plateau. The map says:*

> *Arrrgh, Matey! Count your paces from the gallows to the a quartz boulder, turn Left 90° and walk the same distance; hammer a gold spike into the ground.*
>
> *Count your paces from the gallows to the giant oak, turn Right 90° and walk the counted distance; hammer a silver spike into the ground.*
>
> *Find Ye Buried Treasure midway between the spikes.*

With joy, you bound up the plateau [with the treasure you can say *bye bye* to *annoying Math classes!*] *and immediately spot the giant oak, and quartz boulder. But the gallows has rotted away without a trace.*

Nonetheless, you find the Treasure. How? ◊

[Hint: Using B, K, w for the Bolder's, oaK's and (unknown) galloWs' location, write the treasure's spot as a fnc $\mathbf{t}_{B,K}(w)$ by using $\mathbb{C}$ addition and multiplication.] Alphabetic-order mnemonic:

*B*oulder	*L*eft	gold
oa*K*	*R*ight	silver

SOLVED BY: *Matthew C, Junhao Z., Hani S.*, 2020t. *Nathan T.*, 2021t.

(*Partial soln*) *Sreeram V.*, 2022g. *Maxime A.*, 2023g.

New 46.1: **??** Telescoping polynomial (USAMO 1977.1). *Determine all pairs of positive integers* (K, N) *such that* $[1 + x^N + x^{2N} + \cdots + x^{KN}]$ *is divisible by* $[1 + x + x^2 + \cdots + x^K]$. ◊

Tiling questions

47: ??IFF Chess-domino-tiling criterion. *Consider a 8×8 chess board with 1 black cell and 1 white cell removed. We seek an IFF-condition, on the removed-pair, for the board to be domino-tilable (by $\frac{62}{2} = 31$ dominos), under the assumption that the board is:*

a: *Toroidal: The top-and-bottom edges connect, and the left-and-right edges connect.*

b: *Cylindrical: Just the the left-and-right edges connect.*

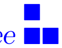
c: *Normal: No edges connect.*

d: *For W,H ∈ $\mathbb{Z}_+$, how does this generalize to W×H board?* ♢

48: ??4mino-tilable rectangles. *A **four-mino** is a 1×4 tile. Which $2N \times 2K$ boards admit a four-mino tiling?* ♢

Solved by: *Keven H.*, 2013t. *Abby T. & Kailey S.*, 2018t.

49: ??N-mino-tilable rectangles. *An **N-mino** is a 1×N tile. For width,height pairs W,H ∈ $\mathbb{Z}_+$, does the W×H board admit an N-mino tiling?* ♢

50: ??Lmino puncture-tilable. *An **Lmino** (pron. "ell-mino") comprises three*  *squares in an "L" shape (all four orientations are allowed).*

*A board is **"Lmino puncture-tilable"** if: No matter which cell is removed, the resulting puntured-board is Lmino tilable.*

Which posint pairs N, K, with $NK \equiv_3 1$, are such that the N×K board is Lmino puncture-tilable? ♢

51: ??Multi-dimensional Lminos. *In class we showed, for each $n \in \mathbb{N}$, that the $2^n \times 2^n$ board is Lmino puncture-tilable.*

Generalize this to a D-dimensional board, $2^n \times 2^n \times \overset{D}{\cdots} \times 2^n$. You will first need to decide what your D-dimensional generalization of an Lmino should be. Are there several reasonable possibilities? ♢

Invariants

Underlying certain problems, is that some *quantity* or some *relation* is preserved under the relevant operations.

***Eg:* Invariant quantity.** Have B be the 8×8 chessboard, but with the lower-right and upper-left cells removed; so $|B| = 62$. We start laying down dominos. Can we cover the board with 31 dominos? *No!*

Why? Initially, the uncovered part of the board (i.e, all of B) has 32 black cells and 30 white cells. These numbers are *not* invariant under placing a domino. But the ***discrepancy***, this difference

$$\dagger: \qquad \#\left\{\begin{matrix}\text{Uncovered}\\ \text{black cells}\end{matrix}\right\} - \#\left\{\begin{matrix}\text{Uncovered}\\ \text{white cells}\end{matrix}\right\},$$

is unaltered by placing a domino —it is invariant. Since the discrepancy is 2 initially, it will *always* be 2, no matter how many dominos we place. But a *covered* board would have a discrepancy of 0, not 2.

***Eg:* Invariant relation.** Our *Lightning bolt alg.* chose "seeds" for the s- and t- columns, so that

$$\ddagger: \qquad r_n = s_n \cdot r_0 + t_n \cdot r_1 ,$$

for $n = 0{,}1$. [The n^{th}: *remainder*, *quotient*, and *Bézout columns* are called r_n, q_n, s_n, t_n.] The LBolt update rule *preserved* relation (‡), in building row n from rows $n-2$ and $n-1$. When we found the index K where $r_K = \text{GCD}(r_0, r_1)$, this invariance handed us the GCD as a linear-combination of r_0 and r_1.

53.1: ?? Coloring a 99-gon (USAMO 1994.2). *Let R,B,Y denote the colors red, blue, yellow, respectively.*

The sides of a 99-gon are initially colored so that, traveling CW (clockwise), consecutive sides are

†: $R,\ B,\ R,\ B,\ \ldots,\ R,\ B,\ R,\ B,\ Y\ .$

Is it possible, still traveling CW, to obtain

‡: $R,\ B,\ R,\ B,\ \ldots,\ R,\ B,\ R,\ Y,\ B$

by a sequence of modifications? A ***modification*** *changes the color of* <u>*one*</u> *side (to one of R,B,Y) under the constraint that at no time may two adjacent sides have the same color.* ♢

SOLVED BY: *Tyler A.*, 2014g. *Christopher P., Nate G.*, 2012g. *Ken D.*, 2017g. *Pietro L.*, 2022t.

Fast is fine; accuracy is final. —*Wyatt Earp*

(Also applies to pickleball)

Rectangle. On a W×W chessboard, cells $\boxed{ABCD}$ form a ***rectangle*** if their coordinates have form (x,y), (x,y'), (x',y'), (x',y), where $x \neq x'$ and $y \neq y'$. [So $A \to B \to C \to D$ is traveling clockwise or counter-clockwise around the corners of a rectangle.] □

54: ??? Chip patterns (USAMO 2015.4). *Poker chips are piled on the cells of a W×W chessboard. Use $^{\#}A$ for the number of chips on cell $A = (x,y)$. The total number of chips on the board is $N \in \mathbb{N}$.*

A ***move*** *chooses a rectangle $\boxed{ABCD}$ that has $^{\#}A$ and $^{\#}C$ both positive. A chip is moved from A to B, and a chip is moved from C to D. The move decrements $^{\#}A$ and $^{\#}C$, and increments $^{\#}B$ and $^{\#}D$.*

Two chip-patterns are ***move-equivalent*** *if there is a sequence of moves carrying one to the other.*

How many move-equivalence classes are there? ♢

Solved by: ?

Stopped at a traffic light, the car in front has vanity plate **ML8ML8**.
What color is the car?

55.1: ?? Pentagon (USAMO 2011.2). *An integer is assigned to each vertex of a regular pentagon so that they sum to 2011. A* ***move*** *of a solitaire game consists of subtracting an integer β from each of the integers at two neighboring vertices and adding 2β to the opposite vertex, which is not adjacent to either of the first two vertices. (The amount β and the vertices chosen can vary from move to move.)*

The game is ***won*** *at a certain vertex if, after some number of moves, that vertex has the number 2011 and the other four vertices have the number 0. Prove that for each choice of the initial integers, there is exactly one vertex at which the game can be won.* ♢

56: ?? Three aces expectation (USAMO 1975.5). *A deck of N playing cards, with three aces, is shuffled "at random" [i.e, the $N!$ many orderings are equally-likely]. The cards are then turned up one-by-one from the top until the second ace appears. Prove that* T, *the expected-number of cards to be turned up, equals* $[N+1]/2$. ◊

SOLVED BY: *Lizzie [Donna] N-C.*, 2017g. *Atharva P.*, 2019t. *Alex T.*, 2021g. *Abhinav P.*, 2023t.

A WONDERFUL BIRD IS THE PELICAN

His bill holds more than his belican.
He can take in his beak,
Enough food for a week,
But I'm damned if I see how the helican.

–Dixon Lanier Merritt

Boomerangs cannot tile a convex polygon

(Problem from David Gale.) A ***boomerang*** is a non-convex quadrilat(eral); call its [$>\pi$] interior-angle "thick". Conversely, a quadrilat with each angle $\le\pi$ (a "thin" angle) is a ***kite***. [So a polygon is convex IFF all its angles are thin.] A dissection of a polygon **P** into *finitely many* quadrilats is a "***quadritiling*** of **P**". [The tiles *need not* be congruent to each other.]

57.1: ??? Boom-Kite Theorem. *Each quadritiling of a convex polygon* **P** *must use a kite.* ◊

57.2: *Fails with "Quad" replaced by "Penta".* Let **P** be the square with vertices $(\pm 2, \pm 2)$. Cut **P** with a polygonal path going from/to

$$(+2,+2) \to (-1,+1) \to (+1,-1) \to (-2,-2)\,.$$

This cuts **P** [which is convex] into two non-convex pentagons [which are congruent to each other].

Exer: Each polygon **Q**, convex or not, admits a (finite) tiling by non-convex *penta*gons. □

Combinatorial Graphs

[Some, but not all, of these problems use induction.]

For these problems, you should draw pictures of your combinatorial graphs.

58.1: *Eg* Gregariousity (USAMO 1982.1). *In a party with 1982 persons, among every group of four there is at least one person who knows each of the other three. What is the minimum number of people in the party who know everyone else?* ◊

Proof. For $N \geq 3$ people, the min-number of ***gregarious*** (someone who knows everyone) people is $N-3$.

Consider the complete graph on N vertices (people); color an edge green/red as the two people do/don't know each other.

WLOG there *is* a red edge $\mathbf{u}$—$\mathbf{v}$. Every other edge $\mathbf{w}$—$\mathbf{x}$ must share a vertex with $\mathbf{u}$—$\mathbf{v}$ [otherwise, the 4-set $\{\mathbf{u},\mathbf{v},\mathbf{w},\mathbf{x}\}$ is ***bad***; nobody knows the other three].

A red-degree–3 vertex is also ruled out; were $\mathbf{u}$—$\mathbf{v}$, $\mathbf{u}$—$\mathbf{v}_2$, $\mathbf{u}$—$\mathbf{v}_3$ distinct edges, then $\{\mathbf{u},\mathbf{v},\mathbf{v}_2,\mathbf{v}_3\}$ would be bad.

Thus, distinct from $\mathbf{u}$—$\mathbf{v}$, the red subgraph has at most two other edges, $\mathbf{u}$—$\widehat{\mathbf{u}}$ and $\mathbf{v}$—$\widehat{\mathbf{v}}$; WLOG it has both. These two edges must *not* be vertex-disjoint, hence $\widehat{\mathbf{u}} = \widehat{\mathbf{v}}$. So Non-gregarious $= \{\mathbf{u},\ \mathbf{v},\ \widehat{\mathbf{u}}=\widehat{\mathbf{v}}\}$. ♦

59: ?? Desegregation problem. *A **coloring** of a graph assigns to each vertex either "aqua" or "red". It is **desegregated**, if each vertex has at least one neighbor of the opposite color from his. [Two vertices are **neighbors** IFF they are connected by an edge.] Prove that each finite connected graph G with $N \geq 2$ vertices, admits a desegregated coloring.* ◊

Hint. This can be done by an *Extremal* or *Induction* argument; can you discover both proofs? (A third proof?) What are generalizations of this graph-theory problem? □

60.1: **??** N-towns Theorem. *Consider a network of $N \geq 1$ towns, each connected to every other town by a one-way*[♡5] *road. Then . . .*

A: *There exists at-least-one universal town. Town α is **universal** if for each other town, β, you can legally bicycle from α to β (possibly passing through intermediate towns).*

SOLVED BY: *John P., 2011t. Zach N., 2012t. Michael E., 2013t. Lizzie [Donna] N-C., 2017g. Noam A. & Riley B. & Caden C., 2020g. Alex T., Nicholas V.N., Allan D., 2021g. Bill Z., 2021t.*

B: *There exists a **2-universal** town; it can access each town using at most two roads [i.e, at most one intermediate town].*

SOLVED BY: *Michael V., Terry T., Alex H., Stephen H., 2011t. Ken D., 2017g. Bill Z., 2021t.*

C: *In a network of $N \geq 3$ towns, it is always possible to reverse at most one road so that, now, every town is universal.*

SOLVED BY: *Ken D., 2017g. Bill Z., 2021t.* ◊

♡5 We have a ***directed graph***; a "***digraph***". This one is a "***complete digraph*** on N vertices"; it has $\binom{N}{2}$ directed-edges, that is, $\frac{1}{2}N[N-1]$ many ***oriented edges***.

61.1: ??Polygamy Problem. *A polygamous community comprises* 100 *women and* 101 *men. Every man has at least one wife. Prove that there is a married couple such that the wife has more husbands than the husband has wives.* ♢

Solved by: *Matthew C.*, 2020t.

Extremal arguments

Here is an example argument.

Defn. [Textbooks vary slightly in their precise defns of ***path***, ***walk***, ***trail***. I will use the defns from Miklos Bona's text.] In a (multi)graph G, a length-N ***trail*** is a sequence

$$\dagger\colon \quad \mathbf{v}_0 \overset{e_1}{—} \mathbf{v}_1 \overset{e_2}{—} \ldots \overset{e_{N-1}}{—} \mathbf{v}_{N-1} \overset{e_N}{—} \mathbf{v}_N\,,$$

where edge e_k runs between vertices $\mathbf{v}_{k-1}$ and $\mathbf{v}_k$ [possibly $\mathbf{v}_{k-1}{=}\mathbf{v}_k$, i.e the edge is a loop]. Edges (hence vertices) may occur more than once.

A ***walk*** is a trail in which no edge is repeated (but vertices may). A ***path*** is a trail in which no vertex is repeated (hence no edge is either).

Say (†) is a trail/walk/path ***between*** $\mathbf{v}_0$ and $\mathbf{v}_N$, or ***connecting*** $\mathbf{v}_0$ and $\mathbf{v}_N$. "Graph G is ***connected***" if each pair of vertices has a trail connected them. □

62: *Ext* ∃ a path. *Fix a connected (possibly infinite) graph G. Then between each two vertices, $\mathbf{u},\mathbf{w} \in \mathbb{V}_G$, there exists a path [no repeated vertices].* ♢

Proof. Fix a *minimun-length* trail (†) between $\mathbf{u}{=}\mathbf{v}_0$ and $\mathbf{w}{=}\mathbf{v}_N$. If there were indices $k{<}\ell$ in $[0\,..\,N]$ with $\mathbf{v}_k = \mathbf{v}_\ell$, then

$$\ddagger\colon \quad \mathbf{v}_0 \overset{e_1}{—} \mathbf{v}_1 \overset{e_2}{—} \ldots \overset{e_k}{—} \mathbf{v}_k{=}\mathbf{v}_\ell \overset{e_\ell}{—} \ldots \overset{e_{N-1}}{—} \mathbf{v}_{N-1} \overset{e_N}{—} \mathbf{v}_N,$$

would be a shorter trail; ⋇. Hence your min-length trail was a path all along.... ♦

Note: The above DESEGREGATION PROBLEM can be done via an extremal argument.

Bashful Boyfriends Story. For a natnum N we have two sets of points, with $|\mathbf{B}| = N = |\mathbf{G}|$, and $\mathbf{B} \cup \mathbf{G}$ comprises $2N$ distinct points.

Set $\mathbf{B}$ comprises the boys' homes, $\mathbf{G}$ the girls' homes. Each boy wants to build a straight sidewalk from his home to his girlfriend's. Boys are bashful, hence don't want to meet other boys when girlfriend-visiting. So the boys want their sidewalks to be disjoint. Indeed, the boys are so bashful that they are willing to change girlfriends in order to not meet another boy.□

63: ?? Bashful Boyfriends. *In the plane, consider sets $|\mathbf{B}| = N = |\mathbf{G}|$, with $|\mathbf{B} \cup \mathbf{G}| = 2N$ and no-three-points-colinear. Then there exists a bijection $\mathcal{D}:\mathbf{B} \hookrightarrow\!\!\!\rightarrow \mathbf{G}$ such that the collection of line-segments $\left\{ \text{Seg}(b, \mathcal{D}(b)) \;\middle|\; b \in \mathbf{B} \right\}$ is pairwise-disjoint.* ◊

[Notation: Boy b's **Date/girlfriend** is $\mathcal{D}(b)$.]

Questions. Can you come up with an extremal proof? An induction proof? Does the result hold if $|\mathbf{B}| = \infty = |\mathbf{G}|$ (the smallest infinity)? Can *no-three-points-colinear* be weakened? □

Number theory

The first few problems can be approached via factoring, or by modular arithmetic.

> *You have to do your own growing no matter how tall your grandfather was.*
> —Abraham Lincoln

64.1: Mod The 14 Problem. *Find all integer-tuples* $\vec{c} := (c_1, c_2, \ldots, c_{14})$ *whose* 4^{th}*-powers satsify*

$$\dagger: \qquad c_1^4 + c_2^4 + \ldots + c_{13}^4 + c_{14}^4 \quad = \quad 31{,}999\,. \qquad \diamondsuit$$

16 *beats up* 14. Trick: Reducing (†) mod-16 gives

$$\ddagger: \qquad c_1^4 + c_2^4 + \ldots + c_{13}^4 + c_{14}^4 \quad \equiv \quad 15\,,$$

where $\equiv$ denotes $\equiv_{16}$. We'll show eqn (†) has <u>*no*</u> soln by showing: *Congruence* (‡) *has no soln.* This latter will follow by proving:

$*$: *Mod*-16, *each* 4^{th}*-power is either* 0 *or* 1.

