Upstart Puzzles (Unartige Raetseln) (Des Casse-tetes Terribles)

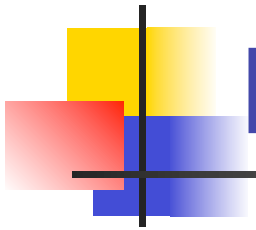
Dennis Shasha

shasha@cs.nyu.edu

Computer Science Dept

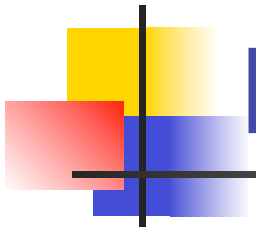
Courant Institute

New York University



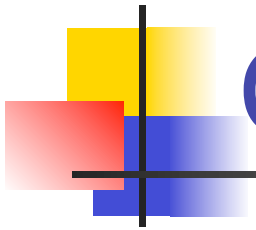
First: why puzzles?

- I’m easily confused.
- When confronted with a difficult problem, I make a puzzle for myself. I try to focus on the “simplest non-trivial instance of the problem” William Shockley. That’s a puzzle.



Example

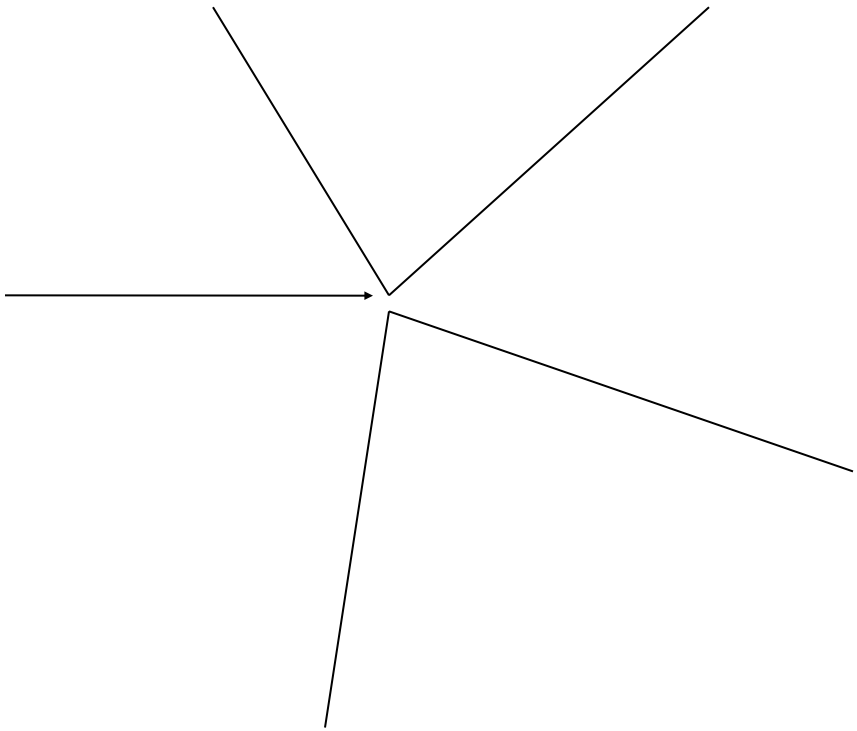
- First job out of college was to design part of the processor of the IBM 3090. Late 70s – mainframes still interesting.
- Problem: circuits would fail intermittently. Had to catch errors anyway.
- Kind of like a puzzle with occasional liars.

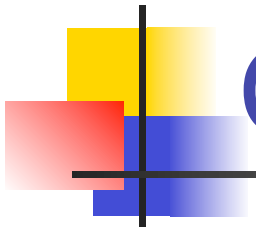


Camper's Puzzle

- You are a camp scout leader.
- You have eight scouts with you.
- You are walking on a path in the woods. You come to a crossroads with 5 paths (yours plus four others).
- Your campsite is a twenty minute walk down one path.

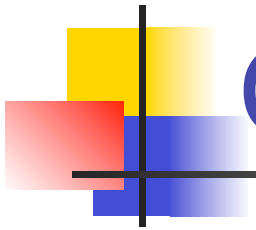
Which of the four unexplored paths has the campsite?





Camper's Puzzle II

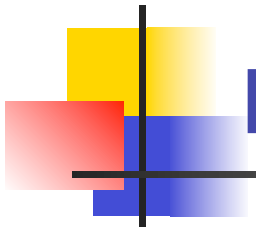
- Darkness falls in an hour.
- You want to divide up your campers and yourself to walk 20 minutes down some path, return 20 minutes later and then figure out where to go.
- Trouble is: two of your campers sometimes (but not always) lie.
- How do you do it?



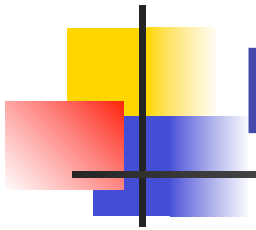
Camper's Puzzle III

- I won't tell you the answer, but I will give you two hints:
  1. You can explore one path by yourself
  2. You may never discover who the liars are.
- Every puzzle suggests variants. Here: can you do this with fewer than 8 campers?

Second: puzzles are a way to make a living

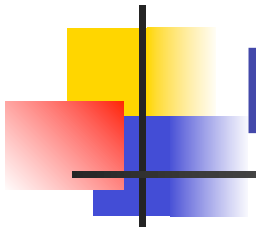


- I create and solve puzzles for a living.
- Biology with colleagues at NYU, Duke, and pharmas.
- Database tuning for gaming, travel, and telecom.
- Financial time series with wall street types.



Betting Puzzle

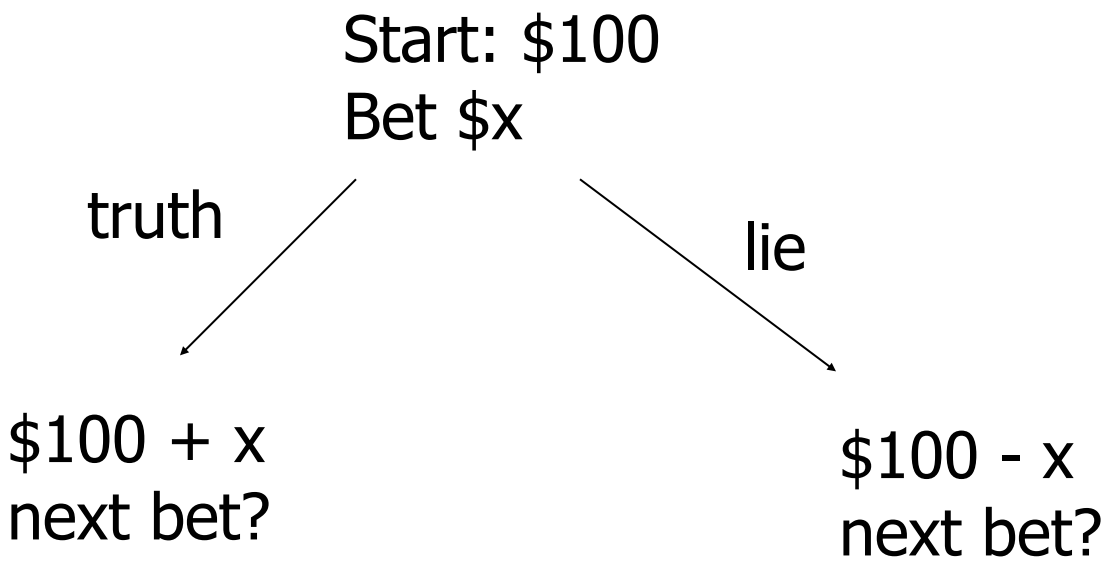
- You are placing even money bets on the flip of a coin.
- You may bet only as much as you have.
- Whole game is three flips.
- Flaky oracle will tell you how the flip will go at least two out of three times correctly.

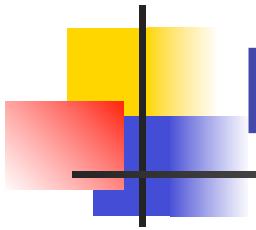


Betting Puzzle II

- Oracle doesn't like you so will try to limit your winnings or even make you lose if possible.
- You start with $100. How much can you guarantee to have at the end no matter when the oracle lies to you?

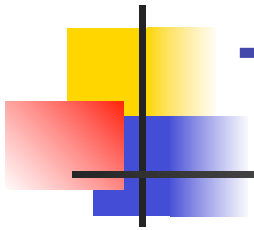
Betting Puzzle III





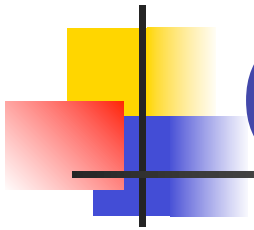
Betting Puzzle IV

- The best you can guarantee is $200 after three bets. (Try it. Hint: first bet is $50).
- This one is easy, but wait till the Intacto upstart.



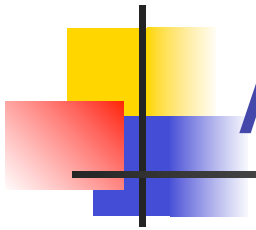
The Puzzlist's Conundrum

- Invent a puzzle to illustrate a principle.
- Find a solution.
- Puzzle suggests an alternative.
- You can't solve the alternative.
- Your friends can't solve it (not even Dr. Ecco).
- That's an upstart!



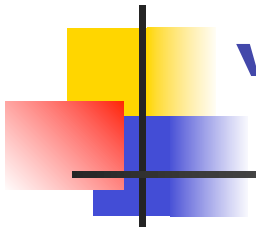
(Dis)Contents

- Amazing Sand Counter
- Architect's Puzzle
- Prime Geometry
- Territory Game
- Hiker's Puzzle
- Strategic Bullying
- Intacto
- Spy vs. Spy



Amazing Sand Counter

- Zero knowledge proofs are protocols in which a Prover wants to demonstrate (perhaps probabilistically) to a Verifier that the Prover knows something, but without revealing to the Verifier what Prover knows.
- Real-world (close): celebrant profs, religious demagogues

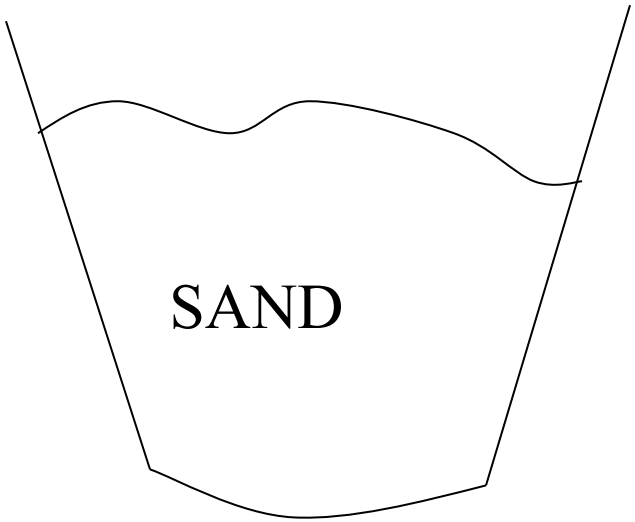


“Serious” Application

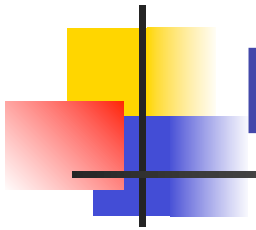
- Zero-knowledge proofs occur in public key cryptography, where my ability to sign a document digitally demonstrates that I know a secret key, but doesn’t reveal that key to you.
- Such applications make use of one-way functions (easy to verify, hard to invert).

Amazing Sand Counter

- Attempt to strip away technicalities.
- Man with gilded hat and waxed mustache: “I am the Amazing Sand Counter. If you put sand into this bucket, I know at a glance how many grains there are… But I won’t tell you.”

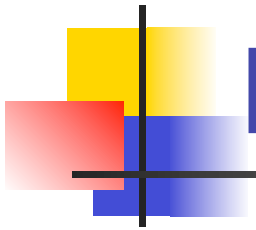


Amazing Sand Counter claims to know the number of grains in the bucket just by looking at it. Do you believe him?



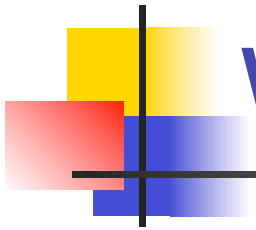
Moves allowed

- Ask Amazing to leave room
- Count small number of grains.
- Add or remove sand to/from bucket.
- Ask 100 questions.
- Cover yourself and bucket with a cloak, but Amazing must get a clear view when tested.



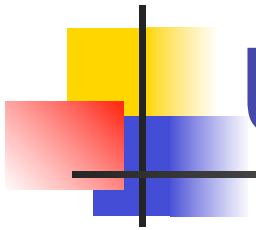
Nature of Experiment

- Pour sand.
- Let Amazing Sand Counter look.
- Ask Amazing to leave.
- Remove a few grains under cloak.
- Invite Amazing to return.
- “How many grains have I removed?”
- Repeat until you disprove or believe.



