Exploring the Catenary Degrees of Singular Arithmetical Congruence Monoids

Scott Chapman

Sam Houston State University

November 13, 2016

The Student Authors

This talk is based on the work completed under my direction at the 2013 PURE REU at the University of Hawaii at Hilo by the following students.

Theo McKenzie, Harvard

and Sherilyn Tamagawa, Scripps College

Prologue

Here are some background papers for this talk.

[1] A. Geroldinger and F. Halter-Koch. Congruence monoids. *ACTA Arithmetica* **112**(2004): 263-296.

[2] M. Banister, M., J. Chaika, S. Chapman, and W. Meyerson. On the arithmetic of arithmetical congruence monoids. *Colloq. Math* **108**(2007), 105-118.

[3] P. Baginski, and S. Chapman. Arithmetic congruence monoids: A survey. In *Combinatorial and Additive Number Theory*, pp. 15-38. Springer New York, 2014.

Prologue

Here are some background papers for this talk.

[1] A. Geroldinger and F. Halter-Koch. Congruence monoids. *ACTA Arithmetica* **112**(2004): 263-296.

[2] M. Banister, M., J. Chaika, S. Chapman, and W. Meyerson. On the arithmetic of arithmetical congruence monoids. *Colloq. Math* **108**(2007), 105-118.

[3] P. Baginski, and S. Chapman. Arithmetic congruence monoids: A survey. In *Combinatorial and Additive Number Theory*, pp. 15-38. Springer New York, 2014.

Prologue

Here are some background papers for this talk.

[1] A. Geroldinger and F. Halter-Koch. Congruence monoids. *ACTA Arithmetica* **112**(2004): 263-296.

[2] M. Banister, M., J. Chaika, S. Chapman, and W. Meyerson. On the arithmetic of arithmetical congruence monoids. *Colloq. Math* **108**(2007), 105-118.

[3] P. Baginski, and S. Chapman. Arithmetic congruence monoids: A survey. In *Combinatorial and Additive Number Theory*, pp. 15-38. Springer New York, 2014.

Prologue

Here are some background papers for this talk.

[1] A. Geroldinger and F. Halter-Koch. Congruence monoids. *ACTA Arithmetica* **112**(2004): 263-296.

[2] M. Banister, M., J. Chaika, S. Chapman, and W. Meyerson. On the arithmetic of arithmetical congruence monoids. *Colloq. Math* **108**(2007), 105-118.

[3] P. Baginski, and S. Chapman. Arithmetic congruence monoids: A survey. In *Combinatorial and Additive Number Theory*, pp. 15-38. Springer New York, 2014.

Motivation

THIS IS A COMMUTATIVE ALGEBRA TALK?

KIND OF.

Theorem

$\mathbb{Z} = \{\ldots -3, -2, -1, 0, 1, 2, 3, \ldots\}$ is a unique factorization domain (UFD).

Theorem

The multiplicative monoid $\mathbb{Z}^\bullet = \{\ldots -3, -2, -1, 1, 2, 3, \ldots\}$ is a unique factorization monoid (UFM).

Motivation

THIS IS A COMMUTATIVE ALGEBRA TALK?

KIND OF.

Theorem

$\mathbb{Z} = \{\ldots -3, -2, -1, 0, 1, 2, 3, \ldots\}$ is a unique factorization domain (UFD).

Theorem

The multiplicative monoid $\mathbb{Z}^\bullet = \{\ldots -3, -2, -1, 1, 2, 3, \ldots\}$ is a unique factorization monoid (UFM).

Motivation

THIS IS A COMMUTATIVE ALGEBRA TALK?

KIND OF.

Theorem

$\mathbb{Z} = \{\ldots -3, -2, -1, 0, 1, 2, 3, \ldots\}$ *is a unique factorization domain (UFD).*

Theorem

The multiplicative monoid $\mathbb{Z}^\bullet = \{\ldots -3, -2, -1, 1, 2, 3, \ldots\}$ *is a unique factorization monoid (UFM).*

Motivation

THIS IS A COMMUTATIVE ALGEBRA TALK?

