The Goldbach Property in Semidomains

(joint work with Pa Crowdmath, Leo Hong, and Nick Zhang)

Victor Gonzalez
(Research Mentors: Dr. Gotti and Dr. Polo)

vmgzlez@mit.edu

MIT

Summer Workshop for the Intrepid Mathematician
(SWIM 2025)

August 5, 2025

Table of Contents

General notation we will use throughout this presentation:

- $\mathbb{N} := \{1, 2, \ldots\}$,
- $\mathbb{N}_0 := \{0\} \cup \mathbb{N} = \{0, 1, 2, \ldots\}$, and
- $\mathbb{P}$ denotes the set of prime numbers.
- For a subset S of the real line $\mathbb{R}$ and $r \in \mathbb{R}$, we set $S_{\geq r} := \{s \in S : s \geq r\}$ and $S_{>r} := \{s \in S : s > r\}$.

Monoids

Definition: A monoid $M = (M, *)$ is a set M equipped with a binary operation $(*)$ on M satisfying the following conditions.

- $*$ is associative: $b * (c * d) = (b * c) * d$ for all $b, c, d \in M$.
- there exists an identity element e such that $b * e = e * b = b$ for all $b \in M$.

Remark: From this point on, we will denote a monoid $(M, *)$ simply by M when the operation is either a generic operation $*$ or it is clear from the context.

Examples of Additive Monoids

Remark: Monoids can be written additively or multiplicatively.

Some additive monoids are:

Examples

- $(\mathbb{N}_0, +)$ is a monoid with identity element 0, because the standard addition is associative.
- Similarly, $(\mathbb{Q}_{\geq 0}, +)$ is an additive monoid with identity element 0.
- $\mathbb{N}_0 \setminus \{1\}$ is a monoid under the standard addition operation.
- $\mathbb{N}_0 \setminus \{2\}$ is a NOT a monoid under the addition operation because $1 \in \mathbb{N}_0 \setminus \{2\}$, but
$$1 + 1 = 2 \notin \mathbb{N}_0 \setminus \{2\}.$$

Examples of Multiplicative Monoids

Some multiplicative monoids are:

Examples

- $(\mathbb{N}, \cdot)$ is a monoid with identity element 1 because $(\cdot)$ is associative.
- Similarly, $(\mathbb{Q}_{>0}, \cdot)$ is a multiplicative monoid with identity element 1.
- For any real number $r \in \mathbb{R}$, the set $S_r := \{r^n : n \in \mathbb{N}_0\}$ is a monoid under the standard operation of multiplication.

Submonoids

Definition: A submonoid of M is subset of M that contains the identity element e and is a monoid with respect to the operation of M.

Additive Submonoids:

Examples

- A numerical monoid S is a submonoid of $(\mathbb{N}_0, +)$ such that $\mathbb{N}_0 \setminus S$ is finite.
  - $\mathbb{N}_0 \setminus \{1\}$.
  - $\{0\} \cup \mathbb{N}_{\geq n}$ (for every $n \in \mathbb{N}$).
- A Puiseux monoid is a submonoid of $(\mathbb{Q}_{\geq 0}, +)$.
  - $\{0\} \cup \mathbb{Q}_{\geq 1}$.
  - For a number $d \in \mathbb{N}_{>1}$, we define $S_{1/d} := \left\{ \frac{m}{d^n} : m, n \in \mathbb{N}_0 \right\}$.

Examples of Submonoids

Multiplicative Submonoids:

Examples

- The set $\{2^n : n \in \mathbb{N}_0\}$ under the standard multiplication is a submonoid of $(\mathbb{N}, \cdot)$.
- The set $\{1\} \cup \mathbb{Q}_{\geq 3}$ under the standard multiplication is a submonoid of $(\mathbb{Q}_{>0}, \cdot)$.
- The set $\mathbb{Q}_{\geq 1/2}$ under multiplication is not a submonoid of $(\mathbb{Q}_{>0}, \cdot)$. Note that
$$\frac{1}{2} \cdot \frac{1}{2} = \frac{1}{4} \notin \mathbb{Q}_{\geq 1/2}.$$

Remark: From now on, we will use multiplicative notation when stating general properties of monoids.