This is immediate for $\{0, \pm2, \pm4, \pm6, 8\}$, the even residue-classes. Happily, this table,

r	$\langle r^2 \rangle_{16}$	$\langle r^4 \rangle_{16}$
±1	1	1
±3	$9 \equiv -7$	1
±5	$25 \equiv -7$	1
±7	$49 \equiv 1$	1

handles the odd residue-classes. ♦

65.1: ?? Digit-nine (USAMO 1998.1). *The set $\{1, 2, \cdots, 1998\}$ has been partitioned into disjoint pairs $\{a_n, b_n\}$, for $n = 1, \ldots, 999$, so that each absolute-difference $|a_n - b_n|$ is 1 or 6. Prove that sum*

$$S := |a_1 - b_1| + |a_2 - b_2| + \ldots + |a_{999} - b_{999}|$$

ends in the digit 9. ◊

SOLVED BY: *Bill Z.*, 2021t.

66.1: ??? Two linear-recurs (USAMO 1973.2). *Let $\vec{\boldsymbol{x}}$ and $\vec{\boldsymbol{y}}$ denote two sequences of integers defined as follows:*

$$x_0 := 1, \quad x_1 := 1, \quad x_{n+1} := 2x_{n-1} + x_n\,;$$
$$y_0 := 1, \quad y_1 := 7, \quad y_{n+1} := 3y_{n-1} + 2y_n\,.$$

Thus, the first few terms of the sequences are:

$$\vec{\boldsymbol{x}} : 1, 1, \ 3, \ 5, \ 11, \ 21, \ldots$$
$$\vec{\boldsymbol{y}} : 1, 7, 17, 55, 161, 487, \ldots$$

Prove that, except for the "1", there is no term which occurs in both sequences. ◊

Solved by: *Junhao Z.*, 2021t.

Addendum. Could a (possibly complex) number α have sequence $n \mapsto \alpha^n$ satisfy the $\vec{\boldsymbol{x}}$-recurrence [but with possibly different initial conditions]? *Yes!*. This happens exactly (exercise!) when α is a root of polynomial

$$f(t) \;:=\; t^2 - t - 2 \overset{\text{note}}{=\!=} [t-2][t - -1]\,.$$

So $x_n = P \cdot 2^n + Q \cdot [-1]^n$ for numbers P, Q that will be determined from the initial conditions.

Similarly, an α has $n \mapsto \alpha^n$ fulfill the $\vec{\boldsymbol{y}}$-recurrence IFF it is a root of

$$g(t) \;:=\; t^2 - 2t - 3 \overset{\text{note}}{=\!=} [t-3][t - -1]\,,$$

whence $y_n = S \cdot 3^n + T \cdot [-1]^n$ for some numbers S, T.

Solving for P, Q, S, T gives

$$*: \qquad \begin{aligned} x_n \;&=\; \big[2 \cdot 2^n \;+\; [-1]^n\big]/3 \quad \textit{and} \\ y_n \;&=\; 2 \cdot 3^n \;-\; [-1]^n\,. \end{aligned}$$

However, I don't know how to use $(*)$ efficiently to solve the problem. □

67.1: ??? Prime yelling (MC2012.3). *With P an odd-prime, P campers sit around a circle. They are labeled* $\mathbf{C}_1$ [camper #1], $\mathbf{C}_2, \ldots, \mathbf{C}_P$, *in clockwise order. Camper* $\mathbf{C}_1$ *yells out "1". One place clockwise,* $\mathbf{C}_2$ *yells "2". Two places clockwise,* $\mathbf{C}_4$ *yells out "3". Continuing forever, after the camper who yelled "n", the camper n-places clockwise from him now yells "n+1"*

Each yell earns that camper a cookie.

a: *Show there's a camper who never gets a cookie.*

b: *Of the* ***lucky*** *campers* [*those who get a cookie*], *is there one who at some point has at least ten more cookies than the other luckies?*

c: *Among the luckies, is there one who at some point has at least ten fewer cookies than the others?* ◊

Patient: *I've had this recurring dream that I'm a famous psychoanalyst.*
Doctor: *How long has this been going on?*
Patient: *Oh, –ever since I was Jung...*

68.1: ?? $a^2 - b^4$ Problem (HMMT2009.1.alg). *Posints a, b have $a^2 - b^4 = 2009$. Compute $a + b$.* ◊

SOLVED BY: *Yifei L.*, 2017g. *James [Matt] B.*, 2020t. . *Alex T.*, 2021g. *Matthew D.*, 2022g.

69.1: ?? Power-sum Problem. *For each odd $n \geq 3$, the integer $f(n) := \frac{1}{2} \cdot [15^n + 19^n]$ is composite.* ◊

SOLVED BY: *Class of*, 2017g. *Sydney E.*, 2020t. *Allan D., Nicholas V.N., Alex T., Max W.*, 2021g.

70.1: ?? Power-4Term Problem. *For natnum n, define*

$$S_n := 3^n + 7^n + 11^n - 6^n .$$

Prove, for odd posints n, that S_n is composite. ◊

SOLVED BY: *Ken D.*, 2017g. *Sydney E.*, 2020t.

71.1: ?? PoT-plus-Square Question. *(Dis)Prove: There are at least seven primes p such that sum*

$$f(p) := 2^p + p^2$$

is prime. ◊

Non-examples. Note 5 is prime, but $f(5) = 57 = 19 \cdot 3$ is composite. In the other direction, the composite 15 yields $f(15) = 32993$, which is prime. Finally, $f(1) = 3$ is prime but the unit 1, alas, is not. □

SOLVED BY: *Keven H.*, 2013t. *Rabon M.*, 2017g. *Jeremy G. & Emily Y.*, 2022g.

72: ?? The $x + \frac{1}{x}$ theorem. *Consider a real* [or complex] *number x that is **good**; sum $x + \frac{1}{x}$ is an integer. Prove, for each posint N, that x^N is good, i.e, $x^N + \frac{1}{x^N}$ is integral.* ◊

E.g: Let $F := \sqrt{5}$ and $y := \frac{3+F}{2}$. Then $\frac{1}{y}$ equals

$$\frac{2}{3+F} = \frac{2\cdot[3-F]}{9-5} = \frac{3-F}{2} .$$

Hence $y + \frac{1}{y} = \frac{3+F}{2} + \frac{3-F}{2} = 3$, so y is good. The theorem implies that $y^2 \overset{\text{note}}{=\!=} \frac{7+3F}{2}$ is good; *is it*? □

Pf of (72), start. For $N \in \mathbb{N}$, let $S_N := [x^N + \frac{1}{x^N}]$. Now ... [*Hint:* The Appendix defines binomial coeffs.] ♦

SOLVED BY: *John P.*, 2011t. *Junhao Z.*, 2020t. *Allan D.*, 2021g. *Nick K.*, 2021t.

73: ?? Recip-sum-is-one (USAMO 1978.3). *An integer* $\boldsymbol{G}$ *is* ***good*** *if there exist posints* $\sigma_1, \ldots, \sigma_N$ (*not necessarily distinct*) *with*

$$*: \qquad \Big[\sum_{j=1}^{N} \sigma_j\Big] = \boldsymbol{G} \quad \text{and} \quad \Big[\sum_{j=1}^{N} \frac{1}{\sigma_j}\Big] = 1\,.$$

Given that $\boldsymbol{\Gamma} \supset [33\,..\,73]$, *prove that* $\boldsymbol{\Gamma} \supset [33\,..\,\infty)$, *where* $\boldsymbol{\Gamma} \subset \mathbb{Z}_+$ *denotes the set of good numbers.* ◊

SOLVED BY: *Rabon M.*, 2017g.

Defn. Call (∗) a "**(*good*) *decomposition*** of $\boldsymbol{G}$". □

74.1: ?? Squarish problem. *Call* $\vec{\boldsymbol{\varepsilon}} = (\varepsilon_1, \ldots, \varepsilon_L)$ *an* ***L-bit-tuple*** *if each* ε_k *is* +1 *or* −1. *Integer* T *is* ***squarish*** *if there exists a natnum* L *and an* L*-bit-tuple* $\vec{\boldsymbol{\varepsilon}}$ *st.*

$$T \quad = \quad \sum_{k=1}^{L} \big[\varepsilon_k \cdot k^2\big]\,.$$

Prove that every integer is squarish. ◊

SOLVED BY: *John P.*, 2011t.

75a: ??? 2-to-2 Problem (USAMO 1991.3). *Sequence*

$$\vec{\boldsymbol{b}} \quad := \quad (1, 2, 2^2, 2^{[2^2]}, 2^{\left[2^{[2^2]}\right]}, \ldots)$$

can be recursively defined as

$$b_0 := 1, \quad \text{and} \quad b_{t+1} := 2^{b_t},$$

for $t = 0, 1, 2, \ldots$. *Then for each modulus* M, *sequence* $\vec{\boldsymbol{b}}$ *is eventually mod-*M *constant.* ◊

76: ??? Odd-divisor Fibonacci (USAMO 1993.4). *Arbitrary posints f_0 and f_1 determine an* ***oddish*** *sequence $\vec{\boldsymbol{f}}$, defined thereafter by letting f_n be the largest odd divisor of $f_{n-2} + f_{n-1}$.*

Prove that $\vec{\boldsymbol{f}}$ is eventually-constant, and determine what this constant $C = C(f_0, f_1)$ is. ◊

Remark. Given a posint $F = 2^e \cdot D$, where $e \in \mathbb{N}$ and D is odd, define $[\![F]\!]$ to be this D. Thus

$$[\![f_{n-2} + f_{n-1}]\!] \quad =: \quad f_n$$

is the update rule. □

77a: ??? Integer-product seq. Thm (USAMO 2009.6).
Suppose $\vec{s} = (s_0, s_1, s_2, \ldots)$ *is an infinite, nonconstant sequence* [i.e, *not* $s_0 = s_1 = s_2 \cdots$] *of rational numbers. Suppose* $\vec{t}$ *is also an infinite, nonconstant, rational sequence with the property that*

†: *For all* j *and* k: Product $[s_j - s_k] \cdot [t_j - t_k]$ is an integer.

Prove that there exists a rational number $r \neq 0$ *st.*

‡: *For all* j *and* k: Values $[s_j - s_k]/r$ and $[t_j - t_k] \cdot r$ are integers. ◊

Hard 78.1: ??? Power-of-Two composite (USAMO 1982.4).
Prove that there exists a positive integer $\boldsymbol{k}$ *such that* $\mathsf{V}_n := 1 + \boldsymbol{k}\cdot 2^n$ *is composite for every posint* n. ◊

[*Ideas:* Covering-systems. Mod-arithmetic.]

79.1: *Example.* The set of ***Threeish-numbers*** is

$$\mathcal{T} := \{1, 4, 7, 10, \ldots\} = \{n \in \mathbb{Z}_+ \mid n \equiv_3 1\} .$$

Ok, so $\mathcal{T}$ is not a ring. But $\mathcal{T}$ is sealed under multiplication, has no ZDs, and the only $\mathcal{T}$-unit is 1; we can make sense of "$\mathcal{T}$-irreducible" and "$\mathcal{T}$-prime".

Factoring 100, these two Threeish-factorizations

$$4 \cdot 25 = 100 = 10 \cdot 10 ,$$

show that none of 4, 10, 25 is Threeish-prime. Yet each *is* Threeish-irreducible. [This, as their only non-trivial $\mathbb{N}$-factorizations use non-Threeish numbers]. □

79.2: ?? Threeish conundrum. *Given a "target" $\mathsf{T} \in [2 .. \infty)$, write its usual $\mathbb{N}$-prime factorization,*

79.3: $$\mathsf{T} = p_1^{E_1} \cdot p_2^{E_2} \cdot \ldots \cdot p_L^{E_L} ,$$

with $p_1, \ldots, p_L$ distinct, and each E_ℓ a posint.

In terms of (79.3), give an IFF-characterization of:

i: *When T is Threeishian.*

ii: *When T is Threeish-irreducible.*

iii: *When T is Threeish-prime.*

iv: *Are there ∞ly many Threeish-primes? –or any at all?* [*Hint:* Look up Dirichlet's thm on arith.-progressions.] ◊

SOLVED BY: *Keven H.*, 2013t.

Calculus ideas

80.1: ?? Tan-of-Sum (HMMT2009.4.gen). *Angles x, y satisfy that*

$$\tan(x) + \tan(y) = 4, \quad \text{and} \quad \cot(x) + \cot(y) = 5.$$

Compute $\tan(x+y)$. ♢

Solved by: *Ken D.*, 2017g. *Hani S.*, 2020t. *Alex T.*, 2021g.

There's a delta for every epsilon

It's a fact that you can always count upon.
There's a delta for every epsilon
And now and again,
There's also an N.

But one condition I must give:
The epsilon must be positive
A lonely life all the others live,
In no theorem
A delta for them.

How sad, how cruel, how tragic,
How pitiful, and other adjec-
Tives that I might mention.
The matter merits our attention.
If an epsilon is a hero,
Just because it is greater than zero,
It must be mighty discouragin'
To lie to the left of the origin.

This rank discrimination is not for us,
We must fight for an enlightened calculus,
Where epsilons all, both minus and plus,
Have deltas
To call their own.

Words and Music by: —*Tom Lehrer*

Video of Lehrer performing the δ-ε song.

Lyrics, and audio of Lehrer performing.

81: ?? Factorial-cosine limit (*Domain specific*). *With n taking on values $1, 2, 3, \ldots$, prove that limit*

$$L := \lim_{n\to\infty} \cos(n! \cdot 2\pi e)$$

exists, and compute it. ♢

Solved by: *Daniel B. & Rabon M.*, 2017g. *Nick K.*, 2021t.

Eating too much cake is the sin of gluttony, whereas Eating too much pi is a-ok, as the sin of pi is zero.

82.1: ?? Graph-chords (*Induction*). *Function $f:[0,1]\to\mathbb{R}$ is **good** if $f(0)=f(1)$ and f is continuous. Length $\Lambda\in(0,1]$ is a **"chord** of f**"** if there exists points $0 \le w < x \le 1$ with $f(w)=f(x)$ and $w+\Lambda = x$.*

*Our Λ is a **universal chord**, **UC**, if every good function has Λ as a chord; by defn, length 1 is a UC.*

Prove that each harmonic number, $1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \ldots$, is universal. [An induction idea can work here.] ◊

Solved by: *Bill Z. & Alejandro T.*, 2021t.

Now we seek to establish the converse:

Creative 82.2: ??? Graph-chords, converse. *Prove that a universal chord must be a harmonic number.* ◊

Solved by: ?

Misc. Problems

These problems are "straightforward" *given* the right tools, e.g, calculus, binomial coeffs, algebra identities, complex numbers. [In contrast, some of the hidden problems –that I reveal as you solve these– are challenging.]

Easy 83.1: ?? Can you spot the frog? *Fred-the-frog jumps on* $\mathbb{N}=\{0,1,2,\ldots\}$, *with unknown hop-length* $h\in\mathbb{Z}_+$. *At time* $t \in \mathbb{N}$, *our friendly frog is at integer* $t\cdot h$.

At time $t = 1, 2, 3, \ldots$, *you shine a spotlight at position* $\mathbf{F}(t)\in\mathbb{Z}_+$; *if the frog is there at time* t, *then you've caught him. Prove that there is a fnc* $\mathbf{F}:\mathbb{Z}_+\to\mathbb{Z}_+$ *which catches Fred, regardless of his hop-length.* ◊

Solved by: *Sienna N. & Patrick O.*, 2019t. *Junhao Z.*, 2020t. *David R., Aubrey S. & Haritha K.*, 2021g. *Kevin J.*, 2022g. *Alexa M.*, 2022t.

83.2: ?? More lily pads. *Now Fred jumps on* $\mathbb{Z}$, *with non-zero hop-length* $h\in\mathbb{Z}$. *He starts at lily-pad* $\ell\in\mathbb{Z}$. *At time* t, *doomed Fred is on pad* $\ell + [th]$.

Although both ℓ *and* h *are unknown, show there exists a Fred-catcher* $\mathbf{G}:\mathbb{Z}_+\to\mathbb{Z}$. [*I.e,* $\mathbf{G}$: *Time*→*Space*.]

Prove or disprove: *There exists a Fred-catcher* $\mathbf{M}:\mathbb{Z}_+\to\mathbb{Z}$ *with this* ***weak-monotonicity***:

$*$: *For all times* $t \le u$ *we have* $|\mathbf{M}(t)| \le |\mathbf{M}(u)|$. ◊

Solved by: *Junhao Z.*, 2020t.

(A third problem awaits...)

How to punctuate `help spot the giraffe`.

Help spot the giraffe. [Locate the giraffe.]

Help spot the giraffe. [Help me put spots on the giraffe.]

Help Spot, the giraffe. [We need to go to Spot's aid.]

Help Spot! –the giraffe! [My dog Spot will protect me from this crazy giraffe!]

Help! —Spot the giraffe [(signed) giraffe named Spot, desperately requesting aid.]

Malaphor

That's the way the cookie cries over spilled milk.

Easy 84.1: ?? Counting idempotent fncs. *Consider a set Γ of cardinality $N := |\Gamma| \in \mathbb{Z}_+$. A map $h:\Gamma\to\Gamma$ is **idempotent** if $h \circ h = h$. Give a formula for I_N, the number of idempotent-maps. Compute I_5.* ♢

[*Ideas:* Get a formula ITOf binomial-coefficients.]

Easy-ish 85.1: ??? Circularly-composite (USAMO 2005.1). *Determine all composite positive integers β for which it is possible to arrange the non-one (positive) divisors of β in a circle, so that no two adjacent divisors are relatively prime.* ♢

Convenience. Use ***bigdiv*** for "*non-one divisor*". E.g, the bigdivs of 6 are $2, 3, 6$,

Use ***blip*** for integer≥2. Blip $\boldsymbol{\beta}$ is ***good*** if its bigdivs can be circularly arranged with adjacent-pairs not coprime. For example, 12 is good as it admits (good) cycle $\circlearrowleft 2, 6, 3, 12, 4 \circlearrowright$. □

86.1: ?? Irreducible fraction. *For each natnum n, prove that fraction $\frac{21n+14}{14n+9}$ is irreducible.* ♢

Contrast. Is $R_n := \frac{17n+14}{2n+9}$, always irreducible? Alas, $R_8 = \frac{136+14}{16+9} = \frac{150}{25}$ which *is* reducible. □

Solved by: ? Morgan F. & Sydney E., 2020t. Alex T. & Nicholas V.N. & Haritha K., 2021g.

