On the periodicity of irreducible elements in arithmetical congruence monoids

Christopher O'Neill

University of California Davis

coneill@math.ucdavis.edu

Joint with Jacob Hartzer (undergraduate)

Jan 6, 2017

Arithmetical congruence monoids (ACMs)

Definition

An *arithmetical congruence monoid* is a **multiplicative** set

$$M_{a,b} = \{a, a+b, a+2b, a+3b, \ldots\} \subset (\mathbb{Z}_{\geq 1}, \cdot)$$

for $0 < a < b$ with $a^2 \equiv a \bmod b$.

Arithmetical congruence monoids (ACMs)

Definition

An *arithmetical congruence monoid* is a **multiplicative** set

$$M_{a,b} = \{a, a+b, a+2b, a+3b, \ldots\} \subset (\mathbb{Z}_{\geq 1}, \cdot)$$

for $0 < a < b$ with $a^2 \equiv a \bmod b$.

Example

The *Hilbert monoid* $M_{1,4} = \{1, 5, 9, 13, 17, 21, 25, 29, 33, \ldots\}$.

Arithmetical congruence monoids (ACMs)

Definition

An *arithmetical congruence monoid* is a **multiplicative** set

$$M_{a,b} = \{a, a+b, a+2b, a+3b, \ldots\} \subset (\mathbb{Z}_{\geq 1}, \cdot)$$

for $0 < a < b$ with $a^2 \equiv a \bmod b$.

Example

The *Hilbert monoid* $M_{1,4} = \{1, 5, 9, 13, 17, 21, 25, 29, 33, \ldots\}$.

- $65 = 5 \cdot 13$

Arithmetical congruence monoids (ACMs)

Definition

An *arithmetical congruence monoid* is a **multiplicative** set

$$M_{a,b} = \{a, a+b, a+2b, a+3b, \ldots\} \subset (\mathbb{Z}_{\geq 1}, \cdot)$$

for $0 < a < b$ with $a^2 \equiv a \bmod b$.

Example

The *Hilbert monoid* $M_{1,4} = \{1, 5, 9, 13, 17, 21, 25, 29, 33, \ldots\}$.

- $65 = 5 \cdot 13$ (prime in $\mathbb{Z} \Rightarrow$ irreducible in $M_{1,4}$).

Arithmetical congruence monoids (ACMs)

Definition

An *arithmetical congruence monoid* is a **multiplicative** set

$$M_{a,b} = \{a, a+b, a+2b, a+3b, \ldots\} \subset (\mathbb{Z}_{\geq 1}, \cdot)$$

for $0 < a < b$ with $a^2 \equiv a \bmod b$.

Example

The *Hilbert monoid* $M_{1,4} = \{1, 5, 9, 13, 17, 21, 25, 29, 33, \ldots\}$.

- $65 = 5 \cdot 13$ (prime in $\mathbb{Z} \Rightarrow$ irreducible in $M_{1,4}$).
- $9, 21, 49 \in M_{1,4}$ are irreducible.

Arithmetical congruence monoids (ACMs)

Definition

An *arithmetical congruence monoid* is a **multiplicative** set

$$M_{a,b} = \{a, a+b, a+2b, a+3b, \ldots\} \subset (\mathbb{Z}_{\geq 1}, \cdot)$$

for $0 < a < b$ with $a^2 \equiv a \bmod b$.

Example

The *Hilbert monoid* $M_{1,4} = \{1, 5, 9, 13, 17, 21, 25, 29, 33, \ldots\}$.

- $65 = 5 \cdot 13$ (prime in $\mathbb{Z} \Rightarrow$ irreducible in $M_{1,4}$).
- $9, 21, 49 \in M_{1,4}$ are irreducible.
- $441 = 9 \cdot 49 = 21 \cdot 21$

Arithmetical congruence monoids (ACMs)

Definition

An *arithmetical congruence monoid* is a **multiplicative** set

$$M_{a,b} = \{a, a+b, a+2b, a+3b, \ldots\} \subset (\mathbb{Z}_{\geq 1}, \cdot)$$

for $0 < a < b$ with $a^2 \equiv a \bmod b$.

Example

The *Hilbert monoid* $M_{1,4} = \{1, 5, 9, 13, 17, 21, 25, 29, 33, \ldots\}$.

- $65 = 5 \cdot 13$ (prime in $\mathbb{Z} \Rightarrow$ irreducible in $M_{1,4}$).
- $9, 21, 49 \in M_{1,4}$ are irreducible.
- $441 = 9 \cdot 49 = 21 \cdot 21$
  $= (3^2) \cdot (7^2) = (3 \cdot 7) \cdot (3 \cdot 7)$.

