Maximal Common Divisors in Puiseux Monoids

Evin Liang, Alexander Wang, and Lerchen Zhong

MIT PRIMES-USA

(Mentored by Dr. Felix Gotti)

PRIMES October Conference
October 12, 2024

Outline

Some Notation

Some Notation Adopted Here

- $\mathbb{N} := \{1, 2, 3, \ldots\}$,
- $\mathbb{N}_0 := \{0\} \cup \mathbb{N} = \{0, 1, 2, \ldots\}$, and
- $\mathbb{P}$ denotes the set of primes.

Commutative Monoids

Definition. A commutative monoid is a pair $(M, *)$, where M is a set and $*$ is a binary operation on M satisfying the following conditions.

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

Definition. Let M be a monoid.

- $\mathcal{U}(M)$ denotes the set of invertible elements of M.

Definition. A subset N of a monoid M is called a submonoid of M if N contains the identity element and is closed under the operation of M.

Remark. For $S \subseteq M$, the arbitrary intersection of (additive) submonoids of M containing S is also a submonoid of M and is denoted by $\langle S \rangle$.

Examples of Monoids

Today's Conventions

- We call a commutative monoid $(M, *)$ simply a monoid if it is cancellative: $b * d = c * d$ implies $b = c$ for all $b, c, d \in M$.
- M is torsion-free if for all $b, c \in M$ and $n \in \mathbb{N}$, the equality $nb = nc$ implies that $b = c$. All monoids are also assumed to be torsion-free.
- For a monoid $(M, *)$, we write M instead of $(M, *)$.

Examples of Monoids

- Additive submonoids of $\mathbb{N}_0$ are called numerical monoids.
  - $\mathbb{N}_0 \setminus \{1\}$ and $\{0\} \cup \mathbb{N}_{\geq n}$ (for every $n \in \mathbb{N}$).
- Additive submonoids of $\mathbb{Q}_{\geq 0}$ are called Puiseux monoids.
  - $\{0\} \cup \mathbb{Q}_{\geq 1}$ and $\left\langle \frac{1}{p} : p \in \mathbb{P} \right\rangle = \left\langle \left\{ \frac{1}{p} : p \in \mathbb{P} \right\} \right\rangle$.

Rank

Definition. Let M be a monoid.
The rank of a monoid M is the dimension of the smallest vector space over $\mathbb{Q}$ containing a copy of M (if it exists).

Examples

- The rank-1 torsion-free monoids are precisely the submonoids of $(\mathbb{Q}, +)$.
- The rank-1 torsion-free monoids that are not groups are precisely the submonoids of $(\mathbb{Q}_{\geq 0}, +)$, i.e., the (nonzero) Puiseux monoids.
- The additive monoid consisting of all lattice points in the first quadrant is a rank-2 monoid.

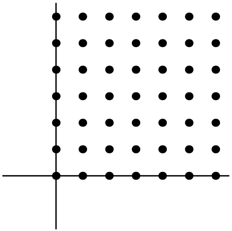
Rank

Definition. Let M be a monoid.

The rank of a monoid M is the dimension of the smallest vector space over $\mathbb{Q}$ containing a copy of M (if it exists).

Examples

- The rank-1 torsion-free monoids are precisely the submonoids of $(\mathbb{Q}, +)$.
- The rank-1 torsion-free monoids that are not groups are precisely the submonoids of $(\mathbb{Q}_{\geq 0}, +)$, i.e., the (nonzero) Puiseux monoids.
- The additive monoid consisting of all lattice points in the first quadrant is a rank-2 monoid.



Atomicity and the ACCP

Definitions. Let M be a monoid.

- A principal ideal of M is a set of the form $a + M$ where $a \in M$.
- We say that M satisfies the ascending chain condition on principal ideals (ACCP) if every ascending chain of principal ideals $a_1 + M \subseteq a_2 + M \subseteq \dots$ is eventually constant.
- If a is an element of M, then a is an atom if whenever $a = b + c$ for elements $b, c \in M$, then either b or c is invertible.
- The set of atoms is denoted $\mathcal{A}(M)$.
- M is atomic if every element can be written as a sum of atoms.

