Results in Additive & Elementary Number Theory Inspired by Carl and Mel

Steven J. Miller: sjm1@williams.edu

Williams College & the Fibonacci Association

http://web.williams.edu/Mathematics/sjmiller/public_html/math/talks/talks.html

INTEGERS 2025: University of Georgia: May 14, 2025

2

MSTDs

Thanks 00

Dedicated to Carl and Mel on their 80th birthdays

images mel nathanson and carl pomerance



Thanks 00

Dedicated to Carl and Mel on their 80th birthdays

images mel nathanson and carl pomerance



https://www.sfgate.com/entertainment/article/

2-000-year-old-man-still-kicking-on-new-dvd-3280712.php



Thanks 00

Dedicated to Carl and Mel on their 80th birthdays

images mel nathanson and carl pomerance





Mel: https://schoengeometry.com/b-fintil.html Cad: https: //bread determined and for a finite state of the set of the set

//home.dartmouth.edu/news/2019/04/big-bang-theory-takes-math-notes-carl-pomerance and the state of the stat

Thanks 00

Research Inspired By Carl and Mel

◊ Inspired by Carl: Avoiding Progressions, Sums, Almost Perfect Numbers (23 colleagues, 8 papers):

Adam Lott, Ajmain Yamin, Alyssa Epstein, Andrew Best, Asimina S. Hamakiotes, Bruce Fang, Chung-Hang Kwan, Eduardo Dueñez, Enrique Treviño, Eva Fourakis, Gwyneth Moreland, Gwyneth Moreland, Jasmine Powell, Karen Huan, Katherine Cordwell, Kimsy Tor, Madeleine Weinstein, Megumi Asada, Nancy Jiang, Nathan McNew, Peter

Cohen, Sarah Manski, Sindy Xin Zhang.

◊ Inspired by MeI: MSTD (41 colleagues, 22 papers):

Amanda Bower, Andrew Keisling, Archit Kulkarni, Astrid Lilly, Brooke Orosz, Carsten Peterson, Chenyang Sun, Dan Scheinerman, David Moon, Dylan King, Elena Kim, Fei Peng, Geoffrey Iyer, Guilherme Zeus Dantas e Moura, Hong Suh, Hung Chu, Jake Wellens, Justin Cheigh, Kevin O'Bryant, Kevin Vissuet, Lily Shao, Liyang Zhang, Luc Robinson, Matthew Phang, Megumi Asada, Nathan McNew, Noah Luntzlara, Oleg Lazarev, Peter Hegarty, Prakod Ngamlamai, Ron Evans, Ruben Ascoli, Ryan Jeong, Sarah Manski, Scott Harvey-Arnold, Sean Pegado, Sean Zhang, Thao Do, Thomas C. Martinez, Victor Luo, Victor Xu.

Polymath Jr

https://geometrynyc.wixsite.com/polymathreu

Our goal is to provide research opportunities to every undergraduate who wishes to explore advanced mathematics. This online program consists of research projects in a variety of mathematical topics and runs in the spirit of the Polymath Project. Each project is mentored by an active researcher with experience in undergraduate mentoring.

Each project consists of 15-25 undergraduates, a main mentor, and graduate students and postdocs as additional mentors. The group works towards solving a research problem and writing a paper. Each participant decides what they wish to obtain from the program, and participates accordingly. The program is partially supported by NSF award DMS-2218374.

Avoiding Progressions and Sums

Thanks 00

History

In 1961: Rankin: subsets of \mathbb{N} avoiding geometric progressions: $\{n, nr, nr^2\}$ and $r \in \mathbb{N} \setminus \{1\}$.



History

In 1961: Rankin: subsets of \mathbb{N} avoiding geometric progressions: $\{n, nr, nr^2\}$ and $r \in \mathbb{N} \setminus \{1\}$.

Simple example: squarefree integers, density $6/\pi^2 \approx 0.60793$.

History

In 1961: Rankin: subsets of \mathbb{N} avoiding geometric progressions: $\{n, nr, nr^2\}$ and $r \in \mathbb{N} \setminus \{1\}$.

Simple example: squarefree integers, density $6/\pi^2 \approx 0.60793$.

Greedy construction asymptotic density approximately 0.71974. McNew improved to about 0.72195.

