REU projects involving non-unique factorization in integral domains and monoids: Past, Present, and Future.

Scott Chapman

Sam Houston State University

January 6, 2017

Prologue

[1] P. Baginski and S. T. Chapman, Factorizations of Algebraic Integers, Block Monoids and Additive Number Theory, *Amer. Math. Monthly* **118**(2011), 901-920.

[2] D.F. Anderson, Elasticity of factorizations in integral domains: a survey, *Lecture Notes in Pure and Appl. Math.* **189**(1997), 1–29.

[3] S. T. Chapman, On the Davenport constant, the cross number and their application in factorization theory, *Lecture Notes in Pure and Applied Mathematics*, Marcel Dekker, **171**(1995), 167-190.

[4] A. Geroldinger and F. Halter-Koch, *Non-unique factorizations. Algebraic, Combinatorial and Analytic Theory*, Chapman & Hall/CRC, 2006.

Prologue

[1] P. Baginski and S. T. Chapman, Factorizations of Algebraic Integers, Block Monoids and Additive Number Theory, *Amer. Math. Monthly* **118**(2011), 901-920.

[2] D.F. Anderson, Elasticity of factorizations in integral domains: a survey, *Lecture Notes in Pure and Appl. Math.* **189**(1997), 1–29.

[3] S. T. Chapman, On the Davenport constant, the cross number and their application in factorization theory, *Lecture Notes in Pure and Applied Mathematics*, Marcel Dekker, **171**(1995), 167-190.

[4] A. Geroldinger and F. Halter-Koch, *Non-unique factorizations. Algebraic, Combinatorial and Analytic Theory*, Chapman & Hall/CRC, 2006.

Prologue

[1] P. Baginski and S. T. Chapman, Factorizations of Algebraic Integers, Block Monoids and Additive Number Theory, *Amer. Math. Monthly* **118**(2011), 901-920.

[2] D.F. Anderson, Elasticity of factorizations in integral domains: a survey, *Lecture Notes in Pure and Appl. Math.* **189**(1997), 1–29.

[3] S. T. Chapman, On the Davenport constant, the cross number and their application in factorization theory, *Lecture Notes in Pure and Applied Mathematics*, Marcel Dekker, **171**(1995), 167-190.

[4] A. Geroldinger and F. Halter-Koch, *Non-unique factorizations. Algebraic, Combinatorial and Analytic Theory*, Chapman & Hall/CRC, 2006.

Prologue

[1] P. Baginski and S. T. Chapman, Factorizations of Algebraic Integers, Block Monoids and Additive Number Theory, *Amer. Math. Monthly* **118**(2011), 901-920.

[2] D.F. Anderson, Elasticity of factorizations in integral domains: a survey, *Lecture Notes in Pure and Appl. Math.* **189**(1997), 1–29.

[3] S. T. Chapman, On the Davenport constant, the cross number and their application in factorization theory, *Lecture Notes in Pure and Applied Mathematics*, Marcel Dekker, **171**(1995), 167-190.

[4] A. Geroldinger and F. Halter-Koch, *Non-unique factorizations. Algebraic, Combinatorial and Analytic Theory*, Chapman & Hall/CRC, 2006.

What is it?

What is the Theory of Non-unique Factorizations?

Origins

The usual example used in an undergraduate Abstract Algebra Textbook to demonstrate that the Fundamental Theorem of Arithmetic can fail in an integral domain is:

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}) \tag{1}$$

in the algebraic number ring $\mathbb{Z}[\sqrt{-5}]$.

The actual argument to complete this observation involves showing two things:

(i) $2, 3, 1 + \sqrt{-5}$ and $1 - \sqrt{-5}$ are all irreducible, and

(ii) 2 (resp. 3) is neither an associate of $(1 + \sqrt{-5})$ nor of $(1 - \sqrt{-5})$ (this is clear once ± 1 are established as the only units of $\mathbb{Z}[\sqrt{-5}]$).

Origins

The usual example used in an undergraduate Abstract Algebra Textbook to demonstrate that the Fundamental Theorem of Arithmetic can fail in an integral domain is:

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}) \tag{1}$$

in the algebraic number ring $\mathbb{Z}[\sqrt{-5}]$.

The actual argument to complete this observation involves showing two things:

(i) $2, 3, 1 + \sqrt{-5}$ and $1 - \sqrt{-5}$ are all irreducible, and

(ii) 2 (resp. 3) is neither an associate of $(1 + \sqrt{-5})$ nor of $(1 - \sqrt{-5})$ (this is clear once ± 1 are established as the only units of $\mathbb{Z}[\sqrt{-5}]$).

Origins

The usual example used in an undergraduate Abstract Algebra Textbook to demonstrate that the Fundamental Theorem of Arithmetic can fail in an integral domain is:

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}) \tag{1}$$

in the algebraic number ring $\mathbb{Z}[\sqrt{-5}]$.

The actual argument to complete this observation involves showing two things:

(i) $2, 3, 1 + \sqrt{-5}$ and $1 - \sqrt{-5}$ are all irreducible, and

(ii) 2 (resp. 3) is neither an associate of $(1 + \sqrt{-5})$ nor of $(1 - \sqrt{-5})$ (this is clear once ± 1 are established as the only units of $\mathbb{Z}[\sqrt{-5}]$).

Origins

Most books fail to point out to the readers that while $\mathbb{Z}[\sqrt{-5}]$ is not a UFD, it does have a rather nice factorization property.

Specifically, if $\alpha_1, \ldots \alpha_n, \beta_1, \ldots, \beta_m$ are irreducible elements of $\mathbb{Z}[\sqrt{-5}]$ with

$$\alpha_1 \cdots \alpha_n = \beta_1 \cdots \beta_m, \tag{2}$$

then $n = m$.

In general, an integral domain with this property is known as a *half-factorial domain* (HFD).

Origins

Most books fail to point out to the readers that while $\mathbb{Z}[\sqrt{-5}]$ is not a UFD, it does have a rather nice factorization property.

Specifically, if $\alpha_1, \ldots \alpha_n, \beta_1, \ldots, \beta_m$ are irreducible elements of $\mathbb{Z}[\sqrt{-5}]$ with

$$\alpha_1 \cdots \alpha_n = \beta_1 \cdots \beta_m, \tag{2}$$

then $n = m$.

In general, an integral domain with this property is known as a *half-factorial domain* (HFD).

Origins

Most books fail to point out to the readers that while $\mathbb{Z}[\sqrt{-5}]$ is not a UFD, it does have a rather nice factorization property.

Specifically, if $\alpha_1, \ldots \alpha_n, \beta_1, \ldots, \beta_m$ are irreducible elements of $\mathbb{Z}[\sqrt{-5}]$ with

$$\alpha_1 \cdots \alpha_n = \beta_1 \cdots \beta_m, \tag{2}$$

then $n = m$.

