Math 310: Introduction to Modern Algebra: Fall '25 (Siena University)

Professor Steven J Miller: sjm1@williams.edu

Homepage:

https://web.williams.edu/Mathematics/sjmiller/public_html/310Fa25/

Lecture 01: 9/2/25: https://youtu.be/pML2PV6-0LM

Introduction: Motivation through Cryptography.
Notes: https://web.williams.edu/Mathematics/sjmiller/public_html/310Fa25/310Fa25_lectures.pdf

Grading / Administrative

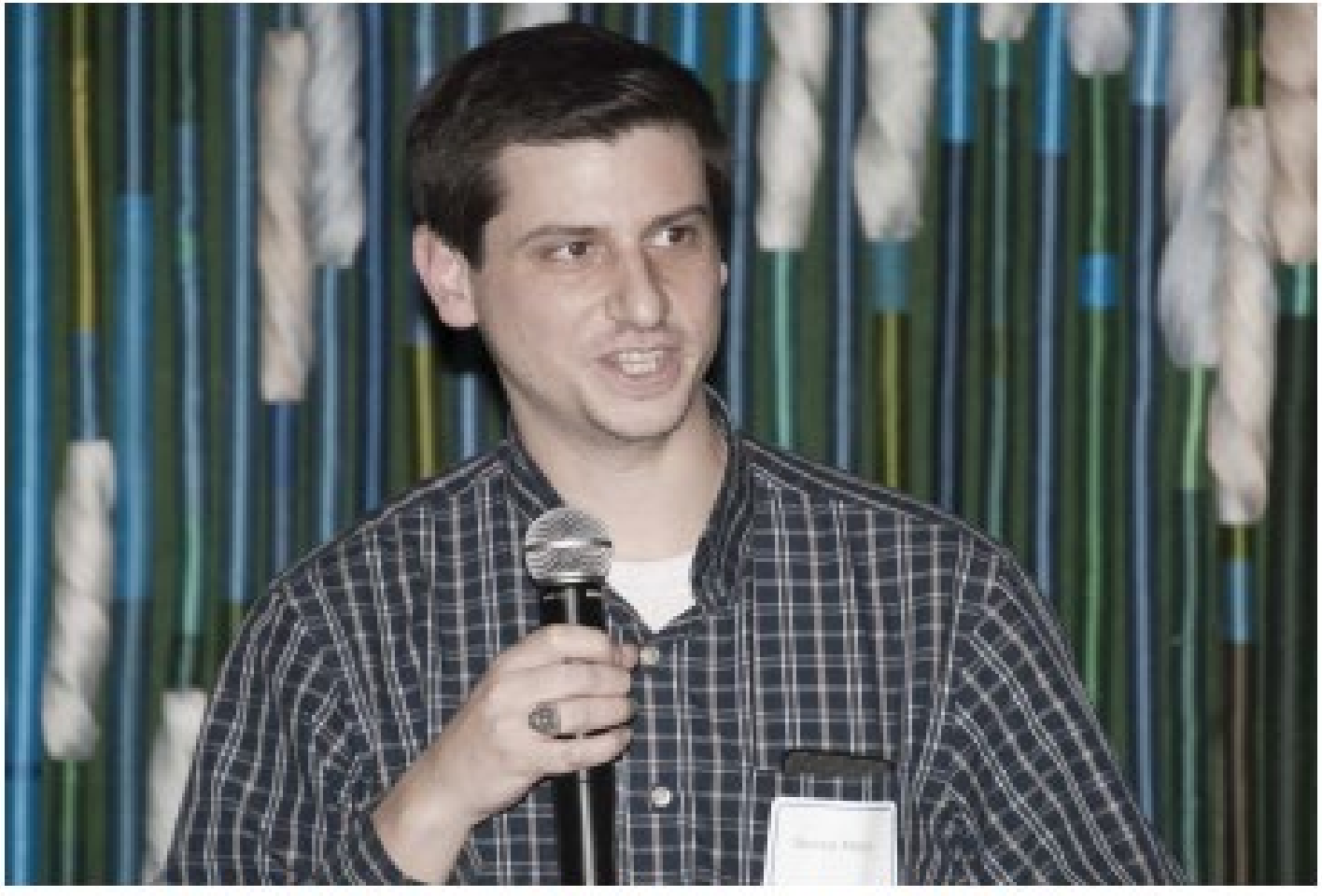
- Move at fast pace: Class Participation: 5%. HW: 15%. Midterm: 40% (if there are two exams only best counts). Final exam: 40%. You may also do a project for 10% of your grade (which reduces all other categories proportionally).
- Pre-reqs: Calc III, basic combinatorics / set theory, linear algebra.

Office hours / feedback

- TBD and when I'm in my office (schedule online)

Being Prepared

Never know when an opportunity presents itself....



S. J. Miller at the Sarnak 61st Dinner

(copyright C. J. Mozzochi, Princeton N.J)

Being Prepared

- Your Job:
  - Be prepared for class: do reading, think about material.
  - Come to me, the TAs and each other with questions.
- My/TAs Job:
  - Provide resources, guiding questions.
  - Be available.

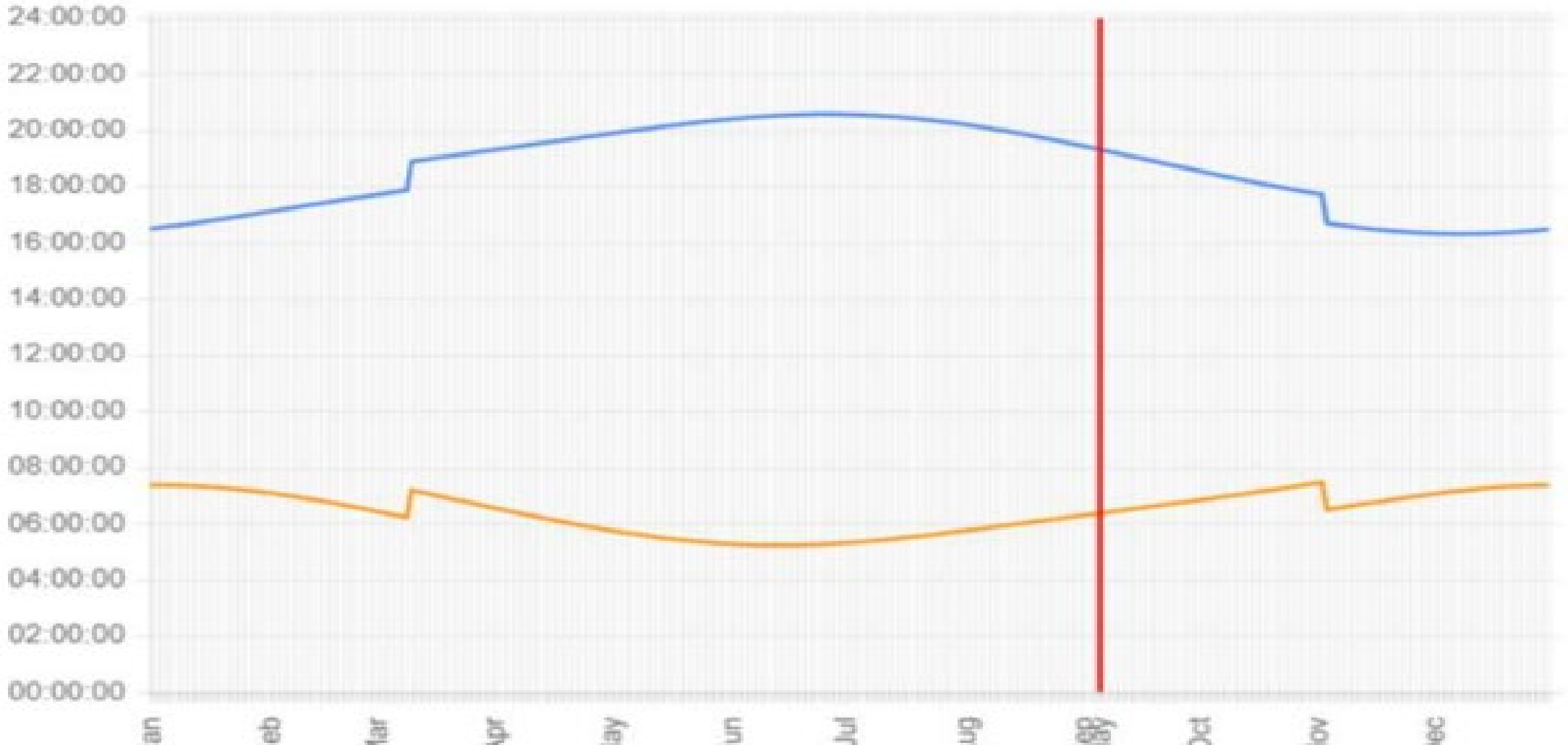
Other: Advice from Jeff Miller

- Party less than the person next to you.
- Take advantage of office hours / mentoring.
- Learn to manage your time: no one else wants to.

Happy to do practice interviews, adjust deadlines....

Year distribution of sunrise and sunset times in North Adams, MA – 2019

https : // sunrise – sunset.org / us / north – adams – ma



Who America is rooting for in the Super Bowl:



Motivation of Modern Algebra through Cryptography:

- Introduction to Cryptography: Alphabet codes pdf

Math 310: Modern Algebra: Fall '25 (Siena)

Professor Steven J Miller: sjm1@williams.edu

Homepage:

https://web.williams.edu/Mathematics/sjmiller/public_html/310Fa25/

Lecture 02: 9/4/24: https://youtu.be/-2TFc7BMcAU

Chapter One: Terminology (1-1, onto, equivalence), Proof Techniques (Induction), Binomial Theorem, Predicting Formulas. Pirate Game Rules.

Notate: 1-1, onto, equivalence

1-1 or injective: means if $f(x) = f(y)$ then $x = y$

↳ example: $f(x) = x$, $f(x) = x - 1$

non-injective: $f(x) = x^2$

onto or surjective: all outputs hit.

$f: S \to T$ $\quad f: S \to f(S)$

$f(x) = x^2$ onto $f: \mathbb{R} \to [0, \infty)$ not $\mathbb{R} \to \mathbb{R}$

Equivalence: reflexive, symmetric, transitive relation

$x \sim x$ $\quad x \sim y \to y \sim x$ $\quad x \sim y$ and $y \sim z$ then $x \sim z$

example: $x \sim y$ if $x - y =$ multiple of 12

Proofs by Induction: Definition, Sum of odds, powers.

$$1+2+3+\cdots+n = S_n$$

$$n+(n-1)+\cdots+1 = S_n$$

$$(n+1)+(n+1)+\cdots+(n+1) = 2S_n$$

$$n(n+1) = 2S_n \Longrightarrow S_n = \frac{n(n+1)}{2}$$

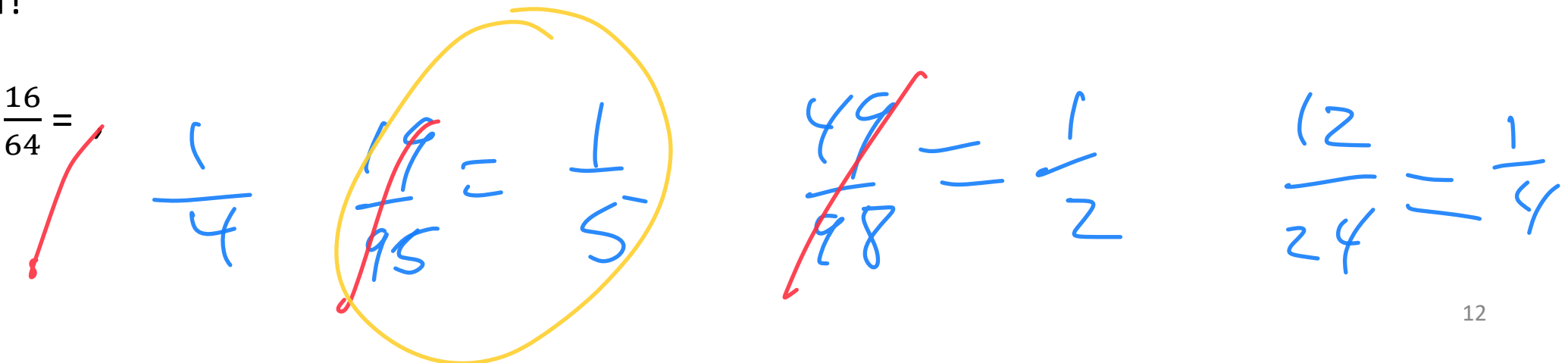
Induction

One of the most important techniques we have for proving results.

Say we have some statement P(n). Perhaps P(n) is “the sum of the first n integers is n(n+1)/2”.

We can check this for various n; every time we check it is true but that is NOT the same as a proof!

Example: $\frac{16}{64}$ =



Induction

Say we have some statement P(n).
Perhaps P(n) is “the sum of the first n integers is n(n+1)/2”.

Imagine we can show the following two statements are true.

1. P(1) is true, and
2. Whenever P(n) is true then P(n+1) is true.

If we can do this we now have P(n) is true for all n!

(Note: Sometimes we start at n=0 not n=1)

Induction

Say we have some statement P(n). Perhaps P(n) is “the sum of the first n integers is n(n+1)/2”.

Imagine we can show the following two statements are true.

1. Base case: P(1) is true, and
2. Inductive Step: Whenever P(n) is true then P(n+1) is true.

Why does this imply that it holds for all n?

Induction (Box, Dirichlet, Pigeonhole Principle)

Imagine we can show the following two statements are true.

1. Base case: P(1) is true, and
2. Inductive Step: Whenever P(n) is true then P(n+1) is true.

Take n=1: thus the second becomes P(1) true implies P(2) true

P(1) is true

P(1) true implies P(2) true

THEREFORE since P(1) is true we now know P(2) is true.

Induction (Box, Dirichlet, Pigeonhole Principle)

Imagine we can show the following two statements are true.

1. Base case: P(1) is true, and
2. Inductive Step: Whenever P(n) is true then P(n+1) is true.

We know P(1) and P(2) are true.

Take n=2: thus the second becomes P(2) true implies P(3) true

P(2) is true

P(2) true implies P(3) true

THEREFORE since P(2) is true we now know P(3) is true.

Induction (Box, Dirichlet, Pigeonhole Principle)

Imagine we can show the following two statements are true.

1. Base case: P(1) is true, and
2. Inductive Step: Whenever P(n) is true then P(n+1) is true.

We know P(1), P(2) and P(3) are true.

Take n=3: thus the second becomes P(3) true implies P(4) true

P(3) is true

P(3) true implies P(4) true

THEREFORE since P(3) is true we now know P(4) is true. AND SO ON!

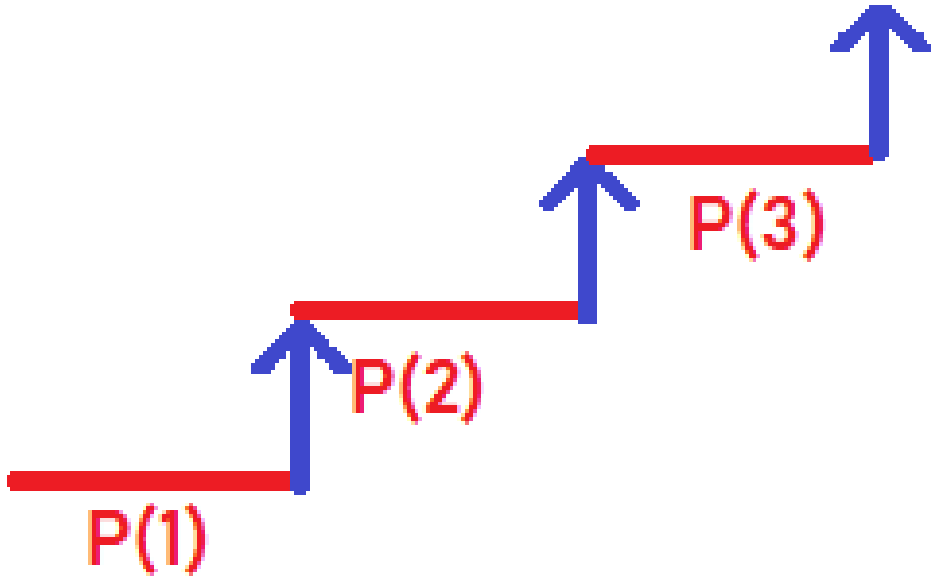
Induction (Box, Dirichlet, Pigeonhole Principle)

To prove P(n) is true for all n, must show

1. Base case: P(1) is true, and
2. Inductive Step: Whenever P(n‘ is true then P(n+1) is true.

This is often viewed

as a staircase.



Example: P(n): 1 + 2 + … + n = n(n+1)/2

To prove P(n) is true for all n, must show

1. Base case: P(1) is true, and
2. Inductive Step: Whenever P(n) is true then P(n+1) is true.

We will prove this by induction. There are two steps.

First we prove P(1) is true, then we show IF P(n) is true THEN P(n+1) is true.

Example: P(n): 1 + 2 + … + n = n(n+1)/2

To prove P(n) is true for all n, must show

1. Base case: P(1) is true, and
2. Inductive Step: Whenever P(n) is true then P(n+1) is true.

Step 1: Base Case: We must show P(1) is true.

Thus we must show that when n=1, we have 1 = 1(1+1)/2.

This however follows immediately!

We are done with the base case.

Example: P(n): 1 + 2 + … + n = n(n+1)/2

To prove P(n) is true for all n, must show

1. Base case: P(1) is true, and
2. Inductive Step: Whenever P(n) is true then P(n+1) is true.

Step 2: Inductive Step: We now get to ASSUME that P(n) is true, and we must show that P(n+1) is true.

We are done with the base case. We could try to do n=2 or n=3 to build up intuition, but it is not necessary.

Example: P(n): 1 + 2 + … + n = n(n+1)/2

To prove P(n) is true for all n, must show

1. Base case: P(1) is true, and
2. Inductive Step: Whenever P(n) is true then P(n+1) is true.

Step 2: Inductive Step: We now get to ASSUME that P(n) is true, and we must show that P(n+1) is true.

Extra work: If n=2 let's check: Does 1+2 = 2(2+1)/2? YES!

Extra work: if n=3 let's check: Does 1+2+3 = 3(3+1)/2? YES!

These extra checks are not a substitute for a proof, but the more values of n that work, the more confident we are that it is true.

Example: P(n): 1 + 2 + … + n = n(n+1)/2

To prove P(n) is true for all n, must show

1. Base case: P(1) is true, and
2. Inductive Step: Whenever P(n) is true then P(n+1) is true.

Step 2: Inductive Step: We now get to ASSUME that P(n) is true, and we must show that P(n+1) is true.

OK, we now get to assume P(n) is true, we want to prove P(n+1) is true.

What does this mean?

P(n) true means we assume 1 + 2 + … + n = n(n+1)/2.

We want to prove that P(n+1): 1 + 2 + … + n + (n+1) = (n+1)(n+1+1)/2 is true.

How should we proceed? When we look at P(n+1), do we see anything related to P(n)?

Example: P(n): 1 + 2 + … + n = n(n+1)/2

To prove P(n) is true for all n, must show

1. Base case: P(1) is true, and
2. Inductive Step: Whenever P(n) is true then P(n+1) is true.

Step 2: Inductive Step: We now get to ASSUME that P(n) is true, and we must show that P(n+1) is true.

OK, we now get to assume P(n) is true, we want to prove P(n+1) is true.

What does this mean?

P(n) true means we assume 1 + 2 + … + n = n(n+1)/2.

We want to prove that P(n+1): 1 + 2 + … + n + (n+1) = (n+1)(n+1+1)/2 is true.

How should we proceed? Notice that the sum for n+1 starts off exactly as the sum for n!

What are we assuming we know about 1 + 2 + … + n? We are assuming it equals ….

Example: P(n): 1 + 2 + … + n = n(n+1)/2

To prove P(n) is true for all n, must show

1. Base case: P(1) is true, and
2. Inductive Step: Whenever P(n) is true then P(n+1) is true.

Step 2: Inductive Step: We now get to ASSUME that P(n) is true, and we must show that P(n+1) is true.

OK, we now get to assume P(n) is true, we want to prove P(n+1) is true.

What does this mean?

P(n) true means we assume 1 + 2 + … + n = n(n+1)/2.

We want to prove that P(n+1): 1 + 2 + … + n + (n+1) = (n+1)(n+1+1)/2 is true.

How should we proceed? Notice that the sum for n+1 starts off exactly as the sum for n!

What are we assuming we know about 1 + 2 + … + n? We are assuming it equals n(n+1)/2.

Thus let's substitute for 1 + 2 + … + n in 1 + 2 + … + n + (n+1).

Example: P(n): 1 + 2 + … + n = n(n+1)/2

To prove P(n) is true for all n, must show

1. Base case: P(1) is true, and
2. Inductive Step: Whenever P(n) is true then P(n+1) is true.

Step 2: Inductive Step: We now get to ASSUME that P(n) is true, and we must show that P(n+1) is true.

OK, we now get to assume P(n) is true, we want to prove P(n+1) is true.

What does this mean?

P(n) true means we assume 1 + 2 + … + n = n(n+1)/2.

We want to prove that P(n+1): 1 + 2 + … + n + (n+1) = (n+1)(n+1+1)/2 is true.

Using the inductive assumption, we have

1 + 2 + … + n + (n+1) = (1 + 2 + … + n) + (n+1) = n(n+1)/2 + (n+1).

Now we just need to show the far right equals our claim, (n+1)(n+1+1)/2. How do we add two fractions?

Example: P(n): 1 + 2 + … + n = n(n+1)/2

To prove P(n) is true for all n, must show

1. Base case: P(1) is true, and
2. Inductive Step: Whenever P(n) is true then P(n+1) is true.

Step 2: Inductive Step: We now get to ASSUME that P(n) is true, and we must show that P(n+1) is true.

OK, we now get to assume P(n) is true, we want to prove P(n+1) is true.

What does this mean?

P(n) true means we assume 1 + 2 + … + n = n(n+1)/2.

We want to prove that P(n+1): 1 + 2 + … + n + (n+1) = (n+1)(n+1+1)/2 is true.

We have 1 + 2 + … + n + (n+1) = n(n+1)/2 + (n+1).

But $\frac{n(n+1)}{2} + (n+1) =$

Example: P(n): 1 + 2 + … + n = n(n+1)/2

To prove P(n) is true for all n, must show

1. Base case: P(1) is true, and
2. Inductive Step: Whenever P(n) is true then P(n+1) is true.

Step 2: Inductive Step: We now get to ASSUME that P(n) is true, and we must show that P(n+1) is true.

OK, we now get to assume P(n) is true, we want to prove P(n+1) is true.

What does this mean?

P(n) true means we assume 1 + 2 + … + n = n(n+1)/2.

We want to prove that P(n+1): 1 + 2 + … + n + (n+1) = (n+1)(n+1+1)/2 is true.

We have 1 + 2 + … + n + (n+1) = n(n+1)/2 + (n+1).

But $\frac{n(n+1)}{2} + (n+1) = \frac{n(n+1)}{2} + \frac{2(n+1)}{2} =$

Example: P(n): 1 + 2 + … + n = n(n+1)/2

To prove P(n) is true for all n, must show

1. Base case: P(1) is true, and
2. Inductive Step: Whenever P(n) is true then P(n+1) is true.

Step 2: Inductive Step: We now get to ASSUME that P(n) is true, and we must show that P(n+1) is true.

OK, we now get to assume P(n) is true, we want to prove P(n+1) is true.

What does this mean?

P(n) true means we assume 1 + 2 + … + n = n(n+1)/2.

We want to prove that P(n+1): 1 + 2 + … + n + (n+1) = (n+1)(n+1+1)/2 is true.

We have 1 + 2 + … + n + (n+1) = n(n+1)/2 + (n+1).

But $\frac{n(n+1)}{2} + (n+1) = \frac{n(n+1)}{2} + \frac{2(n+1)}{2} = \frac{n(n+1) + 2(n+1)}{2} =$

Example: P(n): 1 + 2 + … + n = n(n+1)/2

To prove P(n) is true for all n, must show

1. Base case: P(1) is true, and
2. Inductive Step: Whenever P(n) is true then P(n+1) is true.

Step 2: Inductive Step: We now get to ASSUME that P(n) is true, and we must show that P(n+1) is true.

OK, we now get to assume P(n) is true, we want to prove P(n+1) is true.

What does this mean?

P(n) true means we assume 1 + 2 + … + n = n(n+1)/2.

We want to prove that P(n+1): 1 + 2 + … + n + (n+1) = (n+1)(n+1+1)/2 is true.

We have 1 + 2 + … + n + (n+1) = n(n+1)/2 + (n+1).

But $\frac{n(n+1)}{2} + (n+1) = \frac{n(n+1)}{2} + \frac{2(n+1)}{2} = \frac{n(n+1)+2(n+1)}{2} = \frac{(n+1)(n+2)}{2}$, which is what we needed to show, completing the proof (as n+2 = n+1+1)!

Example: P(n): $1^2 + 2^2 + \ldots + n^2 = n(n+1)(2n+1)/6$

To prove P(n) is true for all n, must show

1. Base case: P(1) is true, and
2. Inductive Step: Whenever P(n) is true then P(n+1) is true.

The proof is similar to what we just did!

Step 1: The Base Case: n=1: Is $1^2 = 1(1+1)(2*1 + 1)/6$? YES!

We don't need to, but we can check other values of n.

If n=2 does $1^2 + 2^2 = 2(2+1)(2*2+1)/6$? YES!

If n=3 does $1^2 + 2^2 + 3^2 = 3(3+1)(2*3 + 1)/6$? YES!

$$0^6 + 1^6 + \ldots + n^6 \approx \int_0^n x^6\,dx$$

$$= \frac{x^7}{7}\Big|_0^n$$

$$= \frac{n^7}{7}$$

Example: P(n): $1^2 + 2^2 + \ldots + n^2 = n(n+1)(2n+1)/6$

To prove P(n) is true for all n, must show

1. Base case: P(1) is true, and
2. Inductive Step: Whenever P(n) is true then P(n+1) is true.

Step 2: Inductive Step: Assume P(n) is true, must show P(n+1) is true.

Since we are assuming P(n) is true, what do we know?

P(n) is true means $1^2 + 2^2 + \ldots + n^2 = n(n+1)(2n+1)/6$.

We must show P(n+1) is true. What is that?

P(n+1) is $1^2 + 2^2 + \ldots + n^2 + (n+1)^2 = (n+1)(n+1+1)(2(n+1)+1)/6$, note the right hand side is (n+1)(n+2)(2n+3)/6.

So is $1^2 + 2^2 + \ldots + n^2 + (n+1)^2 = = n(n+1)(2n+1)/6 + (n+1)^2$.

We have $\frac{n(n+1)(2n+1)}{6} = \frac{6(n+1)2}{6} = \frac{(n+1)(n(2n+1)+\ 6(n+1))}{6} = \frac{(n+1)(2n2+n+6n+6)}{6} = \frac{(n+1)(2n2+7n+6)}{6}$

Doing some algebra, we see $2n2 + 7n + 6$ equals (n+2)(2n+3) by FOIL, completing the proof.

Example: P(n): $1 + 3 + \ldots + (2n-1) = n^2$

To prove P(n) is true for all n, must show

1. Base case: P(1) is true, and
2. Inductive Step: Whenever P(n) is true then P(n+1) is true.

The proof is similar to what we just did!

Step 1: The Base Case: n=1: Is $1 = 1^2$? YES!

We don't need to, but we can check other values of n.

If n=2 does

If n=3 does

Rest of the proof is similar to what we've done before….

Example: P(n): $1 + 3 + \ldots + (2n-1) = n^2$

To prove P(n) is true for all n, must show

1. Base case: P(1) is true, and
2. Inductive Step: Whenever P(n) is true then P(n+1) is true.

The proof is similar to what we just did!

Step 1: The Base Case: n=1: Is $1 = 1^2$? YES!

We don't need to, but we can check other values of n.

If n=2 does $1 + 3 = 2^2$? YES!

If n=3 does $1 + 3 + 5 = 3^2$? YES!

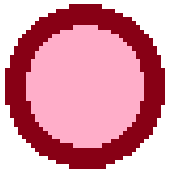
Rest of the proof is similar to what we've done before….

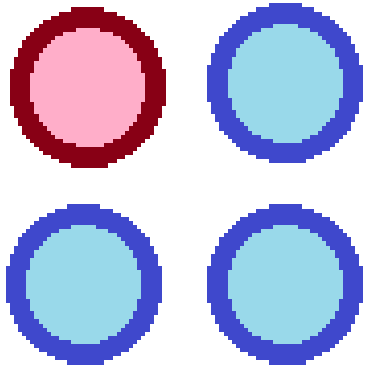
Example: P(n): $1 + 3 + \ldots + (2n-1) = n^2$

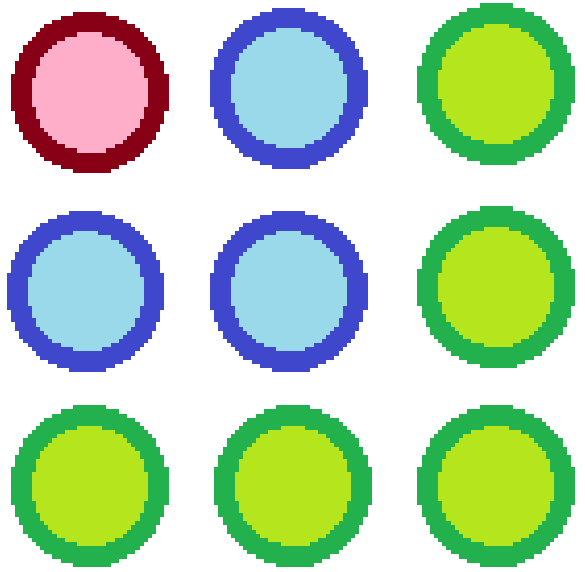
To prove P(n) is true for all n, must show

1. Base case: P(1) is true, and
2. Inductive Step: Whenever P(n) is true then P(n+1) is true.

Can prove in other ways than Induction….







Example: P(n): 133 divides $11^{n+1} + 12^{2n-1}$

To prove P(n) is true for all n, must show

1. Base case: P(1) is true, and
2. Inductive Step: Whenever P(n) is true then P(n+1) is true.

Let's try to show P(1) is true: does 133 divide $11^{1+1} + 12^{2*1-1}$?

Example: P(n): 133 divides $11^{n+1} + 12^{2n-1}$

To prove P(n) is true for all n, must show

1. Base case: P(1) is true, and
2. Inductive Step: Whenever P(n) is true then P(n+1) is true.

Let's try to show P(1) is true: does 133 divide $11^{1+1} + 12^{2*1-1}$?

Yes, as $11^{1+1} + 12^{2*1-1} = 11^2 + 12 = 121 + 12 = 133$, which is clearly a multiple of 133.

Example: P(n): 133 divides $11^{n+1} + 12^{2n-1}$

To prove P(n) is true for all n, must show

1. Base case: P(1) is true, and
2. Inductive Step: Whenever P(n) is true then P(n+1) is true.

Now assume P(n) is true, we must show P(n+1) is true.

Can assume 133 divides $11^{n+1} + 12^{2n-1}$, must show 133 divides $11^{n+1} + 12^{2n-1}$.

$$\begin{aligned} 11^{(n+1)+1} + 12^{2(n+1)-1} &= 11^{n+1+1} + 12^{2n-1+2} \\ &= 11 \cdot 11^{n+1} + 12^2 \cdot 12^{2n-1} \\ &= 11 \cdot 11^{n+1} + (133 + 11)12^{2n-1} \\ &= 11\left(11^{n+1} + 12^{2n-1}\right) + 133 \cdot 12^{2n-1}. \quad \text{(A.6)} \end{aligned}$$

By the inductive assumption 133 divides $11^{n+1} + 12^{2n-1}$; therefore, 133 divides $11^{(n+1)+1} + 12^{2(n+1)-1}$, completing the proof.

Getting a feel for the answer….

We showed $1 + 2 + \ldots + n = n(n+1)/2 = n^2/2 + n/2$.

Is this reasonable?

How can we try to get an UPPER BOUND and a LOWER BOUND for the sum?

$-\infty < 1 \leq n \leq 1 + \cdots + 1$ $\leq n^2 < \infty$

Getting a feel for the answer….

We showed $1 + 2 + \ldots + n = n(n+1)/2 = n^2/2 + n/2$.
Is this reasonable?

How can we try to get an UPPER BOUND and a LOWER BOUND for the sum?

Every term in the sum is at most ???
Every term in the sum is at least ???
The number of terms is ???
Thus an upper bound is ???
Thus a lower bound is ???

Getting a feel for the answer….

We showed $1 + 2 + \ldots + n = n(n+1)/2 = n^2/2 + n/2$.

Is this reasonable?

How can we try to get an UPPER BOUND and a LOWER BOUND for the sum?

Every term in the sum is at most n

Every term in the sum is at least 1

The number of terms is n

Thus an upper bound is $n*n = n^2$

Thus a lower bound is $1*n = n$.

Note there is a large difference between the upper and lower bounds, need to do better.

Getting a feel for the answer….

We showed $1 + 2 + \ldots + n = n(n+1)/2 = n^2/2 + n/2$.
Is this reasonable?

How can we try to get an UPPER BOUND and a LOWER BOUND for the sum?

Every term in the sum is at most n
The number of terms is n
Thus an upper bound is $n*n = n^2$

The last half of the terms are each at least n/2 and there are n/2.
Thus a lower bound is $n/2 * n/2 = n^2/4$.

Now $n^2 / 4 \leq 1 + 2 + \ldots + n \leq n^2$, note these bounds are of the same power in n!

Final thoughts on sums of powers….

Hardest part of the induction is knowing what to PROVE.

How can we find the formula?

Looking at the cases we've done it looks like it is always a polynomial of degree one higher than the power, constant term is zero, leading term (if sum of kth powers) is $n^{k+1} / (k+1)$.

Note 2 points determine a line, 3 points a quadratic (parabola), 4 a cubic, and so on; we can evaluate the sum for a few points and then INTERPOLATE and figure out the polynomial!

Homework: Prove $1^3 + 2^3 + \ldots + n^3 = n^2 (n+1)^2 / 4$.

False proofs by Induction

The following is my favorite false proof by induction. Where is the mistake?

P(n): In any group of n people, everyone has the same name! (Note different groups of n people can have different names).

Let's try to prove this by induction. We must show:

1. Base Case: In any group with 1 person, everyone has the same name.
2. Inductive Step: If everyone in a group of size n has the same name, then everyone in a group of size n+1 has the same name.

False proofs by Induction

The following is my favorite false proof by induction. Where is the mistake?

P(n): In any group of n people, everyone has the same name! (Note different groups of n people can have different names).

Let's try to prove this by induction. We must show:

1. Base Case: In any group with 1 person, everyone has the same name.

PROOF OF BASE CASE: This follows immediately, as….

False proofs by Induction

The following is my favorite false proof by induction. Where is the mistake?

P(n): In any group of n people, everyone has the same name! (Note different groups of n people can have different names).

Let's try to prove this by induction. We must show:

1. Base Case: In any group with 1 person, everyone has the same name.

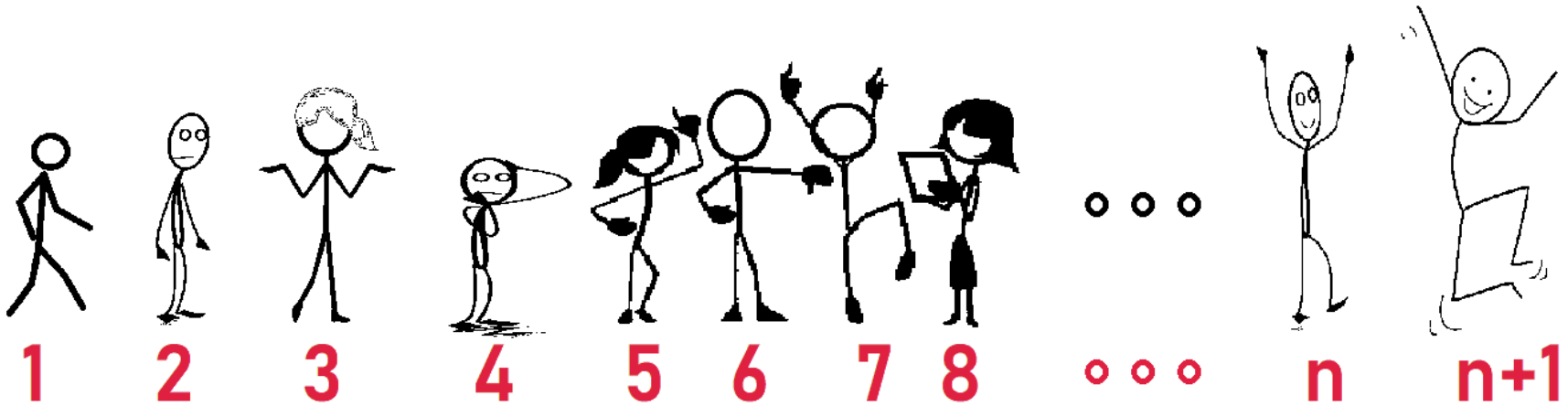
PROOF OF BASE CASE: This follows immediately, as there is only one person in the group, so clearly everyone in the group has the same name!

False proofs by Induction

P(n): In any group of n people, everyone has the same name! (Note different groups of n people can have different names).

Inductive Step: If everyone in a group of size n has the same name, then everyone in a group of size n+1 has the same name.

"PROOF" OF INDUCTIVE STEP: We assume everyone in a group of size n has the same name, must show true for a group of size n+1. Consider a group of n+1 people. How can we use the inductive assumption (all groups of size n have all with the same name)? Can you find some groups of size n?

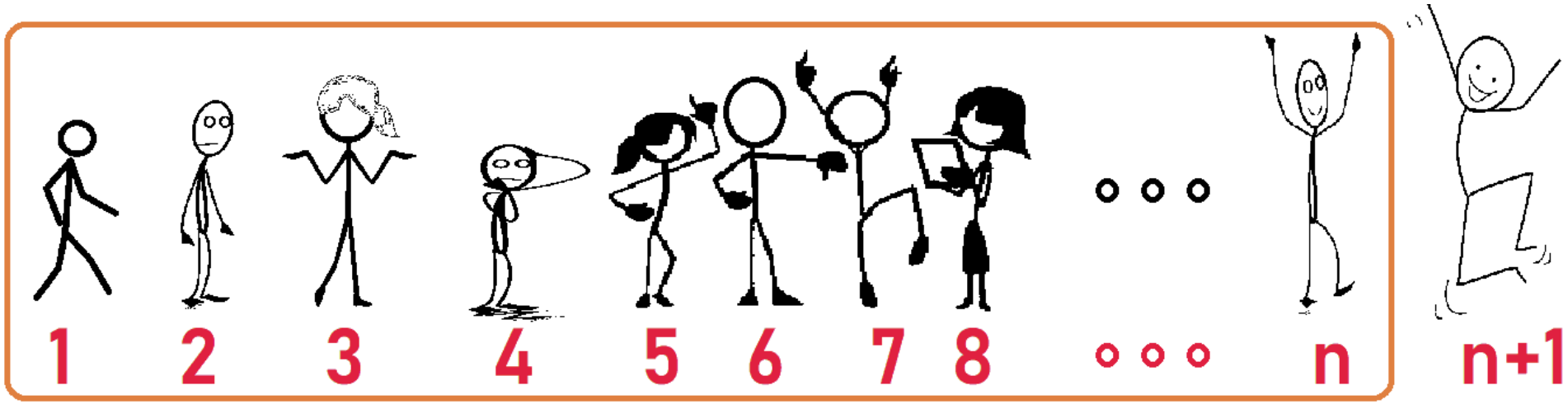


False proofs by Induction

P(n): In any group of n people, everyone has the same name! (Note different groups of n people can have different names).

Inductive Step: If everyone in a group of size n has the same name, then everyone in a group of size n+1 has the same name.

"PROOF" OF INDUCTIVE STEP: We assume everyone in a group of size n has the same name, must show true for a group of size n+1. Consider a group of n+1 people. How can we use the inductive assumption (all groups of size n have all with the same name)? Can you find some groups of size n? First n people all have the same name!

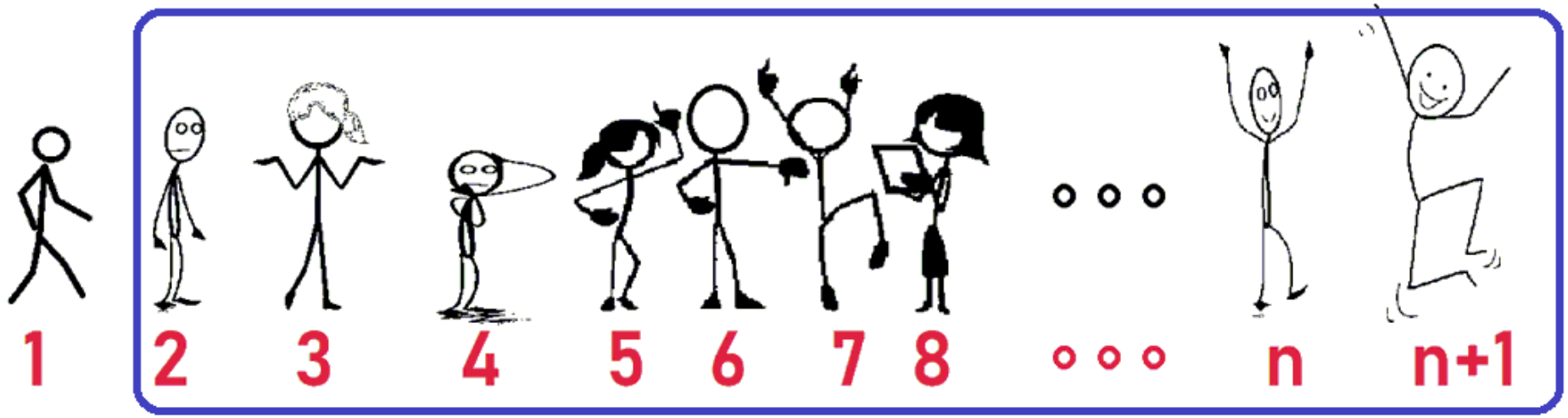


False proofs by Induction

P(n): In any group of n people, everyone has the same name! (Note different groups of n people can have different names).

Inductive Step: If everyone in a group of size n has the same name, then everyone in a group of size n+1 has the same name.

"PROOF" OF INDUCTIVE STEP: We assume everyone in a group of size n has the same name, must show true for a group of size n+1. Consider a group of n+1 people. How can we use the inductive assumption (all groups of size n have all with the same name)? Can you find some groups of size n? Last n people all have the same name!

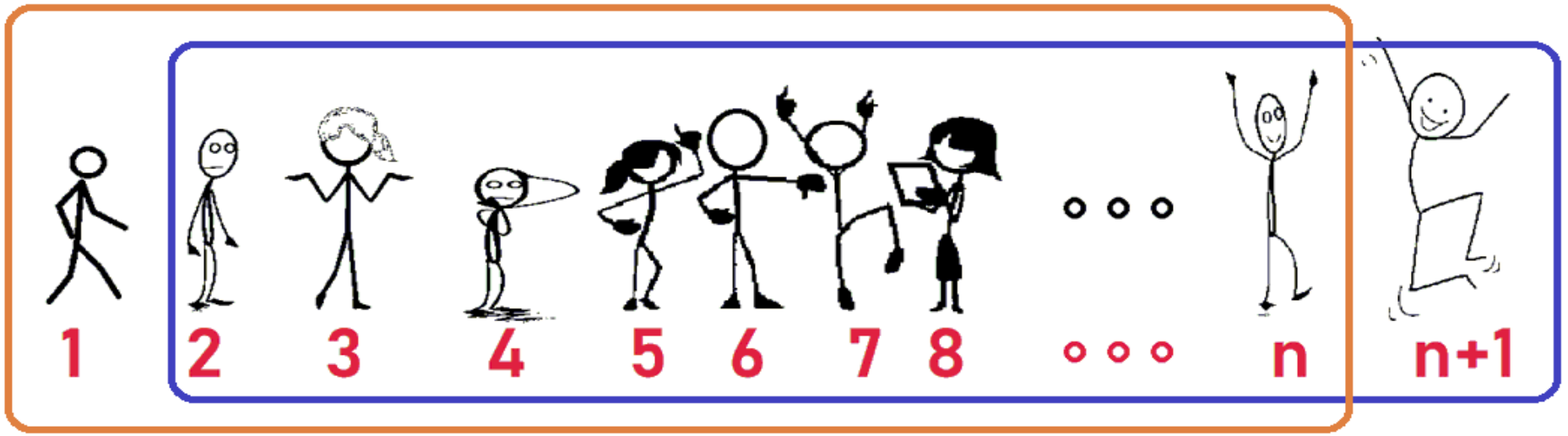


False proofs by Induction

P(n): In any group of n people, everyone has the same name! (Note different groups of n people can have different names).

Inductive Step: If everyone in a group of size n has the same name, then everyone in a group of size n+1 has the same name.

"PROOF" OF INDUCTIVE STEP: We assume everyone in a group of size n has the same name, must show true for a group of size n+1. Consider a group of n+1 people. How can we use the inductive assumption (all groups of size n have all with the same name)? Can you find some groups of size n? Note people 2, 3, …, n are in both groups!

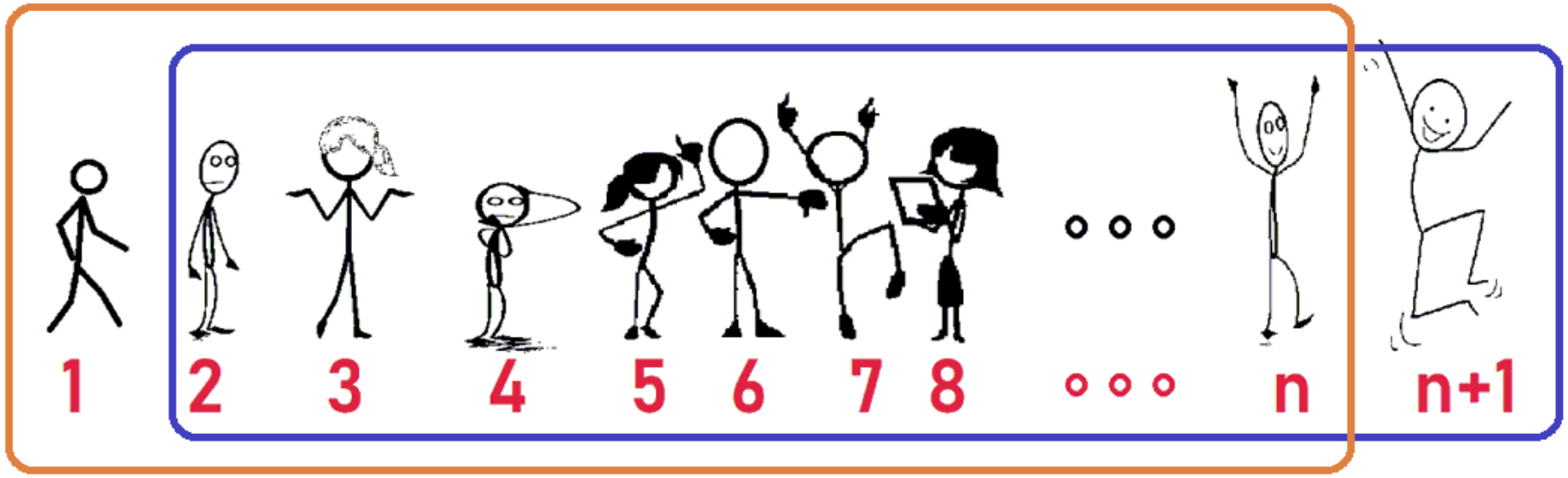


False proofs by Induction

P(n): In any group of n people, everyone has the same name! (Note different groups of n people can have different names).

Inductive Step: If everyone in a group of size n has the same name, then everyone in a group of size n+1 has the same name.

"PROOF" OF INDUCTIVE STEP: We assume everyone in a group of size n has the same name, must show true for a group of size n+1. Consider a group of n+1 people. How can we use the inductive assumption (all groups of size n have all with the same name)? Can you find some groups of size n? Note people 2, 3, …, n are in both groups! Thus everyone in the first n has the same name, everyone in the last n has the same name, and since people 2, 3, …, n are in both that means those two names are the same and our proof is done! If your name is not Steve Miller, you should be skeptical. Mistake?

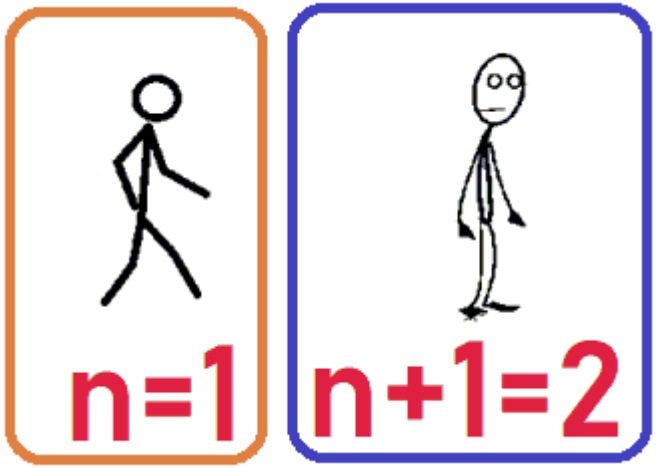


False proofs by Induction

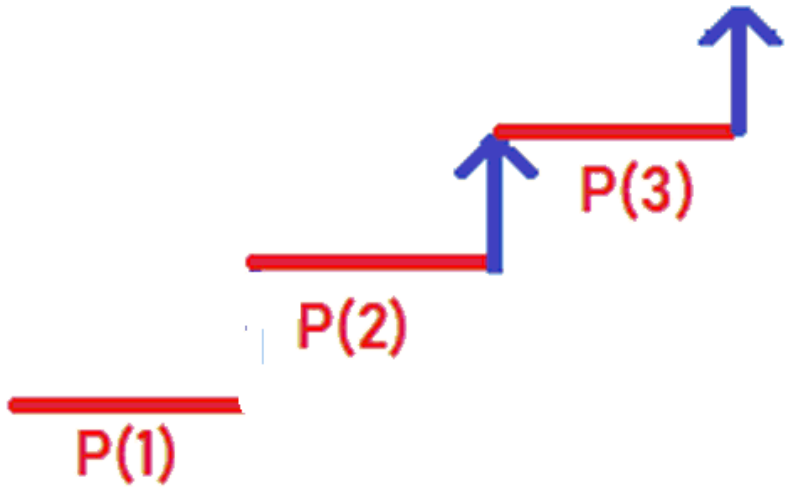
P(n): In any group of n people, everyone has the same name! (Note different groups of n people can have different names).

Inductive Step: If everyone in a group of size n has the same name, then everyone in a group of size n+1 has the same name.

"PROOF" OF INDUCTIVE STEP: The mistake is we drew this for a "large" n. Remember we must show for ANY n that if P(n) is true then P(n+1) is true. If n is 2 or more then there is a person in both groups, but if n=1 there is not!



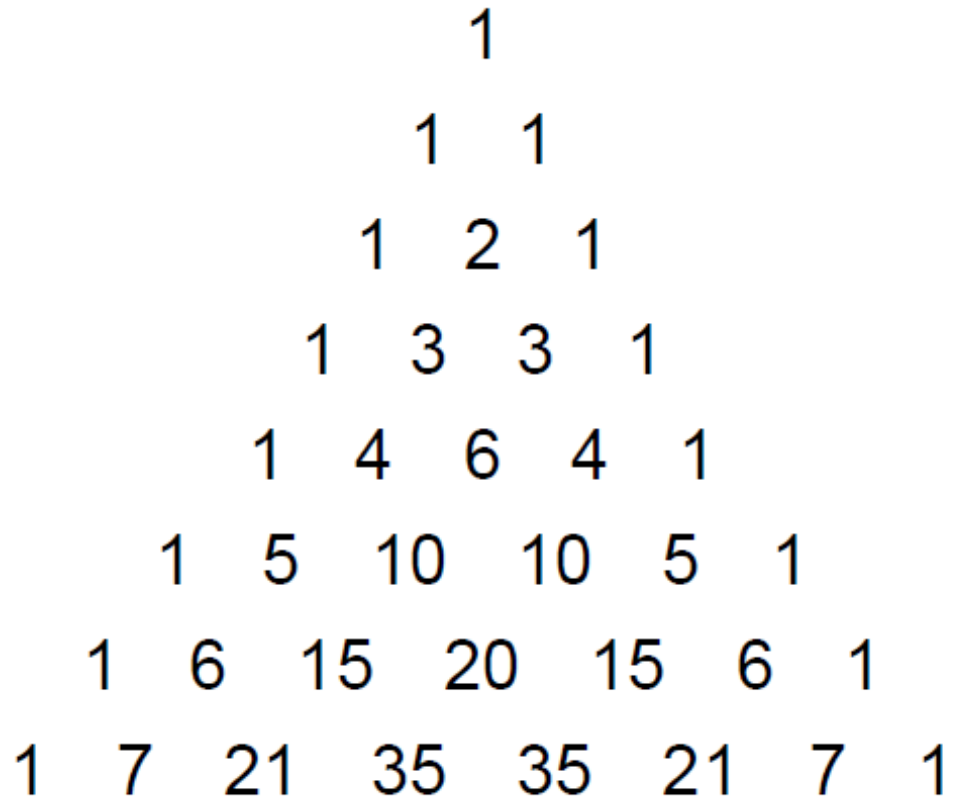
When n=1 we see there is no overlap!



Pascal's Triangle

The numbers in the nth row of Pascal's Triangle are the coefficients we obtain in expanding $(x+y)^n$.

Equivalently, we have two diagonals of 1, and all other elements are the sum of the elements in the row above immediately to the left and immediately to the right.