Puzzle: *There are twelve boxes, one of which contains fabulous riches, and eleven of which contain goats. There is also a large balance, on which you can weigh the boxes. The balance is surrounded by 53 bicycles. Three Monty Halls, one of whom always tells the truth, one of whom always lies, and one of whom answers randomly, will answer a single question. All three say, "I do not know the two numbers", and then look at one another.*

What happened to the other dollar?

–*Ken Kaufman*

87.1: ?? Coefficient-Sum (HMMT2009.2.algebra). *Let* S *be the sum of all the real coefficients of the expansion of* $[1+\mathbf{i}x]^{2009}$. *What is* $\log_2(S)$ *?* ◊

SOLVED BY: *Ken D.*, 2017g. *James [Matt] B.*, 2020t. *Alex T.*, 2021g.

88.1: ?? Reciprocal Sum (HMMT2009.5.algebra). *With* A, B, C *denoting the roots of cubic* $f(x) := x^3 - x + 1$, *compute the sum*

$$\frac{1}{A+1} + \frac{1}{B+1} + \frac{1}{C+1}\,.$$ ◊

SOLVED BY: *Yifei L.*, 2017g. *Nicholas V.N. &, Max W., Alex T., Haritha K.*, 2021g.

89.1: ??? Does $a + 2b$ cover? (USAMO 1996.6). *Determine whether there exists a subset* $\mathbf{X} \subset \mathbb{Z}$ *satisfying:*

> *For each* $\tau \in \mathbb{Z}$ *there is exactly one solution to* $a + 2b = \tau$ *with* $a,b \in \mathbf{X}$. ◊

Removing Foliage

90a: ?? Polynomial-deriv-divisible (Putnam 2016.A1). *Find the smallest natnum* J *such that for every intpoly* $p()$ *and for every* $\mathbf{k} \in \mathbb{Z}$, *the integer*

$$*: \qquad p^{(J)}(\mathbf{k}) \qquad \left[\begin{array}{l}\textit{The } J\textit{-th derivative} \\ \textit{of } p(), \textit{ evaluated at } \mathbf{k}.\end{array}\right]$$

is divisible by 2016. ◊

Solved by: *Rabon M.*, 2017g.

Taylor D. & Hunter R., 2019t.

Alex T., 2021g.

> **zucchini**, n.: *What stylish menagerie animals wear to the beach.* –*JK*

Counting/Probability

Sometimes we have a finite non-void set Ω, a "***good***" subset $G \subset \Omega$. We pick an $\alpha \in \Omega$ "*at random*", i.e, with uniform probability. The probability of α being good is ratio $|G|/|\Omega|$. Often we wish to compute cardinality $|G|$ or to lower-or-upper bound it. To show that *two* subset $G,H \subset \Omega$ have the same probability, sometime we can produce an explicit bijection $G \hookrightarrow\!\!\!\rightarrow H$.

In probability theory, the term ***expected value*** means "average value". E.g, if you roll a fair die, it takes on the values $1, \ldots, 6$ equi-probably, so its expected value (***expectation***) is $\frac{1+2+3+4+5+6}{6} = 7/2$.

Earlier problems in these notes using related ideas: Scheherazade's Stratagem, Three aces expectation.

Easy-ish **91.1: ???** Disjoint Triangles (USAMO 1983.1). *On a circle, six points A, B, C, D, E, F are chosen at random, independently and uniformly w.r.t arclength. Determine the probability that triangles ABC and DEF are disjoint.* ♢

Easy-ish **92.1: ???** Lattice-walk three (HMMT2019.5.Feb.Comb). *Contessa is taking a random lattice walk in the plane, starting at $(1, 1)$. [A random lattice-walk moves* up, down, left, *or* right *1 unit equi-probably at each step.] If she lands on a point of form $(6x, 6y)$ for $x,y \in \mathbb{Z}$, she Wins!; but if she lands on a point of form $(6x+3, 6y+3)$ she Loses. What is her probability, G, of winning?* ♢

93.1: ?? Expected Backtrack (HMMT 2020.7 Nov., Team). *Bob the ant walks on the coordinate plane, starting at* $(0,0)$. *Every second, he moves from one lattice point to a different lattice point at distance* 1, *chosen equi-probably, independently. He continues until he* ***backtracks****, reaching a point he could have reached sooner. E.g, walking* $(0,0)\to(1,0)\to(1,1)\to(1,2)\to(0,2)$, *he will stop at* $(0,2)$ *because he could have traveled* $(0,0)\to(0,1)\to(0,2)$. *Compute* $\mathbf{E}$, *Bob's expected-number of steps before stopping.* ◊

SOLVED BY: *Junhao Z. & Hani S.*, 2021t.

94: ??? Zero mod-3 (USAMO 1979.3). *From integers $k_1, k_2, \ldots, k_N$, a term α is picked at random. A 2nd term, β, is randomly picked, independently of the first. Then a third, γ. Prove the probability that $\alpha + \beta + \gamma$ is divisible by 3 is at least $\frac{1}{4}$.* ◊

[*Ideas:* Let x,y,z be probability that a term chosen from $k_1, k_2, \ldots, k_N$ has mod-3 residue $0, 1, 2$, respectively. Compute the desired probability ITOf x,y,z, then use calculus to minimize that expression over the appropriate set of (x, y, z) triples.]

95.1: ??? Collapse-abc (HMMT 2020.7 Feb., Comb). *Alice writes* 1001 *letters on a blackboard, each one chosen independently and uniformly at random from the set* $S := \{\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c}\}$. *A move consists of erasing two distinct letters from the board and replacing them with the third letter in* S. *What is the probability that Alice can perform a sequence of moves which results in one letter remaining on the blackboard?* ♢

Challenging misc. Problems

96.1: ?? Poly-permutation (USAMO 1974.1). *With* A,B,C *three distinct integers, let f denote a polynomial having integral coefficients. Show it is impossible that* $f(\mathsf{A})=\mathsf{B}$, $f(\mathsf{B})=\mathsf{C}$, *and* $f(\mathsf{C})=\mathsf{A}$. ◊

SOLVED BY: ?, Semester.

Exploration? Does such an f exist if we allow it to be a $\mathbb{Q}$-poly, rather than $\mathbb{Z}$-poly?

Or, keeping f a $\mathbb{Z}$-poly but allowing A,B,C to be rational, does that admit a soln? □

97.1: ??? Decimal divisibility (USAMO 1988.1). *The repeating decimal* $0.ab\cdots k\overline{pq\cdots u}$ *equals* $\frac{\alpha}{\beta}$, *where* $\alpha \perp \beta$ *are posints, and –necessarily– there is at least one decimal before the repeating-part. Prove* β *is divisible by* 2 *or* 5 (*or both*).

[*E.g:* $0.011\overline{36} = 0.01136363636\cdots = \frac{1}{88}$, *and* $88 \mid\!\bullet\, 2$.] ◊

Challenging 98: **??** Multiplicative-coloring (USAMO 2015.3). *A **blip**, B, is a subset of **token-set** $\{1, 2, \ldots, N\}$, where $N \geq 1$. A **coloring** colors each blip either green or red (not both). Let $g(B)$ count the green sub-blips of B,*

*Determine $\Lambda(N)$, the number of **legal-colorings**; those which satisfy*

†: $\forall$ blips B,C: $g(B)\,g(C) \;=\; g(B \cup C)\,g(B \cap C)$. ◊

99: ??Chessboard-config Problem. *In some order, put the numbers* $1, 2, \ldots, 64$ *on the cells* (squares) *of a chessboard; call this a* ***configuration****. For a cell* α*, let* $\alpha_{\mathbf{G}}$ *denote the number placed there by* $\mathbf{G}$*. Two cells* α, β *are* ***adjacent*** *if they touch vertically, horizontally or diagonally. Define the worst-case difference,*

99a: $$\widehat{\mathbf{G}} := \text{Max}\left\{ |\alpha_{\mathbf{G}} - \beta_{\mathbf{G}}| \;\middle|\; \begin{array}{l}\text{Cells } \alpha \text{ and } \beta \\ \text{are adjacent.}\end{array} \right\}$$

What is the minimum (taken over all configurations $\mathbf{G}$) *of* $\widehat{\mathbf{G}}$*?* ♢

As Rousseau could not compose without his cat beside him, so I cannot play chess without my king's bishop. In its absense the game to me is lifeless and void. The vitalizing factor is missing, and I can devise no plan of attack. –Siegbert Tarrasch

I had a toothache during the first game. In the second game I had a headache. In the third game it was an attack of rheumatism. In the fourth game, I wasn't feeling well. And in the fifth game? Well, must one have to win every game?
–Siegbert Tarrasch

100.1: ??? Hexagonal Game (USAMO 2014.4). *Abby and Bert play the* ***"k-game"*** *on an infinite hexagonal grid which, initially, is unmarked. Players alternate, with Abby moving first. Abby marks two adjacent unmarked hexagons. Bert then unmarks some marked hexagon* (anywhere on the board)*. If ever there are k consecutive marked cells in a line* (a ***k-chain***)*, then Abby wins. Find the min value of k for which Abby cannot win,* or *prove that no such minimum exists.* ♢

101.1: ??? Averaging polynomials (USAMO 2002.3). *Fix natnum K. A* ***good*** *polynomial is monic with real coefficients, and has degree-K. Prove that each good $\mathbf{F}(x)$ is the average of two good polynomials with all real roots.* ♢

Never criticize a man until you've walked a mile in his shoes...

102.1: ?? Rational 6×6 grid (USAMO 2004.4). *Alice and Bob play a game on a 6×6 grid. On his turn, a player chooses a rational number not yet in the grid and writes it in an empty cell (i.e, square) of the grid. Alice starts, then players alternate. After all cells have numbers: In each row, color black the cell with the greatest number in that row.*

Alice wins if she can draw a (polygonal) line from the top of the grid to the bottom of the grid that stays in black cells; Bob wins if she can't. [Defn: Two cells in adjacent rows are ***connected*** *IFF they share a vertex.] Find, with proof, a winning strategy for one of the players.* ◊

*... for then, you are a mile away —**and**, you have his shoes.*

103.1: ⁇ 7-5-Prob. *For* $n = 0, 1, \ldots$, *let* $\mathbf{C}_n := 7^n + 5^n$.

Produce a simple formula so that, for coprime natnums $L \geq K$,

$$\mathrm{GCD}(\mathbf{C}_L, \mathbf{C}_K) = \mathit{SimpleFormula}(L, K).$$

[*Guessing a formula may be easy; our goal is a proof!*] ◊

Valiant polynomial. A polynomial f is ***valiant***♡6 if $[w \in \mathbb{Z}] \Rightarrow [f(w) \in \mathbb{Z}]$. Define the k^{th} ***binomial polynomial***

$$\mathcal{B}_K(x) := \frac{x[x-1][x-2]\cdots[x-[K-1]]}{K!},$$

which we can think of as $\binom{x}{K}$.

104.1: ⁇ Binomial-polys are Valiant. *For each* $K \in \mathbb{N}$, *polynomial* $\mathcal{B}_K$ *is valiant.* ◊

104.2: ⁇ Valiants are lin-combs. *Each valiant poly* f *can be written as a finite linear-combination, with integer coefficients, of the binomial polys.* [I.e, $\{\mathcal{B}_k\}_{k=0}^{\infty}$ *is a* $\mathbb{Z}$*-basis for* VALIANT.] ◊

♡6 I.e, its ***VAL***ues are ***INT***egers.

105.1: ?? Half-intersection Problem. *Consider a set* Λ (***tokens***) *with* $|\Lambda| = 4028$, *along with subsets* (***blips***) $\mathrm{B}_1, \mathrm{B}_2, \ldots, \mathrm{B}_{2014} \subset \Lambda$, *where each* $|\mathrm{B}_j| = 2014$. *Prove that there exist distinct indices* i,j *with*

$$|\mathrm{B}_i \cap \mathrm{B}_j| \geq 1007\,.$$

◊

SOLVED BY: *Hani S.*, 2021t.

106.1: ?? Polynomial fit (USAMO 1975.3). *Fix* $\mathcal{N} \in \mathbb{Z}_+$ *and* $J := [0\,..\,\mathcal{N})$. *Let* $P()$ *denote the unique polynomial st.* $\mathrm{Deg}(P) \leq \mathcal{N}-1$ *and*

$$\dagger: \quad \forall k \in J: \quad P(k) = \frac{k}{k+1}\,.$$

Determine the value of $P(\mathcal{N})$. ◊

SOLVED BY: *Daniel S.*, 2019t.

Attempting to park at any major university
–as anyone who has tried to do it will tell you–
is the *10th-ring of torment* in *Dante's Inferno*.

Defn. The ***geometric-mean*** of a set of m non-negative numbers is the m^{th}-root of their product. □

107.1: ?? Integral geometric-mean (USAMO 1984.2). *A subset $\mathcal{G} \subset \mathbb{N}$ is **good** if: The geometric-mean of each (non-void) finite subset of $\mathcal{G}$ is an integer.*

i: *Which posints N admit a good-set of cardinality N? (Such an N is also called **good**.)*

ii: *Is there an infinite good set?* ◊

108.1: ?? Heart-isomorphism. *The $f(x) := 2^x$ map, from $\mathbb{R} \to \mathbb{R}_+$, is a group-isomorphism from $(\mathbb{R}, +, 0)$ onto $(\mathbb{R}_+, \cdot, 1)$. More than a group, the reals form a ring. So f carries this ring*

$$(\mathbb{R},\ +, 0,\ \bullet,\ 1) \quad \text{to a ring,}$$
$$(\mathbb{R}_+, \cdot, 1,\ \heartsuit,\ @)\,,$$

where $\heartsuit$ is a binary operation on $\mathbb{R}_+$, and $@$ is an element of $\mathbb{R}_+$.

What is $@$? And what is the $\heartsuit$ binop? What does $5 \heartsuit 8$ equal? ◊

Solved by: *James [Matt] B.*, 2020t.

King's bad proofs

Here are problems where I did not find an elegant soln, and hope some student can find a more elegant one.

> *To a man who has only a hammer, every problem looks like a nail.* —*Mark Twain* (paraphrased)

109.1: ?? Non-negative polynomial. *On $\mathbb{R}^3$, prove that*

$$\dagger: \quad f(x,y,z) \;:=\; z^6 + x^4y^2 + x^2y^4 - 3x^2y^2z^2\,.$$

is non-negative. ◊

Solved by: *Junhao Z. & Hani S.*, 2021t. *Jeremy G. & Emily Y.*, 2022g.

Student-created conundra

Can you solve your colleagues' challenges?

Notation. For sets $U,A \subset \mathbb{R}$, say "*U* ***avoids*** *A*", written $U \ltimes A$, if: $\forall x,y \in U$: $x+y \notin A$.

110: ??? Sam's Avoidance Problem. *Does there exist an uncountable U with $U \ltimes \mathbb{Q}$?* Prove or give CEX. ◊

Cardinality problems

111.1: ?? Infinite hats. *An infinite set, $\mathbb{P}$, of people, play a game; they either all win, or all lose. At midnight, a white hat or a red hat will appear (Star Trek transporter?) on each person's head. Each sees the color of everyone else's hat, but he cannot see his own hat. Simultaneously, each yells out a guess of his hat-color.*

RESULT: *If ∞ly many are incorrect, then the team loses. If only finitely-many are wrong, then the team wins.*

THE PROBLEM: *They are told the rules in advance. Either prove there is a method for them to win, or else prove that there is no such method.* ◊

Temporary addition to SeLoNotes:

A denumerable set $\mathbf{P} := \{\mathsf{p}_1, \mathsf{p}_2, \mathsf{p}_3, \ldots\}$ of people play a game; they either all win, or all lose. At midnight, a White hat or a Red hat magically appears on each person's head. Each sees the color of everyone else's hat, but he cannot see his own hat. Simultaneously, each yells out a guess of his hat-color.

NOTATION: With W:=White, R:=Red, and color-set $\mathbf{C}:=\{\mathsf{W},\mathsf{R}\}$, the **Color-maps** set is $\mathbf{C}^{\mathbf{P}}$. For color-map $f \in \mathbf{C}^{\mathbf{P}}$, value $f(n)$ is color of hat that f puts on p_n.

Use $\widehat{\mathsf{W}} := \mathsf{R}$ and $\widehat{\mathsf{R}} := \mathsf{W}$.

Let f_N^{Flip} be the color-map h which: *Has* $h(N) = \widehat{f(N)}$, *and has* $h(k){=}f(k)$ *for each* $k \in \mathbf{P} \smallsetminus \{N\}$.

Use $\mathcal{A}(n,f)$ for the color p_n Announces (his "guess") for his hat-color, when the actual color-map is f. *The condition that an announcing scheme $\mathcal{A}$ can not have a person's guess depend on his hat-color, is this:*

†: *For each* $n{\in}\mathbf{P}$ *and each* $f{\in}\mathbf{C}^{\mathbf{P}}$, *the scheme has* $\mathcal{A}(n, f_n^{\mathit{Flip}}) = \mathcal{A}(n,f)$.

Every announcing-scheme $\mathcal{A}$ you use must satisfy (†). You may use the AXIOM OF CHOICE in any of your arguments.

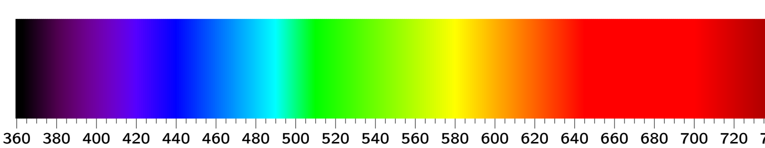
i If ∞ly many are incorrect, then the team loses. If only finitely-many are wrong, then the team wins.