Improved bounds (Riddell, Brown–Gordon, Beiglböck–Bergelson–Hindman–Strauss, Nathanson–O'Bryant, McNew) on the greatest possible upper density of such a set, between 0.81841 and 0.81922.

Results with Colleagues

Generalized to quadratic number fields.

Generalized to algebraic integers (or ideals).

In an imaginary quadratic field with unique factorization did algebraic integers avoiding 3-term geometric progressions.

Generalized to Function Fields and Quaternions (non-commutative!).

Rankin's Greedy Set

1

Rankin constructed and characterized a "greedy set" that avoids any 3-term geometric progressions.

Rankin's Greedy Set

Rankin constructed and characterized a "greedy set" that avoids any 3-term geometric progressions.

Rankin's Greedy Set

Rankin constructed and characterized a "greedy set" that avoids any 3-term geometric progressions.

Rankin's Greedy Set

Rankin constructed and characterized a "greedy set" that avoids any 3-term geometric progressions.

123 A

Rankin's Greedy Set

Rankin constructed and characterized a "greedy set" that avoids any 3-term geometric progressions.

Rankin's Greedy Set

Rankin constructed and characterized a "greedy set" that avoids any 3-term geometric progressions.

1 2 3 **A** 5 6



Rankin's Greedy Set

Rankin constructed and characterized a "greedy set" that avoids any 3-term geometric progressions.

Rankin's Greedy Set

Rankin constructed and characterized a "greedy set" that avoids any 3-term geometric progressions.

Rankin's Greedy Set

Rankin constructed and characterized a "greedy set" that avoids any 3-term geometric progressions.



Rankin's Greedy Set

Rankin constructed and characterized a "greedy set" that avoids any 3-term geometric progressions.

1 2 3 # 5 6 7 8 Ø 10

Rankin's Greedy Set

Rankin constructed and characterized a "greedy set" that avoids any 3-term geometric progressions.

1 2 3 *A* 5 6 7 8 *9* 10 11



Rankin's Greedy Set

Rankin constructed and characterized a "greedy set" that avoids any 3-term geometric progressions.

1 2 3 *A* 5 6 7 8 *S* 10 11 12

Previous work in commutative settings: How does non-commutivity affect the problem in, say, free groups or the Hurwitz quaternions \mathcal{H} ? How does the lack of unique factorization affect the problem in \mathcal{H} ? Previous work in commutative settings: How does non-commutivity affect the problem in, say, free groups or the Hurwitz quaternions \mathcal{H} ? How does the lack of unique factorization affect the problem in \mathcal{H} ?

We construct large subsets of \mathcal{H} that avoid 3-term geometric progressions.

Previous work in commutative settings: How does non-commutivity affect the problem in, say, free groups or the Hurwitz quaternions \mathcal{H} ? How does the lack of unique factorization affect the problem in \mathcal{H} ?

We construct large subsets of \mathcal{H} that avoid 3-term geometric progressions.

Summer 2025: Polymath Jr: Study Octonions?

The Goal

Goal: Construct and bound Greedy and maximally sized sets of quaternions of the Hurwitz Order free of three-term geometric progressions. For definiteness, we exclude progressions of the form

 Q, QR, QR^2

where $Q, R \in \mathcal{H}$ and Norm[R] $\neq 1$.

Polymath Jr 2025: Maybe exclude three terms from

 $Q, QR, RQ, QR^2, RQR, R^2Q.$



For a lower bound, we construct a set with large upper density. Consider $S_N =$

 $\left(\frac{N}{4}, N\right]$

Then the quaternions with norm in S_N have no 3-term progressions in their norms, and thus no 3-term progressions in the elements themselves.

$$\lim_{N\to\infty}\frac{\{q\in\mathcal{H}:\mathsf{Norm}[q]\in\mathcal{S}_N\}}{\{q\in\mathcal{H}:\mathsf{Norm}[q]\leq N\}}\approx.946589.$$

For a lower bound, we construct a set with large upper density. Consider $S_N =$

 $\left(\frac{N}{9}, \frac{N}{8}\right] \cup \left(\frac{N}{4}, N\right]$

Then the quaternions with norm in S_N have no 3-term progressions in their norms, and thus no 3-term progressions in the elements themselves.