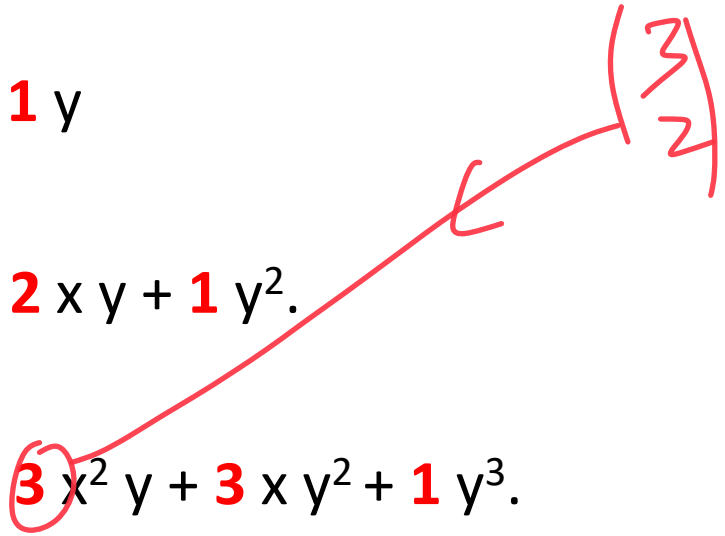
Expanding $(x + y)^n$

$(x + y)^0 = \mathbf{1}$

$(x + y)^1 = \mathbf{1}\,x + \mathbf{1}\,y$

$(x + y)^2 = \mathbf{1}\,x^2 + \mathbf{2}\,x\,y + \mathbf{1}\,y^2.$

$(x + y)^3 = \mathbf{1}\,x^3 + \mathbf{3}\,x^2\,y + \mathbf{3}\,x\,y^2 + \mathbf{1}\,y^3.$



We can keep going and get more and more rows....

1

1 1

1 2 1

1 3 3 1

1 4 6 4 1

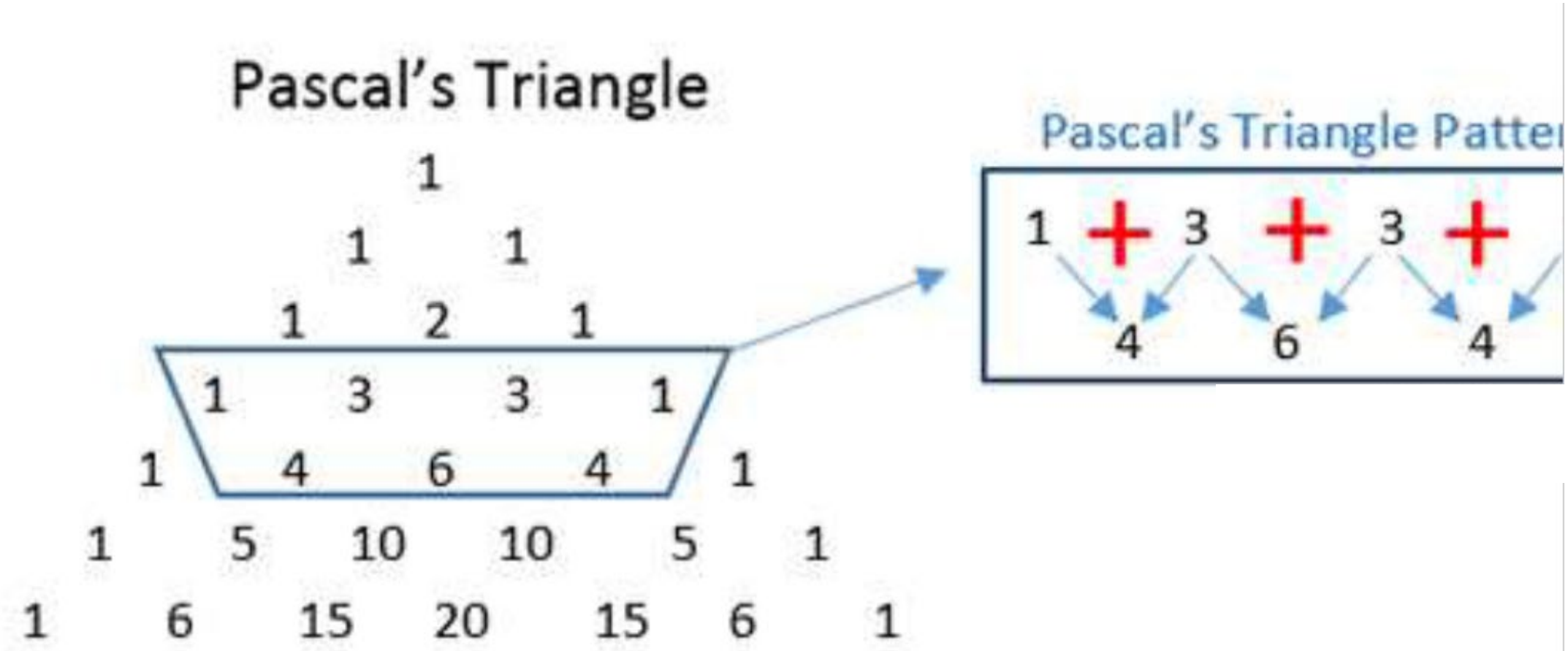
1 5 10 10 5 1

1 6 15 20 15 6 1

1 7 21 35 35 21 7 1

$(x+y)^4 = \binom{4}{0}x^4y^0 + \binom{4}{3}\binom{1}{1}x^3y + \binom{4}{2}\binom{2}{2}x^2y^2 + \cdots$

Why is the Pascal Relation true? Each number is the sum of what is immediately above to the right and to the left.



Sketch of the proof:

Assume we know one row, say

$(x+y)^5 = x^5 + 5\,x^4\,y + 10\,x^3\,y^2 + 10\,x^2\,y^3 + 5\,x\,y^4 + y^5$.

Then

$(x+y)^6 = (x+y)\,(x+y)^5$

$= x\,(x+y)^5 + y\,(x+y)^5$

$= x\,(x^5 + 5\,x^4\,y + 10\,x^3\,y^2 + 10\,x^2\,y^3 + 5\,x\,y^4 + y^5)$
$\quad + y\,(x^5 + 5\,x^4\,y + 10\,x^3\,y^2 + 10\,x^2\,y^3 + 5\,x\,y^4 + y^5)$

$= (x^6 + 5\,x^5\,y + 10\,x^4\,y^2 + 10\,x^3\,y^3 + 5\,x^2\,y^4 + x\,y^5)$
$\quad + (x^5\,y + 5\,x^4\,y^2 + 10\,x^3\,y^3 + 10\,x^2\,y^4 + 5\,x\,y^5 + y^6)$

$= x^6 + 5\,x^5\,y + 10\,x^4\,y^2 + 10\,x^3\,y^3 + 5\,x^2\,y^4 + x\,y^5$
$\quad + x^5\,y + 5\,x^4\,y^2 + 10\,x^3\,y^3 + 10\,x^2\,y^4 + 5\,x\,y^5 + y^6$

$= x^6 + (5+1)\,x^5\,y + (10+5)\,x^4\,y^2 + (10+10)\,x^3\,y^3 + (5+10)\,x^2\,y^4 + (1+5)\,x\,y^5 + y^6$

$= x^6 + 6\,x^5\,y + 15\,x^4\,y^2 + 20\,x^3\,y^3 + 15\,x^2\,y^4 + 6\,x\,y^5 + y^6$

Pascal's Triangle

While we can prove many properties of the coefficients of Pascal's triangle, for small n we can just expand directly.

1

1 1

1 2 1

1 3 3 1

1 4 6 4 1

1 5 10 10 5 1

1 6 15 20 15 6 1

1 7 21 35 35 21 7 1

Binomial Theorem: Proofs by Induction, by Story, ….

Harvard : n

YALE : 1

Have $n+1$ people

want group of $k+1$ people

ways $\binom{n+1}{k+1}$

$$\binom{n}{k}\binom{1}{1} + \binom{n}{k+1}\binom{1}{0} = \binom{n+1}{k+1}$$

Case 1: Happily have the YALE person

#H = k #Y = 1

Case 2: Don't have the Yale person

#H = k+1 #Y = 0

n Princeton

n UPenn

$$\binom{n}{k} = \binom{n}{n-k}$$

Consider $\sum_{k=0}^{n} \binom{n}{k}^2 = \sum_{k=0}^{n} \binom{n}{k}\binom{n}{n-k}$

$\binom{n}{k}$: take k from Princeton

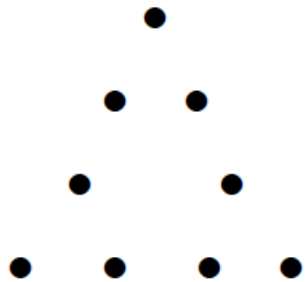
$\binom{n}{n-k}$: take $n-k$ from UPenn

$$= \binom{2n}{n}$$

Pascal's Triangle

Modify Pascal's triangle: • if odd, blank if even.

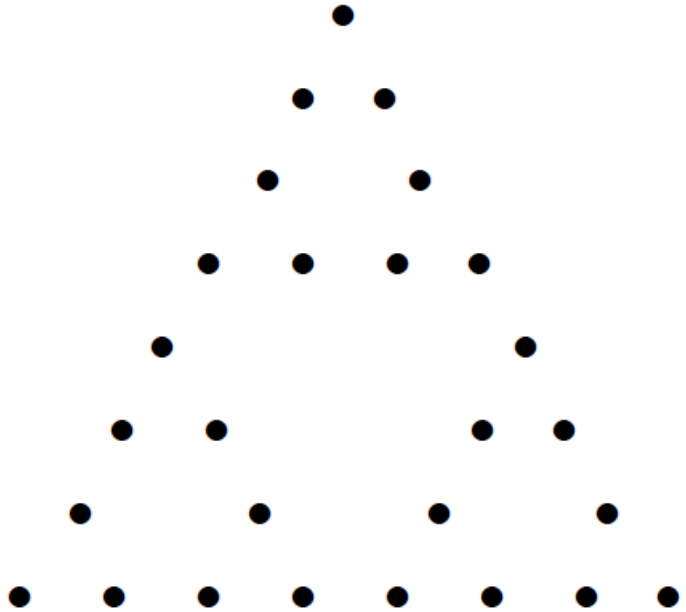
If we have just one row we would see •, if we have four rows we would see



Pascal's Triangle

Modify Pascal's triangle: • if odd, blank if even.

For eight rows we find



Pascal's Triangle

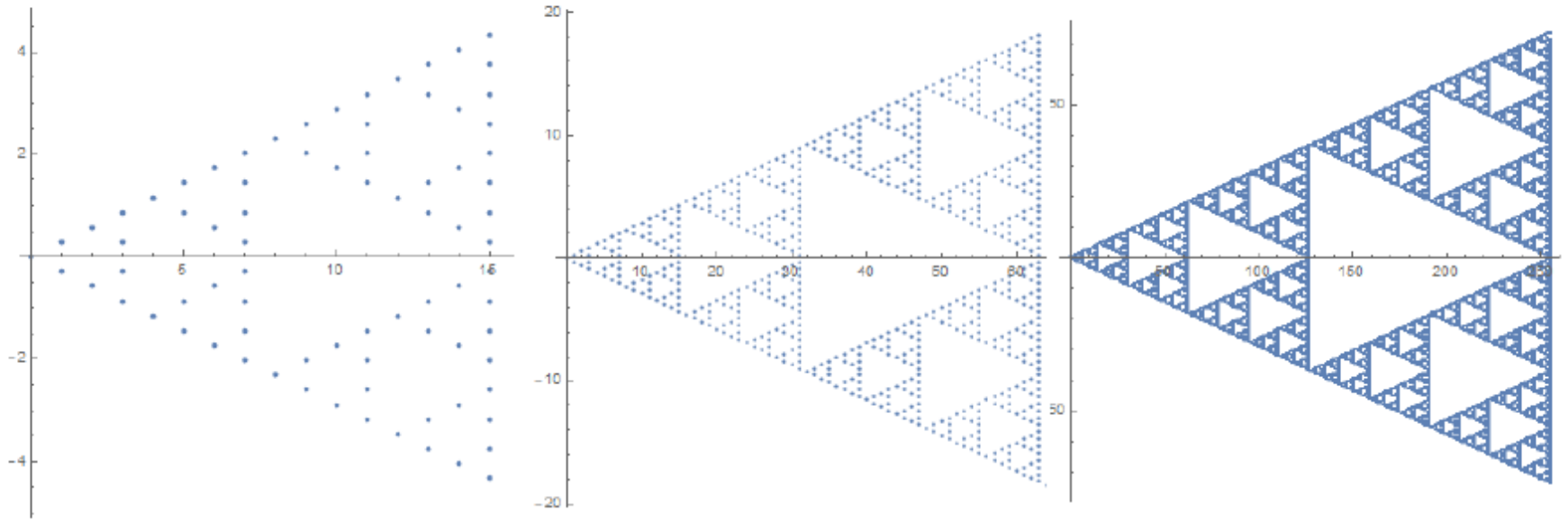


Figure: Plot of Pascal's triangle modulo 2 for 2^4, 2^8 and 2^{10} rows.

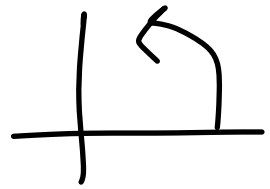
https://www.youtube.com/watch?v=tt4_4YajqRM (start 1:35)
https://youtu.be/_vkGakVt1RA?t=265 (start at 4:25; vertical)

Predicting Formulas: Derivative of a Product

$f(x) = x^m$ $\quad g(x) = x^n$ $\quad f(x)g(x) = x^{m+n}$

$f'(x) = mx^{m-1}$ $\quad g'(x) = nx^{n-1}$ $\quad (f(x)g(x))' = (m+n)x^{m+n-1}$

$f'(x)g(x) + f(x)g'(x) = (m+n)x^{m+n-1}$



$f(x) = \sin x$ $\quad g(x) = \cos x$ $\quad f(x)g(x) = \sin x \cos x = \frac{1}{2}\sin(2x)$

$f'(x) = \cos x$ $\quad g'(x) = -\sin x$ (minus sign) $\quad (f(x)g(x))' = \frac{1}{2}\sin'(2x)(2x)' = \cos(2x)$

$\cos x \cos x - \sin x \sin x$ which is $\cos(2x)$

Believe $(f(x)g(x))' = f'(x)g(x) + f(x)g'(x)$

↳ works if $f(x) = 1$

or $g(x) = 1$

Proof: $\lim_{h\to 0} \dfrac{f(x+h)g(x+h) - f(x)g(x+h) + f(x)g(x+h) - f(x)g(x)}{h}$

$= \lim_{h\to 0} \dfrac{f(x+h) - f(x)}{h} g(x+h) + \lim_{h\to 0} f(x) \dfrac{g(x+h) - g(x)}{h}$

$\to f'(x)\, g(x) + f(x)\, g'(x)$

Pirates and Math:
Dividing the Spoils and Game Theory

Steven J Miller, Williams College (sjm1@williams.edu)
https://web.williams.edu/Mathematics/sjmiller/public_html/



https://www.shutterstock.com/image-vector/cartoon-pirate-walking-plank-260nw-715720567.jpg
shutterstock.com 715720567

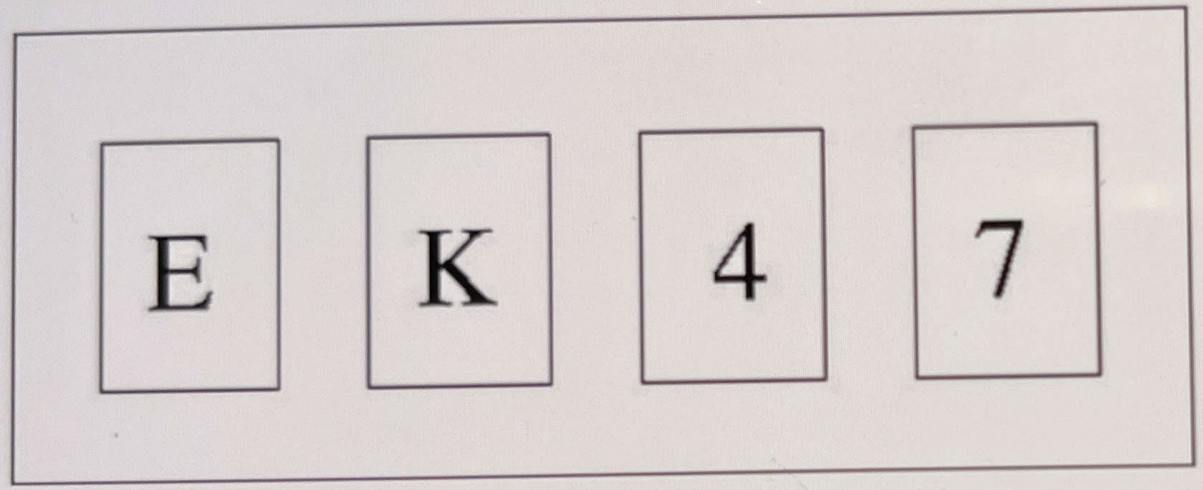


Figure 2.3. *The Wason 4-card task.* Which card(s) must you turn over to verify the rule that if a card shows a vowel on one face, then it has an even number on the other?

Figures-for-The-Righteous-Mind.pdf
Save...

Pirate Riddle

- Five pirates, named 1, 2, 3, 4 and 5.
- Must split 100 gold coins.
- The lowest named pirate alive proposes a division.
- If 50% or more vote for the plan it passes and is done.
- If over 50% vote against the plan it fails, the proposer walks the plank and dies, and the lowest named surviving pirate proposes a plan.
- Repeat till a plan is accepted.
- Assume the pirates are intelligent – what is the final division?

Math 310: Modern Algebra: Fall '25 (Siena)

Professor Steven J Miller: sjm1@williams.edu

Homepage:

https://web.williams.edu/Mathematics/sjmiller/public_html/310Fa25/

Lecture 03: 9/9/25: https://youtu.be/kkcaZLPE4no

Pirate Problem. Chapter Two: Introduction to groups, abstract groups, examples.

Game Rules (again)

- Five pirates, named 1, 2, 3, 4 and 5.
- Must split 100 gold coins.
- The lowest named pirate alive proposes a division.
- If 50% or more vote for the plan it passes and is done.
- If over 50% vote against the plan it fails, the proposer walks the plank and dies, and the lowest named surviving pirate proposes a plan.
- Repeat till a plan is accepted.
- Assume the pirates are intelligent – what is the final division?

Play smaller game and work up....

- ONE PIRATE, #5

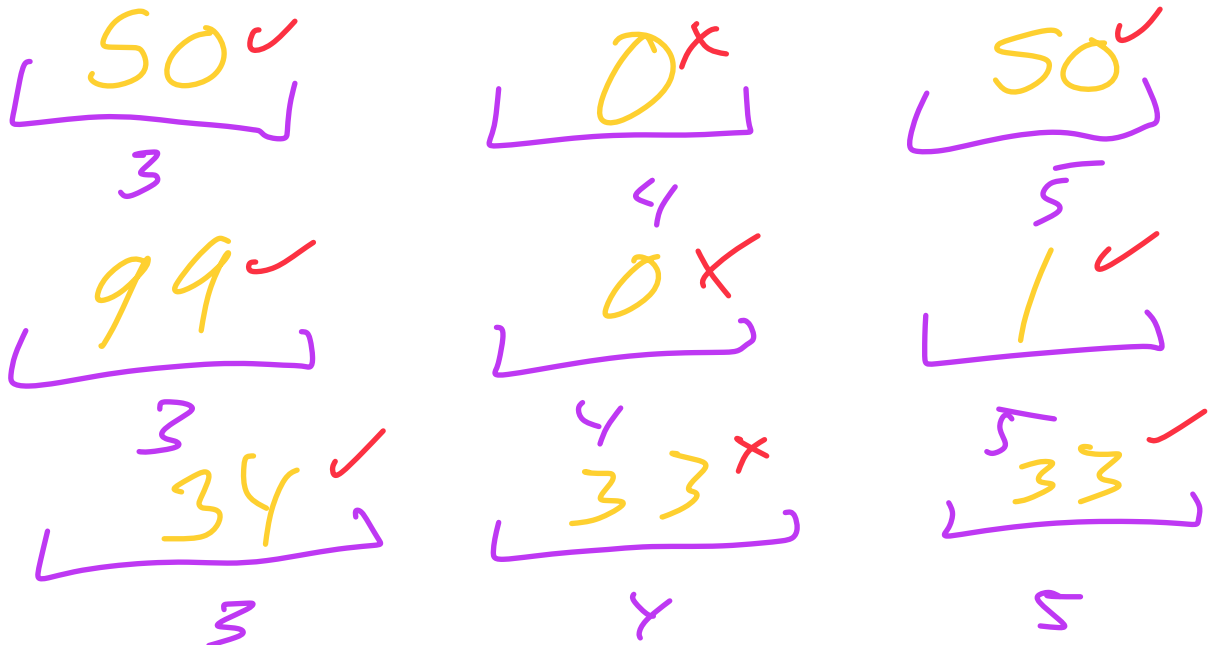
  #5 says I get all: PASSES!

- TWO PIRATES, #4, #5

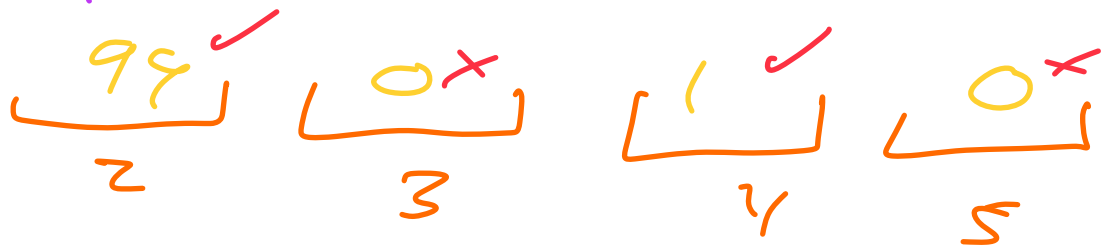
  #4 says I get all, #5 gets none: PASSES!

• THREE PIRATES: #3, #4, #5

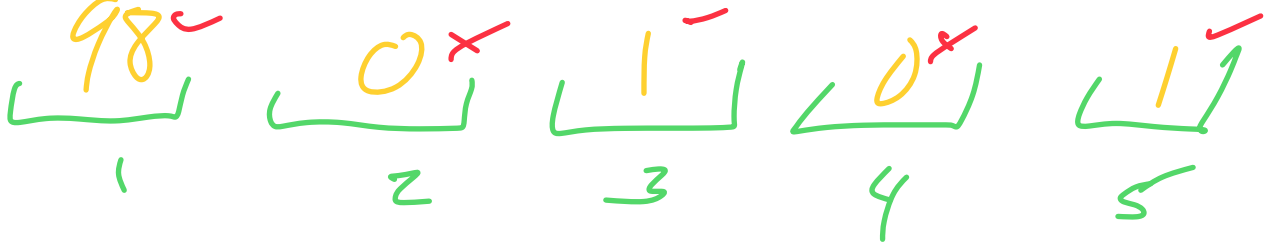
#3 Proposes



• FOUR PIRATES:



• FIVE PIRATES:





Elizabeth fails class due to death

If n non-neg integer: $\begin{cases} 0! = 1 \\ n! = n(n-1)! \text{ if } n \geq 1 \end{cases}$

$n!$ is #ways to order n objects $\boxed{n}\ \boxed{n-1}\ \boxed{n-2} \cdots \boxed{1}$

$3! = 3 \cdot 2 \cdot 1 = 6$

$3!! = ?$ could be $(3!)! = 6! = 720$

↳ actually $n!!$ defined as $n(n-2)(n-4) \cdots \begin{cases} 1 \\ 2 \end{cases}$

My favorite number is $3!!!$

$(3!!)!$ punctuation mark

QWERTY

CC

n objects There are n! ways to arrange Them

1	2	3	4
↓	↓	↓	↓
2	1	4	3

$P_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$

$(1\,2)(3\,4)$

$P_2 P_1 : \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 3 & 1 \end{pmatrix}$ $(1\,4)$

1	2	3	4
↓	↓	↓	↓
2	4	1	3

$P_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$

$(1\,2\,4\,3)$

Matrix $\begin{pmatrix} 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix}$

$$\begin{pmatrix} 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}$$

Sends $\vec{e}_1 \to \vec{e}_2$, $\vec{e}_2 \to \vec{e}_4$, $\vec{e}_3 \to \vec{e}_1$, $\vec{e}_4 \to \vec{e}_3$

Definition 2.6. A *group* consists of a set G together with a composition law

$$G \times G \longrightarrow G,$$
$$(g_1, g_2) \longmapsto g_1 \cdot g_2,$$

satisfying the following axioms:

(a) (***Identity Axiom***) There is an element $e \in G$ such that

$$e \cdot g = g \cdot e = g \quad \text{for all } g \in G.$$

The element e is called the *identity element of* G.

(b) (***Inverse Axiom***) For every $g \in G$ there is an element $h \in G$ such that

$$g \cdot h = h \cdot g = e.$$

The element h is denoted g^{-1} and is called the *inverse of* g.

(c) (***Associative Law***) For all $g_1, g_2, g_3 \in G$, the *associative law* holds; i.e.,

$$g_1 \cdot (g_2 \cdot g_3) = (g_1 \cdot g_2) \cdot g_3.$$

(d) (***Optional Feature: Commutative Law***) If it is further true that

$$g_1 \cdot g_2 = g_2 \cdot g_1 \quad \text{for all } g_1, g_2 \in G,$$

then G is said to be *commutative* or *abelian*.[3,4]

(a) Closure Axiom: $g_1 \cdot g_2 \in G$ for all $g_1, g_2 \in G$,

+, 0 ⊕

Proposition 2.9 (Basic Properties of Groups). *Let G be a group.*

(a) *G has exactly one identity element.*

(b) *Each element of G has exactly one inverse.*

(c) *Let $g, h \in G$. Then $(g \cdot h)^{-1} = h^{-1} \cdot g^{-1}$.*

(d) *Let $g \in G$. Then $(g^{-1})^{-1} = g$.*

Proof of (a) Assume not, so e_1, e_2 are identity elements

So $\forall g \in G: g \cdot e_1 = e_1 \cdot g = g$ and $g \cdot e_2 = e_2 \cdot g = g$

Taking $g = e_1$ yields $e_1 e_1 = e_1 \cdot e_1 = e_1$ and $e_1 \cdot e_2 = e_2 \cdot e_1 = e_1$

Taking $g = e_2$ yields $e_2 \cdot e_1 = e_1 \cdot e_2 = e_2$ and $e_2 \cdot e_2 = e_2 \cdot e_2 = e_2$

$e_2 \cdot e_1 = e_1 \cdot e_2 = e_1$ and e_2

Thus $e_1 = e_2$

Examples of Groups

- $\mathbb{Z}$ under addition, $\mathbb{Q}^+$ under multiplication
- $\mathbb{C}$ under addition
- Clock with n hours under clock arithmetic (addition) $\{0, 1, 2, \ldots, n-1\}$ and $k + j \Rightarrow k + j \bmod n$

  $n = 12$: inverse of 8 is 4 as $4 + 8 \equiv 0 \bmod 12$

  $12 - k + k \equiv 0 \bmod 12$

- Clock group under multiplication $\{1, 2, \ldots, n-1\}$

  If $n = 12$, $4 \cdot 5 \equiv 8 \bmod 12$

  $5 \cdot 5 \equiv 1 \bmod 12$, $7 \cdot 7 \equiv 1 \bmod 12$, $11 \cdot 11 \equiv 1 \bmod 12$

not a group if $n = 12$

Not Groups

- $\mathbb{N}$ under addition
- $\mathbb{Z}$ under multiplication
- $\mathbb{N}$ under multiplication

commutative

$X \cdot 2 \equiv 1 \bmod 12$

$2X = 1$ + multiple of 12

even odd even

Math 310: Modern Algebra: Fall '25 (Siena)

Professor Steven J Miller: sjm1@williams.edu

Homepage:

https://web.williams.edu/Mathematics/sjmiller/public_html/310Fa25/

Lecture 04: 9/11/25: https://youtu.be/cLN3X8eHtBM

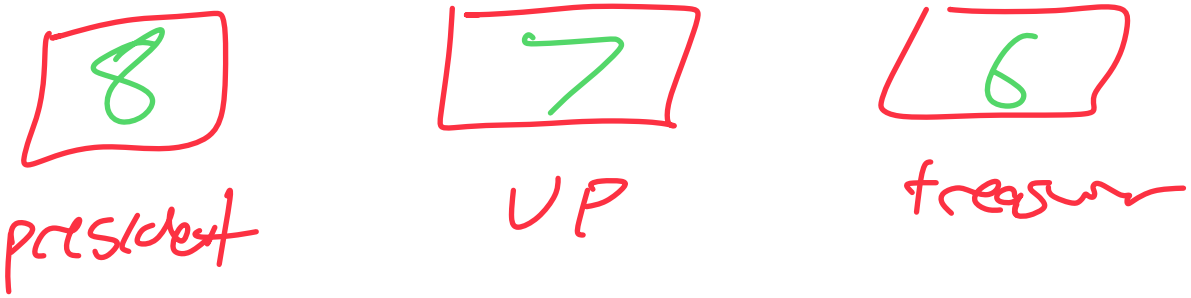
NO PHYSICAL CLASS – use the time to review math from previous classes, meet with me by zoom individually or in groups on any material from previous classes you are uncomfortable with and want to be comfortable with! We will review requested material (binomial coefficients, …).

Combinatorics

$0! = 1$, $n! = n(n-1)!$ if $n \geq 1$ positive integer

Meaning: $n!$ is the # ways to order n objects (order matters)

Choose 3 people from 8 to be officers; all offices are different.



answer is $8 \cdot 7 \cdot 6 = 8 \cdot 7 \cdot 6 \cdot \frac{5!}{5!} = \frac{8!}{5!} = {}_8P_3$

This is $\frac{8!}{(8-3)!}$; if want k from n (order matters) is $\frac{n!}{(n-k)!} = n(n-1)\cdots(n-(k-1)) \cdot \frac{(n-k)!}{(n-k)!}$

Proved the # ways to choose k from n when order matters is $n!/(n-k)! = {}_nP_{n-k}$. ($1 \le k$ Non-neg integers)

What if order doesn't matter?

A, B, C, D : group of 3, order does not matter

ABC, ACB, BAC, BCA, CAB, CBA : 3!

ABC

ABD : 3!

ACD : 3!

BCD : 3!

$n=4$, $k=3$ $\Big\}$ ${}_4P_3 = \frac{4!}{(4-3)!} = \frac{4!}{1!} = 24$

24 ways to choose 3 from 4 if order matters

(if order doesn't matter it is $24/3! = 24/6 = 4$

view as $\frac{{}_4P_3}{3!}$ or $\frac{\frac{4!}{(4-3)!}}{3!} = \frac{4!}{3!(4-3)!}$

$= \frac{1!}{k!(n-k)!}$

If $_nP_k$ is # ways to choose k from n when order matters, remove ordering by dividing by $k!$, $_nC_k = \binom{n}{k} = \frac{n!}{k!(n-k)!}$ when n, k non-neg integers.

Pascal's Triangle



$\binom{n}{k}$ and Pascal

$$(x+y)^n = \sum_{k=0}^{n} a_{n,k} x^k y^{n-k}$$

To have n factors, if choose k to give x then rest, $n-k$, give y

$$a_{n,k} = \binom{n}{k}\binom{n-k}{n-k} = \binom{n}{k}$$

Binomial Theorem: $(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$ or $\sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k$

Application: Calculus

n pos integer $f(x) = x^n$, what is $f'(x)$?

$$f'(x) := \lim_{h \to 0} \frac{f(x+h) - f(x)}{h} = \lim_{h \to 0} \frac{(x+h)^n - x^n}{h}$$

$$= \lim_{h \to 0} \frac{x^n + n x^{n-1} h + \frac{n(n-1)}{2} x^{n-2} h^2 + \binom{n}{3} x^{n-3} h^3 + \cdots + h^n - x^n}{h}$$

$$= \lim_{h \to 0} \left[n x^{n-1} + h(\text{bounded crap}) \right] = n x^{n-1}$$

only need $(x+h)^n = x^n + n x^{n-1} h + (\text{something nice}) h^2$

What is derivative of $x^{3/2}$ or $x^{\sqrt{2}}$?

$f(x) = x^{m/n}$, m, n pos integers

$g(x) = f(x)^n = x^m$ nice function

$g'(x) = n f(x)^{n-1} f'(x)$ (power rule or repeated prod rule) $= m x^{m-1}$ (ok as integer power)

Solve for $f'(x) = \frac{m x^{m-1}}{n f(x)^{n-1}} = \frac{m}{n} \frac{x^{m-1}}{(x^{m/n})^{n-1}}$

$= \frac{m}{n} \frac{x^{m-1}}{x^{\frac{m}{n} n} x^{\frac{m}{n}(-1)}}$

$= \frac{m}{n} \frac{x^{m-1}}{x^m x^{-m/n}} = \frac{m}{n} \frac{x^m x^{-1} x^{m/n}}{x^m}$

$= \frac{m}{n} x^{\frac{m}{n}-1}$

Challenge: $x^{\sqrt{2}} = e^{\sqrt{2}\ln(x)} = e^{\sqrt{2}\log x}$ log for ln

$x^{\sqrt{2}} = \exp(\sqrt{2}(\ln x))$ use chain rule, exp' is the exp fn, and deriv ln' is the one-one function

---

HW: what is $\binom{3}{5}$? It is 0 as cannot take 5 objects from 3 when order does not matter.

If we want $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ even if $k > n$, then

need $\binom{3}{5} = \frac{3!}{5!(-2)!} = 0$ or $\frac{6}{120(-2)!} = 0$

Need $(-2)!$ to be "infinity"

FLT FCT

Math 310: Modern Algebra: Fall '25 (Siena)

Professor Steven J Miller: sjm1@williams.edu

Homepage:

https://web.williams.edu/Mathematics/sjmiller/public_html/310Fa25/

Lecture 05: 9/16/25: https://youtu.be/kBzzyUGNME4

Introduction to Groups (continued): properties, examples (especially the Pythagorean group)

To be a group need a set and a binary relation st

- closure: $\forall g_1, g_2 \in G : g_1 \cdot g_2$ is in G.
- identity: $\exists e \in G$ st $\forall g \in G : e \cdot g = g \cdot e = g$
- inverse: $\forall g \in G \; \exists g^{-1}$ st $g \cdot g^{-1} = g^{-1} \cdot g = e$
- assoc: $\forall g_1, g_2, g_3 \in G : (g_1 \cdot g_2) \cdot g_3 = g_1 \cdot (g_2 \cdot g_3)$

G be real numbers (x,y) st $x^2+y^2=1$

Define $(x,y)\otimes(a,b) = (xa-yb, ya+xb)$

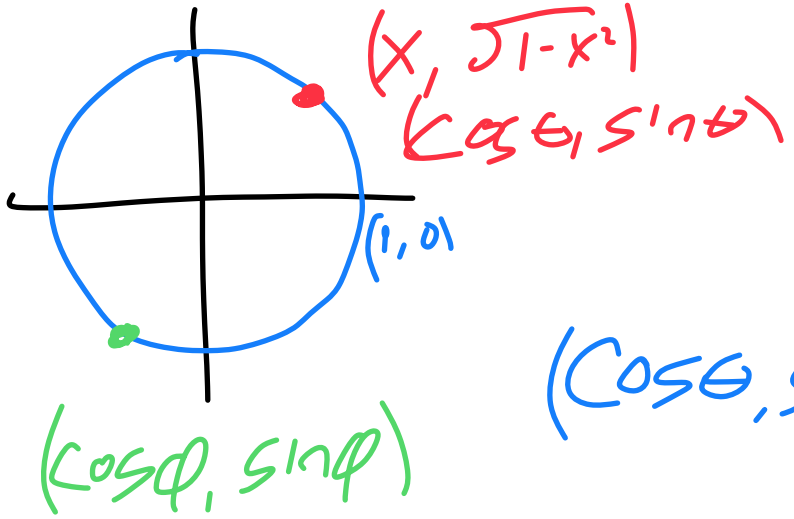
$$(x_1,y_1)\otimes(x_2,y_2) = (x_1x_2-y_1y_2, y_1x_2+x_1y_2) \leftarrow$$
$$= (x_1x_2-y_1y_2, x_1y_2+x_2y_1)$$
$$= (x_1x_2-y_1y_2, x_1y_2+y_1x_2)$$

$(0,1)\otimes(1,0) = (0,1) \in G$ Maybe $(1,0)$ is an identity

$(x,y)\otimes(1,0) = (x,y)$ also $(1,0)\otimes(x,y) = (x,y)$: identity!

$\left(\frac{3}{5},\frac{4}{5}\right)\otimes\left(\frac{1}{\sqrt{2}},\frac{1}{\sqrt{2}}\right) = \frac{1}{5}\frac{1}{\sqrt{2}}(3,4)\otimes(1,1) = \frac{1}{5\sqrt{2}}(-1,7) = \left(\frac{-1}{5\sqrt{2}},\frac{7}{5\sqrt{2}}\right)$

and $\frac{1}{50}+\frac{49}{50} = 1$ ✓ in G



$$(x,y) \otimes (a,b) = (xa - yb, ya + xb)$$

$$(\cos\theta, \sin\theta) \otimes (\cos\varphi, \sin\varphi)$$

$$= (\cos\theta\cos\varphi - \sin\theta\sin\varphi, \sin\theta\cos\varphi + \cos\theta\sin\varphi)$$

$$= (\cos(\theta+\varphi), \sin(\theta+\varphi)) \in G$$

Inverse of $(\cos\theta, \sin\theta)$: to $(\cos\varphi, \sin\varphi)$

Need $\theta + \varphi = 0$ as gives $(\cos 0, \sin 0) = (1,0)$ To $\varphi = -\theta$

Get $(\cos\theta, \sin\theta) \otimes (\cos(-\theta), \sin(-\theta))$

$\sin^2\theta + \cos^2\theta = 1$

$\cos^2\theta = 1 - \sin^2\theta$

$= (\cos\theta, \sin\theta) \otimes (\cos\theta, -\sin\theta) = (\cos^2\theta + \sin^2\theta, 0) = (1,0)$

Leave associativity to you.

$\mathbb{C} = \{ z = x+iy \text{ with } x,y \in \mathbb{R} \text{ and } i = \sqrt{-1} \}$

$(x+iy)(a+ib) = xa + iya + xib + iyib$

$= (xa - yb) + i(ya + xb)$

$(x,y) \otimes (a,b) = (xa - yb, ya + xb)$

If $|z| = 1$ and $|w| = 1$ then $|zw| = 1$

↳ $z = 1e^{i\theta}$ $w = 1e^{i\varphi}$ so $zw = e^{i(\theta+\varphi)}$

Pythagorean triple $a^2 + b^2 = c^2 \iff \left(\frac{a}{c}, \frac{b}{c}\right)$ on unit circle

$\left(\frac{3}{5}, \frac{4}{5}\right) \otimes \left(\frac{3}{5}, \frac{4}{5}\right) = \frac{1}{25}(3,4) \otimes (3,4) = \frac{1}{25}(-7, 24) = \left(\frac{-7}{25}, \frac{24}{25}\right)$

new triple: $7^2 + 24^2 = 25^2$

Proposition 2.9 (Basic Properties of Groups). *Let G be a group.*

(a) *G has exactly one identity element.*

(b) *Each element of G has exactly one inverse.*

(c) *Let $g, h \in G$. Then $(g \cdot h)^{-1} = h^{-1} \cdot g^{-1}$.*

(d) *Let $g \in G$. Then $(g^{-1})^{-1} = g$.*

Proof of (a) Assume not, so e_1, e_2 are identity elements

So $\forall g \in G: g \cdot e_1 = e_1 \cdot g = g$ and $g \cdot e_2 = e_2 \cdot g = g$

Taking $g = e_1$ yields $e_1 e_1 = e_1 \cdot e_1 = e_1$ and $e_1 \cdot e_2 = e_2 \cdot e_1 = e_1$

Taking $g = e_2$ yields $e_2 \cdot e_1 = e_1 \cdot e_2 = e_2$ and $e_2 \cdot e_2 = e_2 \cdot e_2 = e_2$

$e_2 \cdot e_1 = e_1 \cdot e_2 = e_1$ and e_2

Thus $e_1 = e_2$

Proposition 2.9 (Basic Properties of Groups). *Let G be a group.*

(a) *G has exactly one identity element.*

(b) *Each element of G has exactly one inverse.*

(c) *Let $g, h \in G$. Then $(g \cdot h)^{-1} = h^{-1} \cdot g^{-1}$.*

(d) *Let $g \in G$. Then $(g^{-1})^{-1} = g$.*

$2 \cdot (3x - 4) \overset{?}{=} 2 \cdot 8$

$3 \cdot (2x - 7) \overset{?}{=} 3 \cdot 9$

Proof of (b) by contradiction: assume $\exists g$ with two inverses, g_1, g_2

as g_1 is an inverse of g have $g_1 g = g g_1 = e$

" g_2 " " " " " g have $g_2 g = g g_2 = e$

multiply on left: $g_2 g_1 g = \boxed{g_2 g g_1} = g_2 e = g_2$

~~" " left $g_1 g_2 g = g_1 g g_2 = g_1 e = g_1$~~

multiply on right $\boxed{g_2 g g_1} = g g_2 g_1 = e g_1 = g_1$

Study $g_2 g g_1$

$g_2 (g g_1)$

$(g_2 g) g_1$

So $g_2 g g_1$ equals g_2 and equals g_1 QED

$\Rightarrow g_1 = g_2$ and inverse is unique

Proposition 2.9 (Basic Properties of Groups). *Let G be a group.*

(a) *G has exactly one identity element.*

(b) *Each element of G has exactly one inverse.*

(c) *Let $g, h \in G$. Then $(g \cdot h)^{-1} = h^{-1} \cdot g^{-1}$.*

(d) *Let $g \in G$. Then $(g^{-1})^{-1} = g$.*

To prove (c) must show $(gh)(h^{-1}g^{-1}) = e$ and $(h^{-1}g^{-1})(gh) = e$

↳ algebra: $(gh)(h^{-1}g^{-1}) = g(hh^{-1})g^{-1} = geg^{-1} = gg^{-1} = e$

OR $(gh)(h^{-1}g^{-1}) = g\left(h(h^{-1}g^{-1})\right) = g((hh^{-1})g^{-1})$

1 2 3 — 1 2 3

$= g(e \cdot g^{-1}) = gg^{-1} = e$

$(h^{-1}g^{-1})(gh)$ is similar

Proposition 2.9 (Basic Properties of Groups). *Let G be a group.*

(a) *G has exactly one identity element.*

(b) *Each element of G has exactly one inverse.*

(c) *Let $g, h \in G$. Then $(g \cdot h)^{-1} = h^{-1} \cdot g^{-1}$.*

(d) *Let $g \in G$. Then $(g^{-1})^{-1} = g$.*

(d) To show $(g^{-1})^{-1}$ is g, must show $g^{-1}g = gg^{-1} = e$

But, by definition, g^{-1} is defined so that $gg^{-1} = g^{-1}g = e$

done!

Extra credit: If have a finite product in a group, prove can combine any way in pairs if do not switch order: Ex: $((x_1 x_2)x_3)x_4 = (x_1 x_2)(x_3 x_4)$

Definition 2.11. The *order* of a group G, which we denote by $\#G$, is the cardinality of the set of elements of G. In particular, if G is finite, then $\#G$ is simply the number of elements in G. We remark that other common notations for the order of a group are $o(G)$ and $|G|$.

Proposition 2.13. *Let G be a group, let $g \in G$, and let $n \geq 1$ be an integer such that $g^n = e$. Then the order of g divides n.*

If $|G| = 50$ and $g \in G$, can $g^7 = e$? YES: $g = e$

The order of g is the smallest n such that $g^n = e$ and $g^k \neq e$ for any positive $k > 0$, with $k < n$.

Note order of e is 1, if $g \neq e$ is order$(g) = 1$? NO

Consider: $\{e, g, g^2, g^3, \ldots\}$, assume $\#G$ is finite

Must repeat: $g^k = g^l$ with $k < l$ (say $g^\gamma = g^\alpha \Rightarrow g^{-\gamma} g^\gamma = g^{-\gamma} g^\alpha$ or $e = g^\gamma$)

$\{e, g, g^2, \ldots, g^6, e g, g^2, \ldots\}$

$\{e, g, g^2, \ldots, g^{n-1}\}$ with $g^n = e$, $g^k \neq e$ if $k < n$ and $k \geq 1$

Is this a group? YES! as lives in G, call it a subgroup of G, write as $\langle g \rangle$, the subgroup generated by g.

- Closure: $g^{k_1} g^{k_2} = g^{k_3}$ with $0 \leq k_3 < n$
- Identity: e (inherited)
- inverses: yes (inherited, BUT have to show in $\langle g \rangle$)
- assoc: yes: inherited

Math 310: Modern Algebra: Fall '25 (Siena)

Professor Steven J Miller: sjm1@williams.edu

Homepage:

https://web.williams.edu/Mathematics/sjmiller/public_html/310Fa25/

Lecture 06: 9/18/25: https://youtu.be/KqDDHELD33A

Introduction to Groups (continued): properties, examples (especially clock groups)

Definition 2.11. The *order* of a group G, which we denote by $\#G$, is the cardinality of the set of elements of G. In particular, if G is finite, then $\#G$ is simply the number of elements in G. We remark that other common notations for the order of a group are $o(G)$ and $|G|$.

Proposition 2.13. *Let G be a group, let $g \in G$, and let $n \geq 1$ be an integer such that $g^n = e$. Then the order of g divides n.*

If $|G| = 50$ and $g \in G$, can $g^7 = e$? YES: $g = e$

The order of g is the smallest n such that $g^n = e$ and $g^k \neq e$ for any positive $k > 0$, with $k < n$.

Note order of e is 1, if $g \neq e$ is order$(g) = 1$? NO

Consider: $\{e, g, g^2, g^3, \ldots\}$, assume $\#G$ is finite

Must repeat: $g^k = g^l$ with $k < l$ (say $g^\gamma = g^\alpha \Rightarrow g^{-\gamma} g^\gamma = g^{-\gamma} g^\alpha$ or $e = g^\gamma$)

$\{e, g, g^2, \ldots, g^6, e g, g^2, \ldots\}$

$\{e, g, g^2, \ldots, g^{n-1}\}$ with $g^n = e$, $g^k \neq e$ if $k < n$ and $k \geq 1$

Is this a group? YES! as lives in G, call it a subgroup of G, write as $\langle g \rangle$, the subgroup generated by g.

- Closure: $g^{k_1} g^{k_2} = g^{k_3}$ with $0 \leq k_3 < n$
- Identity: e (inherited)
- inverses: yes (inherited, BUT have to show in $\langle g \rangle$)
- assoc: yes: inherited

Proof of Prop 2.13

G is a finite group, $g \in G$ has order $n > 1$

Let $N = \#G$, the number of elements of G.

Set $\{e, g, g^2, \ldots, g^{n-1}\} \subset G$ and $g^n = e$

If $n > N$ then more elements in $\{e, g, g^2, \ldots, g^{n-1}\}$ than in G!

So $n \leq N$.

Write $N = an + r$; a, r integers and $0 \leq r < n$

Want to show $r = 0$.

only elements know: e, g what numbers: N, n, r, a

$g^n = e$ (known), $g^N = ?$

know $g^N = g^{an+r} = g^{an} g^r = (g^n)^a g^r = g^r$

Know $g^n = e$ $\quad g^N = g^r$ where $N = qn + r$, $0 \le r < n$

Cayley data

$\{1, 2, 3, 4\}$ under multiplication mod 5

	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

$1^4 = 1,\ 2^4 = 1,\ 3^4 = 1,\ 4^4 = 1$

$3^4 = (4-1)^4 \equiv (-1)^4 \equiv 1 \pmod 5$

Is this cyclic?

$\langle 2 \rangle = \{1, 2, 4, 3\}$

$\langle 3 \rangle = \{1, 3, 4, 2\}$

$\langle 4 \rangle = \{1, 4\}$

YES: 2 or 3 can be a generator

Chapter Two: Section 3: Examples of Groups:

Example 2.14 (Groups of Integers and Integers Modulo m). addition

Example 2.15 (Additive Groups of Real, Rational, and Complex Numbers).

Example 2.16 (Multiplicatives Group of Real, Rational, and Complex Numbers).

Example 2.18 (Cyclic Groups). $\langle g \rangle = \{e, g, g^2, \cdots, g^{n-1}\}$ and $g^n = e$, n smallest n works

Example 2.19 (Permutation Groups).

Example 2.21 (Matrix Groups).

Example 2.22 (Dihedral Groups).

Example 2.23 (Quaternion Group). Generalization of $\mathbb{C}$

Example for 2.18

$i = \sqrt{-1} : \langle i \rangle = \{1, i, -1, -i\}$

$g = e^{2\pi i/n} : \langle g \rangle = \{1, e^{2\pi i/n}, e^{2\pi i 2/n}, e^{2\pi i 3/n}, \cdots, e^{2\pi i (n-1)/n}\}$

Clock with 12 hours under multiplication

	1	2	3	4	5	6	7	8	9	10	11
1	1	2	3	4	5	6	7	8	9	10	11
2	2	4	6	8	10	0	2	4	6	8	10
3	3		9		3	9	9		3		9
4	4										
5	5										
6	6										
7	7										
8	8										
9	9										
10	10										
11	11										

	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

not closed (bad)

has identity (good)

is assoc (good)

some elements have no inverse (bad)

$x^2 = e$ has four solutions

not cyclic

What about clock arithmetic under multiplication?

Lemma: If n is composite, $\{1, 2, \dots, n-1\}$ is not a group under clock multiplication

Proof: Will show not closed.
Since n is composite, $n = n_1 n_2$ where each ≥ 2
Ex. if $n = 12$ then $n = 3 \cdot 4$ or $n = 2 \cdot 6$
In general, if $n = n_1 n_2$, each $n_k \geq 2$, $n_1 n_2 \notin \{1, 2, \dots, n-1\}$ under clock multiplication. So not closed!

Proof #2: If $n = n_1 n_2$, each $n_k \geq 2$, will show n_1 is not invertible
Imagine n_1 has an inverse on clock with n hours
$\exists a$ such that $a n_1 \equiv 1 \bmod n$
means $\exists b$ such that $a n_1 = 1 + bn$ or $a n_1 = 1 + b n_1 n_2$
Thus $a n_1 - b n_1 n_2 = 1$ or $(a - b n_2) n_1 = 1$ so n_1 divides 1, impossible as $n_1 \geq 2$

What if have a clock with p prime hours under clock multiplication

(7 hours)

	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

closed ✓

assoc ✓

identity ✓

inverse ✓

$\langle 2 \rangle = \{1, 2, 4\}$ as $ord(2) = 3$

$\langle 4 \rangle = \{1, 4, 2\}$ as $ord(4) = 3$

$\langle 6 \rangle = \{1, 6\}$ as $ord(6) = 2$

$\langle 3 \rangle = \{1, 3, 2, 6, 4, 5\}$ as $ord(3) = 6$

$\langle 5 \rangle = \{1, 5, 4, 6, 2, 3\}$ as $ord(5) = 6$

Cyclic group

↳ generated by powers of 3 or 5

(generator is not unique)

Question: If p is prime, is $\{1, 2, \ldots, p-1\}$ a group under mult?

- Assoc: Yes, inherits from regular multiplication.
- Identity: 1
- Closure: assume $m, n \in \{1, 2, \ldots, p-1\}$ and mn not in the set. (mod p)

  $m \cdot n \bmod p$ has to be 0 if not closed.

  So have m, n in $\{1, \ldots, p-1\}$ with $m \cdot n \equiv 0 \bmod p$

  ↳ $\exists\, b$ such that $m \cdot n = 0 + bp$ so $m \cdot n = bp$

  if a prime divides a product it divides at least one factor.

  So if $b \neq 0$ then $p \mid m$ or $p \mid n$, contradiction

  So $b = 0$ and $m \neq 0$, impossible as each is ≥ 1

If a composite divides a product must it divide at least one factor?

↳ NO: 6 divides $4 \cdot 3$ but 6 doesn't divide either.

Inverses: If $m \in \{1, 2, \ldots, p-1\}$ with p prime then there is an n in this set with $m \cdot n \equiv 1 \bmod p$.

Euclidean Algorithm

find gcd of two numbers EFFICIENTLY

Factor by trying all numbers: if $X = 10^{100} \ldots$ are!

If X is composite $X = ab$ and at least one is $\leq \sqrt{X}$

Math 310: Modern Algebra: Fall '25 (Siena)

Professor Steven J Miller: sjm1@williams.edu

Homepage:

https://web.williams.edu/Mathematics/sjmiller/public_html/310Fa25/

Lecture 07: 9/23/25: https://youtu.be/tjhvEV6JX7Q

Introduction to Euclidean Algorithm and Applications, Subgroups, Homomorphisms.

Euclidean Alg

A very efficient way to find integers a, b such that, for given integers x and y, we have

$$ax + by = \gcd(x, y)$$

gcd: greatest common divisor
largest integer dividing x and y

If a and b work, so too does $a+y$ and $b-x$
or $a+ny$ and $b-nx$

Proof a and b exist when x, y relatively prime.

Consider the set $\{ax+by$ with $0 \le a \le y-1,\ 0 \le b \le x-1\}$

Size of set is at most xy

Claim all distinct mod xy

If not, have two pairs with $a_1x+b_1y \equiv a_2x+b_2y \bmod xy$

$$(a_1-a_2)x \equiv (b_2-b_1)y \bmod xy$$

means $\exists\, m$ such that $(a_1-a_2)x = (b_2-b_1)y + mxy$

$(a_1-a_2)x$: multiple of x

$(b_2-b_1)y$: multiple of x

mxy: multiple of x

So x divides b_2-b_1

Thus $b_2=b_1$

Similar argument gives $a_2=a_1$

We have xy pairs, all distinct mod xy

How many remainders are there mod xy? xy

As everything is distinct, must be a choice of a, b

such that $ax + by \equiv 1 \bmod xy$.

$0 \le a \le x-1, \quad 0 \le b \le y-1$

if $x, y \sim 10^{200}$ then # possibilities $\sim 10^{400}$

write $x = \tilde{x} d$
$y = \tilde{y} d$ with $\gcd(\tilde{x}, \tilde{y}) = 1$

USELESS in practice!

Euclidean Algorithm

Find $\gcd(x,y)$ w.l.o.g. assume $x \le y$

- $y = q_1 x + r_1$ $\quad 0 \le r_1 \le x-1$
- $x = q_2 r_1 + r_2$ $\quad 0 \le r_2 \le r_1 - 1$
- $r_1 = q_3 r_2 + r_3$ $\quad 0 \le r_3 \le r_2 - 1$
- $r_2 = q_4 r_3 + r_4$ $\quad 0 \le r_4 \le r_3 - 1$

terminates in at most x steps

$\vdots$

- $r_k = q_{k+2} r_{k+1} + r_{k+2}$ eventually 1 or 0.
- $r_{k+1} = q_{k+3} r_{k+2} + 0$

$\gcd(r_{k+2}, r_{k+1}) = r_{k+2}$

- $y = q_1 x + r_1$ $\quad 0 \le r_1 \le x-1$
- $x = q_2 r_1 + r_2$ $\quad 0 \le r_2 \le r_1 - 1$
- $r_1 = q_3 r_2 + r_3$ $\quad 0 \le r_3 \le r_2 - 1$
- $r_2 = q_4 r_3 + r_4$ $\quad 0 \le r_4 \le r_3 - 1$

Let $d = \gcd(x,y)$ so $d \mid x$ and $d \mid y$

↳ does $d \mid r_1$? $r_1 = y - q_1 x$ so $d \mid r_1$ as $d \mid y$ and $d \mid x$

Imagine $\tilde{d} = \gcd(r_1, x)$: does $\tilde{d} \mid y$? $y = q_1 x + r_1$ so $\tilde{d} \mid y$ as $\tilde{d} \mid x$ and $\tilde{d} \mid r_1$

$\Rightarrow \gcd(x,y) = \gcd(r_1, x)$

$\gcd(x,y) = \gcd(r_1, x) = \gcd(r_2, r_1) = \cdots = \gcd(r_{k+2}, r_{k+1})$

$= r_{k+2}$

Theorem: every two steps of the Euclidean Algorithm decrease the remainder by at least a factor of 2.