In general, an integral domain with this property is known as a *half-factorial domain* (HFD).

Goals

Using the ideal class group (and, more generally, the class number), one can construct a very simple proof of this fact for $\mathbb{Z}[\sqrt{-5}]$.

Carlitz first illustrated this argument in *PAMS* 11(1960), 391-392.

His proof (while short) leads to a deeper understanding of how elements factor in an algebraic ring of integers.

Goals

Using the ideal class group (and, more generally, the class number), one can construct a very simple proof of this fact for $\mathbb{Z}[\sqrt{-5}]$.

Carlitz first illustrated this argument in *PAMS* 11(1960), 391-392.

His proof (while short) leads to a deeper understanding of how elements factor in an algebraic ring of integers.

Goals

Using the ideal class group (and, more generally, the class number), one can construct a very simple proof of this fact for $\mathbb{Z}[\sqrt{-5}]$.

Carlitz first illustrated this argument in *PAMS* 11(1960), 391-392.

His proof (while short) leads to a deeper understanding of how elements factor in an algebraic ring of integers.

A Little More Terminology

Let M be a commutative cancellative monoid in which each nonunit can be written as product of irreducible elements (such a monoid is called *atomic*).

Let $\mathcal{A}(M)$ represent the set of irreducible elements of M and $M^\times$ its set of units.

Note that $\mathcal{A}(M)$ contains the prime elements of M (if there are any!).

A Little More Terminology

Let M be a commutative cancellative monoid in which each nonunit can be written as product of irreducible elements (such a monoid is called *atomic*).

Let $\mathcal{A}(M)$ represent the set of irreducible elements of M and $M^\times$ its set of units.

Note that $\mathcal{A}(M)$ contains the prime elements of M (if there are any!).

A Little More Terminology

Let M be a commutative cancellative monoid in which each nonunit can be written as product of irreducible elements (such a monoid is called *atomic*).

Let $\mathcal{A}(M)$ represent the set of irreducible elements of M and $M^\times$ its set of units.
Note that $\mathcal{A}(M)$ contains the prime elements of M (if there are any!).

The Main Object of Our Interest

For $x \in M \backslash M^\times$, set

$$\mathcal{L}(x) = \{n \mid n \in \mathbb{N} \text{ and there exist } x_1, \ldots, x_n \in \mathcal{A}(M) \text{ with } x = x_1 \cdots x_n\}.$$

We will refer to $\mathcal{L}(x)$ as the *set of lengths of* x in M.

The Main Object of Our Interest

For $x \in M \backslash M^\times$, set

$$\mathcal{L}(x) = \{n \mid n \in \mathbb{N} \text{ and there exist } x_1, \ldots, x_n \in \mathcal{A}(M) \text{ with } x = x_1 \cdots x_n\}.$$

We will refer to $\mathcal{L}(x)$ as the *set of lengths of* x in M.

A Little More Terminology

We can extend $\mathcal{L}(x)$ to a global descriptor by setting

$$\mathcal{L}(M) = \{\mathcal{L}(x) \mid x \in M \backslash M^{\times}\}.$$

We will refer to $\mathcal{L}(M)$ as the *set of lengths of* M.

A Little More Terminology

We can extend $\mathcal{L}(x)$ to a global descriptor by setting

$$\mathcal{L}(M) = \{\mathcal{L}(x) \mid x \in M \backslash M^{\times}\}.$$

We will refer to $\mathcal{L}(M)$ as the *set of lengths of* M.

First Order Factorization Invariants

We can directly read our first two factorization invariants off the set $\mathcal{L}(x)$.

For $x \in M \backslash M^\times$ set

$$L(x) = \sup\{n \mid \text{there are } x_1, \ldots, x_n \in \mathcal{A}(M) \text{ such that } x = x_1 \cdots x_n\}$$

and

$$l(x) = \inf\{n \mid \text{there are } x_1, \ldots, x_n \in \mathcal{A}(M) \text{ such that } x = x_1 \cdots x_n\}.$$

First Order Factorization Invariants

We can directly read our first two factorization invariants off the set $\mathcal{L}(x)$.

For $x \in M \backslash M^\times$ set

$$L(x) = \sup\{n \mid \text{there are } x_1, \ldots, x_n \in \mathcal{A}(M) \text{ such that } x = x_1 \cdots x_n\}$$

and

$$l(x) = \inf\{n \mid \text{there are } x_1, \ldots, x_n \in \mathcal{A}(M) \text{ such that } x = x_1 \cdots x_n\}.$$

First Order Factorization Invariants

We can directly read our first two factorization invariants off the set $\mathcal{L}(x)$.

For $x \in M \backslash M^\times$ set

$$L(x) = \sup\{n \mid \text{there are } x_1, \ldots, x_n \in \mathcal{A}(M) \text{ such that } x = x_1 \cdots x_n\}$$

and

$$l(x) = \inf\{n \mid \text{there are } x_1, \ldots, x_n \in \mathcal{A}(M) \text{ such that } x = x_1 \cdots x_n\}.$$

REU Theorem 1 and 2

REU Theorem (Anderson-Pruis, PAMS, 1991)

Let D be an integral domain and x a nonunit of D. Then the limits

$$\overline{L}(x) = \lim_{n\to\infty} \frac{L(x^n)}{n} \text{ and } \overline{l}(x) = \lim_{n\to\infty} \frac{l(x^n)}{n}$$

both exist (although the first might be ∞).

REU Theorem (Anderson-Pruis, PAMS, 1991)

Let $\alpha \leq \beta$ be real numbers taken from $[0, \infty]$. There exists an integral domain D and nonunit $x \in D$ with

$$\overline{l}(x) = \alpha \text{ and } \overline{L}(x) = \beta.$$

REU Theorem 1 and 2

REU Theorem (Anderson-Pruis, PAMS, 1991)

Let D be an integral domain and x a nonunit of D. Then the limits

$$\overline{L}(x) = \lim_{n\to\infty} \frac{L(x^n)}{n} \text{ and } \overline{l}(x) = \lim_{n\to\infty} \frac{l(x^n)}{n}$$

both exist (although the first might be ∞).

REU Theorem (Anderson-Pruis, PAMS, 1991)

Let $\alpha \leq \beta$ be real numbers taken from $[0, \infty]$. There exists an integral domain D and nonunit $x \in D$ with

$$\overline{l}(x) = \alpha \text{ and } \overline{L}(x) = \beta.$$

A Fundamental Invariant

The *elasticity of* x is defined as

$$\rho(x) = \frac{L(x)}{l(x)}.$$

We can again extend this definition to all of M by setting

$$\rho(M) = \sup\{\rho(x) \mid x \in M \backslash M^\times\}$$

and call $\rho(M)$ the *elasticity of* M.

If $\rho(M) = 1$, then M is called *half-factorial*.