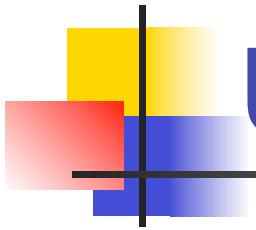
What has this accomplished

- If Amazing Sand Counter makes one mistake, he's finished, but if he gets it right every time, then if n is the max number of grains you could count, you can reduce prob of success by chance to about $1/n^k$
- Zero-knowledge and probabilistic proof.



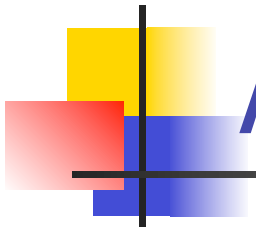
Upstart Variant

- Amazing Sand Counter acquires an earnest tone: “I want to tell you how many grains there are.”
- He gives you a number N.
- How can you be sure (or be convinced with high probability) he is telling the truth after a small amount of work?



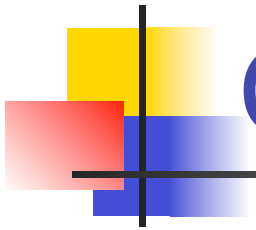
Upstart Specifics

- Given a bucket of sand, a number N claimed by the Amazing Sand Counter, determine whether N is the number of grains in the bucket using at most log N work.
- Work unit = counting a grain, dividing one bucket into two, or asking a question
- Sound easy? Give it a try.



Architect's Problem

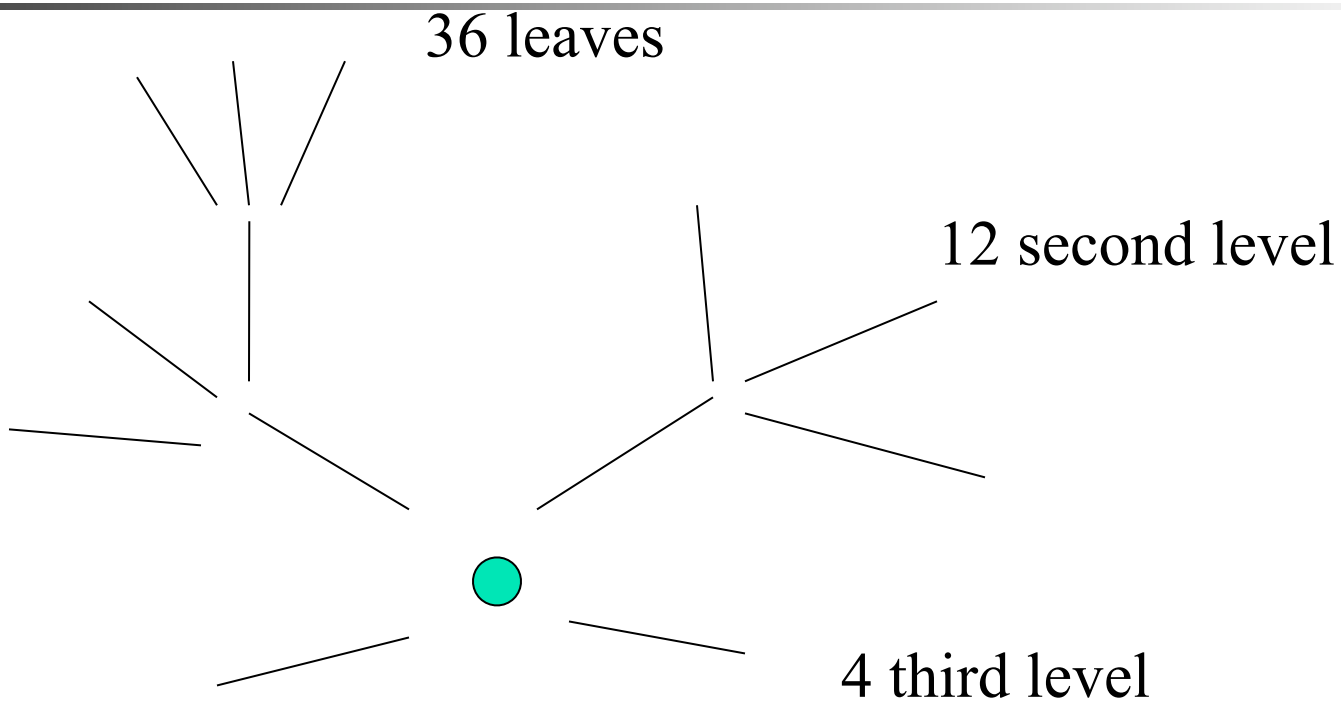
- 1988, A. K. Dewdney invited a puzzle for Scientific American.
- Started out as a problem about building architecture: how many rooms can you have in a ranch house in which each room has 4 doors and you want to get from any room to any other going through at most 6 doors?

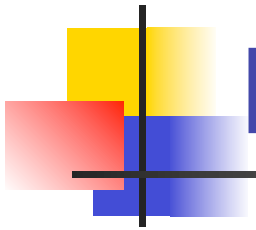


Graph Theory Version

- Rooms and doors are unconstrained so equivalent to: How many nodes can one have in a planar graph with diameter 6 and degree 4?

Tree approach



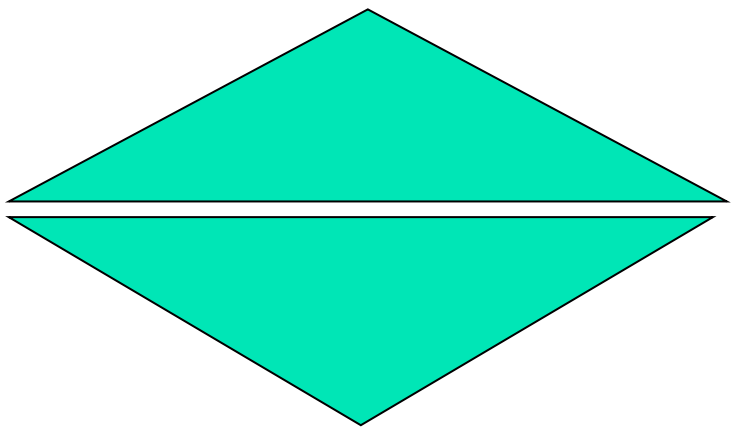


How Many Does Tree Give

- 36 leaves, 12 second level, 4 third level, plus 1 root: 53
- Not bad and I received many solutions like that.
- Is that best?

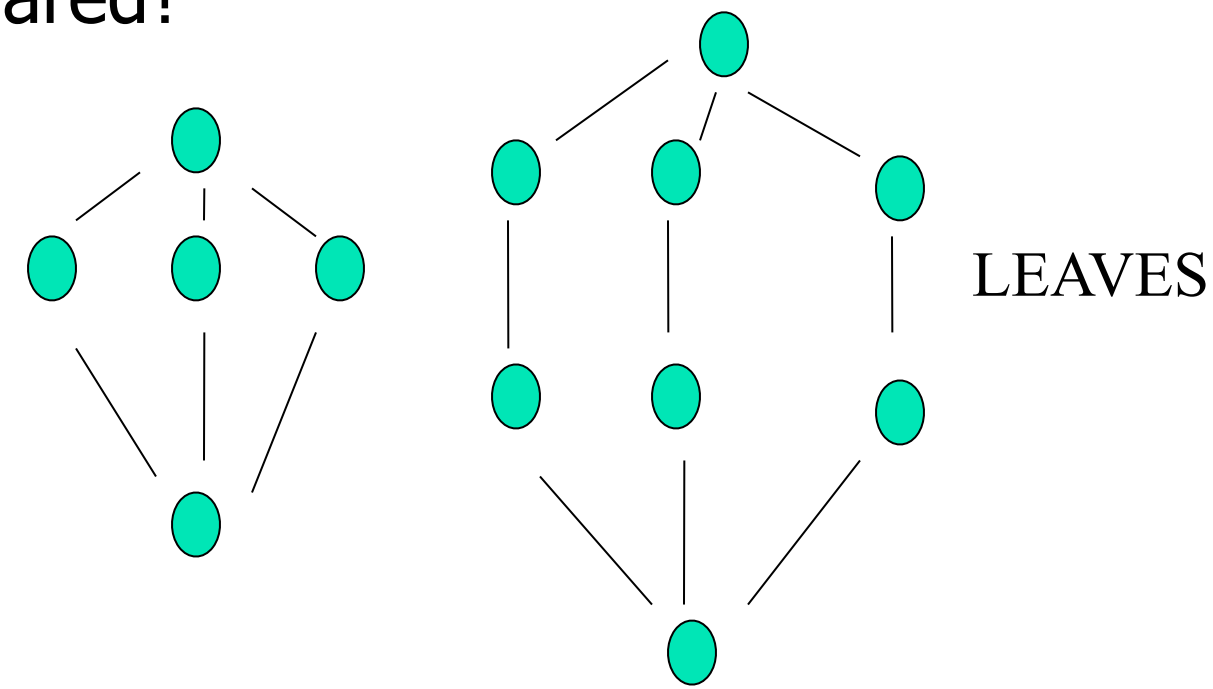
Double-triangle

53 nodes on top
17 new nodes (12 + 4 + 1) on bottom.
Leaves are shared. Total 70



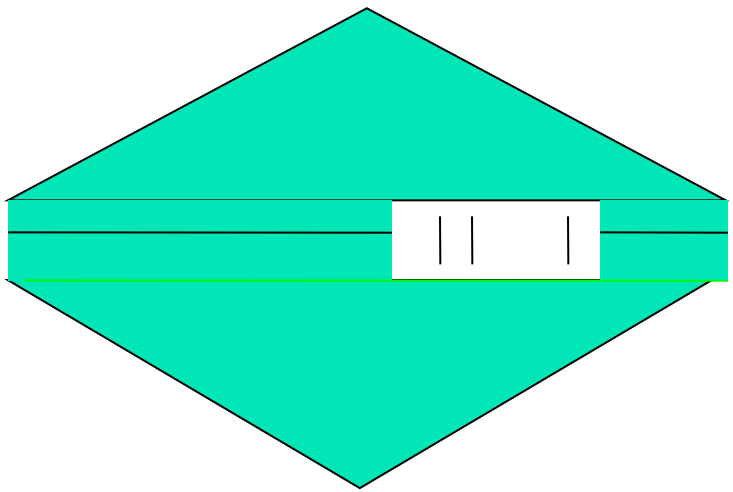
Is that the best?

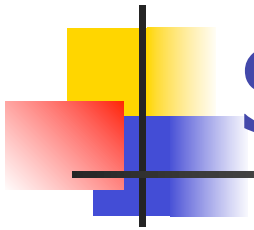
- What if one group of 9 is connected to another group of 9 whereas all other leaves are shared?



Double-triangle

One group of 9 is doubled, so we get 79



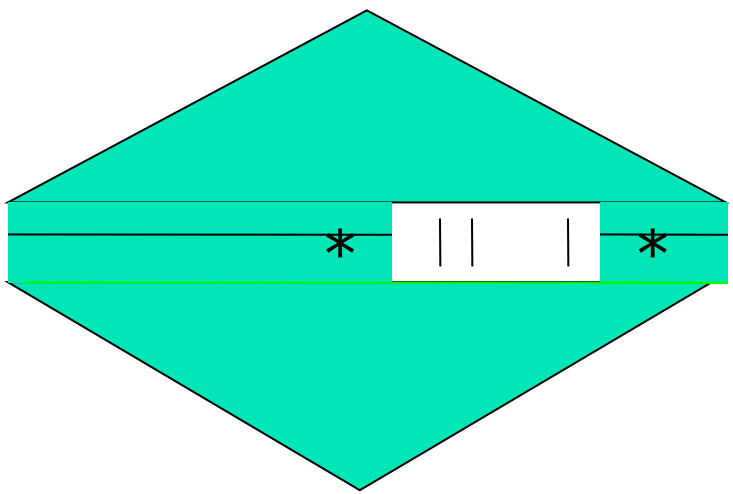


Still more?