Monoids Generated by a Set

Definition: For $S \subseteq M$, the arbitrary intersection of submonoids of M containing S is also a submonoid of M and is denoted by $\langle S \rangle$. The monoid $\langle S \rangle$ can also be defined as the smallest submonoid of M containing S. We say that S is a generating set of M if $M = \langle S \rangle$.

Examples

- The numerical monoid $N := \mathbb{N}_0 \setminus \{1\}$ can be written as $N = \langle 2, 3 \rangle$. Indeed, every number $n \in N$ can be expressed as $n = 2b + 3c$ for some $b, c \in \mathbb{N}_0$.
- The Puiseux monoid $S_{1/d} := \{\frac{m}{d^n} : m, n \in \mathbb{N}_0\}$ can be defined as $S_{1/d} = \langle \frac{1}{d^n} : n \in \mathbb{N}_0 \rangle$.
- Let $q \in \mathbb{Q}_{>0}$. The set $S_q := \langle q^n : n \in \mathbb{N}_0 \rangle$ under addition is a Puiseux monoid.

Properties of Monoids

Some monoids have specific properties.

- We say that a monoid M is commutative if for any $a, b \in M$, $a \cdot b = b \cdot a$.
- We say that a monoid M is cancellative if for any $a, b, c \in M$, the fact that $a \cdot b = a \cdot c$ implies that $b = c$.

Remark: From this point on, we will tacitly assume that every monoid we deal with here is commutative and cancellative.

Examples

- Numerical monoids and Puiseux monoids are commutative and cancellative.
- The monoid $(\mathbb{N}_0, \cdot)$ is not cancellative as $2 \cdot 0 = 3 \cdot 0$, but $2 \neq 3$.

Invertible Elements and Groups

Definition: Let M be a monoid with identity e.

- An element $u \in M$ is called a unit (or an invertible) if $u \cdot v = e$ for some $v \in M$.
- The set of all units of M is denoted by $M^\times$.

Definition:

- A group is a monoid in which every element is a unit.
- The set of units $M^\times$ of a monoid M is a group called the group of units of M.
- We say that M is reduced if the group of units $M^\times$ is the trivial group.

Examples

- $(\mathbb{Z}, +)$ and $(\mathbb{Q}, +)$ are groups.
- $(\mathbb{Z}, \cdot)$ is not a group.
- The monoid $M = (\mathbb{N}, \cdot)$ is reduced as $M^\times = \{1\}$.

Atomicity

Definition: Let M be a monoid. An element $a \in M \backslash M^\times$ is an atom if when $a = b \cdot c$, where $b, c \in M$, then either $b \in M^\times$ or $c \in M^\times$. The set of atoms of M is denoted by $\mathcal{A}(M)$.

Definition: The monoid M is called atomic if every non-invertible element factors into atoms (allowing repetitions).

Examples

- Groups are trivially atomic monoids.
- The monoid $M := (\mathbb{N}_0, +)$ is atomic with $\mathcal{A}(M) = \{1\}$.
- $(\mathbb{N}, \cdot)$ is atomic (Fundamental Theorem of Arithmetic).
- S_q is atomic for every $q \in \mathbb{Q}_{>0} \setminus \mathbb{N}$ such that $q^{-1} \notin \mathbb{N}_{\geq 2}$. Moreover $\mathcal{A}(S_q) = \{q^n : n \in \mathbb{N}\}$.
- $S_{1/2}$ is not atomic.

Semidomains

Definition: A semidomain $S = (S, +, \cdot)$ is a set equipped with 2 binary operations $(+)$ and $(\cdot)$ that has the following properties.