A Fundamental Invariant

The *elasticity of* x is defined as

$$\rho(x) = \frac{L(x)}{l(x)}.$$

We can again extend this definition to all of M by setting

$$\rho(M) = \sup\{\rho(x) \mid x \in M \backslash M^{\times}\}$$

and call $\rho(M)$ the *elasticity of* M.

If $\rho(M) = 1$, then M is called *half-factorial*.

A Fundamental Invariant

The *elasticity of* x is defined as

$$\rho(x) = \frac{L(x)}{l(x)}.$$

We can again extend this definition to all of M by setting

$$\rho(M) = \sup\{\rho(x) \mid x \in M \backslash M^{\times}\}$$

and call $\rho(M)$ the *elasticity of* M.

If $\rho(M) = 1$, then M is called *half-factorial*.

Types of Elasticity

Suppose $\rho(M) < \infty$. If there is a nonunit x in M with

$$\rho(x) = \rho(M),$$

then we say that the elasticity of M is *accepted*.

We call M *fully elastic* if for every rational q with

$$1 \leq q \leq \rho(M),$$

there is a nonunit $x \in M$ with

$$\rho(x) = q.$$

Types of Elasticity

Suppose $\rho(M) < \infty$. If there is a nonunit x in M with

$$\rho(x) = \rho(M),$$

then we say that the elasticity of M is *accepted*.

We call M *fully elastic* if for every rational q with

$$1 \leq q \leq \rho(M),$$

there is a nonunit $x \in M$ with

$$\rho(x) = q.$$

A General Result

REU Theorem (Baginski-Chapman-Crutchfield-Kennedy-Wright, 2006, Results in Mathematics)

Let M be an atomic monoid with accepted elasticity and a prime element. Then M is fully elastic.

A Fundamental Invariant Set

Given $x \in M \setminus M^\times$, write its length set in the form

$$\mathcal{L}(x) = \{n_1, n_2, \ldots, n_k\}$$

where $n_i < n_{i+1}$ for $1 \leq i \leq k-1$. The Δ-*set* of x is defined by $\Delta(x) = \{n_i - n_{i-1} \mid 2 \leq i \leq k\}$ and the *delta set* of M by

$$\Delta(M) = \bigcup_{x \in M \setminus M^\times} \Delta(x).$$

If $d = \min \Delta(M)$, then by a Theorem of Geroldinger

$$\{d\} \subseteq \Delta(M) \subseteq \{d, 2d, \ldots, kd, \ldots\}$$

for some positive integer k.

A Fundamental Invariant Set

Given $x \in M \setminus M^\times$, write its length set in the form

$$\mathcal{L}(x) = \{n_1, n_2, \ldots, n_k\}$$

where $n_i < n_{i+1}$ for $1 \leq i \leq k-1$. The Δ-*set* of x is defined by $\Delta(x) = \{n_i - n_{i-1} \mid 2 \leq i \leq k\}$ and the *delta set* of M by

$$\Delta(M) = \bigcup_{x \in M \setminus M^\times} \Delta(x).$$

If $d = \min \Delta(M)$, then by a Theorem of Geroldinger

$$\{d\} \subseteq \Delta(M) \subseteq \{d, 2d, \ldots, kd, \ldots\}$$

for some positive integer k.

A Fundamental Invariant Set

Given $x \in M \setminus M^\times$, write its length set in the form

$$\mathcal{L}(x) = \{n_1, n_2, \ldots, n_k\}$$

where $n_i < n_{i+1}$ for $1 \leq i \leq k-1$. The Δ-*set* of x is defined by $\Delta(x) = \{n_i - n_{i-1} \mid 2 \leq i \leq k\}$ and the *delta set* of M by

$$\Delta(M) = \bigcup_{x \in M \setminus M^\times} \Delta(x).$$

If $d = \min \Delta(M)$, then by a Theorem of Geroldinger

$$\{d\} \subseteq \Delta(M) \subseteq \{d, 2d, \ldots, kd, \ldots\}$$

for some positive integer k.

Questions

Given an atomic monoid M, here are some questions one can always ask.

1. What is the elasticity of M?
2. When is M half-factorial?
3. Is the elasticity accepted?
4. Is M fully elastic?
5. What is $\Delta(M)$?

Questions

Given an atomic monoid M, here are some questions one can always ask.

1. What is the elasticity of M?
2. When is M half-factorial?
3. Is the elasticity accepted?
4. Is M fully elastic?
5. What is $\Delta(M)$?

Questions

Given an atomic monoid M, here are some questions one can always ask.

1. What is the elasticity of M?
2. When is M half-factorial?
3. Is the elasticity accepted?
4. Is M fully elastic?
5. What is $\Delta(M)$?

Questions

Given an atomic monoid M, here are some questions one can always ask.

1. What is the elasticity of M?
2. When is M half-factorial?
3. Is the elasticity accepted?
4. Is M fully elastic?
5. What is $\Delta(M)$?

Questions

Given an atomic monoid M, here are some questions one can always ask.

1. What is the elasticity of M?
2. When is M half-factorial?
3. Is the elasticity accepted?
4. Is M fully elastic?
5. What is $\Delta(M)$?

Questions

Given an atomic monoid M, here are some questions one can always ask.

1. What is the elasticity of M?
2. When is M half-factorial?
3. Is the elasticity accepted?
4. Is M fully elastic?
5. What is $\Delta(M)$?

Great REU Monoids

Some basic monoids of factorization theory which are great REU monoids.

1. Block Monoids
2. Numerical Monoids
3. Congruence Monoids - Arithmetic Congruence Monoids
4. Rings of integer-valued polynomials

Great REU Monoids

Some basic monoids of factorization theory which are great REU monoids.

1. Block Monoids
2. Numerical Monoids
3. Congruence Monoids - Arithmetic Congruence Monoids
4. Rings of integer-valued polynomials

Great REU Monoids

Some basic monoids of factorization theory which are great REU monoids.

1. Block Monoids
2. Numerical Monoids
3. Congruence Monoids - Arithmetic Congruence Monoids
4. Rings of integer-valued polynomials

Great REU Monoids

Some basic monoids of factorization theory which are great REU monoids.

1. Block Monoids
2. Numerical Monoids
3. Congruence Monoids - Arithmetic Congruence Monoids
4. Rings of integer-valued polynomials

Great REU Monoids

Some basic monoids of factorization theory which are great REU monoids.

1. Block Monoids
2. Numerical Monoids
3. Congruence Monoids - Arithmetic Congruence Monoids
4. Rings of integer-valued polynomials

Block Monoids

Let G be an abelian group. Further, let $\mathcal{F}(G)$ represent the free abelian monoid on G. We write the elements of $\mathcal{F}(G)$ as $C = \prod_{g \in G} g^{v_g(C)}$ where $v_g(C)$ is a nonnegative integer.