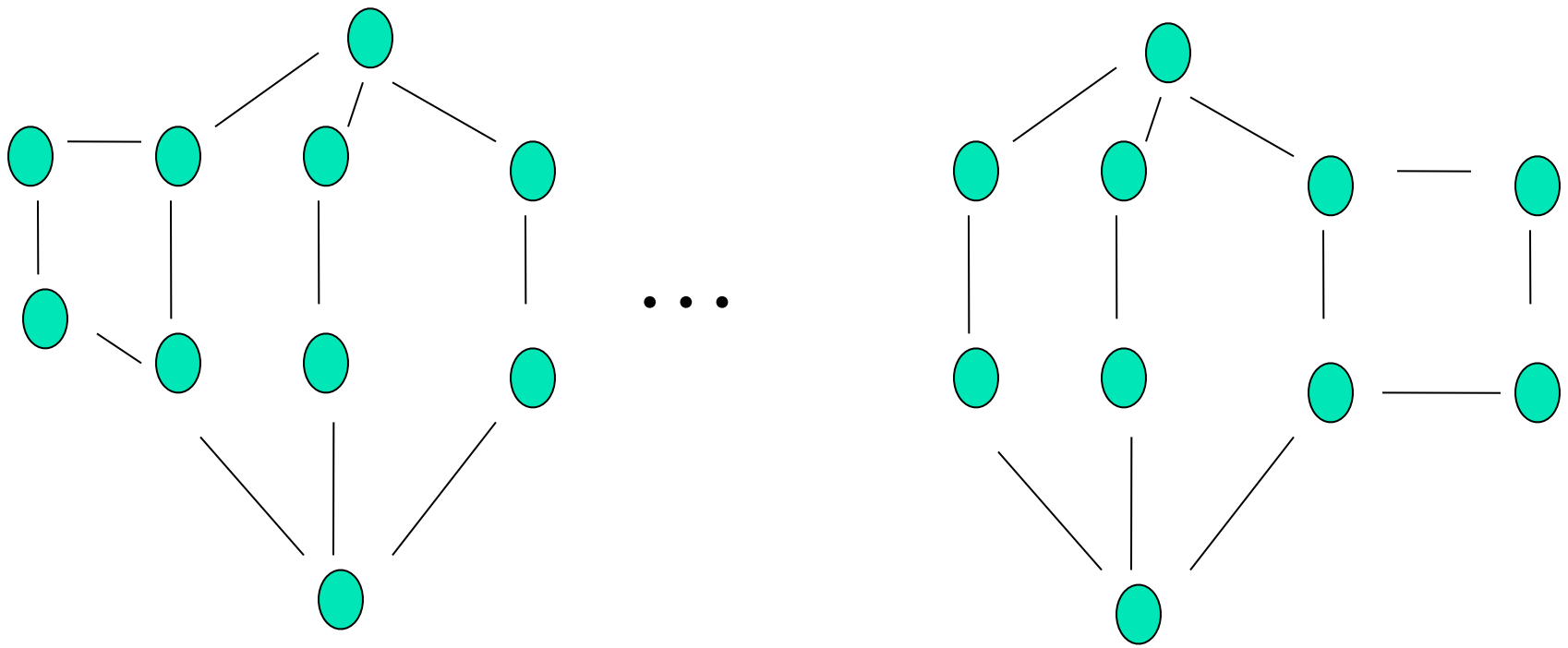
- We now have 70+9 nodes.
- Can we get more?
- Nothing obvious; can’t double everywhere.

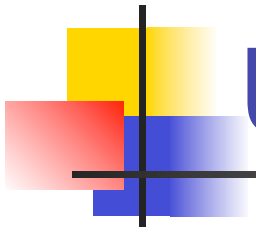
Finished Yet?

A careful look shows you can double up on borders of the 9 already doubled ones.



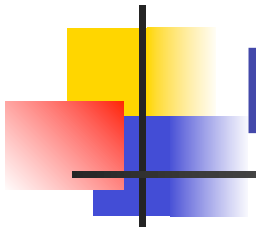
A little delicate: one new pair to each end





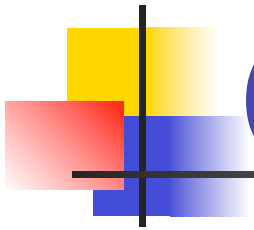
Upstart Architect

- Is there something magical about 81 that is impossible to beat?
- No solid quantitative theory of extremal graphs.
- Or have you found one?



Prime Geometry Game

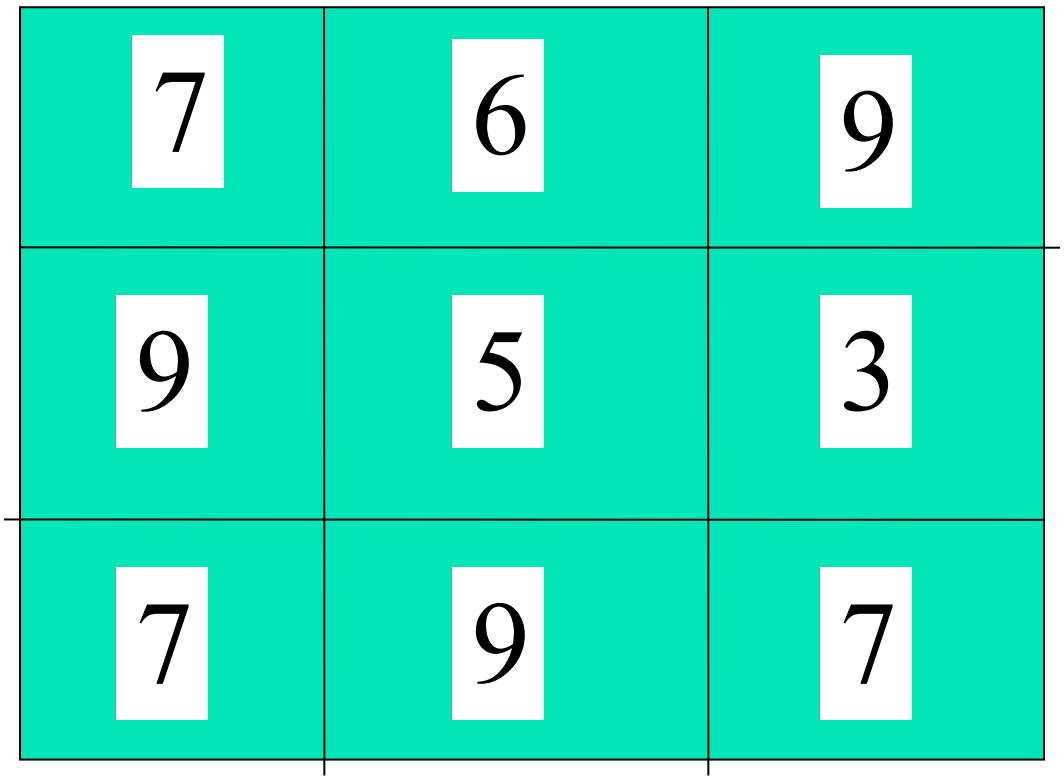
- Primes are a topic of enduring interest. “God gave us primes.” “Describe pictures to alien civilizations using N bits where N is the cube of a prime.”
- Lots is known about the density of primes.
- What about the density of the geometry of primes?



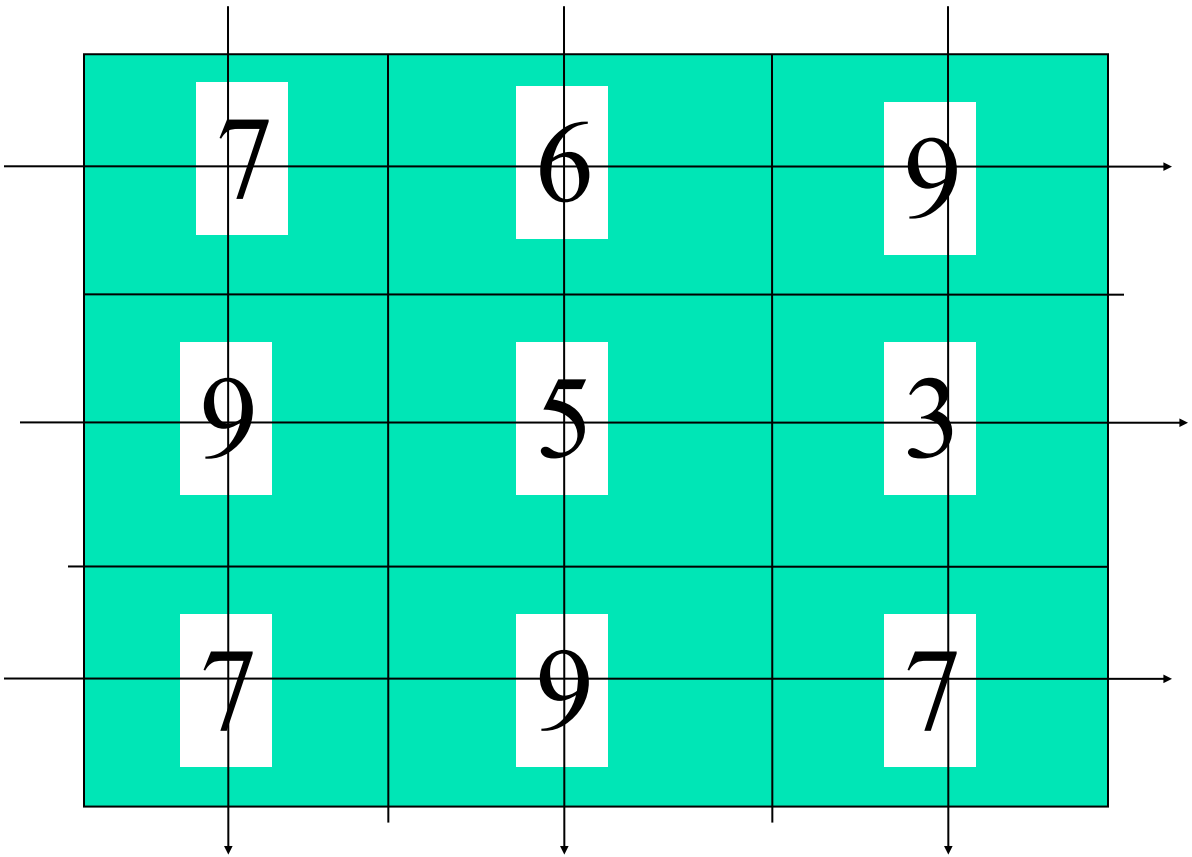
Prime Squares (base 10 version)

- Square grid whose rows and columns are prime numbers. No two rows are same; no two columns are same.
- Ambidextrous if rows are also prime right to left.
- Omnidextrous if ambidextrous and columns are primes down to up and diagonals in all directions.

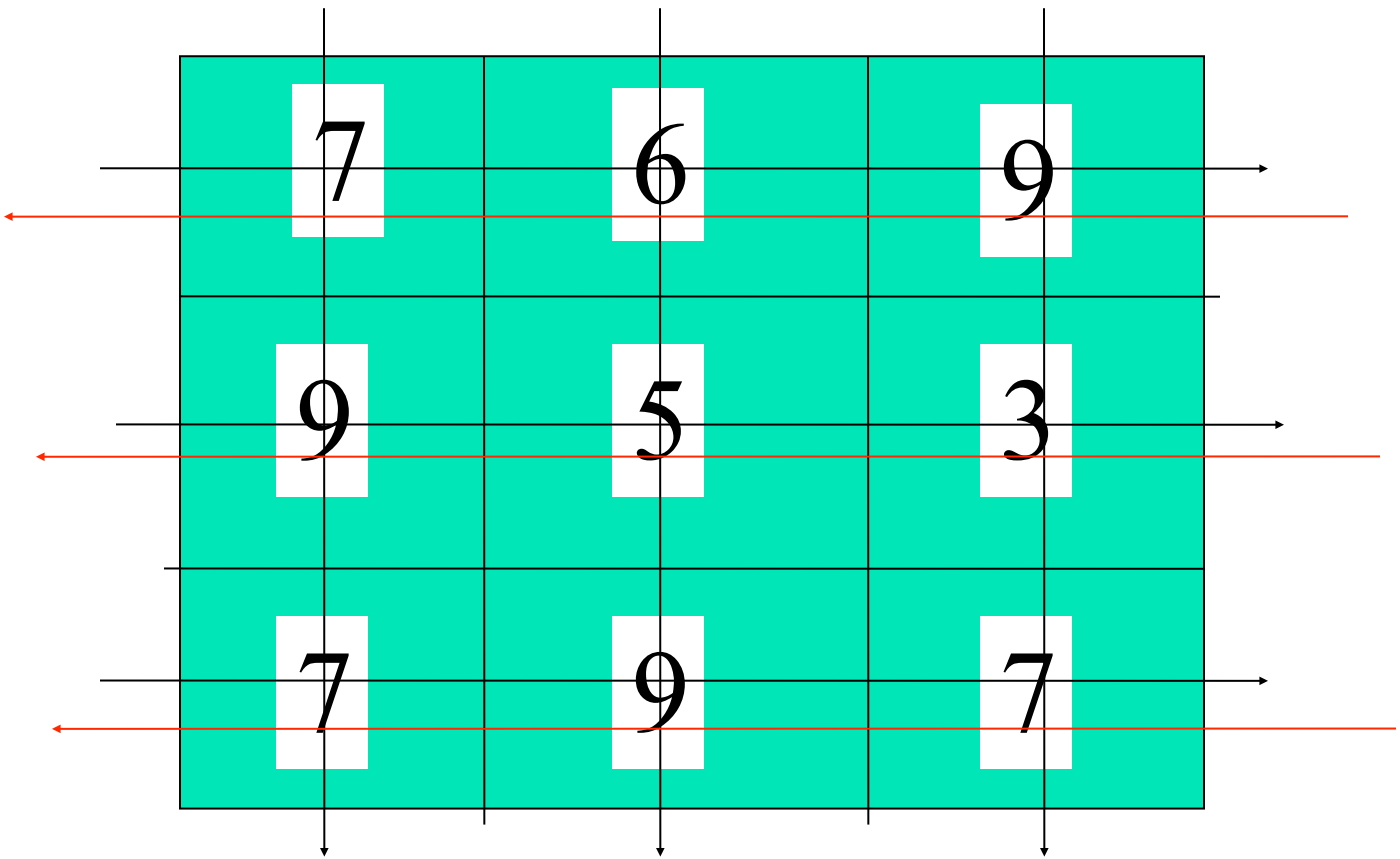
What Kind of Prime Square is this?