$$\lim_{N\to\infty}\frac{\{q\in\mathcal{H}:\mathsf{Norm}[q]\in\mathcal{S}_N\}}{\{q\in\mathcal{H}:\mathsf{Norm}[q]\leq N\}}\approx.946589.$$

For a lower bound, we construct a set with large upper density. Consider $S_N =$

 $\left(\frac{N}{24}, \frac{N}{12}\right] \cup \left(\frac{N}{9}, \frac{N}{8}\right] \cup \left(\frac{N}{4}, N\right]$

Then the quaternions with norm in S_N have no 3-term progressions in their norms, and thus no 3-term progressions in the elements themselves.

$$\lim_{N\to\infty}\frac{\{q\in\mathcal{H}:\mathsf{Norm}[q]\in\mathcal{S}_N\}}{\{q\in\mathcal{H}:\mathsf{Norm}[q]\leq N\}}\approx.946589.$$

For a lower bound, we construct a set with large upper density. Consider $S_N = \begin{pmatrix} \frac{N}{32}, \frac{N}{27} \end{bmatrix} \cup \begin{pmatrix} \frac{N}{24}, \frac{N}{12} \end{bmatrix} \cup \begin{pmatrix} \frac{N}{9}, \frac{N}{8} \end{bmatrix} \cup \begin{pmatrix} \frac{N}{4}, N \end{bmatrix}$

Then the quaternions with norm in S_N have no 3-term progressions in their norms, and thus no 3-term progressions in the elements themselves.

$$\lim_{N \to \infty} \frac{\{q \in \mathcal{H} : \operatorname{Norm}[q] \in S_N\}}{\{q \in \mathcal{H} : \operatorname{Norm}[q] \le N\}} \approx .946589.$$

For a lower bound, we construct a set with large upper density. Consider $S_N = \begin{pmatrix} \frac{N}{40}, \frac{N}{36} \end{bmatrix} \cup \begin{pmatrix} \frac{N}{32}, \frac{N}{27} \end{bmatrix} \cup \begin{pmatrix} \frac{N}{24}, \frac{N}{12} \end{bmatrix} \cup \begin{pmatrix} \frac{N}{9}, \frac{N}{8} \end{bmatrix} \cup \begin{pmatrix} \frac{N}{4}, N \end{bmatrix}$

Then the quaternions with norm in S_N have no 3-term progressions in their norms, and thus no 3-term progressions in the elements themselves.

$$\lim_{N \to \infty} \frac{\{q \in \mathcal{H} : \operatorname{Norm}[q] \in S_N\}}{\{q \in \mathcal{H} : \operatorname{Norm}[q] \le N\}} \approx .946589.$$

For a lower bound, we construct a set with large upper density. Consider $S_N = \left(\frac{N}{48}, \frac{N}{45}\right] \cup \left(\frac{N}{40}, \frac{N}{36}\right] \cup \left(\frac{N}{32}, \frac{N}{27}\right] \cup \left(\frac{N}{24}, \frac{N}{12}\right] \cup \left(\frac{N}{9}, \frac{N}{8}\right] \cup \left(\frac{N}{4}, N\right]$

Then the quaternions with norm in S_N have no 3-term progressions in their norms, and thus no 3-term progressions in the elements themselves.

$$\lim_{N \to \infty} \frac{\{q \in \mathcal{H} : \operatorname{Norm}[q] \in S_N\}}{\{q \in \mathcal{H} : \operatorname{Norm}[q] \le N\}} \approx .946589.$$

Sums of Powers (with Enrique Treviño)

$$S_k(n) = 1^k + 2^k + \cdots + n^k.$$

New Proof of Theorem: Let *k* be a positive integer. There exists a polynomial $g_k \in \mathbb{Q}[x, y]$ such that $g_k(0, 0) = 0$ and

$$\sum_{m=1}^{n} m^{k} = g_{k}(S_{1}(n), S_{2}(n)).$$

Examples:

$$\begin{array}{lll} S_5(n) &=& \frac{3}{2}S_2^2(n)-\frac{1}{2}S_1^2(n).\\ S_6(n) &=& \frac{12}{7}S_1^2(n)S_2(n)-\frac{6}{7}S_1(n)S_2(n)+\frac{1}{7}S_2(n). \end{array}$$