Definition

Let G be an abelian group. The set

$$\mathcal{B}(G) = \left\{ C \;\middle|\; C = \prod_{g \in G} g^{v_g(C)} \text{ with } \sum_{g \in G} v_g(C) g = 0 \right\}$$

forms a submonoid of $\mathcal{F}(G)$ known as the *block monoid of* G.

We call the identity of $\mathcal{B}(G)$, $E = \prod_{g \in G} g^0$, the *empty block*.

A block B divides a block C, denoted $B \mid C$ if there is a block T such that $C = BT$.

Block Monoids

Let G be an abelian group. Further, let $\mathcal{F}(G)$ represent the free abelian monoid on G. We write the elements of $\mathcal{F}(G)$ as $C = \prod_{g \in G} g^{v_g(C)}$ where $v_g(C)$ is a nonnegative integer.

Definition

Let G be an abelian group. The set

$$\mathcal{B}(G) = \left\{ C \;\middle|\; C = \prod_{g \in G} g^{v_g(C)} \text{ with } \sum_{g \in G} v_g(C) g = 0 \right\}$$

forms a submonoid of $\mathcal{F}(G)$ known as the *block monoid of* G.

We call the identity of $\mathcal{B}(G)$, $E = \prod_{g \in G} g^0$, the *empty block*.

A block B divides a block C, denoted $B \mid C$ if there is a block T such that $C = BT$.

Block Monoids

Let G be an abelian group. Further, let $\mathcal{F}(G)$ represent the free abelian monoid on G. We write the elements of $\mathcal{F}(G)$ as $C = \prod_{g \in G} g^{v_g(C)}$ where $v_g(C)$ is a nonnegative integer.

Definition

Let G be an abelian group. The set

$$\mathcal{B}(G) = \left\{ C \;\middle|\; C = \prod_{g \in G} g^{v_g(C)} \text{ with } \sum_{g \in G} v_g(C) g = 0 \right\}$$

forms a submonoid of $\mathcal{F}(G)$ known as the *block monoid of* G.

We call the identity of $\mathcal{B}(G)$, $E = \prod_{g \in G} g^0$, the *empty block*.

A block B divides a block C, denoted $B \mid C$ if there is a block T such that $C = BT$.

Block Monoids

Let G be an abelian group. Further, let $\mathcal{F}(G)$ represent the free abelian monoid on G. We write the elements of $\mathcal{F}(G)$ as $C = \prod_{g \in G} g^{v_g(C)}$ where $v_g(C)$ is a nonnegative integer.

Definition

Let G be an abelian group. The set

$$\mathcal{B}(G) = \left\{ C \;\middle|\; C = \prod_{g \in G} g^{v_g(C)} \text{ with } \sum_{g \in G} v_g(C) g = 0 \right\}$$

forms a submonoid of $\mathcal{F}(G)$ known as the *block monoid of* G.

We call the identity of $\mathcal{B}(G)$, $E = \prod_{g \in G} g^0$, the *empty block*.

A block B divides a block C, denoted $B \mid C$ if there is a block T such that $C = BT$.

An Example

Example

Let $G = \mathbb{Z}_4$. Here

$$\mathcal{B}(\mathbb{Z}_4) = \{\overline{0}^{x_0}\overline{1}^{x_1}\overline{2}^{x_2}\overline{3}^{x_3} \mid \text{each } x_i \geq 0 \text{ and } x_1 + 2x_2 + 3x_3 \equiv 0 \pmod 4\}.$$

Notice that the non-prime irreducible blocks of $\mathcal{B}(\mathbb{Z}_4)$ are as follows:

$$\overline{1}^4, \overline{2}^2, \overline{3}^4, \overline{1}^2\overline{2}^1, \overline{1}^1\overline{3}^1, \text{ and } \overline{2}^1\overline{3}^2.$$

In this monoid it is easy to produce factorizations of blocks into irreducible blocks which differ in length. For instance

$$B = (\overline{1}^4)(\overline{3}^4) = (\overline{1}^1\overline{3}^1)^4$$

is a factorization of B into 2 and 4 irreducible blocks respectfully.

An Example

Example

Let $G = \mathbb{Z}_4$. Here

$$\mathcal{B}(\mathbb{Z}_4) = \{\overline{0}^{x_0}\overline{1}^{x_1}\overline{2}^{x_2}\overline{3}^{x_3} \mid \text{each } x_i \geq 0 \text{ and } x_1 + 2x_2 + 3x_3 \equiv 0 \pmod 4\}.$$

Notice that the non-prime irreducible blocks of $\mathcal{B}(\mathbb{Z}_4)$ are as follows:

$$\overline{1}^4, \overline{2}^2, \overline{3}^4, \overline{1}^2\overline{2}^1, \overline{1}^1\overline{3}^1, \text{ and } \overline{2}^1\overline{3}^2.$$

In this monoid it is easy to produce factorizations of blocks into irreducible blocks which differ in length. For instance

$$B = (\overline{1}^4)(\overline{3}^4) = (\overline{1}^1\overline{3}^1)^4$$

is a factorization of B into 2 and 4 irreducible blocks respectfully.

An Example

Example

Let $G = \mathbb{Z}_4$. Here

$$\mathcal{B}(\mathbb{Z}_4) = \{\overline{0}^{x_0}\overline{1}^{x_1}\overline{2}^{x_2}\overline{3}^{x_3} \mid \text{each } x_i \geq 0 \text{ and } x_1 + 2x_2 + 3x_3 \equiv 0 \pmod 4\}.$$

Notice that the non-prime irreducible blocks of $\mathcal{B}(\mathbb{Z}_4)$ are as follows:

$$\overline{1}^4, \overline{2}^2, \overline{3}^4, \overline{1}^2\overline{2}^1, \overline{1}^1\overline{3}^1, \text{ and } \overline{2}^1\overline{3}^2.$$

In this monoid it is easy to produce factorizations of blocks into irreducible blocks which differ in length. For instance

$$B = (\overline{1}^4)(\overline{3}^4) = (\overline{1}^1\overline{3}^1)^4$$

is a factorization of B into 2 and 4 irreducible blocks respectfully.

An Example

Example

Let $G = \mathbb{Z}_4$. Here

$$\mathcal{B}(\mathbb{Z}_4) = \{\overline{0}^{x_0}\overline{1}^{x_1}\overline{2}^{x_2}\overline{3}^{x_3} \mid \text{each } x_i \geq 0 \text{ and } x_1 + 2x_2 + 3x_3 \equiv 0 \pmod 4\}.$$

Notice that the non-prime irreducible blocks of $\mathcal{B}(\mathbb{Z}_4)$ are as follows:

$$\overline{1}^4, \overline{2}^2, \overline{3}^4, \overline{1}^2\overline{2}^1, \overline{1}^1\overline{3}^1, \text{ and } \overline{2}^1\overline{3}^2.$$

In this monoid it is easy to produce factorizations of blocks into irreducible blocks which differ in length. For instance

$$B = (\overline{1}^4)(\overline{3}^4) = (\overline{1}^1\overline{3}^1)^4$$

is a factorization of B into 2 and 4 irreducible blocks respectfully.