Remark. Every monoid satisfying the ACCP is atomic.

A Motivating Example

Example. For each $n \in \mathbb{N}$, let p_n be the n-th odd prime, and define the Puiseux monoid

$$M := \left\langle \frac{1}{2^{n-1} p_n} : n \in \mathbb{N} \right\rangle.$$

M is Grams' monoid.

Exercise. M is atomic with set of atoms

$$\mathcal{A}(M) = \left\{ \frac{1}{2^{n-1} p_n} : n \in \mathbb{N} \right\}.$$

Exercise. M does not satisfy the ACCP because $\left(\frac{1}{2^n} + M\right)_{n \geq 1}$ forms an ascending chain of principal ideals of M that does not stabilize.

Maximal Common Divisors

Definition.

- Let M be a monoid and let S be a nonempty subset of M.
- We say that $d \in M$ is a common divisor of S if d divides every element of S.
- We say that $d \in M$ is a maximal common divisor of S if d is a common divisor of S and every common divisor of $S - d$ is a unit.

Maximal Common Divisors

We can define several properties of monoids related to maximal common divisors:

- A monoid M is k-MCD ($k \in \mathbb{N}$) if every subset of size k has a maximal common divisor.
- A monoid M is MCD if it is k-MCD for every positive integer k.
- A monoid M is strongly MCD if every nonempty subset (not necessarily finite) of M has an MCD.

Remark. It follows from the definitions that every strongly MCD monoid is an MCD monoid, which in turn is also k-MCD for all $k \in \mathbb{N}$.

Maximal Common Divisors and the ACCP

Fact. It is known that every ACCP monoid is MCD.

Does ACCP imply strongly MCD? Answer: **yes**.

Proposition (L-W-Z 2024)

If a (commutative and cancellative) monoid M satisfies the ACCP, then it is strongly MCD.

Does the converse hold? Answer: **no**.

Example. Consider the monoid $M = \mathbb{R}_{\geq 0}$ of the nonnegative real numbers under addition. Then $\left(\frac{1}{n} + M\right)_{n \geq 1}$ is an ascending chain of principal ideals that does not stabilize. However, every nonempty subset of M has a maximal common divisor, namely its infimum.

This example shows that strongly MCD monoid does not even have to be atomic.

However, the converse does hold for some monoids.

Theorem (L-W-Z 2024)

If a (commutative and cancellative) monoid is countable and strongly MCD, then it satisfies the ACCP.

Integral Domains and Fields

Definition. A (commutative) ring is a triple $(R, +, \cdot)$, where R is a set and $+$ and $\cdot$ are binary operations on R satisfying the following conditions.

- $(R, +)$ is an abelian group whose identity is denoted by 0.
- $(R, \cdot)$ is a (commutative) monoid whose identity is denoted by 1.
- $+$ and $\cdot$ are distributive: $a(b + c) = ab + ac$ for all $a, b, c \in R$.

Examples

- $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ are rings.

Definitions

1. An integral domain is a ring R such that for all $a, b \in R$ the equality $ab = 0$ implies that either $a = 0$ or $b = 0$, in which case, $(R \setminus \{0\}, \cdot)$ is called the multiplicative monoid of R.
2. A field is an integral domain R such that the multiplicative monoid of R is an abelian group.

Examples

- $\mathbb{Q}$ and $\mathbb{R}$ are fields, while $\mathbb{Z}$ is an integral domain that is not a field.

Monoid Domains

Let R be an integral domain, and let M be a monoid.

Definition. The monoid domain $R[M]$ of M over R is the commutative ring with identity consisting of all polynomial expressions in an indeterminate x with coefficients in R and exponents in M (under polynomial-like addition and multiplication).