ACM software package

`ArithmeticalCongruenceMonoid`: a Sage package, available from

`https://www.math.ucdavis.edu/~coneill/acms/`

ACM software package

`ArithmeticalCongruenceMonoid`: a Sage package, available from

`https://www.math.ucdavis.edu/~coneill/acms/`

```
sage: load('/.../ArithmeticalCongruenceMonoid.sage')
sage: H = ArithmeticalCongruenceMonoid(1, 4)
sage: H
Arithmetical Congruence Monoid (1, 4)
```

ACM software package

`ArithmeticalCongruenceMonoid`: a Sage package, available from

`https://www.math.ucdavis.edu/~coneill/acms/`

```
sage: load('/.../ArithmeticalCongruenceMonoid.sage')
sage: H = ArithmeticalCongruenceMonoid(1, 4)
sage: H
Arithmetical Congruence Monoid (1, 4)
sage: H.Factorizations(47224750041)
[[17, 21, 49, 89, 30333],
 [17, 21, 21, 89, 70777],
 [9, 17, 49, 89, 70777]]
```

ACM software package

`ArithmeticalCongruenceMonoid`: a Sage package, available from

`https://www.math.ucdavis.edu/~coneill/acms/`

```
sage: load('/.../ArithmeticalCongruenceMonoid.sage')
sage: H = ArithmeticalCongruenceMonoid(1, 4)
sage: H
Arithmetical Congruence Monoid (1, 4)
sage: H.Factorizations(47224750041)
[[17, 21, 49, 89, 30333],
 [17, 21, 21, 89, 70777],
 [9, 17, 49, 89, 70777]]
sage: H.IsIrreducible(999997)  # takes a few seconds
False
```

ACM software package

`ArithmeticalCongruenceMonoid`: a Sage package, available from

https://www.math.ucdavis.edu/~coneill/acms/

```
sage: load('/.../ArithmeticalCongruenceMonoid.sage')
sage: H = ArithmeticalCongruenceMonoid(1, 4)
sage: H
Arithmetical Congruence Monoid (1, 4)
sage: H.Factorizations(47224750041)
[[17, 21, 49, 89, 30333],
 [17, 21, 21, 89, 70777],
 [9, 17, 49, 89, 70777]]
sage: H.IsIrreducible(999997)  # takes a few seconds
False
sage: H.IrreduciblesUpToElement(10000001)
sage: H.IsIrreducible(999997)  # immediate
False
```

Periodicity in ACMs

Question [Baginski–Chapman, 2014]

When is the list of irreducibles in $M_{a,b}$ (eventually) periodic?

Periodicity in ACMs

Question [Baginski–Chapman, 2014]

When is the list of irreducibles in $M_{a,b}$ (eventually) periodic?

Use `IrreduciblesUpToElement()` to precompute reducible elements:

Periodicity in ACMs

Question [Baginski–Chapman, 2014]

When is the list of irreducibles in $M_{a,b}$ (eventually) periodic?

Use `IrreduciblesUpToElement()` to precompute reducible elements:

$M_{1,4}$:	1,	25,	45,	65,	81,	85,	...
$M_{5,20}$:	25,	125,	225,	325,	425,	525,	...
$M_{7,42}$:	49,	343,	637,	931,	1225,	1519,	...
$M_{51,150}$:	2601,	10251,	17901,	25551,	33201,	40401,	...
$M_{25,200}$:	625,	5625,	10625,	15625,	20625,	25625,	...
$M_{341,620}$:	116281,	327701,	539121,	750541,	923521,	961961,	...

Periodicity in ACMs

Question [Baginski–Chapman, 2014]

When is the list of irreducibles in $M_{a,b}$ (eventually) periodic?

Use `IrreduciblesUpToElement()` to precompute reducible elements:

	$M_{1,4}$:	1,	25,	45,	65,	81,	85,	...
$\rightarrow$	$M_{5,20}$:	25,	125,	225,	325,	425,	525,	...
$\rightarrow$	$M_{7,42}$:	49,	343,	637,	931,	1225,	1519,	...
	$M_{51,150}$:	2601,	10251,	17901,	25551,	33201,	40401,	...
$\rightarrow$	$M_{25,200}$:	625,	5625,	10625,	15625,	20625,	25625,	...
	$M_{341,620}$:	116281,	327701,	539121,	750541,	923521,	961961,	...