Factorial vs. Half-Factorial

Proposition

Let G be an abelian group. The following statements are equivalent.

1. $\mathcal{B}(G)$ *is factorial.*
2. $\mathcal{B}(G)$ *is half-factorial.*
3. $|G| \leq 2$.

Factorial vs. Half-Factorial

Proposition

Let G be an abelian group. The following statements are equivalent.

1. $\mathcal{B}(G)$ *is factorial.*
2. $\mathcal{B}(G)$ *is half-factorial.*
3. $|G| \leq 2$.

A Little Additive Number Theory

Definition

Let G be an abelian group. The *Davenport constant* of G is defined as

$$D(G) = \sup\{\, |B| \mid B \text{ is an irreducible element of } \mathcal{B}(G)\}.$$

No closed formula for the computation of the Davenport constant is known.

Davenport's constant arises in several unexpected areas. Alford, Granville and Pomerance used the bound $D(G) \leq \exp(G)(1 + \log(|G|/\exp(G))$ to prove there are infinitely many Carmichael numbers.

A Little Additive Number Theory

Definition

Let G be an abelian group. The *Davenport constant* of G is defined as

$$D(G) = \sup\{\, |B| \mid B \text{ is an irreducible element of } \mathcal{B}(G)\}.$$

No closed formula for the computation of the Davenport constant is known.

Davenport's constant arises in several unexpected areas. Alford, Granville and Pomerance used the bound $D(G) \leq \exp(G)(1 + \log(|G|/\exp(G))$ to prove there are infinitely many Carmichael numbers.

A Little Additive Number Theory

Definition

Let G be an abelian group. The *Davenport constant* of G is defined as

$$D(G) = \sup\{\, |B| \mid B \text{ is an irreducible element of } \mathcal{B}(G)\}.$$

No closed formula for the computation of the Davenport constant is known.

Davenport's constant arises in several unexpected areas. Alford, Granville and Pomerance used the bound $D(G) \leq \exp(G)(1 + \log(|G|/\exp(G))$ to prove there are infinitely many Carmichael numbers.

A Little Additive Number Theory

If $G = \mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_k}$ is a finite abelian group with $n_i \mid n_{i+1}$ for each $1 \leq i < k$, then set

$$M(G) = \left[\sum_{i+1}^{k}(n_i - 1)\right] + 1.$$

Proposition

Let G be an abelian group.

1. *If $|G| = \infty$, then $D(G) = \infty$.*
2. *If $|G| < \infty$, then $M(G) \leq D(G) \leq |G|$.*

A Little Additive Number Theory

If $G = \mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_k}$ is a finite abelian group with $n_i \mid n_{i+1}$ for each $1 \leq i < k$, then set

$$M(G) = \Big[\sum_{i+1}^{k}(n_i - 1)\Big] + 1.$$

Proposition

Let G be an abelian group.

1. *If $|G| = \infty$, then $D(G) = \infty$.*
2. *If $|G| < \infty$, then $M(G) \leq D(G) \leq |G|$.*

Davenport Facts

It is possible for the upper inequality in Proposition 2 (2) to be strict.
Erdős conjectured in the mid-sixties that $D(G) = M(G)$. It was not until 1969 that this conjecture was disproved.
The group of smallest order that is a counterexample is

$$G_1 = \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_6.$$

If G is of rank less than or equal to 2, then $D(G) = M(G)$.
It is unknown whether there is a counterexample of rank 3, and this, in fact, is an active area of research.

Davenport Facts

It is possible for the upper inequality in Proposition 2 (2) to be strict. Erdős conjectured in the mid-sixties that $D(G) = M(G)$. It was not until 1969 that this conjecture was disproved.

The group of smallest order that is a counterexample is

$$G_1 = \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_6.$$

If G is of rank less than or equal to 2, then $D(G) = M(G)$.
It is unknown whether there is a counterexample of rank 3, and this, in fact, is an active area of research.

Davenport Facts

It is possible for the upper inequality in Proposition 2 (2) to be strict. Erdős conjectured in the mid-sixties that $D(G) = M(G)$. It was not until 1969 that this conjecture was disproved.
The group of smallest order that is a counterexample is

$$G_1 = \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_6.$$

If G is of rank less than or equal to 2, then $D(G) = M(G)$.
It is unknown whether there is a counterexample of rank 3, and this, in fact, is an active area of research.

Davenport Facts

It is possible for the upper inequality in Proposition 2 (2) to be strict. Erdős conjectured in the mid-sixties that $D(G) = M(G)$. It was not until 1969 that this conjecture was disproved.
The group of smallest order that is a counterexample is

$$G_1 = \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_6.$$

If G is of rank less than or equal to 2, then $D(G) = M(G)$.
It is unknown whether there is a counterexample of rank 3, and this, in fact, is an active area of research.

Davenport Facts

It is possible for the upper inequality in Proposition 2 (2) to be strict. Erdős conjectured in the mid-sixties that $D(G) = M(G)$. It was not until 1969 that this conjecture was disproved.
The group of smallest order that is a counterexample is

$$G_1 = \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_6.$$

If G is of rank less than or equal to 2, then $D(G) = M(G)$.
It is unknown whether there is a counterexample of rank 3, and this, in fact, is an active area of research.

On Elasticity

Proposition

If G is a finite abelian group, then $\rho(D) = \frac{D(G)}{2}$. Moreover, the elasticity is accepted.

REU Theorem (Chapman-Holden-Moore, 2006, Rocky Mountain Journal)

Let G be a finite abelian group. If $D(G) = M(G)$ then $\mathcal{B}(G)^*$ is fully elastic.

On Elasticity

Proposition

If G is a finite abelian group, then $\rho(D) = \frac{D(G)}{2}$. Moreover, the elasticity is accepted.

REU Theorem (Chapman-Holden-Moore, 2006, Rocky Mountain Journal)

Let G be a finite abelian group. If $D(G) = M(G)$ then $\mathcal{B}(G)^*$ is fully elastic.