Prove there is a method for the team to always win. You may use the Axiom of Choice: Suppose $\mathcal{F}$ is a collection of **non-void** sets. Then there exists a ***choice function*** $\mathfrak{C}$ mapping $\mathcal{F}$ into $\bigcup_{A\in\mathcal{F}} A$ st. $\mathfrak{C}(A) \in A$, for each $A \in \mathcal{F}$.

ii The rules have changed. Now, the team wins only if no more than 50 people guess wrong.

Prove there *no method* guaranteeing a win. [*Hint:* Given a guessing scheme $\mathcal{A}$, can you use PHP to show there is coloring f causing more than 50 people to guess wrong.]

iii A kind of converse to (ii): *For each posint N: Prove $\exists$ scheme $\mathcal{A}_N$ so that for each color-map f, at most $\lceil \frac{N}{2} \rceil$ among $\{\mathsf{p}_1, \mathsf{p}_2, \ldots, \mathsf{p}_N\}$ guess wrong.* [NB: $\mathbf{P}$ is still *infinite*.]



Difficulties mastered are opportunities won.
—Winston Churchill

§A Appendix: Notation

Number Sets. Expression $k \in \mathbb{N}$ [read as "k is an element of $\mathbb{N}$" or "k in $\mathbb{N}$"] means that k is a natural number; a ***natnum***. Expression $\mathbb{N} \ni k$ [read as "$\mathbb{N}$ ***owns*** k"] is a synonym for $k \in \mathbb{N}$.

$\mathbb{N}$ = natural numbers $= \{0, 1, 2, \dots\}$.

$\mathbb{Z}$ = integers $= \{\dots, -2, -1, 0, 1, \dots\}$. For the set $\{1, 2, 3, \dots\}$ of positive integers, the ***posints***, use $\mathbb{Z}_+$. Use $\mathbb{Z}_-$ for the negative integers, the ***negints***.

$\mathbb{Q}$ = rational numbers $= \{\frac{p}{q} \mid p \in \mathbb{Z} \text{ and } q \in \mathbb{Z}_+\}$. Use $\mathbb{Q}_+$ for the positive rationals and $\mathbb{Q}_-$ for the negative rationals.

$\mathbb{R}$ = reals. The ***posreals*** $\mathbb{R}_+$ and the ***negreals*** $\mathbb{R}_-$.

$\mathbb{C}$ = complex numbers, also called the ***complexes***.

For $\omega \in \mathbb{C}$, let "$\omega > 5$" mean "ω *is **real** and* $\omega > 5$". [Use the same convention for $\ge, <, \le$, and also if 5 is replaced by any real number.]

Use $\overline{\mathbb{R}} = [-\infty, +\infty] := \{-\infty\} \cup \mathbb{R} \cup \{+\infty\}$, the ***extended reals***.

An "***interval of integers***" $[b .. c)$ means the intersection $[b, c) \cap \mathbb{Z}$; ditto for open and closed intervals. So $[\mathrm{e} .. 2\pi] = \{3, 4, 5, 6\} = [3 .. 6] = (2 .. 6]$. We allow b and c to be $\pm\infty$; so $(-\infty .. -1]$ is $\mathbb{Z}_-$. And $[-\infty .. -1]$, is $\{-\infty\} \cup \mathbb{Z}_-$.

Floor function: $\lfloor \pi \rfloor = 3$, $\lfloor -\pi \rfloor = -4$. Ceiling fnc: $\lceil \pi \rceil = 4$. Absolute value: $|-6| = 6 = |6|$ and $|-5 + 2\mathrm{i}| = \sqrt{29}$.

Mathematical objects. Seq: '*sequence*'. poly(s): '*polynomial(s)*'. irred: '*irreducible*'. Coeff: '*coefficient*' and var(s): '*variable(s)*' and parm(s): '*parameter(s)*'. Expr.: '*expression*'. Fnc: '*function*' (so ratfnc: means rational function, a ratio of polynomials). trnfn: '*transformation*'. cty: '*continuity*'. cts: '*continuous*'. diff'able: '*differentiable*'. CoV: '*Change-of-Variable*'. CoI: '*Constant of Integration*'. LoI: '*Limit(s) of Integration*'. RoC: '*Radius of Convergence*'.

Soln: '*Solution*'. Thm: '*Theorem*'. Prop'n: '*Proposition*'. CEX: '*Counterexample*'. eqn: '*equation*'. RhS: '*RightHand side*' of an eqn or inequality. LhS: '*lefthand side*'. Sqrt or Sqroot: '*square-root*', e.g, "the sqroot of 16 is 4". Ptn: '*partition*', <u>*but*</u> pt: '*point*' as in "a fixed-pt of a map".

Binop: '*Binary operator*'. Binrel: '*Binary relation*'.

FTC: '*Fund. Thm of Calculus*'. IVT: '*intermediate-Value Thm*'. MVT: '*Mean-Value Thm*'.

The ***logarithm*** function, defined for $x>0$, is $\log(x) := \int_1^x \frac{\mathrm{d}v}{v}$. Its inverse-fnc is $\exp()$.

For $x>0$, then, $\exp(\log(x)) = x = \mathrm{e}^{\log(x)}$. For real t, naturally, $\log(\exp(t)) = t = \log(\mathrm{e}^t)$.

PolyExp: '*Polynomial-times-exponential*', e.g, $[3 + t^2]\cdot\mathrm{e}^{4t}$. PolyExp-sum: '*Sum of polyexps*'. E.g, $f(t) := 3t\mathrm{e}^{2t} + [t^2]\cdot\mathrm{e}^t$ is a polyexp-sum.

Phrases. WLOG: '*Without loss of generality*'. IFF: '*if and only if*'. TFAE: '*The following are equivalent*'. ITOf: '*In Terms Of*'. OTForm: '*of the form*'. FTSOC: '*For the sake of contradiction*'. And ※ ="Contradiction".

IST: '*It Suffices To*', as in ISTShow, ISTExhibit.

Use w.r.t: '*with respect to*' and s.t: '*such that*'.

Latin: e.g: *exempli gratia*, '*for example*'. i.e: *id est*, '*that is*'. N.B: *Nota bene*, '*Note well*'. inter alia: '*among other things*'. QED: *quod erat demonstrandum*, meaning "end of proof".

Prefix nv- means '*non-void*', e.g "the cartesian product of two nv-sets is non-void". Prefix nt- means '*nontrivial*', e.g "the (positive) nt-divisors of 14 are 2, 7, 14, whereas the *proper* divisors are 1, 2, 7".

Operations on Sets. Use $\in$ for "is an element of". E.g, letting $\mathbb{P}$ be the set of primes, then, $5 \in \mathbb{P}$ yet $6 \notin \mathbb{P}$. Changing the emphasis, $\mathbb{P} \ni 5$ ["$\mathbb{P}$ *owns* 5"] yet $\mathbb{P} \not\ni 6$ ["$\mathbb{P}$ *does-not-own* 6"]

For subsets A and B of the same space, Ω, the ***inclusion relation*** $A \subset B$ means:

$$\forall \omega \in A, \textit{ necessarily } B \ni \omega.$$

And this can be written $B \supset A$. Use $A \subsetneqq B$ for *proper* inclusion, i.e, $A \subset B$ yet $A \neq B$.

The *difference set* $B \setminus A$ is $\{\omega \in B \mid \omega \notin A\}$. Employ A^c for the ***complement*** $\Omega \setminus A$. Use $A \triangle B$ for ***symmetric difference*** $[A \setminus B] \cup [B \setminus A]$. Furthermore

$A \mathbin{\blacksquare} B$,	Sets A & B have *at least* <u>*one*</u> point in common; they intersect.
$A \sqcap B$,	The sets have *no* common point; disjoint.

The symbol "$A \mathbin{\blacksquare} B$" both asserts intersection <u>and</u> represents the set $A \cap B$. For a collection $\mathcal{C} = \{E_j\}_j$ of sets in Ω, let the ***disjoint union*** $\bigsqcup_j E_j$ or $\bigsqcup(\mathcal{C})$ represent the union $\bigcup_j E_j$ *and also* asserts that the sets are pairwise disjoint.

On a set $\mathbf{\Omega}$, each subset $B \subset \mathbf{\Omega}$ engenders $\mathbf{1}_B$, the "***indicator function*** of B". It is the fnc $\mathbf{\Omega} \to \{0, 1\}$ sending points in B to 1, and pts in its complement, $B^c := \mathbf{\Omega} \smallsetminus B$, to 0. [So $\mathbf{1}_B + \mathbf{1}_{B^c}$ is constant-1.] E.g, $\mathbf{1}_{\text{Primes}}(5) = 1$ and $\mathbf{1}_{\text{Primes}}(9) = 0$.

Seqs. A *sequence* $\vec{\boldsymbol{x}}$ abbreviates $(x_0, x_1, x_2, x_3, \ldots)$. For a set Ω, expression "$\vec{\boldsymbol{x}} \subset \Omega$" means $[\forall n\colon x_n \in \Omega]$. Use $\text{Tail}_N(\vec{\boldsymbol{x}})$ for the subsequence

$$(x_N, x_{N+1}, x_{N+2}, \ldots)$$

of $\vec{\boldsymbol{x}}$. Given a fnc $f\colon \Omega \to \Lambda$ and an Ω-sequence $\vec{\boldsymbol{x}}$, let $f(\vec{\boldsymbol{x}})$ be the Λ-sequence $(f(x_1), f(x_2), f(x_2), \ldots)$.

Suppose Ω has an addition and multiplication. For Ω-seqs $\vec{\boldsymbol{x}}$ and $\vec{\boldsymbol{y}}$, then, let $\vec{\boldsymbol{x}} + \vec{\boldsymbol{y}}$ be the sequence whose n^{th} member is $x_n + y_n$. I.e

$$\vec{\boldsymbol{x}} + \vec{\boldsymbol{y}} \quad = \quad [n \mapsto [x_n + y_n]] \,.$$

Similarly, $\vec{\boldsymbol{x}} \cdot \vec{\boldsymbol{y}}$ denotes seq $[n \mapsto [x_n \cdot y_n]]$.

Why did the chicken cross the Möbius strip?
To get to the same side.

I dream of a better world where chickens can cross the road without having their motives questioned.

§B Binomials & Friends

Bi/Multi-nomial coeffs. For a natnum n, use "$n!$" to mean "n ***factorial***"; the product of all posints $\le n$. So $3! = 3 \cdot 2 \cdot 1 = 6$ and $5! = 120$. Also $0! = 1 = 1!$.

For natnum B and arb. complex number α, define

Rising Fctrl: $[\![\alpha \uparrow \mathsf{B}]\!] := \alpha \cdot [\alpha+1] \cdot [\alpha+2] \cdots [\alpha + [\mathsf{B}-1]]$,
Falling Fctrl: $[\![\alpha \downarrow \mathsf{B}]\!] := \alpha \cdot [\alpha-1] \cdot [\alpha-2] \cdots [\alpha - [\mathsf{B}-1]]$.

E.g, $[\![\mathsf{B}\downarrow\mathsf{B}]\!] = \mathsf{B}! = [\![1\uparrow\mathsf{B}]\!]$. Two further examples,

$$\left[\!\!\left[\tfrac{2}{7} \downarrow 4\right]\!\!\right] = \frac{2}{7}\cdot\frac{-5}{7}\cdot\frac{-12}{7}\cdot\frac{-19}{7} \quad\textit{and}\quad [\![1 \downarrow 3]\!] = 1 \cdot 0 \cdot {-1} = 0\,.$$

In particular, for $n \in \mathbb{N}$: If $\mathsf{B} > n$ then $[\![n \downarrow \mathsf{B}]\!] = 0$. We pronounce $[\![5 \downarrow \mathsf{B}]\!]$ as "5 falling-factorial B".

Binomial. The ***binomial coefficient*** $\binom{7}{3}$, read "7 choose 3", means *the number of ways of choosing 3 objects from 7 distinguishable objects.* Emphasising putting 3 objects in our left pocket and the remaining 4 in our right, we may write the coeff as $\binom{7}{3,4}$. [Read as "7 choose 3-comma-4."] Evidently

$$\dagger\!: \quad \binom{\mathsf{N}}{j} \;\overset{\text{with } k := \mathsf{N}-j}{=\!=\!=} \binom{\mathsf{N}}{j,\ k} = \frac{\mathsf{N}!}{j! \cdot k!} = \frac{[\![\mathsf{N}\downarrow j]\!]}{j!}.$$

Note $\binom{7}{0} = \binom{7}{0,7} = 1$. Finally, the Binomial theorem says

$$\text{£:} \qquad [x+y]^{\mathsf{N}} = \sum_{j+k=\mathsf{N}} \binom{\mathsf{N}}{j,k} \cdot x^j y^k\,,$$

where (j,k) ranges over all *ordered* pairs of natural numbers with sum N.

For natnum N, binomials satisfy this addition law:

$$*\!: \quad \binom{\mathsf{N}+1}{\mathsf{B}+1} = \overbrace{\binom{\mathsf{N}}{\mathsf{B}}}^{\text{Pick last object.}} + \overbrace{\binom{\mathsf{N}}{\mathsf{B}+1}}^{\text{Avoid last object.}}\,.$$

Extending this to *all* $\mathsf{B}\in\mathbb{Z}$ forces:

$$\binom{\mathsf{N}}{\mathsf{B}} = 0, \quad \textit{when } \mathsf{B} > \mathsf{N} \textit{ or } \mathsf{B} \textit{ negative.}$$

Case $\mathsf{B}>\mathsf{N}$ is automatic in formula $\binom{\mathsf{N}}{\mathsf{B}} = \frac{[\![\mathsf{N}\downarrow\mathsf{B}]\!]}{\mathsf{B}!}$.

Multinomial. In general, for natural numbers $\mathsf{N} = k_1 + \ldots + k_P$, the ***multinomial coefficient*** $\binom{\mathsf{N}}{k_1,\, k_2,\, \ldots,\, k_P}$ is the number of ways of partitioning N objects, by putting k_1 objects in pocket-one, k_2 objects in pocket-two, …putting k_P objects in the P^{th} pocket. Easily

$$\ddagger\!: \quad \binom{\mathsf{N}}{k_1, k_2, \ldots, k_P} = \frac{\mathsf{N}!}{k_1! \cdot k_2! \cdot \ldots \cdot k_P!}\,.$$

Unsurprisingly, $[x_1 + \ldots + x_P]^{\mathsf{N}}$ equals the sum of terms

$$\text{££:} \qquad \binom{\mathsf{N}}{k_1,\ldots,k_P} \cdot {x_1}^{k_1} \cdot {x_2}^{k_2} \cdots {x_P}^{k_P}\,,$$

taken over all natnum-tuples $\vec{k} = (k_1, \ldots, k_P)$ that sum to N. [That is multinomial analog of the Binomial Thm.]

Define the sum $S_\ell := k_1 + k_2 + \ldots + k_\ell$. Then multinomial LhS(‡) equals this product of binomials:

$$\binom{\mathsf{N}}{k_1} \cdot \binom{\mathsf{N} - S_1}{k_2} \cdot \binom{\mathsf{N} - S_2}{k_3} \cdot \ldots \cdot \binom{\mathsf{N} - S_{P-1}}{k_P}.$$

[The last term is $\binom{k_P}{k_P} \overset{\text{note}}{=\!=} 1$.]

112.1: Geo-power Lemma. *Each posint L and every complex $|u| < 1$ satisfies*

$$\dagger_L: \qquad \frac{1}{[1-u]^L} = \sum_{n=0}^{\infty} \binom{n+L-1}{n,\ L-1} \cdot u^n . \qquad \diamond$$

E.g. Whenever $|u| < 1$: For $L = 2$, we have

$$\frac{1}{[1-u]^2} = \sum_{n=0}^{\infty} \binom{n+1}{1} \cdot u^n = 1 + 2u + 3u^2 + 4u^3 + 5u^4 + \ldots$$

Similarly, $1/[1-u]^3$ equals

$$\sum_{n=0}^{\infty} \binom{n+2}{2} \cdot u^n = 1 + 3u + 6u^2 + 10u^3 + 15u^4 + \ldots \square$$

Proof. The $L{=}1$ case simply says

$$\frac{1}{1-u} = 1 + u + u^2 + u^3 + \ldots ,$$

summing a convergent geometric-series. Inducting on L, we show $(\dagger_L) \Rightarrow (\dagger_{L+1})$ by applying $\frac{1}{L} \cdot \frac{\mathrm{d}}{\mathrm{d}u}$ to $(\dagger_{L+1})$. For the lefthand-side,

$$\frac{1}{L} \cdot \frac{\mathrm{d}}{\mathrm{d}u} \mathrm{LhS}(\dagger_L) = \frac{1}{L} \cdot \frac{-L}{[1-u]^{L+1}} \cdot [-1] = \frac{1}{[1-u]^{L+1}} .$$

Term-by-term diff'ing gives

$$\frac{1}{L} \cdot \frac{\mathrm{d}}{\mathrm{d}u} \mathrm{RhS}(\dagger_L) = \frac{1}{L} \cdot \sum_{k=\mathbf{1}}^{\infty} \binom{k+L-1}{k,\ L-1} \cdot k\, u^{k-1}$$

$$\overset{n\ :=\ k-1}{=\!=\!=} \sum_{n=\mathbf{0}}^{\infty} \frac{n+1}{L} \cdot \binom{n+1+L-1}{n+1,\ L-1} \cdot u^n .$$

Conveniently,

$$\frac{n+1}{L} \cdot \binom{n\ +\ L}{n+1,\ L-1} = \binom{n+L}{n,\ L} .$$

Thus

$$\frac{1}{[1-u]^{L+1}} = \frac{1}{L} \cdot \frac{\mathrm{d}}{\mathrm{d}u} \mathrm{LhS}(\dagger_L)$$

$$= \frac{1}{L} \cdot \frac{\mathrm{d}}{\mathrm{d}u} \mathrm{RhS}(\dagger_L) = \sum_{n=0}^{\infty} \binom{n+L}{n,\ L} \cdot u^n .$$

Happily, this is the desired $(\dagger_{L+1})$. ♦

Calculus applications

Bi/Multi-nomials appear in differentiation formulas.