Periodicity in ACMs

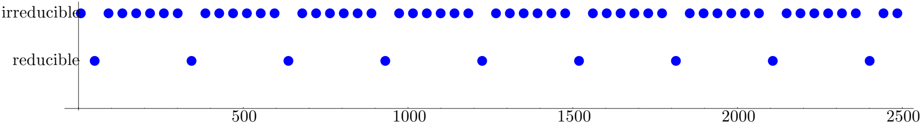
Question [Baginski–Chapman, 2014]

When is the list of irreducibles in $M_{a,b}$ (eventually) periodic?

Use `IrreduciblesUpToElement()` to precompute reducible elements:

	$M_{1,4}$:	1,	25,	45,	65,	81,	85,	...
$\rightarrow$	$M_{5,20}$:	25,	125,	225,	325,	425,	525,	...
$\rightarrow$	$M_{7,42}$:	49,	343,	637,	931,	1225,	1519,	...
	$M_{51,150}$:	2601,	10251,	17901,	25551,	33201,	40401,	...
$\rightarrow$	$M_{25,200}$:	625,	5625,	10625,	15625,	20625,	25625,	...
	$M_{341,620}$:	116281,	327701,	539121,	750541,	923521,	961961,	...

$M_{7,42}$:



The periodic case

Question [Baginski–Chapman, 2014]

When is the list of irreducibles in $M_{a,b}$ (eventually) periodic?

The periodic case

Question [Baginski–Chapman, 2014]

When is the list of irreducibles in $M_{a,b}$ (eventually) periodic?

Theorem

If $a \mid b$ and $a > 1$, then $M_{a,b}$ has periodic irreducible set.

The periodic case

Question [Baginski–Chapman, 2014]

When is the list of irreducibles in $M_{a,b}$ (eventually) periodic?

Theorem

If $a \mid b$ *and* $a > 1$*, then* $M_{a,b}$ *has periodic irreducible set.*

Example

$M_{5,20} = \{5, 25, 45, 65, 85, 105, 125, 145, 165, 185, 205, 225, 245, \ldots\}$

Reducible elements:

$$
\begin{array}{rcl}
25 = 5 \cdot 5 & 525 = 5 \cdot 105 & 1025 = 5 \cdot 205 \\
125 = 5 \cdot 25 & 625 = 5 \cdot 125 & 1125 = 5 \cdot 225 \\
225 = 5 \cdot 45 & 725 = 5 \cdot 145 & 1225 = 5 \cdot 245 \\
325 = 5 \cdot 65 & 825 = 5 \cdot 165 & 1325 = 5 \cdot 265 \\
425 = 5 \cdot 85 & 925 = 5 \cdot 185 & 1425 = 5 \cdot 285
\end{array}
$$

The remaining cases

Question [Baginski–Chapman, 2014]

When is the list of irreducibles in $M_{a,b}$ **not** (eventually) periodic?

The remaining cases

Question [Baginski–Chapman, 2014]

When is the list of irreducibles in $M_{a,b}$ **not** (eventually) periodic?

For $M_{1,4}$, a sequence of $k = 6$ consecutive reducible elements:

$$20884505 = 5 \cdot 4176901 \qquad 20884517 = 17 \cdot 1228501$$
$$20884509 = 9 \cdot 2320501 \qquad 20884521 = 21 \cdot 994501$$
$$20884513 = 13 \cdot 1606501 \qquad 20884525 = 25 \cdot 835381$$

The remaining cases

Question [Baginski–Chapman, 2014]

When is the list of irreducibles in $M_{a,b}$ **not** (eventually) periodic?

For $M_{1,4}$, a sequence of $k = 6$ consecutive reducible elements:

$$20884505 = 5 \cdot 4176901 \qquad 20884517 = 17 \cdot 1228501$$
$$20884509 = 9 \cdot 2320501 \qquad 20884521 = 21 \cdot 994501$$
$$20884513 = 13 \cdot 1606501 \qquad 20884525 = 25 \cdot 835381$$

For $M_{9,12}$, a sequence of $k = 4$ evenly-spaced reducible elements:

$$31995873 = 21 \cdot 1523613 \qquad 31995945 = 45 \cdot 711021$$
$$31995909 = 33 \cdot 969573 \qquad 31995981 = 57 \cdot 561333$$

The remaining cases

Question [Baginski–Chapman, 2014]

When is the list of irreducibles in $M_{a,b}$ **not** (eventually) periodic?