How To Compute Elasticities of Rings of Algebraic Integers

Geroldinger's Theorem (Simple Form)

Let R be an algebraic ring of intgers with divisor class group $G = \mathcal{C}(R)$, R^* the multiplicative monoid of R. There is a monoid homomorphism

$$\varphi : R^* \to \mathcal{B}(G)$$

that is surjective and preserves lengths of factorizations into irreducibles (i.e., $\mathcal{L}(x) = \mathcal{L}(\varphi(x))$ for each $x \in R^*$). Hence

$$\mathcal{L}(R) = \mathcal{L}(\mathcal{B}(G)).$$

Corollary

$$\rho(R) = \frac{D(G)}{2}.$$

How To Compute Elasticities of Rings of Algebraic Integers

Geroldinger's Theorem (Simple Form)

Let R be an algebraic ring of intgers with divisor class group $G = \mathcal{C}(R)$, R^* the multiplicative monoid of R. There is a monoid homomorphism

$$\varphi : R^* \to \mathcal{B}(G)$$

that is surjective and preserves lengths of factorizations into irreducibles (i.e., $\mathcal{L}(x) = \mathcal{L}(\varphi(x))$ for each $x \in R^*$). Hence

$$\mathcal{L}(R) = \mathcal{L}(\mathcal{B}(G)).$$

Corollary

$$\rho(R) = \frac{D(G)}{2}.$$

On Delta Sets

Proposition

For $n \geq 3$, $\Delta(\mathcal{B}(\mathbb{Z}_n)) = \{1, 2, \ldots, n-2\}$.

REU Theorem (Chapman-Gotti-Pelayo, 2014, Colloquium Mathematicum)

Let $n \geq 3$. If $n-2 \in \Delta(B)$ for $B \in \mathcal{B}(Z_n)$, then $\Delta(B) = \{n-2\}$.

On Delta Sets

Proposition

For $n \geq 3$, $\Delta(\mathcal{B}(\mathbb{Z}_n)) = \{1, 2, \ldots, n-2\}$.

REU Theorem (Chapman-Gotti-Pelayo, 2014, Colloquium Mathematicum)

Let $n \geq 3$. If $n-2 \in \Delta(B)$ for $B \in \mathcal{B}(Z_n)$, then $\Delta(B) = \{n-2\}$.

Numerical Monoids

Let S be an additive submonoid of $\mathbb{N} \cup \{0\}$. S is called a *numerical monoid*.

If $\{n_1, \ldots, n_t\}$ is a set of elements of S such that every $x \in S$ can be written in the form

$$x = x_1 n_1 + \cdots x_t n_t$$

then $\{n_1, \ldots, n_t\}$ is called a *generating set of* S.

This is commonly denoted by

$$S = \langle n_1, \ldots, n_t \rangle.$$

It follows from Elementary Number Theory that every numerical monoid S possesses a unique minimal set of generators. If $\gcd\{ s \mid s \in S\} = 1$, then S is called *primitive*. It again follows easily from Number Theory that every numerical monoid S is isomorphic to a primitive numerical monoid.

Numerical Monoids

Let S be an additive submonoid of $\mathbb{N} \cup \{0\}$. S is called a *numerical monoid*.

If $\{n_1, \ldots, n_t\}$ is a set of elements of S such that every $x \in S$ can be written in the form

$$x = x_1 n_1 + \cdots x_t n_t$$

then $\{n_1, \ldots, n_t\}$ is called a *generating set of* S.

This is commonly denoted by

$$S = \langle n_1, \ldots, n_t \rangle.$$

It follows from Elementary Number Theory that every numerical monoid S possesses a unique minimal set of generators. If $\gcd\{ s \mid s \in S\} = 1$, then S is called *primitive*. It again follows easily from Number Theory that every numerical monoid S is isomorphic to a primitive numerical monoid.

Numerical Monoids

Let S be an additive submonoid of $\mathbb{N} \cup \{0\}$. S is called a *numerical monoid*.

If $\{n_1, \ldots, n_t\}$ is a set of elements of S such that every $x \in S$ can be written in the form

$$x = x_1 n_1 + \cdots x_t n_t$$

then $\{n_1, \ldots, n_t\}$ is called a *generating set of* S.

This is commonly denoted by

$$S = \langle n_1, \ldots, n_t \rangle.$$

It follows from Elementary Number Theory that every numerical monoid S possesses a unique minimal set of generators. If $\gcd\{ s \mid s \in S\} = 1$, then S is called *primitive*. It again follows easily from Number Theory that every numerical monoid S is isomorphic to a primitive numerical monoid.

Numerical Monoids

Let S be an additive submonoid of $\mathbb{N} \cup \{0\}$. S is called a *numerical monoid*.

If $\{n_1, \ldots, n_t\}$ is a set of elements of S such that every $x \in S$ can be written in the form

$$x = x_1 n_1 + \cdots x_t n_t$$

then $\{n_1, \ldots, n_t\}$ is called a *generating set of* S.

This is commonly denoted by

$$S = \langle n_1, \ldots, n_t \rangle.$$

It follows from Elementary Number Theory that every numerical monoid S possesses a unique minimal set of generators. If $\gcd\{ s \mid s \in S\} = 1$, then S is called *primitive*. It again follows easily from Number Theory that every numerical monoid S is isomorphic to a primitive numerical monoid.

The Frobenius Number

If $S = \langle n_1, \ldots, n_t \rangle$ then the largest positive integer not in S is called the Frobenius number of S, which we denote $F(S)$.

If $S = \langle a, b \rangle$, then $F(S) = ab - a - b$.

For more than two generators, there is no known closed form for $F(S)$.

The Frobenius Number

If $S = \langle n_1, \ldots, n_t \rangle$ then the largest positive integer not in S is called the Frobenius number of S, which we denote $F(S)$.

If $S = \langle a, b \rangle$, then $F(S) = ab - a - b$.

For more than two generators, there is no known closed form for $F(S)$.

The Frobenius Number

If $S = \langle n_1, \ldots, n_t \rangle$ then the largest positive integer not in S is called the Frobenius number of S, which we denote $F(S)$.

If $S = \langle a, b \rangle$, then $F(S) = ab - a - b$.

For more than two generators, there is no known closed form for $F(S)$.

What is known?

Much is known about the factorization properties of numerical monoids.

REU Theorem (Chapman-Holden-Moore, 2006, Rocky Mountain Journal)

Let $S = \langle n_1, \ldots, n_k \rangle$

1. $\rho(S) = \frac{n_k}{n_1}$.
2. *If $k \geq 2$, then S is not fully elastic.*

REU Theorem (Bowles-Chapman-Kaplan-Reiser, 2006, JAA)

1. *If $S = \langle n, n+d, n+2d, ..., n+kd \rangle$, then $\Delta(S) = \{d\}$.*
2. *If $k \geq 1$ and $d \geq 1$ are positive integers, then there is a numerical monoid S with $\Delta(S) = \{d, 2d, \ldots, kd\}$.*
3. *If $S = \langle n, n+1, n^2 - n - 1 \rangle$, then $\Delta(S) = \{1, 2, \ldots, n-2, 2n-5\}$*

What is known?

Much is known about the factorization properties of numerical monoids.