- $r_1 = q_3 r_2 + r_3$ $\quad 0 \le r_3 \le r_2 - 1$
- $r_2 = q_4 r_3 + r_4$ $\quad 0 \le r_4 \le r_3 - 1$

Claim: $r_4 \le \frac{1}{2} r_2$

Case 1: $r_3 \le \frac{1}{2} r_2$: Then since $r_4 \le r_3$, have $r_4 \le \frac{1}{2} r_2$

Case 2: $r_3 > \frac{1}{2} r_2$

worse case: $r_1 = q_3 r_2 + r_2 - 1$

$r_2 = \boxed{1} (r_2 - 1) + \boxed{?}$

$1 \quad (r_2 - 1) + 1$

Assuming $r_3 > \frac{1}{2} r_2$

$r_2 = \boxed{?}\, r_3 + \boxed{?}$

since $r_3 > \frac{1}{2} r_2$, $2r_3 > r_2$

So $r_2 = 1\, r_3 + r_4$

So $r_4 = r_2 - r_3 < \frac{1}{2} r_2$ ≡

$10^{200} = 2^?$

$\log_{10}(10^{200}) = \log_{10}(2^u)$

$200 = u \log_{10} 2$

so $u = 200 / \log_{10}(2) < 400$

Definition 2.34. Let G be a group. A *subgroup of* G is a subset $H \subset G$ that is itself a group using G's group law. Explicitly, H needs to satisfy the following:

(i) For every $h_1, h_2 \in H$, the product $h_1 \cdot h_2$ is in H. Mathematically, we say that H is *closed* for the group law on G.
(ii) The identity element e is in H.
(iii) For every $h \in H$, the inverse h^{-1} is in H.

What is the linear algebra equivalent? Subspace

Ex: $\{1, 5, 7, 11\}$ under clock multiplication with 12 hours

Subgroups: $\{1, 5, 7, 11\}$, $\{1\}$ trivial subgroups

$\{1, 5\}$, $\{1, 7\}$, $\{1, 11\}$

~~$\{1, 5, 7\}$~~ not a subgroup as $5 \cdot 7 = 11 \bmod 12$

Clock with n hours, Study elements relatively prime to n:

$\mathbb{Z}$ integers

$n\mathbb{Z}$ integer multiples of n: $\{\dots, -2n, -n, 0, n, 2n, \dots\}$

$\mathbb{Z}/n\mathbb{Z} := \{0, 1, 2, \dots, n-1\}$ under clock rules

$(\mathbb{Z}/n\mathbb{Z})^* := \{m \in \mathbb{Z}/n\mathbb{Z} \text{ with } \gcd(m, n) = 1\}$

Ex: $n = 12$: $(\mathbb{Z}/12\mathbb{Z})^* = \{1, 5, 7, 11\}$

$n = 7$: $(\mathbb{Z}/7\mathbb{Z})^* = \{1, 2, 3, 4, 5, 6\}$

$n = p$ prime $(\mathbb{Z}/p\mathbb{Z})^* = \{1, 2, \dots, p-1\}$

Study $(\mathbb{Z}/n\mathbb{Z})^*$ = all integers from 1 to $n-1$ that are relatively prime to n under clock multiplication mod n.

Question: Is this a group?

- Associativity inherited so true
- Identity: yes as $\gcd(1, n) = 1$ so $1 \in (\mathbb{Z}/n\mathbb{Z})^*$
- Closure: assume $x, y \in (\mathbb{Z}/n\mathbb{Z})^*$: So $\gcd(x, n) = \gcd(y, n) = 1$

Then $\gcd(xy, n) = 1$: If not have a prime p dividing xy and n, and if $p \mid xy$ then $p \mid x$ or $p \mid y$ contradicting relative primality.

- Inverses: must show if $x \in (\mathbb{Z}/n\mathbb{Z})^*$ then x has an inverse under multiplication mod n.

Find an element x^{-1} st $x^{-1}x \equiv 1 \bmod n$

Lets use the Euclidean Algorithm with x and n.

Thus $\exists a, b$ such that $ax + bn = \gcd(x, n) = 1$

So $ax + bn = 1$

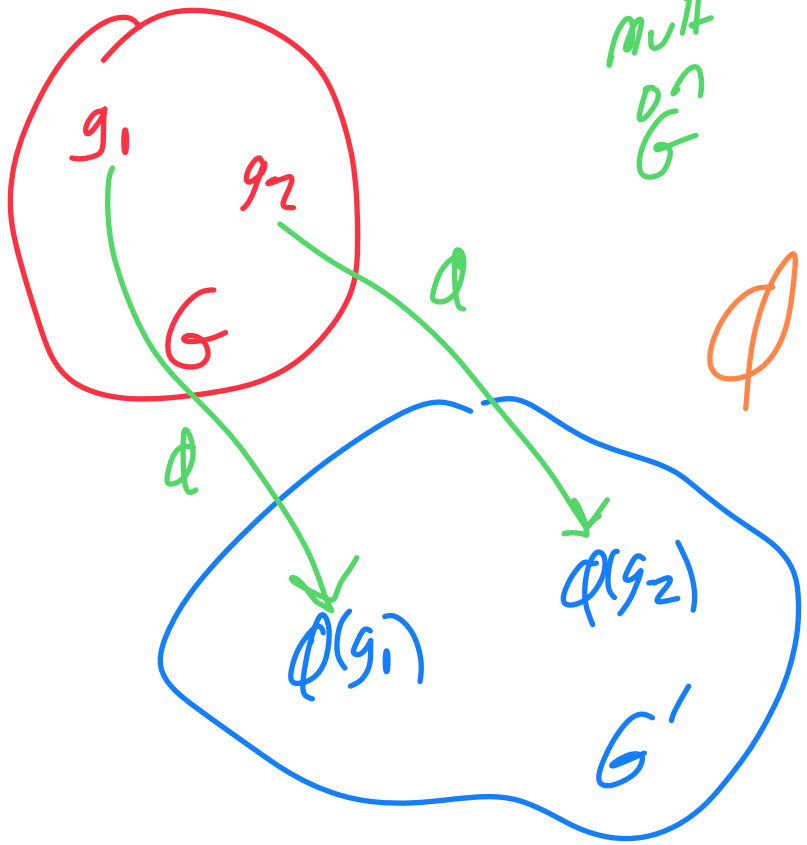
or $ax = 1 - bn$

or $ax \equiv 1 \bmod n$ ∎

Definition 2.24. Let G and G' be groups. A *homomorphism from G to G'* is a function $\phi : G \to G'$ satisfying

$$\phi(g_1 \cdot g_2) = \phi(g_1) \cdot \phi(g_2) \quad \text{for all} \quad g_1, g_2 \in G.$$

mult on G — mult on G'



$$\phi(g_1 *_G g_2) = \phi(g_1) *_{G'} \phi(g_2)$$

order does not matter

$$\sqrt{9+16} \neq \sqrt{9} + \sqrt{16}$$

$$\| \qquad\qquad \| \qquad\qquad \|$$

$$5 \qquad\qquad 7$$

Proposition 2.25. *Let $\phi : G \to G'$ be a homomorphism of groups.*

(a) *Let $e \in G$ be the identity element of G. Then $\phi(e)$ is the identity element of G'.*

(b) *Let $g \in G$. Then $\phi(g^{-1})$ is the inverse of $\phi(g)$ in G'.*

Have $\forall g_1, g_2 \in G$ that $\phi(g_1 \cdot g_2) = \phi(g_1) \cdot \phi(g_2)$

Prove (a)

Take $g_1 = e$ and $g_2 = e$

Thus $\phi(\underbrace{e \cdot e}_{e}) = \phi(e) \cdot \phi(e)$

$\Rightarrow \phi(e) = \phi(e) \cdot \phi(e)$ $\quad \phi(e) \in$ group G'

$[\phi(e)]^{-1} \phi(e) = [\phi(e)]^{-1} \cdot \phi(e) \cdot \phi(e)$

$e' = e' \cdot \phi(e) \rightarrow e' = \phi(e)$

(b) Show $\phi(g^{-1})$ is the inverse of $\phi(g)$

$$\phi(g^{-1}) \cdot \phi(g) = \phi(g^{-1} \cdot g)$$
$$= \phi(e)$$
$$= e'$$

Thus $\phi(g^{-1})$ is the inverse of $\phi(g)$

well, $\phi(g)\phi(g^{-1}) = e'$ must be shown.

Math 310: Modern Algebra: Fall '25 (Siena)

Professor Steven J Miller: sjm1@williams.edu

Homepage:

https://web.williams.edu/Mathematics/sjmiller/public_html/310Fa25/

Lecture 08: 9/25/25: NO CLASS: WORK ON EXAM

Lecture 09: 9/30/25: https://youtu.be/YNiwTza4OHM

Subgroups, Homomorphisms.

Proposition 2.25. *Let $\phi : G \to G'$ be a homomorphism of groups.*

(a) *Let $e \in G$ be the identity element of G. Then $\phi(e)$ is the identity element of G'.*

(b) *Let $g \in G$. Then $\phi(g^{-1})$ is the inverse of $\phi(g)$ in G'.*

$\phi(g_1 \cdot_G g_2) = \phi(g_1) \cdot_{G'} \phi(g_2)$

(b) Know e, e', g, g^{-1}

will do left: $\phi(g^{-1})\phi(g) = \phi(g^{-1}g)$ by defn of ϕ

$= \phi(e)$ as g^{-1} is the inverse of g

$= e'$ by part (a)

Thus $\phi(g^{-1})$ is the left inverse of $\phi(g)$

Definition 2.30. Two groups G_1 and G_2 are said to be *isomorphic* if there is a bijective homomorphism

$\hookrightarrow$ (injective)
onto (surjective)

$$\phi : G_1 \longrightarrow G_2.$$

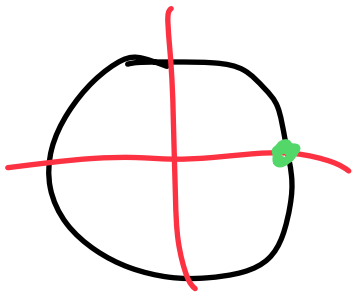
The map ϕ is called an *isomorphism* from G_1 to G_2. Isomorphic groups are essentially the same group, but their elements have been given different names.[9]

$(\mathbb{Z}/7\mathbb{Z})^* = \{1, 2, 3, 4, 5, 6\}$ under clock multiplication with 7 as the # hours

$\langle 3 \rangle, \langle 5 \rangle$

$3 \cdot 4 \equiv 5, \quad 3^{-1} \equiv 5 \mod 7$

$\zeta_6 = e^{2\pi i/6}, \quad \zeta_6^2 = e^{2\pi i\, 2/6}, \quad \zeta_6^3 = e^{2\pi i\, 3/6}, \ \ldots, \ \zeta_6^6 = 1$



cyclic group: $\langle \zeta_6 \rangle$

Try $\phi(\zeta_6) = 3$ or 5; $\phi(\zeta_6) = 2$

6 for 1st spot, 6 for second $\Rightarrow$ 36

Commutative: $\binom{6}{2} + \binom{6}{1} = 15 + 6 = 21$

$\langle g_6 \rangle$ with $g_6 = e^{2\pi i/6}$

$\uparrow$ of the form g_6^k

$\phi(g_1 g_2) = \phi(g_6^{k_1} g_6^{k_2}) = \phi(g_6^{k_1+k_2})$

$\stackrel{?}{=} \phi(g_6^{k_1})\,\phi(g_6^{k_2})$

Prove: If ϕ group homomorphism

Then $\phi(g^k) = \phi(g)^k$

Is $\varphi(g^k) = \varphi(g)^k$?

- If $k=1$ trivial
- If $k=2$ then $\varphi(g^2) = \varphi(g \cdot g) = \varphi(g)\,\varphi(g) = \varphi(g)^2$

group homomorphism

- If $k=3$ then $\varphi(g^3) = \varphi(g \cdot g^2) = \varphi(g)\,\varphi(g^2)$

$= \varphi(g)\,\varphi(g)\,\varphi(g)$

$= \varphi(g)^3$

Prove by Induction

Remark 2.32. Isomorphic groups have identical structural properties. For example, if G_1 and G_2 are isomorphic, then:

(1) If one of them is finite, then they are both finite, and they satisfy $\#G_1 = \#G_2$.

(2) If one of them is abelian, then they are both abelian.

(3) If G_1 has an element of order n, then G_2 also has an element of order n.

(4) More generally, if G_1 has k different elements of order n, then G_2 also has k different elements of order n.

Exercise 2.23 asks you to prove these four assertions.

How to Prove that Groups Are Not Isomorphic?

Example:

$G_1 = \{1, 2, 3, 4\}$ clock mult, 5 hours

$G_2 = \{1, 5, 7, 11\}$ clock mult, 12 hours

↳ all elements are of order 2, not cyclic

But in G_1: $1, 3, 3^2 \equiv 4 \bmod 5$, $3^3 \equiv 2 \bmod 5$, $3^4 \equiv 1 \bmod 5$

so G_1 has an element of order 4, is cyclic

NOT ISOMORPHIC

3-Step Program to Analyze Mathematical Objects

Step 1 (Deconstruction): Break your object into smaller and simpler pieces.

Step 2 (Analysis): Analyze the smaller, simpler pieces.

Step 3 (Reconstruction): Fit the pieces back together.

Definition 2.34. Let G be a group. A *subgroup of* G is a subset $H \subset G$ that is itself a group using G's group law. Explicitly, H needs to satisfy the following:

(i) For every $h_1, h_2 \in H$, the product $h_1 \cdot h_2$ is in H. Mathematically, we say that H is *closed* for the group law on G.
(ii) The identity element e is in H.
(iii) For every $h \in H$, the inverse h^{-1} is in H.

What is the linear algebra equivalent? SUBSPACES

Example 2.38. Let $d \in \mathbb{Z}$, then we can form a subgroup of $\mathbb{Z}$ using the multiples of d,

$$d\mathbb{Z} = \{dn : n \in \mathbb{Z}\}.$$

Find $\varphi : \mathbb{Z} \to d\mathbb{Z}$ that is a group homomorphism?

$\varphi(n) = 0$

Find a non-trivial one!

Guess $\varphi(n) = dn$

$\varphi(n_1 + n_2) = d(n_1 + n_2) = dn_1 + dn_2$

$= \varphi(n_1) + \varphi(n_2)$

Cyclic subgroup of G generated by g, denoted by <g>:

Any element is of the form g^n for some n

$$g^{n_1} g^{n_2} = g^{n_1+n_2}$$

$$\{1,2,3,4,5,6\} \longleftrightarrow \langle \varphi_6 \rangle \text{ with } \varphi_6 = e^{2\pi i/6}$$

$$\varphi_6^2 \varphi_6^4 = \varphi_6^6$$

Definition 2.41. Let $\phi : G \to G'$ be a group homomorphism. The *kernel of* ϕ is the set of elements of G that are sent to the identity element of G',

$$\ker(\phi) = \{g \in G : \phi(g) = e'\}.$$

subset of G.



Thm: $\ker(\phi)$ is a subgroup of G.

Proof: (1) have identity as $\phi(e) = e'$

(2) closure: if $g_1, g_2 \in \ker(\phi)$ then $\phi(g_1) = e' = \phi(g_2)$

then $\phi(g_1 g_2) = \phi(g_1)\phi(g_2) = e' \cdot e' = e'$

(group homom) (assumpt)

(3) assoc is free

If $g \in \ker(\phi)$ must show $g^{-1} \in \ker(\phi)$

$$g\,g^{-1} = e$$

$$\phi(g g^{-1}) = \phi(e)$$ (group homomorphism)

$$\phi(g)\phi(g^{-1}) = e'$$ (property)

$$e' \cdot \phi(g^{-1}) = e'$$ (identity)

$$\phi(g^{-1}) = e' \Rightarrow g^{-1} \in \ker(\phi)$$ ∎

Proposition 2.44. *Let $\phi : G \to G'$ be a group homomorphism.*

(a) $\ker(\phi)$ *is a subgroup of* G.

(b) ϕ *is injective if and only if* $\ker(\phi) = \{e\}$.

Definition 2.45. Let G be a group, and let $H \subset G$ be a subgroup of G. For each $g \in G$, the (left) *coset of H attached to g* is the set

$$gH = \{gh : h \in H\}.$$

Ex: If $H = \{e, h_1, h_2, h_3\}$ Then $gH = \{g, gh_1, gh_2, gh_3\} \subset G$

$\#gH = \#H$

If $x \in gH$ Then $x = ge$ or gh_1 or gh_2 or gh_3 here.

More generally, $x \in gH$ means $x = gh$ for some $h \in H$

Proposition 2.47. *Let G be a finite group, and let $H \subset G$ be a subgroup of G.*

(a) *Every element of G is in some coset of H.* Given $g \in G$, $g = ge \in gH$ as $e \in H$

(b) *Every coset of H has the same number of elements.*

(c) *Let $g_1, g_2 \in G$. Then the cosets g_1H and g_2H satisfy either*

$$g_1H = g_2H \quad \text{or} \quad g_1H \cap g_2H = \emptyset.$$

Using set-theoretic terminology, this says that cosets of H are either equal or disjoint.

(c) Assume have $x \in g_1H \cap g_2H$

Thus $x \in g_1H$ and $x \in g_2H$

have $h_1 \in H$ with $x = g_1h_1$ and an $h_2 \in H$ with $x = g_2h_2$

$\Rightarrow g_1h_1 = g_2h_2$ or $g_1 = g_2h_2h_1^{-1}$

$$g_1H = (g_2h_2h_1^{-1})H = g_2(h_2(h_1^{-1}H))$$

$$= g_2(h_2H)$$

$$= g_2H$$

Lemma: if H is a subgroup of G and $h \in H$ then $hH = H$

More generally: if $g \in G$ then $gG = G$

Proof: If $gg_1 = gg_2 \Rightarrow g^{-1}gg_1 = g^{-1}gg_2 \Rightarrow g_1 = g_2$

map $f_g(x) = gx$ is 1-1

Say want $gx = \tilde{g}$ for some $\tilde{g} \in G$

Try $x = g^{-1}\tilde{g}$ then $gx = gg^{-1}\tilde{g} = \tilde{g}$

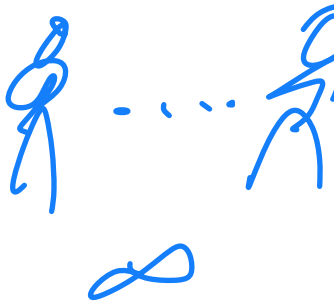
The map $x \mapsto gx$ is 1-1, onto: bijection

as finite, $\#G$ and $\#gG$ is the same.

Hilbert Hotel

Rooms 0, 1, 2, 3, ... full


wants room: 0 → 1, 1 → 2, 2 → 3, 3 → 4, ...



: 0 → 0, 1 → 2, 2 → 4, 3 → 6, ...

Theorem 2.48 (Lagrange's Theorem). *Let G be a finite group, and let H be a subgroup of G. Then*

$$\#G = \#H \cdot (\#\ \textit{of distinct cosets of } G \textit{ in } H),$$

and hence the order of H divides the order of G.

Proof: $G = \bigcup_{g \in G} gH$ as $e \in H$, $ge \in gH$

$G = \bigsqcup_{k=1}^{m} g_k H$ disjoint union

$\#G = (\#H)\, m$

If $g \in G$ then $\langle g \rangle \subset G$

thus as $\langle g \rangle$ is a subgroup, $\text{ord}(g)$ divides $\#G$

$\text{ord}(g)$ is smallest n such that $g^n = e$

If p is prime, $(\mathbb{Z}/p\mathbb{Z})^* = \{1, 2, \ldots, p-1\}$

This group has size $p-1$

so if $a \in (\mathbb{Z}/p\mathbb{Z})^*$ then $a^{p-1} \equiv 1 \bmod p$

$(\mathbb{Z}/n\mathbb{Z})^*$

$(\mathbb{Z}/n\mathbb{Z})^* = \{m \text{ from } 1 \text{ to } n \text{ relatively prime to } n\}$

Ex: $(\mathbb{Z}/12\mathbb{Z})^* = \{1, 5, 7, 11\}$

Euler Totient function ϕ is the # elements in $(\mathbb{Z}/n\mathbb{Z})^*$,
i.e., the number of numbers from 1 to n rel prime to n.

Size of $(\mathbb{Z}/n\mathbb{Z})^*$, $\#(\mathbb{Z}/n\mathbb{Z})^*$, is $\phi(n)$

So if a is rel prime to n!

by Lagrange, $a^{\phi(n)} \equiv 1 \mod n$

If n is prime, $\phi(n) = n-1$

Definition 2.54. Let G_1 and G_2 be groups. The *product* of G_1 and G_2 is the group whose elements consist of ordered pairs

$$G_1 \times G_2 = \{(a, b) : a \in G_1 \text{ and } b \in G_2\}$$

and whose group operation is performed separately on each component. In other words, the product of two elements of $G_1 \times G_2$ is *defined* by the following formula:

$$(a, b) \cdot (a', b') \quad \text{is equal to} \quad (a \cdot a', b \cdot b')$$

- $\cdot$: the group operation for $G_1 \times G_2$
- $a \cdot a'$: G_1's group operation
- $b \cdot b'$: G_2's group operation

Example 2.55. For any non-zero integers m and n, there is a homomorphism

$$\mathbb{Z}/mn\mathbb{Z} \longrightarrow (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z}),$$
$$a \bmod mn \longmapsto (a \bmod m, a \bmod n).$$

Theorem 2.56 (Structure Theorem for Finite Abelian Groups)**.** *Let G be a finite abelian group. Then there are integers $m_1, \ldots, m_r$ so that*

$$G \cong (\mathbb{Z}/m_1\mathbb{Z}) \times (\mathbb{Z}/m_2\mathbb{Z}) \times \cdots \times (\mathbb{Z}/m_r\mathbb{Z}).$$

Further, we may take $m_1, \ldots, m_r$ to be prime powers.

Proof. See Section 11.9.1. □

Example 2.57 (Projections and Inclusions). Products of groups come with two natural *projection homomorphisms*

$$p_1 : G_1 \times G_2 \longrightarrow G_1, \qquad (a, b) \longmapsto a,$$

$$p_2 : G_1 \times G_2 \longrightarrow G_2, \qquad (a, b) \longmapsto b,$$

and two natural *inclusion homomorphisms*

$$\iota_1 : G_1 \longrightarrow G_1 \times G_2, \qquad a \longmapsto (a, e_2),$$

$$\iota_2 : G_2 \longrightarrow G_1 \times G_2, \qquad b \longmapsto (e_1, b).$$

The inclusion maps are injective, but the projections have kernels,

$$\ker(p_1) = \{e_1\} \times G_2 \quad \text{and} \quad \ker(p_2) = G_1 \times \{e_2\}.$$

Fermat's little Theorem (FIT)

Let gcd(a,n) = 1. Then $a^{\varphi(n)} = 1$.

If n = prime p Then $\Rightarrow a^{p-1} \equiv 1 \mod p$.

$\gcd(5,6) = 1$

If 6 is prime Then $5^{6-1} \equiv 1 \mod 6$

So what is $5^5 \mod 6$? $(5^2)^2 \cdot 5$

$5^2 \equiv 1$ so $5^5 \equiv 5^2 \cdot 5^2 \cdot 5 \equiv 1 \cdot 1 \cdot 5 \equiv 5 \mod 6$

as $5 \not\equiv 1 \mod 6 \Longrightarrow$ 6 is composite!

Carmichael

Math 310: Modern Algebra: Fall '25 (Siena)

Professor Steven J Miller: sjm1@williams.edu

Homepage:

https://web.williams.edu/Mathematics/sjmiller/public_html/310Fa25/

Ring Theory Lecture

Lecture 10: 10/2/25: https://youtu.be/N2yL7qvrwaQ

Chapter Three: Fast Multiplication, Rings (Definitions, Examples, Properties)

Fermat's little Theorem (FIT)

Let gcd(a,n) = 1. Then $a^{\varphi(n)} = 1$. Useless without Fast Multiplication!

If n = prime p, then $\varphi(p) = p-1 \Rightarrow a^{p-1} \equiv 1 \bmod p$

mult to get a^{100}? 99 : Need Fast Mult / Exponentation

$x \cdot x = x^2$

$x^2 x^2 = x^4$ ←

$x^4 x^4 = x^8$

$x^8 x^8 = x^{16}$

$x^{16} x^{16} = x^{32}$ ←

$x^{32} x^{32} = x^{64}$ ←

$100 = 64 + 36$

$= 64 + 32 + 4$

$x^{100} = x^{64} x^{32} x^4$

Cost is 8 multiplications

$x \cdot x = x^2$

$x^2 \cdot x^2 = x^4$

$\vdots$

$x^{2^{k-1}} \; x^{2^{k-1}} = x^{2^k}$

$2^k \simeq n$

$k \simeq \log_2 n = \frac{\ln(n)}{\ln(2)}$

If $n = 10^{200}$ then $k \simeq \log_2 10^{200}$

$= 200 \log_2 10$

≤ 800

worse case: cost $\simeq 2 \log_2 n$

$x^{100} = x^{64}\, x^{32}\, x^4$

$x \cdot x = x^2$

$x^2\, x^2 = x^4$ ←

$x^4\, x^4 = x^8$

$x^8\, x^8 = x^{16}$

$x^{16}\, x^{16} = x^{32}$ ←

$x^{32}\, x^{32} = x^{64}$ ←

$(x, 1)$

$(x^2, 1)$

(x^4, x^4)

(x^8, x^4)

(x^{16}, x^4)

(x^{32}, x^{36})

(x^{64}, x^{100})

Only ever store 2 items

Horner's Algorithm

$$f(x) = 7x^4 - 13x^3 + 11x^2 - 8x + 12$$

$$f(2) = 7 \cdot 2^4 - 13 \cdot 2^3 + 11 \cdot 2^2 - 8 \cdot 2 + 12$$

$\#\text{mult} = 10$ $\quad$ $\#\text{add} = 4$

$$f(x) = a_d x^d + a_{d-1} x^{d-1} + \cdots + a_0$$

$\#\text{mult}$ is $d + \cdots + 1 + 0 = \dfrac{d(d+1)}{2} \sim d^2$

$\#\text{add}$ is d

addition is cheap

two d-digit #s, on the order of d operations

mult is expensive

two d-digit #s, on order of d^2

$$f(x) = 7x^4 - 13x^3 + 11x^2 - 8x + 12$$

$$((7x - 13)x + 11)x - 8)x + 12$$

$-13x^3$

$7x^4$

Cost is 4 mult (or d in general)

Naively poly of deg d costs $\sim d^2$ mult

↳ using Horner costs $\sim d$ mult

↳ if poly is special of the form x^d, costs $\sim 2 \log_2 d$ mult

often can do better in special cases

Chapter 3: Rings — Part 1

Generalizing integers: two operations….

square matrices

$A, B \longrightarrow A + B$

$A, B \longrightarrow A \cdot B$ if square

$M_{n\times n}(\mathbb{R}) = \{ n\times n \text{ matrices with real entries} \}$

if $n = 1$ get real numbers

Definition 3.1. A *ring* R is a set with two operations, generally called *addition* and *multiplication* and written

$$\underbrace{a+b}_{\text{addition}} \quad \text{and} \quad \underbrace{a\cdot b \text{ or } ab}_{\text{multiplication}},$$

satisfying the following axioms:

(1) The set R with its addition law $+$ is an abelian group. The identity element of this group is denoted 0 or 0_R.

(2) The set R with its multiplication law $\cdot$ is almost a group, but its elements are not required to have inverses.[2] Explicitly, the multiplication law of a ring has the following properties:

- There is an element $1_R \in R$ satisfying[3,4]

$$1_R \cdot a = a \cdot 1_R = a \quad \text{for all } a \in R.$$

  As with 0_R versus 0, if there is no ambiguity we often write 1 instead of 1_R.
- The associative law holds,

$$a\cdot(b\cdot c) = (a\cdot b)\cdot c \quad \text{for all } a,b,c \in R.$$

(3) [Distributive Law] For all $a,b,c \in R$ we have

$$a\cdot(b+c) = a\cdot b + a\cdot c \quad \text{and} \quad (b+c)\cdot a = b\cdot a + c\cdot a.$$

(4) [Optional Feature: Commutative Law] If further $a\cdot b = b\cdot a$ for all $a,b \in R$, then the ring is said to be *commutative*.

a+b = b+a Set

a·b not nec b·a

under multiplication:

(1) identity

(2) assoc

(3) closure

Proposition 3.2. *Let R be a ring.*

(a) $0_R \cdot a = 0_R$ *for all* $a \in R$.

(b) $(-a) \cdot (-b) = a \cdot b$ *for all* $a, b \in R$. *In particular, we have* $(-1_R) \cdot a = -a$.

0_R is the additive identity

additive inverse of a

Proof. (a) We start with $1_R = 1_R + 0_R$, which is true because 0_R is the identity for addition. We multiply both sides by a and compute

$$\begin{aligned} a &= a \cdot 1_R && \text{since } 1_R \text{ is the identity for multiplication,} \\ &= a \cdot (1_R + 0_R) && \text{since } 0_R \text{ is the identity for addition,} \\ &= a \cdot 1_R + a \cdot 0_R && \text{distributive law,} \\ &= a + a \cdot 0_R && \text{since } 1_R \text{ is the identity for multiplication.} \end{aligned}$$

$a = a$

$a \cdot 1 = a \cdot (1+0)$

We now "subtract" a from both sides. But this one time we will spell out every detail so that you can see how the different ring axioms come into play:

$$\begin{aligned} 0_R &= (-a) + a && \text{definition of inverse for addition,} \\ &= (-a) + (a + a \cdot 0_R) && \text{from our earlier calculation,} \\ &= \big((-a) + a\big) + a \cdot 0_R && \text{associativity of addition,} \\ &= 0_R + a \cdot 0_R && \text{definition of inverse for addition,} \\ &= a \cdot 0_R && \text{since } 0_R \text{ is the identity for addition.} \end{aligned}$$

Proposition 3.2. *Let R be a ring.*

(a) $0_R \cdot a = 0_R$ *for all* $a \in R$.

(b) $(-a) \cdot (-b) = a \cdot b$ *for all* $a, b \in R$. *In particular, we have* $(-1_R) \cdot a = -a$.

Try to do (b)

Maybe do $(-a)b = -(ab)$ } first

and $a(-b) = -(ab)$ }

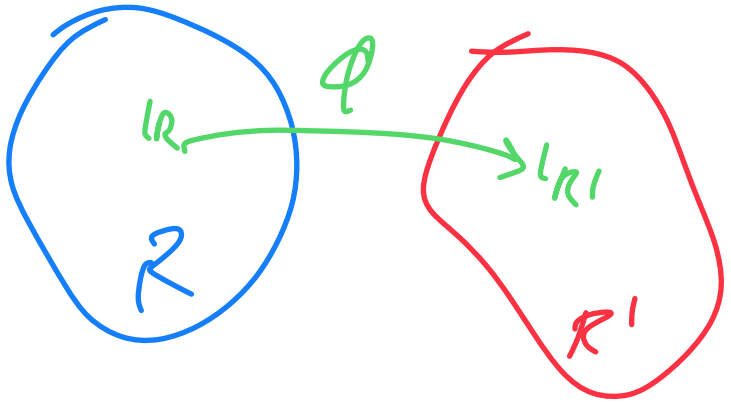
Maybe prove useful results:

$$-(-a) = a$$

Think $\tan(\arctan x) = x$

Definition 3.3. Let R and R' be rings. A *ring homomorphism from R to R'* is a function $\phi : R \to R'$ satisfying[5]

$$\begin{aligned} \phi(1_R) &= 1_{R'}, \\ \phi(a+b) &= \phi(a) + \phi(b) \quad \text{for all } a, b \in R, \\ \phi(a \cdot b) &= \phi(a) \cdot \phi(b) \quad \text{for all } a, b \in R. \end{aligned}$$



The *kernel of* ϕ is the set of elements that are sent to $0_{R'}$

$$\ker(\phi) = \{a \in R : \phi(a) = 0_{R'}\}.$$

As with groups, we say that R and R' are *isomorphic* if there is a bijective homomorphism $\phi : R \to R'$, and we call such a map ϕ an *isomorphism*.

Note $\ker(\phi) \subset R$, is $\ker(\phi)$ a subring?

define the ring $\mathbb{Z}/m\mathbb{Z}$ to be the set of congruence classes.

$m=12$:

$a+12\mathbb{Z} = \{x = a+12k \text{ for some integer } k\}$

$\mathbb{Z}/12\mathbb{Z}$ as $\{0+12\mathbb{Z}, 1+12\mathbb{Z}, \ldots, 11+12\mathbb{Z}\}$

$(7+12\mathbb{Z}) + (9+12\mathbb{Z}) = 16+12\mathbb{Z}$ or $4+12\mathbb{Z}$

$\hookrightarrow 16+12\mathbb{Z} = \{16+12k : k \text{ integer}\} = \{\ldots, -8, 4, 16, 28, \ldots\}$

$4+12\mathbb{Z} = \{4+12l : l \text{ integer}\} = \{\ldots -8, 4, 16, 28, \ldots\}$

$f : (16+12\mathbb{Z}) \to (4+12\mathbb{Z})$

$f(x) = x-12$

Both $4+12\mathbb{Z}$ and $16+12\mathbb{Z}$ same often use $4+12\mathbb{Z}$

$(7+12\mathbb{Z}) \cdot (9+12\mathbb{Z}) = (63+12\mathbb{Z}) = 3+12\mathbb{Z}$

$(7+12k)\,(9+12l) = 7\cdot 9 + 7\cdot 12l + 12k\cdot 9 + 12k\cdot 12l$

$= 63 + 12(7l + k9 + k\cdot 12l)$

$= 3 + 12\cdot 5 + 12(7l + k9 + k\cdot 12l)$

$= 3 + 12(5 + 7l + k9 + k\cdot 12l)$

$\mathbb{Z}/12\mathbb{Z} = \{0+12\mathbb{Z}, 1+12\mathbb{Z}, \ldots, 11+12\mathbb{Z}\} = R$

- additive identity: $0+12\mathbb{Z}$
- mult identity: $1+12\mathbb{Z}$

Issues in mult inverse: $a+12\mathbb{Z}$ if $\gcd(a,12) > 1$

$(4+12\mathbb{Z})(x+12\mathbb{Z}) = 1+12\mathbb{Z}$

$4x+12\mathbb{Z} = 1+12\mathbb{Z}$

need to find integer k such that $4x+12k = 1+12l$

for some l, need $1 = 4x+12k-12l = 4(x+3k-3l)$

Impossible: RHS is mult of 4

Example 3.5 (Gaussian Integers: $\mathbb{Z}[i]$). Here is another interesting subring of $\mathbb{C}$. It is called the *ring of Gaussian integers* and consists of the set

$$\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}.$$

$i = \sqrt{-1}$

$i^2 = -1$

$(a+bi)+(c+di) = (a+c) + (b+d)i$

$(a+bi)(c+di) = ac + bci + adi + bidi$

$= ac + bci + adi - bd$

$= (ac - bd) + (bc + ad)i$

additive identity is $0 + 0i$

mult identity is $1 + 0i$

$(a+bi)(c+di) = 1$

$|z|^2 = z \cdot \bar{z} = x^2 + y^2$

if $z = x+iy$

$|zw|^2 = |z|^2 |w|^2$

$|a+bi|^2 \; |c+di|^2 = 1$ $\quad a, b, c, d$ integers

$|a^2+b^2| \; |c^2+d^2| = 1$

$1 \qquad 1$

$a^2+b^2 = 1$ to have a chance at being invertible

e.g. $1, -1, i, -i$

Example 3.6 (Polynomial Rings: $R[x]$). Polynomials provide a method for creating bigger (and better?) rings from rings that we already know. Thus given any commutative ring R, we can use R to build the *ring of polynomials over* R,

$$R[x] = \left\{ \begin{array}{l} \text{polynomials } a_0 + a_1 x + a_2 x^2 + \cdots + a_d x^d \text{ of all} \\ \text{possible degrees with coefficients } a_0, a_1, \ldots, a_d \in R \end{array} \right\}.$$

polynomials of finite deg, as (deg d) * (deg d) = deg 2d

$$E_c : R[x] \longrightarrow R, \quad E_c(f) = f(c).$$

The evaluation map E_c is a ring homomorphism,[6] as you will verify in Exercise 3.8, and its kernel is exactly the set of polynomials that have a factor of $x - c$.

In RSA : secret primes P, Q, e

public $N = PQ$ and d with $ed \equiv 1 \bmod (P-1)(Q-1)$

Message M: send $M^e \bmod N$,

decrypt by doing $(M^e \bmod N)^d \bmod N$

Show $(M \bmod N)(M \bmod N) = M^2 \bmod N$

Math 310: Modern Algebra: Fall '25 (Siena)

Professor Steven J Miller: sjm1@williams.edu

Homepage:
https://web.williams.edu/Mathematics/sjmiller/public_html/310Fa25/

Ring Theory Lecture

Lecture 11: 10/7/25: No class, work on exam

Lecture 12: 10/9/25: https://youtu.be/DyCgWgCD3tg

Chapter Three: More Rings: Examples, Properties

Definition 3.1. A *ring* R is a set with two operations, generally called *addition* and *multiplication* and written

$$\underbrace{a+b}_{\text{addition}} \quad \text{and} \quad \underbrace{a\cdot b \text{ or } ab}_{\text{multiplication}},$$

satisfying the following axioms:

(1) The set R with its addition law $+$ is an abelian group. The identity element of this group is denoted 0 or 0_R.

(2) The set R with its multiplication law $\cdot$ is almost a group, but its elements are not required to have inverses.[2] Explicitly, the multiplication law of a ring has the following properties:

- There is an element $1_R \in R$ satisfying[3,4]

$$1_R \cdot a = a \cdot 1_R = a \quad \text{for all } a \in R.$$

  As with 0_R versus 0, if there is no ambiguity we often write 1 instead of 1_R.
- The associative law holds,

$$a\cdot(b\cdot c) = (a\cdot b)\cdot c \quad \text{for all } a,b,c \in R.$$

(3) [Distributive Law] For all $a,b,c \in R$ we have

$$a\cdot(b+c) = a\cdot b + a\cdot c \quad \text{and} \quad (b+c)\cdot a = b\cdot a + c\cdot a.$$

(4) [Optional Feature: Commutative Law] If further $a\cdot b = b\cdot a$ for all $a,b \in R$, then the ring is said to be *commutative*.

a+b = b+a Set

a·b not nec b·a

under multiplication:

(1) identity

(2) assoc

(3) closure

What properties from integers hold in rings?

Unique Factorization:

If n is a pos integer, $\exists!$ representation $n = p_1^{r_1} \cdots p_k^{r_k}$ where the p_i's are prime and $p_1 < p_2 < \cdots < p_k$.

Example of a ring: let X be a non-rational complex number. Consider $S_X = \{a + bX : a, b \in \mathbb{Z}\}$.

Is this a ring?

↳ if not, for what X is it a ring?

Consider $S'_\pi = \{a + b\pi : a, b \in \mathbb{Z}\}$

Addition: $0 = 0 + 0\pi$

$(a + b\pi) + (\tilde{a} + \tilde{b}\pi) = (a + \tilde{a}) + (b + \tilde{b})\pi$ ✓

int int

leave the rest of addition for you

Mult: $1 = 1 + 0\pi$

Closure: $(a + b\pi)(c + d\pi) \stackrel{?}{=} (e + f\pi)$?

$x^3 = 1$

$(a + 0\pi)(c + 0\pi) = e + f\pi$ $\Big[e = ac,\ f = 0$

$(0 + \pi)(0 + \pi) = \pi^2 = e + f\pi$

Any $\pi^2 - f\pi - e = 0 \to \pi = \dfrac{f \pm \sqrt{f^2 + 4e}}{2}$

$x^3 = 1 \Rightarrow x^3 - 1 = 0$

$(x-1)(x^2+x+1)$

$x = 1$ or $x = \frac{-1 \pm \sqrt{1-4}}{2}$

or $\frac{-1 \pm \sqrt{-3}}{2}$

$x^3 + x^2 + x$

$-x^2 - x - 1$

$x^3 - 1$

$x^3 = 2$ one root is $2^{1/3}$ or $\sqrt[3]{2}$

Study $S_x = \{a+bx : a,b \in \mathbb{Z}\}$ for $x = \sqrt{n}$, n not square

Addition: Ring properties hold

Mult: $1 = 1+0x$

Assoc free as these are complex numbers

Closure: $(a+bx)(c+dx)$

$= ac + bcx + adx + bdx^2$

$= (\underbrace{ac+bdn}_{\text{int}}) + (\underbrace{bc+ad}_{\text{int}})x$ closed!

$S_{-5} = \{a + b\sqrt{-5}\}$

$\sqrt{-5} = i\sqrt{5}$

$z = a + b\sqrt{-5} \qquad \bar{z} = a - b\sqrt{-5}$

$2 \cdot 3 = 6 = (1 + \sqrt{-5})(1 - \sqrt{-5})$

$2(a + b\sqrt{-5}) = 1 + \sqrt{-5}$

$2a + 2b\sqrt{-5} = 1 + \sqrt{-5}$

impossible

$(1 + \sqrt{-5})(a + b\sqrt{-5}) = 2$

$(a - 5b) + (a + 5)\sqrt{-5} = 2$

$a + 5a$

$6a = 2$

impossible

0

so $a = -5$

If $x = \sqrt[3]{2}$ then $S_x = \{a + b\sqrt[3]{2}\}$ not a ring

$$S_{\sqrt[3]{2}} = \{a_1 + b_1\sqrt[3]{2} + c_1(\sqrt[3]{2})^2 : a, b, c \in \mathbb{Z}\}$$

$\sqrt[3]{2}$ $\sqrt[3]{2}$

$$\left[a_1 + b_1\sqrt[3]{2} + c_1(\sqrt[3]{2})^2\right]\left[a_2 + b_2\sqrt[3]{2} + c_2(\sqrt[3]{2})^2\right]$$

This is a ring!

Ex: if α solves a poly of deg n with integer coeff and no lower degree poly, then

$$R_\alpha = \{a_1 + a_2\alpha + a_3\alpha^2 + \cdots + a_{n-1}\alpha^{n-1} : a_k \in \mathbb{Z}\}$$ is a ring

Example 3.9 (Homomorphism from $\mathbb{Z}$). For every ring R, there is a unique homomorphism

$$\phi : \mathbb{Z} \longrightarrow R.$$

$\phi(1) = 1_R$, $\phi(0) = 0_R$: By defn of a ring homomorphism

$\varphi(a+b) = \varphi(a) + \varphi(b)$
$\varphi(ab) = \varphi(a)\varphi(b)$

$\varphi(2) = \varphi(1+1) = \varphi(1) + \varphi(1) = 1_R + 1_R = 2 \cdot 1_R$

$\varphi(3) = \varphi(2+1) = \varphi(2) + \varphi(1) = 2 \cdot 1_R + 1_R = 3 \cdot 1_R$

By induction: $\varphi(n) = n \cdot 1_R$ if n is a pos integer.

$\varphi(0) = \varphi(1 + (-1)) = \varphi(1) + \varphi(-1) = 0_R \Rightarrow \varphi(-1) = -\varphi(1)$

or $\varphi(-1) = -1_R$

$$\varphi(-2) = \varphi((-1)+(-1)) = \varphi(-1)+\varphi(-1) = -1_R + -1_R = -2_R$$

$$\varphi(-2) = \varphi((-1)*2) = \varphi(-1)*\varphi(2)$$

$$= -1_R * 2\cdot 1_R$$

$$= -2 1_R$$

$$\varphi(-n) = \varphi((-1)n) = \varphi(-1)\varphi(n) = -1_R * n\,1_R = -n\,1_R$$

Explore $\varphi: \mathbb{Q} \to R$: freedom?

Definition 3.10. A *field* is a commutative ring R with the property that every non-zero element of R has a multiplicative inverse. In other words, for every $a \in R$ with $a \neq 0$ there is a $b \in R$ satisfying $ab = 1$.

Only one time 0 is invertible: $R = \{0\}$

Often want $0_R \neq 1_R$

Not all rings are fields: $\mathbb{Z}$, $\mathbb{Z}/12\mathbb{Z}$ fail

Rings that are a field: $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$

Is $\mathbb{Z}_{\sqrt{-5}} = \{a + b\sqrt{-5} : a, b \in \mathbb{Z}\}$ a field?

$(a+b\sqrt{-5})(c+d\sqrt{-5}) = 1$ try $a=0, b=1$

$(\sqrt{-5})(c+d\sqrt{-5}) = 1$

$\Rightarrow c\sqrt{-5} - 5d = 1 \Rightarrow d = -\frac{1}{5}$ impossible

$c = 0$

or $c\sqrt{-5} = 1+5d$

or $\sqrt{-5} = \frac{1+5d}{c} \in \mathbb{Q}$ false

Consider $\{a+b\sqrt{-5} : a,b \in \mathbb{Q}\}$: field?

Is a ring:

$(a+b\sqrt{-5})(c+d\sqrt{-5}) = 1$

$(ac-5bd) + (bc+ad)\sqrt{-5} = 1$

$ac-5bd$: 1

$bc+ad$: 0

so $ac-5bd = 1$

$bc+ad = 0$

a, b given

c, d free

$ac - 5bd = 1$

$bc + ad = 0$

$$\begin{pmatrix} a & -5b \\ b & a \end{pmatrix} \begin{pmatrix} c \\ d \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

$A\vec{x} = \vec{b}$

$\vec{x} = A^{-1}\vec{b}$

so $\begin{pmatrix} c \\ d \end{pmatrix} = \begin{pmatrix} a & -5b \\ b & a \end{pmatrix}^{-1} \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ entries are rational

det is $a^2 + 5b^2$ and is 0 only if $a = b = 0$

which gives $0 + 0\sqrt{-5} = 0$

Definition 3.13. Let R be a commutative ring. An element $a \in R$ is called a *zero divisor* if $a \neq 0$ and there is some non-zero $b \in R$ such that $ab = 0$. The ring R is an *integral domain* if it has no zero divisors. Equivalently, the ring R is an integral domain if the only way to get $ab = 0$ is to have either $a = 0$ or $b = 0$.

Example of a non-integral ring: has zero divisors

$(\mathbb{Z}/12\mathbb{Z})$: $3 \cdot 4 \equiv 0 \bmod 12$

$(\mathbb{Z}/n\mathbb{Z})$ if n is composite

Hope: $(\mathbb{Z}/p\mathbb{Z})$ is an integral ring if p prime

Proposition 3.15 (Cancellation Property for Integral Domains). *A commutative ring R is said to have the* cancellation property *if for every choice of $a, b, c \in R$, the following implication is true:*

$$ab = ac \iff b = c \text{ or } a = 0.$$

A commutative ring has the cancellation property if and only if it is an integral domain.

Prove cancellation → integral domain

integral domain → cancellation

Fun Fact: $\sin^2 x = \sin x \cdot \sin x$

$= (1 - \cos x)(1 + \cos x)$

Math 355: Modern Algebra: Fall '25 (Siena)

Professor Steven J Miller: sjm1@williams.edu

Homepage:
https://web.williams.edu/Mathematics/sjmiller/public_html/310Fa25/

Ring Theory Lecture

Lecture 13: 10/14/25: https://youtu.be/_klYSaw-DWM

Chapter Three: RSA (Applications of Group Theory), Math Missed

Alice always sends to Bob, Charlie or Eve tries to intercept.

Bob does the following (could have b subscripts):

- Secret: $p = 15217$, $q = 17569$, $d = 80998505$.
- Public: $N = pq = 267347473$, $e = 3141593$.
- Note: $ed = 1 \bmod (p-1)(q-1)$.
- **Message:** $M = 195632041$, **send** $M^e \bmod N$ **or** $X = 121209473$.
- Decrypt: $X^d \bmod N$ or 195632041.

A lot of implementation issues.

- How do we find large primes? How large is large?
- How do we find e and d so that $ed = 1 \bmod (p-1)(q-1)$?
- How do we compute $M^e \bmod N$ efficiently? Fast Exponentiation
- Can Eve determine d from e and N? ?

How do we find e and d so that $ed = 1 \bmod (p-1)(q-1)$?

$\varphi(pq)$

Imagine d and $\varphi(pq)$ rel prime.

Euclidean algorithm: $\exists a, b$ st $ad + b\varphi(pq) = 1$

Thus $ad \equiv 1 \bmod \varphi(pq)$

So take $e = a$ we win!

Fast by Euclidean Alg

If $\gcd(d, \varphi(pq)) > 1$ choose a new d

↳ keep going till get a gcd of 1.

Extra Credit: Prove doesn't take too long.

If $(p-1)(q-1)$ has a lot of prime factors, easier for gcd to be >1

Best Case: $p-1, q-1$ prime (p, q big primes)

Best Reasonable Hope: $\frac{p-1}{2}, \frac{q-1}{2}$ prime

$p=7$: $\frac{p-1}{2}=3$, $p=11$: $\frac{11-1}{2}=5$

Sophie Germain Primes

Always True.

$p=13$: $\frac{13-1}{2}=6$ ~~FALSE~~

Are there infinitely many primes? How many up to x?

Euclid and Growth Rate

Assume only finitely many: $p_1, p_2, p_3, \ldots, p_n$

Consider $x = p_1 \cdot p_2 \cdots p_n + 1$ (Ex. $x = 2 \cdot 3 \cdot 5 + 1) = 31$

Case 1: x is prime

as $x > p_1, p_2, \ldots, p_n$,
it is a new prime
not on the list,
contradiction.

Case 2: x is not prime

$x > 1$, not prime $\Rightarrow$ composite
so $\exists p$ dividing x
$p \neq p_1, p_2, \ldots, p_n$ as
remainder is 1: Thus
found a new prime!

Exercise: implies # primes at most x is at least a constant times $\log_2(\log_2 x)$.

Truth is about $\frac{x}{\log(x)}$.

$\#\{n \le x \text{ such that } n = m^2\} \sim \sqrt{x}$

$\#\{n \le x \text{ such that } n = m^3\} \sim \sqrt[3]{x}$

$\#\{n \le x \text{ such that } n = m^k \text{ for some } k \ge 2\} \sim \sqrt{x}$

$X := p_1 p_2 \cdots p_n + 1$

$n = 1$ $\quad 2$ $\quad$ so $X = 2+1 \Longrightarrow 3$ $\quad$ prime

$n = 2$ $\quad 2, 3$ $\quad$ so $X = 2 \cdot 3 + 1 \Rightarrow 7$ $\quad$ prime

$n = 3$ $\quad 2, 3, 7$ so $X = 2 \cdot 3 \cdot 7 + 1 \Rightarrow 43$ $\quad$ prime

Question: Is it always prime?

$n = 4$: $2, 3, 7, 43$: $X = 2 \cdot 3 \cdot 7 \cdot 43 + 1 = 42 \cdot 43 + 1$

$= 1807$

Composite

Salvage: $X_n = p_1 p_2 \cdots p_n + 1$: prime

$X_3 = 2 \cdot 3 \cdot 5 + 1 = 31$ prime, $X_4 = 2 \cdot 3 \cdot 5 \cdot 7 + 1 = 211$ prime ...
Fails at 13

Are there infinitely many primes? How many up to x?

Fermat Primes and Growth Rate

Fermat numbers: $F_n = 2^{2^n} + 1$: Are these prime? always? If not, how often?

Consider $x^{2n+1} + 1 = 0$: root $x = -1$

$$(x+1)(x^{2n} - x^{2n-1} - x^{2n-2} - \cdots - x + 1) = 0$$

If $x = 2$, the $2^{2n+1} + 1$ is never prime

only chance to be prime is exponent is a power of 2

$$F_n = 2^{2^n} + 1$$

$F_n = 2^{2^n} + 1$

$n = 0 \quad F_0 = 3$

$n = 1 \quad F_1 = 5$

$n = 2 \quad F_2 = 17$

$n = 3 \quad F_3 = 257$

$n = 4 \quad F_4 = 65537$

} Prime!

$$F_{m+1} = F_0 F_1 \cdots F_m + 2$$

↳ induction

↳ brute force: use $F_n = 2^{2^n} + 1$

$\gcd(F_{m+1}, F_k) = 1 \text{ or } 2$ for $k \leq m$

But F_n is always odd so gcd is 1.

As relatively prime, each number gives a new prime not previously seen.

Write this up rigorously

$F_n = 2^{2^{m+k}} + 1$

$F_m = 2^{2^m} + 1$

$F_n = 2^{2^{m+k} - 2^m}$ F_m has same gcd as gcd of old

$= 2^{2^{m+k}} + 1 - 2^{2^{m+k}} - 2^{2^{m+k} - 2^m}$

$= -\left(2^{2^{m+k}} - 2^m - 1\right)$

$= -\left(2^{2^m(2^k - 1)} - 1\right)$

gcd same as $2^{2^m(2^{k-1})} - 1$ and $2^{2^m} + 1$

$\left[2^{2^m(2^{k-1})} + 1\right] - 2^{2^m(2^k - 2)}\left[2^{2^m} + 1\right]$

all at negative

$2^{2^m(2^k - 2)} + 1$ and $2^{2^m} + 1$

$\left[2^{2^m(2^{k-2})} + 1\right] - 2^{2^m(2^k - 3)}\left[2^{2^m} + 1\right]$

all at negative

$2^{2^m(2^k - 3)} - 1$

⋮

$2^{2^m(2^k - 2^k)} \pm 1$ So is 1.

Note
This
rigorous!

Are there infinitely many primes? How many up to x?