Example. For $f := x^4 + x^{\frac{3}{2}}$ and $g := x^{\frac{3}{2}} + 1$ in the monoid domain $\mathbb{Z}[\mathbb{Q}_{\geq 0}]$,

$$f + g = x^4 + 2x^{\frac{3}{2}} + 1 \quad \text{and} \quad f \cdot g = x^{4+\frac{3}{2}} + x^4 + x^3 + x^{\frac{3}{2}}.$$

Examples of Monoid Domains

- The polynomial ring $R[x]$ is the monoid domain $R[\mathbb{N}_0]$.
- The Laurent polynomial ring $R[x^{\pm 1}]$ is the monoid domain $R[\mathbb{Z}]$.

Prime Reciprocal Puiseux Monoids

Definition. Let $(p_n)_{n \geq 1}$ be a strictly increasing sequence of primes.

$$M := \left\langle \frac{1}{p_n p_{n+2}} : n \in \mathbb{N} \right\rangle$$

is the 2-prime reciprocal Puiseux monoid of $(p_n)_{n \geq 1}$.

Remark. For a 2-prime reciprocal monoid, the following statements hold:

- M is atomic with
$$\mathcal{A}(M) = \left\{ \frac{1}{p_n p_{n+2}} : n \in \mathbb{N} \right\}.$$
- M does not satisfy the ACCP because $\left(\frac{1}{p_{2n}} + M \right)_{n \geq 1}$ forms an ascending chain of principal ideals of M that does not stabilize.

Problem (Open Question)

Let M be a 2-prime reciprocal Puiseux monoid, and let F be a field. Is the monoid domain $F[M]$ atomic?

Representation of Elements in Prime Reciprocal Puiseux Monoids

Theorem (L-W-Z 2024)

Let $(p_n)_{n\geq 1}$ be a strictly increasing sequence of primes, and let M be the 2-prime reciprocal Puiseux monoid induced by $(p_n)_{n\geq 1}$. Then each $q \in M$ can be written as follows:

$$q = c + \sum_{i=-1}^{n_q-2} c_{i+2} \frac{1}{p_i p_{i+2}},$$

where $n_q = \max(\{0\} \cup \{i \in \mathbb{N} : v_{p_i}(q) < 0\})$, $p_{-1} = p_0 = 1$, and $c, c_i \in \mathbb{N}_0$ for every $i \in [0, n-1]$.

Corollary. For every q, if $n_q \geq 1$, $\frac{1}{p_{n_q-2}p_{n_q}}$ divides q.

MCDs in Prime Reciprocal Puiseux Monoids

Theorem (L-W-Z 2024)

Any 2-prime reciprocal Puiseux monoid is an MCD monoid.

As all Puiseux monoids are submonoids of $\mathbb{Q}_{\geq 0}$ and thus countable, we get as a corollary of our earlier result:

Corollary. Any 2-prime reciprocal Puiseux monoid is MCD but not strongly MCD.

Grams-like Puiseux Monoids

Problem (Open Questions)

Let M be Grams' monoid, and let F be a field. Is the monoid domain $F[M]$ atomic?

Let $(d_n)_{n \ge 1}$ be a strictly increasing sequence of positive integers, and let $(p_n)_{n \ge 1}$ be a sequence of pairwise distinct primes such that $p_n \nmid d_m$ for any $m, n \in \mathbb{N}$. Now consider the following Puiseux monoids:

$$M := \Big\langle \frac{1}{d_n p_n} : n \in \mathbb{N} \Big\rangle \quad \text{and} \quad N := \Big\langle \frac{1}{d_n} : n \in \mathbb{N} \Big\rangle.$$

We call M the Grams-like monoid of the sequences $(d_n)_{n \ge 1}$ and $(p_n)_{n \ge 1}$ or, simply, a Grams-like monoid.

Remark. It is easy to verify that

1. M is atomic with $\mathcal{A}(M) = \big\{ \frac{1}{d_n p_n} : n \in \mathbb{N} \big\}$.
2. If N is a valuation monoid, then M does not satisfy the ACCP.

Representation of Elements in Grams-like Monoids

Proposition (L-W-Z 2024)

Let M be a Grams-like monoid. Each element $q \in M$ can be uniquely written as follows:

$$q = c_0(q) + \sum_{n \in \mathbb{N}} c_n(q) \frac{1}{d_n p_n},$$

where $c_0(q) \in N$ and $(c_n(q))_{\geq 1}$ is a sequence of nonnegative integers that eventually stabilizes to 0 such that $c_n(q) \in [0, p_n - 1]$ for every $n \in \mathbb{N}$.