REU Theorem (Chapman-Holden-Moore, 2006, Rocky Mountain Journal)

Let $S = \langle n_1, \ldots, n_k \rangle$

1. $\rho(S) = \frac{n_k}{n_1}$.
2. *If* $k \geq 2$, *then* S *is not fully elastic.*

REU Theorem (Bowles-Chapman-Kaplan-Reiser, 2006, JAA)

1. *If* $S = \langle n, n+d, n+2d, ..., n+kd \rangle$, *then* $\Delta(S) = \{d\}$.
2. *If* $k \geq 1$ *and* $d \geq 1$ *are positive integers, then there is a numerical monoid* S *with* $\Delta(S) = \{d, 2d, \ldots, kd\}$.
3. *If* $S = \langle n, n+1, n^2 - n - 1 \rangle$, *then* $\Delta(S) = \{1, 2, \ldots, n-2, 2n-5\}$

What is known?

Much is known about the factorization properties of numerical monoids.

REU Theorem (Chapman-Holden-Moore, 2006, Rocky Mountain Journal)

Let $S = \langle n_1, \ldots, n_k \rangle$

1. $\rho(S) = \frac{n_k}{n_1}$.
2. *If* $k \geq 2$, *then* S *is not fully elastic.*

REU Theorem (Bowles-Chapman-Kaplan-Reiser, 2006, JAA)

1. *If* $S = \langle n, n+d, n+2d, ..., n+kd \rangle$, *then* $\Delta(S) = \{d\}$.
2. *If* $k \geq 1$ *and* $d \geq 1$ *are positive integers, then there is a numerical monoid* S *with* $\Delta(S) = \{d, 2d, \ldots, kd\}$.
3. *If* $S = \langle n, n+1, n^2 - n - 1 \rangle$, *then* $\Delta(S) = \{1, 2, \ldots, n-2, 2n-5\}$

More of What is known?

REU Theorem (Chapman-Hoyer-Kaplan, 2009, Aequationes Mathematicae)

If $S = \langle n_1, \ldots, n_k \rangle$ is a primitive numerical monoid, with $n_1 < n_2 < \cdots < n_k$, then for all $x \geq 2kn_2n_k^2$ we have $\Delta(x) = \Delta(x + n_1n_k)$. In other words, the sequence $\{\Delta(x)\}_{x \in S}$ is eventually periodic.

Do Sets of Lengths Characterize Numerical Monoids

Conjecture

If G and G' are finite abelian groups with $|\ G\ | > 3$ and $|\ G'\ | > 3$, then $\mathcal{L}(\mathcal{B}(G)) = \mathcal{L}(\mathcal{B}(G'))$ implies $G \cong G'$.

Numerical Monoids have much different behavior. Let

$$S = \langle a, a+d, \ldots, a+kd \rangle \text{ and } S' = \langle a', a'+d', \ldots, a'+k'd' \rangle$$

be numerical monoids with $\gcd(a, d) = \gcd(a', d') = 1$, $1 \leq k < a$, and $1 \leq k' < a'$.

REU Theorem (Amos-Chapman-Hine-Paixao, 2007, Integers)

$\mathcal{L}(S) = \mathcal{L}(S')$ if and only if $d = d'$. $\frac{a}{k} = \frac{a'}{d'}$, and $\gcd(a, k) \geq 2$, $\gcd(a', k') \geq 2$.

Do Sets of Lengths Characterize Numerical Monoids

Conjecture

If G and G' are finite abelian groups with $|\ G\ | > 3$ and $|\ G'\ | > 3$, then $\mathcal{L}(\mathcal{B}(G)) = \mathcal{L}(\mathcal{B}(G'))$ implies $G \cong G'$.

Numerical Monoids have much different behavior. Let

$$S = \langle a, a+d, \ldots, a+kd \rangle \text{ and } S' = \langle a', a'+d', \ldots, a'+k'd' \rangle$$

be numerical monoids with $\gcd(a, d) = \gcd(a', d') = 1$, $1 \leq k < a$, and $1 \leq k' < a'$.

REU Theorem (Amos-Chapman-Hine-Paixao, 2007, Integers)

$\mathcal{L}(S) = \mathcal{L}(S')$ if and only if $d = d'$. $\frac{a}{k} = \frac{a'}{d'}$, and $\gcd(a, k) \geq 2$, $\gcd(a', k') \geq 2$.

Do Sets of Lengths Characterize Numerical Monoids

Conjecture

If G and G' are finite abelian groups with $|\ G\ | > 3$ and $|\ G'\ | > 3$, then $\mathcal{L}(\mathcal{B}(G)) = \mathcal{L}(\mathcal{B}(G'))$ implies $G \cong G'$.

Numerical Monoids have much different behavior. Let

$$S = \langle a, a+d, \ldots, a+kd \rangle \text{ and } S' = \langle a', a'+d', \ldots, a'+k'd' \rangle$$

be numerical monoids with $\gcd(a, d) = \gcd(a', d') = 1$, $1 \leq k < a$, and $1 \leq k' < a'$.

REU Theorem (Amos-Chapman-Hine-Paixao, 2007, Integers)

$\mathcal{L}(S) = \mathcal{L}(S')$ if and only if $d = d'$. $\frac{a}{k} = \frac{a'}{d'}$, and $\gcd(a, k) \geq 2$, $\gcd(a', k') \geq 2$.

Congruence Monoids

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).

Theorem (James & Niven, 1954 PAMS)

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

Congruence Monoids

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).

Theorem (James & Niven, 1954 PAMS)

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

The Other Extreme

REU Theorem (Bannister-Chaika-Chapman-Myerson, 2007, Elemente der Mathematik)

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

If $\Gamma = \{\overline{x}\}$ (i.e., $\mathbb{Z}_\Gamma$ is an arithmetic sequence that is multiplicatively closed), then $\mathbb{Z}_\Gamma$ is called an *arithmetic congruence monoid* or *ACM*.

The Other Extreme

REU Theorem (Bannister-Chaika-Chapman-Myerson, 2007, Elemente der Mathematik)

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

If $\Gamma = \{\overline{x}\}$ (i.e., $\mathbb{Z}_\Gamma$ is an arithmetic sequence that is multiplicatively closed), then $\mathbb{Z}_\Gamma$ is called an *arithmetic congruence monoid* or *ACM*.

Examples

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*

Examples

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.

A Theorem

REU Theorem (Bannister-Chaika-Chapman-Myerson, 2007, Colloquium Mathematicum)

1. $\rho(M_{1,b}) = \frac{D(\mathbb{Z}_n^\times)}{2}$.
2. *If $M_{a,b}$ is global, then $\rho(M_{a,b}) = \infty$.*
3. *If $M_{a,b}$ is local, then $\rho(M_{a,b}) = \frac{n+k-1}{k}$ where n is the smallest integer such that $p^n \in M_{a,b}$.*

A Theorem

REU Theorem (Bannister-Chaika-Chapman-Myerson, 2007, Colloquium Mathematicum)

1. $\rho(M_{1,b}) = \frac{D(\mathbb{Z}_n^\times)}{2}$.
2. *If* $M_{a,b}$ *is global, then* $\rho(M_{a,b}) = \infty$.
3. *If* $M_{a,b}$ *is local, then* $\rho(M_{a,b}) = \frac{n+k-1}{k}$ *where* n *is the smallest integer such that* $p^n \in M_{a,b}$.