Special value proofs and ζ(s) and Growth Rates

$$\zeta(s) := \sum_{n=1}^{\infty} \frac{1}{n^s} \qquad \mathrm{Re}(s) > 1$$

$$= \prod_{p \text{ prime}} \left(1 - \frac{1}{p^s}\right)^{-1}$$

(Euler Product)

Geometric Series Formula + Fundamental Theorem of Arithmetic

$$\zeta(s) = \sum_{n=1}^{\infty} 1/n^s = \prod_{p \text{ prime}} (1 - 1/p^s)^{-1} \qquad \mathrm{Re}(s) > 1$$

- $\lim_{s \to 1^+} \zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n}$ diverges

$\Rightarrow$ must be as many primes as otherwise product converges.

Harmonic Series Diverges

- $1 + \frac{1}{2} + \underbrace{\left(\frac{1}{3} + \frac{1}{4}\right)} + \underbrace{\left(\frac{1}{5} + \frac{1}{6} + \frac{1}{7} + \frac{1}{8}\right)} + \underbrace{\left(\frac{1}{9} + \cdots + \frac{1}{16}\right)} + \cdots$

$$\geq 2 \cdot \frac{1}{4} \qquad \geq 4 \cdot \frac{1}{8} \qquad \geq 8 \cdot \frac{1}{16}$$

$$\geq 1 + \frac{1}{2} + \frac{1}{2} + \frac{1}{2} + \frac{1}{2} + \cdots$$

- $H = \text{Heart} + \text{Hold}$

$H = \sum 1/n \quad H_{even} = \sum_{n\,even} 1/n \quad H_{odd} = \sum_{n\,odd} 1/n$

assume sum converges!

$H = H_{even} + H_{odd}$

$H_{odd}: \; 1 + \frac{1}{3} + \frac{1}{5} + \cdots$

$H_{even}: \; \frac{1}{2} + \frac{1}{4} + \frac{1}{6} + \cdots$ so $H_{odd} > H_{even}$

Claim $H_{even} = \frac{1}{2} H$, $H_{even} = \frac{1}{2\cdot 1} + \frac{1}{2\cdot 2} + \frac{1}{2\cdot 3} + \frac{1}{2\cdot 4} + \cdots$

$H = \frac{1}{2} H + H_{odd} \Rightarrow \frac{1}{2} H = H_{odd}$

or $H = H_{odd} + H_{odd} > H_{odd} + H_{even} = H$

Integral Test

$$1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n} \approx \int_1^n \frac{1}{t}\,dt$$

$$= \ln(n) - \ln(1)$$

$$= \ln(n)$$

$$\zeta(2) = \underbrace{\sum_{n=1}^{\infty} \frac{1}{n^2}}_{} = \prod_p \left(1 - 1/p^2\right)^{-1}$$

$$\frac{\pi^2}{6} \notin \mathbb{Q}$$

If only finitely many primes

Then $\prod_p \left(1 - 1/p^2\right)^{-1} \in \mathbb{Q}$

$\Rightarrow \pi^2 \in \mathbb{Q}$, contradiction.

Irrationality measure and lower bounds for π(x) (with David Burt, Sam Donow, Matthew Schiffman and Ben Wieland), The Pi Mu Epsilon Journal **(14** (2017), no. 7, 421-429**)** pdf
https://web.williams.edu/Mathematics/sjmiller/public_html/math/papers/LowerBoundCardPrimes50.pdf

Showed $\#\{\text{primes} \le x\}$ is at least $\log\log\log x$

- Euclid gives $\log\log x$
- Tchebyshev is $x/\log x$
- My proof used irrationality measure bounds on π^2, which used the Prime Number Theorem that $\#\{p \le x\} \sim \frac{x}{\log x}$.

Euclid-Mullin Sequence: https://oeis.org/A000945

A000945 Euclid-Mullin sequence: a(1) = 2, a(n+1) is smallest prime factor of 1 + Product_{k=1..n} a(k). 101
(Formerly M0863 N0329)

2, 3, 7, 43, 13, 53, 5, 6221671, 38709183810571, 139, 2801, 11, 17, 5471, 52662739, 23003, 30693651606209, 37, 1741, 1313797957, 887, 71, 7127, 109, 23, 97, 159227, 643679794963466223081509857, 103, 1079990819, 9539, 3143065813, 29, 3847, 89, 19, 577, 223, 139703, 457, 9649, 61, 4357

(list; graph; refs; listen; history; text; internal format)

OFFSET 1,1

COMMENTS "Does the sequence ... contain every prime? ... [It] was considered by Guy and Nowakowski and later by Shanks, [Wagstaff 1993] computed the sequence through the 43rd term. The computational problem inherent in continuing the sequence further is the enormous size of the numbers that must be factored. Already the number a(1)* ... *a(43) + 1 has 180 digits." - Crandall and Pomerance

If this variant of Euclid-Mullin sequence is initiated either with 3, 7 or 43 instead of 2, then from a(5) onwards it is unchanged. See also A051614. - Labos Elemer, May 03 2004

Wilfrid Keller informed me that a(1)* ... *a(43) + 1 was factored as the product of two primes on Mar 09 2010 by the GNFS method. See the post in the Mersenne Forum for more details. The smaller 68-digit prime is a(44). Terms a(45)-a(47) were easy to find. Finding a(48) will require the factorization of a 256-digit number. See the b-file for the four new terms. - T. D. Noe, Oct 15 2010

On Sep 11 2012, Ryan Propper factored the 256-digit number by finding a 75-digit factor by using ECM. Finding a(52) will require the factorization of a 335-digit number. See the b-file for the terms a(48) to a(51). - V. Raman, Sep 17 2012

Needs longer b-file. - N. J. A. Sloane, Dec 18 2015

A056756 gives the position of the k-th prime in this sequence for each k. - Jianing Song, May 07 2021

Named after the Greek mathematician Euclid (flourished c. 300 B.C.) and the American engineer and mathematician Albert Alkins Mullin (1933-2017). - Amiram Eldar, Jun 11 2021

In Ribenboim 2004, a wrong value of a(8) is given, 6221271 instead of 6221671. - Stefano Spezia, Mar 27 2025

REFERENCES

Richard Crandall and Carl Pomerance, Prime Numbers: A Computational Perspective, Springer, NY, 2001; see p. 6.

Richard Guy and Richard Nowakowski, Discovering primes with Euclid, Delta (Waukesha), Vol. 5, pp. 49-63, 1975.

Paulo Ribenboim, The Little Book of Bigger Primes, Springer-Verlag NY 2004. See p. 5.

N. J. A. Sloane, A Handbook of Integer Sequences, Academic Press, 1973 (includes this sequence).

N. J. A. Sloane and Simon Plouffe, The Encyclopedia of Integer Sequences, Academic Press, 1995 (includes this sequence).

Samuel S. Wagstaff, Jr., Computing Euclid's primes, Bull. Institute Combin. Applications, Vol. 8 (1993), pp. 23-32.

LINKS

Ryan Propper, Table of n, a(n) for n = 1..51 (first 47 terms from T. D. Noe)

Andrew R. Booker, On Mullin's second sequence of primes, Integers, Vol. 12, No. 6 (2012), pp. 1167-1177; arXiv preprint, arXiv:1107.3318 [math.NT], 2011-2013.

Andrew R. Booker, A variant of the Euclid-Mullin sequence containing every prime, arXiv preprint arXiv:1605.08929 [math.NT], 2016.

How do we find large primes? How large is large?

Using Fermat's Little Theorem:

If p is prime and $\gcd(a,p)=1$ Then

$$a^{p-1} \equiv 1 \bmod p.$$

More generally: if $\gcd(a,n)=1$ Then $a^{\varphi(n)} \equiv 1 \bmod n$

So if $\gcd(a,n)=1$ and $a^{n-1} \not\equiv 1 \bmod n$, n not prime.

Proved 6 composite: $5^{6-1} \equiv 5 \not\equiv 1 \bmod 6$, 6 Composite

Pythagorean triples

(a, b, c) with $a^2 + b^2 = c^2$

$(3, 4, 5)$, $(6, 8, 10)$, $(12, 16, 20)$, $(15, 20, 25)$, ...

$(a/c, b/c)$ with $(a/c)^2 + (b/c)^2 = 1$

$f_c(x) = x + c \bmod 26$

$$f_{c_{100}}\left(\cdots\left(f_{c_2}\left(f_{c_1}(x)\right)\right)\right) = f_{c_1 + \cdots + c_{100} \bmod 26}(x)$$

https://en.wikipedia.org/wiki/Carmichael_number

In number theory, a **Carmichael number** is a composite number n which in modular arithmetic satisfies the congruence relation:

$$b^n \equiv b \pmod{n}$$

for all integers b.[1] The relation may also be expressed[2] in the form:

$$b^{n-1} \equiv 1 \pmod{n}$$

for all integers b that are relatively prime to n. They are infinite in number.[3]

They constitute the comparatively rare instances where the strict converse of Fermat's Little Theorem does not hold. This fact precludes the use of that theorem as an absolute test of primality.[4]

The Carmichael numbers form the subset K_1 of the Knödel numbers.

The Carmichael numbers were named after the American mathematician Robert Carmichael by Nicolaas Beeger, in 1950. Øystein Ore had referred to them in 1948 as numbers with the "Fermat property", or "*F* numbers" for short.[5]



Robert Daniel

Overview [edit]

The first seven Carmichael numbers, from 561 to 8911, were all found by the Czech mathematician Václav Šimerka in 1885[11] (thus preceding not just Carmichael but also Korselt, although Šimerka did not find anything like Korselt's criterion).[12] His work, published in Czech scientific journal *Časopis pro pěstování matematiky a fysiky*, however, remained unnoticed.

Korselt was the first who observed the basic properties of Carmichael numbers, but he did not give any examples.

That 561 is a Carmichael number can be seen with Korselt's criterion. Indeed, $561 = 3 \cdot 11 \cdot 17$ is square-free and $2 \mid 560$, $10 \mid 560$ and $16 \mid 560$. The next six Carmichael numbers are (sequence A002997 in the OEIS):

$$\begin{aligned}
1105 &= 5 \cdot 13 \cdot 17 && (4 \mid 1104; && 12 \mid 1104; && 16 \mid 1104)\\
1729 &= 7 \cdot 13 \cdot 19 && (6 \mid 1728; && 12 \mid 1728; && 18 \mid 1728)\\
2465 &= 5 \cdot 17 \cdot 29 && (4 \mid 2464; && 16 \mid 2464; && 28 \mid 2464)\\
2821 &= 7 \cdot 13 \cdot 31 && (6 \mid 2820; && 12 \mid 2820; && 30 \mid 2820)\\
6601 &= 7 \cdot 23 \cdot 41 && (6 \mid 6600; && 22 \mid 6600; && 40 \mid 6600)\\
8911 &= 7 \cdot 19 \cdot 67 && (6 \mid 8910; && 18 \mid 8910; && 66 \mid 8910).
\end{aligned}$$

In 1910, Carmichael himself[13] also published the smallest such number, 561, and the numbers were later named after him.



Václav Šimerka listed the first seven Carmichael numbers

Jack Chernick[14] proved a theorem in 1939 which can be used to construct a subset of Carmichael numbers. The number $(6k + 1)(12k + 1)(18k + 1)$ is a Carmichael number if its three factors are all prime. Whether this formula produces an infinite quantity of Carmichael numbers is an open question (though it is

Paul Erdős heuristically argued there should be infinitely many Carmichael numbers. In 1994 W. R. (Red) Alford, Andrew Granville and Carl Pomerance used a bound on Olson's constant to show that there really do exist infinitely many Carmichael numbers. Specifically, they showed that for sufficiently large n, there are at least $n^{2/7}$ Carmichael numbers between 1 and n.[3]

Thomas Wright proved that if a and m are relatively prime, then there are infinitely many Carmichael numbers in the arithmetic progression $a + k \cdot m$, where $k = 1, 2, \ldots$.[15]

Löh and Niebuhr in 1992 found some very large Carmichael numbers, including one with 1,101,518 factors and over 16 million digits. This has been improved to 10,333,229,505 prime factors and 295,486,761,787 digits,[16] so the largest known Carmichael number is much greater than the largest known prime.

https://annals.math.princeton.edu/wp-content/uploads/annals-v160-n2-p12.pdf

PRIMES is in P

By Manindra Agrawal, Neeraj Kayal, and Nitin Saxena*

Abstract

We present an unconditional deterministic polynomial-time algorithm that determines whether an input number is prime or composite.

4. The algorithm and its correctness

Input: integer $n > 1$.

1. If ($n = a^b$ for $a \in \mathcal{N}$ and $b > 1$), output COMPOSITE.
2. Find the smallest r such that $o_r(n) > \log^2 n$.
3. If $1 < (a, n) < n$ for some $a \leq r$, output COMPOSITE.
4. If $n \leq r$, output PRIME.[1]
5. For $a = 1$ to $\lfloor \sqrt{\phi(r)} \log n \rfloor$ do
   if $((X + a)^n \neq X^n + a \pmod{X^r - 1, n})$, output COMPOSITE;
6. Output PRIME.

$\mathcal{N}$ and $\mathcal{Z}$ denote the set of natural numbers and integers respectively. Given $r \in \mathcal{N}$, $a \in \mathcal{Z}$ with $(a,r) = 1$, the *order of a modulo r* is the smallest number k such that $a^k = 1 \pmod{r}$. It is denoted as $o_r(a)$. For $r \in \mathcal{N}$, $\phi(r)$ is *Euler's totient function* giving the number of numbers less than r that are relatively prime to r. It is easy to see that $o_r(a) \mid \phi(r)$ for any a, $(a,r) = 1$.

General Code

Consider an army with 10 generals. One wants a security system such that any three of them can determine the code to launch nuclear missiles, but no two of them can.

It is possible to devise such a system by using a quadratic polynomial, such as ax^2 + bx + c; to launch the missiles, one must input (a,b,c).

What information should be given to the generals so that any three can find (a,b,c) but no two can? What about the general situation with N generals and any M can launch (but no set of M-1) can?

Irrationality

Saw role irrationality played in when sets are rings.

How do we prove numbers are irrational?

- Rational irrational proofs (with David Montague), Mathematics Magazine **(85** (2012), no. 2, 110--114**).** pdf (expanded version: pdf; letter from Nerode and Tennenbaum on history of proof: pdf)

- Geometric Proofs of the Irrationality of Square-Roots for Select Integers (Zongyun Chen, Steven J. Miller and Chenghan Wu), to appear in the Fibonacci Quarterly. pdf

$\sqrt{2}$ Is Irrational

Standard Proof: Assume $\sqrt{2} = a/b$.

WLOG, assume b is the smallest denominator among all fractions that equal $\sqrt{2}$.

$2b^2 = a^2$ thus $a = 2m$ is even.

$a = (2k+1)$

$a^2 = (2k+1)(2k+1) =$

$4k^2 + 4k + 1$

$= 2(2k^2 + 2k) + 1$

odd

Then $2b^2 = 4m^2$ so $b^2 = 2m^2$ so $b = 2n$ is even.

Thus $\sqrt{2} = a/b = 2m/2n = m/n$, contradicts minimality of n.

(Could also do by contradiction from a, b relatively prime.)

Tennenbaum's Proof

Assume $\sqrt{2} = a/b$ with b minimal.

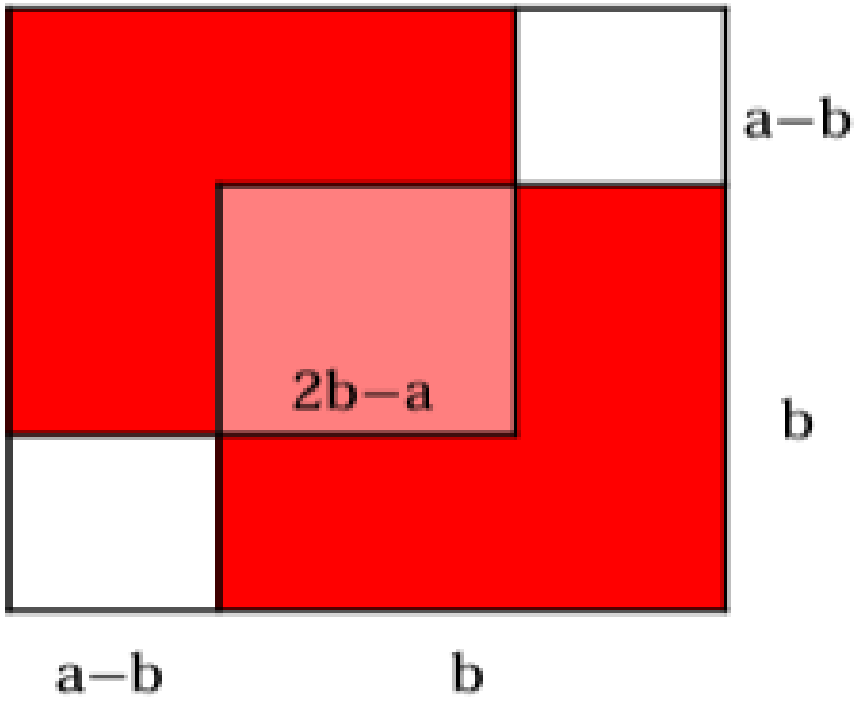


Figure: $2b^2 = a^2$ so $(2b-a)^2 = 2(a-b)^2$ and $\sqrt{2} = \frac{2b-a}{a-b}$.

As $0 < a - b < b$ (if not, $a - b \geq b$ so $a \geq 2b$ and $\sqrt{2} = a/b \geq 2$), contradicts minimality of b.

Assume $\sqrt{3} = a/b$ with b minimal.

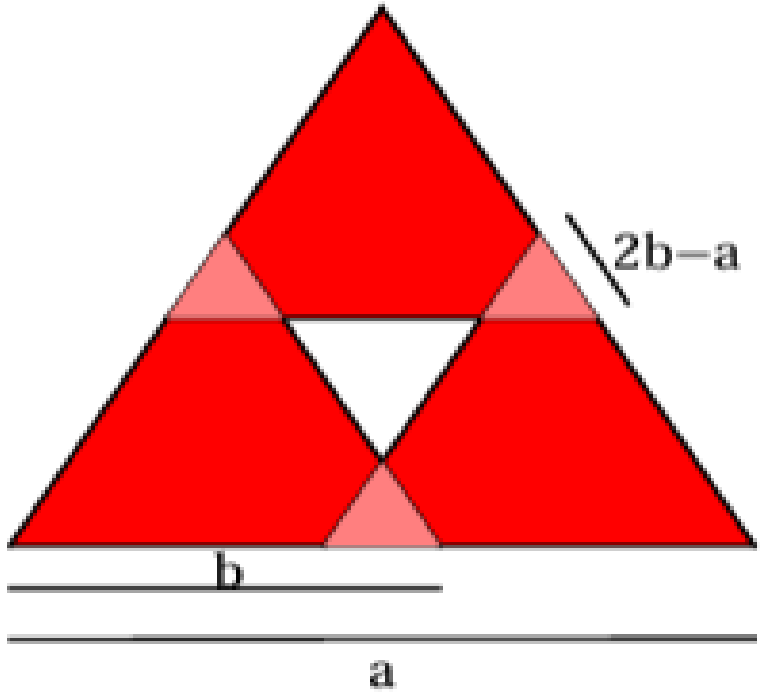


Figure: Geometric proof of the irrationality of $\sqrt{3}$. The white equilateral triangle in the middle has sides of length $2a - 3b$.

Have $3(2b - a)^2 = (2a - 3b)^2$ so $\sqrt{3} = (2a - 3b)/(2b - a)$, note $2b - a < b$ (else $b \geq a$), violates minimality.

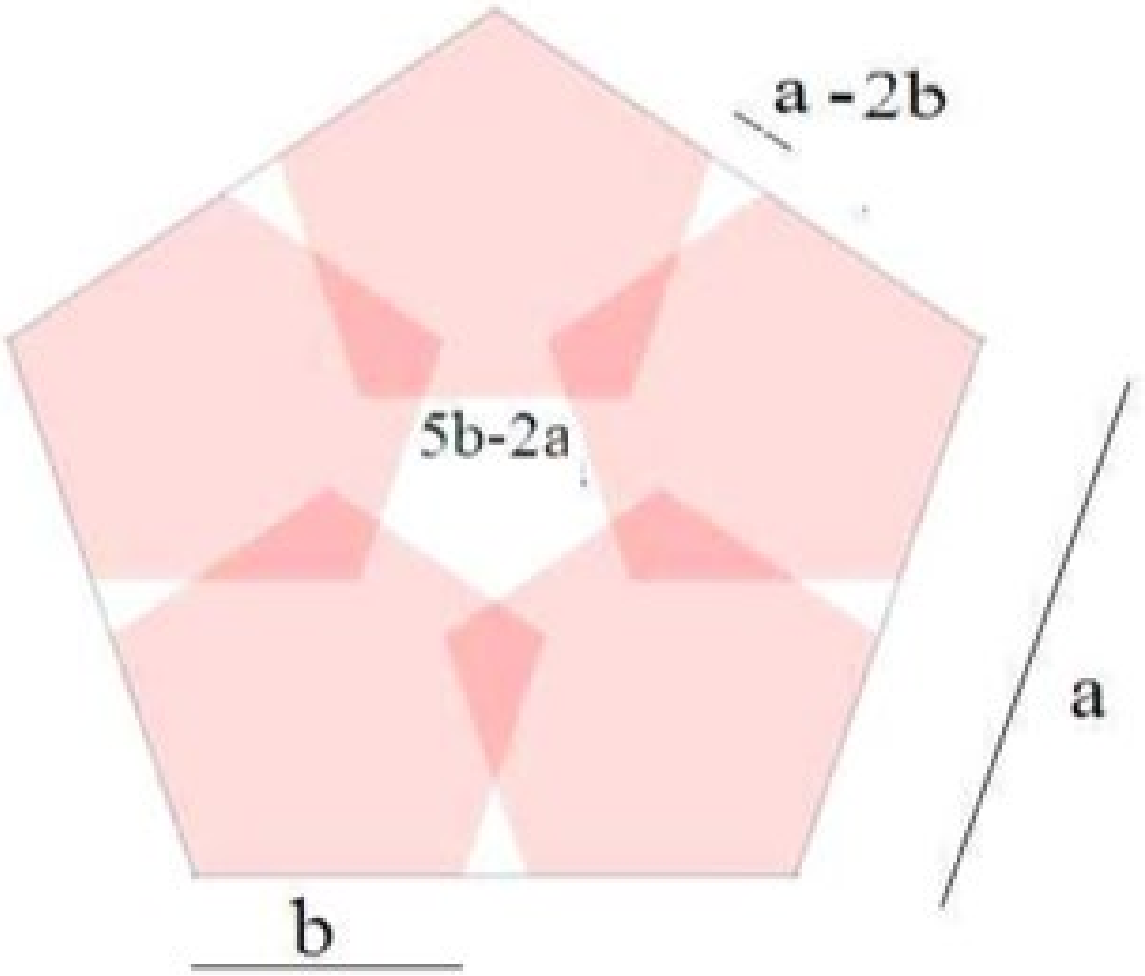
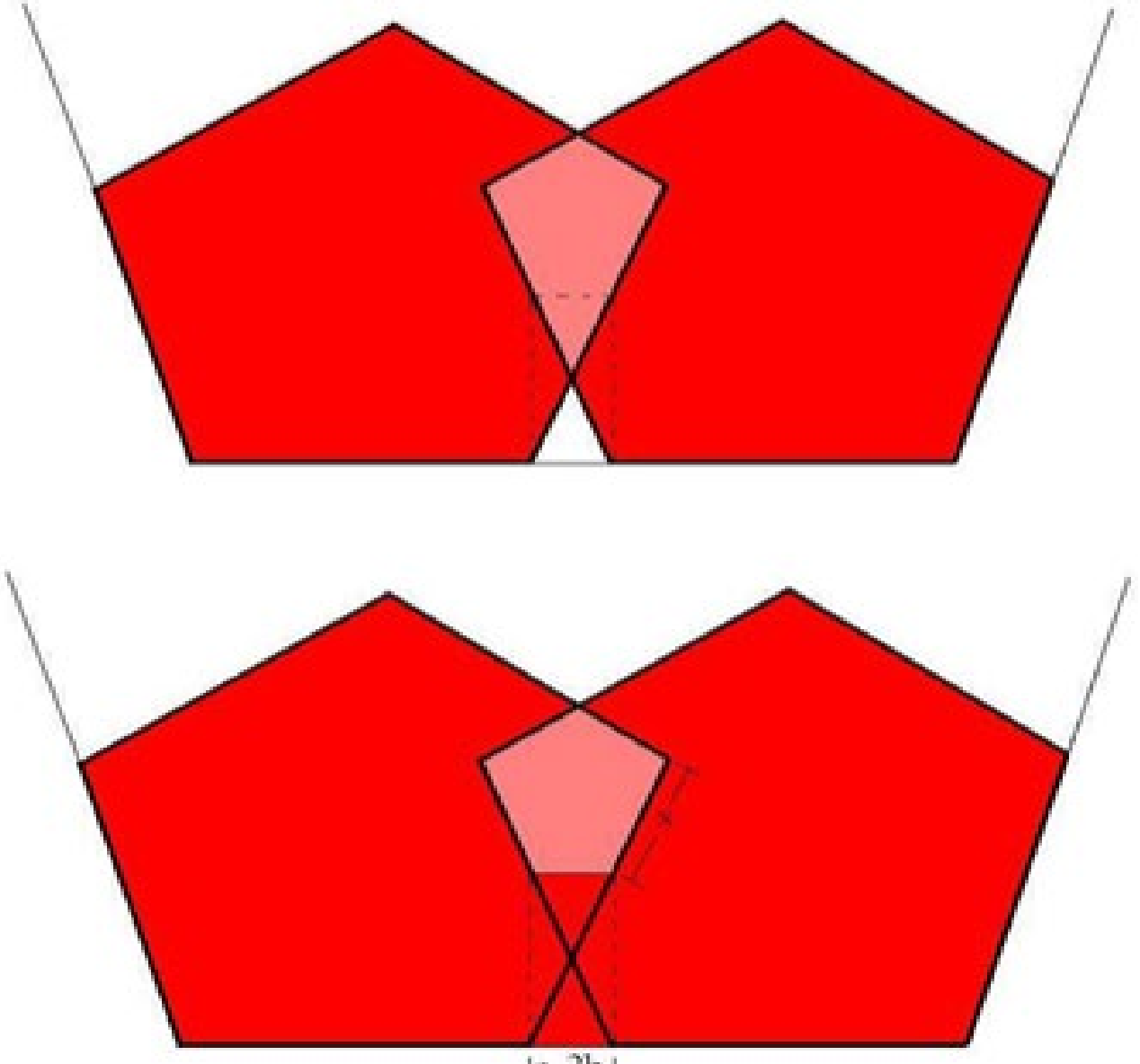


Figure: Geometric proof of the irrationality of $\sqrt{5}$.


|a-2b|

A straightforward analysis shows that the five doubly covered pentagons are all regular, with side length $a - 2b$, and the middle pentagon is also regular, with side length $b - 2(a - 2b) = 5b - 2a$.

We now have a smaller solution, with the five doubly counted regular pentagons having the same area as the omitted pentagon in the middle. Specifically, we have $5(a - 2b)^2 = (5b - 2a)^2$; as $a = b\sqrt{5}$ and $2 < \sqrt{5} < 3$, note that $a - 2b < b$ and thus we have our contradiction.

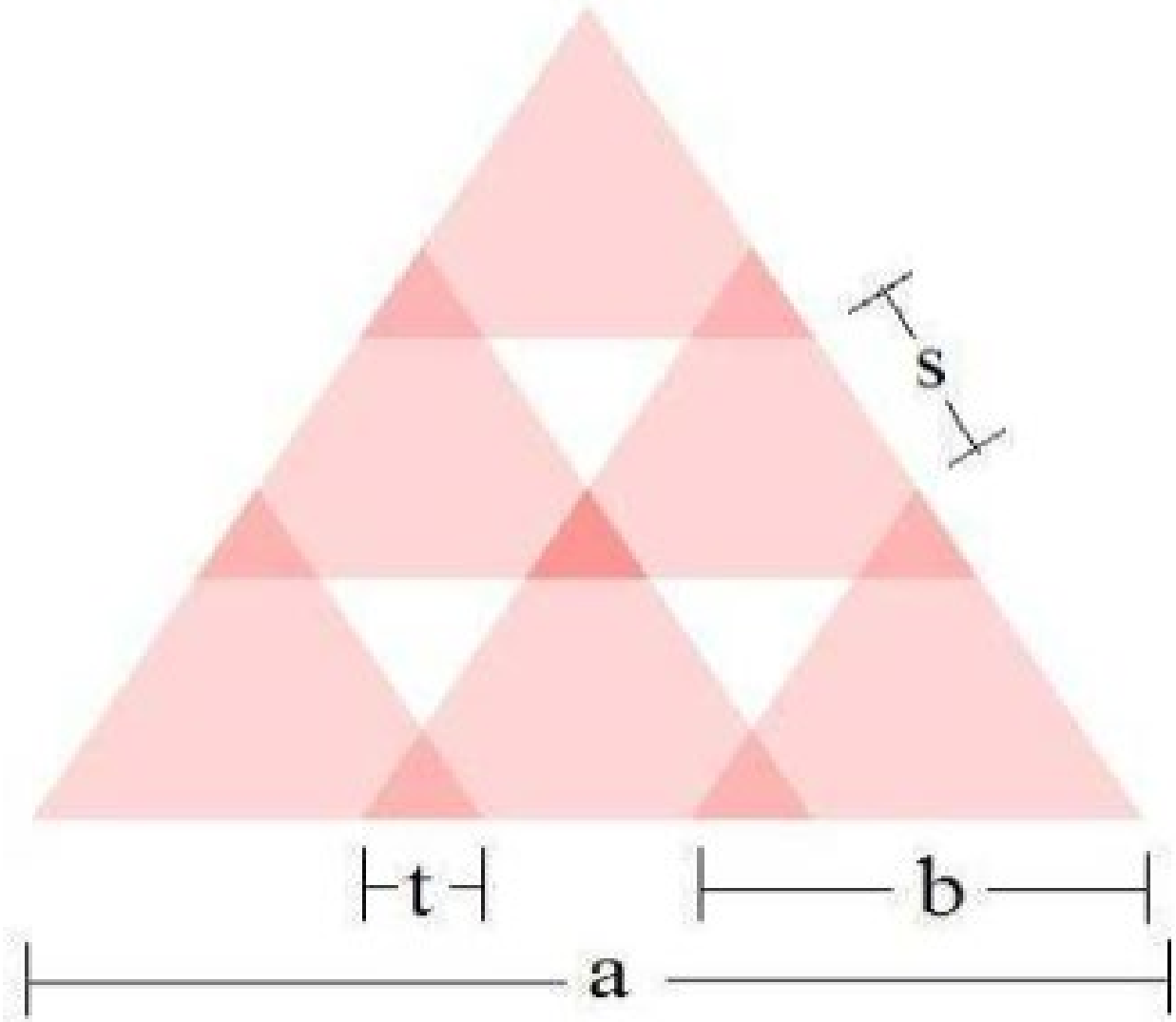


Figure: Geometric proof of the irrationality of $\sqrt{6}$.

How far can we extend this argument?

Have irrationality of square-roots of 3, 6, 10, 15…? 21, 28, 36

Triangle numbers

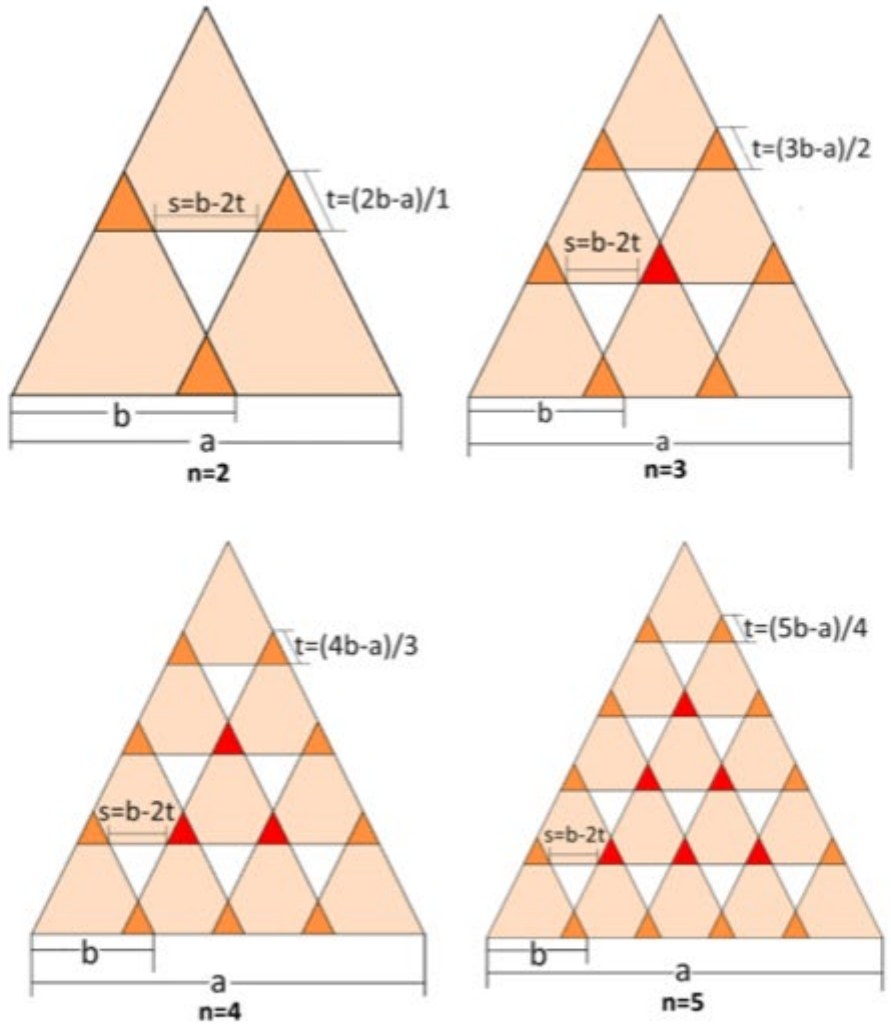


FIGURE 4. The proof of the irrationality of $\sqrt{n(n+1)/2}$ when n is 2, 3, 4, and 5.

Math 355: Modern Algebra: Fall '25 (Siena)

Professor Steven J Miller: sjm1@williams.edu

Homepage:
https://web.williams.edu/Mathematics/sjmiller/public_html/310Fa25/

Ring Theory Lecture

Lecture 14: 10/16/25: Zoom: discussed exam.

Lecture 15: 10/21/25: https://youtu.be/kojN5hfnrt4

Chapter Three: General Code Riddle, More Rings

General Code

Consider an army with 10 generals. One wants a security system such that any three of them can determine the code to launch nuclear missiles, but no two of them can.

It is possible to devise such a system by using a quadratic polynomial, such as ax^2 + bx + c; to launch the missiles, one must input (a,b,c).

What information should be given to the generals so that any three can find (a,b,c) but no two can? What about the general situation with N generals and any M can launch (but no set of M-1) can?

Try giving each general a subset of $\{a,b,c\}$

Case 1: A general gets all 3

↳ could launch, thus cannot do.

Case 2: A general gets two, wlog say $\{a,b\}$

↳ if someone knows c, the two can launch. Thus cannot do.

case 3: Each general knows only 1

$1 \to a$, $2 \to b$, $3 \to c$, $4 \to$ wlog a, knew 1, 2, 4 cannot launch!

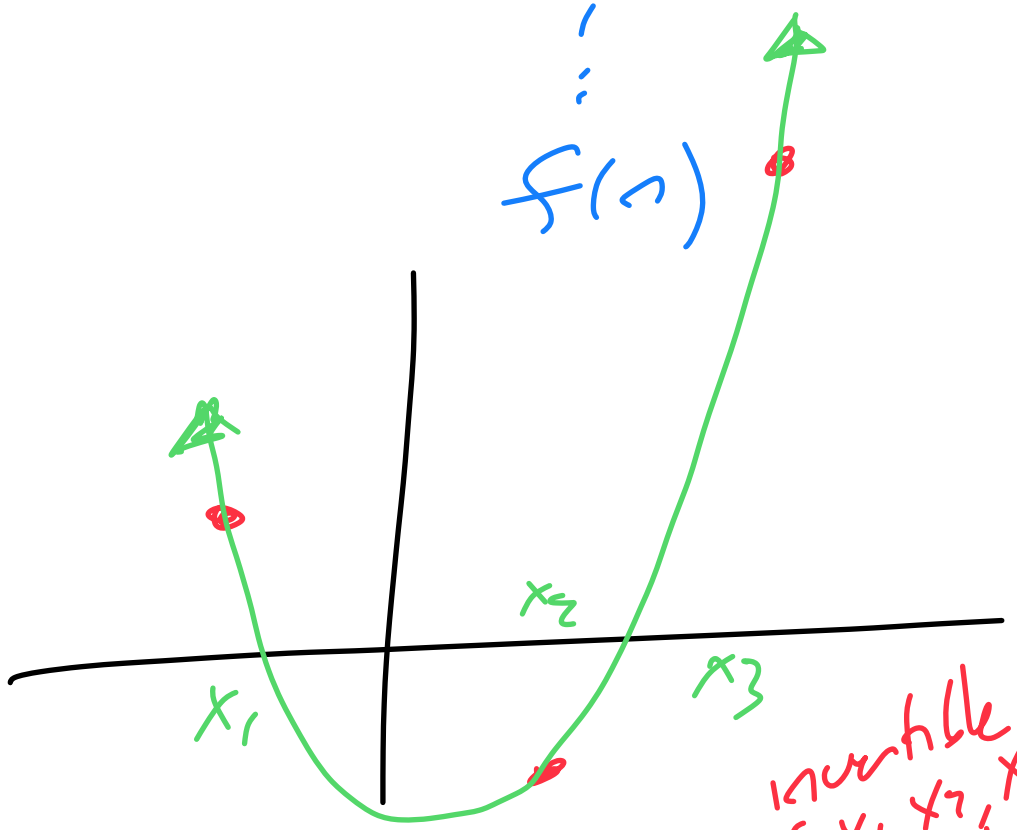
$f(x) = ax^2 + bx + c$, giving a, b or c doesn't work

General	Information:	Points
1	$f(1)$	$(1, f(1))$
2	$f(2)$	$(2, f(2))$
⋮	⋮	⋮
n	$f(n)$	$(n, f(n))$

2 points uniquely determine a line

3 points a parabola

4 points a cubic



$$ax_1^2 + bx_1 + c = y_1,$$
$$ax_2^2 + bx_2 + c = y_2$$
$$ax_3^2 + bx_3 + c = y_3$$

invertible if x_1, x_2, x_3 distinct

$$\begin{pmatrix} x_1^2 & x_1 & 1 \\ x_2^2 & x_2 & 1 \\ x_3^2 & x_3 & 1 \end{pmatrix} \begin{pmatrix} a \\ b \\ c \end{pmatrix} = \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix}$$

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} b_1 \\ b_2 \end{pmatrix}$$

$$\alpha x_1 + \beta x_2 = b_1$$

$$\gamma x_1 + \delta x_2 = b_2$$

$A\vec{x} = \vec{b}$ want $\vec{x} = A^{-1}\vec{b}$

no soln if lines are parallel, if det = 0, might have no soln

$$\begin{pmatrix} 1 & 2 \\ 2 & 4 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 3 \\ 6 \end{pmatrix}$$

$\times 2$

$$1x_1 + 2x_2 = 3$$

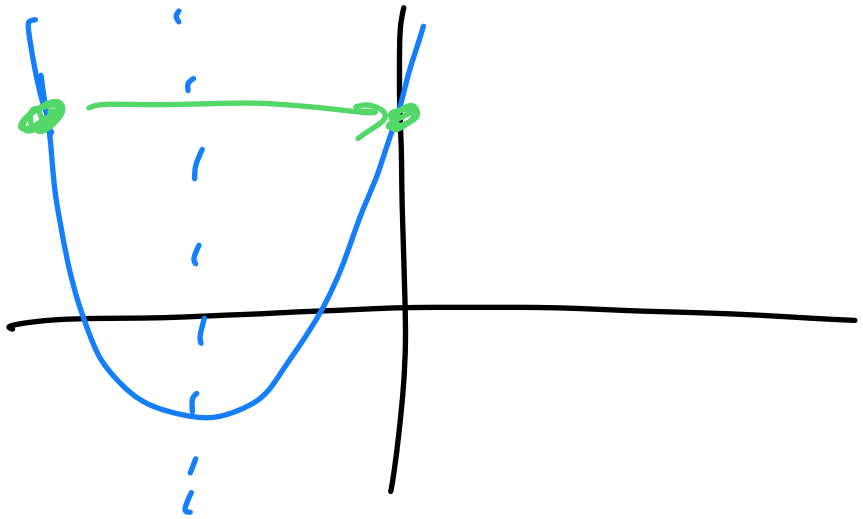
$$2x_1 + 4x_2 = 6$$

∞ many solns: same line

det is 0

Making some more important: Say need "10" to launch

$a_9x^9 + \cdots + a_1x + a_0 : (a_0, a_1, \ldots, a_9)$



Give president 10 points

Give provost 9 points

Give deans 4 points

↳ assume 8 deans

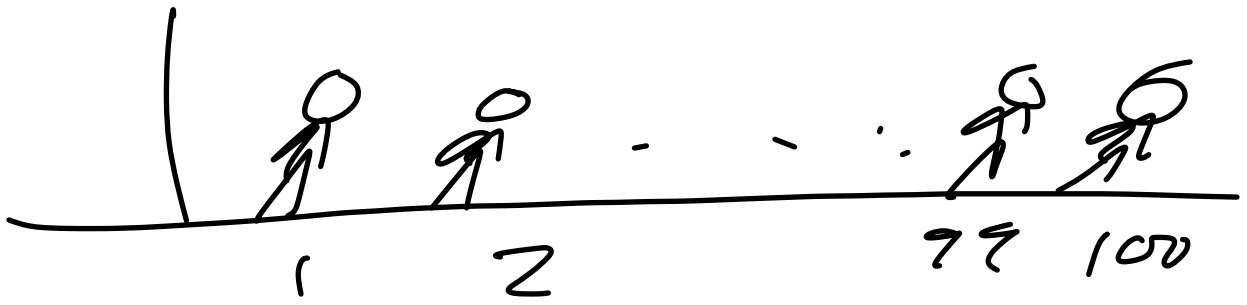
assume 2 are married

↳ couple get same points, or maybe 3 of 4 same

Hat Riddles

100 hats: each W or B

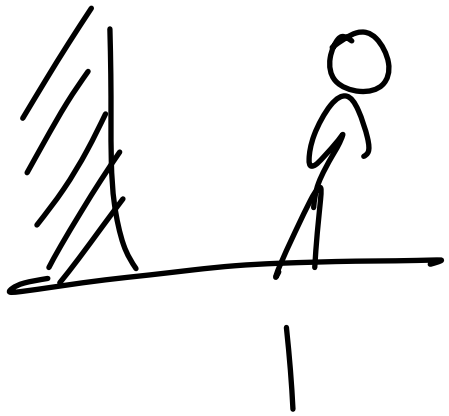
people are in a line, person k sees 1, 2, ..., k-1 and no one else.



100 are mathematicians. Strategize first.

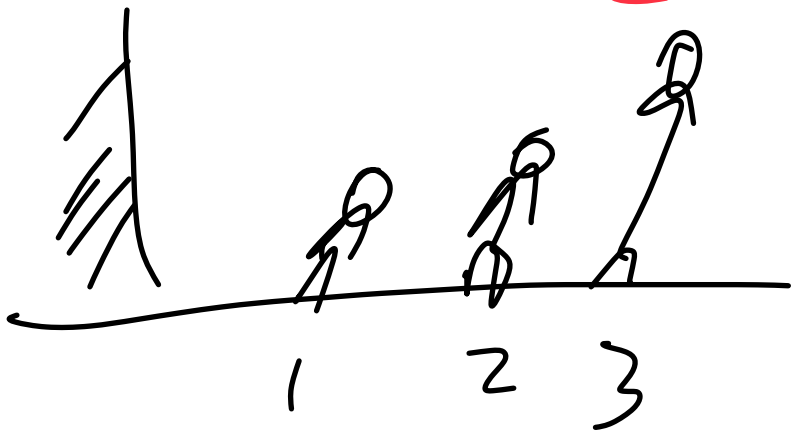
Evil prof hears, chooses hat assignments.

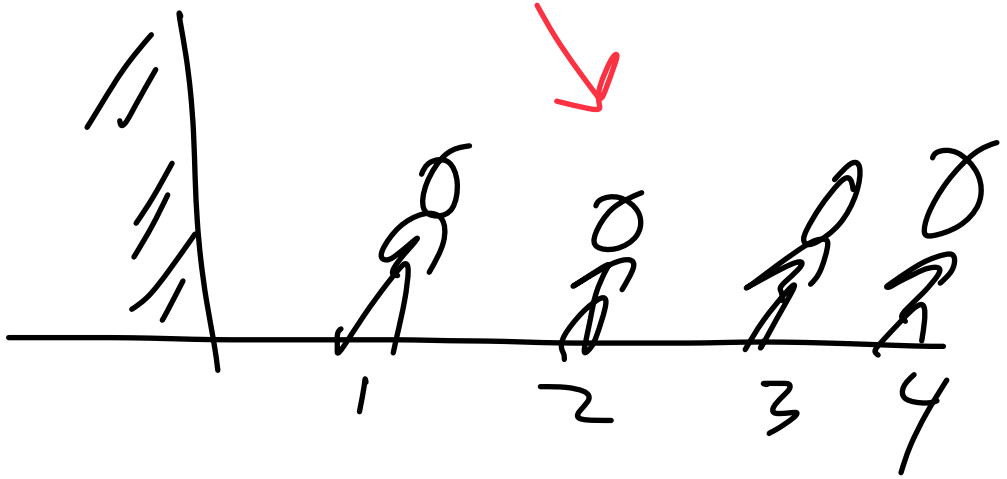
At time 1, person 100 speaks, 1 second later person 2, then 1 second later person 3... says W or B. If correct team gets $1,000,000; if wrong prof gets $1,000,000. How much can you ensure ya get?





Say color of hat in front





Proposition 3.15 (Cancellation Property for Integral Domains). *A commutative ring R is said to have the* cancellation property *if for every choice of $a, b, c \in R$, the following implication is true:*

$$ab = ac \iff b = c \text{ or } a = 0.$$

A commutative ring has the cancellation property if and only if it is an integral domain.

$\Rightarrow$ Assume R has the cancellation property, show it is an IntDom

Proof by contradiction: assume not an Integral domain

↳ have x and y with $xy = 0$ but $x, y \neq 0$

$a = x \quad b = y \quad c = 0$



have $\left.\begin{array}{l} ab = xy = 0 \\ ac = x0 = 0 \end{array}\right\}$ $ab = ac$ but $b \neq c$ and $a \neq 0$

Contradicts R has the cancellation property ☑

If $1=0$ then $R=\{0\}$

Definition 3.16. Let R be a commutative ring.[9] The *group of units of* R is the subset R^* of R defined by

$$R^* = \{a \in R : \text{there is some } b \in R \text{ satisfying } ab = 1\}.$$

The group law on R^* is ring multiplication. The elements of R^* are called *units*.

Proposition 3.17. *The set of units R^* is a group, with group law being ring multiplication.*

Proof: assoc: $u_1(u_2u_3) \stackrel{?}{=} (u_1u_2)u_3$: inherited as R ring

identity: $1 \in R$, $1 \in R^*$ as $1 \cdot 1 = 1$

inverse: if $a \in R$ is $a^{-1} \in R$?

As $a \in R$, $\exists\, b$ st $ab=1$, so $b = a^{-1}$

(need $ba=1$ but as R is commutative get for free)

a^{-1} is in R as there is a $c \in R$ st $a^{-1}c = 1 : c = a$

Definition 3.16. Let R be a commutative ring.[9] The *group of units of* R is the subset R^* of R defined by

$$R^* = \{a \in R : \text{there is some } b \in R \text{ satisfying } ab = 1\}.$$

The group law on R^* is ring multiplication. The elements of R^* are called *units*.

Proposition 3.17. *The set of units R^* is a group, with group law being ring multiplication.*

Proof (cont)

Closure: If $a_1, a_2 \in R^*$ then $a_1 a_2 \in R^*$

as $a_1 \in R^* \Rightarrow \exists b_1$ st $a_1 b_1 = 1$, $b_1 = a_1^{-1}$

$a_2 \in R^* \Rightarrow \exists b_2$ st $a_2 b_2 = 1$, $b_2 = a_2^{-1}$

To prove $(a_1 a_2) \in R^*$ find b_{12} st $(a_1 a_2) b_{12} = 1$

TRY $b_{12} = b_1 b_2 = a_1^{-1} a_2^{-1}$: $(a_1 a_2) a_1^{-1} a_2^{-1} = a_1 a_1^{-1} a_2 a_2^{-1} = 1$

So found b_{12} st $(a_1 a_2) b_{12} = 1$, so $a_1 a_2 \in R^*$ ☑

Needed results….

Theorem 1.32. *Let $a, b \in \mathbb{Z}$ be integers, not both 0. Then there are integers $u, v \in \mathbb{Z}$ satisfying*

$$au + bv = \gcd(a, b).$$

Euclidean Algorithm

If a prime divides a product (Steven J. Miller and Cesar Silva), College Mathematics Journal. (**48** (2017), no. 2, 123--128): https://web.williams.edu/Mathematics/sjmiller/public_html/math/papers/PrimeDividesProduct_MillerSilva40.pdf

ABSTRACT. One of the greatest difficulties encountered by all in their first proof intensive class is subtly assuming an unproven fact in a proof. The purpose of this note is to describe a specific instance where this can occur, namely in results related to unique factorization and the concept of the greatest common divisor.

p divides x y implies p divides x or y.

Proof: $p \mid xy$, wlog $p \nmid x$ show $p \mid y$
Use Euclidean Algorithm with 2 of x, y, p

Choose 2 of x, y, p know $p \mid xy$, $p \nmid x$

(x, y) or (x, p) or (y, p)

$\exists a, b$ st $ax + bp = \gcd(x, p) = 1$

$\exists a, b$ st $ay + bp = \gcd(y, p)$

have integers a, b with $ax + bp = 1$ (Eq #1)

know $p \mid xy$

multiply Eq #1 by y: $axy + bpy = y$

as $p \mid xy$, $xy = mp$ so $amp + bpy = y$

or $(am + by)p = y$

see $p \mid y$ as claimed ∎

Definition 3.10. A *field* is a commutative ring R with the property that every non-zero element of R has a multiplicative inverse. In other words, for every $a \in R$ with $a \neq 0$ there is a $b \in R$ satisfying $ab = 1$.

Proposition 3.20. *Let $m \geq 1$ be an integer. Then*

$$(\mathbb{Z}/m\mathbb{Z})^* = \{a \bmod m : \gcd(a, m) = 1\}.$$

In particular, if p is a prime number, then $\mathbb{Z}/p\mathbb{Z}$ is a field, often denoted $\mathbb{F}_p$.

Ex: $(\mathbb{Z}/12\mathbb{Z})^* = \{1, 5, 7, 11\}$

For second part: $\{1, 2, 3, \ldots, p-1\}$ are all invertibles

Proof: $x \in \{1, 2, \ldots, p-1\}$ so $\gcd(x, p) = 1$

so by Euclidean Alg $\exists\, a, b$ st $ax + bp = 1$ or $ax = 1 - bp$

so $ax \equiv 1 \bmod p$ so x is invertible with inverse a

Math 355: Modern Algebra: Fall '25 (Siena)

Professor Steven J Miller: sjm1@williams.edu

Homepage:
https://web.williams.edu/Mathematics/sjmiller/public_html/310Fa25/

Ring Theory Lecture

Lecture 16: 10/23/25: https://youtu.be/1td84DBXdMc

Chapter Three: 100 Hat Riddle, Ideals

Steve Miller's Math Riddles

Mad as a Hatter

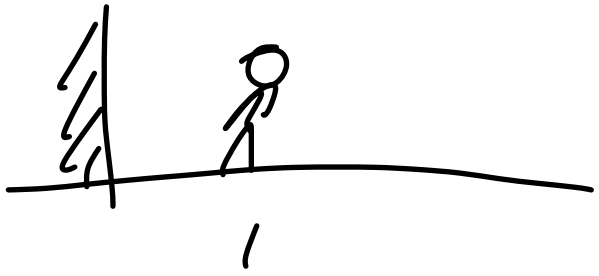
100 mathematicians are standing in a line, wearing a black or white hat. Each mathematician can ONLY see the color of the hats of the people in front of them. So the first person sees no hats, the last sees 99.

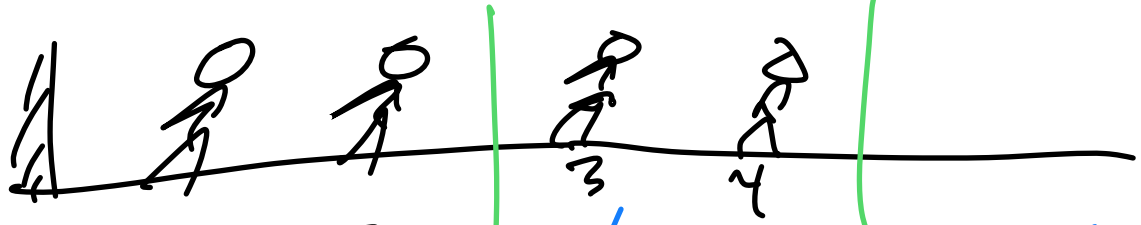
The mathematicians are allowed to talk to each other and decide upon a strategy, for a government rep is coming to cut off funding. Each person can only say “black” or “white.” If you correctly say what color hat you’re wearing, your funding is continued and you live. If you’re wrong, you lose your funding, and you may as well be dead.

How many mathematicians can you guarantee will keep their funding?

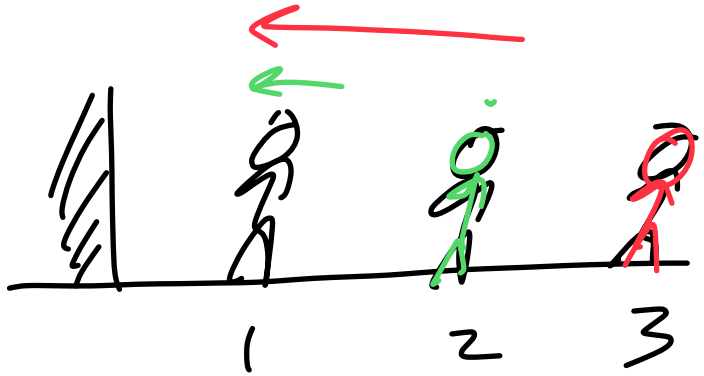
You are not allowed you use “tricks,” say a person delays one second before answering means A, two seconds means B, … You have to answer IMMEDIATELY what color hat you’re wearing.

