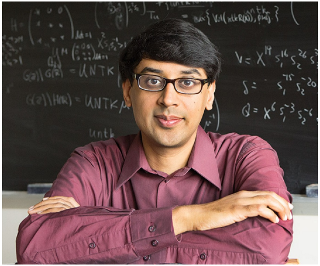
The Factorial Function and Generalization

Based on the Paper of Manjul Bhargava

Nitesh Mathur

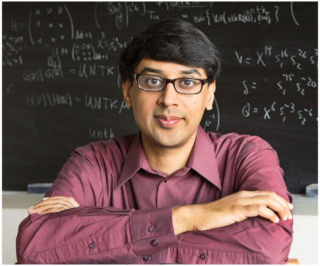
March 9, 2018

About the Author



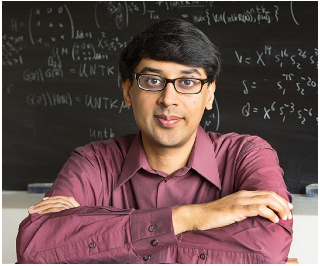
About the Author

- Paper Published in 2000



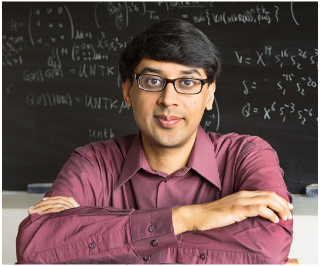
About the Author

- Paper Published in 2000
- Since worked on Higher Composition Laws, 15 and 290 Theorems, and Average Rank of Elliptic Curves



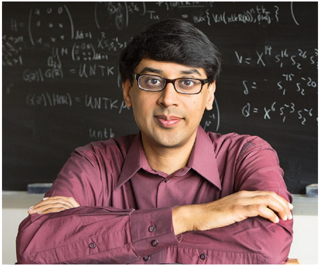
About the Author

- Paper Published in 2000
- Since worked on Higher Composition Laws, 15 and 290 Theorems, and Average Rank of Elliptic Curves
- Fields Medal Recipient in 2014



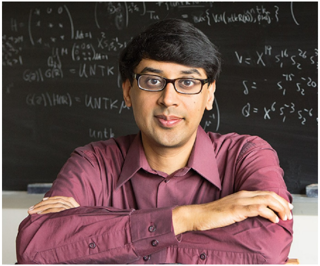
About the Author

- Paper Published in 2000
- Since worked on Higher Composition Laws, 15 and 290 Theorems, and Average Rank of Elliptic Curves
- Fields Medal Recipient in 2014
- Doctoral Advisor: Andrew Wiles



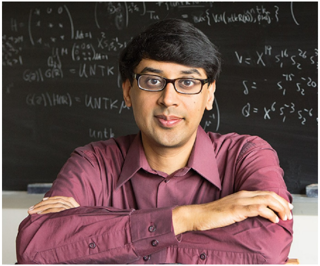
About the Author

- Paper Published in 2000
- Since worked on Higher Composition Laws, 15 and 290 Theorems, and Average Rank of Elliptic Curves
- Fields Medal Recipient in 2014
- Doctoral Advisor: Andrew Wiles
- Professor at Princeton, Leiden University, and adjunct professor in several others.



About the Author

- Paper Published in 2000
- Since worked on Higher Composition Laws, 15 and 290 Theorems, and Average Rank of Elliptic Curves
- Fields Medal Recipient in 2014
- Doctoral Advisor: Andrew Wiles
- Professor at Princeton, Leiden University, and adjunct professor in several others.
- Musician (Tabla Player)



Introduction

Introduction

- Definition: $n! = \prod_{k=1}^{n} k = n(n-1)(n-2)...(3)(2)(1)$

Introduction

- Definition: $n! = \prod_{k=1}^{n} k = n(n-1)(n-2)...(3)(2)(1)$
- Examples: $5! = (5)(4)(3)(2)(1) = 120$

- Definition: $n! = \prod_{k=1}^{n} k = n(n-1)(n-2)...(3)(2)(1)$
- Examples: $5! = (5)(4)(3)(2)(1) = 120$
- The Gamma Function

Introduction

- Definition: $n! = \prod_{k=1}^{n} k = n(n-1)(n-2)...(3)(2)(1)$
- Examples: $5! = (5)(4)(3)(2)(1) = 120$
- The Gamma Function
- $\Gamma(z) = \int_0^\infty t^{z-1}e^{-t}\ dt$

