

A Case Study in Factorization Theory: Arithmetical Congruence Monoids

Paul Baginski

University of California, Berkeley

The Art of Factorization in Multiplicative Structures
Trinity University, San Antonio, Texas
22 May 2007

Arithmetic Sequences

Consider an arithmetic sequence:

$$a, a + b, a + 2b, a + 3b, \dots = \{x \in \mathbb{N} \mid x \equiv a \pmod{b}\}$$

When is it multiplicatively closed? (semigroup)

Arithmetic Sequences

Consider an arithmetic sequence:

$$a, a + b, a + 2b, a + 3b, \dots = \{x \in \mathbb{N} \mid x \equiv a \pmod{b}\}$$

When is it multiplicatively closed? (semigroup)

Example

When $a = 1$ then $(1 + rb)(1 + sb) \equiv 1 \pmod{b}$, so $\{x \in \mathbb{N} \mid x \equiv 1 \pmod{b}\}$ is multiplicatively closed.

Arithmetic Sequences

Consider an arithmetic sequence:

$$a, a + b, a + 2b, a + 3b, \dots = \{x \in \mathbb{N} \mid x \equiv a \pmod{b}\}$$

When is it multiplicatively closed? (semigroup)

Example

When $a = 1$ then $(1 + rb)(1 + sb) \equiv 1 \pmod{b}$, so $\{x \in \mathbb{N} \mid x \equiv 1 \pmod{b}\}$ is multiplicatively closed.

Generally we need

$$\begin{aligned}(a + rb)(a + sb) &\equiv a \pmod{b} \\ a^2 &\equiv a \pmod{b}\end{aligned}$$

Arithmetical Congruence Monoids

Definition

If $0 < a \leq b$ and $a^2 \equiv a \pmod{b}$, then

$$M_{a,b} := \{x \in \mathbb{N} \mid x \equiv a \pmod{b}\} \cup \{1\}$$

is a multiplicative monoid known as an *arithmetical congruence monoid*.

Historically, $M_{1,4}$ was known as the Hilbert monoid.

The case where $a = 1$ is very special.

Non-unique Factorization

In $M_{1,4}$ we have $441 = 21 \cdot 21 = 9 \cdot 49$. This is a half-factorial monoid.

Non-unique Factorization

In $M_{1,4}$ we have $441 = 21 \cdot 21 = 9 \cdot 49$. This is a half-factorial monoid.

In $M_{4,6}$, we have $1000 = 10^3 = 4 \cdot 250$. Not even half-factorial.

Membership Criterion

Let $d = \gcd(a, b)$ and $m = b/d$. Then:

① $d = 1$ iff $a = 1$

Membership Criterion

Let $d = \gcd(a, b)$ and $m = b/d$. Then:

- 1 $d = 1$ iff $a = 1$
- 2 $\gcd(a, m) = \gcd(d, m) = 1$

Membership Criterion

Let $d = \gcd(a, b)$ and $m = b/d$. Then:

- 1 $d = 1$ iff $a = 1$
- 2 $\gcd(a, m) = \gcd(d, m) = 1$
- 3 $M_{a,b} = d\mathbb{N} \cap M_{1,m} \cup \{1\}$

Prime Elements

$x \in M_{a,b}$ is *prime* iff whenever $x|yz$, then $x|y$ or $x|z$.

Prime Elements

$x \in M_{a,b}$ is *prime* iff whenever $x|yz$, then $x|y$ or $x|z$.

In $M_{1,b}$, any prime number $p \equiv 1 \pmod{b}$ is a prime element of $M_{1,b}$. There are infinitely many such prime numbers by Dirichlet's Theorem.

Prime Elements

$x \in M_{a,b}$ is *prime* iff whenever $x|yz$, then $x|y$ or $x|z$.

In $M_{1,b}$, any prime number $p \equiv 1 \pmod{b}$ is a prime element of $M_{1,b}$. There are infinitely many such prime numbers by Dirichlet's Theorem.

If $a \neq 1$, then $M_{a,b}$ has no prime elements.

If $a \neq 1$, then $M_{a,b}$ has no prime elements.

Proof: Suppose $x \in M$ prime. Then $x = d^k p_1^{e_1} \dots p_r^{e_r}$ in \mathbb{N} and $x \equiv 1 \pmod{m}$. Therefore $\gcd(p_i, m) = 1$. Since $\gcd(d, m) = 1$, there exists $\alpha \geq 1$ such that $d^\alpha \equiv 1 \pmod{m}$.

If $a \neq 1$, then $M_{a,b}$ has no prime elements.