- $(S, +)$ is a monoid, with identity denoted by 0.
- $(S \setminus \{0\}, \cdot)$ is a monoid with identity denoted by 1 $(1 \neq 0)$. This is the multiplicative monoid of S and is denoted by S^*.
- For any $a, b, c \in S$, we see that $a \cdot (b + c) = a \cdot b + a \cdot c$.

Examples of Semidomains

Examples

- $(\mathbb{N}_0, +, \cdot)$ is a semidomain.
  - $(\mathbb{N}_0, +)$ is a monoid with identity 0.
  - $(\mathbb{N}, \cdot)$ is a monoid with identity 1.
  - the distributive property holds.
- Similarly, $(S_q, +, \cdot)$ is a semidomain.
- Given a semidomain S, we let $S[x]$ denote the set of polynomials with coefficients in S. It turns out that $S[x]$ is a semidomain under the standard addition and multiplication of polynomials. This is called the polynomial extension of S.

  Remark: Observe that for every $r \in \mathbb{R}$, we can define S_r as

  $$S_r := \{f(r) : f(x) \in \mathbb{N}_0[x]\}.$$

  For convenience, we will write either S_r or $\mathbb{N}_0[r]$ interchangeably.

Cyclic Semidomain

Remark

- For $q \in \mathbb{Q}_{>0}$, we call cyclic rational semidomain to the Puiseux monoid S_q generated by the nonnegative powers of q, i.e.,

$$S_q = \langle q^n : n \in \mathbb{N}_0 \rangle.$$

- Similarly, for $r \in \mathbb{R}_{>0} \setminus \mathbb{Q}$, we call cyclic algebraic semidomain to the Puiseux monoid S_r generated by the nonnegative powers of r, i.e.,

$$S_r = \langle r^n : n \in \mathbb{N}_0 \rangle.$$

Multiplicative Subsets of a Semidomain

Definition: A subset A of a semidomain S is a multiplicative subset of S if A is a submonoid of S^*.

Examples

- If S is a semidomain, then $S^\times$ is a multiplicative subset of S.
- If S is a semidomain and $s \in S$, then the set $\{s^n : n \in \mathbb{N}_0\}$ is a multiplicative subset of S.

Equivalence classes (quick recap)

Equivalence relation

On a set X, a relation $\sim$ is an equivalence relation if it is:

- **Reflexive:** $x \sim x$ for all $x \in X$,
- **Symmetric:** $x \sim y \Rightarrow y \sim x$,
- **Transitive:** $x \sim y$ and $y \sim z \Rightarrow x \sim z$.

Equivalence Classes

For $x \in X$, the equivalence class of x is

$$[x] = \{\, y \in X : y \sim x \,\}.$$

Classes partition X: every element lies in exactly one class. The set of all classes is denoted $X/\!\sim$.

Localizations

Definition: Let S be a semidomain, and let A be a multiplicative subset of S. Now set $R := (S \times A)/\sim$, where $\sim$ is an equivalence relation on $S \times A$ defined by $(s, d) \sim (s', d')$ if and only if $sd' = ds'$. We let $\frac{s}{d}$ denote the equivalence class of (s, d). Define the following operations in R:

$$\frac{s}{d} \cdot \frac{s'}{d'} = \frac{ss'}{dd'} \quad \text{and} \quad \frac{s}{d} + \frac{s'}{d'} = \frac{sd' + ds'}{dd'}.$$

Proposition

The triple $(R, +, \cdot)$ is a semidomain called the localization of S at A.

We denote the localization of S at A by $A^{-1}S$.

Localization – concrete examples

Examples

- **Fractions of natural numbers.**

$$S = \mathbb{N}_0, \qquad A = \mathbb{N} = \{1, 2, 3, \dots\}.$$

$$\text{Note that } A^{-1}S = \left\{ \frac{m}{n} \,:\, m, n \in \mathbb{N}_0,\ n \neq 0 \right\} = \mathbb{Q}_{\geq 0}.$$

So we recover the non-negative rationals.