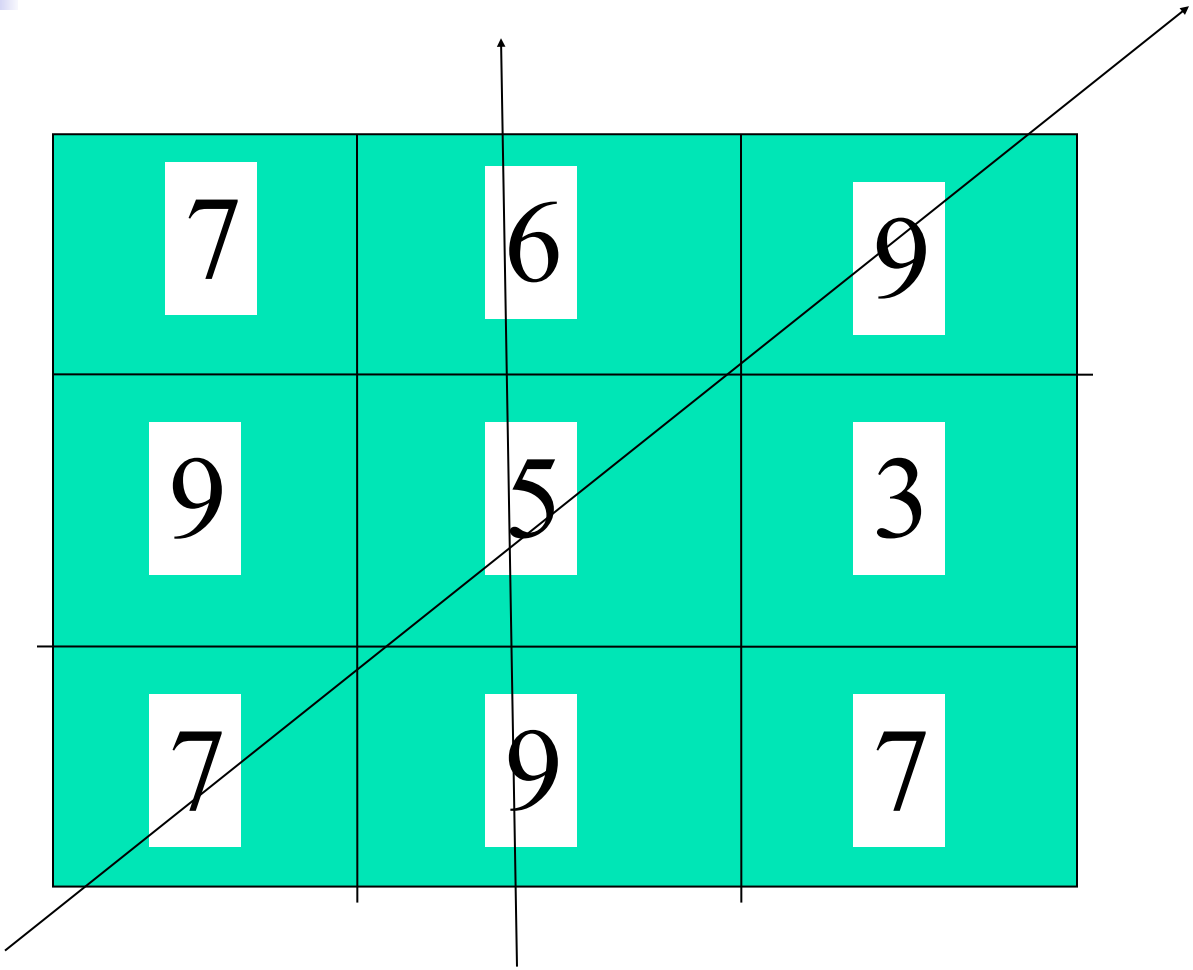
It's a Prime Square



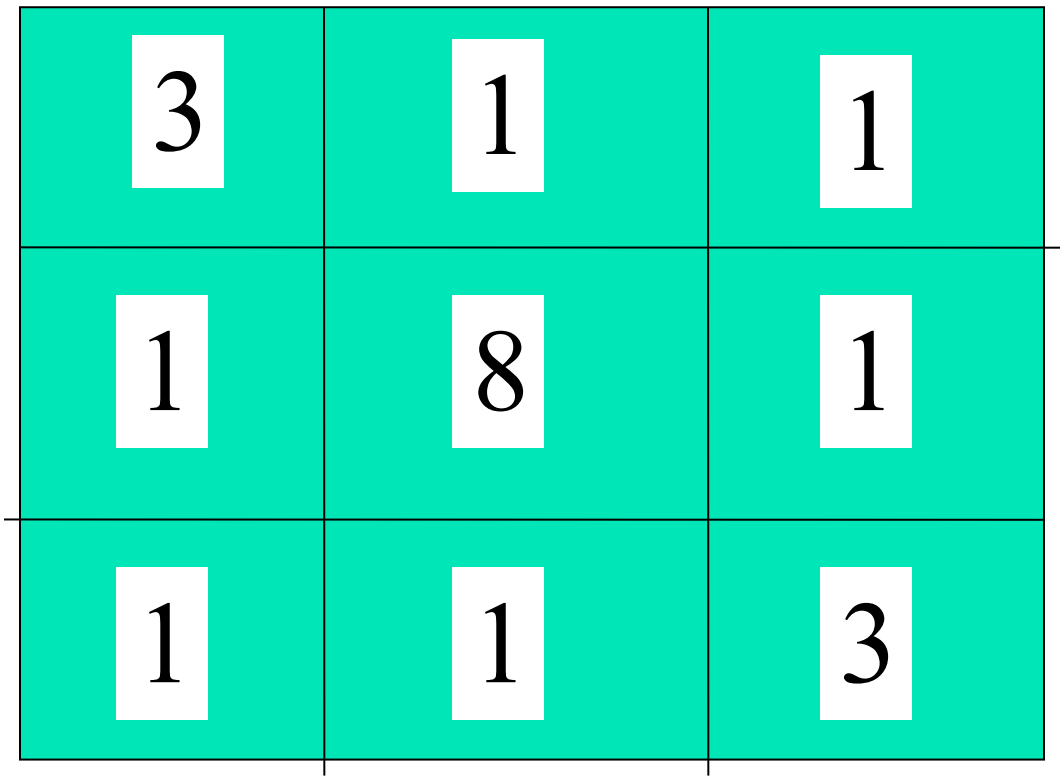
It's an Ambidextrous Prime Square

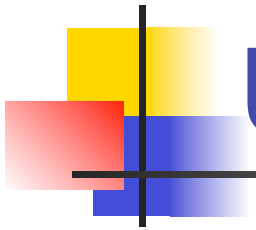


It's not Omnidextrous



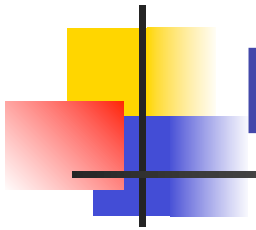
An Omnidextrous Prime 3-square using three digits





Upstart Questions

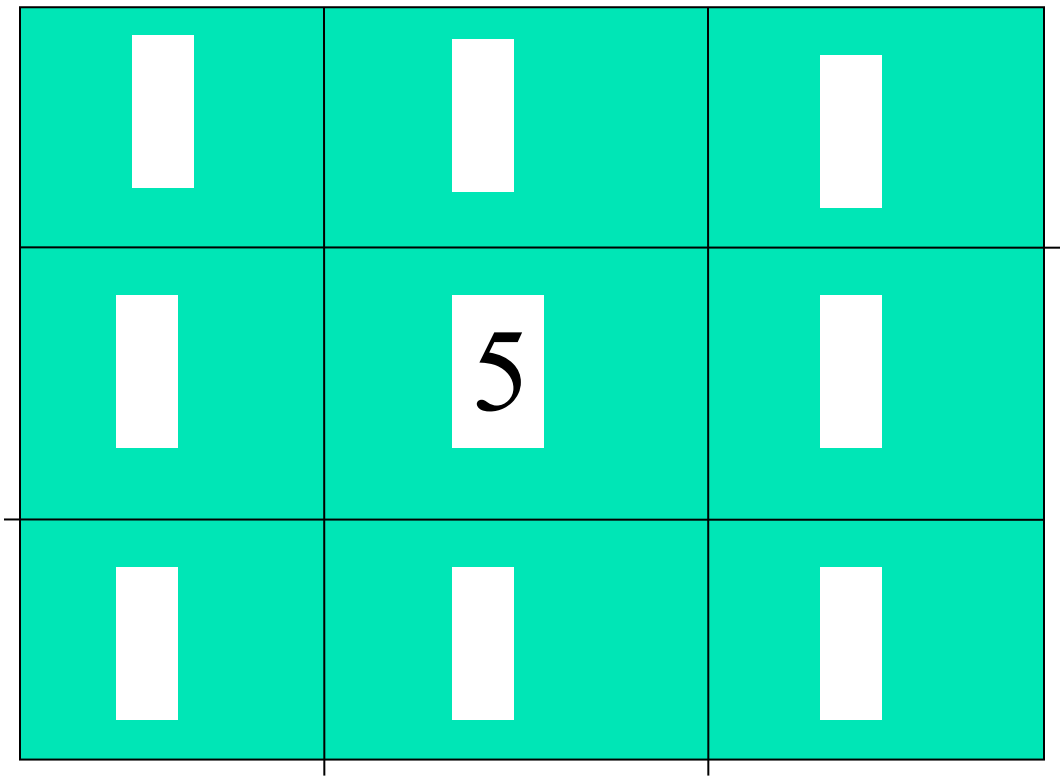
- For which n are there prime ambidextrous/omnidextrous n-squares? (Density of primes suggests that prime n-squares should be easy to find as n gets larger.)
- For each such n, how few digits can be used?



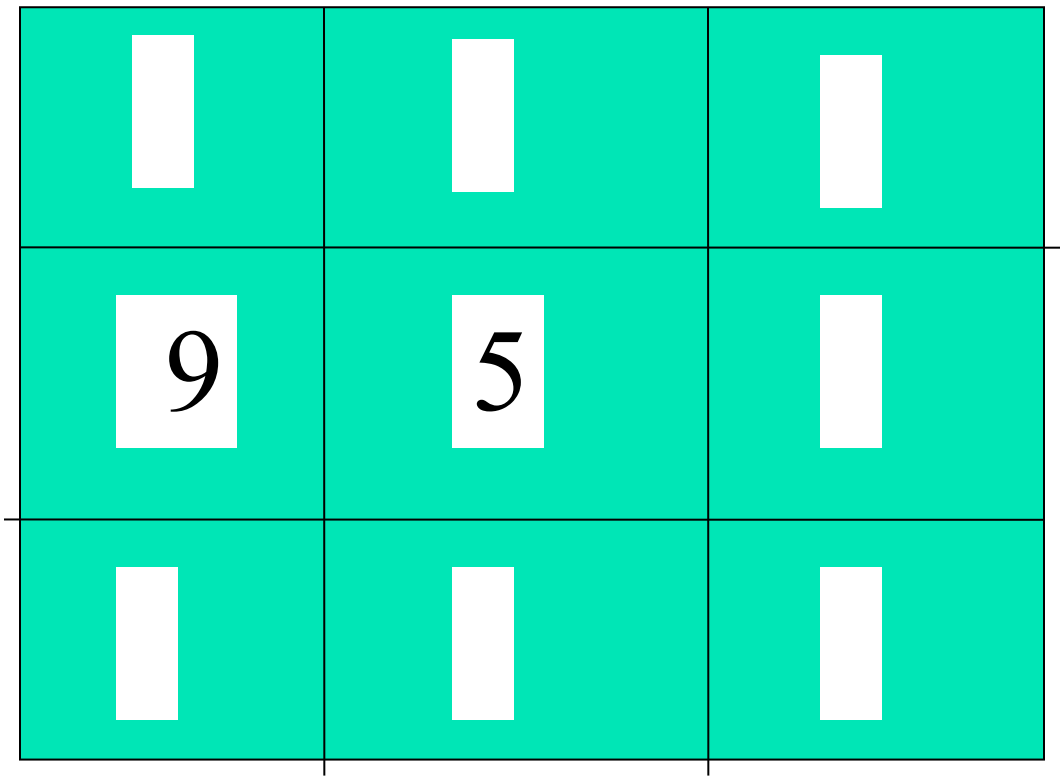
Prime Geometry Game

- Suppose we can play a game on an n x n board, n odd, in which players alternate by placing numbers on the board except the second player gets the last two moves.
- If a move completes one or more n digit primes in any direction for the first time, then the player gets points = number of new primes.