Communicated by Gergely Harcos.





say hat color of person in front, 50%



	1	2	3
same	B	B	
different	B	W	
different	W	B	
same	W	W	

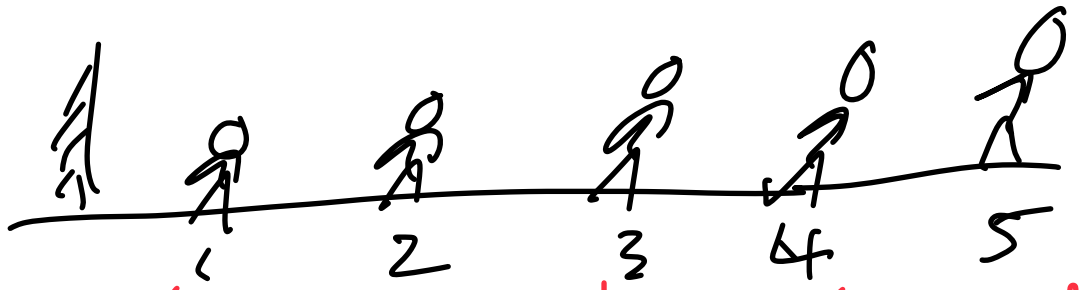
B if both same color

W if both different colors

2/3

Can you do 3/4?

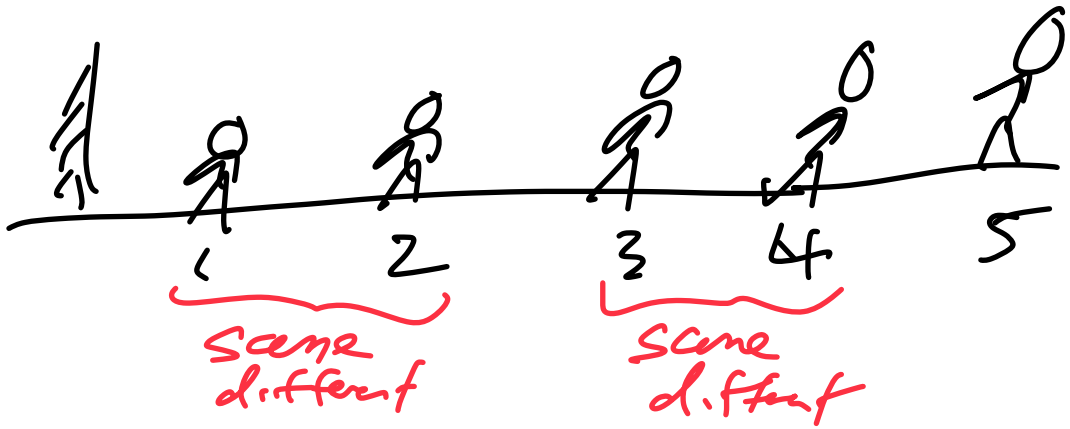
Here is 4/5



same different

same different

B if both pairs same parity W if not



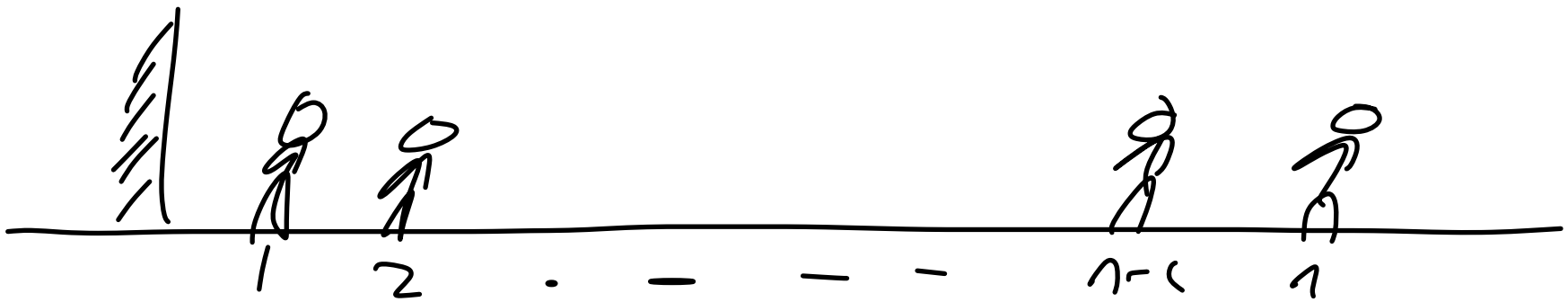
1 2	3 4	5
same	same	B
same	different	W
different	same	W
different	different	B

B W W B

diff diff

B ← W ← W ← B ← B

4/5



100% in the limit

Last person says B if even # black hats and W if have even # white hats; since #B + #W = 99, exactly one is even. PARITY!

100 says B and 99 sees 34 black hats, so 99 has white hat



work the # black hats in binary!
have B = 1 and W = 0
use last $\lfloor \log_2 n \rfloor$ people to say the # of black hats person n sees.

Definition 3.26. Let R be a commutative ring. An *ideal* of R is a non-empty subset $I \subseteq R$ with the following two properties:

- If $a \in I$ and $b \in I$, then $a + b \in I$.
- If $a \in I$ and $r \in R$, then $ra \in I$. (same as $ar \in I$)

Similar to rings and subrings, groups and subgroups.

Looking at subsets of items of interest.

- Closed under addition
- Closed under multiplication:
  $a, b \in I$ must $ab \in I$?
  ↳ Take $r = b$ and get $ab \in I$ (same as $I \subset R$)

Definition 3.27. Let R be a commutative ring, and let $c \in R$. The *principal ideal generated by* c, denoted cR or (c), is the set of all multiples of c,

$$cR = (c) = \{rc : r \in R\}.$$

Is This an ideal?

- If $a, b \in (c)$ Then $\exists\, r_a, r_b$ s.t $a = r_a c$ and $b = r_b c$

  Then $a + b = r_a c + r_b c = (r_a + r_b)c \in (c)$

  (distributive law)

  as $r_a + r_b \in R$

  So let $r = r_a + r_b$

  and Thus $a + b = rc$.

- If $a \in (c)$ then $\forall r \in R$, $ra \in (c)$.

  As $a \in (c)$ $\exists\, \tilde{r}$ such that $\tilde{r}c = a$, Thus $ra = (r\tilde{r})a = \hat{r}a$,

  where $\hat{r} = r\tilde{r} \in R$ and Thus $ra \in (c)$

$(c) = \{rc : r \in R\}$

$(0) = \{0\}$

$(1) = \{r1 : r \in R\} = R$

$\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$

$(2) = \{\ldots, -4, -2, 0, 2, 4, \ldots\}$

$(3) = \{\ldots, -6, -3, 0, 3, 6, \ldots\}$

(4) or (5)

$(n) = \{\ldots, -2n, -n, 0, n, 2n, \ldots\}$

$(c) = \{rc : r \in R\}$

R = polynomials with integer coefficients of finite degree in X

$= \mathbb{Z}[X] := \{a_n X^n + \cdots + a_1 X + a_0 : a_i \in \mathbb{Z}, n \text{ non-neg integer}\}$

$(X) = \{rX : r \in \mathbb{Z}[X]\}$: all polynomials with zero constant term

If I give you $a_1, a_2, \ldots, a_n \in R$, is there ALWAYS an ideal containing them? YES! R works! Is there something smaller?

Definition 3.31. Let R be a commutative ring, and let I be an ideal of R. Then for each element $a \in R$, the *coset of* a is the set

$$a + I = \{a + c : c \in I\}.$$

$x \in a+I$ $y \in a+I$ must $x+y \in a+I$?

Take $R=\mathbb{Z}$, $I=(12)$, $a+I = \{a+c : c \in (12)\}$

$= \{a+12m \text{ for some } m\}$.

Study $a \in \{0,\dots,11\}$; note $13+(12) = 1+(12)$

↳ wlog our representatives live in $\{0,\dots,11\}$

If $a=3$, $x \in 3+(12)$ and $y \in 3+(12)$

↳ take $x=15$, $y=27$ and $x+y = 15+27 = 42$

and $42 = 6+3\cdot 12 \in 6+(12)$ not in $3+(12)$

3.7. Prime Ideals and Maximal Ideals

Definition 3.37. Let R be a commutative ring. An ideal I of R is a *prime ideal* if $I \neq R$ and if whenever a product of elements $ab \in I$, then either $a \in I$ or $b \in I$.

We observe that if I is a prime ideal, then it also has the following property:

$$a \notin I \text{ and } b \notin I \implies ab \notin I.$$

This statement is the contrapositive of, and hence logically equivalent to, the stated definition of prime ideal.

Definition 3.40. Let R be a commutative ring. An ideal I is called a *maximal ideal* if $I \neq R$ and if there are no ideals properly contained between I and R. In other words, if J is an ideal and $I \subseteq J \subseteq R$, then either $J = I$ or $J = R$.

PRIME IDEAL

Ex: $\mathbb{Z}$, $(n) = \{\ldots, -2n, -n, 0, n, 2n, \ldots\}$

$(2) = \{\ldots, -12, 0, 12, \ldots\}$

$(7) = \{\ldots, -7, 0, 7, \ldots\}$

Definition 3.37. Let R be a commutative ring. An ideal I of R is a *prime ideal* if $I \neq R$ and if whenever a product of elements $ab \in I$, then either $a \in I$ or $b \in I$.

We observe that if I is a prime ideal, then it also has the following property:

$$a \notin I \text{ and } b \notin I \implies ab \notin I.$$

This statement is the contrapositive of, and hence logically equivalent to, the stated definition of prime ideal.

Is (12) a prime ideal? NO! $3 \cdot 4 \in (12)$ but $3, 4 \notin (12)$

Is (7) a prime ideal? YES! $a \cdot b \in (7)$ Then $\exists r$ s.t. $ab = 7r$

as $7 \mid 7r \Rightarrow 7 \mid ab$ and thus $7 \mid a$ or $7 \mid b$

Proved (p) is a prime ideal if p is prime,

(n) is not a prime ideal if n is composite.

Let $R=\mathbb{Z}$, is (n) maximal and if so for what n?

Definition 3.40. Let R be a commutative ring. An ideal I is called a *maximal ideal* if $I \neq R$ and if there are no ideals properly contained between I and R. In other words, if J is an ideal and $I \subseteq J \subseteq R$, then either $J = I$ or $J = R$.

$n=1$: $(1)=\mathbb{Z}$, this is all of $R=\mathbb{Z}$.

$n=2$: $(2)=\{\ldots,-4,-2,0,2,4,\ldots\}$

$(2) \subseteq J \subseteq \mathbb{Z}$

if (2) is maximal then only J that work are $J=(2)$ and $J=\mathbb{Z}$

Proof only $J=(2)$ and $\mathbb{Z}$ work.

↪ Assume $J \neq (2)$, must show $J=\mathbb{Z}$.

As $J \supseteq (2)$ and $J \neq (2)$, must have some $x \in J$ with $x \notin (2)$

Then x is odd so $\exists n$ st $x=2n+1$

As $-2n \in (2)$ By additive closure $x-2n = x+(-2n) \in J$

But $x-2n=1$ so $1 \in J$ so multiplicative closure $r \cdot 1 \in J$ thus $J=R$.

Conjecture: p prime, (p) is maximal.

Conjecture: n composite, (n) is not maximal.

↳ $n = ab$ with $a, b \neq 1$

$$(ab) \subsetneq (a), (b) \subsetneq R = \mathbb{Z}$$

is $(ab) \subsetneq (a)$ and $(ab) \subsetneq (b)$

↳ find something in (a) not in (ab)

$R = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$

$(a) = \{\ldots, -3a, -2a, -a, 0, a, 2a, 3a, \ldots\}$

$(ab) = \{\ldots, -3ab, -2ab, -ab, 0, ab, 2ab, 3ab, \ldots\}$

↳ as $a \in (a)$ but $a \notin (b)$, $(ab) \subsetneq (a)$

↳ as $1 \in R$ but $1 \notin (a)$, $(a) \subsetneq R$

thus (ab) is not maximal

Theorem 3.43. *Let R be a commutative ring, and let I an ideal with $I \neq R$.*

(a) *I is a prime ideal if and only if the quotient ring R/I is an integral domain.*

(b) *I is a maximal ideal if and only if the quotient ring R/I is a field.*

Corollary 3.44. *Every maximal ideal is a prime ideal.*

Vector Spaces — Part 1

Chapter 4

Thinking abstractly, we observe that vectors allow two sorts of operations:

- We can multiply a vector by a number. This is called *scalar multiplication*. Scalars are $\mathbb{R}$ or $\mathbb{C}$
- We can add two vectors. This is called *vector addition*.

Definition 4.1. A *field* is a commutative ring F with the property that for every $a \in F$ with $a \neq 0$ there is a $b \in F$ satisfying $ab = 1$.

Definition 4.3. Let F be a field. A *vector space with field of scalars* F, or alternatively an *F-vector space*, is an abelian group V with addition operation $+$ and with a rule for multiplying a vector $\boldsymbol{v} \in V$ by a scalar $c \in F$ to obtain a new vector $c\boldsymbol{v} \in V$. Vector addition and scalar multiplication are required to satisfy the following axioms:

(1) [Identity Law]

$$1\boldsymbol{v} = \boldsymbol{v} \text{ for all } \boldsymbol{v} \in V.$$

(2) [Distributive Law #1]

$$c(\boldsymbol{v}_1 + \boldsymbol{v}_2) = c\boldsymbol{v}_1 + c\boldsymbol{v}_2 \text{ for all } \boldsymbol{v}_1, \boldsymbol{v}_2 \in V \text{ and all } c \in F.$$

(3) [Distributive Law #2]

$$(c_1 + c_2)\boldsymbol{v} = c_1\boldsymbol{v} + c_2\boldsymbol{v} \text{ for all } \boldsymbol{v} \in V \text{ and all } c_1, c_2 \in F.$$

(4) [Associative Law]

$$(c_1c_2)\boldsymbol{v} = c_1(c_2\boldsymbol{v}) \text{ for all } \boldsymbol{v} \in V \text{ and all } c_1, c_2 \in F.$$

The identity element of V is called the *zero vector* and is denoted by $\mathbf{0}$. It should not be confused with $0 \in F$, which is the zero element of the field F.

Definition 4.5. Let F be a field, and let V and W be F-vector spaces. A *linear transformation* from V to W is a function

$$L : V \longrightarrow W$$

satisfying:

$$L(c_1\boldsymbol{v}_1 + c_2\boldsymbol{v}_2) = c_1L(\boldsymbol{v}_1) + c_2L(\boldsymbol{v}_2) \quad \text{for all } \boldsymbol{v}_1, \boldsymbol{v}_2 \in V \text{ and all } c_1, c_2 \in F.$$

If we want to specify the scalar field, we will say that L is an F-linear transformation.

Matrices! $A(c_1\vec{v}_1 + c_2\vec{v}_2) = A(c_1\vec{v}_1) + A(c_2\vec{v}_2)$

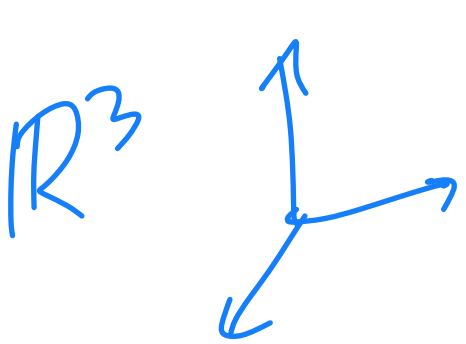
$= c_1A\vec{v}_1 + c_2A\vec{v}_2$

Definition 4.11. Let V be an F-vector space. A *finite*[5] *basis for* V is a finite set of vectors $\mathcal{B} = \{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n\} \subset V$ with the following property:

> Every vector $\boldsymbol{v} \in V$ can be written in the form
>
> $$\boldsymbol{v} = a_1\boldsymbol{v}_1 + a_2\boldsymbol{v}_2 + \cdots + a_n\boldsymbol{v}_n$$
>
> for exactly one choice of scalars $a_1, \ldots, a_n \in F$.

An expression of the form $a_1\boldsymbol{v}_1 + \cdots + a_n\boldsymbol{v}_n$ is called a *linear combination of* $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$.

Theorem 4.18 (Invariance of Dimension)**.** *Let V be a vector space that has a finite basis. Then every basis for V has exactly the same number of elements.*



$\vec{e}_1 = (1,0,0)$

$\vec{e}_2 = (0,1,0)$

$\vec{e}_3 = (0,0,1)$

$\vec{v}_1 = (1,0,0)$

$\vec{v}_2 = (1,1,0)$

$\vec{v}_3 = (1,1,1)$

$\{a + b\sqrt{2} + c\sqrt{3} : a, b, c \in \mathbb{Q}\}$ $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} : a, b, c, d \in \mathbb{Q}\}$

closed under addition

not closed under mult

Exercise: show $\nexists a, b, c \in \mathbb{Q}$ st $\sqrt{6} = a + b\sqrt{2} + c\sqrt{3}$

closed under add and mult

what are the dimensions here?

The Finite Field $\mathbb{F}_p$

p prime

$\{0, 1, 2, \ldots, p-1\}$ under clock arithm

every non-zero element is invertible: field

↳ if n composite, $\{0, 1, 2, \ldots, n-1\}$ not a field.

Math 355: Modern Algebra: Fall '25 (Siena)

Professor Steven J Miller: sjm1@williams.edu

Homepage:
https://web.williams.edu/Mathematics/sjmiller/public_html/310Fa25/

Ring Theory Lecture

Lecture 17: 10/28/25:

https://youtu.be/8NiIJemPb9Q

Chapter Three: Finishing Rings, Solving Polynomials

Proposition 5.15. *Let L/F be an extension of fields, and let $\alpha_1, \ldots, \alpha_n \in L$. Then there is a unique field K with the following properties:*

(i) $F \subseteq K \subseteq L$.
(ii) $\alpha_1, \ldots, \alpha_n \in K$.
(iii) *If K' is a field satisfying $F \subseteq K' \subseteq L$ and $\alpha_1, \ldots, \alpha_n \in K'$, then $K \subseteq K'$.*

The field K is denoted $F(\alpha_1, \ldots, \alpha_n)$ and is called the extension field of F generated by $\alpha_1, \ldots, \alpha_n$. *The definition says that $F(\alpha_1, \ldots, \alpha_n)$ is the smallest subfield of L that contains both F and $\alpha_1, \ldots, \alpha_n$.*

Field $\mathbb{Q}$ Field $\mathbb{C}$

$\sqrt{2}, \sqrt{3} \in K$ $\mathbb{Q} \subseteq K \subseteq \mathbb{C}$

Is there a $k \in K$ st $k\sqrt{2} = 1 \Rightarrow \frac{1}{\sqrt{2}} \in K$

$\sqrt{2}+\sqrt{3} \in K$, $m\sqrt{2} + n\sqrt{3}$ for all integers m, n

$\frac{\sqrt{3}}{\sqrt{2}} \in K$

Question: if $a, b, c, d \in \mathbb{Q}$
$a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$
form a field containing $\sqrt{2}, \sqrt{3}$,
is it smallest?

Is $\sqrt{6} = a + b\sqrt{2} + c\sqrt{3}$ for some $a, b, c \in \mathbb{Q}$?

Extra Credit: Figure it out!

Definition 5.16. Let K/F be an extension of fields. The *degree of* K *over* F, denoted $[K : F]$, is the dimension of K when viewed as an F-vector space,

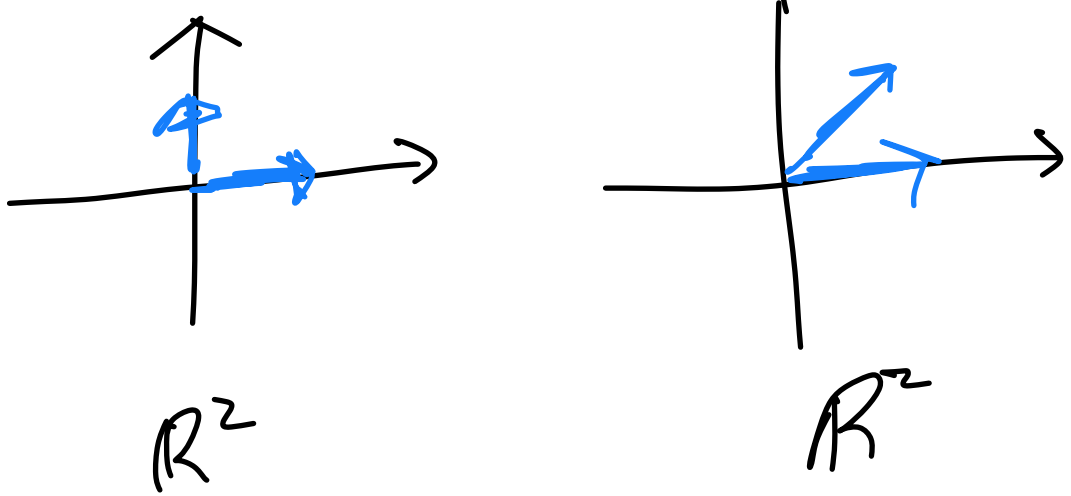
$$n := [K : F] = \dim_F(K).$$

$\exists$ elements $k_1, k_2, \ldots, k_n \in K$ st

$\forall k \in K \quad \exists f_1, \ldots, f_n \in F$ st

$$k = f_1 k_1 + \cdots + f_n k_n$$

Lin Alg:



basis vectors same

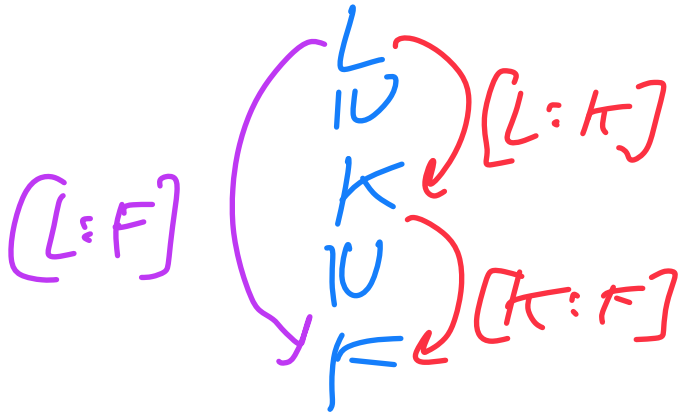
1st vectors are $\perp$, not in 2nd

Theorem 5.18 (Multiplicativity of Degree in Towers of Fields). *Let $L/K/F$ be extensions of fields; i.e., L is an extension field of K, and K is an extension field of F, so we may also view L as an extension field of F.*

(a) *If both of the degrees $[L : K]$ and $[K : F]$ are finite, then $[L : F]$ is also finite, and the degrees satisfy the relation*

$$[L : F] = [L : K] \cdot [K : F]. \tag{5.1}$$

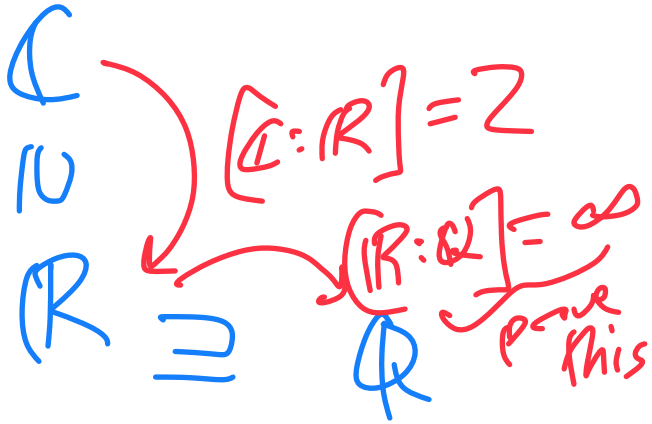
(b) *If either of the degrees $[L : K]$ and $[K : F]$ is infinite, then $[L : F]$ is also infinite.*



How is $[L:F]$ related to $[L:K]$ and $[K:F]$

answer: equals the product

Ex:



$z \in \mathbb{C}$: $z = r_1 c_1 + \cdots + r_n c_n$

Basis: $c_1 = 1$ $c_2 = i$

to prove basis: show $\mathbb{C} \neq \mathbb{R} <$ for any fixed $c \in \mathbb{C}$

write this up rigorously

5.5. Polynomial Rings

Definition 5.19. Let F be a field, and let $f(x) \in F[x]$ be a non-zero polynomial. We write the polynomial $f(x)$ as

$$f(x) = a_0 + a_1 x + \cdots + a_d x^d \quad \text{with } a_d \neq 0.$$

Then the *degree of* f is

$$\deg(f) = d.$$

By convention, we set $\deg(0) = -\infty$, a quantity that is smaller than every real number. Further, if $a_d = 1$, then we say that f is a *monic polynomial*.

$f(x) = \sum_{n=1}^{d_1} a_n x^n$ $\quad g(x) = \sum_{m=1}^{d_2} b_m x^m$ $\quad \deg(fg) = d_1 + d_2$

$a_{d_1} \neq 0$ $\quad b_{d_2} \neq 0$

$f(x)g(x) = a_{d_1} b_{d_2} x^{d_1+d_2} + \text{lower order terms}$

$a_{d_1} b_{d_2}$: is this non-zero? Yes as a field

$\mathbb{Z}/6\mathbb{Z}$: $2 \cdot 3 \equiv 0 \bmod 6$: deg can be lower in a ring.

$$\deg(f \cdot g) = \deg(f) + \deg(g)$$

mult

addition

Imagine $g(x) = 0$

$\deg(f \cdot 0) = \deg(f) + \deg(0)$

$\deg(0) = \deg(f) + \deg(0)$

↳ either $\deg(0) = -\infty$ or $\deg(0) = \infty$

---

g is constant, $g(x) = c \neq 0$

$\deg(f \cdot c) = \deg(f) + \deg(c)$

$\deg(f) = \deg(f) + \deg(c) \Rightarrow \deg(c) = 0$

Proposition 5.20 (Division-with-Remainder for Polynomials). *Let F be a field, and let $f(x), g(x) \in F[x]$ be a polynomials with $g(x) \neq 0$. Then there are unique polynomials $q(x), r(x) \in F[x]$ satisfying*

$$f(x) = g(x)q(x) + r(x) \quad \text{with} \quad \deg(r) < \deg(g). \tag{5.4}$$

$f(x) = a_n x^n + \cdots + a_0$

$g(x) = b_m x^m + \cdots + b_0$ wlog $m \le n$

$\left[\frac{a_n}{b_m} x^{n-m}\right] g(x) = a_n x^n + \cdots$

need field so $\frac{1}{b_m}$ exists

Theorem 5.21. *Let F be a field, and let $I \subseteq F[x]$ be an ideal in the ring $F[x]$. Then I is a principal ideal.*

Theorem 5.26. *Let F be a field, and let $f(x) \in F[x]$ be a non-zero polynomial. The following are equivalent:*

(a) *The polynomial $f(x)$ is irreducible.*

(b) *The principal ideal $f(x)F[x]$ generated by $f(x)$ is a maximal ideal.*

(c) *The quotient ring $F[x]/f(x)F[x]$ is a field.*

Theorem 5.27. *Let F be a field, let $f(x) \in F[x]$ be an irreducible polynomial, let $I_f = f(x)F[x]$ be the principal ideal generated by $f(x)$, and let $K_f = F[x]/I_f$ be the indicated quotient ring.*

(a) *The ring K_f is a field.*

(b) *We may identify the field F with a subfield of K_f via the map $F \to K_f$ defined by $c \mapsto c + I_f$.*

(c) *The polynomial $f(x)$ has a root in the field K_f.*

(d) *The field K_f is a finite extension of the field of F. Its degree is given by*

$$[K_f : F] = \deg(f).$$

5.7. Finite Fields

Proposition 5.28. *Let F be a finite field.*

(a) *The characteristic of F is prime.*

(b) *Let $p = \mathrm{char}(F)$. Then the finite field $\mathbb{F}_p$ is a subfield of F, in the sense that there is a unique injective homomorphism*

$$\mathbb{F}_p \hookrightarrow F.$$

(c) *The number of elements of F is given by the formula*

$$\#F = p^{[F:\mathbb{F}_p]}.$$

In particular, the number of elements in a finite field is always a power of a prime.

Much of math is about solving equations.

Example: polynomials: Assume coeff of highest deg is non-zero

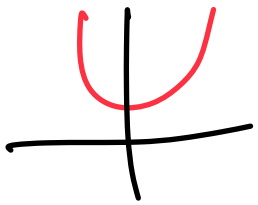
- $ax + b = 0$, root $x = -b/a$.
- $ax^2 + bx + c = 0$, roots $(-b \pm \sqrt{b^2 - 4ac})/2a$.
- Cubic, quartic: formulas exist in terms of coefficients; not for quintic and higher.

Quadratic Formula

$ax^2+c=0 \Rightarrow ax^2=-c,\ x^2=-c/a,\ x=\pm\sqrt{-c/a}$

$a(x-h)^2+c=0 \Rightarrow a(x-h)^2=-c,\ (x-h)^2=-\frac{c}{a},\ x=h\pm\sqrt{-\frac{c}{a}}$

vertex form



$ax^2+bx+c=\tilde{a}(x-h)^2+\tilde{c}$

Completing the square: $ax^2+bx+c=a\left(x^2+\frac{b}{a}x+\frac{b^2}{4a^2}-\frac{b^2}{4a^2}\right)+c$

$=a\left(x^2+\frac{b}{a}x+\frac{b^2}{4a^2}\right)-\frac{b^2}{4a}+c$

$=a\left(x+\frac{b}{2a}\right)^2-\frac{b^2-4ac}{4a}$

$\Rightarrow a\left(x+\frac{b}{2a}\right)^2=\frac{b^2-4ac}{4a} \Rightarrow \left(x+\frac{b}{2a}\right)^2=\frac{b^2-4ac}{4a^2}$

$$\left(x + \frac{b}{2a}\right)^2 = \frac{b^2 - 4ac}{(2a)^2}$$

$$x + \frac{b}{2a} = \pm \frac{\sqrt{b^2 - 4ac}}{2a}$$

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

Cubic: For fun, here's the solution to $ax^3 + bx^2 + cx + d = 0$

wlog $a=1$ $b \to b/a$ $c \to c/a$, $d \to \frac{d}{a}$

wlog $b=0$

```
Solve[a x^3 + b x^2 + c x + d == 0, x]
```

$$\left\{\left\{x \to -\frac{b}{3a} - \frac{2^{1/3}\left(-b^2+3ac\right)}{3a\left(-2b^3+9abc-27a^2d+\sqrt{4\left(-b^2+3ac\right)^3+\left(-2b^3+9abc-27a^2d\right)^2}\right)^{1/3}} + \frac{\left(-2b^3+9abc-27a^2d+\sqrt{4\left(-b^2+3ac\right)^3+\left(-2b^3+9abc-27a^2d\right)^2}\right)^{1/3}}{3\times 2^{1/3}a}\right\},\right.$$

$$\left\{x \to -\frac{b}{3a} + \frac{\left(1+i\sqrt{3}\right)\left(-b^2+3ac\right)}{3\times 2^{2/3}a\left(-2b^3+9abc-27a^2d+\sqrt{4\left(-b^2+3ac\right)^3+\left(-2b^3+9abc-27a^2d\right)^2}\right)^{1/3}} - \frac{\left(1-i\sqrt{3}\right)\left(-2b^3+9abc-27a^2d+\sqrt{4\left(-b^2+3ac\right)^3+\left(-2b^3+9abc-27a^2d\right)^2}\right)^{1/3}}{6\times 2^{1/3}a}\right\},$$

$$\left.\left\{x \to -\frac{b}{3a} + \frac{\left(1-i\sqrt{3}\right)\left(-b^2+3ac\right)}{3\times 2^{2/3}a\left(-2b^3+9abc-27a^2d+\sqrt{4\left(-b^2+3ac\right)^3+\left(-2b^3+9abc-27a^2d\right)^2}\right)^{1/3}} - \frac{\left(1+i\sqrt{3}\right)\left(-2b^3+9abc-27a^2d+\sqrt{4\left(-b^2+3ac\right)^3+\left(-2b^3+9abc-27a^2d\right)^2}\right)^{1/3}}{6\times 2^{1/3}a}\right\}\right\}$$

One of three solutions to quartic $ax^4 + bx^3 + cx^2 + dx + e = 0$

wlog $a = 1$, $b = 0$
replace x with $x - r$ to shift
roots, can move to a new poly
with $b = 0$

```
Solve[a x^4 + b x^3 + c x^2 + d x + e == 0, x]
```

$$\left\{\left\{x \to -\frac{b}{4a} - \frac{1}{2}\sqrt{\frac{b^2}{4a^2} - \frac{2c}{3a} + \frac{\left(2^{1/3}\left(c^2 - 3bd + 12ae\right)\right)}{\left(3a\left(2c^3 - 9bcd + 27ad^2 + 27b^2e - 72ace + \sqrt{-4\left(c^2 - 3bd + 12ae\right)^3 + \left(2c^3 - 9bcd + 27ad^2 + 27b^2e - 72ace\right)^2}\right)^{1/3}\right)} + \frac{1}{3 \times 2^{1/3} a}\left(2c^3 - 9bcd + 27ad^2 + 27b^2e - 72ace + \sqrt{-4\left(c^2 - 3bd + 12ae\right)^3 + \left(2c^3 - 9bcd + 27ad^2 + 27b^2e - 72ace\right)^2}\right)^{1/3}} - \frac{1}{2}\sqrt{\frac{b^2}{2a^2} - \frac{4c}{3a} - \frac{\left(2^{1/3}\left(c^2 - 3bd + 12ae\right)\right)}{\left(3a\left(2c^3 - 9bcd + 27ad^2 + 27b^2e - 72ace + \sqrt{-4\left(c^2 - 3bd + 12ae\right)^3 + \left(2c^3 - 9bcd + 27ad^2 + 27b^2e - 72ace\right)^2}\right)^{1/3}\right)} - \frac{1}{3 \times 2^{1/3} a}\left(2c^3 - 9bcd + 27ad^2 + 27b^2e - 72ace + \sqrt{-4\left(c^2 - 3bd + 12ae\right)^3 + \left(2c^3 - 9bcd + 27ad^2 + 27b^2e - 72ace\right)^2}\right)^{1/3} - \left(-\frac{b^3}{a^3} + \frac{4bc}{a^2} - \frac{8d}{a}\right) \Big/ \left(4\sqrt{\frac{b^2}{4a^2} - \frac{2c}{3a} + \frac{\left(2^{1/3}\left(c^2 - 3bd + 12ae\right)\right)}{\left(3a\left(2c^3 - 9bcd + 27ad^2 + 27b^2e - 72ace + \sqrt{-4\left(c^2 - 3bd + 12ae\right)^3 + \left(2c^3 - 9bcd + 27ad^2 + 27b^2e - 72ace\right)^2}\right)^{1/3}\right)} + \frac{1}{3 \times 2^{1/3} a}\left(2c^3 - 9bcd + 27ad^2 + 27b^2e - 72ace + \sqrt{-4\left(c^2 - 3bd + 12ae\right)^3 + \left(2c^3 - 9bcd + 27ad^2 + 27b^2e - 72ace\right)^2}\right)^{1/3}}}\right)\right\}\right\},$$

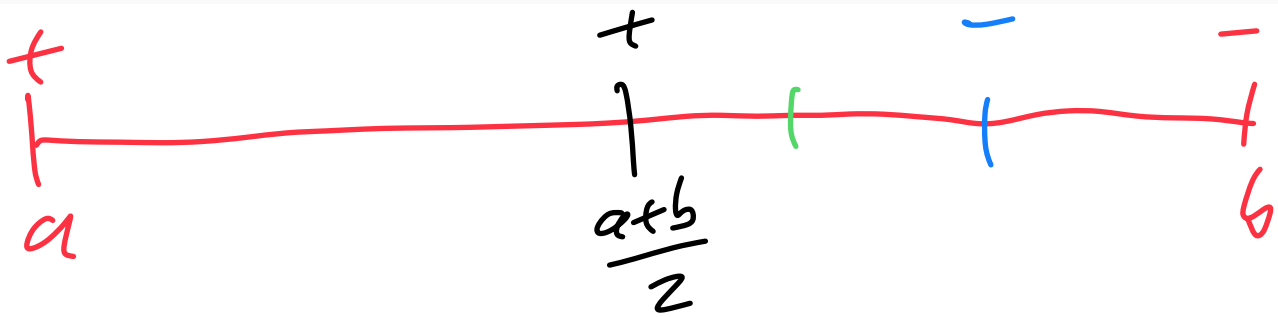
Divide and Conquer: Partial plot of continuous function $f(x)$

Must cross x-axis b/w 0 and 1
↳ crosses at least once
↳ # crossings is odd



Divide and Conquer

Assume f is continuous, $f(a) < 0 < f(b)$. Then f has a root between a and b. To find, look at the sign of f at the midpoint $f\left(\frac{a+b}{2}\right)$; if sign positive look in $[a, \frac{a+b}{2}]$ and if negative look in $[\frac{a+b}{2}, b]$. Lather, rinse, repeat.



if do 10 times, size of final interval is $\frac{\text{original length}}{2^{10}} \approx \frac{\text{original length}}{1000}$

(0 iterations $\approx$ 3 decimal digits.

Divide and Conquer (continued)

How fast? Every 10 iterations uncertainty decreases by a factor of $2^{10} = 1024 \approx 1000$.

Thus 10 iterations essentially give three decimal digits.

		f(x) = x^2 - 3, sqrt(3)		1.732051		
n	left	right	f(left)	f(right)	left error	right error
1	1	2	-2	1	0.732051	-0.26795
2	1.5	2	-0.75	1	0.232051	-0.26795
3	1.5	1.75	-0.75	0.0625	0.232051	-0.01795
4	1.625	1.75	-0.35938	0.0625	0.107051	-0.01795
5	1.6875	1.75	-0.15234	0.0625	0.044551	-0.01795
6	1.71875	1.75	-0.0459	0.0625	0.013301	-0.01795
7	1.71875	1.734375	-0.0459	0.008057	0.013301	-0.00232
8	1.726563	1.734375	-0.01898	0.008057	0.005488	-0.00232
9	1.730469	1.734375	-0.00548	0.008057	0.001582	-0.00232
10	1.730469	1.732422	-0.00548	0.001286	0.001582	-0.00037

Figure: Approximating $\sqrt{3} \approx 1.732050807568877293527446341 51$.

Tangent Line

One of most important uses of calculus; approximate a curve by a straight line.

Locally good: for small changes in time, speed approximately constant.

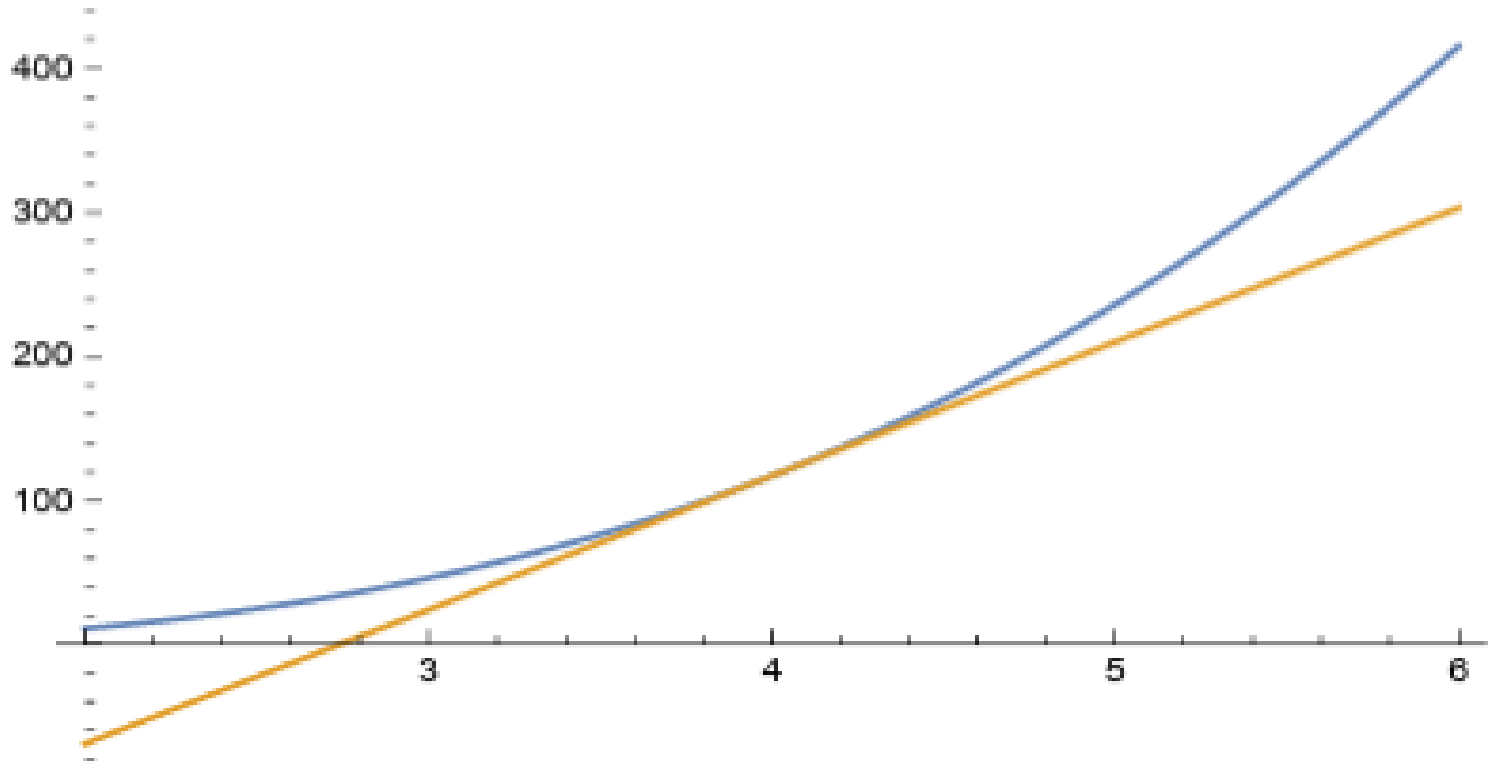
New location $f(x)$ is approximately $f(x_0) + f'(x_0)(x - x_0)$ (where start plus speed at x_0 times elapsed time).

Get the tangent line by Point-Slope: $P = (x_0, f(x_0))$ and slope $m = f'(x_0)$.

Tangent Line

New location $f(x)$ is approximately $f(x_0) + f'(x_0)(x - x_0)$ (where start plus speed at x_0 times elapsed time).

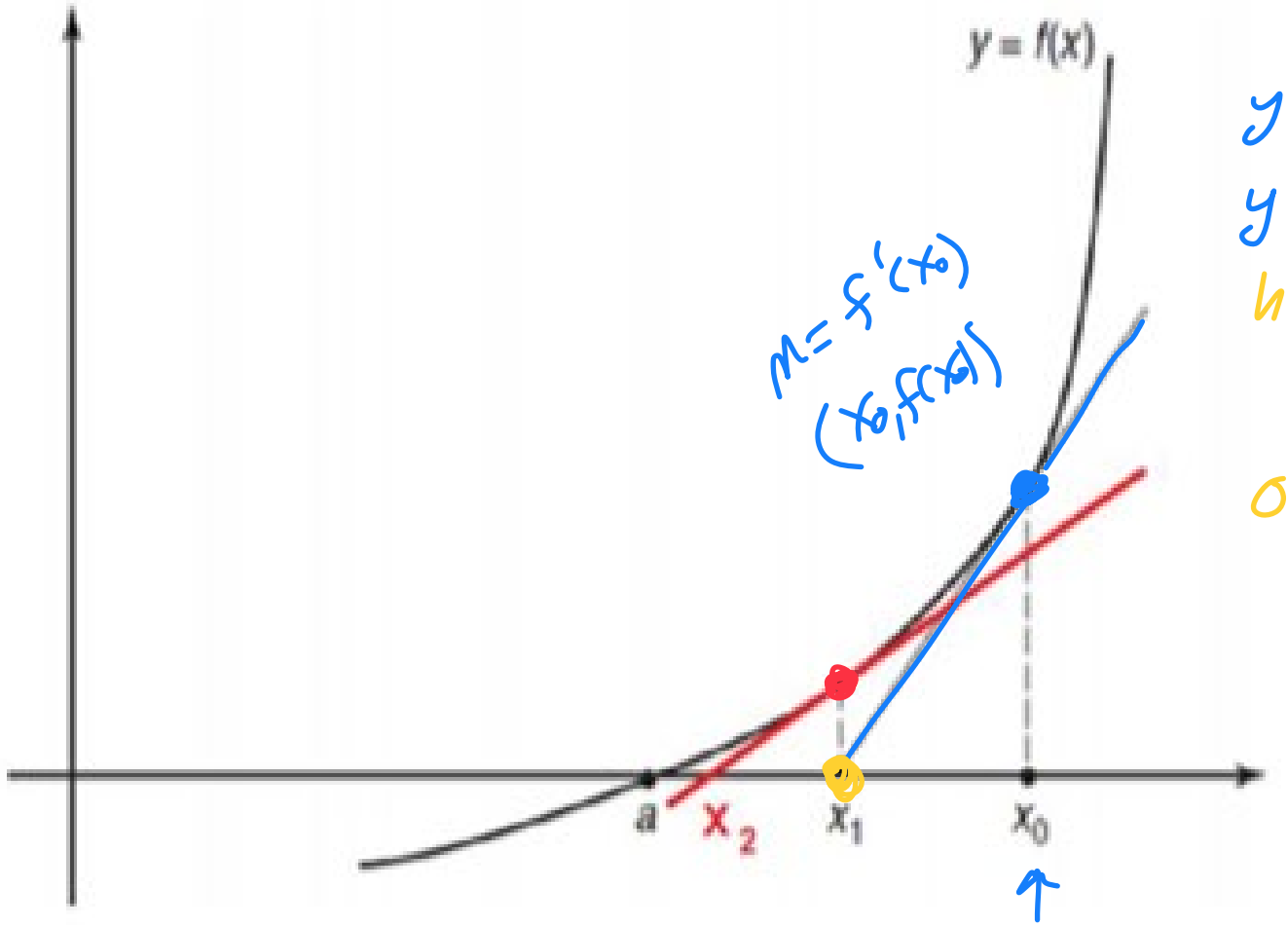
Get the tangent line by Point-Slope: $P = (x_0, f(x_0))$ and slope $m = f'(x_0)$.
$f(x) = 2x^3 - 3x + 1$, $f'(x) = 6x^2 - 3$, $x_0 = 4$.



Newton's Method

Assume f is continuous and differentiable. We generate a sequence hopefully converging to the root of $f(x) = 0$ as follows. Given x_n, look at the tangent line to the curve $y = f(x)$ at x_n; it has slope $f'(x_n)$ and goes through $(x_n, f(x_n))$ and gives line $y - f(x_n) = f'(x_n)(x - x_n)$. This hits the x-axis at $y = 0, x = x_{n+1}$, and yields $x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)}$.

Newton's Method



$y - y_0 = m(x - x_0)$

$y - f(x_0) = f'(x_0)(x - x_0)$

hits at a point

$(x_1, 0)$

$0 - f(x_0) = f'(x_0)(x_1 - x_0)$

$x_1 - x_0 = -\frac{f(x_0)}{f'(x_0)}$

$x_1 = x_0 - \frac{f(x_0)}{f'(x_0)}$

need $f'(x_0) \neq 0$

Newton's Method

$x_1 = x_0 - \frac{f(x_0)}{f'(x_0)}$

$x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)}$

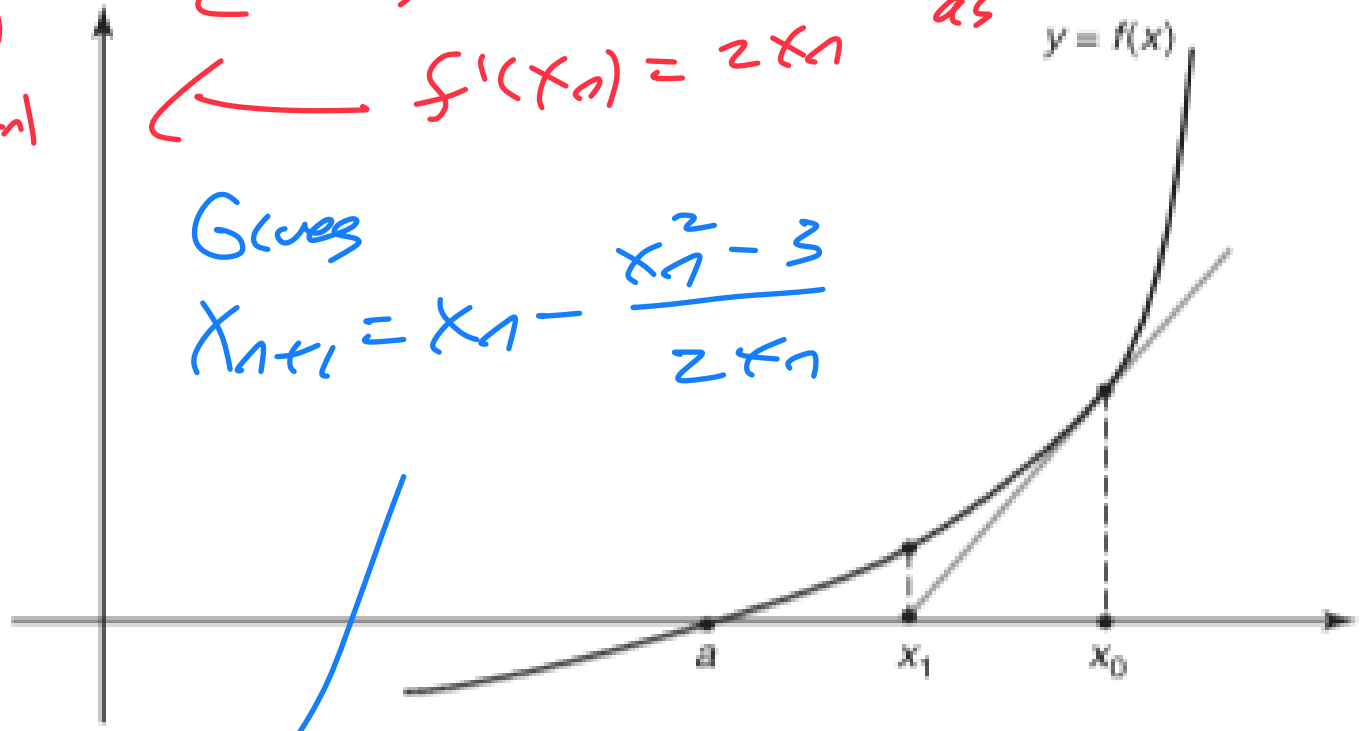
$f(x) = x^2 - 3$ roots are $\pm\sqrt{3}$

$f(x_n) = x_n^2 - 3$

$f'(x_n) = 2x_n$ as $f'(x) = 2x$

Gives

$$x_{n+1} = x_n - \frac{x_n^2 - 3}{2x_n}$$



looking for root of $x^2 - 3 = 0$ or $\pm\sqrt{3}$

Lucky if $x_n = \sqrt{3}$

$x_{n+1} = \frac{1}{2}\left(\sqrt{3} + \frac{3}{\sqrt{3}}\right)$

$= \frac{1}{2}(\sqrt{3} + \sqrt{3})$

$= \sqrt{3}$

Stable!

For example, $f(x) = x^2 - 3$ after algebra get

$$x_{n+1} = \frac{1}{2}\left(x_n + \frac{3}{x_n}\right).$$

is this reasonable?

Doing the algebra: Approximating roots of $f(x) = 0$

Have n^{th} approx x_n to the root of $f(x) = 0$, want next, x_{n+1}.
Tangent line $y = f(x)$ at point $(x_n, f(x_n))$ with slope $m = f'(x_n)$:

$$y = f(x_n) + f'(x_n)(x - x_n).$$

Tangent line hits x-axis when $y = 0$, call that x_{n+1}, so

$$0 = f(x_n) + f'(x_n)(x_{n+1} - x_n).$$

If $f(x) = x^2 - 3$: $f'(x) = 2x$, $f(x_n) = 2x_n^2 - 3$, $f'(x_n) = 2x_n$:

$$-\frac{f(x_n)}{f'(x_n)} = x_{n+1} - x_n \quad \text{or} \quad x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)}, \quad \text{thus}$$

$$x_{n+1} = x_n - \frac{x_n^2 - 3}{2x_n} = \frac{2x_n^2 - x_n^2 + 3}{x_n} = \frac{1}{2}\left(x_n + \frac{3}{x_n}\right).$$

Rational Approximations: $\sqrt{3} = 1.7320508076\ldots$

$$x_{n+1} = \frac{1}{2}\left(x_n + \frac{3}{x_n}\right)$$

$$x_0 = 2$$

$$x_1 = \frac{1}{2}\left(x_0 + \frac{3}{x_0}\right) = \frac{1}{2}\left(2 + \frac{3}{2}\right) = \frac{7}{4} = 1.75$$

$$x_2 = \frac{1}{2}\left(x_1 + \frac{3}{x_1}\right) = \frac{1}{2}\left(\frac{7}{4} + \frac{12}{7}\right) = \frac{1}{2}\left(\frac{49+48}{28}\right)$$

$$= \frac{97}{56} \approx 1.7321\ldots$$

Rational Approximations: $\sqrt{3} = 1.7320508076\ldots$

$$x_{n+1} = \frac{1}{2}\left(x_n + \frac{3}{x_n}\right)$$

$$x_0 = 2$$

$$x_1 = \frac{1}{2}\left(2 + \frac{3}{2}\right) = \frac{7}{4} = 1.75$$

$$x_2 = \frac{1}{2}\left(\frac{7}{4} + \frac{3}{7/4}\right) = \frac{97}{56} \approx 1.732142857\ldots$$

$$x_3 = \frac{1}{2}\left(\frac{97}{56} + \frac{3}{97/56}\right) = \frac{18817}{10864} \approx 1.7320508100$$

Newton's Method

n	x[n]	1.0 x[n]	Sqrt[3] - x[n]
0	2	2.0000000000000000000000000000000000000000	-0.26794919243112270647255365849412763305 7
1	$\frac{7}{4}$	1.7500000000000000000000000000000000000000	-0.01794919243112270647255365849412763305 7
2	$\frac{97}{56}$	1.7321428571428572062984585500089451670 65	-0.00009204957397984932969651563698477591 4
3	$\frac{18817}{10864}$	1.7320508100147276042690691610914655029774	$-2.44585024697329003551916445190 8 \times 10^{-9}$

Sqrt[3] = 1.7320508075688772935274463415058723669428

x[5] = 1.7320508075688772935274463415058723678037

x[4] = 1.7320508075688772952543539460721719142351

$$\sqrt{3} = 1.7320508075688772935274463415058723669428$$

$$x_5 = 1.7320508075688772935274463415058723678037$$

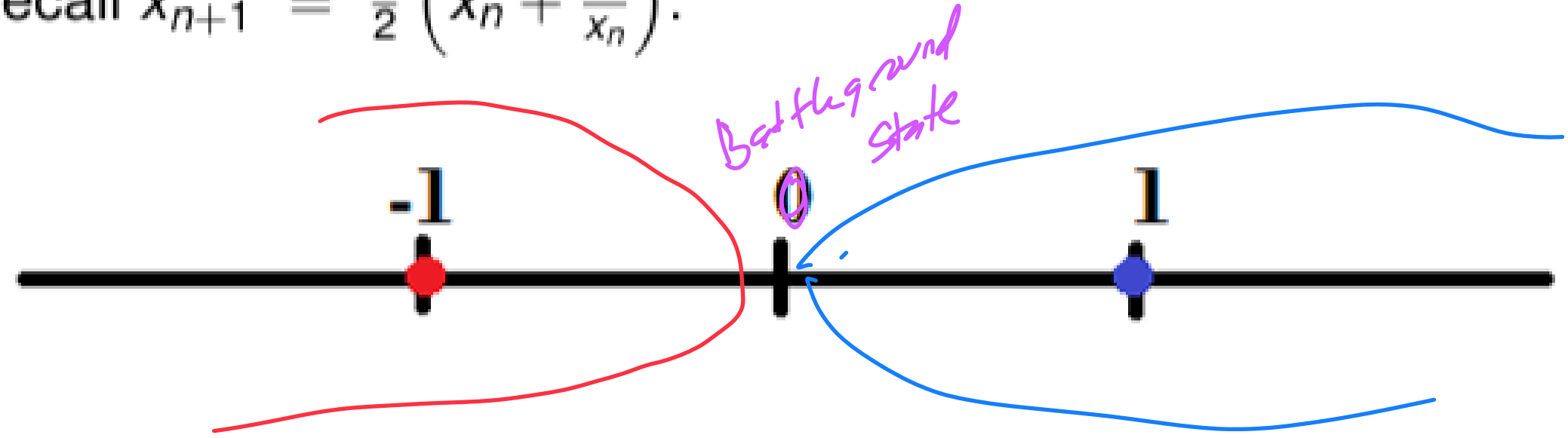
$$x_5 = \frac{100297827341137305 7}{5790697761454023 04}.$$

Newton Method: $x^2 - 3 = 0$

Consider $x^2 - 1 = (x - 1)(x + 1) = 0$.