113a: Product Rule. *For natnum N, and N-times differentiable functions f and g:*

$$*:\qquad [f\cdot g]^{(N)} \;=\; \sum_{j+k=N} \binom{N}{j,\,k}\cdot f^{(j)}\cdot g^{(k)}\,,$$

*where (j,k) ranges over all **ordered pairs** of natural numbers with sum N.* ♢

E.g: $[f\cdot g]^{(4)} = fg^{(4)} + 4f^{(1)}g^{(3)} + 6f^{(2)}g^{(2)} + 4f^{(3)}g^{(1)} + f^{(4)}g$.

113b: Lemma. *For posints N, J, K with $J+K = N+1$,*

$$¥:\qquad \binom{N}{J-1,\;K} + \binom{N}{J,\;K-1} \;=\; \binom{N+1}{J,\;K}\,.$$ ♢

Proof. The LhS(¥) equals

$$\frac{J}{J}\cdot\frac{N!}{[J-1]!\,K!} \;+\; \frac{N!}{J!\,[K-1]!}\cdot\frac{K}{K} \;=\; \frac{[J+K]\cdot N!}{J!\,K!}\,,$$

which equals RhS(¥). ♦

Pf of (113a). At $N{=}0$, our $(*)$ says $fg = fg$; a tautology. Fixing N for which $(*)$ holds, note $[f\cdot g]^{(N+1)}$ equals $\sum_{j+k=N}\binom{N}{j,k}\,[f^{(j)}\cdot g^{(k)}]'$, which equals

$$\overbrace{\sum_{j+k=N}\binom{N}{j,k}\,f^{(j+1)}g^{(k)}}^{A} \;+\; \overbrace{\sum_{j+k=N}\binom{N}{j,k}\,f^{(j)}g^{(k+1)}}^{B}\,.$$

Letting $J := j{+}1$ and $K := k$, rewrite A as

$$†:\qquad A \;=\; \sum_{\substack{J+K\,=\,N+1,\\ J\,\geq\,1}} \binom{N}{J-1,\,K}\cdot f^{(J)}g^{(K)}\,.$$

Similarly, with $K := k{+}1$ and $J := j$, rewrite B as

$$‡:\qquad B \;=\; \sum_{\substack{J+K\,=\,N+1,\\ K\,\geq\,1}} \binom{N}{J,\,K-1}\cdot f^{(J)}g^{(K)}\,.$$

Separating out the $K{=}0$ term from (†) and the $J{=}0$ term from (‡), says that $A+B$ equals

$$\binom{N}{N,\,0}f^{(N+1)}g^{(0)} \;+\; \binom{N}{0,\,N}f^{(0)}g^{(N+1)}$$
$$+\sum_{\substack{J+K\,=\,N+1,\\ J,K\,\geq\,1}}\left[\binom{N}{J-1,\;K} + \binom{N}{J,\;K-1}\right]\cdot f^{(J)}g^{(K)}\,.$$

Use the lemma, (¥), to rewrite the summand. Thus $A+B$ equals

$$f^{(N+1)}g^{(0)} + f^{(0)}g^{(N+1)} \;+ \sum_{\substack{J+K\,=\,N+1,\\ J,K\,\geq\,1}}\binom{N+1}{J,\;K}\cdot f^{(J)}g^{(K)}\,.$$

And this equals $\displaystyle\sum_{j+k=N+1}\binom{N+1}{j,\,k}\cdot f^{(j)}g^{(k)}$, as desired. ♦

Larger product. Given a tuple $\mathbf{J} = (j_1,\ldots,j_P)$ of natnums, let ${+}\mathbf{J} := j_1 + \cdots + j_P$. With $N := {+}\mathbf{J}$, let $\binom{N}{\mathbf{J}}$ mean multinomial coeff $\binom{N}{j_1,\,j_2,\,\ldots,\,j_P}$. Finally, given a tuple $\vec{\boldsymbol{f}} := (f_1,\ldots,f_P)$ of differentiable fncs, let $\vec{\boldsymbol{f}}^{(\mathbf{J})}$ abbreviate this product of derivatives:

$$\vec{\boldsymbol{f}}^{(\mathbf{J})} \;:=\; f_1^{(j_1)}\cdot f_2^{(j_2)}\cdot\ldots\cdot f_P^{(j_P)}\,.$$

[When tuple $\mathbf{J}$ is used this way, it is called a ***multi-index***.]

113c: Gen. Product Rule. *Fix natnum N, posint P, and N-times differentiable functions, $\vec{\boldsymbol{f}} := (f_1,\ldots,f_P)$. Then*

$$V_P:\qquad [f_1\cdot\ldots\cdot f_P]^{(N)} \;=\; \sum_{\mathbf{J}\,:\,{+}\mathbf{J}=N}\binom{N}{\mathbf{J}}\cdot\vec{\boldsymbol{f}}^{(\mathbf{J})}\,.$$ ♢

Proof. Eqn (V_1) asserts tautology $f_1^{(N)} = f_1^{(N)}$. We proceed by induction on P. Fixing P such that (V_P), we now establish (V_{P+1}).

Fix $P{+}1$ fncs $f_1,\ldots,f_P,g$, and let $\Phi := f_1\cdot\ldots\cdot f_P$. Then $[f_1\cdot\ldots\cdot f_P\cdot g]^{(N)}$ is $[\Phi\cdot g]^{(N)}$. By $(*)$, it equals

$$*1:\qquad \sum_{s+k=N}\binom{N}{s,\,k}\cdot\Phi^{(s)}\cdot g^{(k)}\,,$$

where (s,k) ranges over all natnum-pairs with sum N. Courtesy (V_P), our $\Phi^{(s)}$ equals

$$\sum_{\mathbf{J}\,:\,{+}\mathbf{J}\,=\,s}\binom{s}{\mathbf{J}}\cdot\vec{\boldsymbol{f}}^{(\mathbf{J})}\,,\qquad \textit{where } \mathbf{J} = (j_1,\ldots,j_P).$$

Plugging this in to $(*1)$ gives

$$*2:\qquad \sum_{s+k=N}\left[\,\sum_{\mathbf{J}:\,{+}\mathbf{J}\,=\,s}\binom{N}{s,\,k}\binom{s}{\mathbf{J}}\cdot\vec{\boldsymbol{f}}^{(\mathbf{J})}\cdot g^{(k)}\right].$$

But product $\binom{N}{s,\,k}\binom{s}{\mathbf{J}}$ equals multinomial $\binom{N}{j_1,\ldots,j_P,k}$. Renaming k to j_{P+1}, and g to f_{P+1}, writes (∗2) as

$$\sum_{\substack{j_1+\ldots+j_P+j_{P+1}\\ =N}} \binom{N}{j_1,\,\ldots,\,j_{P+1}} \cdot f_1^{(j_1)}\cdot\ldots\cdot f_P^{(j_P)}\cdot f_{P+1}^{(j_{P+1})},$$

which indeed is RhS of (V_{P+1}). ♦

Deriv(product). Consider $f(t) := 3^t$, $g(t) := \sin(5t)$ and $h(t) := \mathrm{e}^{7t}$. The 6^{th}-derivative, $[f\cdot g\cdot h]^{(6)}$, is a sum of terms. *What is the coeff of the* $f''\cdot g'\cdot h'''$ *term?*

Soln. By the generalized product rule, (113c), the coefficient of $f^{(2)}g^{(1)}h^{(3)}$ is

$$\binom{6}{2,\,1,\,3} \stackrel{\text{note}}{=\!=} \binom{6}{2}\binom{4}{1}\binom{3}{3} = \frac{6\cdot 5}{2\cdot 1}\cdot\frac{4}{1}\cdot 1 = 60\,.$$

Continuing, note:

$$f^{(2)} = [\log(3)]^2\cdot f;\quad g^{(1)}(t) = 5\cos(5t);\quad h^{(3)} = 7^3\cdot h.$$

So one summand in the sum forming $[f\cdot g\cdot h]^{(6)}$, is

$$60\cdot\log(3)^2\cdot 5\cdot 7^3\cdot\left[3^t\cdot\cos(5t)\cdot\mathrm{e}^{7t}\right].$$ ♦

Number Theory

Use $\equiv_N$ to mean "congruent mod N". Let $n \perp k$ mean that n and k are co-prime [no prime in common].

Use $k \bullet\!| \, n$ for "k divides n". Its negation $k \not\bullet\!| \, n$ means "k does <u>not</u> divide n." Use $n \, |\!\bullet k$ and $n \, |\!\not\bullet k$ for "n is/is-not a multiple of k." Finally, for p a prime and E a natnum: Use double-verticals, $\mathsf{p}^E \bullet\!\| \, n$, to mean that E is the ***highest*** power of p which divides n. Or write $n \, \|\!\bullet \mathsf{p}^E$ to emphasize that this is an assertion about n. [E.g, $2^3 \bullet\!\| \, 40$ since $8 \bullet\!| \, 40$ yet $16 \not\bullet\!| \, 40$.]

Use ***PoT*** for Power of Two and ***PoP*** for Power of (a) Prime.

Euler φ. For N a posint, use $\Phi(N)$ or Φ_N for the <u>set</u> $\{r \in [1 \mathinner{..} N] \mid r \perp N\}$. The cardinality $\varphi(N) := |\Phi_N|$ is the ***Euler phi function***. [So $\varphi(N)$ is the cardinality of the multiplicative group, Φ_N, in the $\mathbb{Z}_N$ ring.] Easily, $\varphi(\mathsf{p}^L) = [\mathsf{p}-1] \cdot \mathsf{p}^{L-1}$, for prime p and posint L. Less easily, when $K \perp N$, then $\varphi(KN) = \varphi(K) \cdot \varphi(N)$

Use ***EFT*** for the Euler-Fermat Thm, which says: *Suppose that integers* $\mathbf{b} \perp N$, *with* N *positive. Then* $\mathbf{b}^{\varphi(N)} \equiv_N 1$.

§C Polynomials

Use ***poly*** for "polynomial". An integer-coefficient poly is a $\mathbb{Z}$-poly or an ***intpoly***. With rational coeffs, it is a $\mathbb{Q}$-poly or ***ratpoly***. An F-poly has its coeffs come from a *field* F. (A commutative ring is ok too).

The poly ***Zip*** has all of its coefficients zero. Say that a poly is 5-***topped*** if its degree is *strictly* less than 5. Over a field F, the set of (single variable) N-topped polys forms an N*-dimensional vectorspace*.

(See also Prof.King's Primer on Polynomials)

Discriminant. The ***discriminant*** of quadratic [i.e, $A \neq 0$] polynomial $q(z) := Az^2 + Bz + C$ is

114.1: $$\operatorname{Discr}(q) \quad := \quad B^2 - 4AC\,.$$

The zeros ["roots"] of q are

114.2: $$\operatorname{Roots}(q) \quad = \quad \frac{1}{2A}\Big[-B \pm \sqrt{\operatorname{Discr}(q)}\;\Big]\,.$$

Hence when A,B,C are *real*, then the zeros of q form a complex-conjugate pair. And q has a *repeated root* IFF $\operatorname{Discr}(q)$ is zero.

A monic $\mathbb{R}$-irreducible quadratic has form

114.3: $$q(x) \;=\; x^2 - \mathcal{S}x + \mathcal{P} \;=\; [x - Z]\cdot[x - \overline{Z}]\,,$$

where $Z \in \mathbb{C} \smallsetminus \mathbb{R}$. Note $\mathcal{S} = Z + \overline{Z} = 2\operatorname{Re}(Z)$ is the *Sum* of the roots. And $\mathcal{P} = Z \cdot \overline{Z} = |Z|^2$ is the *Product* of the roots. The g discriminant, $\operatorname{Discr}(g)$, equals

114.4: $$\mathcal{S}^2 - 4\mathcal{P} \overset{\text{note}}{=\!=} [Z - \overline{Z}]^2 \;=\; -4\cdot[\operatorname{Im}(Z)]^2\,.$$

Completing-the-square yields

114.5: $$q(x) \;=\; \big[x - \tfrac{\mathcal{S}}{2}\big]^2 \,+\, F^2, \text{ where } F := |\operatorname{Im}(Z)|\,,$$

which is easily checked. [Exercise]

115: List lemma. *Fix h, a $\mathbb{Z}$-poly ["intpoly", a polynomial with integer coeffs]. Then for each two integers k,ℓ, difference $k - \ell$ divides $h(k) - h(k)$.* *Pf.* Exercise.◊

116: Fundamental Theorem of Algebra (Gauss and friends). *Consider a monic $\mathbb{C}$-polynomial*

$$g(t) \;:=\; t^N + B_{N-1}t^{N-1} + \ldots + B_1 t + B_0\,.$$

Then g factors completely over $\mathbb{C}$ as

$$g(t) \;=\; [t - Z_1]\cdot[t - Z_2]\cdot\ldots\cdot[t - Z_N]\,,$$

for a list $Z_1, \ldots, Z_N \in \mathbb{C}$, possibly with repetitions. This list is unique up to reordering.

*If g is a **real** polynomial, i.e $\overline{g} = g$, then g factors over $\mathbb{R}$ as a product of monic $\mathbb{R}$-irreducible linear and $\mathbb{R}$-irred. quadratic polynomials. The product is unique up to reordering.*

Proof. A proof-sketch is in Primer on Polynomials on my Teaching page.Also: A proof-sketch is in Primer on Polynomials on my Teaching page. ◊

Summation polynomials. Fnc f on $\mathbb{N}$ has ***summation function***

117a: $$\widehat{f}(N) \;:=\; \sum_{\ell\in[0\,..\,N)} f(\ell)\,.$$

If f is a polynomial of degree $L \in \mathbb{N}$, then $\widehat{f}$ is a polynomial of degree $L+1$.

To see this, define the L^{th} ***binomial polynomial***, for $L\in\mathbb{N}$, by

117b: $$\mathcal{B}_L(x) \;:=\; \frac{x\cdot[x-1]\cdot[x-2]\cdots[x-[L-1]]}{L!}\,,$$

which we may also write as $\binom{x}{L} = \frac{[\![x\downarrow L]\!]}{L!}$. Rewrite the binomial identity $\binom{n}{L+1} = \binom{n-1}{L+1} + \binom{n-1}{L}$ as

$$\binom{n-1}{L} \;=\; \binom{n}{L+1} - \binom{n-1}{L+1}. \quad \textit{So } \widehat{\mathcal{B}_L}(N) \textit{ equals}$$

$$\sum_{n=1}^{N}\binom{n-1}{L} = \sum_{n=1}^{N}\Big[\binom{n}{L+1} - \binom{n-1}{L+1}\Big] \;=\; \binom{N}{L+1} - \binom{0}{L+1}.$$

This last equals $\mathcal{B}_{L+1}(N)$, since $\binom{0}{L+1} = 0$ [because $L+1$ is positive]. Hence

117c: $$\widehat{\mathcal{B}_L} \;=\; \mathcal{B}_{L+1}\,.$$

The binomial polys $\{\mathcal{B}_L\}_{L=0}^{\infty}$ form a basis for the vectorspace of polys. Since the $f \mapsto \widehat{f}$ map is linear, we can compute the summation-poly of arbitrary polynomials. [ASIDE: Stronger, collection $\{\mathcal{B}_L\}_{L=0}^{\infty}$ is a $\mathbb{Z}$-basis for the set of $\mathbb{Z}$-valued polynomials (the "valiant" polys); however, this fact isn't obvious.]

Low-degree summations. Here we go!:

$$1+2+3+\cdots+N \;=\; \frac{N[N+1]}{2} \;=\; \frac{N^2+N}{2}.$$

$$1^2+2^2+3^2+\cdots+N^2 \;=\; \frac{N[N+1][2N+1]}{6} = \frac{2N^3+3N^2+N}{6}.$$

$$1^3+2^3+3^3+\cdots+N^3 \;=\; \Big[\frac{N[N+1]}{2}\Big]^2 \;=\; \frac{N^4+2N^3+N^2}{4}.$$

$$1^4+2^4+3^4+\cdots+N^4 \;=\; \frac{N[N+1][2N+1][3N^2+3N-1]}{30} \;=\; \frac{6N^5+15N^4+10N^3-N}{30}.$$

$$1^5+2^5+3^5+\cdots+N^5 \;=\; \frac{\big[N[N+1]\big]^2\cdot[2N^2+2N-1]}{12} \;=\; \frac{2N^6+6N^5+5N^4-N^2}{12}.$$

Letting $\mathbf{p}_L(x) := x^L$, the above LhS are $\widehat{\mathbf{p}_L}(N+1)$.

§D Theorem Grabbag

We start with just a touch of LINEAR ALGEBRA.

Defn. A ***linear combination*** of two vectors $\vec{v}$,$\vec{w}$ is a sum of form $\alpha\vec{v}+\beta\vec{w}$ where α,β are scalars.