Proof: Suppose $x \in M$ prime. Then $x = d^k p_1^{e_1} \dots p_r^{e_r}$ in \mathbb{N} and $x \equiv 1 \pmod{m}$. Therefore $\gcd(p_i, m) = 1$. Since $\gcd(d, m) = 1$, there exists $\alpha \geq 1$ such that $d^\alpha \equiv 1 \pmod{m}$.

Case 1: $r = 0$, so $x = d^k$. Then k is the order of d modulo m . Pick a prime q such that $q \equiv d^{-1} \pmod{m}$ and $\gcd(q, d) = 1$. Then $x | x(dq)^{k+1} = (dq)^{k+1}$.

If $a \neq 1$, then $M_{a,b}$ has no prime elements.

Proof: Suppose $x \in M$ prime. Then $x = d^k p_1^{e_1} \dots p_r^{e_r}$ in \mathbb{N} and $x \equiv 1 \pmod{m}$. Therefore $\gcd(p_i, m) = 1$. Since $\gcd(d, m) = 1$, there exists $\alpha \geq 1$ such that $d^\alpha \equiv 1 \pmod{m}$.

Case 1: $r = 0$, so $x = d^k$. Then k is the order of d modulo m . Pick a prime q such that $q \equiv d^{-1} \pmod{m}$ and $\gcd(q, d) = 1$. Then $x | x(dq^{k+1}) = (dq)^{k+1}$.

Case 2: $r \geq 1$. Then $1 \leq k \leq \alpha$, otherwise x reducible. Pick a new prime q such that $q \equiv 1 \pmod{m}$ and $\gcd(q, d) = 1$. Then $x | x(qd^\alpha) = (d^\alpha)(dq p_1^{e_1} \dots p_r^{e_r})$.

Irreducibles

All nontrivial $M_{a,b}$ have infinitely many (non-prime) irreducibles, by Dirichlet's theorem.

Irreducibles

All nontrivial $M_{a,b}$ have infinitely many (non-prime) irreducibles, by Dirichlet's theorem.

Consider

$$\gamma(M_{a,b}) = \limsup_{n \rightarrow \infty} \frac{|\mathcal{A}(M_{a,b}) \cap [1, n]|}{|M_{a,b} \cap [1, n]|}$$

Irreducibles

All nontrivial $M_{a,b}$ have infinitely many (non-prime) irreducibles, by Dirichlet's theorem.

Consider

$$\gamma(M_{a,b}) = \limsup_{n \rightarrow \infty} \frac{|\mathcal{A}(M_{a,b}) \cap [1, n]|}{|M_{a,b} \cap [1, n]|}$$

For $M_{1,b}$, this is at worst the prime density modulo b , and should be a fairly small number.

Irreducibles

All nontrivial $M_{a,b}$ have infinitely many (non-prime) irreducibles, by Dirichlet's theorem.

Consider

$$\gamma(M_{a,b}) = \limsup_{n \rightarrow \infty} \frac{|\mathcal{A}(M_{a,b}) \cap [1, n]|}{|M_{a,b} \cap [1, n]|}$$

For $M_{1,b}$, this is at worst the prime density modulo b , and should be a fairly small number.

For $M_{a,b}$, we can show that if x is reducible, then $x + b$ is irreducible. So $\gamma(M_{a,b}) \geq \frac{1}{2}$.

Can construct $M_{a,b}$ such that $\gamma(M_{a,b}) = \frac{p-1}{p}$ for any odd prime p .

Transfer Homomorphisms

Definition

A monoid homomorphism $\phi : M \rightarrow N$ is a *transfer homomorphism* if 1) every element of N is associate to an element of $\phi(M)$, and 2) whenever $\phi(x) = ab$ then there are $y, z \in M$ such that $yz = x$ and $\phi(y)$ is associate to a and $\phi(z)$ is associate to b .

Transfer Homomorphisms

Definition

A monoid homomorphism $\phi : M \rightarrow N$ is a *transfer homomorphism* if 1) every element of N is associate to an element of $\phi(M)$, and 2) whenever $\phi(x) = ab$ then there are $y, z \in M$ such that $yz = x$ and $\phi(y)$ is associate to a and $\phi(z)$ is associate to b .

There is a transfer homomorphism $\phi : M_{1,b} \rightarrow \mathcal{B}(\mathbb{Z}_b^*)$.
[Halter-Koch]

Elasticity definitions

The *elasticity* of x is $\rho(x) = \frac{\max \mathcal{L}(x)}{\min \mathcal{L}(x)}$. The *elasticity* of M is $\rho(M) = \sup_{x \in M} \rho(x)$.

M has *accepted elasticity* if there is $x \in M$ with $\rho(x) = \rho(M)$.

M has *full elasticity* if for every $q \in \mathbb{Q} \cap [1, \rho(M))$ there is an $x \in M$ with $\rho(x) = q$.