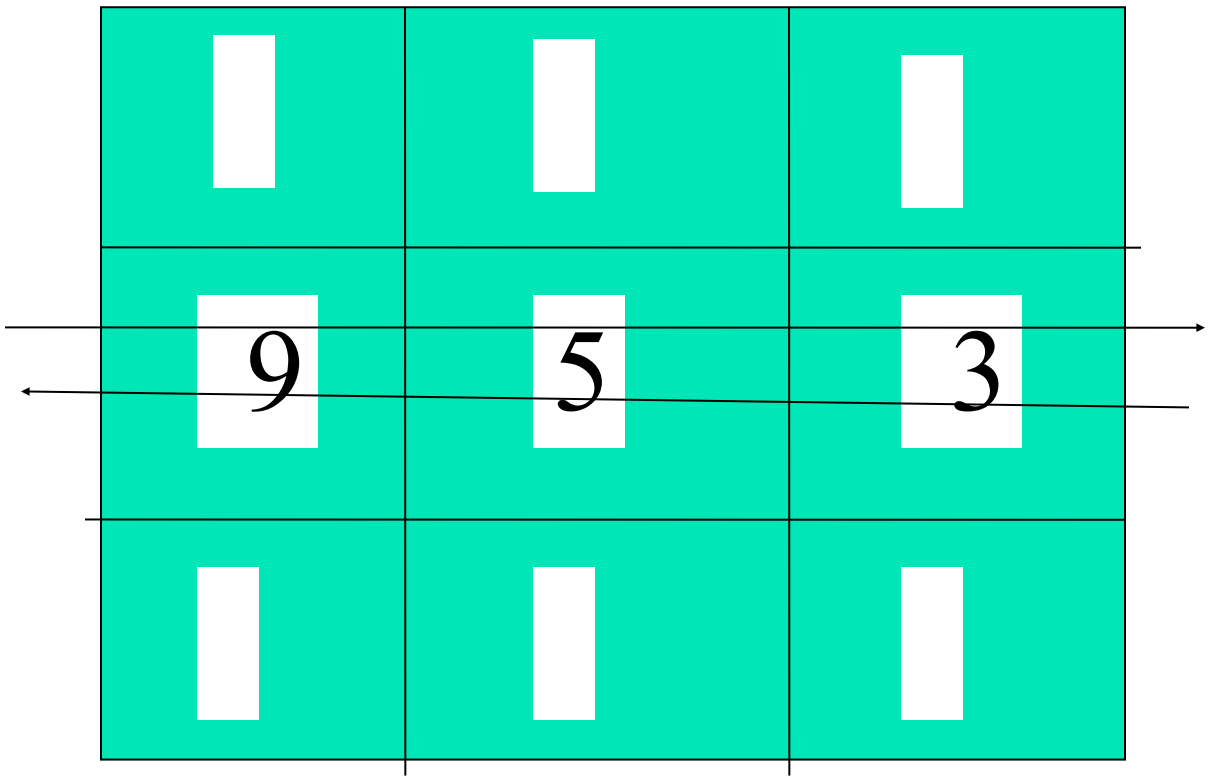
Development of Game: Player 1



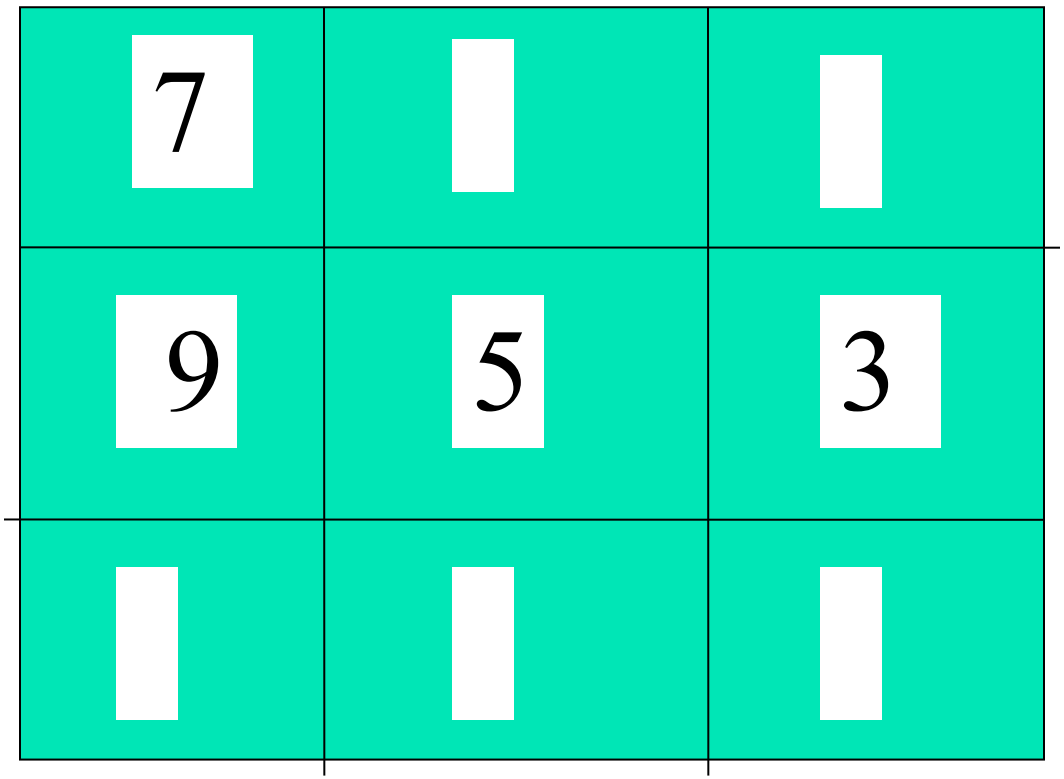
Development of Game: Player 2



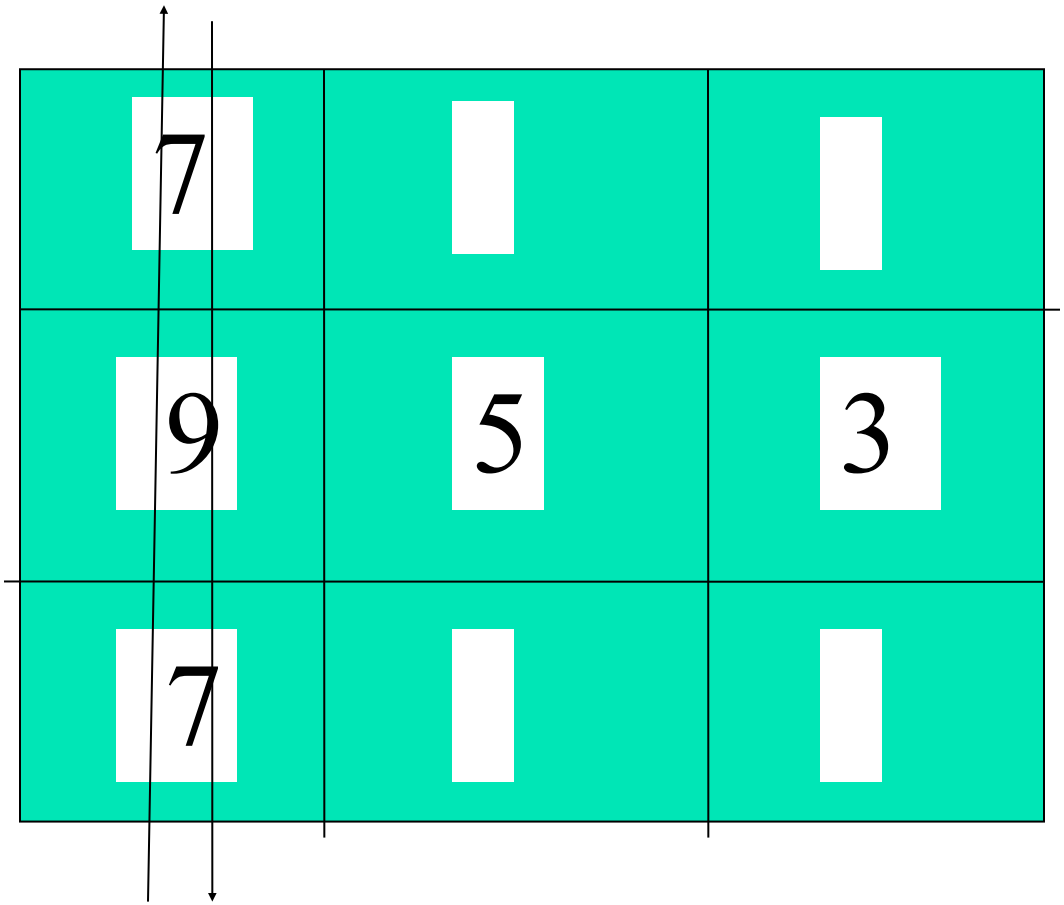
Development of Game: Player 1 wins two



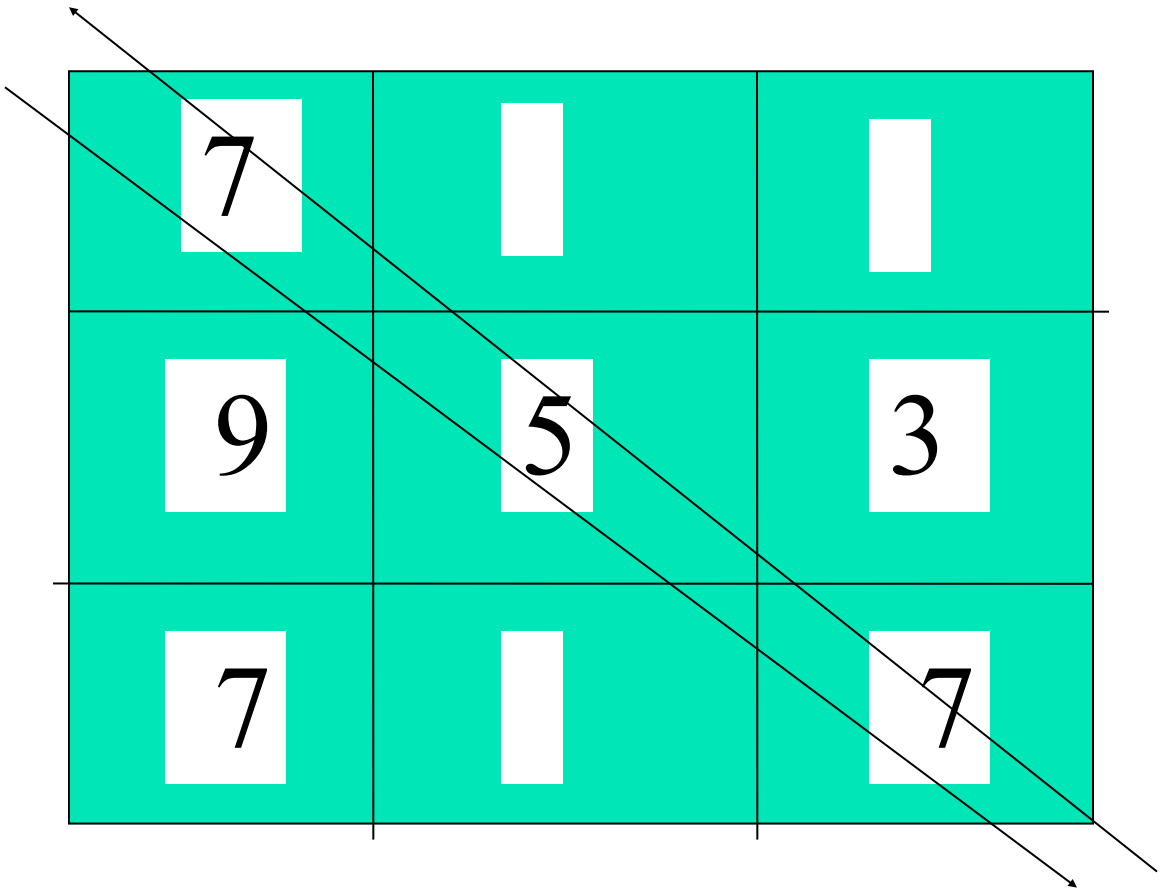
Development of Game: Player 2



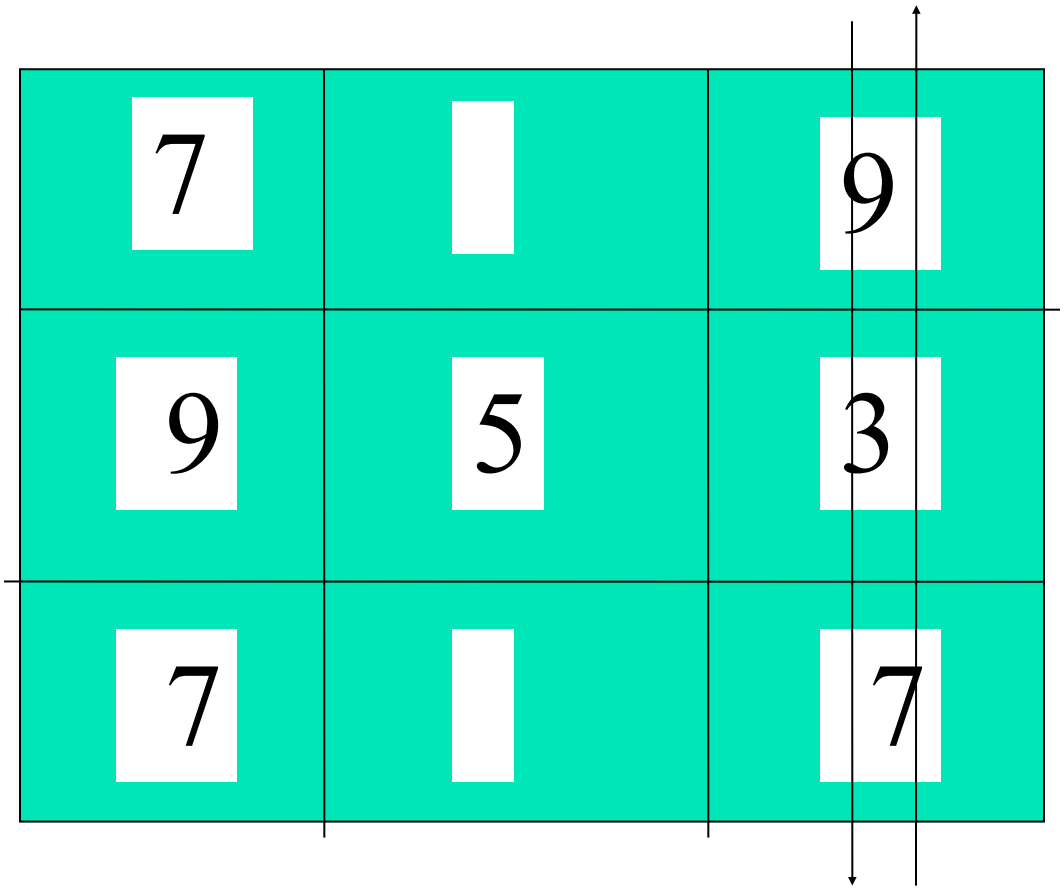
Development of Game: Player 1 wins two more (4)



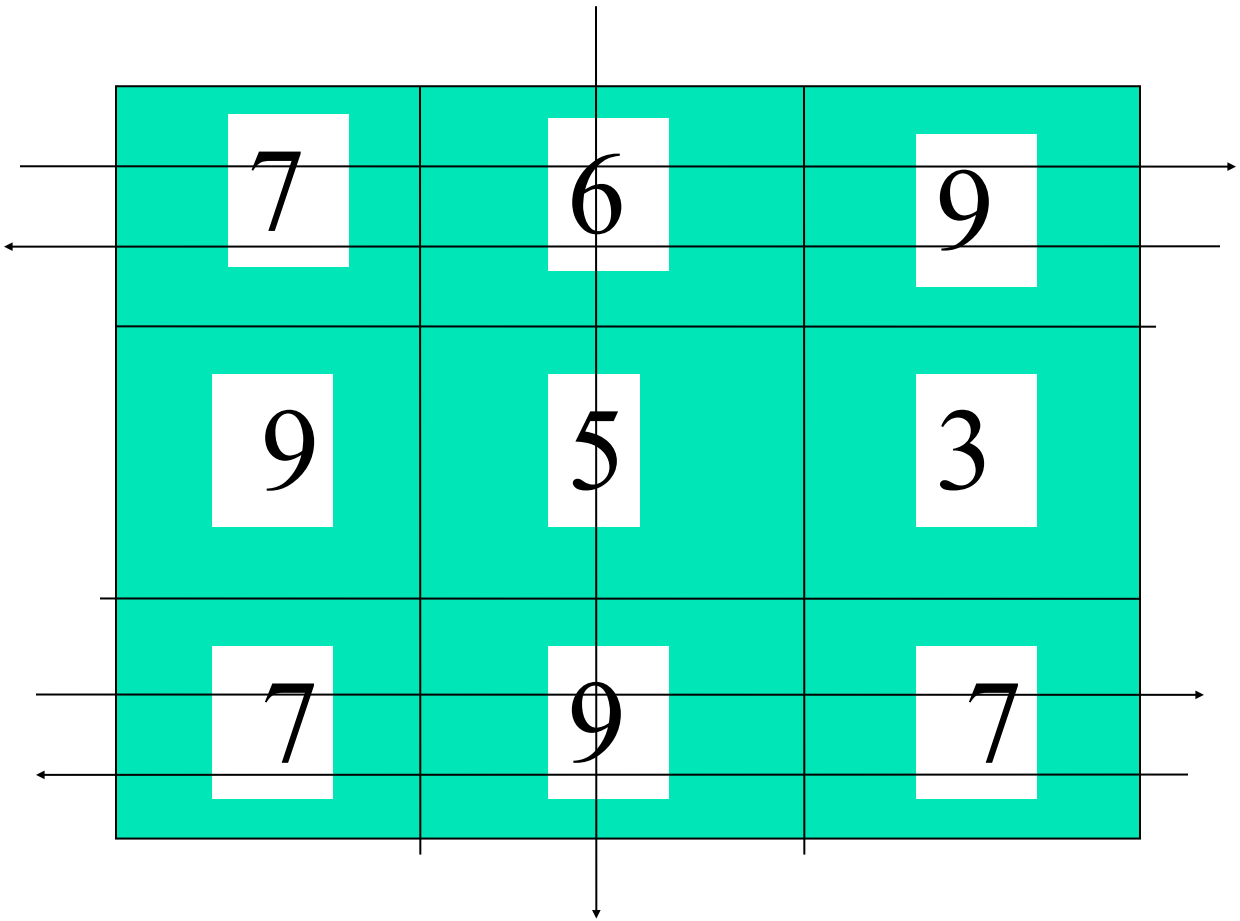
Development of Game: Player 2 wins two

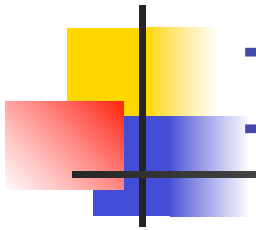


Development of Game: Player 1 wins two more (6)



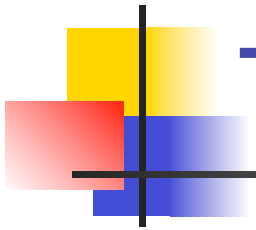