[Abbr: ***linear-comb***, ***lincomb***.] A ***lincomb*** of a *list* $\vec{v}_1,\ldots,\vec{v}_N$ is a sum of form $\sum_{j=1}^N \alpha_j\vec{v}_j$

An ***integer-lincomb*** (or $\mathbb{Z}$-***lincomb***) means that each scalar α_j is an integer. □

118: Lemma. *A common divisor d of integer-list $K_1,\ldots,K_N$ divides every integer-lincomb of the list. In particular, $\text{GCD}(K_1,\ldots,K_N)$ divides every integer-lincomb.* *Proof.* Exercise. ◊

Application. Evidently $\mathbf{302} \perp \mathbf{201}$ since

$$[2\cdot\mathbf{302}] - [3\cdot\mathbf{201}] = 1.$$

[Thus each common divisor of **302** and **201** divides 1.] □

119: Bézout's lemma. *Each N-tuple $(K_1,\ldots,K_N)$ of integers admits a **Bézout tuple**: A tuple $(s_1,\ldots,s_N)$; of integers s.t $\sum_{j=1}^N [s_jK_j] = \text{GCD}(K_1,\ldots,K_N)$.* ◊

Convexity. In $\mathbf{V}:=\mathbb{R}^N$, or any $\mathbb{R}$-vectorspace, it is possible to define the ***line seqment*** between two points $\mathbf{p}$,$\mathbf{r}\in\mathbf{V}$:

†: $$\text{Seg}(\mathbf{p},\mathbf{r}) := \Big\{x\mathbf{p} + [1-x]\mathbf{r} \;\Big|\; 0\le x\le 1\Big\}.$$

A subset $\mathbf{\Omega}\subset\mathbf{V}$ is ***convex*** if $\mathbf{\Omega}$ is sealed under line-segment, ie,

‡: $$\forall\,\mathbf{p},\mathbf{r}\in\mathbf{\Omega}: \quad \text{Seg}(\mathbf{p},\mathbf{r}) \subset \mathbf{\Omega}.$$

A point $\mathbf{q}\in\mathbf{\Omega}$ is an "***interior point*** of $\mathbf{\Omega}$ in $\mathbf{V}$" if *there exists* a radius $\varepsilon>0$ s.t ball $\text{Bal}_\varepsilon(\mathbf{q})\subset\mathbf{\Omega}$; here

∗: $$\text{Bal}_\varepsilon(\mathbf{q}) := \{\mathbf{u}\in\mathbf{V} \mid \text{Dist}(\mathbf{u},\mathbf{q})<\varepsilon\}.$$

Finally, $\mathbf{\Omega}$ is ***strictly convex*** if for each $\mathbf{p}\neq\mathbf{r}$ in $\mathbf{\Omega}$, each point $\mathbf{q}$ which is interior to $\text{Seg}(\mathbf{p},\mathbf{r})$ is interior to $\mathbf{\Omega}$, i.e,

‡‡: *When $0<x<1$, then $x\mathbf{p}+[1-x]\mathbf{r}$ is an interior point of $\mathbf{\Omega}$ in $\mathbf{V}$.*

Functions. Below, $\mathbf{V}$ is $\mathbb{R}$ or $\mathbb{R}^N$ [or any $\mathbb{R}$-vectorspace]. The ***graph*** of a function $f:\mathbf{V}\to\mathbb{R}$ is the set of points $(\mathbf{u},f(\mathbf{u}))$, for $\mathbf{u}\in\mathbf{V}$. So the graph is a subset of vectorspace $\mathbf{V}\times\mathbb{R}$. Define the set of point *above* and *below* this graph, as

$$G_f^+ := \Big\{(\mathbf{u},y) \;\Big|\; \mathbf{u}\in\mathbf{V} \;\&\; y\in\mathbb{R} \;\&\; y\ge f(\mathbf{u})\Big\};$$

$$G_f^- := \Big\{(\mathbf{u},y) \;\Big|\; \mathbf{u}\in\mathbf{V} \;\&\; y\in\mathbb{R} \;\&\; y\le f(\mathbf{u})\Big\}.$$

Fnc f is (***strictly***) ***convex-up*** if G_f^+ is a (strictly) convex set. And f is (***strictly***) ***convex-down*** if G_f^- is (strictly) convex. [The older terms for *convex-down* and *convex-up* were "concave fnc" and "convex fnc".]

If f is defined on only a subset $\Omega\subset\mathbf{V}$, i.e $f:\Omega\to\mathbb{R}$, these definitions still apply *as long as* Ω is a convex subset of $\mathbf{V}$.

122: Jensen's inequality. *On an interval $J\subset\mathbb{R}$, consider points $Q_\mathbf{v}\in J$, for each $\mathbf{v}$ in a countable indexing-set $\mathcal{C}$. We have a probability-distr $\mathsf{P}()$ on $\mathcal{C}$. Then for each convex-down fnc $L:J\to\mathbb{R}$*

122a: $$L\Big(\sum_{\mathbf{v}\in\mathcal{C}} \mathsf{P}(\mathbf{v})\cdot Q_\mathbf{v}\Big) \ge \sum_{\mathbf{v}\in\mathcal{C}} \mathsf{P}(\mathbf{v})\cdot L(Q_\mathbf{v}).$$

Now suppose L is strictly convex-down. Then:

122b: *Equality in (122a) IFF the probability-distr is concentrated on a single point.*

IOWords, having removed all zero-probability elements from $\mathcal{C}$, the map $\mathbf{v}\mapsto Q_\mathbf{v}$ is constant.

Proof. Exercise. [Or see picture on blackboard.] ◊

Misc. tools.

123: Prime-binomial Lem. *Fix a prime p. Then each $k \in (0\,..\,p)$ satisfies* $\binom{p}{k} \equiv_p 0$. *I.e,* $\binom{p}{k} \bullet\!\!| \; p$. ♢

See Pascal's triangle, rows $2, 3, 5, 7$.

Pf. Our $k \geq 1$, so $p \bullet\!\!| \; [\![p \downarrow k]\!]$, the falling factorial. And p does *not* divide $k!$, since $k < p$. Hence p divides $\binom{p}{k} \stackrel{\text{note}}{=\!=} [\![p \downarrow k]\!] \big/ k!$. ♦

Here is an application.

123a: Lemma. *For x,y integers,* $[x+y]^p \equiv x^p + y^p$. ♢

Pf. Well, $[x + y]^p \stackrel{\text{Bin.thm}}{=\!=\!=} \sum_{k=0}^{p} \binom{p}{k} \cdot x^k y^{p-k}$, which equals

$$x^p + y^p + \sum_{k=1}^{p-1} \binom{p}{k} \cdot x^k y^{p-k} \stackrel{\text{by (123)}}{\equiv\!\equiv} x^p + y^p + \mathbf{0}.$$ ♦

Prelim. Suppose a finite group G acts on a finite set Ω. The ***stabilizer*** $\mathrm{Stab}_G(\boldsymbol{s})$ of a point $\boldsymbol{s} \in \Omega$ is $\{g \in G \mid g(\boldsymbol{s}) = \boldsymbol{s}\}$. So the G-orbit of $\boldsymbol{s}$ corresponds 1-to-1 with the (left-)cosets of subgroup $\mathrm{Stab}_G(\boldsymbol{s})$. In particular

$$*: \quad |\mathrm{Orbit}(\boldsymbol{s})| \quad \textit{divides} \quad |G|.$$

This is part of the Orbit-Stabilizer thm.

For natnums $\lambda > \upsilon$, recollect that binomial coefficient $\binom{\upsilon}{\lambda}$ is zero. Recall also that $\binom{0}{0} = 1$. □

124.1: Lucas's binomial thm. *Express natnums $\mathcal{U}$,$\mathcal{L}$ in base p, where p is prime, as*

$$\mathcal{U} = \boldsymbol{\upsilon}_K \cdot p^K + \boldsymbol{\upsilon}_{K-1} \cdot p^{K-1} + \ldots + \boldsymbol{\upsilon}_2 p^2 + \boldsymbol{\upsilon}_1 p + \boldsymbol{\upsilon}_0$$

and

$$\mathcal{L} = \boldsymbol{\lambda}_K \cdot p^K + \boldsymbol{\lambda}_{K-1} \cdot p^{K-1} + \ldots + \boldsymbol{\lambda}_2 p^2 + \boldsymbol{\lambda}_1 p + \boldsymbol{\lambda}_0 \,,$$

where each $\boldsymbol{\upsilon}_n, \boldsymbol{\lambda}_n \in [0 .. p)$. Then we have mod-$p$ congruence

$$\dagger: \quad \binom{\mathcal{U}}{\mathcal{L}} \equiv_p \prod_{n=0}^{K} \binom{\boldsymbol{\upsilon}_n}{\boldsymbol{\lambda}_n}.$$

[*Mnemonic: $\mathcal{U}$ for Upper number, $\mathcal{L}$ for Lower.*] ◊

Proof (From Wikipedia). Fix a set, B, of cardinality $\mathcal{U}$. Partition B into $\boldsymbol{\upsilon}_n$ many cycles of length p^n. This product of cyclic groups,

$$G := \mathsf{C}_{p^K} \times \mathsf{C}_{p^{K-1}} \times \ldots \times \mathsf{C}_p \times \mathsf{C}_1$$

acts on B by rotating the cycles.

Consequently, G acts on Ω, the collection of size-$\mathcal{L}$ subsets of B. Since $|G| = \prod_{n=0}^{K} p^n$ is a power of prime p, each G-orbit has size a power of p, courtesy ($*$). Thus

$$\ddagger: \quad \binom{\mathcal{U}}{\mathcal{L}} \overset{\text{note}}{=\!=} |\Omega| \equiv_p |\{\text{Set of } G\text{-fixed-points}\}|.$$

Our goal is now $\mathrm{RhS}(\ddagger) \overset{?}{=} \mathrm{RhS}(\dagger)$.

Fixed-pts. A size-$\mathcal{L}$ subset $S \subset \mathrm{B}$ is G-invariant IFF S is a union of some of the cycles comprising B.

First suppose there *is* such a fixed-pt, S. Let α_n be the number length-p^n cycles that it fills. As B only has $\boldsymbol{\upsilon}_n$ many p^n-cycles, necessarily $\alpha_n \leq \boldsymbol{\upsilon}_n < p$. The uniqueness of base-p representations now asserts that each $\boxed{\alpha_n = \boldsymbol{\lambda}_n}$, since $\sum_{n=0}^{K} \alpha_n p^n = |S| = \mathcal{L}$. Consequently each $\boxed{\boldsymbol{\lambda}_n \leq \boldsymbol{\upsilon}_n}$, and the number of such fixed-points is precisely $\mathrm{RhS}(\dagger)$. Conversely, if each $\boldsymbol{\lambda}_n \leq \boldsymbol{\upsilon}_n$, then there *are* fixed-pts.

Finally, having **no** G-fixed-pts corresponds to $\boldsymbol{\lambda}_n > \boldsymbol{\upsilon}_n$ for *some* index n, whence $\mathrm{RhS}(\dagger)$ is zero. ♦

AM-GM. The ***arithmetic*** and ***geometric means*** of a list $\vec{c} := (c_1, \ldots, c_N)$ of non-negative numbers, are

$$\mathrm{AM}(\vec{c}) := \frac{c_1 + \ldots + c_N}{N}, \quad \mathrm{GM}(\vec{c}) := \sqrt[N]{c_1 \cdot \ldots \cdot c_N}.$$

[The AM is well-defined in those rings where every sum OTForm $1+1+\ldots+1$ has a reciproval.] □

125.1: AM-GM inequality. *For non-negative list $\vec{c}$,*

$$‡: \qquad \frac{c_1 + \ldots + c_N}{N} \geq \sqrt[N]{c_1 \cdot \ldots \cdot c_N}$$

with equality IFF $c_1 = c_2 = \ldots = c_N$. ◊

Pf $N \leq 2$. Cases $N = 0,1$ are trivial. For $N=2$, note

$$\sqrt{xy} \leq \tfrac{x+y}{2} \overset{(*)}{\iff} 4xy \leq [x+y]^2 \Leftrightarrow 0 \leq [x-y]^2, \blacklozenge$$

since$^{(*)}$ $x,y \geq 0$.

Pf $N>2$. Fix $S \geq 0$. The simplex, Δ, of non-neg N-tuples with $\sum(\vec{c}) = S$, is compact. Hence $\prod(\vec{c})$ attains a maximum at, say, $\vec{e}$. Were $\vec{e}$ non-constant, then WLOG $e_1 \neq e_2$. Thus $S>0$, so each $e_j > 0$. Among non-neg pairs (c_1, c_2) whose sum equals e_1+e_2, product $c_1 \cdot c_2$ is uniquely maximized when $c_1 = c_2$. This contradicts that pair (e_1, e_2) gave maximum product [here, we are using that product $\prod_{j=3}^{N} e_j$ is positive.] ♦

Reciprocal tables in $\mathbb{Z}_p$

Reciprocals

Modulo 2:

x	$\langle 1/x\rangle_2$
1	1

Modulo 3:

x	$\langle 1/x\rangle_3$
±1	±1

Modulo 5:

x	$\langle 1/x\rangle_5$	x	$\langle 1/x\rangle_5$
±1	±1	±2	∓2

Modulo 7:

x	$\langle 1/x\rangle_7$	x	$\langle 1/x\rangle_7$
±1	±1		
±2	∓3	±3	∓2

Modulo 11:

x	$\langle 1/x\rangle_{11}$	x	$\langle 1/x\rangle_{11}$
±1	±1		
±2	∓5	±4	±3
±3	±4	±5	∓2

Modulo 13:

x	$\langle 1/x\rangle_{13}$	x	$\langle 1/x\rangle_{13}$
±1	±1	±4	∓3
±2	∓6	±5	∓5
±3	∓4	±6	∓2

Modulo 17:

x	$\langle 1/x\rangle_{17}$	x	$\langle 1/x\rangle_{17}$
±1	±1	±5	±7
±2	∓8	±6	±3
±3	±6	±7	±5
±4	∓4	±8	∓2

Modulo 19:

x	$\langle 1/x\rangle_{19}$	x	$\langle 1/x\rangle_{19}$
±1	±1		
±2	∓9	±6	∓3
±3	∓6	±7	∓8
±4	±5	±8	∓7
±5	±4	±9	∓2

Modulo 23:

x	$\langle 1/x\rangle_{23}$	x	$\langle 1/x\rangle_{23}$
±1	±1		
±2	∓11	±7	±10
±3	±8	±8	±3
±4	±6	±9	∓5
±5	∓9	±10	±7
±6	±4	±11	∓2

Multiplication

```
  7 |  2   3
----|--------
  2 | -3
  3 | -1   2
```

```
 11 |   2   3   4   5
----|----------------
  2 |   4
  3 |  -5  -2
  4 |  -3   1   5
  5 |  -1   4  -2   3
```

```
 13 |   2   3   4   5   6
----|--------------------
  2 |   4
  3 |   6  -4
  4 |  -5  -1   3
  5 |  -3   2  -6  -1
  6 |  -1   5  -2   4  -3
```

```
 17 |   2   3   4   5   6   7   8
----|----------------------------
  2 |   4
  3 |   6  -8
  4 |   8  -5  -1
  5 |  -7  -2   3   8
  6 |  -5   1   7  -4   2
  7 |  -3   4  -6   1   8  -2
  8 |  -1   7  -2   6  -3   5  -4
```

```
 19 |   2   3   4   5   6   7   8   9
----|--------------------------------
  2 |   4
  3 |   6   9
  4 |   8  -7  -3
  5 |  -9  -4   1   6
  6 |  -7  -1   5  -8  -2
  7 |  -5   2   9  -3   4  -8
  8 |  -3   5  -6   2  -9  -1   7
  9 |  -1   8  -2   7  -3   6  -4   5
```

```
 23 |   2   3   4   5   6   7   8   9  10  11
----|----------------------------------------
  2 |   4
  3 |   6   9
  4 |   8 -11  -7
  5 |  10  -8  -3   2
  6 | -11  -5   1   7 -10
  7 |  -9  -2   5 -11  -4   3
  8 |  -7   1   9  -6   2  10  -5
  9 |  -5   4 -10  -1   8  -6   3 -11
 10 |  -3   7  -6   4  -9   1  11  -2   8
 11 |  -1  10  -2   9  -3   8  -4   7  -5   6
```

§E Rings

Semigroups & Monoids. A ***semigroup*** is a pair $(S, \bullet)$, where $\bullet$ is an associative *binary operation* [***binop***] on set S. A special case is a ***monoid***. It is a triple $(S, \bullet, \mathbf{e})$, where $\bullet$ is an associative binop on S, and $\mathbf{e} \in S$ is a two-sided identity elt.

Axiomatically:

G1: Binop $\bullet$ is ***associative***, i.e $\forall\alpha,\beta,\gamma \in S$, necessarily $[\alpha \bullet \beta] \bullet \gamma = \alpha \bullet [\beta \bullet \gamma]$.

G2: Elt $\mathbf{e}$ is a ***two-sided identity element***, i.e $\forall\alpha \in S$: $\alpha \bullet \mathbf{e} = \alpha$ and $\mathbf{e} \bullet \alpha = \alpha$.

Moreover, we call S a ***Group*** if t.fol also holds.

G3: Each elt admits a ***two-sided inverse element***: $\forall\alpha$, $\exists\beta$ such that $\alpha \bullet \beta = \mathbf{e}$ and $\beta \bullet \alpha = \mathbf{e}$.

When the binop is '+', *addition*, then write the inverse of α as $-\alpha$ and call it "***negative*** α". We then use 0 for the id-elt.

When the binop is '*multiplication*', write the inverse of α as α^{-1} and call it the "***reciprocal*** of α" We use 1 for the id-elt. Usually, one omits the binop-symbol and writes $\alpha\beta$ for $\alpha\bullet\beta$.

For an *abstract* binop '$\bullet$', we often write α^{-1} for the inverse of α ["α inverse"], and omit the binop-symbol. If $\bullet$ is ***commutative*** [$\forall\alpha,\beta$, necessarily $\alpha \bullet \beta = \beta \bullet \alpha$] then we call S a ***commutative group***.

Rings/Fields. A ***ring*** is a five-tuple $(\Gamma, +, 0, \cdot, 1)$ with these axioms.

R1: Elements 0 and 1 are distinct; $0 \neq 1$.

R2: Triple $\left(\Gamma, +, 0\right)$ is a commutative group.

R3: Triple $\left(\Gamma, \cdot, 1\right)$ is monoid.

R4: Mult. ***distributes-over*** addition from the *left*, $\alpha[x+y] = [\alpha x] + [\alpha y]$, and from the *right*, $[x+y]\alpha = [x\alpha] + [y\alpha]$; this, for all $\alpha,x,y \in \Gamma$.

Our Γ is a ***commutative ring*** (abbrev.: ***commRing***) if the multiplication is commutative.

When Γ is commutative: Say that $\alpha \bullet\!| \beta$ [α ***divides*** β] if *there exists* $\mu \in \Gamma$ s.t $\alpha\mu = \beta$. This is the same relation as $\beta |\!\bullet \alpha$ [β is a multiple of α].