KIND OF.

Theorem

$\mathbb{Z} = \{\ldots -3, -2, -1, 0, 1, 2, 3, \ldots\}$ *is a unique factorization domain (UFD).*

Theorem

The multiplicative monoid $\mathbb{Z}^\bullet = \{\ldots -3, -2, -1, 1, 2, 3, \ldots\}$ *is a unique factorization monoid (UFM).*

Our Object of Interest

Definition

Let $\Gamma \subseteq \mathbb{Z}_n = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$ be a multiplicatively closed subset. The subset

$$\mathbb{Z}_\Gamma = \{n \in \mathbb{Z} \mid n \equiv x \pmod{n} \text{ for some } \overline{x} \in \Gamma\} \cup \{1\}.$$

is a multiplicatively closed subset of $\mathbb{Z}$ known as a *congruence monoid* (of modulus n).

A Classic Result

Theorem (James & Niven, 1954 PAMS)

Let $n \geq 2$ be a positive integer. A congruence monoid S_Γ is a UFM if and only if $\Gamma = \{\overline{x} \mid \gcd(x, n) = 1\}$.

An alternate proof of this result can be found in Halter-Koch (Semigroup Forum 1991) which uses the notion of a *divisor theory*

$$\text{divisor theory} \Rightarrow \text{Krull domains.}$$

A Classic Result

Theorem (James & Niven, 1954 PAMS)

Let $n \geq 2$ be a positive integer. A congruence monoid S_Γ is a UFM if and only if $\Gamma = \{\overline{x} \mid \gcd(x, n) = 1\}$.

An alternate proof of this result can be found in Halter-Koch (Semigroup Forum 1991) which uses the notion of a *divisor theory*

divisor theory $\Rightarrow$ Krull domains.

A Classic Result

Theorem (James & Niven, 1954 PAMS)

Let $n \geq 2$ be a positive integer. A congruence monoid S_Γ is a UFM if and only if $\Gamma = \{\overline{x} \mid \gcd(x, n) = 1\}$.

An alternate proof of this result can be found in Halter-Koch (Semigroup Forum 1991) which uses the notion of a *divisor theory*

$$\text{divisor theory} \Rightarrow \text{Krull domains.}$$

The Other Extreme

Theorem

If $\Gamma = \{\overline{x} \mid \gcd(x, n) \neq 1\}$, *then* $\mathbb{Z}_\Gamma$ *is a half-factorial monoid.*

Half-factorial means that if

$$\alpha_1 \cdots \alpha_s = \beta_1 \cdots \beta_t$$

where each α_i and β_j is irreducible, then $s = t$.

The Other Extreme

Theorem

If $\Gamma = \{\overline{x} \mid \gcd(x, n) \neq 1\}$, *then* $\mathbb{Z}_\Gamma$ *is a half-factorial monoid.*

Half-factorial means that if

$$\alpha_1 \cdots \alpha_s = \beta_1 \cdots \beta_t$$

where each α_i and β_j is irreducible, then $s = t$.

A Special Case

If $\Gamma = \{\overline{x}\}$, then $\mathbb{Z}_\Gamma$ is called an *arithmetical congruence monoid* (or ACM).

Hence, an ACM is merely an arithmetic sequence that is closed under multiplication.

Example

$$1, 5, 9, 13, 17, 21, \ldots = 1 + 4\mathbb{N}_0$$

is known as the *Hilbert Monoid*.

Example

$$1, 4, 10, 16, 22, \ldots = 4 + 6\mathbb{N}_0 \cup \{1\}$$

is known as *Myerson's monoid*

A Special Case

If $\Gamma = \{\overline{x}\}$, then $\mathbb{Z}_\Gamma$ is called an *arithmetical congruence monoid* (or ACM).

Hence, an ACM is merely an arithmetic sequence that is closed under multiplication.

Example

$$1, 5, 9, 13, 17, 21, \ldots = 1 + 4\mathbb{N}_0$$

is known as the *Hilbert Monoid*.