Definition. Let M be a Grams-like monoid. For each $q \in M$, we call

$$c_0(q) + \sum_{n \in \mathbb{N}} c_n(q) \frac{1}{d_n p_n}$$

the canonical sum decomposition of q provided that the element $c_0(q)$ and the sequence $(c_n(q))_{n \geq 1}$ satisfy the conditions specified in the above proposition.

Immediate Consequences

Corollary. Let M be a Grams-like monoid. For any $q_1, q_2 \in M$ such that $q_1 \mid_M q_2$, let

$$q_1 = c_0(q_1) + \sum_{n \in \mathbb{N}} c_n(q_1) \frac{1}{d_n p_n} \quad \text{and} \quad q_2 = c_0(q_2) + \sum_{n \in \mathbb{N}} c_n(q_2) \frac{1}{d_n p_n}$$

be the canonical sum decompositions of q_1 and q_2, respectively. Then the following statements hold.

1. $c_0(q_1) \mid_N c_0(q_2)$.
2. $c_n(q_2) = (c_n(q_1) + c_n(q_2 - q_1)) \pmod{p_n}$ for every $n \in \mathbb{N}$.
3. If $c_0(q_1) = c_0(q_2)$, then $c_0(q_2 - q_1) = 0$.
4. If $c_0(q_1) = c_0(q_2)$, then $c_n(q_1) + c_n(q_2 - q_1) < p_n$ for every $n \in \mathbb{N}$.
5. If $c_0(q_1) = c_0(q_2)$, then $c_n(q_1) \leq c_n(q_2)$ for every $n \in \mathbb{N}$.

MCD and MCD-finite Properties of Grams-like Monoids

Theorem (L-W-Z 2024)

Let M be a Grams-like monoid.

- *If N is a valuation monoid, then M is an MCD monoid.*
- *M is MCD-finite if and only if N is MCD-finite.*

An Atomic Monoid that is not 2-MCD

Example. Let p_n denote the n-th prime number. Consider the rank-2 submonoid M of $\mathbb{Q}^2_{\geq 0}$ defined in the following way:

$$M := \left\langle \left(\frac{1}{2^n p_{2n}}, 0 \right), \left(\frac{1}{2^n p_{2n+1}}, \frac{1}{p_{2n+1}} \right) : n \in \mathbb{N} \right\rangle.$$

Fact. Every element in the defining generating set of M is an atom.

Proposition (L-W-Z 2024)

$(1,0)$ *and* $(1,1)$ *do not have a maximal common divisor. Therefore, M is an atomic monoid that is not 2-MCD.*

Acknowledgements

- We would like to thank our mentor Dr. Felix Gotti for guiding and supporting us throughout the research process.
- We would also like to thank to the MIT PRIMES program for making this research opportunity possible.
- Finally, we would like to thank our parents for supporting our research and participating in MIT PRIMES and all of you for listening to our presentation.

References

- D. D. Anderson, D. F. Anderson, and M. Zafrullah, *Factorizations in integral domains*, J. Pure Appl. Algebra **69** (1990) 1–19.
- J. Coykendall and F. Gotti, *On the atomicity of monoid algebras*, J. Algebra **539** (2019) 138–151.
- R. Gilmer, *Commutative Semigroup Rings*, Chicago Lectures in Mathematics, The University of Chicago Press, London, 1984.
- F. Gotti and B. Li, *Atomic semigroup rings and the ascending chain condition on principal ideals*, Proc. Amer. Math. Soc. **151** (2023) 2291–2302.
- A. Grams, *Atomic rings and the ascending chain condition for principal ideals*, Proc. Cambridge Philos. Soc., **75** (1974) 321–329.
- M. Roitman, *Polynomial extensions of atomic domains*, J. Pure Appl. Algebra **87** (1993) 187–199.

End of Presentation

THANK YOU!