Introduction

- Definition: $n! = \prod_{k=1}^{n} k = n(n-1)(n-2)...(3)(2)(1)$
- Examples: $5! = (5)(4)(3)(2)(1) = 120$
- The Gamma Function
- $\Gamma(z) = \int_0^\infty t^{z-1}e^{-t}\ dt$
- $\Gamma(n) = (n-1)!$

Introduction

- Definition: $n! = \prod_{k=1}^{n} k = n(n-1)(n-2)...(3)(2)(1)$
- Examples: $5! = (5)(4)(3)(2)(1) = 120$
- The Gamma Function
- $\Gamma(z) = \int_0^\infty t^{z-1} e^{-t} \, dt$
- $\Gamma(n) = (n-1)!$
- $\Gamma(5) = 4! = 24, \Gamma(1/2) = \sqrt{\pi}$

Factorial Function in Number Theory

Factorial Function in Number Theory

- **Theorem 1**
  For any nonnegative integers, k and $l, (k+l)!$ is a multiple of $k!l!$.

Factorial Function in Number Theory

- **Theorem 1**
  For any nonnegative integers, k and $l, (k+l)!$ is a multiple of $k!l!$.
- **Theorem 2** Let f be a primitive polynomial of degree k and let $d(\mathbb{Z}, f) = \text{gcd}\{f(a) : a \in \mathbb{Z}\}$ Then, $d(\mathbb{Z}, f)$ divides $k!$.

Factorial Function in Number Theory

- **Theorem 1**
  For any nonnegative integers, k and $l, (k+l)!$ is a multiple of $k!l!$.
- **Theorem 2** Let f be a primitive polynomial of degree k and let $d(\mathbb{Z}, f) = \text{gcd}\{f(a) : a \in \mathbb{Z}\}$ Then, $d(\mathbb{Z}, f)$ divides $k!$.
- **Theorem 3**
  Let $a_0, a_1, ...a_n \in \mathbb{Z}$ be any $n+1$ integers. Then their product of their pairwise differences

$$\prod_{i<j}(a_i - a_j)$$

is a multiple of $0!1!...n!$

Factorial Function in Number Theory

- **Theorem 1**
  For any nonnegative integers, k and l, $(k+l)!$ is a multiple of $k!l!$.
- **Theorem 2** Let f be a primitive polynomial of degree k and let $d(\mathbb{Z}, f) = \text{gcd}\{f(a) : a \in \mathbb{Z}\}$ Then, $d(\mathbb{Z}, f)$ divides $k!$.
- **Theorem 3**
  Let $a_0, a_1, ...a_n \in \mathbb{Z}$ be any $n+1$ integers. Then their product of their pairwise differences
  $$\prod_{i<j}(a_i - a_j)$$
  is a multiple of $0!1!...n!$
- **Theorem 4** The number of polynomial functions from $\mathbb{Z}$ to $\mathbb{Z}/n\mathbb{Z}$ is given by
  $$\prod_{k=0}^{n-1} \frac{n}{\text{gcd}(n, k!)}$$

Motivation

These theorems are true on $\mathbb{Z}$.

Is there a "Generalized Factorial Function" so that for any subset S of $\mathbb{Z}$, the theorems mentioned above still remain true?

p-Ordering

Let $S \subset \mathbb{Z}$ and fix a prime p.

p-Ordering

Let $S \subset \mathbb{Z}$ and fix a prime p.

- Choose $a_0 \in S$

p-Ordering

Let $S \subset \mathbb{Z}$ and fix a prime p.

- Choose $a_0 \in S$
- Choose $a_1 \in S$ that minimizes the highest power of p dividing $a_1 - a_0$

p-Ordering

Let $S \subset \mathbb{Z}$ and fix a prime p.

- Choose $a_0 \in S$
- Choose $a_1 \in S$ that minimizes the highest power of p dividing $a_1 - a_0$
- Choose an element $a_2 \in S$ that minimizes the highest power of p dividing $(a_2 - a_0)(a_2 - a_1)$

p-Ordering

Let $S \subset \mathbb{Z}$ and fix a prime p.