Example

$$1, 4, 10, 16, 22, \ldots = 4 + 6\mathbb{N}_0 \cup \{1\}$$

is known as *Myerson's monoid*

A Special Case

If $\Gamma = \{\overline{x}\}$, then $\mathbb{Z}_\Gamma$ is called an *arithmetical congruence monoid* (or ACM).

Hence, an ACM is merely an arithmetic sequence that is closed under multiplication.

Example

$$1, 5, 9, 13, 17, 21, \ldots = 1 + 4\mathbb{N}_0$$

is known as the *Hilbert Monoid*.

Example

$$1, 4, 10, 16, 22, \ldots = 4 + 6\mathbb{N}_0 \cup \{1\}$$

is known as *Myerson's monoid*

A Special Case

If $\Gamma = \{\overline{x}\}$, then $\mathbb{Z}_\Gamma$ is called an *arithmetical congruence monoid* (or ACM).

Hence, an ACM is merely an arithmetic sequence that is closed under multiplication.

Example

$$1, 5, 9, 13, 17, 21, \ldots = 1 + 4\mathbb{N}_0$$

is known as the *Hilbert Monoid*.

Example

$$1, 4, 10, 16, 22, \ldots = 4 + 6\mathbb{N}_0 \cup \{1\}$$

is known as *Myerson's monoid*

Types of ACMs

Thus every ACM can be written uniquely in the form

$$M_{a,b} = a + b\mathbb{N}_0 \cup \{1\}$$

and they break into three catagories.

Regular ACMs: These correspond to $a = 1$.

Singlar ACMs: These come in two types:

Local: $\gcd(a, b) = p^n$ for some prime p;

Global: $\gcd(a, b) = d > 1$ and d is composite and not a power of a prime.

Types of ACMs

Thus every ACM can be written uniquely in the form

$$M_{a,b} = a + b\mathbb{N}_0 \cup \{1\}$$

and they break into three catagories.

Regular ACMs: These correspond to $a = 1$.

Singlar ACMs: These come in two types:

Local: $\gcd(a, b) = p^n$ for some prime p;

Global: $\gcd(a, b) = d > 1$ and d is composite and not a power of a prime.

Types of ACMs

Thus every ACM can be written uniquely in the form

$$M_{a,b} = a + b\mathbb{N}_0 \cup \{1\}$$

and they break into three catagories.

Regular ACMs: These correspond to $a = 1$.

Singlar ACMs: These come in two types:

Local: $\gcd(a, b) = p^n$ for some prime p;

Global: $\gcd(a, b) = d > 1$ and d is composite and not a power of a prime.

Types of ACMs

Thus every ACM can be written uniquely in the form

$$M_{a,b} = a + b\mathbb{N}_0 \cup \{1\}$$

and they break into three catagories.

Regular ACMs: These correspond to $a = 1$.

Singlar ACMs: These come in two types:

Local: $\gcd(a, b) = p^n$ for some prime p;

Global: $\gcd(a, b) = d > 1$ and d is composite and not a power of a prime.

Types of ACMs

Thus every ACM can be written uniquely in the form

$$M_{a,b} = a + b\mathbb{N}_0 \cup \{1\}$$

and they break into three catagories.

Regular ACMs: These correspond to $a = 1$.

Singlar ACMs: These come in two types:

Local: $\gcd(a, b) = p^n$ for some prime p;

Global: $\gcd(a, b) = d > 1$ and d is composite and not a power of a prime.

The Regular Case

If $a = 1$, then the factorization properties of $M_{1,b}$ are identical to those of the multiplicative monoid of a Dedekind domain D with class group $\mathbb{Z}_b^\times$ where each divisor class of the class group contains a nonzero prime ideal.

For instance, $\rho(M_{1,b}) = \frac{D(\mathbb{Z}_n^\times)}{2}$.

Moreover, if $M_{a,b}$ is global, then $\rho(M_{a,b}) = \infty$.

If $M_{a,b}$ is local, then $\rho(M_{a,b}) = \frac{n+k-1}{k}$ where n is the smallest integer such that $p^n \in M_{a,b}$.