Development of Game: Player 2 gets five (7)





In general?

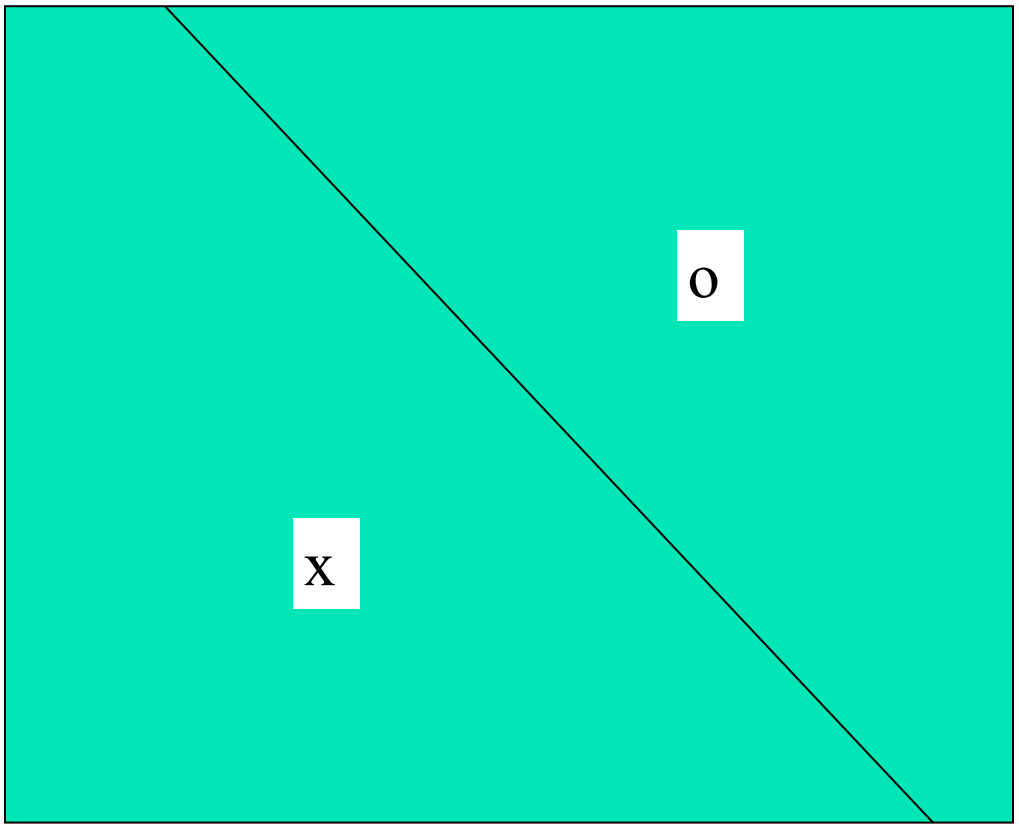
- First player has a big advantage at the beginning, but second player wins many points at end by filling the last two places.
- Can you find a guaranteed winner for n x n prime square, where n is odd?



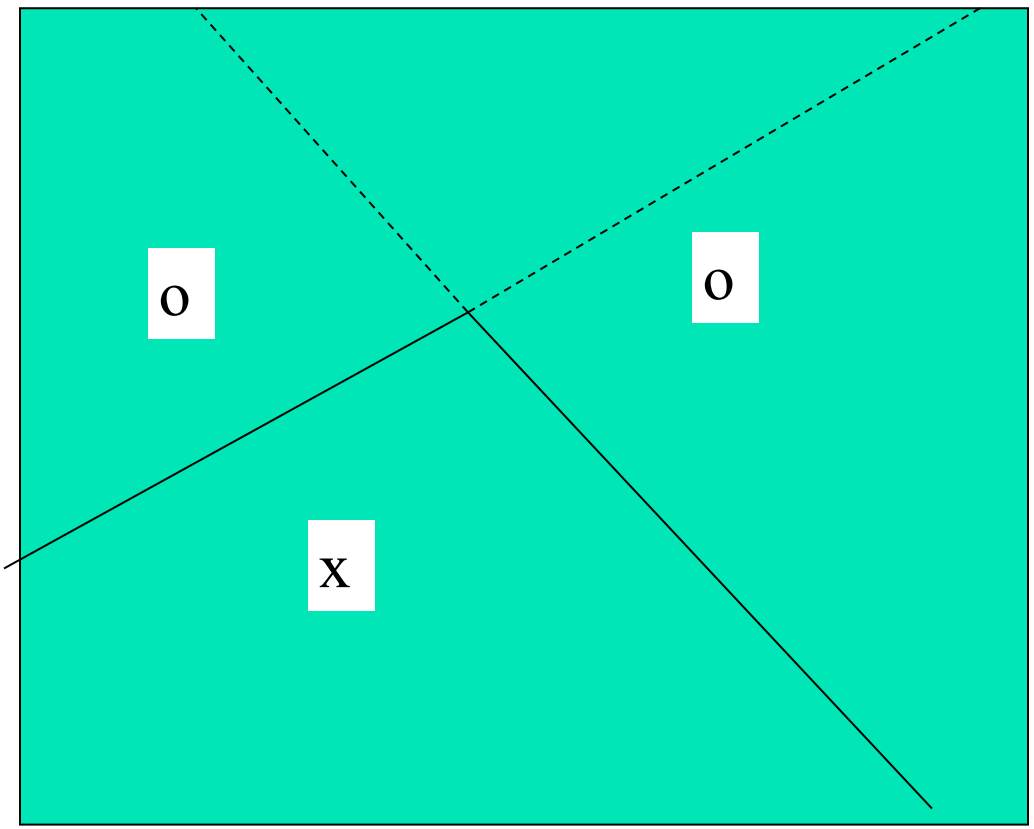
Territory Game

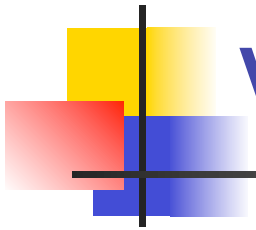
- Best real estate can be underwater.
- Islands can define borders.
- Falklands/Malvinas brought the belligerents to Dr. Ecco in 1991.
- Borders at sea determined by a Voronoi diagram.