Zero-divisors. Fix $\alpha \in \Gamma$. Elt $\beta \in \Gamma$ is a "(***two-sided***) ***annihilator*** of α" if $\alpha\beta = 0 = \beta\alpha$. An α is a (***two-sided***) ***zero-divisor*** if it admits a *non-zero* annihilator. So 0 is a ZD, since $0 \cdot 1 = 0 = 1 \cdot 0$, and $1 \neq 0$. We write the *set* of Γ–zero-divisors as

$$\mathrm{ZD}_\Gamma \quad \text{or} \quad \mathrm{ZD}(\Gamma)\,.$$

[E.g: In the $\mathbb{Z}_{15}$ ring, note $9 \not\equiv 0$ and $10 \not\equiv 0$, yet $9{\cdot}10$ *is* $\equiv 0$. So each of 9 and 10 is a "*non-trivial zero-divisor* in $\mathbb{Z}_{15}$".]

An $\alpha \in \Gamma$ is a Γ-***unit*** if $\exists\beta \in \Gamma$ st. $\alpha\beta = 1 = \beta\alpha$. Use

$$\mathbf{U}_\Gamma \quad \text{or} \quad \mathbf{U}(\Gamma)$$

for the units group. In the special case when Γ is $\mathbb{Z}_N$, I will write Φ_N for its units group, to emphasize the relation with the Euler-phi fnc, since $\varphi(N) := |\Phi_N|$. [Some texts use $\mathbf{U}(N)$ for the $\mathbb{Z}_N$ units group.]

Integral domains, Fields. A ***commutative ring*** is a ring in which the multiplication is commutative. A commRing with no (non-zero) zero-divisors [that is, $\mathrm{ZD}_\Gamma = \{0\}$] is called an ***integral domain*** (***intDomain***), or sometimes just a ***domain***.

An intDomain F in which every non-zero element is a unit [i.e $\mathbf{U}(F) = F \setminus \{0\}$] is a ***field***. That is to say, F is a commRing where triple $(F \setminus \{0\}, \cdot, 1)$ is a group.

Examples. The fields we know are: $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ and, for p prime, $\mathbb{Z}_p$.

Every ring has the "trivial zero-divisor" —zero itself. The ring of integers doesn't have others. In contrast, the non-trivial zero-divisors of $\mathbb{Z}_{12}$ comprise $\{\pm 2, \pm 3, \pm 4, 6\}$.

In $\mathbb{Z}$ the units are ± 1. But in $\mathbb{Z}_{12}$, the ring of integers mod-12, the set of units, $\Phi(12)$, is $\{\pm 1, \pm 5\}$. In the ring $\mathbb{Q}$ of rationals, *each* non-zero element is a unit. In the ring $\mathbb{G} := \mathbb{Z} + \mathbf{i}\mathbb{Z}$ of ***Gaussian integers***, the units group is $\{\pm 1, \pm\mathbf{i}\}$. [Aside: Units($\mathbb{G}$) is cyclic, generated by $\mathbf{i}$. And Units($\mathbb{Z}_{12}$) is not cyclic. For which N is $\Phi(N)$ cyclic?] □

Irreducibles, Primes. Consider $(\Gamma, +, 0, \cdot, 1)$, a commutative ring[♡7]. An elt $\alpha \in \Gamma$ is a ***zero-divisor*** [abbrev **ZD**] if there exists a *non-zero* $\beta \in \Gamma$ st. $\alpha\beta = 0$.

In contrast, an element $u \in \Gamma$ is a ***unit*** if $\exists w \in \Gamma$ st. $u \cdot w = 1$. This w, written as u^{-1}, is called the ***reciprocal*** [or ***multiplicative-inverse***] of u. [When an element *has* a mult-inverse, this mult-inverse is unique.]

Exer 1a: If α divides a unit, $\alpha \bullet\!| \; u$, then α is a unit.

Exer 1b: If $\gamma \mid\!\bullet \; z$ with $z \in$ ZD, then γ is a zero-divisor.

Exer 2: In an arbitrary ring Γ, the set ZD(Γ) is *disjoint* from Units(Γ).

An element $p \in \Gamma$ is:

i: Γ-***irreducible*** if p is a non-unit, non-ZD, such that for each Γ-factorization $p = x \cdot y$, either x or y is a Γ-unit. [Restating, using the definition below: Either $x \approx 1, y \approx p$, or $x \approx p, y \approx 1$.]

ii: Γ-***prime*** if p is a non-unit, non-ZD, such that for each pair $c,d \in \Gamma$: If $p \bullet\!| \; [c \cdot d]$ then *either* $p \bullet\!| \; c$ or $p \bullet\!| \; d$.

Associates. In a *commutative* ring, elts α and β are ***associates***, written $\alpha \approx \beta$, if *there exists* a unit u st. $\beta = u\alpha$. [For emphasis, we might say ***strong associates***.] They are ***weak-associates***, written $\alpha \sim \beta$, if $\alpha \bullet\!| \; \beta$ *and* $\alpha \mid\!\bullet \; \beta$ [i.e, $\alpha \in \beta\Gamma$ and $\beta \in \alpha\Gamma$].

Ex 3: Prove *Assoc* $\Rightarrow$ *weak-Assoc*.

Ex 4: If $\alpha \sim \beta$ and $\alpha \notin$ ZD, then α, β are (strong) associates.

Ex 5: In $\mathbb{Z}_{10}$, zero-divisors $2, 4$ *are* weak-associates. [This, since $2 \cdot 2 \equiv 4$ and $4 \cdot 3 = 12 \equiv 2$.] Are $2, 4$ (strong) associates?

Ex 6: With $d \bullet\!| \; \alpha$, prove: *If α is a non-ZD, then d is a non-ZD.* And: *If α is a unit, then d is a unit.*

126: Lemma. *In a commRing[♡7] Γ, each prime $\boldsymbol{\alpha}$ is irreducible.* ♢

Proof. Consider factorization $\boldsymbol{\alpha} = xy$. Since $\boldsymbol{\alpha} \bullet\!| \; xy$, WLOG $\boldsymbol{\alpha} \bullet\!| \; x$, i.e $\exists c$ with $\boldsymbol{\alpha} c = x$. Hence

$$*: \qquad \boldsymbol{\alpha} = xy = \boldsymbol{\alpha} cy .$$

By defn, $\boldsymbol{\alpha} \notin$ ZD. We may thus cancel in $(*)$, yielding $1 = cy$. So y is a unit. ♦

[♡7] More generally, a commutative monoid.

There are rings[♡8] with irreducible elements p which are nonetheless not prime. However...

127: Lemma. *Suppose commRing Γ satisfies the Bézout condition, that each GCD is a linear-combination. Then each irreducible $\boldsymbol{\alpha}$ is prime.* ♢

Pf. Suppose $\boldsymbol{\alpha} \bullet\!| \; c \cdot d$. WLOG $\boldsymbol{\alpha} \not\bullet\!| \; c$. Let $g := \text{GCD}(\boldsymbol{\alpha}, c)$. Were $g \approx \boldsymbol{\alpha}$, then $\boldsymbol{\alpha} \bullet\!| \; g \bullet\!| \; c$, a contradiction. Thus, since $\boldsymbol{\alpha}$ is irreducible, our $g \approx 1$.

Bézout produces $S, T \in \Gamma$ with

$$1 = S\boldsymbol{\alpha} + Tc . \quad \textit{Hence}$$

$$*: \qquad d = S\boldsymbol{\alpha}d + Tcd = Sd\boldsymbol{\alpha} + Tcd .$$

By hyp, $\boldsymbol{\alpha} \bullet\!| \; cd$, hence $\boldsymbol{\alpha}$ divides RhS($*$). So $\boldsymbol{\alpha} \bullet\!| \; d$. ♦

128: Lemma. *In commRing Γ, if prime p divides product $\alpha_1 \cdots \alpha_K$ then $p \bullet\!| \; \alpha_j$ for some j.* [Exer. 7] ♢

129: Prime-uniqueness thm. *In commRing Γ, suppose*

$$p_1 \cdot p_2 \cdot p_3 \cdots p_K = q_1 \cdot q_2 \cdot q_3 \cdots q_L$$

are equal products-of-primes. Then $L = K$ and, after permuting the p primes, each $p_k \approx q_k$. ♢

Pf. [From Ex.4, previously, for non-ZD, relations $\sim$ and $\approx$ are the same.] For notational simplicity, we do this in $\mathbb{Z}_+$, in which case $p_k \approx q_k$ will be replaced by $p_k = q_k$.

FTSOC, consider a CEX which minimizes sum $K+L$; necessarily positive. WLOG $L \geq 1$. Thus $K \geq 1$. [Otherwise, q_L divides a unit, forcing q_L to be a unit; see Ex.1a.] By the preceding lemma, q_L divides *some* p_k; WLOG $q_L \bullet\!| \; p_K$. Thus $q_L = p_K$ [since p_K is prime and q_L is not a unit]. Cancelling now gives $p_1 \cdot p_2 \cdots p_{K-1} = q_1 \cdot q_2 \cdots q_{L-1}$, giving a CEX with a *smaller* $[K-1] + [L-1]$ sum. ♦

[♡8] Consider the ring, Γ, of polys with coefficients in $\mathbb{Z}_{12}$. There, $x^2 - 1$ factors as $[x-5][x+5]$ *and* as $[x-1][x+1]$. Thus none of the four linear terms is prime. Yet each is Γ-irreducible. (Why?) This ring Γ has zero-divisors (yuck!), but there are natural subrings of $\mathbb{C}$ where Irred$\not\Rightarrow$Prime.

Example where $\sim\ \neq\ \approx$. Here a modification of an example due to Irving ("Kap") Kaplansky.

Let Ω be the ring of real-valued *continuous* fncs on $[-2,2]$. Define $\mathcal{E},\mathcal{D} \in \Omega$ by: *For* $t \geq 0$:

$$\mathcal{E}(t) \;=\; \mathcal{D}(t) \;:=\; \left\{\begin{matrix} t-1 & \text{if } t \in [1,2] \\ 0 & \text{if } t \in [0,1] \end{matrix}\right\}.$$

And for $t \leq 0$ define

$$\mathcal{E}(t) \;:=\; \mathcal{E}(-t) \quad \textit{and} \quad \mathcal{D}(t) \;:=\; -\mathcal{D}(-t)\,.$$

[So $\mathcal{E}$ is an Even fnc; $\mathcal{D}$ is odD.] Note $\mathcal{E} = f\mathcal{D}$ and $\mathcal{D} = f\mathcal{E}$, where

$$f(t) \;:=\; \left\{\begin{matrix} 1 & \text{if } t \in [1,\,2] \\ t & \text{if } t \in [-1,\,1] \\ -1 & \text{if } t \in [-2,-1] \end{matrix}\right\}.$$

Hence $\mathcal{E} \sim \mathcal{D}$. [This f is not a unit, since $f(0) = 0$ has no reciprocal. However, f is a *non*-ZD: For if $fg = \mathbf{0}$, then g must be zero on $[-2,2] \smallsetminus \{0\}$. Cty of g then forces $g \equiv \mathbf{0}$.]

Could there be a unit $u \in \Omega$ with $u\mathcal{D} = \mathcal{E}$? Well

$$u(2) = \frac{\mathcal{E}(2)}{\mathcal{D}(2)} \overset{\text{note}}{=\!=} +1\,, \quad \textit{and} \quad u(-2) = \frac{\mathcal{E}(-2)}{\mathcal{D}(-2)} \overset{\text{note}}{=\!=} -1\,.$$

Cty of $u()$ forces u to be zero somewhere on interval $(-2,2)$, hence u is *not* a unit. □

Addendum. By Ex.4, both $\mathcal{E}$ and $\mathcal{D}$ must be zero-divisors. [Exer.8: Exhibit a function $g \in \Omega$, *not* the zero-fnc, such that $\mathcal{E} \cdot g \equiv \mathbf{0}$.] □

§F ℂ-exp-cos-sin

The algebraic structure of $\mathbb{R}$ can be consistently extended to a larger field, by adjoining a sqroot of negative 1. This is conventionally[♡9] called $\mathbf{i}$, so $\mathbf{i}^2 = -1 = [-\mathbf{i}]^2$. Extending $\mathbb{R}$ by $\mathbf{i}$ produces field

$$\mathbb{C} \;:=\; \{x\mathbf{1} + y\mathbf{i} \mid \textit{where } x \textit{ and } y \textit{ are real}\}.$$

[I've written $x\mathbf{1} + y\mathbf{i}$ to emphasize that the additive structure of $\mathbb{C}$ is that of a 2-dimensional $\mathbb{R}$-vectorspace, with basis vectors $\mathbf{1}$ and $\mathbf{i}$. In practice, we write $2 + 3\mathbf{i}$, not $2\cdot\mathbf{1} + 3\mathbf{i}$.]

A geometric picture of $\mathbb{C}$, with the ***real axis*** horizontal, and the ***imaginary axis*** vertical, is called the ***Argand plane*** or the ***complex plane***.

Write ***real-part*** and ***imaginary-part*** extractors as, e.g, for $z := 2 - 3\mathbf{i}$, give

$$\mathrm{Re}(z) = 2 \quad \textit{and} \quad \mathrm{Im}(z) = -3$$

since $z = 2\cdot 1 + [-3]\cdot\mathbf{i}$. The ***absolute-value*** or ***modulus*** of z is its distance to the origin; so

$$|z| \;=\; \sqrt{\mathrm{Re}(z)^2 + \mathrm{Im}(z)^2}\,.$$

[Here, $|2 - 3\mathbf{i}| = \sqrt{4+9} = \sqrt{13}$.] The ***complex conjugate*** of this z is $\overline{z} = 2 + 3\mathbf{i}$. For a general $\omega = x + y\mathbf{i}$ with $x,y \in \mathbb{R}$, observe that

$$\mathrm{Re}(\omega) := x = \frac{\omega + \overline{\omega}}{2},\quad \mathrm{Im}(\omega) := y = \frac{\omega - \overline{\omega}}{2\mathbf{i}};$$

$$\overline{\omega} \;=\; \mathrm{Re}(\omega) - \mathrm{Im}(\omega)\mathbf{i};$$

$$|\omega|^2 \;\overset{\text{Pythag. thm}}{=\!=\!=}\; x^2 + y^2 \;=\; \omega\overline{\omega}\,.$$

(Complex-)conjugation $\omega \mapsto \overline{\omega}$ is an *involution* of $\mathbb{C}$, since $\overline{\overline{\omega}} = \omega$. For complex polynomial $f(z) = \sum_{j=0}^{N} \mathbf{c}_j z^j$, define $\overline{f}(z) := \sum_{j=0}^{N} \overline{\mathbf{c}_j}\, z^j$, its ***conjugate polynomial***. Thus

$$\overline{f(z)} \;=\; \overline{f}(\overline{z})\,,$$

since $\overline{\mu + \nu} = \overline{\mu} + \overline{\nu}$ and $\overline{\mu\nu} = \overline{\mu}\cdot\overline{\nu}$ for $\mu,\nu \in \mathbb{C}$.

Multiplying complex numbers corresponds to multiplying their moduli and adding their angles.

[♡9] Electrical engineers use $\mathbf{j}$ rather than $\mathbf{i}$, as "i" is used to represent current/amperage in EE. Also, while boldface $\mathbf{i}$ is a sqroot of −1, we still have non-boldface i as a variable. E.g, we *could* [but wouldn't] write $7\mathbf{i} + \sum_{i=3}^{4} i^2 \overset{\text{note}}{=\!=} 7\mathbf{i} + 3^2 + 4^2$.

To write a quotient $\frac{\nu}{\alpha}$ in std $x + \mathbf{i}y$ form, note

$$\frac{\nu}{\alpha} \;=\; \frac{\nu\overline{\alpha}}{\alpha\overline{\alpha}} \;=\; \nu\overline{\alpha}/|\alpha|^2$$

So write $\nu\overline{\alpha}$ in std form, then divide by real $|\alpha|^2$.

See W: Complex number and W: Argand plane for arithmetic with complex numbers.

Let's extend the exponential fnc to $\mathbb{C}$.

130a: Defn. *For $z \in \mathbb{C}$, define*

$$\exp(z) := \mathrm{e}^z := \sum_{n=0}^{\infty} \frac{1}{n!}\cdot z^n = 1 + z + \tfrac{1}{2}z^2 + \tfrac{1}{6}z^3 + \ldots;$$

$$\cos(z) := \sum_{k=0}^{\infty} \frac{[-1]^k}{[2k]!}\cdot z^{2k} = 1 - \tfrac{1}{2}z^2 + \tfrac{1}{24}z^4 - \ldots;$$

$$\sin(z) := \sum_{k=0}^{\infty} \frac{[-1]^k}{[2k+1]!}\cdot z^{2k+1} = z - \tfrac{1}{6}z^3 + \tfrac{1}{120}z^5 - \ldots.$$

Each series has ∞-RoC. ◊

Since we have absolute convergence of each series, we can re-order terms without changing convergence.