- Choose $a_0 \in S$
- Choose $a_1 \in S$ that minimizes the highest power of p dividing $a_1 - a_0$
- Choose an element $a_2 \in S$ that minimizes the highest power of p dividing $(a_2 - a_0)(a_2 - a_1)$
- For the k^{th} step, choose an element $a_k \in S$ that minimizes the highest power of p dividing $(a_k - a_0)(a_k - a_1) \cdot \ldots \cdot (a_k - a_{k-1})$

p-Ordering

Let $S \subset \mathbb{Z}$ and fix a prime p.

- Choose $a_0 \in S$
- Choose $a_1 \in S$ that minimizes the highest power of p dividing $a_1 - a_0$
- Choose an element $a_2 \in S$ that minimizes the highest power of p dividing $(a_2 - a_0)(a_2 - a_1)$
- For the k^{th} step, choose an element $a_k \in S$ that minimizes the highest power of p dividing $(a_k - a_0)(a_k - a_1) \cdot \ldots \cdot (a_k - a_{k-1})$
- Notation: For each $k, v_k(S, p)$ represents the highest power of p that fulfills the above expression $\{v_0(S, p), v_1(S, p), ..\}$

Example

Let S be the set of all primes. $S = \{2, 3, 5, 7...\}$ and fix prime $p = 2$

Example

Let S be the set of all primes. $S = \{2, 3, 5, 7...\}$ and fix prime $p = 2$

- Let $a_0 = 19$

Example

Let S be the set of all primes. $S = \{2, 3, 5, 7...\}$ and fix prime $p = 2$

- Let $a_0 = 19$
- We need to pick a_1.
  The highest power of p that divides $2 - a_0 = -17$ is $2^0 = 1$

Example

Let S be the set of all primes. $S = \{2, 3, 5, 7...\}$ and fix prime $p = 2$

- Let $a_0 = 19$
- We need to pick a_1.
  The highest power of p that divides $2 - a_0 = -17$ is $2^0 = 1$
- Let's pick a_2 $(a_2 - 19)(a_2 - 2)$. Pick
  $a_2 = 5 \Rightarrow (5 - 19)(5 - 2) = (-14)(3) = (2 \cdot -7)(3)$
  The highest power of p that divides $(a_2 - 19)(a_2 - 2)$ is $2^1 = 2$.

Example

Let S be the set of all primes. $S = \{2, 3, 5, 7...\}$ and fix prime $p = 2$

- Let $a_0 = 19$
- We need to pick a_1.
  The highest power of p that divides $2 - a_0 = -17$ is $2^0 = 1$
- Let's pick a_2 $(a_2 - 19)(a_2 - 2)$. Pick
  $a_2 = 5 \Rightarrow (5 - 19)(5 - 2) = (-14)(3) = (2 \cdot -7)(3)$
  The highest power of p that divides $(a_2 - 19)(a_2 - 2)$ is $2^1 = 2$.
- Similarly, for a_3, we need $(a_3 - 19)(a_3 - 2)(a_3 - 5)$. In this case, the highest power of p that divides the product above is $a_3 = 17$
  $(17 - 19)(17 - 2)(17 - 5) = (-2)(15)(2^2 \cdot 3)$ The corresponding power here is $2^3 = 8$.

Example

Let S be the set of all primes. $S = \{2, 3, 5, 7...\}$ and fix prime $p = 2$

- Let $a_0 = 19$
- We need to pick a_1.
  The highest power of p that divides $2 - a_0 = -17$ is $2^0 = 1$
- Let's pick a_2 $(a_2 - 19)(a_2 - 2)$. Pick
  $a_2 = 5 \Rightarrow (5 - 19)(5 - 2) = (-14)(3) = (2 \cdot -7)(3)$
  The highest power of p that divides $(a_2 - 19)(a_2 - 2)$ is $2^1 = 2$.
- Similarly, for a_3, we need $(a_3 - 19)(a_3 - 2)(a_3 - 5)$. In this case, the highest power of p that divides the product above is $a_3 = 17$
  $(17 - 19)(17 - 2)(17 - 5) = (-2)(15)(2^2 \cdot 3)$ The corresponding power here is $2^3 = 8$.
- Similarly for the rest a_k

Examples Continued

- The p-ordering for $p = 2$ is as follows: $\{19, 2, 5, 17, 23, 31, ...,\}$ and its corresponding p-sequence is as follows, $\{1, 1, 2, 8, 16, 128, ...\}$

Back to Theory

Back to Theory

- Construct such a p ordering for every p (Note: Not unique)

Back to Theory

- Construct such a p ordering for every p (Note: Not unique)
- **Punchline 1**: The associated p-sequence of S is independent of the choice of p-ordering.