A Theorem

REU Theorem (Bannister-Chaika-Chapman-Myerson, 2007, Colloquium Mathematicum)

1. $\rho(M_{1,b}) = \frac{D(\mathbb{Z}_n^\times)}{2}$.
2. *If* $M_{a,b}$ *is global, then* $\rho(M_{a,b}) = \infty$.
3. *If* $M_{a,b}$ *is local, then* $\rho(M_{a,b}) = \frac{n+k-1}{k}$ *where* n *is the smallest integer such that* $p^n \in M_{a,b}$.

Another Theorem

REU Theorem (Baginski-Chapman-Schaeffer, 2008, J. Théorie Nombres Bordeaux)

Suppose $M_{a,b}$ is a local ACM with $\gcd(a,b) = p^\alpha$ and β the smallest integer with $p^\beta \in M_{a,b}$.

1. *If $\alpha = \beta = 1$, then $\Delta(M_{a,b}) = \emptyset$.*
2. *If $\alpha = \beta > 1$, then $\Delta(M_{a,b}) = \{1\}$.*
3. *If $\alpha < \beta$, then $\Delta(M_{a,b}) = [1, \beta/\alpha)$.*

Another Theorem

REU Theorem (Baginski-Chapman-Schaeffer, 2008, J. Théorie Nombres Bordeaux)

Suppose $M_{a,b}$ is a local ACM with $\gcd(a,b) = p^\alpha$ and β the smallest integer with $p^\beta \in M_{a,b}$.

1. *If $\alpha = \beta = 1$, then $\Delta(M_{a,b}) = \emptyset$.*
2. *If $\alpha = \beta > 1$, then $\Delta(M_{a,b}) = \{1\}$.*
3. *If $\alpha < \beta$, then $\Delta(M_{a,b}) = [1, \beta/\alpha)$.*

Another Theorem

REU Theorem (Baginski-Chapman-Schaeffer, 2008, J. Théorie Nombres Bordeaux)

Suppose $M_{a,b}$ is a local ACM with $\gcd(a,b) = p^\alpha$ and β the smallest integer with $p^\beta \in M_{a,b}$.

1. *If $\alpha = \beta = 1$, then $\Delta(M_{a,b}) = \emptyset$.*
2. *If $\alpha = \beta > 1$, then $\Delta(M_{a,b}) = \{1\}$.*
3. *If $\alpha < \beta$, then $\Delta(M_{a,b}) = [1, \beta/\alpha)$.*

Integer-Valued Polynomials

Set

$$\mathrm{Int}(\mathbb{Z}) = \{f(x) \in \mathbb{Q}[x] \mid f(z) \in \mathbb{Z} \forall\, z \in \mathbb{Z}\}.$$

$\mathrm{Int}(\mathbb{Z})$ is the celebrated "ring of polynomials integer-valued over $\mathbb{Z}$."

$\mathrm{Int}(\mathbb{Z})$ is a $\mathbb{Z}$-module with free basis $\binom{x}{0} = 1$ and for $n \geq 1$,

$$\binom{x}{n} = \frac{x(x-1)\cdots(x-n+1)}{n!}.$$

Integer-Valued Polynomials

Set

$$\mathrm{Int}(\mathbb{Z}) = \{f(x) \in \mathbb{Q}[x] \mid f(z) \in \mathbb{Z} \forall\, z \in \mathbb{Z}\}.$$

$\mathrm{Int}(\mathbb{Z})$ is the celebrated "ring of polynomials integer-valued over $\mathbb{Z}$."

$\mathrm{Int}(\mathbb{Z})$ is a $\mathbb{Z}$-module with free basis $\binom{x}{0} = 1$ and for $n \geq 1$,

$$\binom{x}{n} = \frac{x(x-1)\cdots(x-n+1)}{n!}.$$

Integer-Valued Polynomials

Set

$$\mathrm{Int}(\mathbb{Z}) = \{f(x) \in \mathbb{Q}[x] \mid f(z) \in \mathbb{Z} \forall\, z \in \mathbb{Z}\}.$$

$\mathrm{Int}(\mathbb{Z})$ is the celebrated "ring of polynomials integer-valued over $\mathbb{Z}$."

$\mathrm{Int}(\mathbb{Z})$ is a $\mathbb{Z}$-module with free basis $\binom{x}{0} = 1$ and for $n \geq 1$,

$$\binom{x}{n} = \frac{x(x-1)\cdots(x-n+1)}{n!}.$$

A Basic Lemma

Lemma

For $n \geq 1$, the polynomial $\binom{x}{n}$ is irreducible in $\mathrm{Int}(\mathbb{Z})$.

Corollary

$\rho(\mathrm{Int}(\mathbb{Z})) = \infty$.

Proof.

$$n \cdot \binom{x}{n} = \binom{x}{n-1}(x - n + 1).$$

□

A Basic Lemma

Lemma

For $n \geq 1$, the polynomial $\binom{x}{n}$ is irreducible in $\mathrm{Int}(\mathbb{Z})$.

Corollary

$\rho(\mathrm{Int}(\mathbb{Z})) = \infty$.

Proof.

$$n \cdot \binom{x}{n} = \binom{x}{n-1}(x - n + 1).$$

□

Full Elasticity

REU Theorem (Chapman-McClain, 2005, Journal of Algebra)

Let $q \geq 1$ be a rational number. Then there is a polynomial $f(x) \in \mathrm{Int}(\mathbb{Z})$ with

$$\rho(f(x)) = q.$$

Hence, $\mathrm{Int}(\mathbb{Z})$ is fully elastic.

REU Theorem (Chapman-McClain, 2005, Journal of Algebra)

Let t be a non-zero rational. t is the leading coefficient of infinitely many irreducible polynomials in $\mathrm{Int}(\mathbb{Z})$.

Full Elasticity

REU Theorem (Chapman-McClain, 2005, Journal of Algebra)

Let $q \geq 1$ be a rational number. Then there is a polynomial $f(x) \in \mathrm{Int}(\mathbb{Z})$ with

$$\rho(f(x)) = q.$$

Hence, $\mathrm{Int}(\mathbb{Z})$ is fully elastic.

REU Theorem (Chapman-McClain, 2005, Journal of Algebra)

Let t be a non-zero rational. t is the leading coefficient of infinitely many irreducible polynomials in $\mathrm{Int}(\mathbb{Z})$.