The Regular Case

If $a = 1$, then the factorization properties of $M_{1,b}$ are identical to those of the multiplicative monoid of a Dedekind domain D with class group $\mathbb{Z}_b^\times$ where each divisor class of the class group contains a nonzero prime ideal.

For instance, $\rho(M_{1,b}) = \frac{D(\mathbb{Z}_n^\times)}{2}$.

Moreover, if $M_{a,b}$ is global, then $\rho(M_{a,b}) = \infty$.

If $M_{a,b}$ is local, then $\rho(M_{a,b}) = \frac{n+k-1}{k}$ where n is the smallest integer such that $p^n \in M_{a,b}$.

The Regular Case

If $a = 1$, then the factorization properties of $M_{1,b}$ are identical to those of the multiplicative monoid of a Dedekind domain D with class group $\mathbb{Z}_b^\times$ where each divisor class of the class group contains a nonzero prime ideal.

For instance, $\rho(M_{1,b}) = \frac{D(\mathbb{Z}_n^\times)}{2}$.

Moreover, if $M_{a,b}$ is global, then $\rho(M_{a,b}) = \infty$.

If $M_{a,b}$ is local, then $\rho(M_{a,b}) = \frac{n+k-1}{k}$ where n is the smallest integer such that $p^n \in M_{a,b}$.

The Regular Case

If $a = 1$, then the factorization properties of $M_{1,b}$ are identical to those of the multiplicative monoid of a Dedekind domain D with class group $\mathbb{Z}_b^\times$ where each divisor class of the class group contains a nonzero prime ideal.

For instance, $\rho(M_{1,b}) = \frac{D(\mathbb{Z}_n^\times)}{2}$.

Moreover, if $M_{a,b}$ is global, then $\rho(M_{a,b}) = \infty$.

If $M_{a,b}$ is local, then $\rho(M_{a,b}) = \frac{n+k-1}{k}$ where n is the smallest integer such that $p^n \in M_{a,b}$.

Definitions

Suppose that M is reduced, $x \in M$ is not the identity, and that

$$F : x = \alpha_1 \cdots \alpha_n \beta_1 \cdots \beta_s \text{ and } F' : x = \alpha_1 \cdots \alpha_n \gamma_1 \cdots \gamma_t$$

are distinct atomic factorizations such that $\beta_i \neq \gamma_j$ for all i, j.

With notation as above, we define $\gcd(F, F') = \alpha_1 \cdots \alpha_n$ and the *distance* between F and F' by $d(F, F') = \max\{s, t\}$. Extend d to all pairs of factorizations by $d(F, F) = 0$.

Definitions

Suppose that M is reduced, $x \in M$ is not the identity, and that

$$F : x = \alpha_1 \cdots \alpha_n \beta_1 \cdots \beta_s \text{ and } F' : x = \alpha_1 \cdots \alpha_n \gamma_1 \cdots \gamma_t$$

are distinct atomic factorizations such that $\beta_i \neq \gamma_j$ for all i, j.

With notation as above, we define $\gcd(F, F') = \alpha_1 \cdots \alpha_n$ and the *distance* between F and F' by $d(F, F') = \max\{s, t\}$. Extend d to all pairs of factorizations by $d(F, F) = 0$.

The Distance is Amazing

The distance function acts as a metric. The following for a numerical monoid can easily be shown (and are in fact true in general).

Theorem

Let F_1, F_2 and F_3 be factorizations of x in a numerical monoid S.

1. $\mathrm{d}(F_1, F_2) = 0$ *if and only if* $F_1 = F_2$.
2. $\mathrm{d}(F_1, F_2) = \mathrm{d}(F_2, F_1)$.
3. $\mathrm{d}(F_1, F_2) \leq \mathrm{d}(F_1, F_3) + \mathrm{d}(F_3, F_2)$.
4. $\mathrm{d}(F_3F_1, F_3F_2) = \mathrm{d}(F_1, F_2)$.
5. $\mathrm{d}(F_1^k, F_2^k) = k\mathrm{d}(F_1, F_2)$.