Hilbert Case

$$\rho(M_{1,b}) = \frac{D(\mathbb{Z}_b^*)}{2}$$

This elasticity is accepted.

Fully elastic for most b where $D(\mathbb{Z}_b^*)$ is known. For other b , unknown whether fully elastic. [Chapman, Holden, Moore 2006]

non-Hilbert case

Theorem (Banister, Chaika, Chapman, Meyerson 2007)

If $d = p^\alpha$, then $\rho(M_{a,b}) = \frac{\beta + \alpha - 1}{\alpha}$, where $\beta \geq \alpha$ is the least integer such that $p^\beta \in M_{a,b}$.

non-Hilbert case

Theorem (Banister, Chaika, Chapman, Meyerson 2007)

If $d = p^\alpha$, then $\rho(M_{a,b}) = \frac{\beta + \alpha - 1}{\alpha}$, where $\beta \geq \alpha$ is the least integer such that $p^\beta \in M_{a,b}$.

If d is not a prime power, then $\rho(M_{a,b}) = \infty$.

Accepted Elasticity

Banister, Chaika, Chapman, Meyerson give examples of accepted and non-accepted elasticity.

Example

$M_{4,6}$ has elasticity $\frac{2-1+1}{1} = 2$, but its elasticity is not accepted.

Full Elasticity

Theorem

If $\rho(M_{a,b}) = \infty$, then $M_{a,b}$ not fully elastic.

If $\rho(M_{a,b})$ finite, examples of full elasticity and non-full elasticity.

Half-factorial

Theorem

$M_{a,b}$ is half-factorial iff:

- 1 $a = 1$ and $b = 1, 2, 3, 4,$ or $6,$ or
- 2 $a = p$ prime and $a|b$

Krull Monoid

Definition

M is a *Krull monoid* if there exists a free abelian monoid D and a homomorphism $\delta : M \rightarrow D$ such that:

- 1 $x|y$ in M if $\delta(x)|\delta(y)$ in D , and
- 2 every $\beta \in D$ is the gcd of some finite set of elements in $\delta(M)$.

In this case, $D/\delta(M)$ forms a group, known as the *class group* of M .

Krull for Hilbert Monoids

$M_{1,b}$ embeds into $\mathcal{F}(p \in \mathbb{P} \mid \gcd(p, b) = 1)$ in the required way, so $M_{1,b}$ is Krull.

Krull for Hilbert Monoids

$M_{1,b}$ embeds into $\mathcal{F}(\mathfrak{p} \in \mathbb{P} \mid \gcd(\mathfrak{p}, b) = 1)$ in the required way, so $M_{1,b}$ is Krull.

The class group is \mathbb{Z}_b^* .

Krull for non-Hilbert Monoids

Recall: $M_{a,b} = d\mathbb{N} \cap M_{1,m} \cup \{1\}$.

Krull for non-Hilbert Monoids

Recall: $M_{a,b} = d\mathbb{N} \cap M_{1,m} \cup \{1\}$.

Intuitively: the set of all gcds of $M_{a,b}$ is $d\mathcal{F}(p \in \mathbb{P} \mid \gcd(p, m) = 1)$. But this is not free, so $M_{a,b}$ is not Krull.

Delta Sets

If $\mathcal{L}(x) = \{t_1, \dots, t_k\}$ then $\Delta(x) = \{t_{i+1} - t_i \mid i < k\}$.

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

Delta Sets for $M_{1,b}$

$\Delta(M_{1,b})$ are just Delta sets of block monoids, which have only been computed in a small number of cases.

Proposition

If $M_{1,b}$ is not half-factorial, then $\min \Delta(M_{1,b}) = 1$.

Delta Sets for d prime power

If $d = p^\alpha$ is a prime power, set $\beta \geq \alpha$ the least integer such that $d \in M_{a,b}$.

Theorem (Baginski, Chapman, Schaeffer 2006)

- 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 $\Delta(M_{a,b}) = [1, \frac{\beta}{\alpha})$

Delta Sets for d non-prime power.

If d is not a prime power, then we know $\Delta(M_{a,b})$ is finite, with minimum value 1 and a bound on its maximum value. Several cases have been determined entirely.

Table of Properties

	$M_{1,b}$	$M_{a,b}$ $d = p^\alpha$ / d not prime power
Primes	∞	none
Irreducibles	scarce	dense
$\rho(M)$	$\frac{D(G)}{2}$	finite / infinite
accepted ρ	yes	sometimes / never
fully elastic	sometimes	sometimes / never
Krull monoid	yes	no
Class group	\mathbb{Z}_b^*	0
$\Delta(M)$	sometimes known	known / unknown
Catenary Degree	?	known / unknown