Problems for Polymath Jr 2025

- How many representations if increase the number of functions; use S_k for k ≤ K, how many polynomials of these give S_m(n) for m > K?
- If can only use S_k for $k \in \mathcal{K}$ which powers doable?
- From Suaib Lateef: Claim (proved for small *n*):

if
$$a_1 + \dots + a_{n-1} = 2 \cdot n - 2$$

 $a_1^2 + \dots + a_{n-1}^2 = 3 \cdot n - 2$
 \vdots
 $a_1^{n-1} + \dots + a_{n-1}^{n-1} = n \cdot n - 2$
then $a_1^n + \dots + a_{n-1}^n = (n+1) \cdot n - 2$.

Thanks 00

L'Hopital (with Eduardo Duenez and Asimina Hamakiotes)

Use

$$1 + x + x^2 + \cdots + x^n = \frac{x^{n+1} - 1}{x - 1},$$

apply x d/dx to each side k times, take limit as $x \rightarrow 1$, use L'Hopital, get formula for sum of k^{th} powers!

L'Hopital (with Eduardo Duenez and Asimina Hamakiotes)

Use

$$1 + x + x^2 + \cdots + x^n = \frac{x^{n+1} - 1}{x - 1},$$

apply x d/dx to each side k times, take limit as $x \rightarrow 1$, use L'Hopital, get formula for sum of k^{th} powers!

Easy to see must be a polynomial of degree k + 1, but algebra nightmare:

After taking the limit as x approaches 1 of the right hand side and applying L'Hopital four times, we get

$$\lim_{\epsilon \to 1} \frac{n^2 x^{n+4} + (-3n^2 - 2n + 1)x^{n+3} + (3n^2 + 4n)x^{n+2} - (n+1)^2 x^{n+1} - x^3 + x}{(x-1)^4} \; = \; \frac{2n^3 + 3n^2 + n}{6},$$

which is the desired $p_2(n) = n(n+1)(2n+1)/6$. Note we know we must apply L'Hopital's rule exactly four times, as the limit exists and fewer times results in a zero denominator.

Polymath Jr 2025: Good path thru the algebra? Do d/dx instead and combinatorics?

More Sums Than Differences

Definitions

A finite set of integers, |A| its size. Form

- Sumset: $A + A = \{a_i + a_j : a_i, a_j \in A\},\$
- Difference set: $A A = \{a_i a_j : a_i, a_j \in A\}.$

Definitions

A finite set of integers, |A| its size. Form

- Sumset: $A + A = \{a_i + a_j : a_i, a_j \in A\},\$
- Difference set: $A A = \{a_i a_j : a_i, a_j \in A\}$.

Definition

Difference dominated: |A - A| > |A + A|Balanced: |A - A| = |A + A|Sum dominated (or MSTD): |A + A| > |A - A|.

What could cause a set to be sum-dominated? Difference-dominated?

What could cause a set to be sum-dominated? Difference-dominated?

•
$$x + x = 2x$$
, but $x - x = 0$.

What could cause a set to be sum-dominated? Difference-dominated?

•
$$x + x = 2x$$
, but $x - x = 0$.

•
$$x + y = y + x$$
, but $x - y \neq y - x$.

What could cause a set to be sum-dominated? Difference-dominated?

•
$$x + x = 2x$$
, but $x - x = 0$.

•
$$x + y = y + x$$
, but $x - y \neq y - x$.

Nathanson, Problems in Additive Number Theory. "With the right way of counting the vast majority of sets satisfy |A - A| > |A + A|."

Theorem (Martin-O'Bryant): If each set $A \subseteq [0, n-1]$ is equally likely, then a positive percentage of sets are sum-dominant in the limit. More precisely:

$$\lim_{n\to\infty}\frac{\#\{A\subseteq [0,n-1];\ A \text{ is sum-dominant}\}}{2^n}\approx 0.00045.$$

Generalizing Martin-O'Bryant

- What if we pick random subsets in a different way?
- Construct A ⊆ {1,..., n} ⊂ Z randomly by picking each element independently with probability p(n).
 - Uniform case corresponds to p(n) = 1/2 constant.
 - Let *p*(*n*) decay to 0 as *n* → ∞ (smaller sets are more likely to be picked).