Roots are 1, -1; if we start at a point x_0 do we approach a root? If so which?

Recall $x_{n+1} = \frac{1}{2}\left(x_n + \frac{1}{x_n}\right)$.

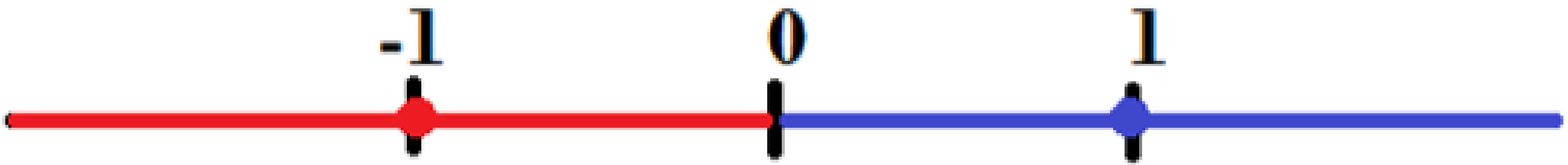


Newton Method: $x^2 - 3 = 0$

Consider $x^2 - 1 = (x - 1)(x + 1) = 0$.

Roots are 1, -1; if we start at a point x_0 do we approach a root? If so which?

Recall $x_{n+1} = \frac{1}{2}\left(x_n + \frac{1}{x_n}\right)$.



What are the roots to $x^3 - 1 = 0$?

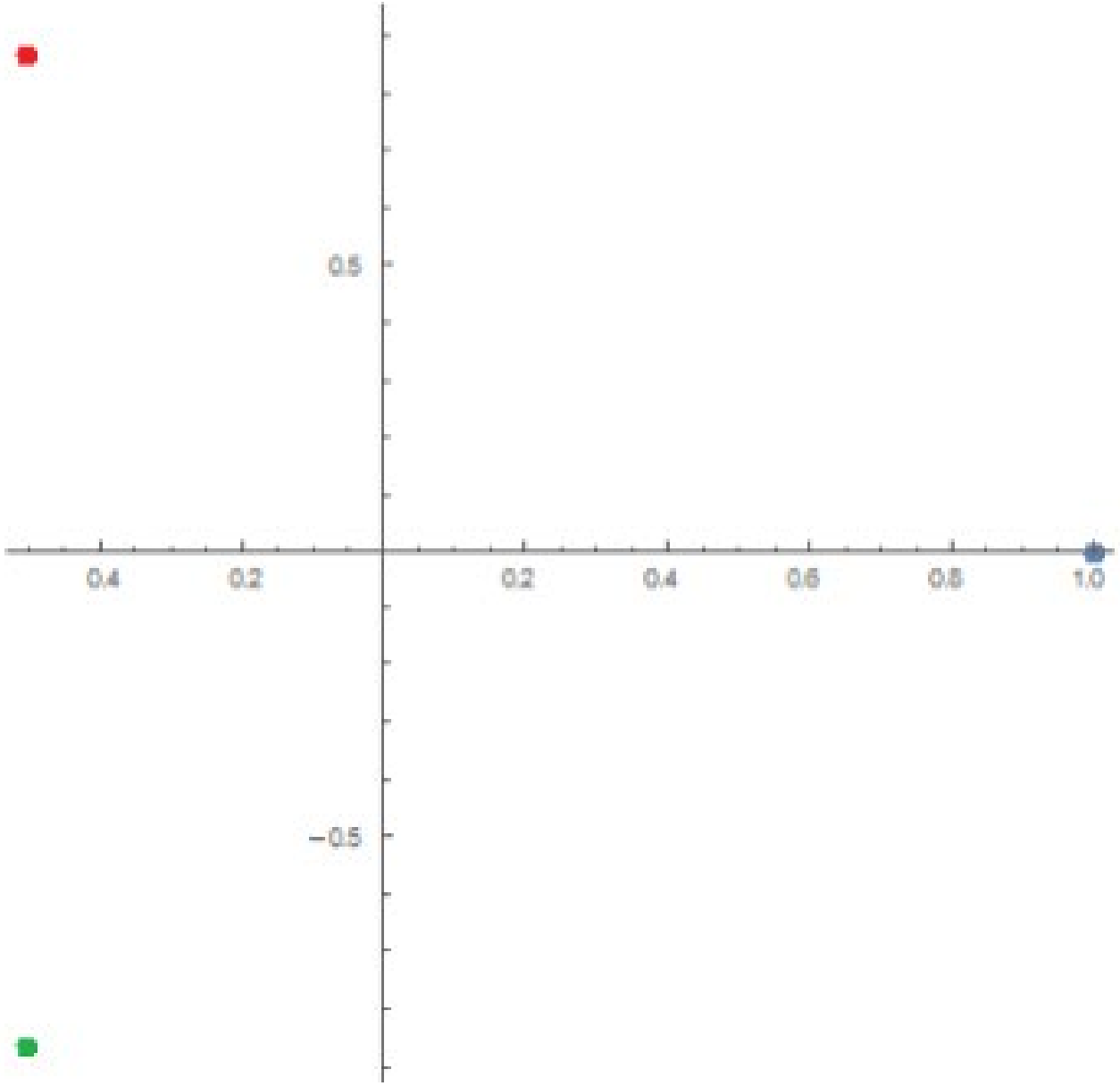
Here comes Complex Numbers!

$\mathbb{C} = \{x + iy : x, y \in \mathbb{R}, i = \sqrt{-1}\}$.

$$
\begin{aligned}
x^3 - 1 &= (x-1)(x^2 + x + 1) \\
&= (x-1) \cdot \left(x - \frac{-1 + \sqrt{1^2 - 4 \cdot 1 \cdot 1}}{2}\right) \cdot \left(x - \frac{-1 - \sqrt{1^2 - 4 \cdot 1 \cdot 1}}{2}\right) \\
&= (x-1) \cdot \left(x - \frac{-1 + \sqrt{-3}}{2}\right) \cdot \left(x - \frac{-1 - \sqrt{-3}}{2}\right) \\
&= (x-1) \cdot \left(x - \frac{-1 + i\sqrt{3}}{2}\right) \cdot \left(x - \frac{-1 - i\sqrt{3}}{2}\right).
\end{aligned}
$$

Roots are $1,\ -1/2 + i\sqrt{3}/2,\ -1/2 - i\sqrt{3}/2$.

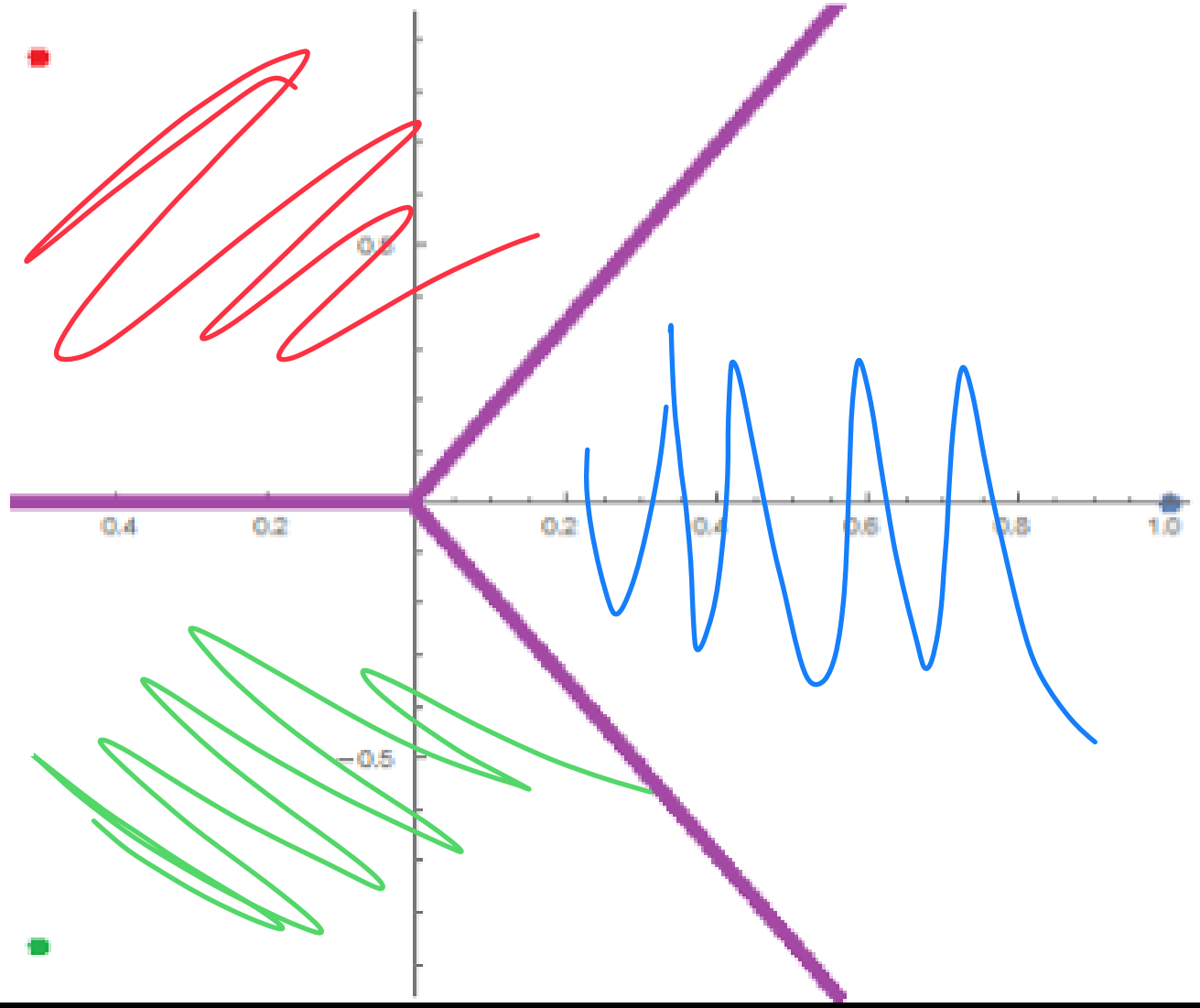
If start at (x, y), what root do you iterate to?



Newton Fractal: $x^3 - 1 = 0$:

https://www.youtube.com/watch?v=ZsFixqGFNRc

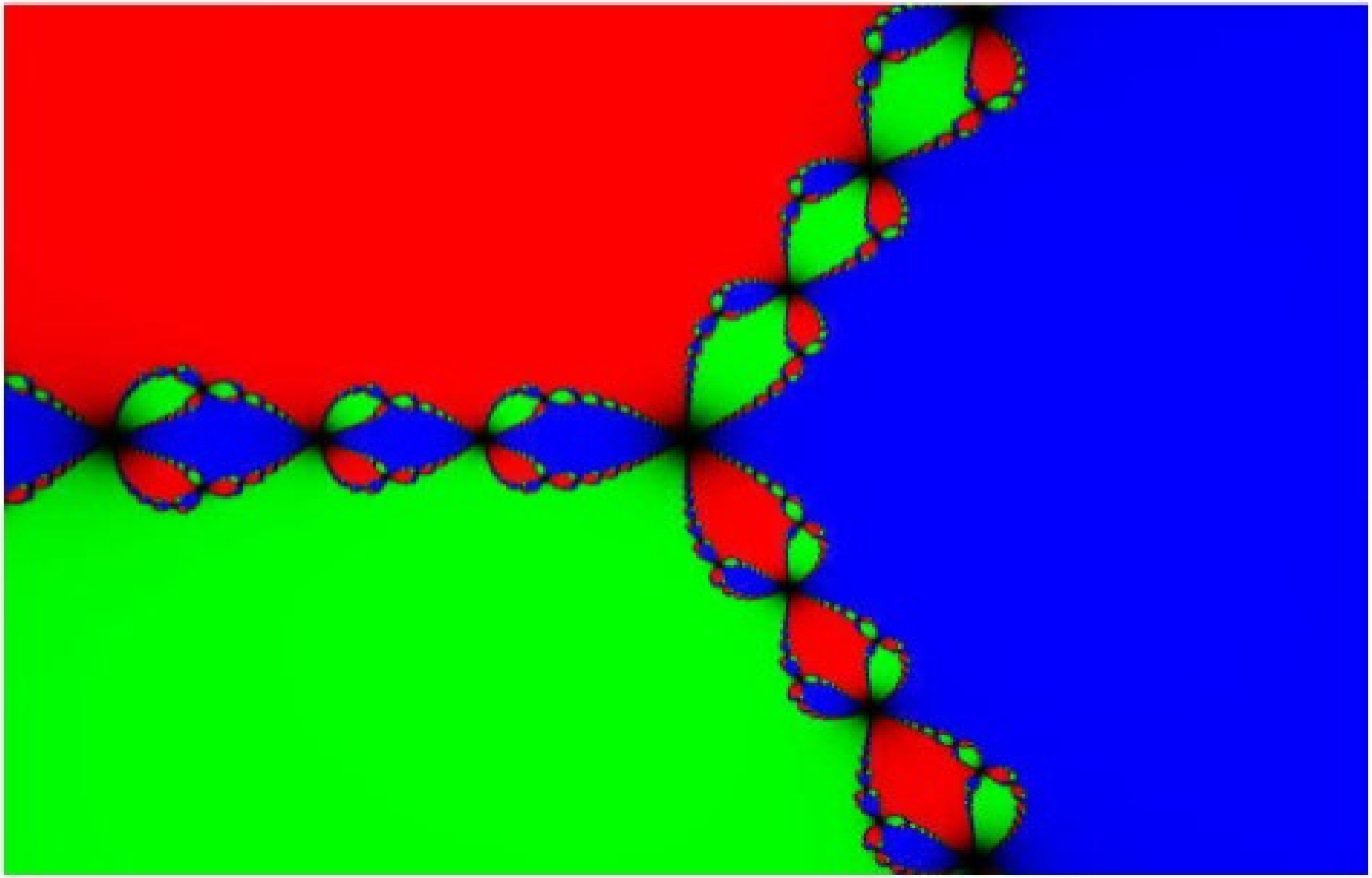
If start at (x, y), what root do you iterate to? Guess



Newton Fractal: $x^3 - 1 = 0$:

https://www.youtube.com/watch?v=ZsFixqGFNRc

https://www.youtube.com/watch?v=ZsFixqGFNRc



From C to Shining C: Complex Dynamics from Combinatorics to Coastlines, Maritime Studies Program of Williams College and Mystic Seaport, Mystic, CT, October 20, 2017. pdf (video here: https://youtu.be/TMILk79N_Bs) Michigan Math Circle, April 30, 2020. pdf Hampshire College 8/8/2022 (video: https://youtu.be/GO3EbWUesBQ) pdf

Mandelbrot Set:

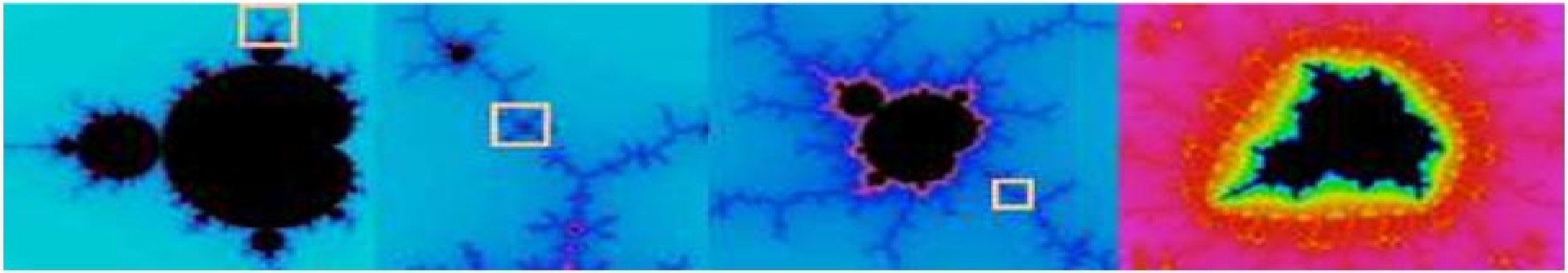
https://www.youtube.com/watch?v=0jGaio87u3A

Definition: Set of all complex numbers $c = x + iy$ $(i = \sqrt{-1})$ such that if $f_c(u) = u^2 + c$ then the sequence

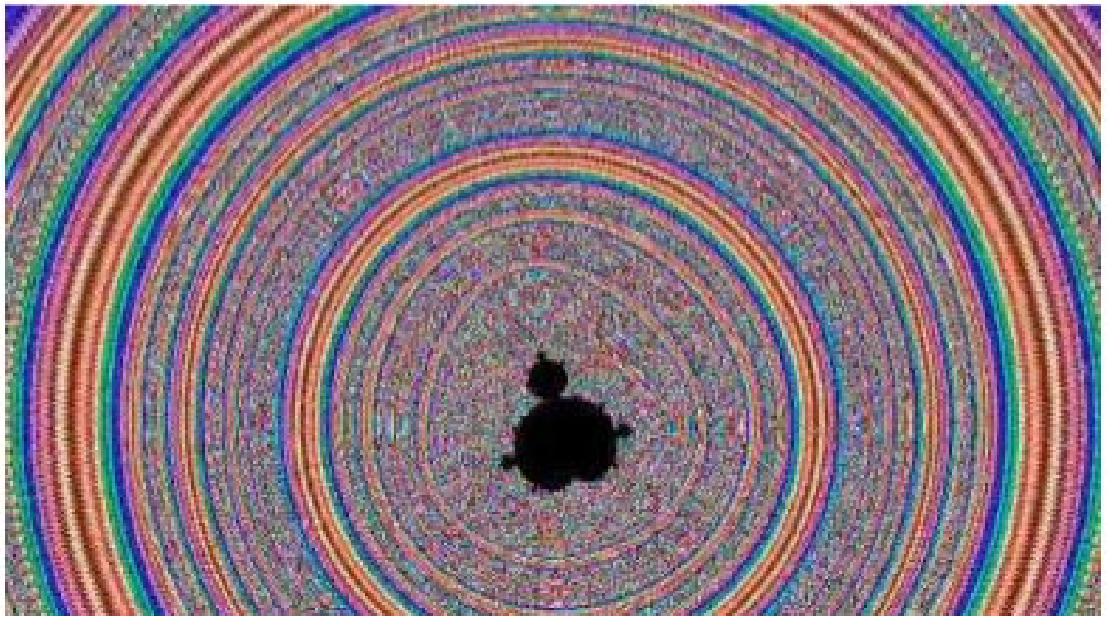
$$z_1 = f_c(0), \quad z_2 = f_c(z_1) = f_c(f_c(0)), \quad \cdots, \quad z_{n+1} = f_c(z_n)$$

remains bounded as $n \to \infty$.

Zooming in....



Extreme zoom!



https://www.youtube.com/watch?v=0jGaio87u3A

https://www.youtube.com/watch?v=9j2yV1nLCEI

https://www.youtube.com/watch?v=ZsFixqGFNRc

https://www.youtube.com/watch?v=PD2XgQOyCCk

https://www.youtube.com/watch?v=vfteiiTfE0c

Math 310: Modern Algebra: Fall '25 (Siena)

Professor Steven J Miller: sjm1@williams.edu

Homepage:

https://web.williams.edu/Mathematics/sjmiller/public_html/310Fa25/

Lecture 18: 10/30/25:

https://youtu.be/ctKaCKfjxUs

More Groups, Benford's Law

Abel–Ruffini theorem

From Wikipedia, the free encyclopedia

https://en.wikipedia.org/wiki/Abel%E2%80%93Ruffini_theorem

Not to be confused with Abel's theorem.

In mathematics, the **Abel–Ruffini theorem** (also known as **Abel's impossibility theorem**) states that there is no solution in radicals to general polynomial equations of degree five or higher with arbitrary coefficients. Here, *general* means that the coefficients of the equation are viewed and manipulated as indeterminates.

The theorem is named after Paolo Ruffini, who made an incomplete proof in 1799[1] (which was refined and completed in 1813[2] and accepted by Cauchy) and Niels Henrik Abel, who provided a proof in 1824.[3][4]

The term can also refer to the slightly stronger result that there are equations of degree five and higher that cannot be solved by radicals. This does not follow from Abel's statement of the theorem, but is a corollary of his proof, as his proof is based on the fact that some polynomials in the coefficients of the equation are not the zero polynomial. This improved statement follows directly from Galois theory § A non-solvable quintic example. Galois theory implies also that

$$x^5 - x - 1 = 0$$

is the simplest equation that cannot be solved in radicals, and that *almost all* polynomials of degree five or higher cannot be solved in radicals.

The impossibility of solving in degree five or higher contrasts with the case of lower degree: one has the quadratic formula, the cubic formula, and the quartic formula for degrees two, three, and four, respectively.

Definition 6.1. Let G be a group, and let H be a subgroup of G. We denote the set of (left) cosets of G by

$$G/H = \{\text{(left) cosets of } H\}.$$

Ex: $G = \mathbb{Z}$ $H = 12\mathbb{Z}$

$\mathbb{Z}/12\mathbb{Z} = \{0+H, 1+H, \ldots, 11+H\}$

Maybe G/H is a group

↳ to understand G:
↳ understand H
↳ understand G/H
↳ understand putting together

Break into simpler pieces

Definition 6.2 (Proposed Coset Multiplication Algorithm)**.** Let G be a group, and let H be a subgroup of G.

Input:	Cosets $\mathcal{C}_1$ and $\mathcal{C}_2$ of H.
Computation:	Choose an element $g_1 \in \mathcal{C}_1$ and an element $g_2 \in \mathcal{C}_2$.
Output:	The coset $g_1 g_2 H$ containing the product $g_1 g_2$.

Recall: two cosets are the same or disjoint

$\mathbb{Z}/12\mathbb{Z}$ $3+12\mathbb{Z}$ and $8+12\mathbb{Z}$

$\Downarrow$ $\Downarrow$

3 or 15 8 or 20

$(3,8)12\mathbb{Z} = (24)12\mathbb{Z}$ is this $12\mathbb{Z}$?

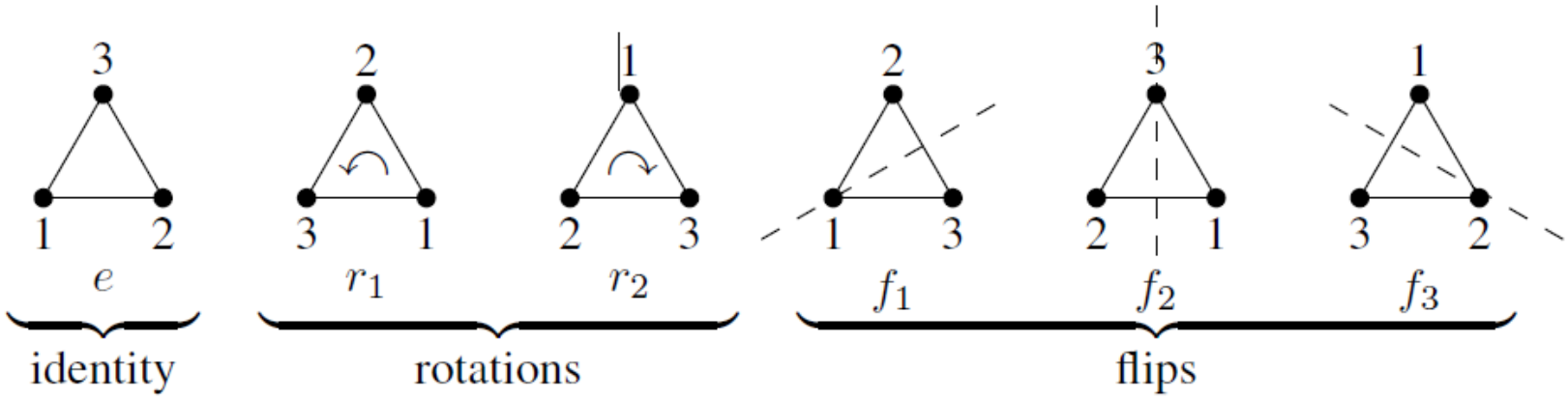
$12\mathbb{Z} = \{\ldots, -24, -12, 0, 12, 24, \ldots\}$

$(24)12\mathbb{Z}$ is the unique coset containing 24

Example 2.46. We consider the dihedral group

$$\mathcal{D}_3 = \{e, r_1, r_2, f_1, f_2, f_3\}$$

associated to an equilateral triangle; cf. Example 2.22. As illustrated in Figure 8, it contains two rotations r_1 and r_2 and three flips (reflections) f_1, f_2, f_3.



ways to reorder {1,2,3} is 3! = 6

$r_1 f_1 \stackrel{?}{=} f_1 r_1$

$\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix} = \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix} \neq \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix} = \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$

Subgroups: $\mathcal{D}_3, \{e\}, \{e, r_1, r_1^2\}, \{e, r_2, r_2^2\}, \{e, f_1\}, \{e, f_2\}, \{e, f_3\}$

any other subgroups? Normal?

For all cosets $\mathcal{C}_1$ and $\mathcal{C}_2$ of H, for all pairs of elements $g_1, g_1' \in \mathcal{C}_1$, and for all pairs of elements $g_2, g_2' \in \mathcal{C}_2$, we want it to be true that

$$g_1 g_2 H = g_1' g_2' H.$$

$g_1 g_2 H$ vs $g_1' g_2' H$

$g_1, g_1' \in \mathcal{C}_1$: means $g_1 = a_1 + h_1$

$g_1' = a_1 + h_1'$

Definition 6.5. Let G be a group, let $H \subset G$ be a subgroup, and let $g \in G$. The *g-conjugate of H* is the subgroup

$$g^{-1}Hg = \{g^{-1}hg : h \in H\}.$$

We say that H is a *normal subgroup of G* if it satisfies

$$g^{-1}Hg = H \quad \text{for every } g \in G.$$

If G is abelian, then $g^{-1}Hg = H$

Example 6.6. If G is an abelian group, then every subgroup $H \subseteq G$ is normal, since $g^{-1}hg = h$.

Explore!

$\mathbb{Z}/n\mathbb{Z}$: should things be normal? YES!

If $g^{-1}Hg = H$ then given any $x \in H$ $g^{-1}xg = \tilde{x} \in H$

or $xg = g\tilde{x}$ $x, \tilde{x} \in H$

not saying $xg = gx$ says $xg = g\tilde{x}$, x and $\tilde{x}$ both in H

Proposition 6.9. *Let $\phi : G \to G'$ be a homomorphism of groups. Then $\ker(\phi)$ is a normal subgroup of G.*

ϕ homomorphism: $\phi(g_1 g_2) = \phi(g_1)\phi(g_2)$

(By induction $\phi(g_1 \cdots g_n) = \phi(g_1) \cdots \phi(g_n)$)

Know $\phi(e) = e'$

$\ker(\phi) = \{g \in G : \phi(g) = e'\}$

Showed earlier is a subgroup.

Consider $g^{-1}\ker(\phi)g$: does this equal $\ker(\phi)$

↳ consider $x \in g^{-1}\ker(\phi)g$: $\exists\, y \in \ker(\phi)$ s.t. $x = g^{-1}yg$

$\phi(g^{-1}yg) = \phi(g^{-1})\underbrace{\phi(y)}_{e'}\phi(g)$

$= \phi(g^{-1})e'\phi(g) = \phi(g^{-1})\phi(g) = \phi(g^{-1}g)$

$= \phi(e) = e'$ ∎

Proposition 6.10. *Let G be a group, and let $H \subset G$ be a subgroup.*

(a) *If $g^{-1}Hg \subseteq H$ for all $g \in G$, then H is a normal subgroup of G; i.e., it is enough to check one inclusion.*

(b) *For all $g \in G$, the conjugate set $g^{-1}Hg$ is a subgroup of G.*

(c) *For all $g \in G$, the map $H \to g^{-1}Hg$ defined by $h \mapsto g^{-1}hg$ is a group isomorphism. In particular, if H is finite, then H and its conjugates have the same number of elements.*

Try to prove

a) Why is it enough to do $g^{-1}Hg \subseteq H$ for all g?

↳ Trick: Instead of g take g^{-1}: $(g^{-1})^{-1} H g^{-1} \subseteq H$

As $(g^{-1})^{-1} = g$ get $gHg^{-1} \subseteq H$ or $H \subseteq g^{-1}Hg$

by mult on the left by g^{-1} and right by g.

Lemma 6.11. *Let G be a group, and let H be a normal subgroup of G. Suppose taht $g_1, g_1', g_2, g_2' \in G$ satisfy*

$$g_1'H = g_1H \quad \text{and} \quad g_2'H = g_2H.$$

Then

$$g_1'g_2'H = g_1g_2H.$$

Exercise: Prove if H is a subgroup and $h \in H$ then $hH = H$

H could be a group

If H is a group, is $HH = H$?

↳ As $e \in H$: $e \cdot H \subset HH$ so $H \subset HH$

↳ by closure $h_1, h_2 \in H \to h_1h_2 \in H \implies HH \subset H$: YES!

If $g_1'H = g_1H$ means $g_1'e = g_1h_1$ for some $h_1 \in H$

So $g_1' = g_1h_1$ and $g_2' = g_2h_2$ for some $h_1, h_2 \in H$

$g_1'g_2'H = g_1(h_1g_2h_2)H$ hope $h_1g_2 = g_2\tilde{h}_1$

since normal: $h_1g_2 = g_2\tilde{h}_1$

Thus $g_1'g_2'H = g_1g_2\tilde{h}_1h_2H = g_1g_2H$

Theorem 6.12. *Let G be a group, and let H be a normal subgroup of G.*

(a) *The collection of cosets G/H is a group via the well-defined group operation*

$$g_1H \cdot g_2H = g_1g_2H. \tag{6.7}$$

(b) *The map*

$$\phi : G \longrightarrow G/H, \quad \phi(g) = gH,$$

is a homomorphism whose kernel is $\ker(\phi) = H$.

(c) *Let*

$$\psi : G \longrightarrow G'$$

be a homomorphism with the property that $H \subseteq \ker(\psi)$. Then there is a unique homomorphism

$$\lambda : G/H \longrightarrow G' \quad \textit{satisfying} \quad \lambda(gH) = \psi(g).$$

(d) *If we take $H = \ker(\psi)$ in* (c)*, then the homomorphism*

$$\lambda : G/\ker(\psi) \longrightarrow G'$$

is injective. In particular, we get an isomorphism

$$\lambda : G/\ker(\psi) \xrightarrow{\text{isomorphism}} \text{Image}(\lambda) \subseteq G'.$$

Chapter 8: Fields — Part 2

8.1. Algebraic Numbers and Transcendental Numbers

Definition 8.1. Let L/F be an extension of fields, and let $\alpha \in L$. We say that α is *algebraic over* F if α is the root of a non-zero polynomial in $F[x]$. Otherwise we say that α is *transcendental over* F.

Who cares about such small differences?
First 125 digits of some famous numbers….

3.14159265358979323846264338327950288419716939937510582097494459230781640628620899
86280348253421170679821480865132823066470938446095505 82

$= \pi$

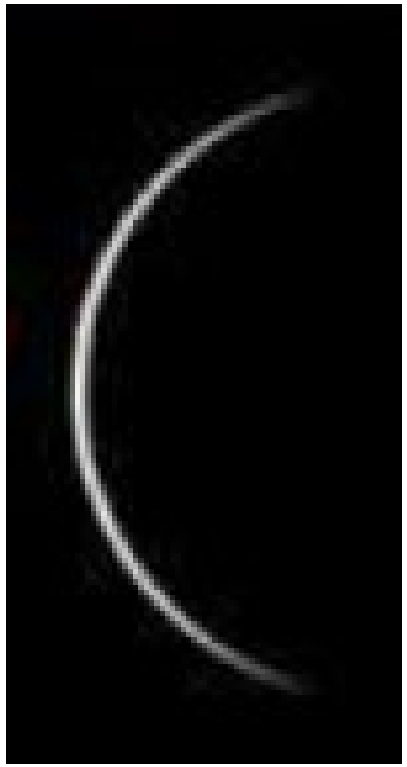
0.21000100000000000000010000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000010000000000000

Liouville's constant $\sum 10^{-n!}$

1.73205080756887729352744634150587236780342043159474350440560235337023472538513619 67287407483961914067549514584243297576904296 9

$= \sqrt{3}$

So I can see 96% of the eclipse here, I don't think it's worth driving 90 minutes for just 4%.





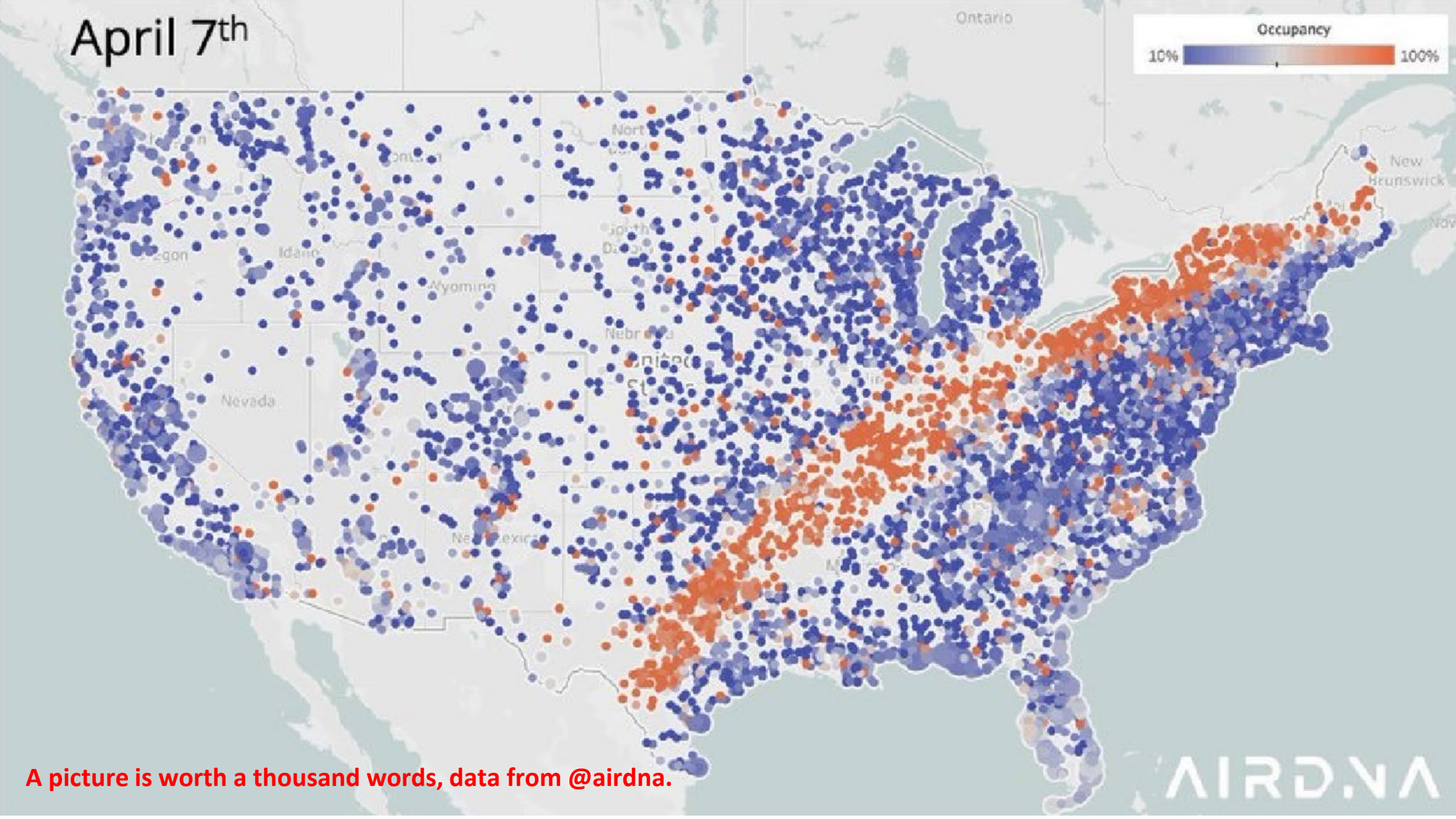

First from https://i.ytimg.com/vi/0TLAG0IeQBE/hqdefault.jpg, second from https://www.nbcnews.com/news/us-news/total-solar-eclipse-photos-2024-rcna146832 (Forth Worth), last two by me (Middlebury, VT): April 8, 2024.

Main term can dwarf lower order terms….





First from me (April 8, 2024 at Middlebury, VT); second from https://www.wgauradio.com/news/national/missing-totality/OJDGRCOH5DJLHO3FXJK2UMW3QQ/



A picture is worth a thousand words, data from @airdna.

Adjust to changing times….

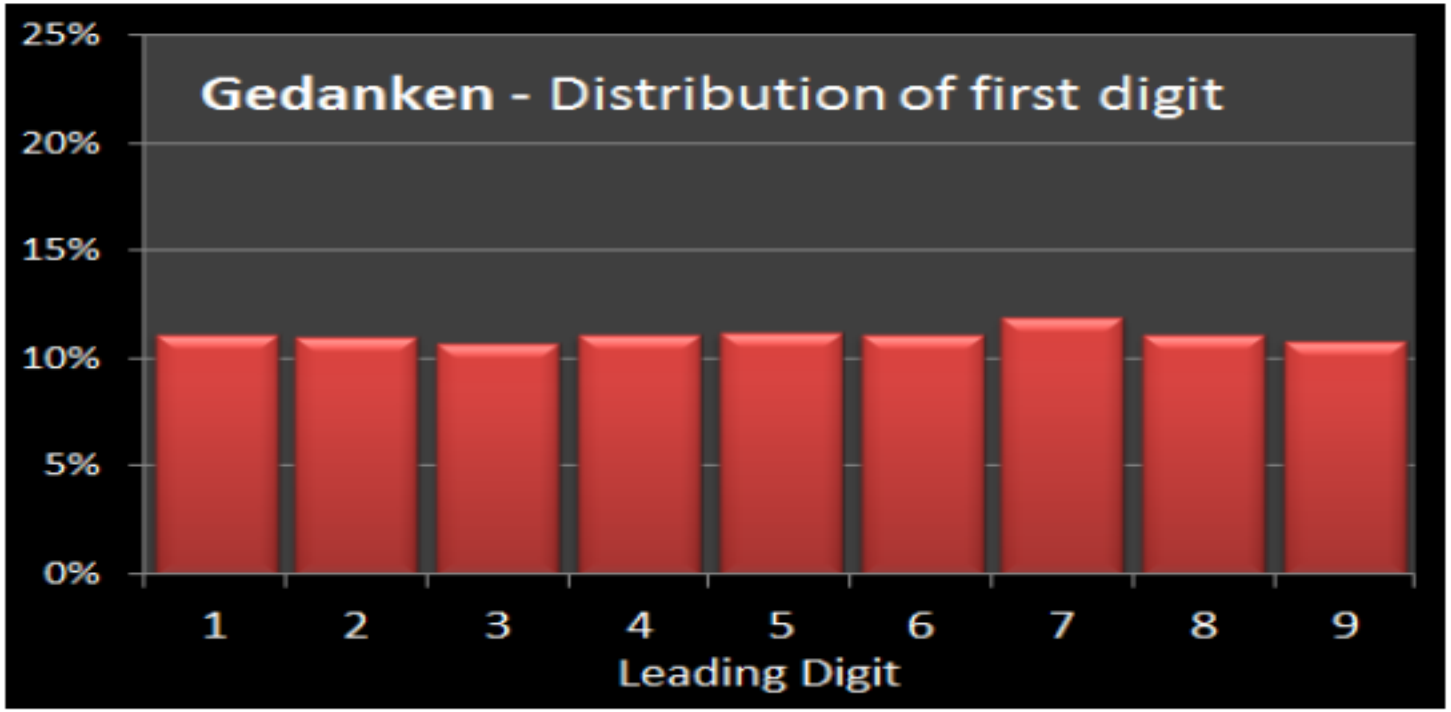




Left is inn we stayed at, took almost an hour to check in b/c only one person could handle the computer for arrivals.
Right is a froyo place, normally closed on Mondays, called and said open as today is the eclipse, huge crowds, went twice!

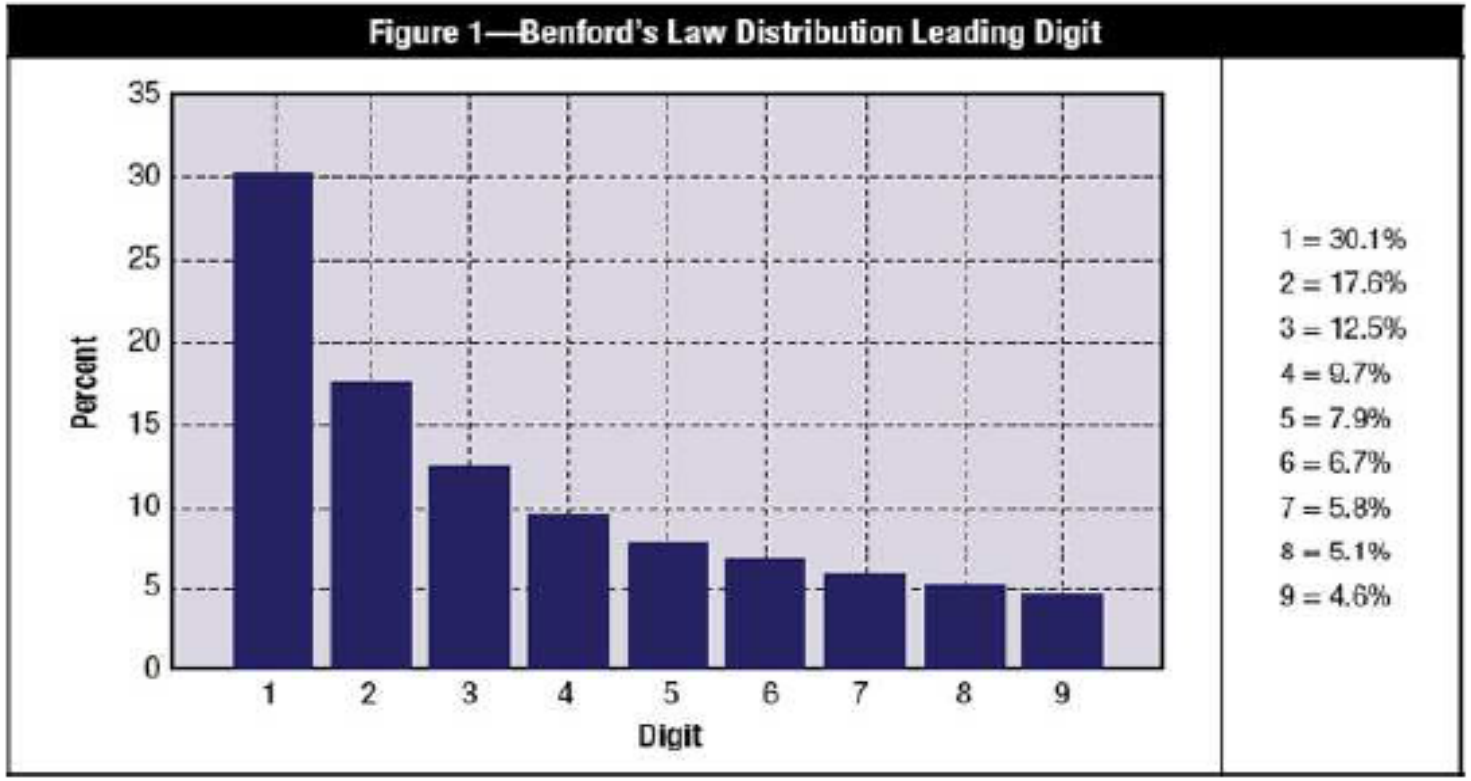
Benford's Law: Why the IRS and others care about Number Theory (and you should too!), PIMS Distinguished Lecture, UNBC, November 4, 2020 (https://youtu.be/NSuXJRIFcXc). pdf Vassar College pdf (https://youtu.be/fm3s-xjcnAE).

Motivating Question: For a nice data set, such as the Fibonacci numbers, stock prices, street addresses of college employees and students, ..., what percent of the leading digits are 1?



Natural guess: 10% (but immediately correct to 11%!).

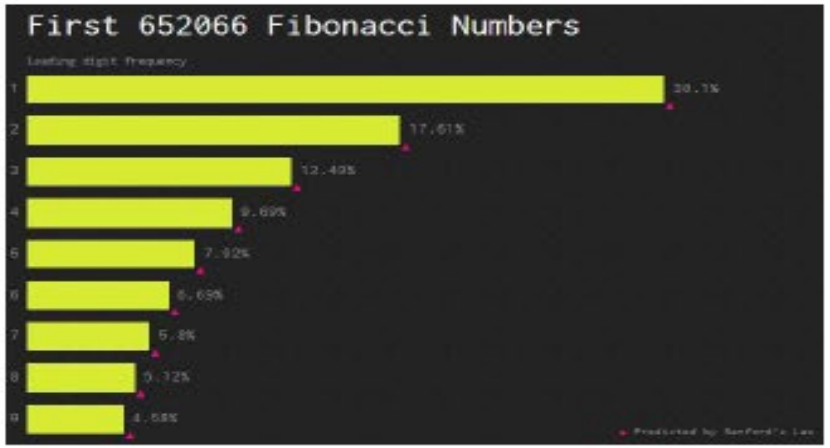
Motivating Question: For a nice data set, such as the Fibonacci numbers, stock prices, street addresses of college employees and students, ..., what percent of the leading digits are 1?



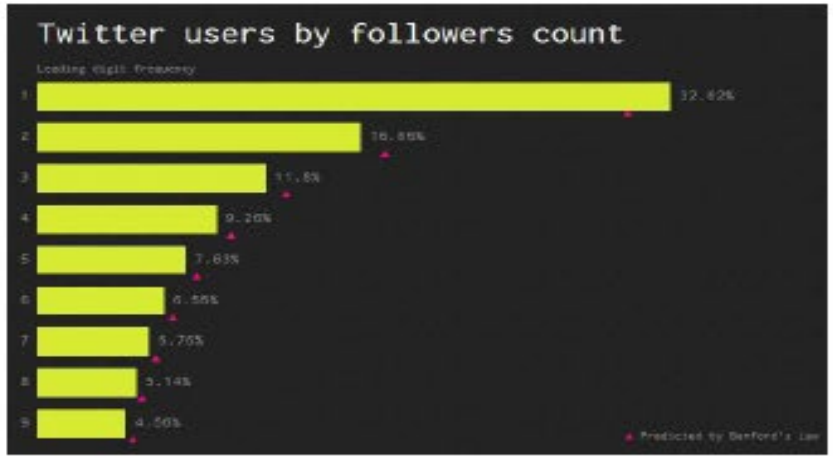
Answer: Benford's law!

Examples with First Digit Bias

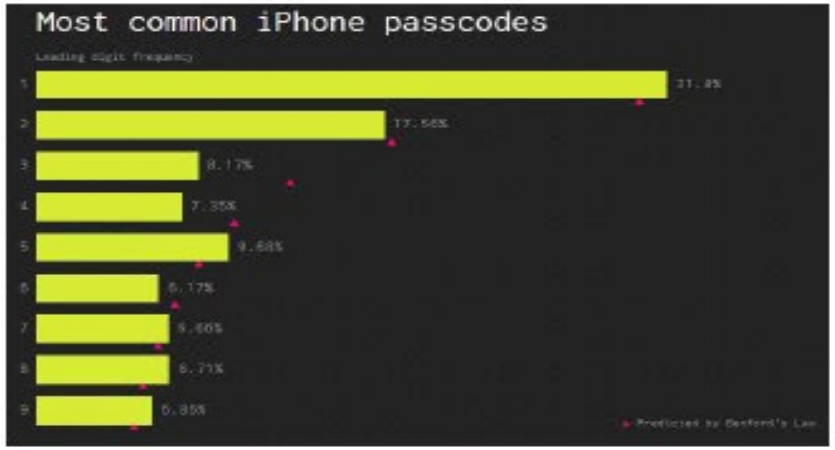
Fibonacci numbers



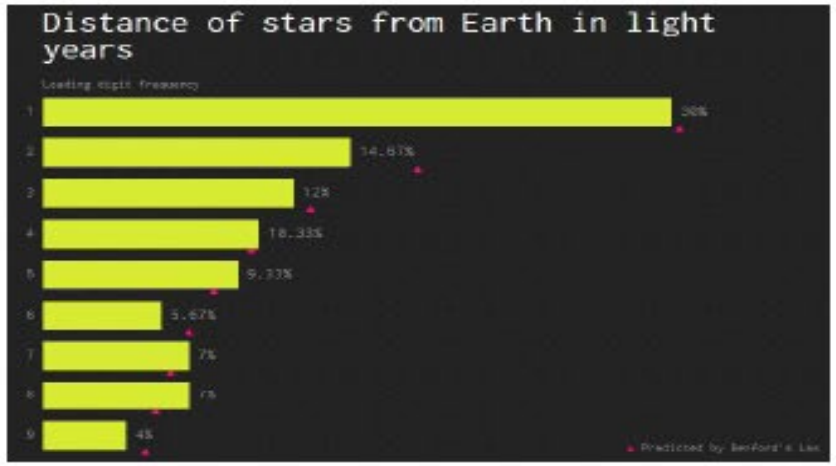
Twitter users by # followers



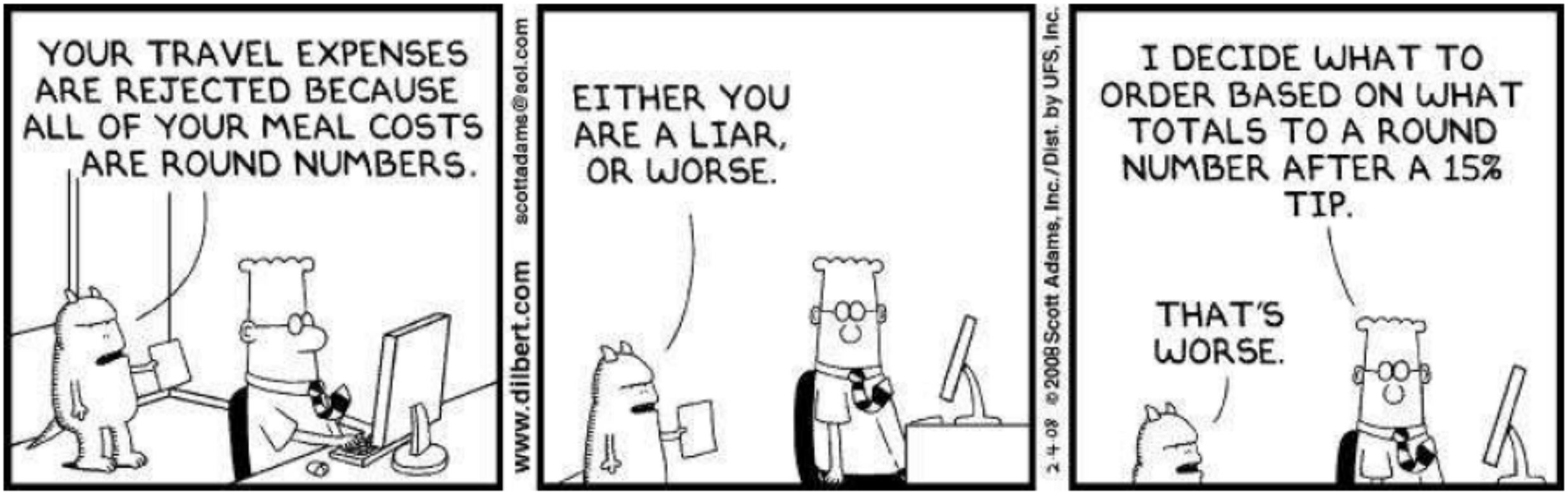
Most common iPhone passcodes



Distance of stars from Earth



- A math test indicating fraud is *not* proof of fraud: unlikely events, alternate reasons.



Applications

- Analyzing round-off errors.
- Determining the optimal way to store numbers.
- Detecting tax and image fraud, and data integrity.