Back to Theory

- Construct such a p ordering for every p (Note: Not unique)
- **Punchline 1**: The associated p-sequence of S is independent of the choice of p-ordering.
- **Punchline 2** Let S be any subset of $\mathbb{Z}$. Then the *factorial function* of S, denoted by $k!_S$ is defined by

$$k!_s = \prod_p v_k(S, p)$$

Back to Example

Back to Example

- The p-ordering for the prime subset of $\mathbb{Z}$ is as follows:

Back to Example

- The p-ordering for the prime subset of $\mathbb{Z}$ is as follows:
- $p = 2$
  p-ordering: $\{19, 2, 5, 17, 23, 31, ..., \}$
  p-sequence is as follows, $\{1, 1, 2, 8, 16, 128, ...\}$

Back to Example

- The p-ordering for the prime subset of $\mathbb{Z}$ is as follows:
- $p = 2$
  p-ordering: $\{19, 2, 5, 17, 23, 31, ..., \}$
  p-sequence is as follows, $\{1, 1, 2, 8, 16, 128, ...\}$
- $p = 3$
  p-ordering: $\{2, 3, 7, 5, 13, 17, 19, ...\}$
  p-sequence: $\{1, 1, 1, 3, 3, 9, ...\}$

Examples

- $4!_P = 48, 6!_p = 11520, ...$
- Notice, one has to multiply across. Each k represents an index in each p-sequence.

Table of values of $v_k(P, p)$ and $k!_P$

	$p = 2$	$p = 3$	$p = 5$	$p = 7$	$p = 11$	...	$k!_P$
$k = 0$	1	1	1	1	1	...	1×1×1×1×1×... = 1
$k = 1$	1	1	1	1	1	...	1×1×1×1×1×... = 1
$k = 2$	2	1	1	1	1	...	2×1×1×1×1×... = 2
$k = 3$	8	3	1	1	1	...	8×3×1×1×1×... = 24
$k = 4$	16	3	1	1	1	...	16×3×1×1×1×... = 48
$k = 5$	128	9	5	1	1	...	128×9×5×1×1×... = 5760
$k = 6$	256	9	5	1	1	...	256×9×5×1×1×... = 11520

The Natural Numbers

The Natural Numbers

- Consider $\mathbb{N} \subset \mathbb{Z}$ The natural ordering of $\mathbb{N} = \{1, 2, 3, ...\}$ is a p-ordering of $\mathbb{N}$.
  The p-sequences of $\mathbb{N}$ are as follows:

The Natural Numbers

- Consider $\mathbb{N} \subset \mathbb{Z}$ The natural ordering of $\mathbb{N} = \{1, 2, 3, ...\}$ is a p-ordering of $\mathbb{N}$.
  The p-sequences of $\mathbb{N}$ are as follows:
- p = 2: $\{1, 1, 2, 2, 8, 8, 16, 16, ...\}$

The Natural Numbers

- Consider $\mathbb{N} \subset \mathbb{Z}$ The natural ordering of $\mathbb{N} = \{1, 2, 3, ...\}$ is a p-ordering of $\mathbb{N}$.
  The p-sequences of $\mathbb{N}$ are as follows:
- p = 2: $\{1, 1, 2, 2, 8, 8, 16, 16, ...\}$
- p = 3: $\{1, 1, 1, 3, 3, 3, 9, 9, 9, ...\}$

The Natural Numbers

- Consider $\mathbb{N} \subset \mathbb{Z}$ The natural ordering of $\mathbb{N} = \{1, 2, 3, ...\}$ is a p-ordering of $\mathbb{N}$.
  The p-sequences of $\mathbb{N}$ are as follows:
- p = 2: $\{1, 1, 2, 2, 8, 8, 16, 16, ...\}$
- p = 3: $\{1, 1, 1, 3, 3, 3, 9, 9, 9, ...\}$
- p = : $\{1, 1, 1, 1, 1, 5, 5, 5, 5, 5, 25, ..\}$