- **The semidomain $\mathbb{N}_0[\frac{1}{p}]$.**

$$S = \mathbb{N}_0, \qquad A := \{p^k : k \in \mathbb{N}_0\}, \text{ for a prime } p$$

Note that the elements of $A^{-1}\mathbb{N}_0$ are fractions $\frac{n}{d}$ with n being a nonnegative integer and d being a nonnegative power of p. As we observed before, this semidomain is $\mathbb{N}_0\left[\frac{1}{p}\right]$.

Localization – concrete examples

Examples

- **Laurent Cyclic Rational Semidomain.**

$$S = \mathbb{N}_0[q], \qquad A = \{q^n : n \in \mathbb{N}_0\}.$$

We note that $A^{-1}S = \mathbb{N}_0[q, q^{-1}] = \Big\{ \sum_{k=-m}^{\ell} a_k q^k \ : \ a_k \in \mathbb{N}_0 \Big\}.$

Remark: If we replace q by an indeterminate x over $\mathbb{N}_0$, the localization $\mathbb{N}_0[x, x^{-1}]$ is called the Laurent polynomial extension of $\mathbb{N}_0$.

History

- The Goldbach conjecture was introduced by Goldbach in a 1742 letter to Euler. The conjecture asserts that every even integer greater than 2 can be expressed as the sum of two prime numbers.
- The conjecture remains one of the most ancient and renowned unsolved problems in mathematics, but several authors have explored analogues for various classes of polynomial rings.
- In 1965, Hayes demonstrated that polynomials $f \in \mathbb{Z}[x]$ with $\deg(f) > 1$ can be represented as the sum of two irreducibles.
- Hayes' work was later extended by Saidak, Kozek, and Pollack.

History

- More recently, Liao and Polo initiated the study of analogues of the Goldbach conjecture for Laurent polynomial semidomains. Specifically, they showed that every $f \in \mathbb{N}_0[x^{\pm 1}]$ that is not a monomial can be written as the sum of at most two irreducibles provided that $f(1) > 3$.
- Kaplan and Polo (2024) extended this result to a more general class of additively atomic semidomain satisfying $\mathcal{A}_+(S) = S^\times$.
- E. Li, A. Mopuri, and C. Zhang extended several of the results of Kaplan and Polo to group semidomains.

First Question

The first problem of our research project was to find all positive real numbers r such that the semidomain $\mathbb{N}_0[r]$ satisfied an analogue of the Goldbach conjecture.

Question 1

(a) Find all $q \in \mathbb{Q}^+$ such that $\mathbb{N}_0[q]$ satisfies an analogue of the Goldbach conjecture.
(b) Find all $r \in \mathbb{R}^+$ such that $\mathbb{N}_0[r]$ satisfies an analogue of the Goldbach conjecture.

First Results

- If r is transcendental, then $\mathbb{N}_0[r] \equiv \mathbb{N}_0[x]$ (a polynomial extension), so no analogue of Goldbach conjecture holds.
- If $r \in \mathbb{N}$, then $\mathbb{N}_0[r] \equiv \mathbb{N}_0$, so the only known analogue is the classical weak Goldbach conjecture.

Theorem (CrowdMath, 2024)

Let $r \in \mathbb{Q}_{>0}$. Then:

1. If $r = \frac{1}{n}$ for some $n \in \mathbb{N}$, every element of $\mathbb{N}_0[r]$ can be expressed as a sum of at most $4\ell + 4$ irreducibles, for some $\ell \in \mathbb{N}_0$.
2. If $r = \frac{p}{q}$ with $p, q \in \mathbb{N}$, $\gcd(p, q) = 1$, and $1 < p < q$, then $\mathbb{N}_0[r]$ satisfies no Goldbach-type analogue.
3. If $r = \frac{p}{q}$ with $p, q \in \mathbb{N}$, $\gcd(p, q) = 1$, and $p > q$, then $\mathbb{N}_0[r]$ likewise satisfies no Goldbach-type analogue.