Background Material

- Modulo: $a = b \mod c$ if $a - b$ is an integer times c; thus $17 = 5 \mod 12$, and $4.5 = .5 \mod 1$.
- Significand: $x = S_{10}(x) \cdot 10^k$, k integer, $1 \le S_{10}(x) < 10$. Thus $2020.1701 = 2.0201701 \cdot 10^3$.
- $S_{10}(a) = S_{10}(b)$ if and only if a and b have the same leading digits. Note $\log_{10} a = \log_{10} S_{10}(b) + k$.
- Key observation: $\log_{10}(x) = \log_{10}(\widetilde{x}) \mod 1$ if and only if x and $\widetilde{x}$ have the same leading digits.

$e^{ix} = \cos x + i \sin x$

Thus often study $y = \log_{10} x \mod 1$.
Advanced: $e^{2\pi i u} = e^{2\pi i (u \mod 1)}$.

Fourier Analysis

Equidistribution

$\{y_n\}_{n=1}^{\infty}$ is equidistributed modulo 1 if probability $y_n \bmod 1 \in [a, b]$ tends to $b - a$:

$$\frac{\#\{n \leq N : y_n \bmod 1 \in [a, b]\}}{N} \to b - a.$$

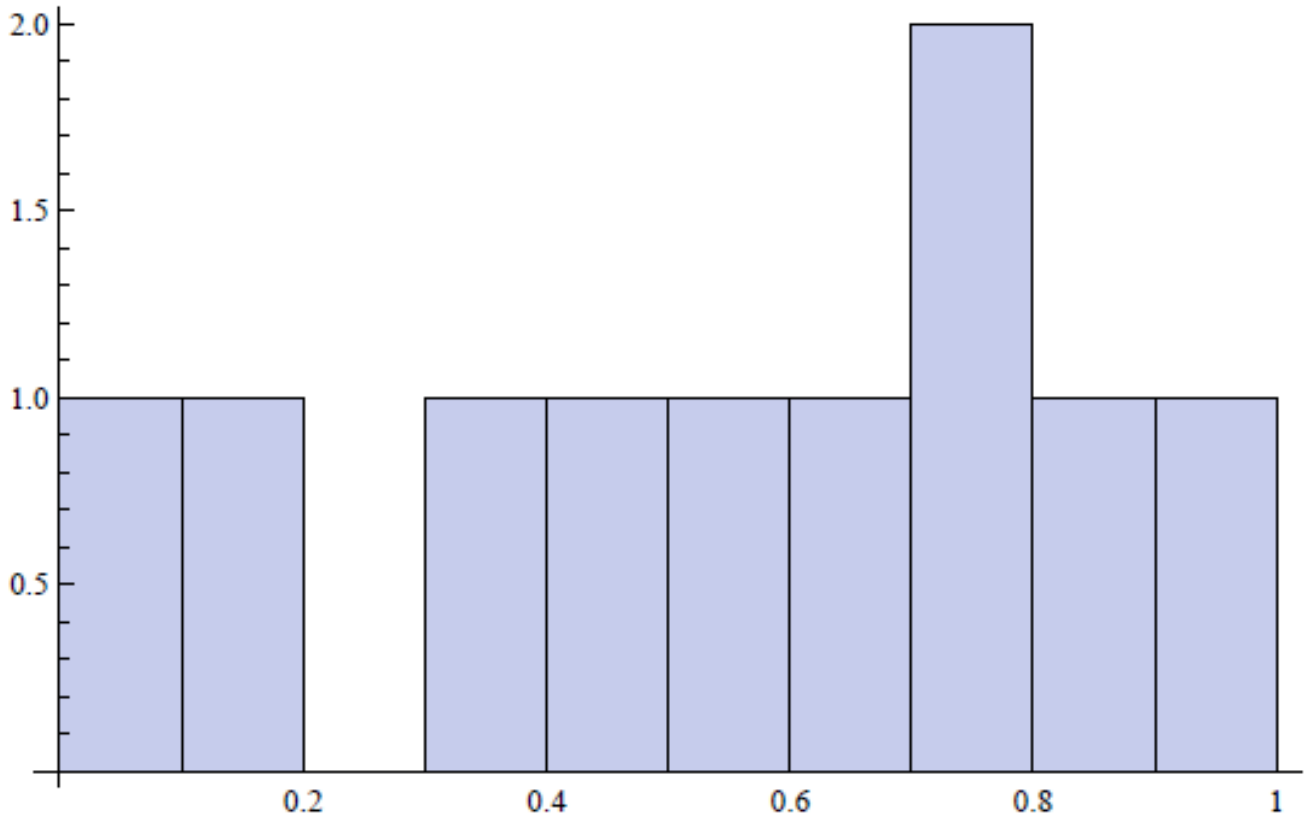
$[a,b] \subset [0,1]$

- Thm: $\beta \notin \mathbb{Q}$, $n\beta$ is equidistributed mod 1.

$\beta = 1/5$: $\{n\beta \bmod 1\} = \{0, 1/5, 2/5, 3/5, 4/5\}$

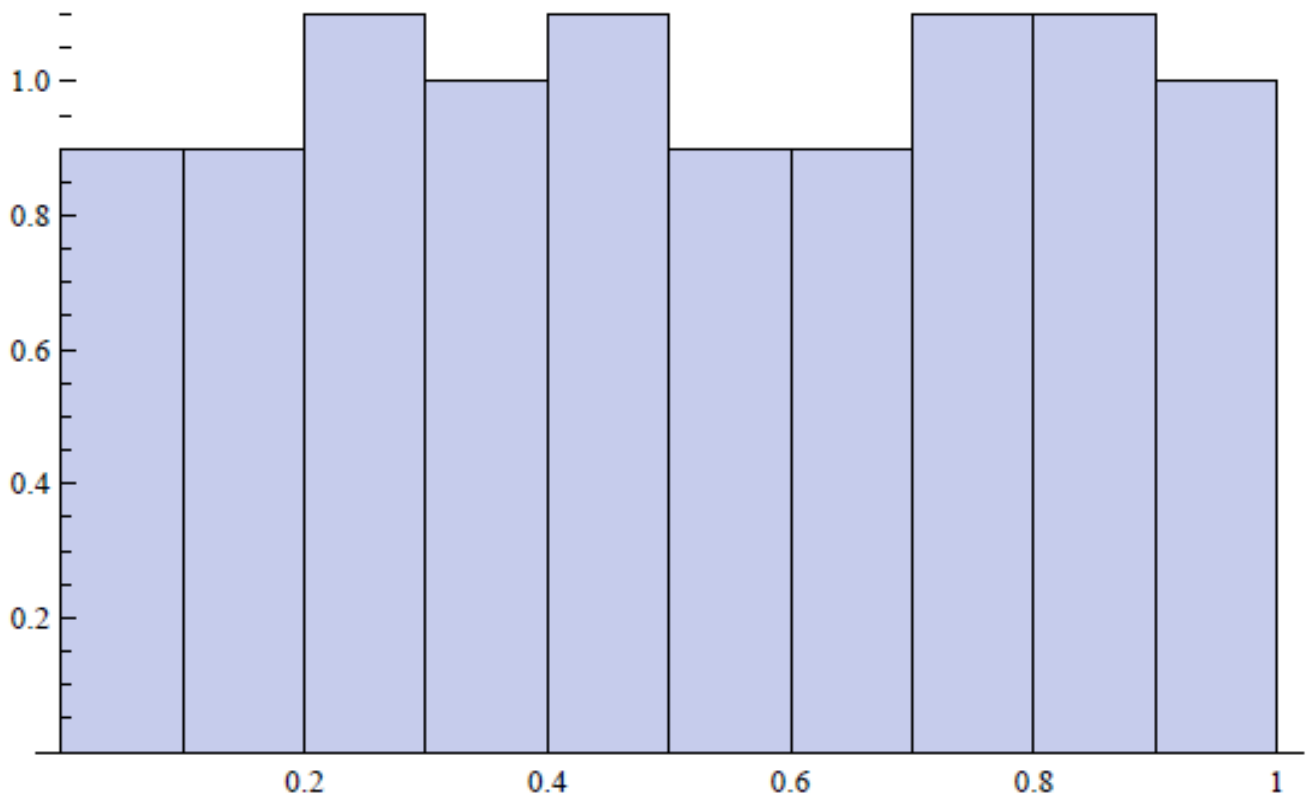
- Examples: $\log_{10} 2$, $\log_{10}\left(\frac{1+\sqrt{5}}{2}\right) \notin \mathbb{Q}$.

Example of Equidistribution: $n\sqrt{\pi} \bmod 1$



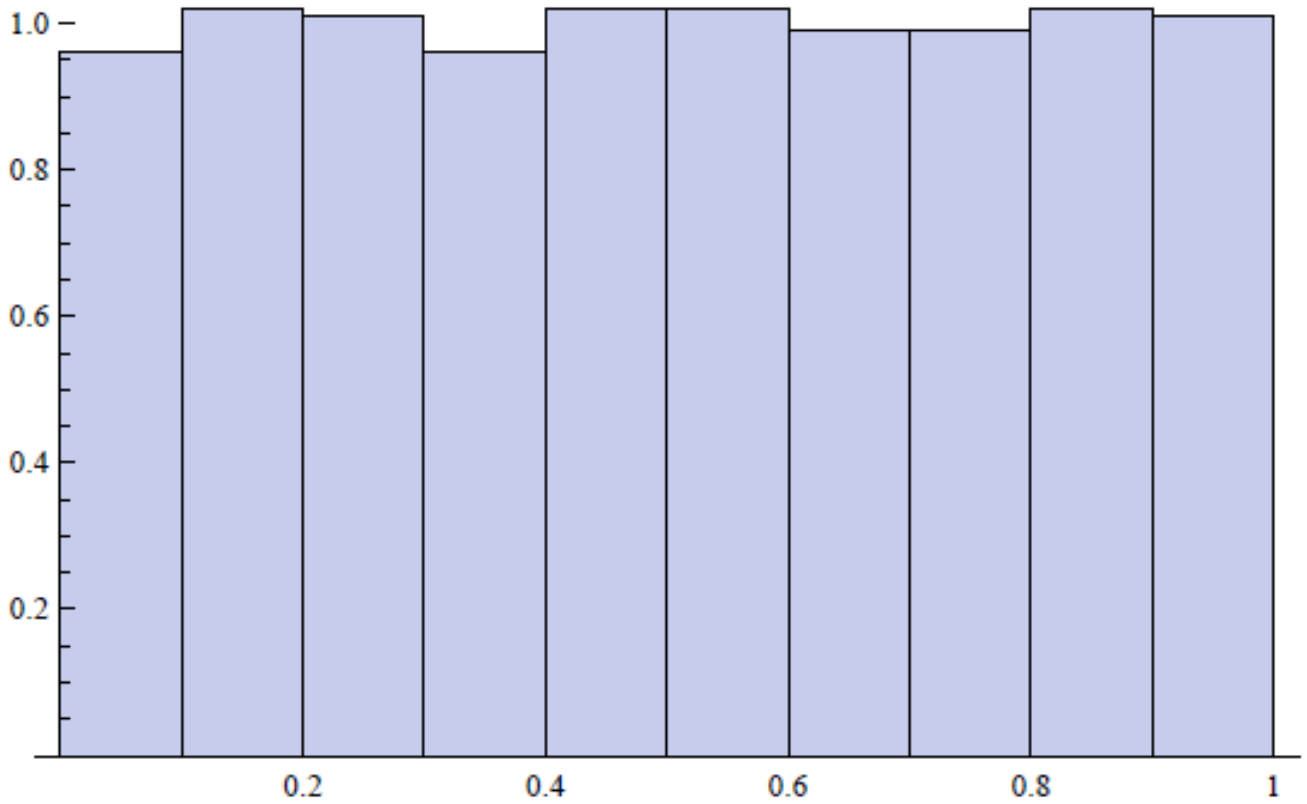
$n\sqrt{\pi} \bmod 1$ for $n \leq 10$

Example of Equidistribution: $n\sqrt{\pi}$ mod 1



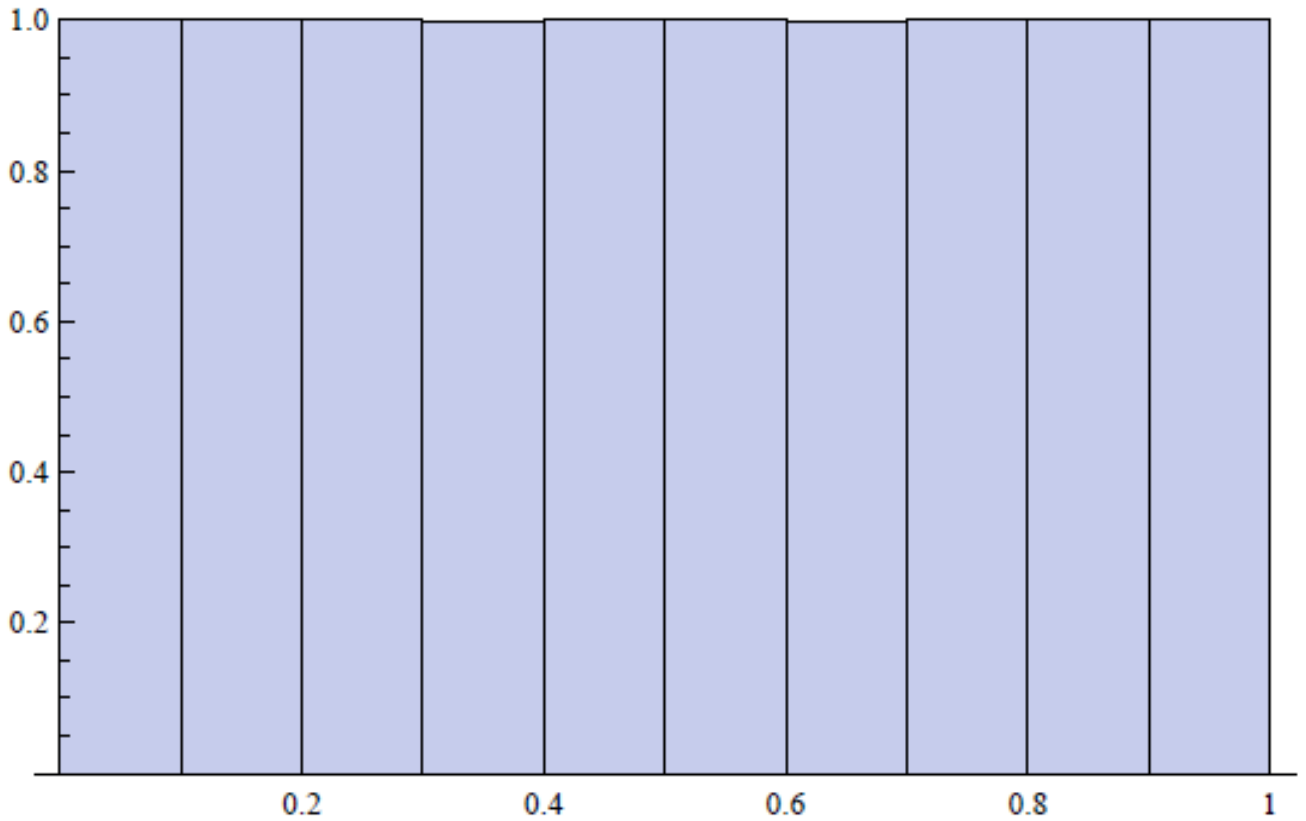
$n\sqrt{\pi}$ mod 1 for $n \leq 100$

Example of Equidistribution: $n\sqrt{\pi} \bmod 1$



$n\sqrt{\pi} \bmod 1$ for $n \leq 1000$

Example of Equidistribution: $n\sqrt{\pi} \bmod 1$



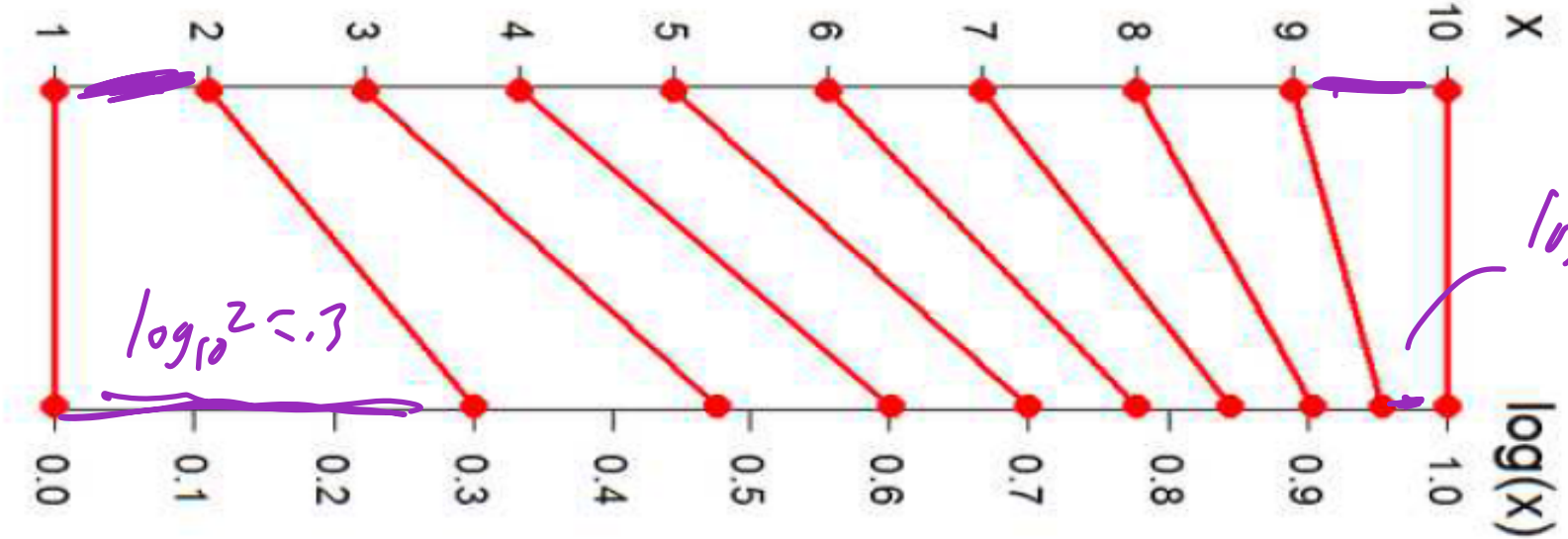
$n\sqrt{\pi} \bmod 1$ for $n \leq 10,000$

Fundamental Equivalence

Data set $\{x_i\}$ is Benford base B if $\{y_i\}$ is equidistributed mod 1, where $y_i = \log_B x_i$.

$$x = S_{10}(x) \cdot 10^k \text{ then}$$

$$\log_{10} x = \log_{10} S_{10}(x) + k = \log_{10} S_{10}x \bmod 1.$$



Significands

$\log_{10} 2 \approx .3$

$\log_{10} 10 - \log_{10} 9$

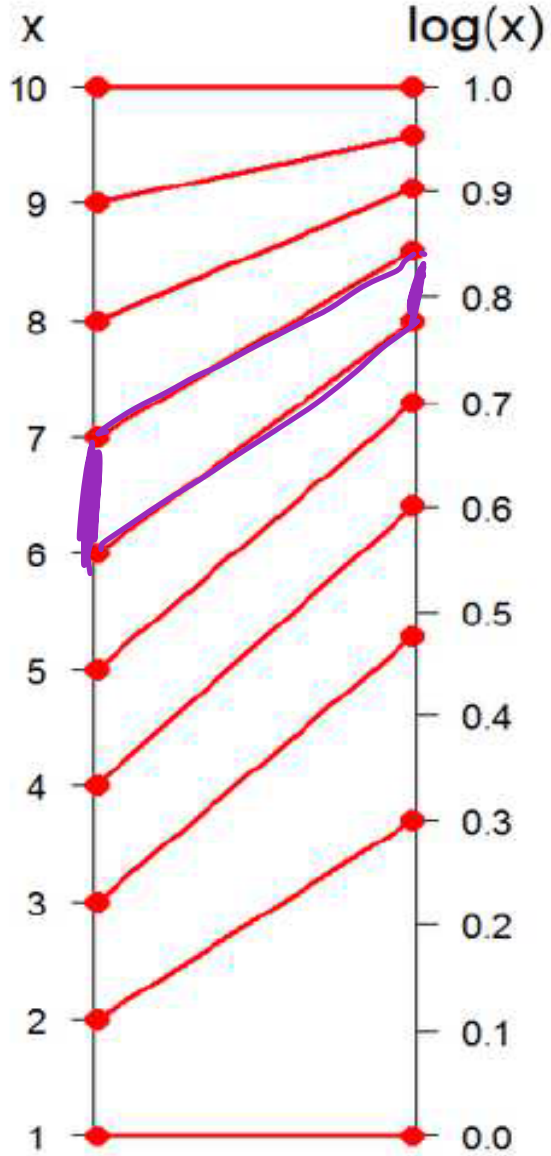
$\log(\text{sig})$

Logarithms and Benford's Law

Ex: $\log\frac{1+1}{1}+\log\frac{2+1}{2}+\log\frac{3+1}{3}+\cdots+\log\frac{9+1}{9}=\log_{10}\left(\frac{2}{1}\cdot\frac{3}{2}\cdot\frac{4}{3}\cdots\frac{10}{9}\right)=\log_{10}10=1$

$$\begin{aligned}&\text{Prob}(\text{leading digit } d)\\ &=\log_{10}(d+1)-\log_{10}(d)\\ &=\log_{10}\left(\tfrac{d+1}{d}\right)\\ &=\log_{10}\left(1+\tfrac{1}{d}\right).\end{aligned}$$

Have Benford's law $\leftrightarrow$ mantissa of logarithms of data are uniformly distributed



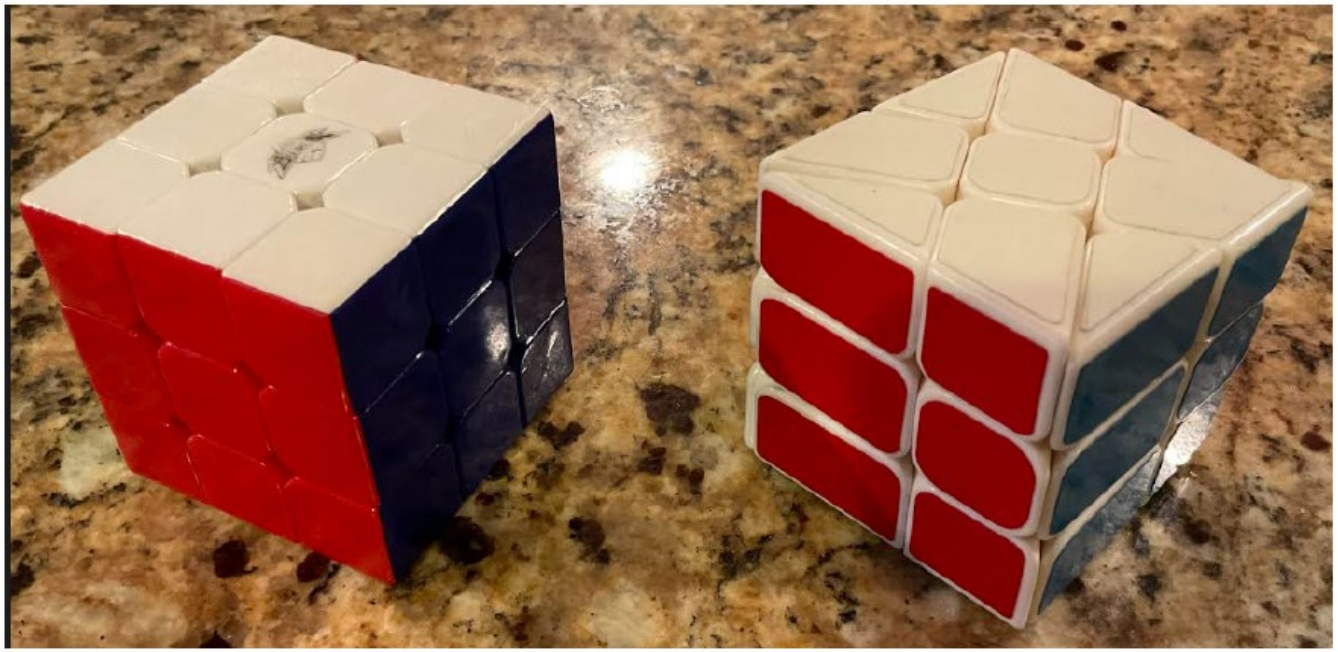
Benford's Law (Digit Bias)

$d+1$

$d=$

Equi-distributed under $\log_{10}$

The Power of the Right Perspective





- 2^n is Benford base 10 as $\log_{10} 2 \notin \mathbb{Q}$.
- Fibonacci numbers are Benford base 10.

  $F_{n+1} = F_n + F_{n-1}$.

  Guess $F_n = r^n$: $r^{n+1} = r^n + r^{n-1}$ or $r^2 = r + 1$.

  Roots $r = (1 \pm \sqrt{5})/2$.

  General solution: $F_n = c_1 r_1^n + c_2 r_2^n$.

  Binet: $F_n = \frac{1}{\sqrt{5}} \left(\frac{1+\sqrt{5}}{2} \right)^n - \frac{1}{\sqrt{5}} \left(\frac{1-\sqrt{5}}{2} \right)^n$.

  $\log_{10} F_n \simeq \log_{10}(1/\sqrt{5}) + n \left[\log_{10} \frac{1+\sqrt{5}}{2} \right]$

  as $n \to \infty$ goes to 0
- Most linear recurrence relations Benford:
  - $a_{n+1} = 2a_n - a_{n-1}$
  - take $a_0 = a_1 = 1$ or $a_0 = 0$, $a_1 = 1$.

$F_{n+1} \le F_n + F_n$ or $F_{n+1} \le 2F_n$ so F_n growing slower than 2^n

Similarly can show growing faster than $\sqrt{2}^n$

$\sqrt{2}^n \le F_n \le 2^n$

HW: Show $\frac{1+\sqrt{5}}{2} < 2$

$\log_{10}$

First 60 values of 2^n (only displaying 30)

1	1024	1048576	digit	#	Obs Prob	Benf Prob
2	2048	2097152	1	18	.300	.301
4	4096	4194304	2	12	.200	.176
8	8192	8388608	3	6	.100	.125
16	16384	16777216	4	6	.100	.097
32	32768	33554432	5	6	.100	.079
64	65536	67108864	6	4	.067	.067
128	131072	134217728	7	2	.033	.058
256	262144	268435456	8	5	.083	.051
512	524288	536870912	9	1	.017	.046

First 60 values of 2^n (only displaying 30)

			digit	#	Obs Prob	Benf Prob
1	1024	1048576	1	18	.300	.301
2	2048	2097152	2	12	.200	.176
4	4096	4194304	3	6	.100	.125
8	8192	8388608	4	6	.100	.097
16	16384	16777216	5	6	.100	.079
32	32768	33554432	6	4	.067	.067
64	65536	67108864	7	2	.033	.058
128	131072	134217728	8	5	.083	.051
256	262144	268435456	9	1	.017	.046
512	524288	536870912				

$2^{10} \approx 10^3$ $2^{10} = 1024$

First 60 values of 2^n (only displaying 30): $2^{10} = 1024 \approx 10^3$.

			digit	#	Obs Prob	Benf Prob
1	1024	1048576	1	18	.300	.301
2	2048	2097152	2	12	.200	.176
4	4096	4194304	3	6	.100	.125
8	8192	8388608	4	6	.100	.097
16	16384	16777216	5	6	.100	.079
32	32768	33554432	6	4	.067	.067
64	65536	67108864	7	2	.033	.058
128	131072	134217728	8	5	.083	.051
256	262144	268435456	9	1	.017	.046
512	524288	536870912				

First 1000 values of 2^n (only displaying 30): $2^{10} = 1024 \approx 10^3$.

			digit	#	Obs Prob	Benf Prob
1	1024	1048576	1	301	0.301	.301
2	2048	2097152	2	176	0.176	.176
4	4096	4194304	3	125	0.125	.125
8	8192	8388608	4	97	0.097	.097
16	16384	16777216	5	79	0.079	.079
32	32768	33554432	6	69	0.069	.067
64	65536	67108864	7	56	0.056	.058
128	131072	134217728	8	52	0.052	.051
256	262144	268435456	9	45	0.045	.046
512	524288	536870912				

χ^2 values for α^n, $1 \leq n \leq N$ (5% 15.5).

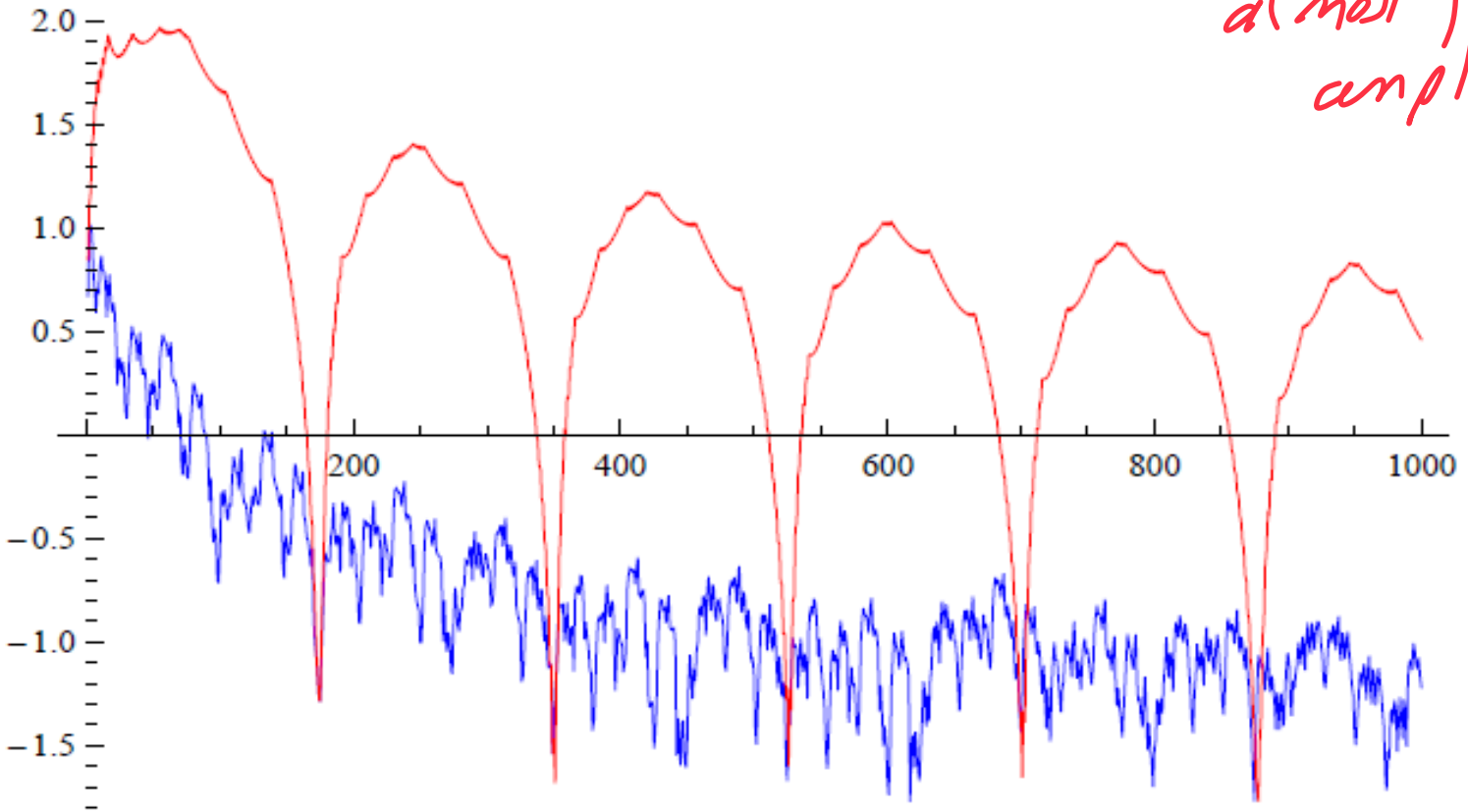
N	$\chi^2(\gamma)$	$\chi^2(e)$	$\chi^2(\pi)$
100	0.72	0.30	46.65
200	0.24	0.30	8.58
400	0.14	0.10	10.55
500	0.08	0.07	2.69
700	0.19	0.04	0.05
800	0.04	0.03	6.19
900	0.09	0.09	1.71
1000	0.02	0.06	2.90

looking at first N digits of $\pi, e, \sqrt{\pi}$ for $1 \leq n \leq N$

Chi-Square test to compare observed with predicted

Logarithms and Benford's Law: Base 10 (5%: $\log(\chi^2) \approx 2.74$)

$\log(\chi^2)$ vs N for π^n (red) and e^n (blue), $n \in \{1, \ldots, N\}$.



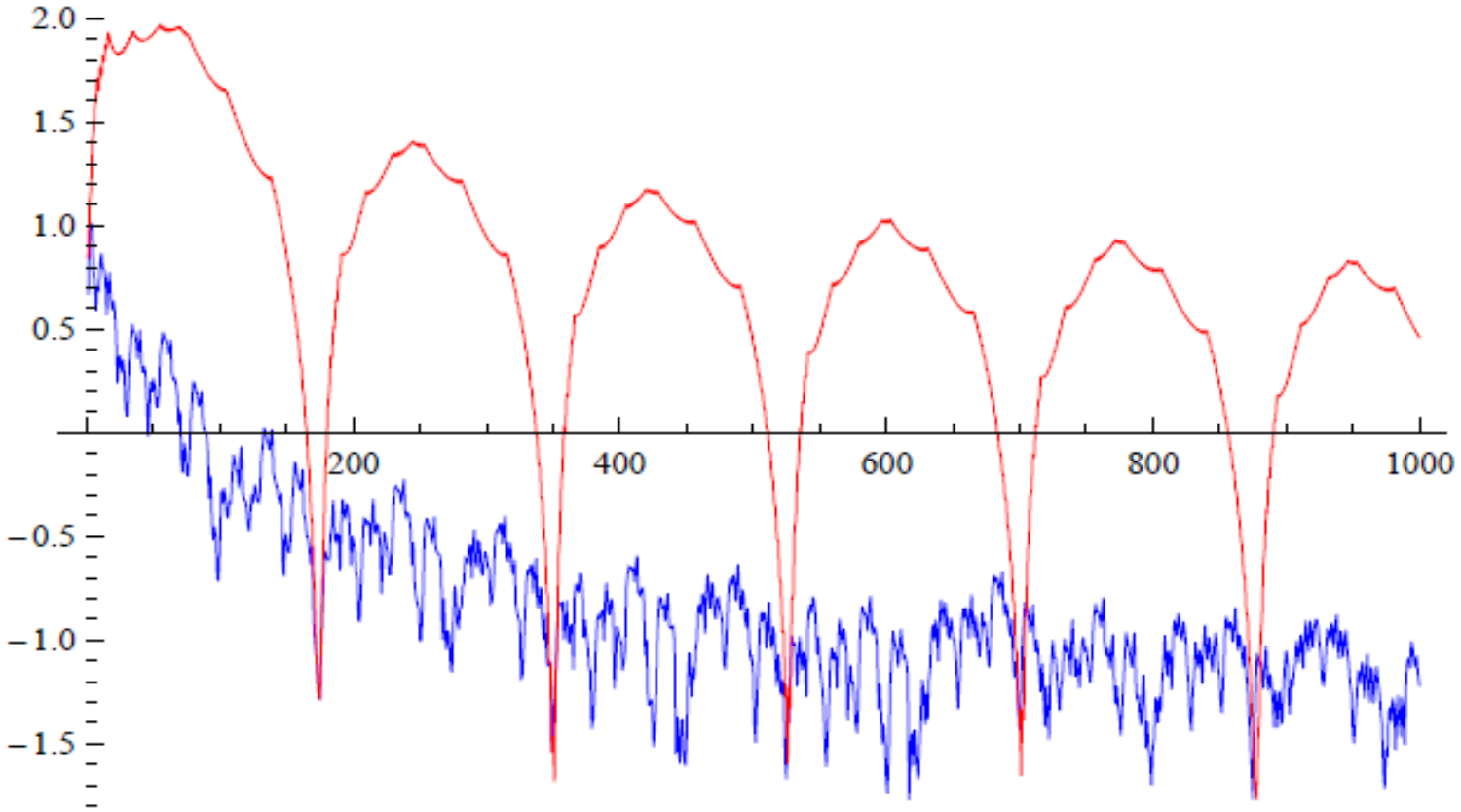
almost periodic with amplitude decreasing

π

e

Logarithms and Benford's Law: Base 10 (5%: $\log(\chi^2) \approx 2.74$)

$\log(\chi^2)$ vs N for π^n (red) and e^n (blue), $n \in \{1, \ldots, N\}$. Note $\pi^{175} \approx 1.0028 \cdot 10^{87}$.



Benford's law, or, Why the IRS cares about Number Theory.

- Brown University: https://www.youtube.com/watch?v=rCsavxidCZ4 (slides here, technical talk: Benford good, Products, Chains)
- Carnegie Mellon: http://youtu.be/z2Rx1w5UDnk (slides here, technical talk: L-fns, 3x+1, Decompositions)
- Williams College: http://youtu.be/JmBXZCbbwas (slides here, colloquium talk to all faculty, more general than the Brown / Carnegie Mellon)
- Benford's Law: Why the IRS and others care about Number Theory (and you should too!), Cross-domain Conference on Benford's Law application, Stresa, Italy, July 10, 2019. pdf PIMS Distinguished Lecture, UNBC, November 14, 2019 (changed to 11/4/2020: video here: https://youtu.be/NSuXJRIFcXc). pdf

Math 355: Modern Algebra: Fall '25 (Siena)

Professor Steven J Miller: sjm1@williams.edu

Homepage:
https://web.williams.edu/Mathematics/sjmiller/public_html/310Fa25/

Groups II:

Lecture 19: 11/4/25:

Chapter Six: Groups: Part II: Orbits, Stabilizers, Sylow Theorem

Is there a group of size n for all $n \geq 1$?

Yes: look at integers mod n under clock laws

$\zeta_n = e^{2\pi i/n}$: $\{1, \zeta_n, \zeta_n^2, \dots, \zeta_n^{n-1}\}$ under mult

equivalent

For what n are there two groups?

$n=1$? Only possibility is $\{e\}$

$n=2$? $\{e, x\}$ $x \neq e$, $x = x^{-1}$

$n=3$? $\{e, x, y\}$: what are $x^2, x^3, x^4, \dots$

$y^2, y^3, y^4, \dots$

xy

yx

$n=3$, $G=\{e,x,y\}$, all 3 distinct

$x^2 = e, x$ or y

↳ if $x^2 = x$ then $x^{-1}x^2 = x^{-1}x$ or $x=e$, contradiction

↳ Could $x^2=e$ if $\#G=3$?

If $x^2=e$ then $\{e,x\}$ is a subgroup of order 2, but $2 \nmid 3$ contradiction by Lagrange.

$\Rightarrow x^2 = y$

So $G = \{e, x, x^2\}$

Analyzed $n =$ 1 (UNIT), 2, 3 (PRIME)

Conj: If n is prime only one group.

Say $n = p$ prime, $\{e, x_2, x_3, \dots, x_p\}$

What is the order of x_2?

$\{e, x_2, x_2^2, x_2^3, \dots, x_2^{k-1}\}$ with $x_2^k = e$, k smallest that works

By Lagrange $k \mid p$ but p is prime

↳ $k \in \{1, p\}$

↳ If $k = 1$ then $x_2 = e$, assuming $x_2 \neq e$

$\Rightarrow k = p$, $\text{ord}(x_2) = p$ so

$G = \{e, x_2, x_2^2, \dots, x_2^{p-1}\}$ only one choice

Try n=4: Can we have two distinct groups?

$\{e, x, x^2, x^3\}$: has an element of order 4

$(\mathbb{Z}/12\mathbb{Z})^\times = \{1, 5, 7, 11\}$ all elements order 2

Necessary and Sufficient

required good enough

Sequence $\{a_n\}$ and study $\sum_{n=1}^{\infty} a_n$

For sum to converge, necessary that $a_n \to 0$

Not sufficient: $1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \cdots$ diverges to ∞

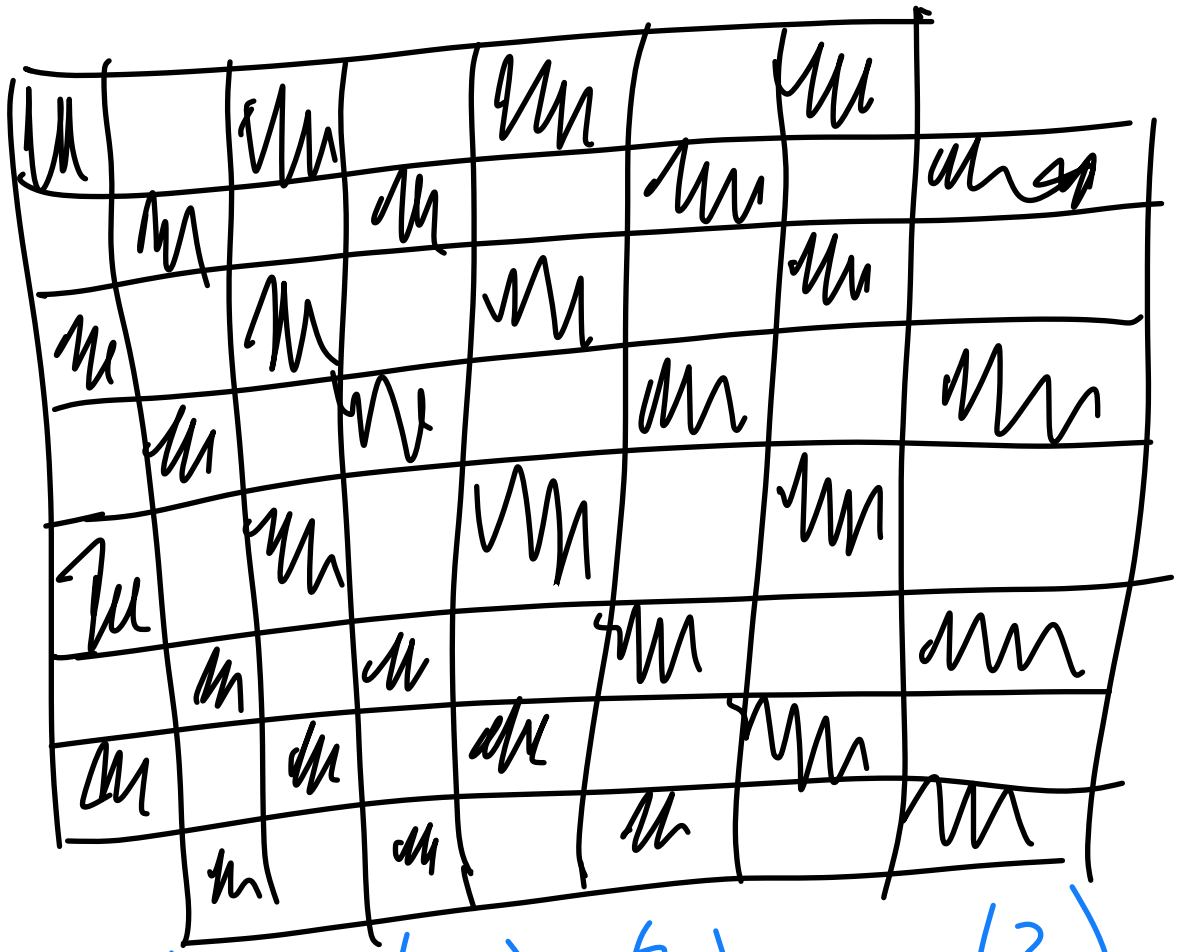
Sufficient condition:

Ratio Test: if $\lim_{n\to\infty} \left|\frac{a_{n+1}}{a_n}\right| = \rho < 1$ then sum converges

Ex: $a_n = 1/n^2$ then $1 + \frac{1}{4} + \frac{1}{9} + \frac{1}{16} + \cdots$ converges

but $\rho = 1$

Checkerboard Problem

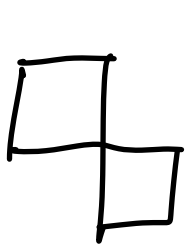


$\begin{pmatrix} \#B \\ \#W \end{pmatrix} = \begin{pmatrix} 32 \\ 30 \end{pmatrix} \to \begin{pmatrix} 31 \\ 29 \end{pmatrix} \to \begin{pmatrix} 30 \\ 28 \end{pmatrix} \cdots \to \begin{pmatrix} 2 \\ 0 \end{pmatrix}$

PARITY

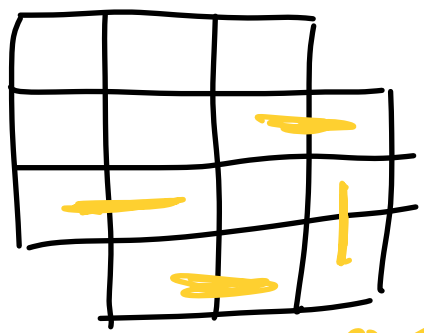
impossible



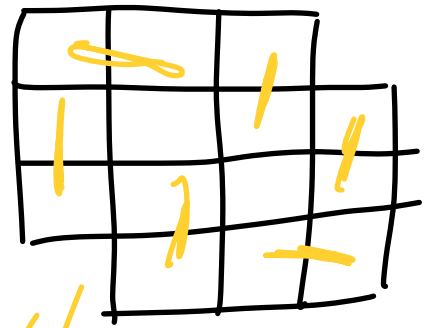


NO

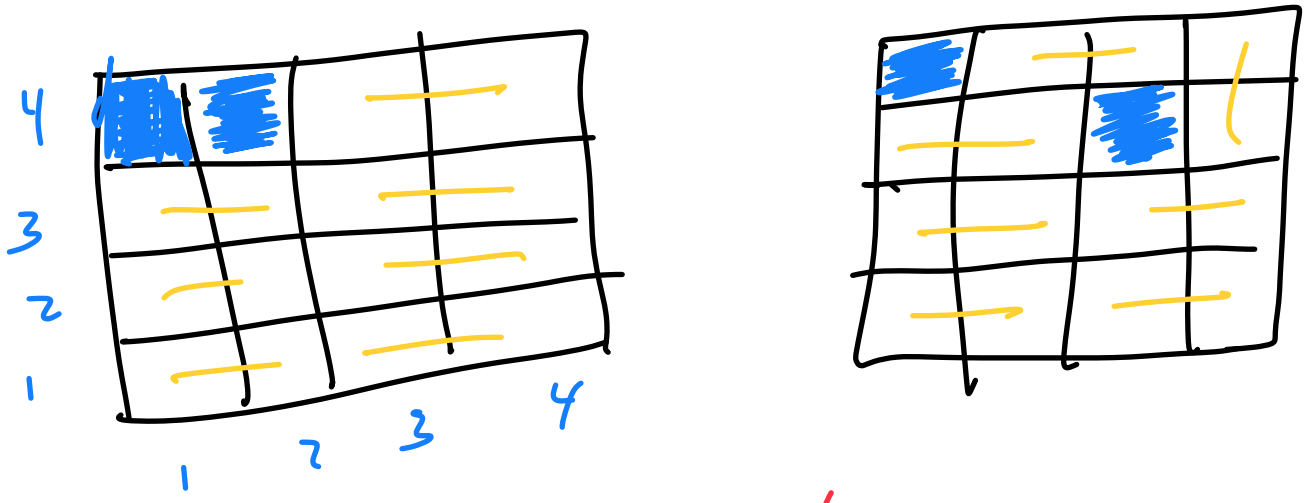
if $n \times n$ with n odd, have an odd # of pts, each tile takes even #.



impossible



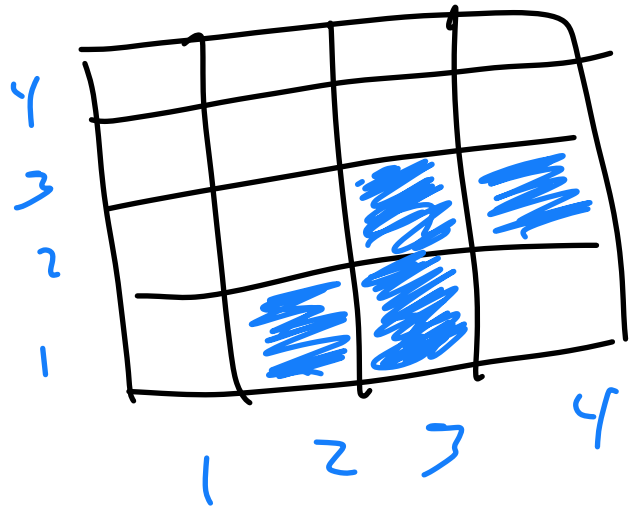
What if remove 1 Black and 1 white?



Can you always tile with 2×1 if remove any 2 squares of opposite parity on a n×n board, n even?

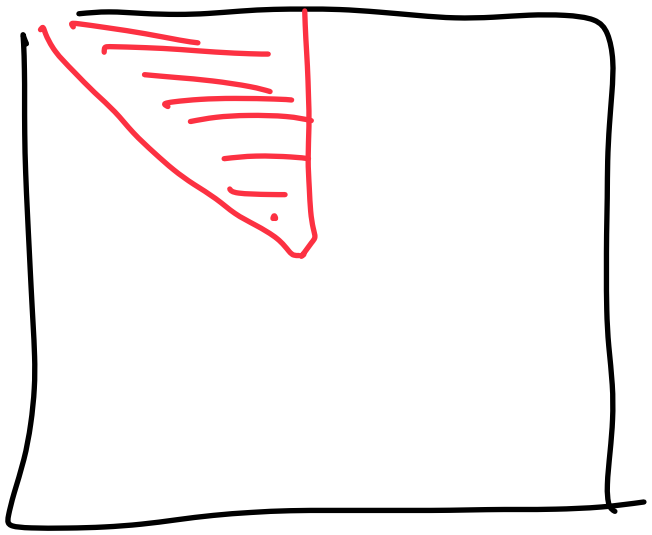
↳ if yes, how many ways?

What if create 2 Black and 2 white?



Not always possible

necessary but not sufficient to have created same number of each color



Say $n=4$

Grp $\{1, x, x^2, x^3\}$ where $x^4 = e$

$\{1, x, y, z\}$ where $x^2 = y^2 = z^2 = e$ and $xy = z = yx$, $xz = y = zx$, $yz = x = zy$ } abelian

↳ if $xy = e$ then $y = x^{-1}$ but $x = x^{-1}$ so $y = x$

so $xy \neq e$

and $xy \neq x$ else $y = e$

and $xy \neq y$ else $x = e$

Is there another group of size 4? If yes, must it be abelian?

$n = 4$: $\{e, x, y, _\}$

Case 1: $x^2 = e$

~~Case 2: $x^3 = e$~~

Lagrange

Case 3: $x^4 = e$

yes: already did cyclic

↳ have element y, $\text{ord}(y) = 2$ or 4

↳ if $\text{ord}(y) = 4$ then $\{e, y, y^2, y^3\}$ and $x = y^2$

this is the cyclic case

↳ assume $\text{ord}(y) = 2$

$\{e, x, y, \underbrace{\quad}_{xy = yx}\}$ $x^2 = e = y^2$, x, y unequal

$xy = yx \Rightarrow (xy)(xy) = (xy)(yx) = x(yy)x = xex = x^2 = e$

this is our $\{1, 5, 7, 11\}$ from before

$n = 9$

If $\exists\, x \in G$ with $\text{ord}(x) = 9$, then G cyclic

Know cyclic if $\exists$ element of order 9, so assume no element has order 9.

So all elements that are not e have order 3

$$\{e, x, x^2, y, y^2, xy, _, _, _, _\}$$

$(xy)^2 =$ something already have

$x^2y =$ " " "

$yx =$ " " "

IF $xyxy = x$

$yxy = e$

$y^3xy^3 = y^2ey^2$

$x = y^4$

$x = y$ contra

IF $xyxy = x^2$

$yxy = x$

$xy = y^2x$

$xyx^{-1} = y^2$

6.2. Groups Acting on Sets

Definition 6.13. Let G be a group, and let X be a set. An *action of G on X* is a rule that assigns to each element $g \in G$ and each element $x \in X$ another element $g \cdot x \in X$, so that the following two axioms hold:

Identity Axiom : $e \cdot x = x$ for all $x \in X$.

Associative Axiom : $(g_1 g_2) \cdot x = g_1 \cdot (g_2 \cdot x)$ for all $x \in X$ and all $g_1, g_2 \in G$.

If given G, can always take X to be $\{0\}$, G

Linear Algebra

X = vectors, G = translations, rotations, ...

Orthogonal matrices: $\{Q \text{ st } QQ^T = Q^T Q = I\}$

$GL_n(\mathbb{R}) = \{$ nxn invertible matrices with real entries$\}$

What are the elements of X to which x is sent by the action of G? This set is called the *orbit of* x and is denoted by

$$Gx = \{g \cdot x : g \in G\}.$$

What are the elements of G that leave x unchanged? This set is called the *stabilizer of* x and is denoted by

$$G_x = \{g \in G : g \cdot x = x\}.$$

The stabilizer G_x is a subgroup of G; see Proposition 6.19(a).

$G_x \subset G$

Proposition 6.19. *Let G be a group that acts on a set X.*

(a) *Let $x \in X$. The stabilizer G_x is a subgroup of G.*

(b) *Define a relation $\sim$ on X by the following rule:*

$$x \sim y \quad \text{if} \quad y = gx \quad \text{for some} \quad g \in G.$$

Then $\sim$ is an equivalence relation, and

$$(\text{the equivalence class of } x) = (\text{the orbit } Gx \text{ of } x).$$

Proof of (a) Show G_x is a subgroup. (know $G_x \subset G$)

- Closure: $g_1, g_2 \in G_x$ show $g_1 g_2 \in G_x$.
  Is know $g_1 x = x$ and $g_2 x = x$ as $g_1, g_2 \in G_x$
  $$\text{So } (g_1 g_2)x = g_1(g_2 x) = g_1 x = x$$
  assoc $\quad g_2 \in G_x \quad g_1 \in G_x$
- Identity: know $e \cdot x = x$ so $e \in G_x$
- Assoc: inherited
- Inverses: if $g \in G_x$ then $gx = x$ so $g^{-1}(gx) = g^{-1}x$ or $(g^{-1}g)x = g^{-1}x$
  so $ex = x$ or $x = x$ and $g^{-1} \in G_x$

\frac{\overline{\xi}}{\xi}



Proposition 6.19. *Let G be a group that acts on a set X.*

(c) *Let $x \in X$. There is a well-defined bijection*

$$\alpha : G/G_x \longrightarrow Gx$$

defined by the following algorithm:

Input:	A coset $\mathcal{C}$ of the subgroup G_x.
Computation:	Choose an element $g \in \mathcal{C}$.
Output:	$\alpha(\mathcal{C})$ is the element $g \cdot x$ in the orbit Gx.