Generalizing Martin-O'Bryant

- What if we pick random subsets in a different way?
- Construct A ⊆ {1,..., n} ⊂ Z randomly by picking each element independently with probability p(n).
 - Uniform case corresponds to p(n) = 1/2 constant.
 - Let *p*(*n*) decay to 0 as *n* → ∞ (smaller sets are more likely to be picked).

Theorem (Hegarty and Miller, 2009)

Let $A \subseteq \{1, ..., n\} \subset \mathbb{Z}$ be chosen randomly in this way where p(n) = o(1). Then

Prob(A is difference-dominated) \rightarrow 1 as $n \rightarrow \infty$.

Say $A \subseteq [0, n-1]$, $x \in A + A$ if we can find $a_1, a_2 \in A$ such that $a_1 + a_2 = x$.

Say $A \subseteq [0, n-1]$, $x \in A + A$ if we can find $a_1, a_2 \in A$ such that $a_1 + a_2 = x$.

If x is near n there are many possibilities for a_1, a_2 .

Say $A \subseteq [0, n-1]$, $x \in A + A$ if we can find $a_1, a_2 \in A$ such that $a_1 + a_2 = x$.

If x is near n there are many possibilities for a_1, a_2 .

With high probability, the middle is full.

Say $A \subseteq [0, n-1]$, $x \in A + A$ if we can find $a_1, a_2 \in A$ such that $a_1 + a_2 = x$.

If x is near n there are many possibilities for a_1, a_2 .

With high probability, the middle is full.

The trick is to control the fringes.

Notation

• As adding sets and not multiplying, set

$$kA = \underbrace{A + \cdots + A}_{\text{k times}}.$$

• $[a, b] = \{a, a+1, \ldots, b\}.$



Questions

• Can we find a set A such that |kA + kA| > |kA - kA|?

- Can we find a set A such that |A + A| > |A A| and |2A + 2A| > |2A 2A|?
- Can we find a set A such that |kA + kA| > |kA kA| for all k?

Questions

- Can we find a set A such that |kA + kA| > |kA kA|? Yes.
- Can we find a set A such that |A + A| > |A A| and |2A + 2A| > |2A 2A|? Yes.
- Can we find a set A such that |kA + kA| > |kA kA| for all k? No. (No such set exists.)

Question: Can we find A with |kA + kA| > |kA - kA|?

• One set is enough to show a positive percentage.

- One set is enough to show a positive percentage.
- How do we find one set?

- One set is enough to show a positive percentage.
- How do we find one set?
- Computer simulations? We couldn't find a set for k = 2; the probability of finding some of these sets is less than 10^{-16} .

- One set is enough to show a positive percentage.
- How do we find one set?
- Computer simulations? We couldn't find a set for k = 2; the probability of finding some of these sets is less than 10^{-16} .
- If A is symmetric (A = c A for some c) then

$$|\mathbf{A} + \mathbf{A}| = |\mathbf{A} + (\mathbf{c} - \mathbf{A})| = |\mathbf{A} - \mathbf{A}|.$$

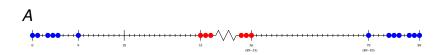
Example: |2A + 2A| > |2A - 2A|

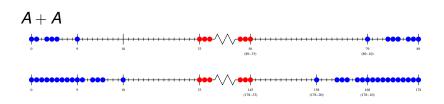
$A = \{0, 1, 3, 4, 5, 9\} \cup [33, 56] \cup \{79, 83, 84, 85, 87, 88, 89\}$

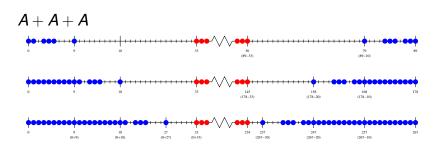


$\begin{array}{l} \textit{A} + \textit{A} = & [0,9] \cup \{10,12,13,14,18\} \cup [33,145] \\ & \cup \{158,162,163,164,166,167\} \cup [168,178] \end{array}$