The Natural Numbers

- Consider $\mathbb{N} \subset \mathbb{Z}$ The natural ordering of $\mathbb{N} = \{1, 2, 3, ...\}$ is a p-ordering of $\mathbb{N}$.
  The p-sequences of $\mathbb{N}$ are as follows:
- p = 2: $\{1, 1, 2, 2, 8, 8, 16, 16, ...\}$
- p = 3: $\{1, 1, 1, 3, 3, 3, 9, 9, 9, ...\}$
- p = : $\{1, 1, 1, 1, 1, 5, 5, 5, 5, 5, 25, ..\}$
- p = 7: $\{1, 1, 1, 1, 1, 1, 1, 7, 7, 7, 7, 7, ..\}$
  Check Your Results:

The Natural Numbers

- Consider $\mathbb{N} \subset \mathbb{Z}$ The natural ordering of $\mathbb{N} = \{1, 2, 3, ...\}$ is a p-ordering of $\mathbb{N}$.
  The p-sequences of $\mathbb{N}$ are as follows:
- p = 2: $\{1, 1, 2, 2, 8, 8, 16, 16, ...\}$
- p = 3: $\{1, 1, 1, 3, 3, 3, 9, 9, 9, ...\}$
- p = : $\{1, 1, 1, 1, 1, 5, 5, 5, 5, 5, 25, ..\}$
- p = 7: $\{1, 1, 1, 1, 1, 1, 1, 7, 7, 7, 7, 7, ..\}$
  Check Your Results:
- $0!_{\mathbb{N}} = 1 * 1 * 1 * 1 * 1... = 1$

The Natural Numbers

- Consider $\mathbb{N} \subset \mathbb{Z}$ The natural ordering of $\mathbb{N} = \{1, 2, 3, ...\}$ is a p-ordering of $\mathbb{N}$.
  The p-sequences of $\mathbb{N}$ are as follows:
- p = 2: $\{1, 1, 2, 2, 8, 8, 16, 16, ...\}$
- p = 3: $\{1, 1, 1, 3, 3, 3, 9, 9, 9, ...\}$
- p = : $\{1, 1, 1, 1, 1, 5, 5, 5, 5, 5, 25, ..\}$
- p = 7: $\{1, 1, 1, 1, 1, 1, 1, 7, 7, 7, 7, 7, ..\}$
  Check Your Results:
- $0!_{\mathbb{N}} = 1 * 1 * 1 * 1 * 1... = 1$
- $2!_{\mathbb{N}} = 2 * 1 * 1 * 1 * 1... = 2$

The Natural Numbers

- Consider $\mathbb{N} \subset \mathbb{Z}$ The natural ordering of $\mathbb{N} = \{1, 2, 3, ...\}$ is a p-ordering of $\mathbb{N}$.
  The p-sequences of $\mathbb{N}$ are as follows:
- p = 2: $\{1, 1, 2, 2, 8, 8, 16, 16, ...\}$
- p = 3: $\{1, 1, 1, 3, 3, 3, 9, 9, 9, ...\}$
- p = : $\{1, 1, 1, 1, 1, 5, 5, 5, 5, 5, 25, ..\}$
- p = 7: $\{1, 1, 1, 1, 1, 1, 1, 7, 7, 7, 7, 7, ..\}$
  Check Your Results:
- $0!_{\mathbb{N}} = 1 * 1 * 1 * 1 * 1... = 1$
- $2!_{\mathbb{N}} = 2 * 1 * 1 * 1 * 1... = 2$
- $3!_{\mathbb{N}} = 2 * 3 * 1 * 1 * 1... = 6$

The Natural Numbers

- Consider $\mathbb{N} \subset \mathbb{Z}$ The natural ordering of $\mathbb{N} = \{1, 2, 3, ...\}$ is a p-ordering of $\mathbb{N}$.
  The p-sequences of $\mathbb{N}$ are as follows:
- p = 2: $\{1, 1, 2, 2, 8, 8, 16, 16, ...\}$
- p = 3: $\{1, 1, 1, 3, 3, 3, 9, 9, 9, ...\}$
- p = : $\{1, 1, 1, 1, 1, 5, 5, 5, 5, 5, 25, ..\}$
- p = 7: $\{1, 1, 1, 1, 1, 1, 1, 7, 7, 7, 7, 7, ..\}$
  Check Your Results:
- $0!_{\mathbb{N}} = 1 * 1 * 1 * 1 * 1... = 1$
- $2!_{\mathbb{N}} = 2 * 1 * 1 * 1 * 1... = 2$
- $3!_{\mathbb{N}} = 2 * 3 * 1 * 1 * 1... = 6$
- $7!_{\mathbb{N}} = 16 * 9 * 5 * 1.... = 720$