The Distance is Amazing

The distance function acts as a metric. The following for a numerical monoid can easily be shown (and are in fact true in general).

Theorem

Let F_1, F_2 and F_3 be factorizations of x in a numerical monoid S.

1. $\mathrm{d}(F_1, F_2) = 0$ *if and only if* $F_1 = F_2$.
2. $\mathrm{d}(F_1, F_2) = \mathrm{d}(F_2, F_1)$.
3. $\mathrm{d}(F_1, F_2) \leq \mathrm{d}(F_1, F_3) + \mathrm{d}(F_3, F_2)$.
4. $\mathrm{d}(F_3F_1, F_3F_2) = \mathrm{d}(F_1, F_2)$.
5. $\mathrm{d}(F_1^k, F_2^k) = k\mathrm{d}(F_1, F_2)$.

More Definitions

An *N-chain of factorizations* from F to F' is a sequence $F_0, \ldots, F_k$ such that each F_i is a factorization of x, $F_0 = F$ and $F_k = F'$, and $d(F_i, F_{i+1}) \leq N$ for all $i < k$.

The catenary degree of x, denoted $c(x)$, is the least $N \in \mathbb{Z}_{\geq 0} \cup \{\infty\}$ such that for any two factorizations F, F' of x there is an N-chain between F and F'.

The catenary degree of the monoid M is defined as

$$c(M) = \sup\{\, c(x) \mid x \in M \setminus M^\times \,\}.$$

Note: If S does not have unique factorization, then $\mathrm{c}(S) \geq 2$ and if $\mathrm{c}(S) = 2$, then S is half-factorial.

More Definitions

An *N-chain of factorizations* from F to F' is a sequence $F_0, \ldots, F_k$ such that each F_i is a factorization of x, $F_0 = F$ and $F_k = F'$, and $d(F_i, F_{i+1}) \leq N$ for all $i < k$.

The catenary degree of x, denoted $c(x)$, is the least $N \in \mathbb{Z}_{\geq 0} \cup \{\infty\}$ such that for any two factorizations F, F' of x there is an N-chain between F and F'.

The catenary degree of the monoid M is defined as

$$c(M) = \sup\{\, c(x) \mid x \in M \setminus M^\times \,\}.$$

Note: If S does not have unique factorization, then $\mathrm{c}(S) \geq 2$ and if $\mathrm{c}(S) = 2$, then S is half-factorial.

More Definitions

An *N-chain of factorizations* from F to F' is a sequence $F_0, \ldots, F_k$ such that each F_i is a factorization of x, $F_0 = F$ and $F_k = F'$, and $d(F_i, F_{i+1}) \leq N$ for all $i < k$.

The catenary degree of x, denoted $c(x)$, is the least $N \in \mathbb{Z}_{\geq 0} \cup \{\infty\}$ such that for any two factorizations F, F' of x there is an N-chain between F and F'.

The catenary degree of the monoid M is defined as

$$c(M) = \sup\{\, c(x) \mid x \in M \setminus M^\times \,\}.$$

Note: If S does not have unique factorization, then $\mathrm{c}(S) \geq 2$ and if $\mathrm{c}(S) = 2$, then S is half-factorial.

More Definitions

An *N-chain of factorizations* from F to F' is a sequence $F_0, \ldots, F_k$ such that each F_i is a factorization of x, $F_0 = F$ and $F_k = F'$, and $d(F_i, F_{i+1}) \leq N$ for all $i < k$.

The catenary degree of x, denoted $c(x)$, is the least $N \in \mathbb{Z}_{\geq 0} \cup \{\infty\}$ such that for any two factorizations F, F' of x there is an N-chain between F and F'.

The catenary degree of the monoid M is defined as

$$c(M) = \sup\{\, c(x) \mid x \in M \setminus M^\times \,\}.$$

Note: If S does not have unique factorization, then $\mathrm{c}(S) \geq 2$ and if $\mathrm{c}(S) = 2$, then S is half-factorial.