130b: Lemma. *Fix $\alpha,\beta \in \mathbb{C}$. Then*

$$\mathrm{e}^\alpha \cdot \mathrm{e}^\beta \;=\; \mathrm{e}^{\alpha+\beta}\,.$$ ◊

Proof. For natnum N, recall the Binomial thm which says that

$$*: \qquad \sum_{j+k=N} \binom{N}{j,k} \cdot \alpha^j \beta^k \;=\; [\alpha + \beta]^N\,,$$

where the sum is over all ordered-pairs (j,k) of natnums. By its defn [and abs.convergence], $\mathrm{e}^\alpha\mathrm{e}^\beta$ equals

$$\Big[\sum_{j=0}^{\infty} \frac{1}{j!}\cdot\alpha^j\Big] \cdot \Big[\sum_{k=0}^{\infty} \frac{1}{k!}\cdot\beta^k\Big] \;=\; \sum_{N=0}^{\infty}\Big[\sum_{j+k=N} \frac{1}{j!}\frac{1}{k!}\cdot\alpha^j\beta^k\Big].$$

But $\frac{1}{j!\cdot k!}$ equals $\frac{1}{N!}\cdot\frac{N!}{j!\cdot k!}$. Hence $\mathrm{e}^\alpha\mathrm{e}^\beta$ equals

$$\sum_{N=0}^{\infty} \frac{1}{N!}\Big[\sum_{j+k=N} \binom{N}{j,k}\cdot\alpha^j\beta^k\Big] \overset{\text{by } (*)}{=\!=\!=} \sum_{N=0}^{\infty} \frac{1}{N!}[\alpha+\beta]^N\,,$$

which is the defn of $\mathrm{e}^{\alpha+\beta}$. ♦

130c: Lemma. *For θ,x,y,z complex numbers:*

130.1:
$$\mathsf{e}^{\mathbf{i}\,\theta} \;=\; [\cos(\theta) \,+\, \mathbf{i}\sin(\theta)] \;=:\; \mathrm{cis}(\theta)\,. \quad \textit{Hence}$$

130.2:
$$\frac{\mathsf{e}^{\mathbf{i}\,\theta} + \mathsf{e}^{-\mathbf{i}\,\theta}}{2} = \cos(\theta)\,,\quad \frac{\mathsf{e}^{\mathbf{i}\,\theta} - \mathsf{e}^{-\mathbf{i}\,\theta}}{2\mathbf{i}} = \sin(\theta)\,. \; \textit{Also,}$$

130.3:
$$\mathsf{e}^{x\pm\mathbf{i}y} \;=\; \mathsf{e}^{x}\cdot\mathsf{e}^{\pm\mathbf{i}\,y} \;=\; \mathsf{e}^{x}\cdot[\cos(y) \,\pm\, \mathbf{i}\sin(y)]\,,$$

since $\cos(-y) = \cos(y)$ *and* $\sin(-y) = -\sin(y)$.

When θ is real, then,

130.4: $\mathrm{Re}(\mathsf{e}^{\mathbf{i}\,\theta}) \;=\; \cos(\theta)$ *and* $\mathrm{Im}(\mathsf{e}^{\mathbf{i}\,\theta}) \;=\; \sin(\theta)$.

Since the coefficients in their power-series expansions are all real, our $\exp()$,$\cos()$,$\sin()$ *fncs each commute with complex-conjugation, i.e*

130.5: $\overline{\exp(z)}=\exp(\overline{z})$, $\overline{\cos(z)}=\cos(\overline{z})$, $\overline{\sin(z)}=\sin(\overline{z})$;

Translation-identities & addition-identities

130.6:
$$\cos(z-\tfrac{\pi}{2}) \;=\; \sin(z)\,,\quad \sin(z+\tfrac{\pi}{2}) = \cos(z)\,,$$
$$\cos(\alpha\pm\beta) \;=\; \cos(\alpha)\cos(\beta) \;\mp\; \sin(\alpha)\sin(\beta),$$
$$\sin(\alpha\pm\beta) \;=\; \cos(\alpha)\sin(\beta) \;\pm\; \sin(\alpha)\cos(\beta).$$

extend to the complex plane. Finally,

130.7:
$\mathrm{Range}(\exp) = \mathbb{C}\smallsetminus\{0\}$ *is the punctured* $\mathbb{C}$.
And $\mathrm{Range}(\cos) = \mathbb{C} = \mathrm{Range}(\sin)$.

130.8: *All zeros of* [*complex*] $\cos()$ *lie in* $\mathbb{R}$. *Hence* $\cos()$ *has only one period, that of* $2\boldsymbol{\pi}$. ♢ *Both statements hold for* $\sin()$.

Pf of (130.7). For $\mathrm{Range}(\cos) \stackrel{?}{=} \mathbb{C}$, target $\frac{\tau}{2}\in\mathbb{C}$ requires z with $\cos(z) = \tau/2$. With $R := \mathsf{e}^{\mathbf{i}z}$, then, we need $R + \frac{1}{R} = \tau$, i.e $R^2 - \tau R + 1 = 0$. This quad.eqn *has* a solution $R \in \mathbb{C}$. As R=0 is not a soln, necessarily $R \in \mathrm{Range}(\exp)$. ♦

Pf of (130.8). Fix a $z = x + \mathbf{i}y$ st. $\cos(z) = 0$. Thus

$$\begin{aligned} 0 = 2\cos(z) \;&=\; \exp(\mathbf{i}\cdot[x+\mathbf{i}y]) + \exp(-\mathbf{i}\cdot[x+\mathbf{i}y]) \\ &=\; \exp(-y+\mathbf{i}x) \,+\, \exp(y-\mathbf{i}x) \\ &=\; \mathsf{e}^{-y}\mathrm{cis}(x) + \mathsf{e}^{y}\mathrm{cis}(-x)\,. \end{aligned}$$

Since these summands cancel, they must have equal abs.values. Since x and y are real, then,

$$*: \qquad \mathsf{e}^{-y} \;=\; \mathsf{e}^{-y}\cdot|\mathrm{cis}(x)| \;=\; \mathsf{e}^{y}\cdot|\mathrm{cis}(-x)| \;=\; \mathsf{e}^{y}.$$

But $\mathbb{R}$-exp() is 1-to-1, so $(*)$ implies that $-y = y$. Hence $y = 0$, i.e z is real. ♦

130e: Lemma. *Familar derivative relations,* $\exp' = \exp$ *and* $\cos' = -\sin$ *and* $\sin' = \cos$, *continue to hold.* ♢

Same-frequency cosines/sines. Consider a sum of same-frequency cosines

$$h(t) \;:=\; \sum_{j=1}^{N} \mathrm{A}_j\cdot\cos(\mathrm{P}_j \,+\, \mathrm{F}\cdot t)\,,$$

where $\mathrm{A}_j\in\mathbb{R}$ is *amplitude*, $\mathrm{P}_j\in\mathbb{R}$ is *phase-shift* and $\mathrm{F}\in\mathbb{R}$ determines the *frequency*. [Courtesy (130.6), we could include sine fncs in the sum.] We seek a phase-shift $\boldsymbol{\theta}$ and amplitude $\mathbf{R}\geq 0$ so that

$$h(t) \;=\; \mathbf{R}\cdot\cos(\boldsymbol{\theta} \,+\, \mathrm{F}t)\,.$$

From (130.4), we have that $h(t)$ equals

$$\sum_{j=1}^{N} \mathrm{A}_j\cdot\mathrm{Re}(\mathsf{e}^{\mathbf{i}[\mathrm{P}_j+\mathrm{F}t]}) \stackrel{\text{note}}{=\!=} \mathrm{Re}\Big(\sum_{j=1}^{N} \mathrm{A}_j\cdot\mathsf{e}^{\mathbf{i}[\mathrm{P}_j+\mathrm{F}t]}\Big)$$
$$= \mathrm{Re}\Big(\Big[\sum_{j=1}^{N} \mathrm{A}_j\cdot\mathsf{e}^{\mathbf{i}\mathrm{P}_j}\Big]\cdot\mathsf{e}^{\mathbf{i}\mathrm{F}t}\Big)\,.$$

Thus we are led to define $\mathbf{S}\in\mathbb{C}$ and X,$Y\in\mathbb{R}$ by

$$\dagger: \qquad \mathbf{S} \;:=\; \Big[\sum_{j=1}^{N} \mathrm{A}_j\cdot\mathsf{e}^{\mathbf{i}\mathrm{P}_j}\Big] \;=:\; X \,+\, \mathbf{i}Y\,.$$

Since each A_j and P_j is real,

$$X \;=\; \sum_{j=1}^{N} \mathrm{A}_j\cdot\cos(\mathrm{P}_j) \quad \text{and} \quad Y \;=\; \sum_{j=1}^{N} \mathrm{A}_j\cdot\sin(\mathrm{P}_j)\,.$$

130f: Same-freq Lemma. [*With notation from above.*] *Set* $\mathbf{R} := |\mathbf{S}| \overset{note}{=\!=} \sqrt{X^2+Y^2}$.

If $\mathbf{S}=0$, *then* $h()$ *is the zero-fnc; so can set* $\boldsymbol{\theta} := 0$. *Otherwise, if* $X=0$, *then set* $\boldsymbol{\theta}$ *to* $\frac{\pi}{2}$ *or* $-\frac{\pi}{2}$ *as* Y *is positive or negative.*

Otherwise: If $X>0$ *then set* $\boldsymbol{\theta} := \arctan(Y/X)$; *and if* $X<0$ *then set* $\boldsymbol{\theta} := \pi + \arctan(Y/X)$.

With $\mathbf{R}, \boldsymbol{\theta}$ *defined as above*

$$\ddagger: \quad \left[\sum_{j=1}^{N} \mathrm{A}_j \cdot \cos(\mathrm{P}_j + \mathrm{F}\cdot t)\right] = \mathbf{R}\cdot\cos(\boldsymbol{\theta} + \mathrm{F}t). \quad \lozenge$$

130g: *E.g.* Compute reals $\mathbf{R}\geq 0$ and phase-shift $\boldsymbol{\theta}$ st.
$\mathbf{R}\cos(\boldsymbol{\theta}+8t) = \cos(\frac{\pi}{3}+8t) + \cos(\frac{5\pi}{3}+8t) - \sqrt{2}\cos(\frac{7\pi}{4}+8t)$.

SOLN: Applying (†), above,

$$\mathbf{S} = e^{\mathbf{i}\frac{\pi}{3}} + e^{\mathbf{i}\frac{5\pi}{3}} - \sqrt{2}e^{\mathbf{i}\frac{7\pi}{4}} \overset{\text{Geometry}}{=\!=\!=} \mathbf{i}.$$

Hence $\mathbf{R} = |\mathbf{i}| = 1$ and $\boldsymbol{\theta} = \mathrm{Arg}(\mathbf{i}) = \frac{\pi}{2}$. □

Hyperbolic trig fncs

(Text commented-out.)

§G Morphisms

Homomorphism. Given binrels $(\mathbf{X}, \mathsf{R})$ and $(\mathbf{\Omega}, \mathsf{Q})$, a map $f\colon\mathbf{X}\to\mathbf{\Omega}$ is a ***binrel-homomorphism*** if

131a: $$\forall y,z\in\mathbf{X}: \quad y\,\mathsf{R}\,z \implies f(y)\,\mathsf{Q}\,f(z)$$

This f can be many-to-one, and *need not* be surjective. [Two $\mathbf{X}$-elts not R-related might nonetheless have their f-images Q-related.] Call f a ***binrel-embedding*** if f is injective with this IFF:

131b: $$\forall y,z\in\mathbf{X}: \quad y\,\mathsf{R}\,z \iff f(y)\,\mathsf{Q}\,f(z)\,.$$

IOWords, $(\mathbf{X}, \mathsf{R})$ is *binrel-**isomorphic*** (see below) to a *sub-structure* of $\mathbf{\Omega}$.

When R and Q are lax partial-orders, $(\mathbf{X}, \leqslant)$ and $(\mathbf{\Omega}, \preccurlyeq)$, then (131a) is an ***order-homomorphism*** and (131b) is an ***order-embedding***. □

Isomorphism. Consider Foo, an abstract class of objects. [So Foo might be vector-space or group or ring or field or topological-space or game or...]. A map $f\colon\mathbf{X}\to\mathbf{\Omega}$ is a **Foo-*homomorphism*** (abbrev: **Foo-*hom***) if f preserves Foo-structure. [This f might be neither injective nor surjective.]

E.g: When Foo is topological-space then a Foo-hom is called a '*continuous* map'. When Foo is vector-space then a Foo-hom is a '*linear* map'.

If $f\colon\mathbf{X}\hookrightarrow\!\!\!\!\rightarrow\mathbf{\Omega}$ is a *bijection*, and both f and f^{-1} are Foo-homs, then f is a **Foo-*isomorphism*** [E.g: The map $x\mapsto 3^x$ is a group-isomorphism from $(\mathbb{R},+,0)$ onto $(\mathbb{R}_+,\cdot,1)$. When Foo is topological-space, a Foo-isomorphism is called a ***homeomorphism***.] N.B: *Iso-morph* means *Same-form*. *Homo-morph also* means *Same-form*; in this case, in a weaker form.

[Caveat: In *Latin*, *homo* means 'Man' or 'Human'; e.g *homo sapien*. In *Greek*, *homo* means 'same', 'identical'; e.g the *arm of a human*, the *foreleg of a dog*, the *wing of a bat*, and the *front-fin of a whale* (all mammals) are *homologous structures*.]

An isomorphism $f\colon\mathbf{X}\hookrightarrow\mathbf{\Omega}$ to a sub-structure of $\mathbf{\Omega}$ is sometimes called an ***embedding*** or an ***into-isomorphism***. [E.g: The $\mathbb{R}\to\mathbb{R}\times\mathbb{R}$ map $x\mapsto(x,3x)$ is a vector-space embedding. The $\mathbb{R}^3\to\mathbb{R}^2$ map $(x,y,z)\mapsto(5y,0)$ is a vector-space hom that is neither 1-to-1 nor onto.] □

Automorphism. An isomorphism $f\colon\mathbf{X}\hookrightarrow\!\!\!\!\rightarrow\mathbf{X}$ from a structure to itself *could* be called an '*auto-isomorphism*'; but we contract it to ***automorphism***.

[E.g: The map $x\mapsto -x$ is a group-automorphism of additive group $(\mathbb{Q},+,0)$. On $\mathbb{C}$, the complex plane, the map $z\mapsto\overline{z}$ (the complex conjugate of z) is a field-automorphism.]

The set of Foo-automorphisms of a Foo-structure $\mathbf{X}$ is an (algebraic) ***group*** under composition, $\circ$. [E.g: Let $\mathbb{Q}_{\neq 0}$ denote the non-zero rationals. Each "multiplier" $M\in\mathbb{Q}_{\neq 0}$ engenders a group-automorphism of $(\mathbb{Q},+,0)$ under the map $q\mapsto M\cdot q$. Since multiplication is associative, the automorphism group of $(\mathbb{Q},+,0)$ is (group-)isomorphic to $(\mathbb{Q}_{\neq 0},\cdot,1)$.] □

Confession. I made up the terms 'binrel-homomorphism' and 'binrel-embedding'. Probably 'order-homomorphism' is used. Term 'order-embedding' *definitely* is used.

All branches of Mathematics use 'homomorphism', 'isomorphism', 'automorphism'. Less common is ***endomorphism***; a homomorphism from a structure to itself. Thus

	$\mathbf{X}\to\mathbf{\Omega}$	$\mathbf{X}\to\mathbf{X}$
Weak:	homomorphism	endomorphism
Strong:	isomorphism	automorphism

[People working in Category theory have additional words; *monomorphism*, *epimorphism*. We don't invite such people to our parties...] □

§H A few countable ordinals

Defn. Element m of poset $(\mathbf{X}, <)$ is ***minimal*** if $\forall b \in \mathbf{X}$: $[b \le m] \Rightarrow [b = m]$. The poset is ***well-founded*** if each non-void $\mathbf{X}$-subset admits a minimal elt.

A ***descending-chain*** has form $x_1 > x_2 > x_3 > \ldots$ and could be finite or infinite. Given the Axiom of Choice (AC), poset $(\mathbf{X}, <)$ is *well-founded* IFF it has no ∞-descending-chain.

A well-founded total-order is a ***well-order***. □

Ordinals. For us, an ***order-type*** is an equiv-class of total-orders under *order-isomorphism*. E.g: $(\mathbb{N}, \le)$ and $([5 .. \infty), \le)$ and $(\{2^n\}_{n=9}^{\infty}, \bullet|)$ all have the same order-type.

We can think of an ***ordinal*** as the order-type of a well-order. [A ***von Neumann ordinal*** is way of assigning a particular well-ordered-set to each well-order equiv-class.] □

Example countable ordinals. Let's exhibit subsets of $\mathbb{Q}_{\ge 0}$ that are well-ordered under $<$, making use of the "*compression function*" $f(q) := \frac{q}{q+1}$.

Given a set S, let $f(S)$ be $\{f(s) \mid s \in S\}$. And let, e.g, $5 + S$ mean $\{5+s \mid s \in S\}$.

The smallest infinite ordinal is called ω_0, often abbreviated ω; it has the order-type of $\mathbb{N}$, which I'll write as $\omega \leftrightarrow \mathbb{N}$.

Let $S_1 := f(\mathbb{N}) \overset{\text{note}}{\subset} [0, 1)$. Our f is order-preserving, so $\omega \leftrightarrow S_1$. Thus $S_1 \sqcup [1 + S_1]$ has order-type $\omega + \omega = \omega \cdot 2$. [Notice that $2 \cdot \omega = \omega$; ordinal add./mult. are not commutative.] Continuing the idea gives

$$\bigsqcup_{k=0}^{\infty} [k + S_1]$$

which has order-type $\omega \cdot \omega$. Iterating this idea produces

†: $$S_n := f\Big(\bigsqcup_{k=0}^{\infty} [k + S_{n-1}]\Big).$$

Since $S_n \leftrightarrow S_{n-1} \cdot \omega$, it follows that each $S_n \leftrightarrow \omega^n$.

Although this process can keep going, e.g,

‡: $$\bigsqcup_{k=0}^{\infty} [k + S_k]$$

has order-type ω^ω, we will stop here.

Choice function. Consider $\mathcal{C}$, a set of *non-void* sets.

A "***choice function*** for $\mathcal{C}$" is a function $f: \mathcal{C} \to \bigcup(\mathcal{C})$ satisfying $\forall P \in \mathcal{C}$: $f(P) \in P$.

I.e, for each patch $P \in \mathcal{C}$, function f picks an element of P. See

`https://en.wikipedia.org/wiki/Axiom_of_choice` □

133: Axiom of Choice. *Suppose $\mathcal{C}$ is a collection of non-void sets. Then $\mathcal{C}$ admits a choice function. I.e, $\{h \mid h$ is a choice function for $\mathcal{C}\}$ is non-empty.* ◊

(*For zoom writing*)

§Index, with symbols and abbrevs at the End

That's All, Folks! –*Bugs Bunny*