Second Question

One of the key goals of our research was to study the connection of Goldbach conjecture analogues with localizations.

Question 2

Assume that every non-constant Laurent polynomial in $A^{-1}S[x, x^{-1}]$ can be written as the sum of two irreducibles. Does the same property hold in the semidomain $S[x, x^{-1}]$?

Second Result

Theorem (Crowdmath, 2024)

Let $S_{3/4}$ be the rational cyclic semidomain generated by $\frac{3}{4}$, and let A be the set of atoms of $S_{3/4}$. Then the following statements hold.

1. $A^{-1}S = \langle \left(\frac{3}{4}\right)^n : n \in \mathbb{Z} \rangle$.
2. $(A^{-1}S)[x, x^{-1}]$ has the Goldbach-type property.
3. $S[x, x^{-1}]$ does not have the Goldbach-type property.

References

H. Fox, A. Goel, and S. Liao, *Arithmetic of semisubtractive semidomains*, arXiv:https://arxiv.org/pdf/2311.07060.

F. Gotti and H. Polo, *On the arithmetic of polynomial semidomains*, Forum Math. **35** (2023) 1179–1197.

D. R. Hayes, *A Goldbach theorem for polynomials with integral coefficients*, Amer. Math. Monthly **72** (1965) 45–46.

N. Kaplan and H. Polo, *A Goldbach theorem for Laurent series semidomains*. Submitted. Preprint on arXiv: `https://arxiv.org/abs/2312.14888`

S. Liao and H. Polo, *A Goldbach theorem for Laurent polynomials with positive integer coefficients*, Amer. Math. Monthly **131** (2024) 704–711.

References

A. Lin, H. Rabinovitz, and Q. Zhang, *The Furstenberg property in Puiseux monoids*. Semigroup Forum (to appear). Preprint on arXiv: https://arxiv.org/abs/2309.12372

E. Li, A. Mopuri, and C. Zhang, *Goldbach theorems for group semidomains*. Submitted. Preprint on arXiv: https://arxiv.org/abs/2412.00590

F. Gotti and H. Rabinovitz, *On the ascent of atomicity to monoid algebras*, J. Algebra **663** (2025) 857–881.

A. Grams, *Atomic rings and the ascending chain condition for principal ideals*, Proc. Cambridge Philos. Soc., **75** (1974) 321–329.

N. Lebowitz-Lockard, *On domains with properties weaker than atomicity*, Comm. Algebra **47** (2019) 1862–1868.

References

F. W. Levi, *Arithmetische Gesetze im Gebiete diskreter Gruppen*, Rend. Circ. Mat. Palermo **35** (1913) 225–236.

J. Okninński, *Commutative monoid rings with krull dimension*. In: Semigroups Theory and Applications (Eds. H. Jürgensen, G. Lallement, and H. J. Weinert), pp. 251–259. Lecture Notes in Mathematics, vol. 1320. Springer, Berlin, Heidelberg, 1988.

M. Roitman, *Polynomial extensions of atomic domains*, J. Pure Appl. Algebra **87** (1993) 187 –199.

Acknowledgments

On the name of all my CrowdMath collaborators, I would like to thank

- our research mentors, **Dr. Felix Gotti** and **Dr. Harold Polo**, for the time and effort poured into our mathematical research journey during the fall term of CrowdMath 2024, and also
- the organizers of **CrowdMath** for making mathematical research accessible and free for all high schoolers and undergrads around the world.

In addition, I am grateful to

- the organizers of **SWIM 2025** for providing this exotic venue where young math enthusiasts have the opportunity to talk about their mathematical research, and
- **all of you** for your attention!