Voronoi Diagram of two points



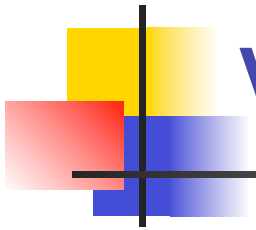
Voronoi Diagram of three stones (except two os)





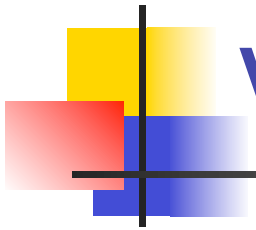
Voronoi Definition

- Given a set of stones, a Voronoi diagram is a tessellation of the plane into polygons such that (i) every stone is in the interior of one polygon and (ii) for every point p in the polygon P containing stone x, p is closer to x than to any other stone.



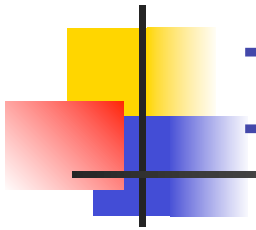
Voronoi/Territory Game

- Given k stones each, first player places a stone, then second player places two stones, then first player places one stone, second player one stone, until the first player places kth stone.
- You win if your polygons contain more area than my polygons.



Voronoi Upstart Questions

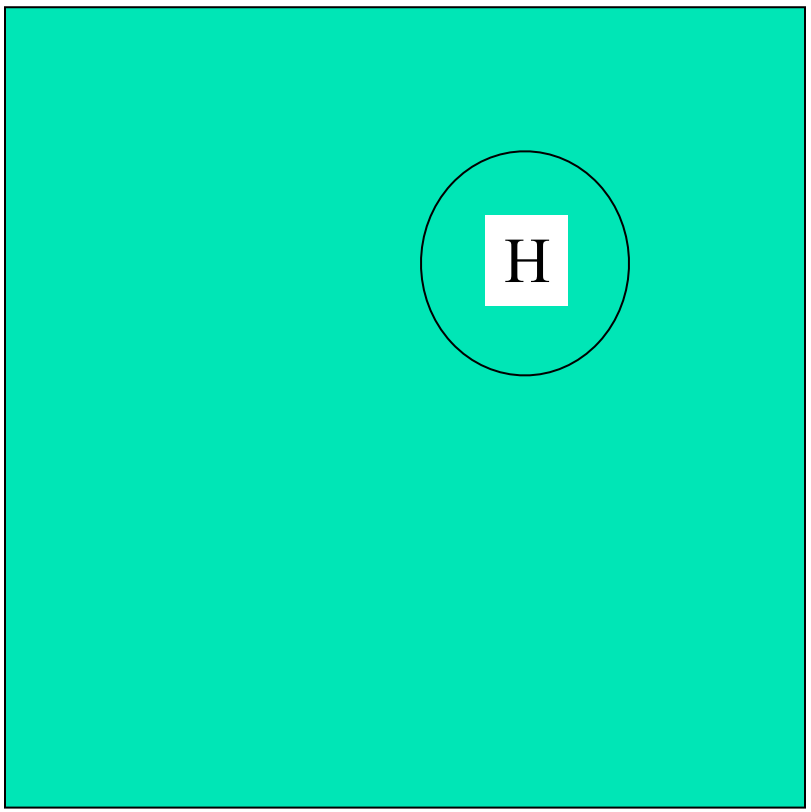
- Does either player have a winning strategy?
- Can the winning strategy extend to the place/snatch variant in which k stones are laid down by each player and then j ($j < k$) are removed?
- Look up “voronoi game” on google.



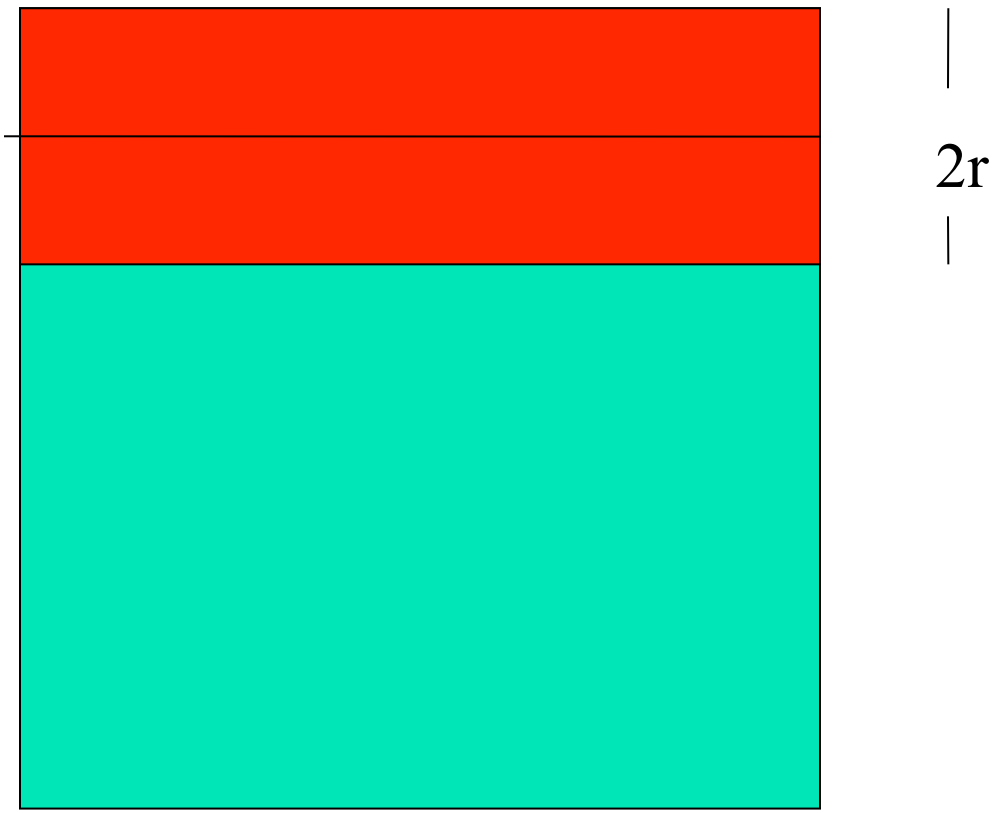
Injured Hiker's Problem

- A hiker is injured in a thick forest in a square valley of size m x m.
- His distress signal has a range of r (<m/2)
- You may start at any edge of the square and you want to guarantee to detect the signal by traveling continuously as little as possible.

Hiker's distress signal has a limited range

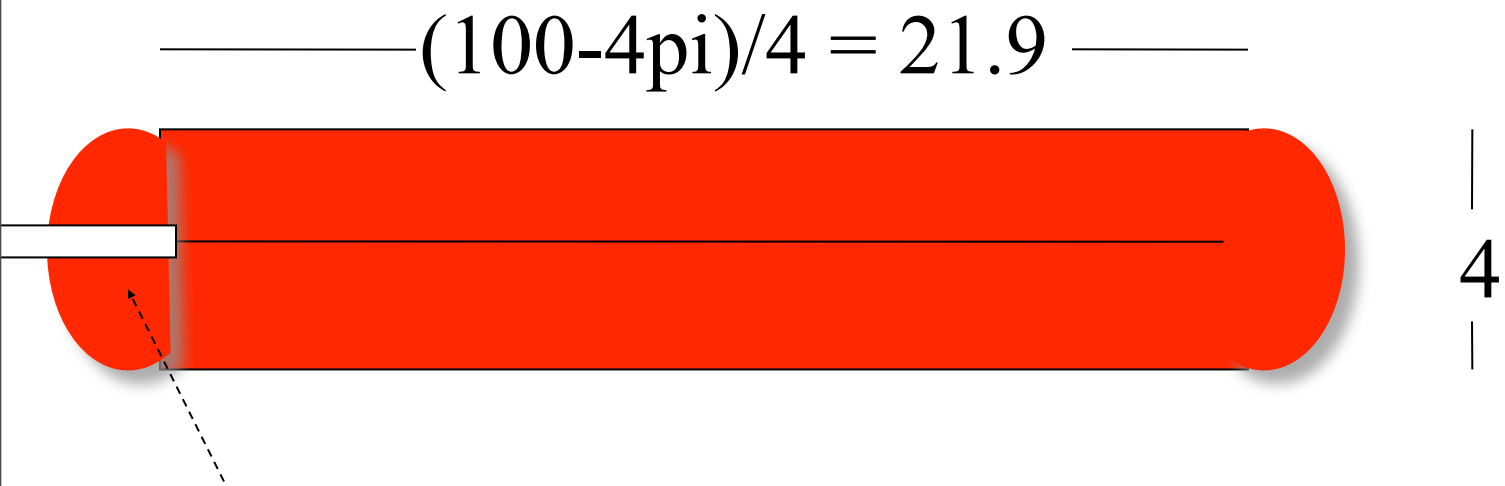


Line segment covers 2r swath



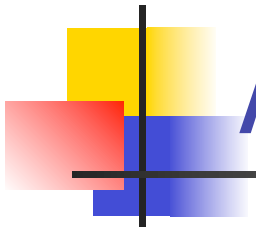
Does long rectangle give

Tack on a semi-circle at both

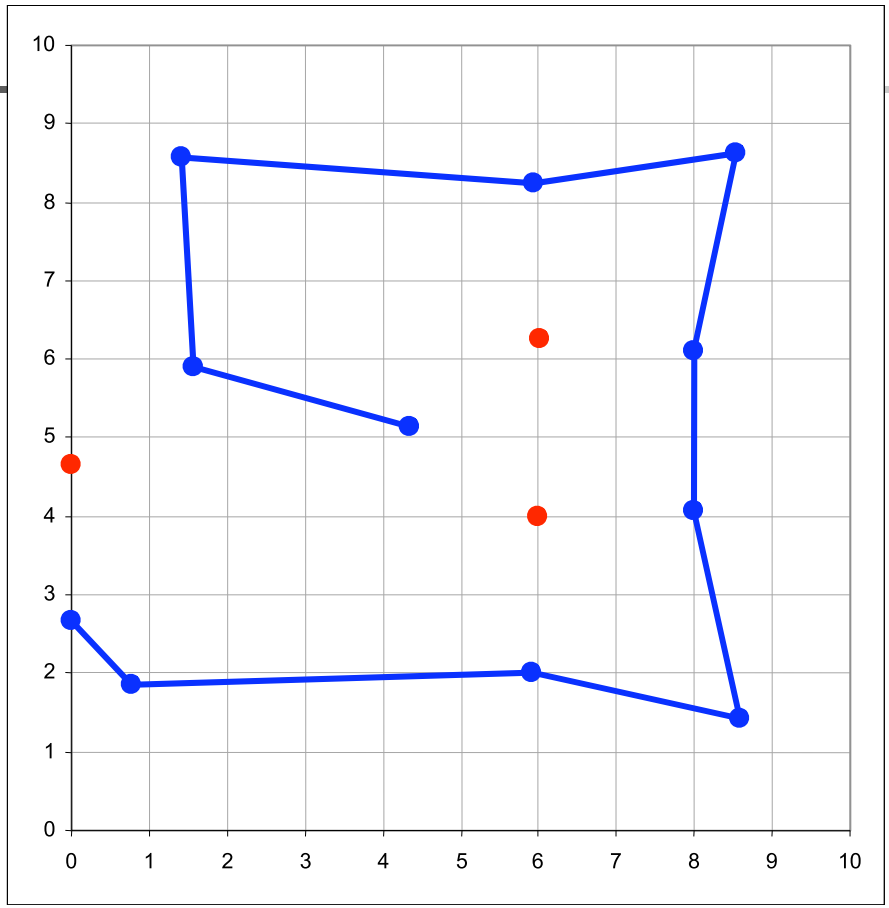


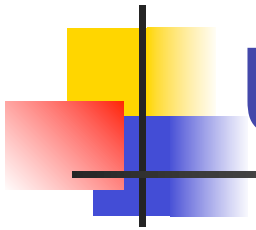
Narrow road to the edge

DeMaine father/son Achievement



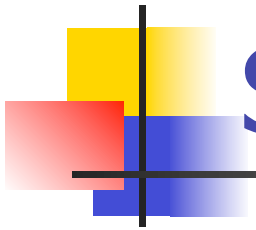
- Assume m is 10 miles and the hiker's distress transmitter has a 2 mile range.
- Demaine duo found a sub-30 mile search path with a strange figure made up of line segments including several slightly non-perpendicular angles.
- Better solution by Matthew Self


10
9
8
7
6
5
4
3
2
1
0
0 1 2 3 4 5 6 7 8 9 10



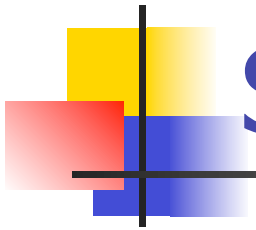
Upstart Hiker's

- How close to 21.9 miles is possible?
- What happens if you have some speed, say 1 mile per 10 minutes and the distress signal goes on and off at alternating minutes?