More Examples

Sl. No.	Set S	$k!_S$
1	Set of natural numbers	$k!$
2	Set of even integers	$2^k \times k!$
3	Set of integers of the form $an + b$	$a^k \times k!$
4	Set of integers of the form 2^n	$(2^k - 1)(2^k - 2) \ldots (2^k - 2^{k-1})$
5	Set of integers of the form q^n for some prime q	$(q^k - 1)(q^k - 2) \ldots (q^k - q^{k-1})$
6	Set of squares of integers	$(2k)!/2$

Revisit Theorems

Revisit Theorems

- **Theorem 1**
  For any nonnegative integers, k and $l, (k+l)!_S$ is a multiple of $k!_S l!_S$.

Revisit Theorems

- **Theorem 1**
  For any nonnegative integers, k and $l, (k+l)!_S$ is a multiple of $k!_S l!_S$.
- **Theorem 2** Let f be a primitive polynomial of degree k and let $d(S, f) = \gcd\{f(a) : a \in S\}$ Then, $d(S, f)$ divides $k!_S$.

Revisit Theorems

- **Theorem 1**
  For any nonnegative integers, k and $l, (k+l)!_S$ is a multiple of $k!_S l!_S$.
- **Theorem 2** Let f be a primitive polynomial of degree k and let $d(S,f) = \gcd\{f(a) : a \in S\}$ Then, $d(S,f)$ divides $k!_S$.
- **Theorem 3**
  Let $a_0, a_1, ...a_n \in S$ be any $n+1$ integers. Then their product of their pairwise differences

$$\prod_{i<j}(a_i - a_j)$$

  is a multiple of $0!_S 1!_S ... n!_S$

Revisit Theorems

- **Theorem 1**
  For any nonnegative integers, k and $l, (k+l)!_S$ is a multiple of $k!_S l!_S$.
- **Theorem 2** Let f be a primitive polynomial of degree k and let $d(S, f) = \text{gcd}\{f(a) : a \in S\}$ Then, $d(S, f)$ divides $k!_S$.
- **Theorem 3**
  Let $a_0, a_1, ...a_n \in S$ be any $n+1$ integers. Then their product of their pairwise differences
  $$\prod_{i<j}(a_i - a_j)$$
  is a multiple of $0!_S 1!_S ... n!_S$
- **Theorem 4** The number of polynomial functions from S to $\mathbb{Z}/n\mathbb{Z}$ is given by
  $$\prod_{k=0}^{n-1} \frac{n}{\text{gcd}(n, k!_S)}$$

The Rest of the Paper

The Rest of the Paper

- A bunch of proofs.

The Rest of the Paper

- A bunch of proofs.
- Generalization to Dedekind Rings.

The Rest of the Paper

- A bunch of proofs.
- Generalization to Dedekind Rings.
- Generalization to Higher Dimensions.

The Rest of the Paper

- A bunch of proofs.
- Generalization to Dedekind Rings.
- Generalization to Higher Dimensions.
- Applications

Posed Questions

Posed Questions

- For a subset $S \subset \mathbb{Z}$, is there a natural combinatorial interpretation of $k!_S$.

Posed Questions

- For a subset $S \subset \mathbb{Z}$, is there a natural combinatorial interpretation of $k!_S$.
- What is the natural combinatorial interpretation for $\binom{n}{k}_S = \dfrac{n!_S}{k!_S(n-k)!_S}$ coefficients?

Posed Questions

- For a subset $S \subset \mathbb{Z}$, is there a natural combinatorial interpretation of $k!_S$.
- What is the natural combinatorial interpretation for $\binom{n}{k}_S = \dfrac{n!_S}{k!_S(n-k)!_S}$ coefficients?
- What is the "binomial theorem" for generalized binomial?

Sources

Bhargava, Manjul (2000). "The Factorial Function and Generalizations" (PDF). The American Mathematical Monthly. 107 (9): 783–799.

Thank You!

- Dr. O'Neil
- Dr. Donahue
- Jon Bolin
- Journal Club

Questions?