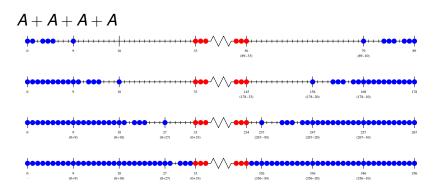
| 000000000 | 01000111 | *********** | | | | | |
|-----------|----------|-------------|---|------------|--------|---------|-----|
| 6 9 | 9 i | 8 3 | 3 | 145 1: | 8 | 168 | 178 |
| | | | 0 | 8-33) (178 | -200 0 | 178-10) | |

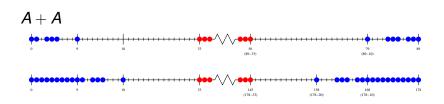


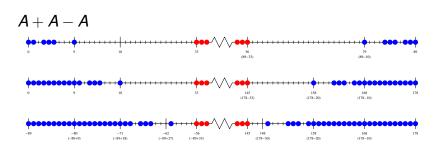




|2A+2A| > |2A-2A|

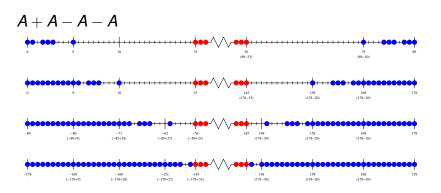






MSTDs

|2A+2A| > |2A-2A|



Question: Does a set A exist such that |A + A| > |A - A|and |A + A + A + A| > |A + A - A - A|?

Question: Does a set A exist such that |A + A| > |A - A|and |A + A + A + A| > |A + A - A - A|?

Yes!

 $\begin{aligned} \textbf{A} &= \{0, 1, 3, 4, 7, 26, 27, 29, 30, 33, 37, 38, 40, 41, 42, 43, \\ &\quad 46, 49, 50, 52, 53, 54, 72, 75, 76, 78, 79, 80\} \end{aligned}$

In fact, we can find a *k*-generational set for all *k*.

Idea of proof: We can find A_j such that $|jA_j + jA_j| > |jA_j - jA_j|$ for a specific $1 \le j \le k$.



Idea of proof: We can find A_j such that $|jA_j + jA_j| > |jA_j - jA_j|$ for a specific $1 \le j \le k$.

Combine the A_i using the method of base expansion.



Avoiding Progressions and Sums

MSTDs

Thanks 00

Limiting behavior of kA

Avoiding Progressions and Sums

MSTDs

Thanks

Limiting behavior of kA

Question: Can we find A with |kA + kA| > |kA - kA| for all k?

No. No such set exists.

Limiting behavior of kA

Question: Can we find A with |kA + kA| > |kA - kA| for all k?

No. No such set exists.

It turns out that all sets have a sort of limiting behavior.

MSTDs

Thanks 00

Stabilizing Fringes

Example: $A = \{0, 3, 5, 6, 8, 9, 10, 11, 12, 15, 16, 20\}$



Figure: A

MSTDs

Thanks 00

Stabilizing Fringes

Example: $A = \{0, 3, 5, 6, 8, 9, 10, 11, 12, 15, 16, 20\}$



Figure: A



Figure: A + A



Avoiding Progressions and Sums

MSTDs

Thanks 00

$$|kA - kA|$$
 vs. $|kA + kA|$

Nathanson: For any set *A*, *kA* becomes stabilized before k reaches $\max(A)^2 \cdot |A|$.

We improve this bound to max(A).

|kA - kA| vs. |kA + kA|

Theorem

For any set A, kA becomes difference-dominated or balanced before k reaches $2 \cdot \max(A)$.

Proof Idea:

- The middle quickly becomes full, and the remaining fringes are finite.
- kA ⊆ kA kA. Any sum can eventually be written as a difference.

Because the form stabilizes, this means $kA - kA \supseteq kA + kA$ when *k* large.

MSTDs

Thanks 00

Future Work: SMALL / Polymath Jr 2025

Extend to *d*-dimensional MSTD sets.

More generally, any order and number of (nontrivial) comparisons.

Thanks

Thanks

Thanks to:

- University of Michigan, Williams College,
- NSF Grants DMS0850577, DMS1347804, DMS1659037, DMS2113535, DMS2113535, DMS2218374, DMS2241623, DMS2313292, DMS2341670, DMS0600848, DMS0970067, DMS1265673, DMS1561945,
- Conference Organizers, and of course
- Carl and Mel.