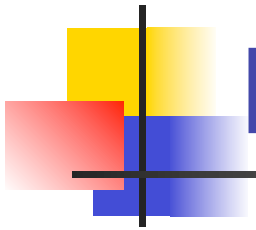
Strategic Bullying

- Wars/fights often happen because one or both sides think they will win easily.
- Alliances can sometimes lead to peace, or not.
- Is there a simple insightful model?



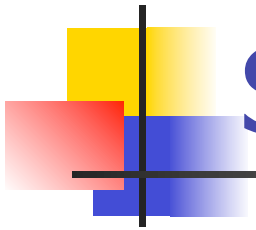
Strength and Stability

- Suppose that each agent A has a strength s, represented A:s.
- Alliance is sum of strengths.
- In conflict, alliance with most strength wipes out losing alliance. Booty divided. No gain/loss in strength to fighters.
- Attacker confronting a stronger defensive alliance simply gives up.



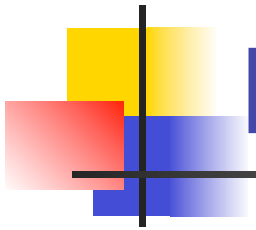
Example

- A: 4, B: 2, C: 1. A attacks both of the others and simply wins.
- A: 4, B: 3, C: 2. If A threatens B, then C will form an alliance with B. However, C is not willing to form an alliance with B to threaten A.
- Do you see why?
- Divide and conquer could work for A.



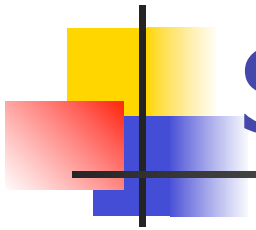
Stability

- A: s alone is stable. No fight.
- A:s, B: s is stable.
- However, A: s, B: s, C: s is not stable because any two can wipe out the third and then be stable.
- A: s, B: s, C: s, D: s ?



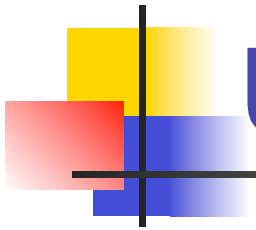
Risk-averse or Risk-ready

- Risk-averse: Don't attack if as a result, someone with your strength could be wiped out.
- Risk-ready: Don't attack if everyone with your strength will be wiped out.
- A: s, B: s, C: s, D: s is stable if risk-averse, but not risk-ready.



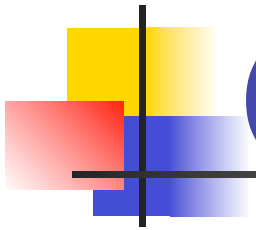
Stability Theorem

- If a set X has a stable proper subset Y such that Y has more than half the total strength of X, then X is unstable.
- Works for either risk-ready or risk-averse.
- Ex: A:1, B:2, C:3, D:4, E: 5, F: 6



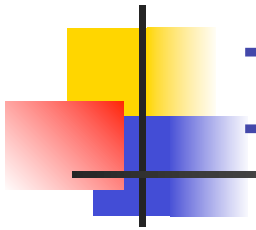
Upstart challenge

- Given a set of agents with strengths, is the set stable?
- If not, is it possible to find the largest subset that is stable under risk-averse settings?



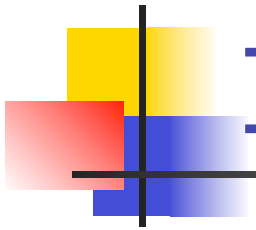
(In)Conclusions

- As Dr. Ecco reminds me, puzzles have a personality.
- Some nasty, some sweet. Some fiendish.
- The best ones are fiendish.
- Still open.



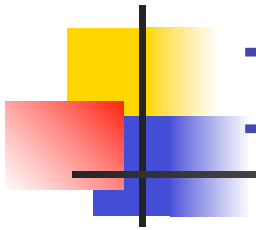
Intacto

- Movie with Max von Sydow and others: premise is that luck is a quality that sticks to a person but can be removed by a special touch.
- Much of the movie concerns the search for lucky people.
- Run through a forest blindfolded: too slow, you lose; too fast, you hit a tree.



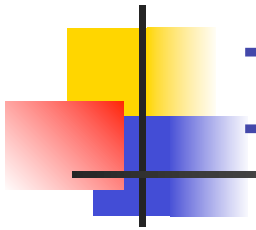
Intacto Purified

- N people, B bets.
  Initial wealth 100 units.
- Each bet is an even money bet depending on the flip of a single fair coin that all people see.
- Each person bets an amount of his/her choosing (but no more than he/she has at that bet) on either heads or tails.



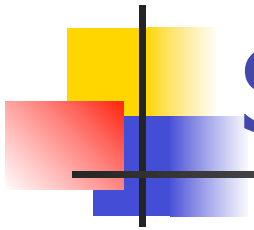
Intacto Purified Goal

- Get greatest number of units after the B bets (ties are no good).
- Greatest number of units → you win. Else, you lose.



Intacto Purified Confession

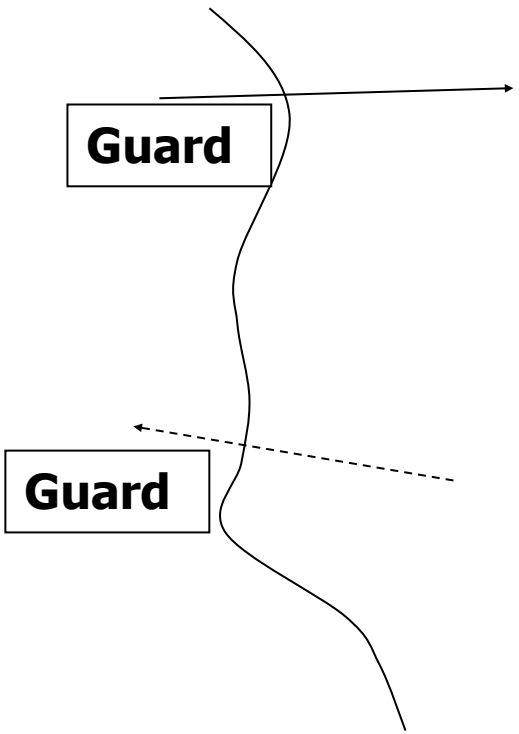
- This one may not be that hard but I like it because it shows something about human nature:
  If there are only a few people pursuing a goal, then they are likely to take fewer risks. Many, then more risks. Extreme sports, ballet, … corporate executive suites?

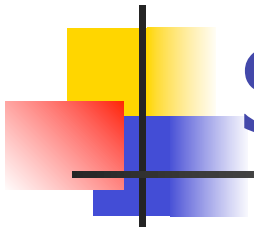


Spy vs. Spy

- In 1958, John McCarthy proposed the following puzzle to Michael Rabin.
- **There are two countries in a state of war. One country is sending spies into the other country. The spies do their spying and then they come back. They are in danger of being shot by their own guards as they try to cross the border.**

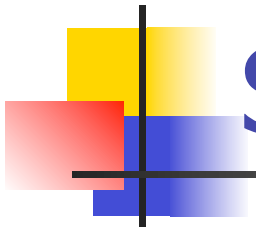
Spies Enter and Leave





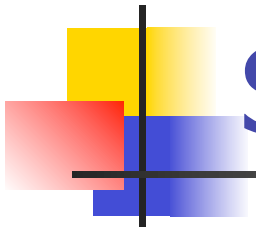
Spy vs. Spy Goal

- **So you want to have a password mechanism. The assumption is that the spies are high caliber people and can keep a secret. But the border guards go to the local bars and chat---so whatever you tell them will be known to the enemy**



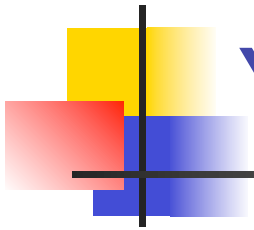
Spy vs. Spy Goal

- **Can you devise an arrangement where the spy will be able to come safely through, but the enemy will not be able to introduce its own spies by using information entrusted to the guards?**



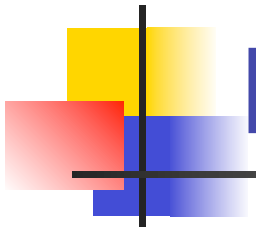
Spy vs. Spy Hint

- **Rabin made use of the following procedure first introduced by Von Neumann to generate pseudo-random numbers: take an n digit number x, square it and take the middle n digits yielding y.**
- **Easy to go from x to y, but hard from y to x….**



Your Turn

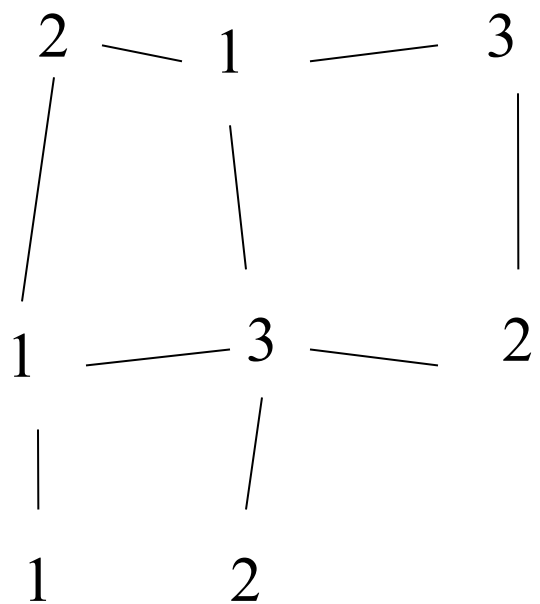
- Answers? ....



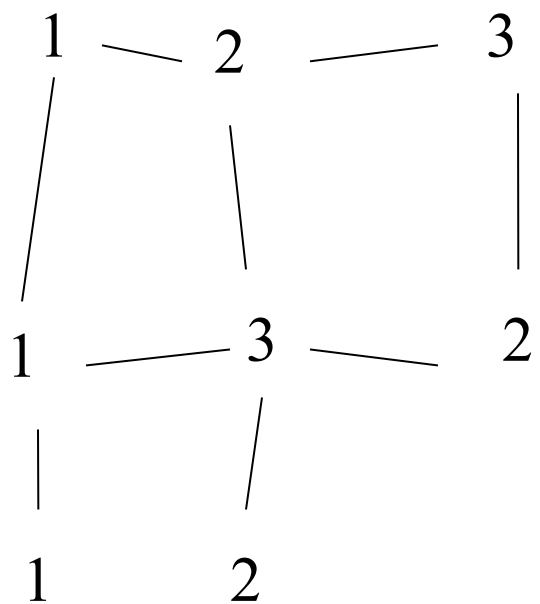
Diplomacy for Fanatics

- I’m not a cynic, really….
- Graph with k populations all mutually antagonistic.
- Want to swap node colors using fewest pairwise swaps so all nodes of same color are connected. (Connection graph is planar.)

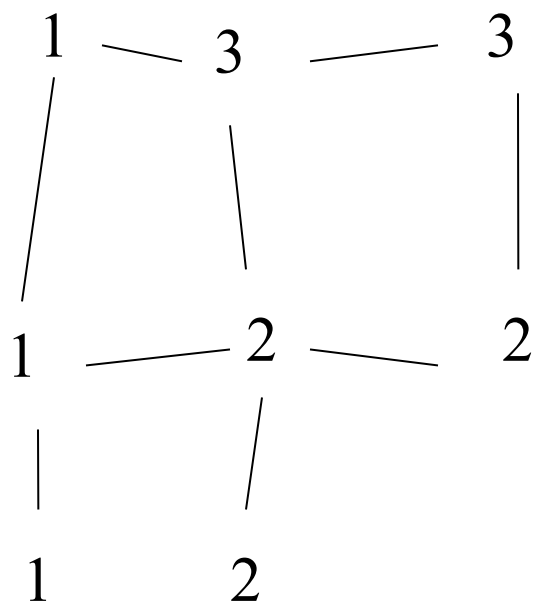
Two swaps are enough

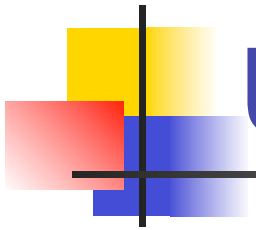


Swap 1



Swap 2





Upstart Fanatic Diplomacy

- Here the swaps were among neighboring nodes.
- Another variant is to ask about the fewest swaps whether among neighbors or not.
- I don’t know how to solve this problem in any reasonable time as the graph grows.