For $M_{1,4}$, a sequence of $k = 6$ consecutive reducible elements:

$$20884505 = 5 \cdot 4176901 \qquad 20884517 = 17 \cdot 1228501$$
$$20884509 = 9 \cdot 2320501 \qquad 20884521 = 21 \cdot 994501$$
$$20884513 = 13 \cdot 1606501 \qquad 20884525 = 25 \cdot 835381$$

For $M_{9,12}$, a sequence of $k = 4$ evenly-spaced reducible elements:

$$31995873 = 21 \cdot 1523613 \qquad 31995945 = 45 \cdot 711021$$
$$31995909 = 33 \cdot 969573 \qquad 31995981 = 57 \cdot 561333$$

Idea

Look for (arbitrarily) long sequences of evenly-spaced reducible elements.

The main theorem

Question [Baginski–Chapman, 2014]

When is the list of irreducibles in $M_{a,b}$ **not** (eventually) periodic?

The main theorem

Question [Baginski–Chapman, 2014]

When is the list of irreducibles in $M_{a,b}$ **not** (eventually) periodic?

Lemma

Let $g = \gcd(a, b)$. *The elements*

$$g(a + jb) + (a + b - g)\prod_{i=1}^{k}(a + ib) \quad \textit{for} \quad j = 1, \ldots, k$$

are all reducible, with constant difference gb.

The main theorem

Question [Baginski–Chapman, 2014]

When is the list of irreducibles in $M_{a,b}$ **not** (eventually) periodic?

Lemma

Let $g = \gcd(a, b)$. *The elements*

$$g(a + jb) + (a + b - g)\prod_{i=1}^{k}(a + ib) \quad \textit{for} \quad j = 1, \ldots, k$$

are all reducible, with constant difference gb.

The main theorem

Question [Baginski–Chapman, 2014]

When is the list of irreducibles in $M_{a,b}$ **not** (eventually) periodic?

Lemma

Let $g = \gcd(a, b)$*. The elements*

$$g(a + jb) + (a + b - g)\prod_{i=1}^{k}(a + ib) \quad \textit{for} \quad j = 1, \ldots, k$$

are all reducible, with constant difference gb*.*

The main theorem

Question [Baginski–Chapman, 2014]

When is the list of irreducibles in $M_{a,b}$ **not** (eventually) periodic?

Lemma

Let $g = \gcd(a, b)$. *The elements*

$$g(a + jb) + (a + b - g)\prod_{i=1}^{k}(a + ib) \quad \textit{for} \quad j = 1, \ldots, k$$

are all reducible, with constant difference gb.

The main theorem

Question [Baginski–Chapman, 2014]

When is the list of irreducibles in $M_{a,b}$ **not** (eventually) periodic?

Lemma

Let $g = \gcd(a, b)$*. The elements*

$$g(a + jb) + (a + b - g)\prod_{i=1}^{k}(a + ib) \quad \textit{for} \quad j = 1, \ldots, k$$

are all reducible, with constant difference gb*.*

The main theorem

Question [Baginski–Chapman, 2014]

When is the list of irreducibles in $M_{a,b}$ **not** (eventually) periodic?

Lemma

Let $g = \gcd(a, b)$. *The elements*

$$g(a + jb) + (a + b - g)\prod_{i=1}^{k}(a + ib) \quad \textit{for} \quad j = 1, \ldots, k$$

are all reducible, with constant difference gb.

Theorem

$M_{a,b}$ *has periodic irreducible set if and only if* $a \mid b$ *and* $a > 1$.

References

P. Baginski and S. Chapman,
Arithmetic congruence monoids: a survey,
Combinatorial and additive number theory - CANT 2011 and 2012, 15–38, Springer Proc. Math. Stat., 101, Springer, New York, 2014.

J. Hartzer and C. O'Neill,
On the periodicity of irreducible elements in arithmetical congruence monoids,
preprint. (`arXiv: math.NT/1606.00376`)

J. Hartzer and C. O'Neill,
ArithmeticalCongruenceMonoid (Sage software),
`https://www.math.ucdavis.edu/~coneill/acms/`.

References

P. Baginski and S. Chapman,
Arithmetic congruence monoids: a survey,
Combinatorial and additive number theory - CANT 2011 and 2012, 15–38, Springer Proc. Math. Stat., 101, Springer, New York, 2014.

J. Hartzer and C. O'Neill,
On the periodicity of irreducible elements in arithmetical congruence monoids,
preprint. (`arXiv: math.NT/1606.00376`)

J. Hartzer and C. O'Neill,
ArithmeticalCongruenceMonoid (Sage software),
`https://www.math.ucdavis.edu/~coneill/acms/`.

Thanks!