In particular, if G is finite, then

$$\#Gx = \frac{\#G}{\#G_x}.$$

Math 355: Modern Algebra: Fall '25 (Siena)

Professor Steven J Miller: sjm1@williams.edu

Homepage:
https://web.williams.edu/Mathematics/sjmiller/public_html/310Fa25/

Groups II:

Lecture 20: 11/6/25:

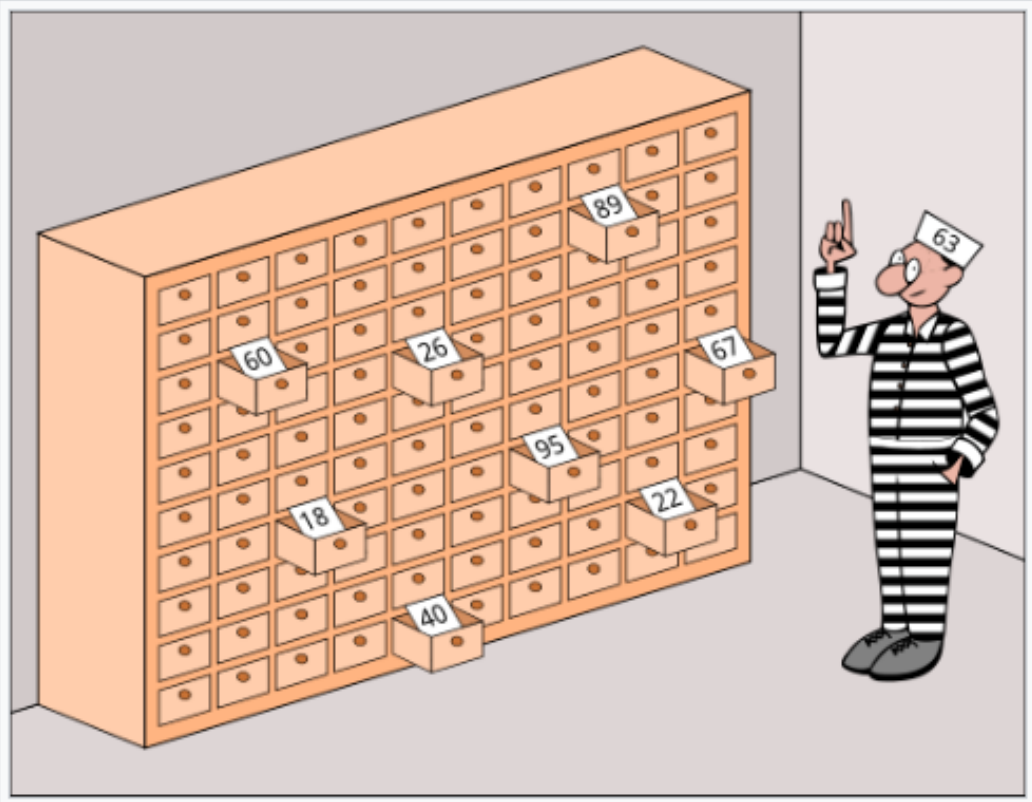
https://youtu.be/OYlJPTiLdwM

Chapter Six: Groups: Part II: Orbits, Stabilizers, Sylow Theorem

From Wikipedia, the free encyclopedia

https://en.wikipedia.org/wiki/100_prisoners_problem

The **100 prisoners problem** is a mathematical problem in probability theory and combinatorics. In this problem, 100 numbered prisoners must find their own numbers in one of 100 drawers in order to survive. The rules state that each prisoner may open only 50 drawers and cannot communicate with other prisoners after the first prisoner enters to look in the drawers. If all 100 prisoners manage to find their own numbers, they all survive, but if even one prisoner can't find their number, they all die. At first glance, the situation appears hopeless, but a clever strategy offers the prisoners a realistic chance of survival.



Each prisoner has to find their own number in one of 100 drawers, but may open only 50 of the drawers.

Anna Gál and Peter Bro Miltersen first proposed the problem in 2003.

Naive: $\text{Prob}(\text{all live}) = \left(\frac{50}{100}\right)^{100}$

$= \left(\left(\frac{1}{2}\right)^{10}\right)^{10} = \left(\frac{1}{2^{10}}\right)^{10} \approx \left(\frac{1}{10^3}\right)^{10} \approx \frac{1}{10^{30}}$

Open 1, if 1 has 7 then open 7, if 7 has 23 open 23, ...

$1 \to 7 \to 23 \to 81 \to 4 \to 97 \to \cdots$

Must it loop to 1 eventually? YES!

OK if less than or equal to 50 steps

$$\begin{pmatrix} 1 & 2 & 3 & \cdots & 100 \\ n_1 & n_2 & n_3 & \cdots & n_{100} \end{pmatrix} = \begin{pmatrix} n_1 \cdots n_{k_1} \\ n_1 \cdots n_{k_1} \end{pmatrix} \begin{pmatrix} n_{k_1+1} \cdots n_{k_2} \\ n_{k_1+1} \cdots n_{k_2} \end{pmatrix} \cdots$$

disjoint cycles

need each to have length ≤ 50

Could we have a long cycle? YES!

$$\begin{pmatrix} 1 & 2 & 3 & \cdots & 99 & 100 \\ 2 & 3 & 4 & \cdots & 100 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 & \cdots & 49 & 50 & 51 & 52 & \cdots & 98 & 99 & 100 \\ 2 & 3 & 4 & \cdots & 50 & 52 & 51 & 1 & \cdots & 98 & 99 & 100 \end{pmatrix}$$

Given 100 and 50, cycle of length 51 bad

$\cap$ $\frac{1}{2}$ $\frac{1}{2}+1$

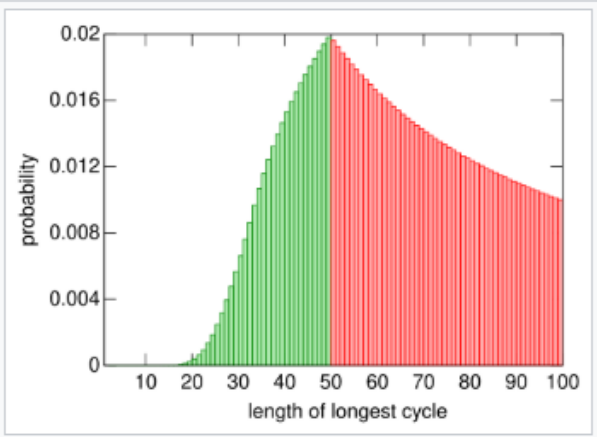
Can have at most one cycle of length ≥ 51

Contents hide

(Top)
Problem
Solution
Strategy
Examples
Permutation representation
Probability of success
Asymptotics
Optimality
History
Variants
Empty boxes
The malicious director
One prisoner may make one change
Any prisoner who finds their number is free
Monty Hall problem
Odd number of tries

Probability of success [edit]

In the initial problem, the 100 prisoners are successful if the longest cycle of the permutation has a length of at most 50. Their survival probability is therefore equal to the probability that a random permutation of the numbers 1 to 100 contains no cycle of length greater than 50. This probability is determined in the following.



Probability distribution of the length of the longest cycle of a random permutation of the numbers 1 to 100. The green area corresponds to the survival probability of the prisoners.

A permutation of the numbers 1 to 100 can contain at most one cycle of length $l > 50$. There are exactly $\binom{100}{l}$ ways to select the numbers of such a cycle (see combination). Within this cycle, these numbers can be arranged in $(l-1)!$ ways since there are l permutations to represent distinct cycles of length l because of cyclic symmetry. The remaining numbers can be arranged in $(100-l)!$ ways. Therefore, the number of permutations of the numbers 1 to 100 with a cycle of length $l > 50$ is equal to

$$\binom{100}{l} \cdot (l-1)! \cdot (100-l)! = \frac{100!}{l}.$$

# of ways to choose l numbers · order what is left · # orders on a cycle/circle

The probability, that a (uniformly distributed) random permutation contains no cycle of length greater than 50 is calculated with the formula for single events and the formula for complementary events thus given by

$$1 - \left[\frac{1}{100!}\left(\frac{100!}{51} + \ldots + \frac{100!}{100}\right)\right] = 1 - \left(\frac{1}{51} + \ldots + \frac{1}{100}\right) = 1 - (H_{100} - H_{50}) \approx 0.31183,$$

+ H50 − H50

where H_n is the n-th harmonic number. Therefore, using the cycle-following strategy the prisoners survive in a surprising 31% of cases.[3]

$$1-\left(\frac{1}{51}+\cdots+\frac{1}{100}\right) = 1-\left(1+\frac{1}{2}+\cdots+\frac{1}{100}-\left[1+\frac{1}{2}+\cdots+\frac{1}{50}\right]\right)$$

$$= 1-\left(H_{100}-H_{50}\right)$$

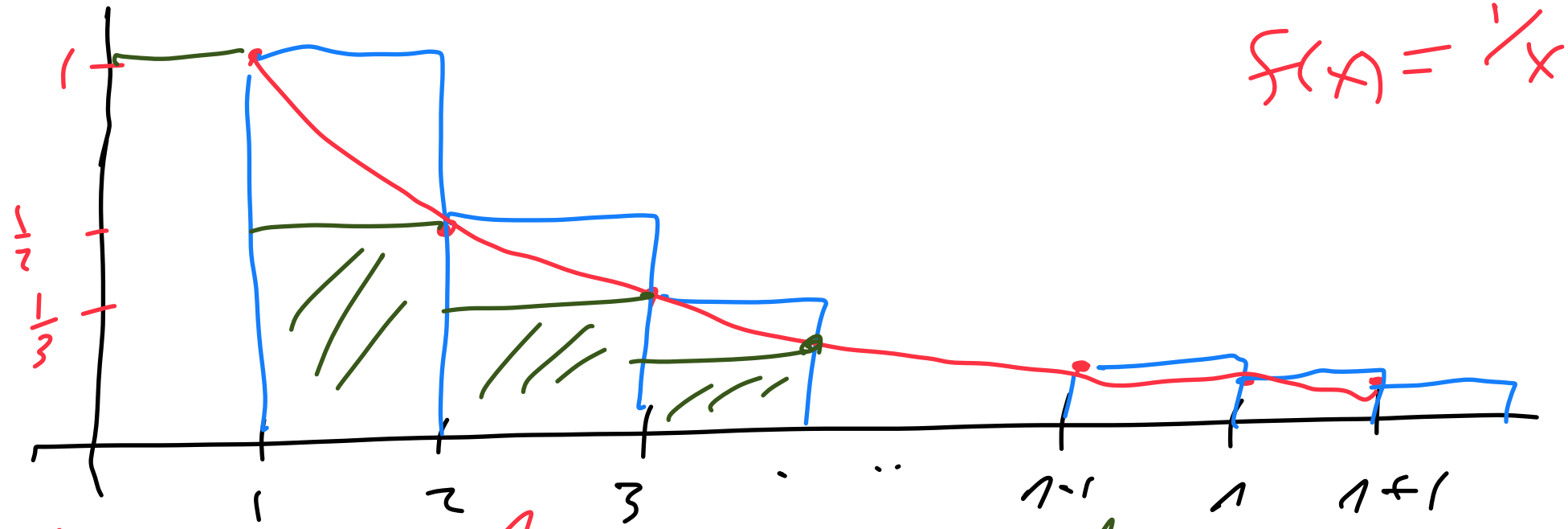
n and $n/2$ would be $1-\left(H_n - H_{n/2}\right)$

or $1+H_{n/2}-H_n$

Integral Test

If $\{a_n\}$ is non-decreasing or non-increasing then

$$\sum_{k=1}^{n} a_k \sim \int_1^n f(x)\,dx$$ where $f(k) = a_k$ and for ex $a_k = 1/k$, $f(x) = 1/x$



$$\int_1^n f(x)\,dx \le \sum_{k=1}^{n} a_k \le 1 + \int_1^n f(x)\,dx$$

$$H_n = \ln(n) + \gamma + \frac{1}{2n} + \text{smaller}$$

$$1 + H_{n/2} - H_n$$

$$= 1 + \left[\ln(n/2) + \gamma + \frac{1}{n} + \text{smaller} \right]$$

$$- \left[\ln(n) + \gamma + \frac{1}{2n} + \text{smaller} \right]$$

$$= 1 - \ln(2) + \frac{1}{2n} + \text{smaller}$$

$$\ln(n/2) - \ln n$$

$$= \ln \frac{n/2}{n}$$

$$= \ln \frac{1}{2}$$

$$= -\ln 2$$

$$\approx -.69$$

https://en.wikipedia.org/wiki/Harmonic_number

$$H_n \sim \ln n + \gamma + \frac{1}{2n} - \sum_{k=1}^{\infty} \frac{B_{2k}}{2kn^{2k}}$$
$$= \ln n + \gamma + \frac{1}{2n} - \frac{1}{12n^2} + \frac{1}{120n^4} - \cdots,$$

where B_k are the Bernoulli numbers.

The numerical value of Euler's constant, to 50 decimal places, is:[1]

https://en.wikipedia.org/wiki/Euler%27s_constant

0.57721 56649 01532 86060 65120 90082 40243 10421 59335 939

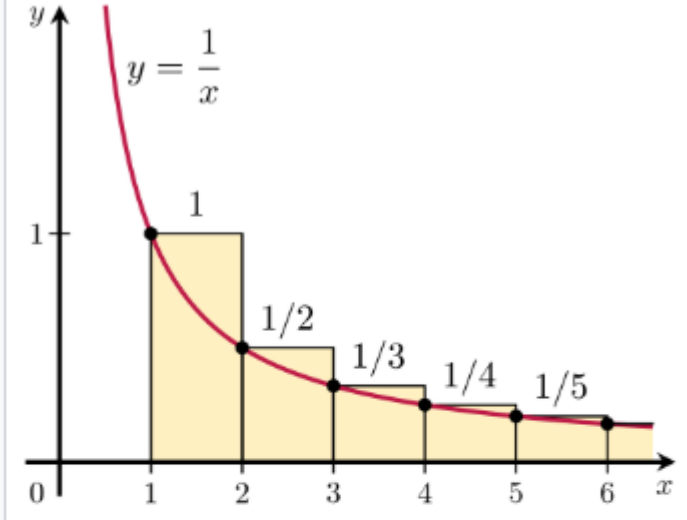
The exponential generating functions are

$$\frac{t}{e^t - 1} = \frac{t}{2}\left(\coth\frac{t}{2} - 1\right) = \sum_{m=0}^{\infty} \frac{B_m^- t^m}{m!}$$
$$\frac{te^t}{e^t - 1} = \frac{t}{1 - e^{-t}} = \frac{t}{2}\left(\coth\frac{t}{2} + 1\right) = \sum_{m=0}^{\infty} \frac{B_m^+ t^m}{m!}.$$

where the substitution is $t \to -t$. The two generating functions only differ by t.

Two conventions are used in the literature, denoted here by B_n^- and B_n^+; they differ only for $n = 1$, where $B_1^- = -1/2$ and $B_1^+ = +1/2$.

https://en.wikipedia.org/wiki/Bernoulli_number



Graph demonstrating a connection between harmonic numbers and the natural logarithm. The harmonic number H_n can be interpreted as a Riemann sum of the integral:

$$\int_1^{n+1} \frac{dx}{x} = \ln(n+1).$$

6.2. Groups Acting on Sets

Definition 6.13. Let G be a group, and let X be a set. An *action of G on X* is a rule that assigns to each element $g \in G$ and each element $x \in X$ another element $g \cdot x \in X$, so that the following two axioms hold:

$$\textit{Identity Axiom}: \quad e \cdot x = x \quad \text{for all } x \in X.$$

$$\textit{Associative Axiom}: \quad (g_1 g_2) \cdot x = g_1 \cdot (g_2 \cdot x) \quad \text{for all } x \in X \text{ and all } g_1, g_2 \in G.$$

What are the elements of X to which x is sent by the action of G? This set is called the *orbit of x* and is denoted by

$$Gx = \{g \cdot x : g \in G\}.$$

What are the elements of G that leave x unchanged? This set is called the *stabilizer of x* and is denoted by

$$G_x = \{g \in G : g \cdot x = x\}.$$

$\leftarrow$ not empty, contains e

The stabilizer G_x is a subgroup of G; see Proposition 6.19(a).

Proposition 6.19. *Let G be a group that acts on a set X.*

(a) *Let $x \in X$. The stabilizer G_x is a subgroup of G.*

(b) *Define a relation $\sim$ on X by the following rule:*

$$x \sim y \quad \text{if} \quad y = gx \quad \text{for some} \quad g \in G.$$

Then $\sim$ is an equivalence relation, and

$$(\text{the equivalence class of } x) = (\text{the orbit } Gx \text{ of } x).$$

- Reflexive: is $x \sim x$? Yes! taking $g = e$ gives $x = e \cdot x$
- Symmetric: if $x \sim y$ is $y \sim x$?
  - ↳ $x \sim y$ means $\exists g \in G$ st $y = g \cdot x$
    Must find $\tilde{g} \in G$ with $x = \tilde{g} y$; take $\tilde{g} = g^{-1}$ as $g^{-1} y = x$
- Transitive: if $x \sim y$, $y \sim z$ show $x \sim z$
  - ↳ $x \sim y$ means $\exists g_1 \in G$ with $y = g_1 x$
    $y \sim z$ means $\exists g_2 \in G$ with $z = g_2 y$
    note $z = g_2 y = g_2 (g_1 x) = (g_2 g_1) x$, so $z \sim x$ with $g = g_2 g_1$ ∎

Proposition 6.19. *Let G be a group that acts on a set X.*

(c) *Let $x \in X$. There is a well-defined bijection*

$$\alpha : G/G_x \longrightarrow Gx$$

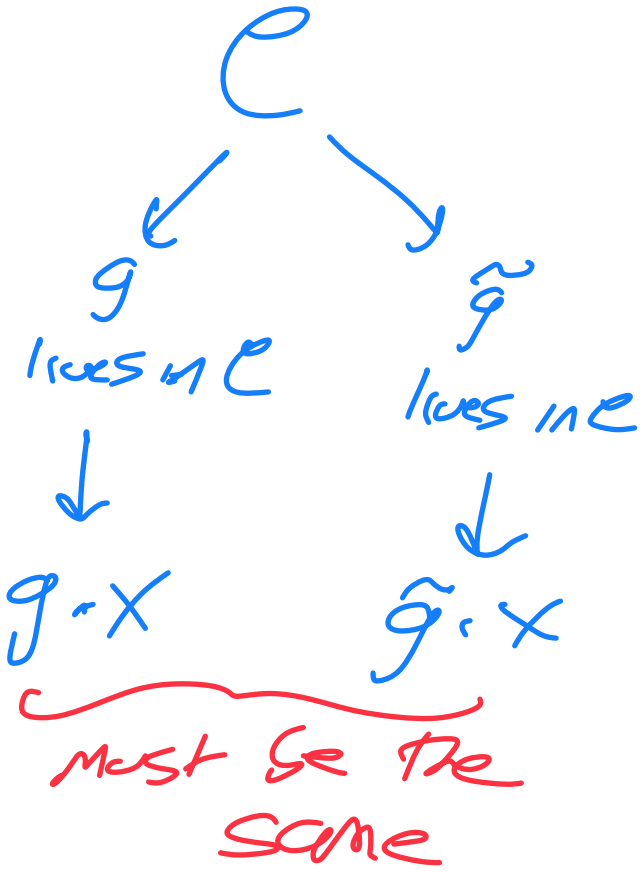
input is cosets output is orbit

defined by the following algorithm:

Input:	A coset $\mathcal{C}$ of the subgroup G_x.
Computation:	Choose an element $g \in \mathcal{C}$.
Output:	$\alpha(\mathcal{C})$ is the element $g \cdot x$ in the orbit Gx.

In particular, if G is finite, then

$$\#Gx = \frac{\#G}{\#G_x}.$$



Map is well defined

If $g, \tilde{g} \in \mathcal{C}$ then $\exists\, c \in G_x$ such that $g = \tilde{g}c$

So $gx = (\tilde{g}c)x = \tilde{g}(cx) = \tilde{g}x$ so well defined!

$c \in G_x$

cosets G/G_x

$eG_x, g_1G_x, g_2G_x, \ldots$

$\mathbb{Z}/12\mathbb{Z}$

$G = \mathbb{Z}$ $\quad H = 12\mathbb{Z}$

Cosets $\mathbb{Z}/12\mathbb{Z}$ cover

$0+12\mathbb{Z},\ 1+12\mathbb{Z},\ \cdots,\ 11+12\mathbb{Z}$

$H = G_x$ $\quad G/G_x$ is the cosets of G by $H = G_x$

$1+12\mathbb{Z} \Rightarrow 1,\ 13,\ 25,\ -12$

$13+12\mathbb{Z} = 1+12\mathbb{Z}$

Group G Coset H

$G/H = e+H, a_2+H, \cdots, a_n+H$

$\bigcup_{k=1}^{n} a_k H = G$ (here $a_1 = e$)

Cosets $g_1+H, g_2+H, \cdots, g_{\#G}+H$

Two cosets are identical or disjoint

So take a set of disjoint cosets st have everything

If $H=\{e\}$ Then $n = \#G$

If $H = G$ Then $n = 1$

Prove $\#Gx = \#G / \#G_x$

orbit — Group — Stabilizer

Lagrange's Theorem

Group G, subgroup H, $[G:H]$ = # of cosets of G by H

Then $\#G = [G:H] \#H$

↳ Proof: $\#G = \bigcup_{k=1}^{[G:H]} a_k H$

same size: $\#H$

We want $\#Gx = \#G / \#G_x$

↳ rewrite: $\#G = \#Gx \cdot \#G_x$ done if $\#Gx = [G:G_x]$

Need to show $\#G/G_x$ is equal to $\#Gx$

If show map is 1-1 and onto, win

- onto: Say $y \in Gx$ so $\exists g$ st $gx = y$

  But $G = \cup a_k G_x$

  So $g \in G \Rightarrow g$ is in some coset

  That coset maps to y.

- 1-1: say g_1, g_2 in different cosets

  Could $g_1 x = g_2 x$?

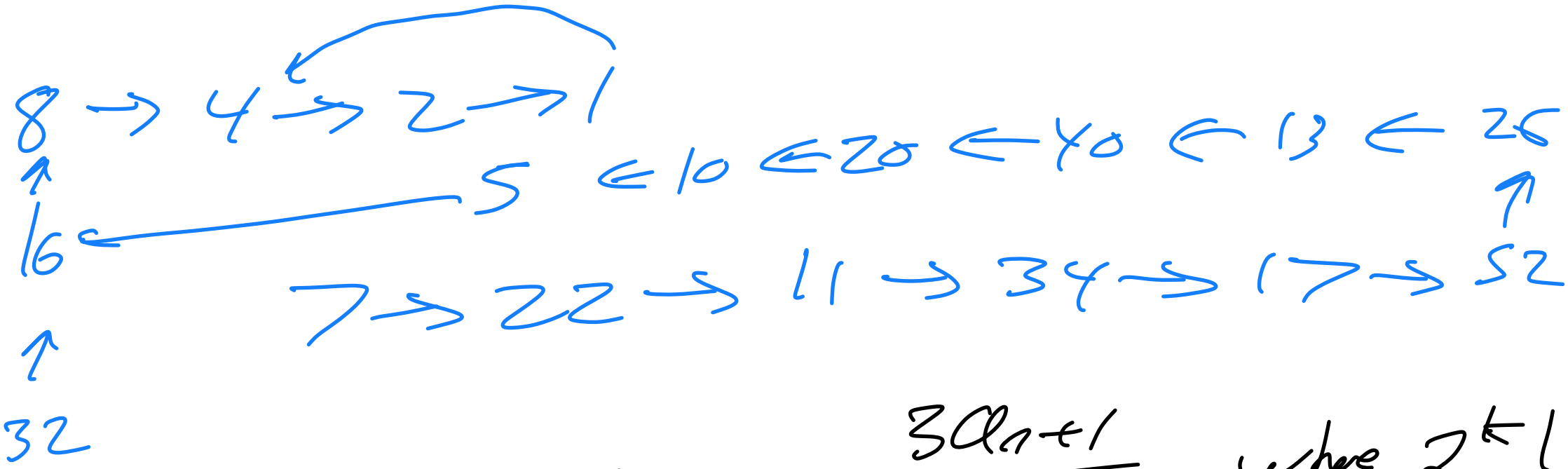
  Assume $g_1 x = g_2 x$ Then $x = g_1^{-1}(g_2 x)$

  $x = (g_1^{-1} g_2) x$

  Thus $g_1^{-1} g_2 \in G_x \Rightarrow g_1^{-1} g_2 = g$ some $g \in G_x$ or $g_2 = g_1 g$ so in same coset.

3x+1 Problem

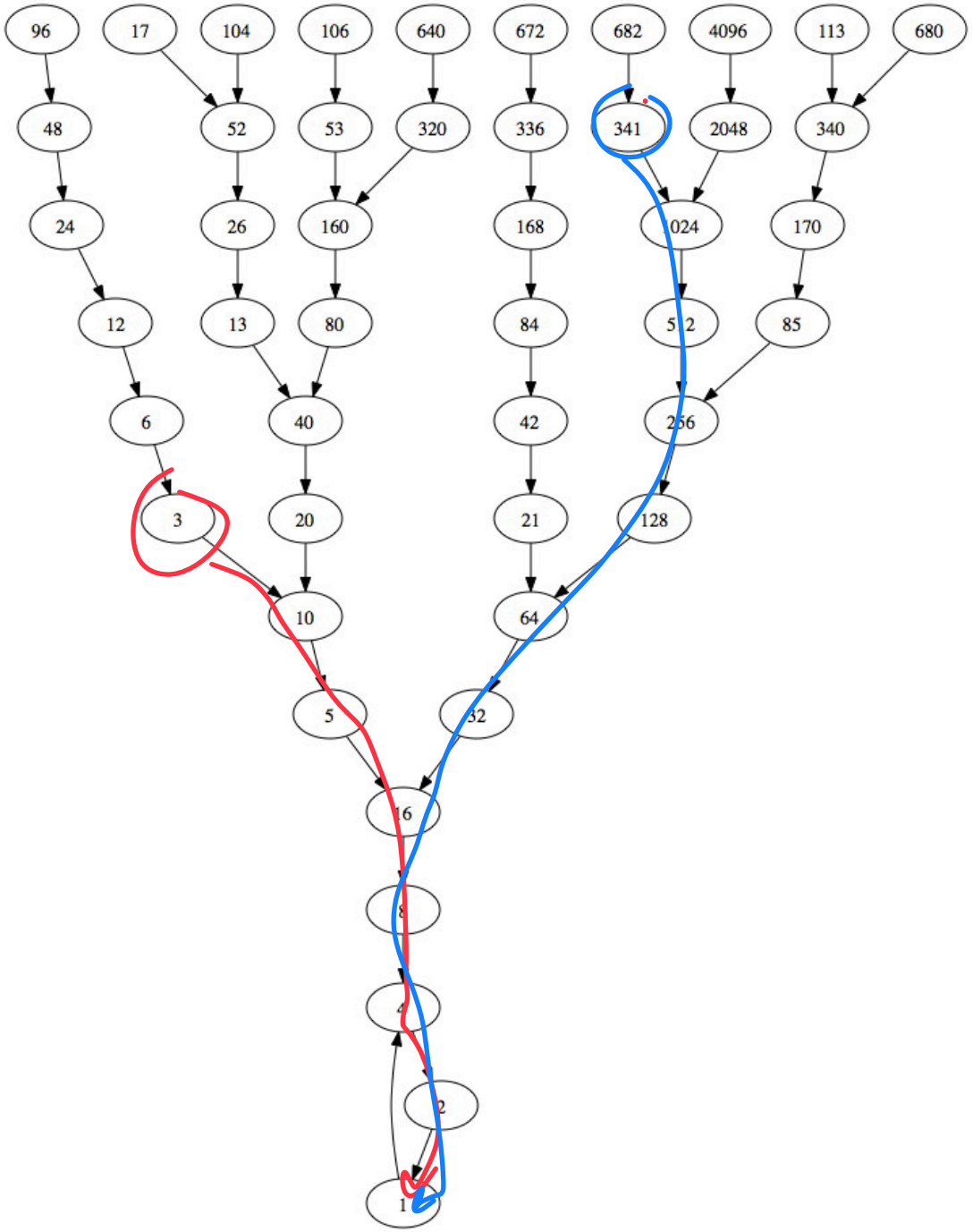
$$a_{n+1} = \begin{cases} 3a_n + 1 & \text{if } a_n \text{ odd} \\ a_n/2 & \text{if } a_n \text{ even} \end{cases}$$



accelerated Map! on odd numbers

$$a_{n+1} = \frac{3a_n+1}{2^k}$$

where $2^k \mid 3a_n+1$ but $2^{k+1} \nmid 3a_n+1$



http://www.andrewduncan.net/chaos/orbits/collatz.html

6.3. The Orbit-Stabilizer Counting Theorem

Let G be a finite group that acts on a finite set X. We start by proving a powerful theorem relating the sizes of X, G, and the various orbits and stabilizers. This counting theorem has many applications. It will be a crucial tool in our proof of Sylow's theorem in Section 6.4.

Theorem 6.21 (Orbit-Stabilizer Counting Theorem)**.** *Let G be a finite group that acts on a finite set X. Choose $x_1, \ldots, x_k \in X$ so that $Gx_1, \ldots, Gx_k$ are the distinct orbits of elements of X. Then*[4]

$$\#X = \sum_{i=1}^{k} \#Gx_i = \sum_{i=1}^{k} \frac{\#G}{\#G_{x_i}}.$$

Definition 6.23. Let G be a group. The *center of* G, denoted $Z(G)$, is the set of elements of G that commute with every element of G,

$$Z(G) = \{g \in G : gg' = g'g \text{ for every } g' \in G\}.$$

Remark 6.24. We leave it for you to prove that the center of G is a subgroup of G, and indeed, it is a normal subgroup; see Exercise 6.18.

Theorem 6.25. *Let p be a prime, and let G be a finite group with p^n elements for some $n \geq 1$. Then $Z(G) \neq \{e\}$; i.e., G contains a non-identity element that commutes with every element of G.*

Corollary 6.26. *Let p be prime, and let G be a group with p^2 elements. Then G is an abelian group.*

Proof. To ease notation, we let

$$Z = Z(G).$$

Lagrange tells us that the order of the center Z divides $\#G = p^2$, so

$$\#Z = 1 \quad \text{or} \quad \#Z = p \quad \text{or} \quad \#Z = p^2.$$

Theorem 6.25 tells us that $Z \neq \{e\}$, and hence $\#Z \neq 1$.

We next assume that $\#Z = p$, and we use this assumption to derive a contradiction. Remark 6.24 says that the center Z is a normal subgroup of G Hence we can form the quotient group G/Z, and Lagrange tells us that

$$\#(G/Z) = \#G/\#Z = p^2/p = p.$$

Thus G/Z is a group of prime order, so Proposition 2.47 tells us that it is cyclic. Let hZ be a coset that generates the group G/Z,

$$G/Z = \{Z, hZ, h^2Z, \ldots, h^{p-1}Z\},$$

In particular, this implies that[5]

$$G = Z \cup hZ \cup h^2Z \cup \cdots \cup h^{p-1}Z,$$

since every element of G is in some coset of Z.

Now let $g_1, g_2 \in G$ be arbitrary elements of G. They are each in some coset of Z, so

$$g_1 = h^{i_1}z_1 \quad \text{and} \quad g_2 = h^{i_2}z_2 \quad \text{for some } z_1, z_2 \in Z \text{ and some } 0 \le i_1, i_2 \le p-1.$$

Then using the fact that z_1 and z_2 are in the center of G, we compute

$$\begin{aligned} g_1g_2 = (h^{i_1}z_1)(h^{i_2}z_2) &= (h^{i_1}h^{i_2})(z_1z_2) = h^{i_1+i_2}z_2z_1 \\ &= (h^{i_2}h^{i_1})(z_2z_1) = (h^{i_2}z_2)(h^{i_1}z_1) = g_2g_1. \end{aligned}$$

Yikes! We've shown that every element of G commutes with every other element of G. This means that $Z = G$, which contradicts the assumption that $\#Z = p$.

To recapitulate, we know that $\#Z$ equals 1, p, or p^2, and we've ruled out $\#Z = 1$ and $\#Z = p$, so we must have $\#Z = p^2$. Hence $Z = G$, which completes the proof that G is abelian. □

Lemma 6.30. *Let p be prime, let $n \geq 0$, and let $m \geq 1$ with $p \nmid m$. Then the binomial coefficient $\binom{p^n m}{p^n}$ is not divisible by p.*

$$\binom{p^n m}{p^n} = \frac{p^n m \cdot (p^n m - 1) \cdot (p^n m - 2) \cdots (p^n m - p^n + 1)}{p^n \cdot (p^n - 1) \cdot (p^n - 2) \cdots 3 \cdot 2 \cdot 1} = \prod_{r=0}^{p^n - 1} \frac{p^n m - r}{p^n - r}.$$

How might we create a subgroup of G having order p^n? Suppose we take a subset $A \subseteq G$ having p^n elements. How can we tell if A a subgroup? One way to check is via the equivalence

$$A \text{ is a subgroup} \quad \Longleftrightarrow \quad aA = A \text{ for every } a \in A,$$

6.4. Sylow's Theorem

Theorem 6.29 (The First Part of Sylow's Theorem)**.** *Let G be a finite group, let p be a prime, and let p^n be the largest power of p that divides $\#G$. Then G has a subgroup of order p^n.*

Definition 6.31. Let G be a finite group, let p be a prime, and let p^n be the largest power of p that divides $\#G$. A subgroup $H \subseteq G$ with $\#H = p^n$ is called a *p-Sylow subgroup of G*. Theorem 6.29 tells us that G has at least one Sylow subgroup.

Remark 6.32. It is in fact true more generally that if p^r divides $\#G$, then G has a subgroup of order p^r, even if p^r isn't the largest power of p dividing $\#G$. See Exercise 6.22.

Theorem 6.35 (Sylow's Theorem)**.** *Let G be a finite group, and let p be a prime.*

(a) *G has at least one p-Sylow subgroup, i.e., there is a subgroup $H \subseteq G$ with $\#H = p^n$, where p^n is the largest power of p dividing $\#G$.*

(b) *Let H_1 and H_2 be p-Sylow subgroups of G. Then H_1 and H_2 are conjugate, i.e., there is some $g \in G$ so that $H_2 = g^{-1}H_1g$.*

(c) *Let H be a p-Sylow subgroup of G, and let k be the number of distinct p-Sylow subgroups of G. Then*

$$k \mid \#G \quad \text{and} \quad k \equiv 1 \pmod{p}.$$

(The divisibility follows from the more precise formula $k \cdot \#N_G(H) = \#G$.)

Math 355: Modern Algebra: Fall '25 (Siena)

Professor Steven J Miller: sjm1@williams.edu

Homepage:

https://web.williams.edu/Mathematics/sjmiller/public_html/310Fa25/

Groups II:

Lecture 21: 11/11/25:

https://youtu.be/uymDmjjpwP0

Chapter Six: Groups: Orbits, Stabilizers, Sylow Theorem, Exponential Function and Trig

Definition 6.23. Let G be a group. The *center of* G, denoted $Z(G)$, is the set of elements of G that commute with every element of G,

$$Z(G) = \{g \in G : gg' = g'g \text{ for every } g' \in G\}.$$

Remark 6.24. We leave it for you to prove that the center of G is a subgroup of G, and indeed, it is a normal subgroup; see Exercise 6.18.

Proof: • identity: show $e \in Z(G)$

• closure: $g_1, g_2 \in Z(G)$ and $g \in G$

Then $g(g_1 g_2) = (g g_1) g_2 = (g_1 g) g_2$

$= g_1(g g_2) = g_1(g_2 g) = (g_1 g_2) g$

• assoc: inherits

• inverse: leaving as exercise: show if $g \in Z(G)$

So is g^{-1}

∎

Theorem 6.25. *Let p be a prime, and let G be a finite group with p^n elements for some $n \geq 1$. Then $Z(G) \neq \{e\}$; i.e., G contains a non-identity element that commutes with every element of G.*

Proof: $\#X = \sum_{k=1}^{n} \#G / \#G_{x_k}$

Take $X = G$, how shall G act on itself?

Define: $g \cdot x$ to be $g^{-1}xg$ (conjugation)

↳ if $g^{-1}xg = x \Rightarrow xg = gx$ (multiply g on left)

If x commutes with g then $g^{-1}xg = x$

Stabilizer of x, G_x, is all g which commute with x.

$\#X = p^n$ $\quad \#G = p^n$ $\quad \#G_{x_k} \in \{1, p, p^2, \ldots, p^n\}$

$\#G / \#G_{x_k} \in \{p^n, p^{n-1}, \ldots, 1\}$

$$\#X = \sum_{k=1}^{n} \#G / \#G_{x_k}$$

$$p^n = \sum_{k=1}^{n} p^{n-r_k} \quad \text{where } r_k \in \{n, n-1, \ldots, 0\}$$

p^n: multiple of p

$\sum_{k=1}^{n} p^{n-r_k}$: multiple of p

↳ term $p^{n-r_k} = \frac{\#G}{\#G_{x_k}}$ is not a multiple of p only when $\#G_{x_k} = p^n$

Ndk: $G_e = \{g \text{ st } g^{-1}eg = e\} = G$

At least one term on RHS is not a multiple of p

Must be at least one more element with stabilizer of size p^n else RHS is (multiple of p) + 1, contradicts $p \mid$ LHS.

So $\exists x$ st stabilizer is all of G, means x commutes with all of G, so $x \in Z(G)$ (and $x \neq e$)

$$\iiint_{\text{sphere}(R)} (x^2+y^2)\,dV$$

$$dV = \rho^2 \sin\varphi \, d\rho \, d\theta \, d\varphi$$

$$z = \rho\cos\varphi$$

$$x = \rho\sin\varphi\cos\theta$$

$$y = \rho\sin\varphi\sin\theta$$

$$= \int_{\text{bounds}} \int\int \rho^2\sin^2\varphi \cdot \rho^2 \sin\varphi \, d\rho \, d\theta \, d\varphi$$

$(1-\cos^2\varphi)\cos\varphi$

$$x^2 + y^2 + z^2 - z^2 = \rho^2 - z^2$$

$$= \int_{\text{bounds}} \iiint (\rho^2 - \rho^2\cos^2\varphi)\,\rho^2\sin\varphi \, d\rho \, d\theta \, d\varphi$$

$$\int_{\varphi=0}^{\pi} \cos^2\varphi \sin\varphi \, d\varphi =$$

$$\int_{\varphi=0}^{\pi} \cos^2\varphi \sin\varphi \, d\varphi$$

$u = \cos\varphi$ $\quad du = -\sin\varphi \, d\varphi$ (minus sign) $(-\sin\ \ )$

$\varphi = 0, u = 1$

$\varphi = \pi, u = -1$

$$-\int_{1}^{-1} u^2 \, du = \int_{-1}^{1} u^2 \, du = \frac{u^3}{3}\Big|_{-1}^{1} = \frac{2}{3}$$

$u =$ $\quad dv =$

Corollary 6.26. *Let p be prime, and let G be a group with p^2 elements. Then G is an abelian group.*

Proof. To ease notation, we let

$$Z = Z(G).$$

Lagrange tells us that the order of the center Z divides $\#G = p^2$, so

$$\#Z = 1 \quad \text{or} \quad \#Z = p \quad \text{or} \quad \#Z = p^2.$$

Theorem 6.25 tells us that $Z \neq \{e\}$, and hence $\#Z \neq 1$.

We next assume that $\#Z = p$, and we use this assumption to derive a contradiction. Remark 6.24 says that the center Z is a normal subgroup of G Hence we can form the quotient group G/Z, and Lagrange tells us that

$$\#(G/Z) = \#G/\#Z = p^2/p = p.$$

Thus G/Z is a group of prime order, so Proposition 2.47 tells us that it is cyclic. Let hZ be a coset that generates the group G/Z,

$$G/Z = \{Z, hZ, h^2Z, \ldots, h^{p-1}Z\},$$

In particular, this implies that[5]

$$G = Z \cup hZ \cup h^2Z \cup \cdots \cup h^{p-1}Z,$$

since every element of G is in some coset of Z.

Now let $g_1, g_2 \in G$ be arbitrary elements of G. They are each in some coset of Z, so

$$g_1 = h^{i_1}z_1 \quad \text{and} \quad g_2 = h^{i_2}z_2 \quad \text{for some } z_1, z_2 \in Z \text{ and some } 0 \le i_1, i_2 \le p-1.$$

Then using the fact that z_1 and z_2 are in the center of G, we compute

$$\begin{aligned} g_1g_2 &= (h^{i_1}z_1)(h^{i_2}z_2) = (h^{i_1}h^{i_2})(z_1z_2) = h^{i_1+i_2}z_2z_1 \\ &= (h^{i_2}h^{i_1})(z_2z_1) = (h^{i_2}z_2)(h^{i_1}z_1) = g_2g_1. \end{aligned}$$

Yikes! We've shown that every element of G commutes with every other element of G. This means that $Z = G$, which contradicts the assumption that $\#Z = p$.

To recapitulate, we know that $\#Z$ equals 1, p, or p^2, and we've ruled out $\#Z = 1$ and $\#Z = p$, so we must have $\#Z = p^2$. Hence $Z = G$, which completes the proof that G is abelian. □

$p=3$, $\#G=9$

If $\exists$ element of order 9, then G is cyclic. Assume all $x \neq e$ have order 3.

$\{e, x, x^2, y, y^2, xy, \ldots$

Could xy be one of these?

If $xy=e \to y = x^{-1} = x^2$

If $xy=x \to y = e$

If $xy=x^2 \to y = x$

If $xy=y \to x=e$

If $xy=y^2 \to x=y$

Lemma 6.30. *Let p be prime, let $n \geq 0$, and let $m \geq 1$ with $p \nmid m$. Then the binomial coefficient $\binom{p^n m}{p^n}$ is not divisible by p.*

$$\binom{p^n m}{p^n} = \frac{p^n m \cdot (p^n m - 1) \cdot (p^n m - 2) \cdots (p^n m - p^n + 1)}{p^n \cdot (p^n - 1) \cdot (p^n - 2) \cdots 3 \cdot 2 \cdot 1} = \prod_{r=0}^{p^n - 1} \frac{p^n m - r}{p^n - r}.$$

power of p dividing $p^n m - r$ is same as for $p^n - r$.

Does this fill by induction?

write r as $p^a b$ where $p \nmid b$ and $0 \leq a < n$

↳ so $\dfrac{p^n m - r}{p^n - r} = \dfrac{p^n m - p^a b}{p^n - p^a b} = \dfrac{p^a}{p^a} \cdot \dfrac{p^{n-a} m - b}{p^{n-a} - b}$

multiples of p as $n - a > 0$

as b is not a mult of p, top/bottom not a mult of p

How might we create a subgroup of G having order p^n? Suppose we take a subset $A \subseteq G$ having p^n elements. How can we tell if A a subgroup? One way to check is via the equivalence

$$A \text{ is a subgroup} \iff aA = A \text{ for every } a \in A,$$

$\Rightarrow$ Consider aA, must show equals A.

↳ choose $x \in A$ must find $\tilde{x}$ st $a\tilde{x} = x$

Take $\tilde{x} = a^{-1}x \in A$ by closure!

Then $a\tilde{x} = a(a^{-1}x) = (aa^{-1})x = ex = x$

Shows $A \subset aA \subset A$ by closure, so done.

$\Leftarrow$ Assume $\forall a \in A \quad aA = A$: prove A is a subgroup.

Pf: • assoc: inherited

• closure: $a_1, a_2 \in A$ is $a_1 a_2 \in A$?

Must show $(a_1 a_2)A = A$

But $(a_1 a_2)A = a_1(a_2 A) = a_1 A = A$

• inverses: if $a \in A$ show $a^{-1} A$.

But $a \in A \rightarrow aA = A$ mult on left by a^{-1}

$\hookrightarrow a^{-1} a A = a^{-1} A$ or $eA = a^{-1}A$ or $A = a^{-1}A$

• identity: Must show $e \in A$.

If $a \in A$ since $aA = A$ Then $\exists x \in A$

s.t. $ax = a \Rightarrow x = e$ so $e \in A$ ∎

6.4. Sylow's Theorem

Theorem 6.29 (The First Part of Sylow's Theorem)**.** *Let G be a finite group, let p be a prime, and let p^n be the largest power of p that divides $\#G$. Then G has a subgroup of order p^n.*

Definition 6.31. Let G be a finite group, let p be a prime, and let p^n be the largest power of p that divides $\#G$. A subgroup $H \subseteq G$ with $\#H = p^n$ is called a *p-Sylow subgroup of G*. Theorem 6.29 tells us that G has at least one Sylow subgroup.

Remark 6.32. It is in fact true more generally that if p^r divides $\#G$, then G has a subgroup of order p^r, even if p^r isn't the largest power of p dividing $\#G$. See Exercise 6.22.

Theorem 6.35 (Sylow's Theorem)**.** *Let G be a finite group, and let p be a prime.*

(a) *G has at least one p-Sylow subgroup, i.e., there is a subgroup $H \subseteq G$ with $\#H = p^n$, where p^n is the largest power of p dividing $\#G$.*

(b) *Let H_1 and H_2 be p-Sylow subgroups of G. Then H_1 and H_2 are conjugate, i.e., there is some $g \in G$ so that $H_2 = g^{-1}H_1g$.*

(c) *Let H be a p-Sylow subgroup of G, and let k be the number of distinct p-Sylow subgroups of G. Then*

$$k \mid \#G \quad \text{and} \quad k \equiv 1 \pmod{p}.$$

(The divisibility follows from the more precise formula $k \cdot \#N_G(H) = \#G$.)

6.4. Sylow's Theorem

Theorem 6.29 (The First Part of Sylow's Theorem). *Let G be a finite group, let p be a prime, and let p^n be the largest power of p that divides $\#G$. Then G has a subgroup of order p^n.*

USE $\#X = \sum_{i=1}^{k} \#G / \#G_{x_i}$

What is X? All subsets of size p?

How does G act on X? Left multiplication

$(x^2)' = 2x$ $\quad (x^{3/2})' = \frac{3}{2}x^{\frac{1}{2}}$ $\quad (x^{\sqrt{2}})' = \sqrt{2}\,x^{\sqrt{2}-1}$

$$\lim_{h\to 0} \frac{f(x+h)-f(x)}{h}$$

$(x+h)^2 = x^2+2xh+h^2$

Binomial Thm

$(x+h)^n$

$(x+h)^{3/2} = ?$

$$\lim_{h\to 0} \frac{(x+h)^{3/2}-x^{3/2}}{h} * \frac{(x+h)^{\frac{3}{2}}+x^{3/2}}{(x+h)^{3/2}+x^{3/2}}$$

$$= \lim_{h\to 0} \frac{(x+h)^3-x^3}{h} \cdot \frac{1}{(x+h)^{3/2}+x^{3/2}}$$

$3x^2$

$\frac{1}{2x^{3/2}}$

for $(x^{3/2})'$ could also do:

$$f(x) = x^{3/2} \qquad g(x) = f(x)^2 = x^3$$

so $g'(x) = 2f(x)f'(x) = 3x^2$

thus $f'(x) = \frac{3}{2}\frac{x^2}{f(x)} = \frac{3}{2}\frac{x^2}{x^{3/2}} = \frac{3}{2}x^{\frac{1}{2}}$

$$x^{\sqrt{2}} = e^{\sqrt{2}\ln x} = \sum_{n=0}^{\infty} \frac{(\sqrt{2}\ln x)^n}{n!}$$

Exponential Function and Trigonometry

$$\exp(x) := \sum_{n=0}^{\infty} \frac{x^n}{n!} \qquad x \in \mathbb{C}, \text{ write } e^x$$

$$e^x e^y = e^{x+y}$$

$$\left(\sum_{n=0}^{\infty} \frac{x^n}{n!}\right)\left(\sum_{m=0}^{\infty} \frac{y^m}{m!}\right) \stackrel{?}{=} \sum_{k=0}^{\infty} \frac{(x+y)^k}{k!}$$

$$\sum_{k=0}^{\infty} \sum_{l=0}^{k} \frac{x^{k-l} y^l}{(k-l)!\, l!} \frac{k!}{k!} = \sum_{k=0}^{\infty} \frac{1}{k!} \underbrace{\sum_{l=0}^{\infty} \binom{k}{l} x^{k-l} y^l}_{(x+y)^k}$$

$e^{ix} = \cos x + i\sin x$

$e^{-ix} = \cos(-x) + i\sin(-x)$

$= \cos x - i\sin x$

$e^{ix}e^{-ix} = e^0 = 1$

$(\cos x + i\sin x)(\cos x - i\sin x) = 1$

$\cos^2 x + \sin^2 x = 1$

$e^{ix}e^{iy} = e^{i(x+y)}$

$(\cos x + i\sin x)(\cos y + i\sin y) = \cos(x+y) + i\sin(x+y)$

$\cos x\cos y - \sin x\sin y = \cos(x+y)$

$\sin x\cos y + \cos x\sin y = \sin(x+y)$

$e^X e^Y = e^Z$ and why care (differential equations!)

$$e^x = \sum_{n=0}^{\infty} x^n / n! \qquad x \in \mathbb{C}$$

$$e^A = \sum_{n=0}^{\infty} \frac{A^n}{n!}$$

need A to be a square matrix

Baker–Campbell–Hausdorff formula

8 languages

Article Talk Read Edit View history Tools

From Wikipedia, the free encyclopedia

$[X,Y]=XY-YX$

In mathematics, the **Baker–Campbell–Hausdorff formula** gives the value of Z that solves the equation

$$e^X e^Y = e^Z$$

for possibly noncommutative X and Y in the Lie algebra of a Lie group. There are various ways of writing the formula, but all ultimately yield an expression for Z in Lie algebraic terms, that is, as a formal series (not necessarily convergent) in X and Y and iterated commutators thereof. The first few terms of this series are:

$$Z = X + Y + \frac{1}{2}[X,Y] + \frac{1}{12}[X,[X,Y]] - \frac{1}{12}[Y,[X,Y]] + \cdots,$$

where "$\cdots$" indicates terms involving higher commutators of X and Y. If X and Y are sufficiently small elements of the Lie algebra $\mathfrak{g}$ of a Lie group G, the series is convergent. Meanwhile, every element g sufficiently close to the identity in G can be expressed as $g = e^X$ for a small X in $\mathfrak{g}$. Thus, we can say that *near the identity* the group multiplication in G —written as $e^X e^Y = e^Z$—can be expressed in purely Lie algebraic terms. The Baker–Campbell–Hausdorff formula can be used to give comparatively simple proofs of deep results in the Lie group–Lie algebra correspondence.

If X and Y are sufficiently small $n \times n$ matrices, then Z can be computed as the logarithm of $e^X e^Y$, where the exponentials and the logarithm can be computed as power series. The point of the Baker–Campbell–Hausdorff formula is then the highly nonobvious claim that $Z := \log\left(e^X e^Y\right)$ can be expressed as a series in repeated commutators of X and Y.

https://en.wikipedia.org/wiki/Baker%E2%80%93Campbell%E2%80%93Hausdorff_formula

The first few terms are well-known, with all higher-order terms involving $[X,Y]$ and commutator nestings thereof (thus in the Lie algebra):

$$
\begin{aligned}
Z(X,Y) &= \log(\exp X \exp Y) \\
&= X + Y + \frac{1}{2}[X,Y] + \frac{1}{12}\left([X,[X,Y]] + [Y,[Y,X]]\right) \\
&\quad - \frac{1}{24}[Y,[X,[X,Y]]] \\
&\quad - \frac{1}{720}\left([Y,[Y,[Y,[Y,X]]]] + [X,[X,[X,[X,Y]]]]\right) \\
&\quad + \frac{1}{360}\left([X,[Y,[Y,[Y,X]]]] + [Y,[X,[X,[X,Y]]]]\right) \\
&\quad + \frac{1}{120}\left([Y,[X,[Y,[X,Y]]]] + [X,[Y,[X,[Y,X]]]]\right) \\
&\quad + \frac{1}{240}\left([X,[Y,[X,[Y,[X,Y]]]]]\right) \\
&\quad + \frac{1}{720}\left([X,[Y,[X,[X,[X,Y]]]]] - [X,[X,[Y,[Y,[X,Y]]]]]\right) \\
&\quad + \frac{1}{1440}\left([X,[Y,[Y,[Y,[X,Y]]]]] - [X,[X,[Y,[X,[X,Y]]]]]\right) + \cdots
\end{aligned}
$$

The above lists all summands of order 6 or lower (i.e. those containing 6 or fewer X's and Y's). The $X \leftrightarrow Y$ (anti-)/symmetry in alternating orders of the expansion, follows from $Z(Y,X) = -Z(-X,-Y)$. A complete elementary proof of this formula can be found in the article on the derivative of the exponential map.

Matrix Lie group illustration [edit]

For a matrix Lie group $G \subset \mathrm{GL}(n, \mathbb{R})$ the Lie algebra is the tangent space of the identity *I*, and the commutator is simply $[X, Y] = XY - YX$; the exponential map is the standard exponential map of matrices,

$$\exp X = e^X = \sum_{n=0}^{\infty} \frac{X^n}{n!}.$$

When one solves for *Z* in

$$e^Z = e^X e^Y,$$

using the series expansions for $\exp$ and $\log$ one obtains a simpler formula:

$$Z = \sum_{n>0} \frac{(-1)^{n-1}}{n} \sum_{\substack{r_i+s_i>0 \\ 1\le i\le n}} \frac{X^{r_1} Y^{s_1} \cdots X^{r_n} Y^{s_n}}{r_1! s_1! \cdots r_n! s_n!}, \quad \|X\| + \|Y\| < \log 2, \|Z\| < \log 2.$$

[nb 2] The first, second, third, and fourth order terms are:

- $z_1 = X + Y$
- $z_2 = \frac{1}{2}(XY - YX)$
- $z_3 = \frac{1}{12}\left(X^2Y + XY^2 - 2XYX + Y^2X + YX^2 - 2YXY\right)$
- $z_4 = \frac{1}{24}\left(X^2Y^2 - 2XYXY - Y^2X^2 + 2YXYX\right).$

The formulas for the various z_j's is *not* the Baker–Campbell–Hausdorff formula. Rather, the Baker–Campbell–Hausdorff formula is one of various expressions for z_j's *in terms of repeated commutators of* X *and* Y. The point is that it is far