Invariants of non-unique factorization

Christopher O'Neill

Texas A&M University

coneill@math.tamu.edu

Joint with Roberto Pelayo

October 21, 2014

Factorial domains

Definition

An integral domain R is *factorial* if for each non-unit $r \in R$,

1. there is a *factorization* $r = u_1 \cdots u_k$ as a product of irreducibles, and
2. this factorization is unique (up to reordering and unit multiple).

Factorial domains

Definition

An integral domain R is *factorial* if for each non-unit $r \in R$,

1. there is a *factorization* $r = u_1 \cdots u_k$ as a product of irreducibles, and
2. this factorization is unique (up to reordering and unit multiple).

Example

$\mathbb{Z}$ is factorial: each $z = p_1 \cdots p_k$ for primes $p_1 \cdots p_k$.

Factorial domains

Definition

An integral domain R is *atomic* if for each non-unit $r \in R$,

1. there is a *factorization* $r = u_1 \cdots u_k$ as a product of irreducibles, ~~and~~
2. ~~this factorization is unique (up to reordering and unit multiple~~).

Example

$\mathbb{Z}$ is factorial: each $z = p_1 \cdots p_k$ for primes $p_1 \cdots p_k$.

Factorial domains

Definition

An integral domain R is *atomic* if for each non-unit $r \in R$,

1. there is a *factorization* $r = u_1 \cdots u_k$ as a product of irreducibles, ~~and~~
2. ~~this factorization is unique (up to reordering and unit multiple)~~.

Example

$\mathbb{Z}$ is factorial: each $z = p_1 \cdots p_k$ for primes $p_1 \cdots p_k$.

Example

If $R = \mathbb{Z}[\sqrt{-5}]$, then $6 \in R$ has two distinct factorizations:

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

Factorial domains

Definition

An integral domain R is *atomic* if for each non-unit $r \in R$,

1. there is a *factorization* $r = u_1 \cdots u_k$ as a product of irreducibles, ~~and~~
2. ~~this factorization is unique (up to reordering and unit multiple)~~.

Example

$\mathbb{Z}$ is factorial: each $z = p_1 \cdots p_k$ for primes $p_1 \cdots p_k$.

Example

If $R = \mathbb{Z}[\sqrt{-5}]$, then $6 \in R$ has two distinct factorizations:

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

To prove: define a *valuation* $a + b\sqrt{-5} \mapsto a^2 + 5b^2$.

Factorial domains

Definition

An integral domain R is *atomic* if for each non-unit $r \in R$,

1. there is a *factorization* $r = u_1 \cdots u_k$ as a product of irreducibles, ~~and~~
2. ~~this factorization is unique (up to reordering and unit multiple)~~.

Example

$\mathbb{Z}$ is factorial: each $z = p_1 \cdots p_k$ for primes $p_1 \cdots p_k$.

Example

If $R = \mathbb{Z}[\sqrt{-5}]$, then $6 \in R$ has two distinct factorizations:

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

To prove: define a *valuation* $a + b\sqrt{-5} \mapsto a^2 + 5b^2$.
The point: it's nontrivial.

Factorial domains

Definition

An integral domain R is *atomic* if for each non-unit $r \in R$,

1. there is a *factorization* $r = u_1 \cdots u_k$ as a product of irreducibles, ~~and~~
2. ~~this factorization is unique (up to reordering and unit multiple)~~.

Example

$\mathbb{Z}$ is factorial: each $z = p_1 \cdots p_k$ for primes $p_1 \cdots p_k$.

Example

Factorial domains

Definition

An integral domain R is *atomic* if for each non-unit $r \in R$,

1. there is a *factorization* $r = u_1 \cdots u_k$ as a product of irreducibles, ~~and~~
2. ~~this factorization is unique (up to reordering and unit multiple~~).

Example

$\mathbb{Z}$ is factorial: each $z = p_1 \cdots p_k$ for primes $p_1 \cdots p_k$.

Example

Let $R = \mathbb{C}[x^2, x^3]$.

Factorial domains

Definition

An integral domain R is *atomic* if for each non-unit $r \in R$,

1. there is a *factorization* $r = u_1 \cdots u_k$ as a product of irreducibles, ~~and~~
2. ~~this factorization is unique (up to reordering and unit multiple)~~.

Example

$\mathbb{Z}$ is factorial: each $z = p_1 \cdots p_k$ for primes $p_1 \cdots p_k$.

Example

Let $R = \mathbb{C}[x^2, x^3]$.

1. x^2 and x^3 are irreducible.

Factorial domains

Definition

An integral domain R is *atomic* if for each non-unit $r \in R$,

1. there is a *factorization* $r = u_1 \cdots u_k$ as a product of irreducibles, ~~and~~
2. ~~this factorization is unique (up to reordering and unit multiple)~~.

Example

$\mathbb{Z}$ is factorial: each $z = p_1 \cdots p_k$ for primes $p_1 \cdots p_k$.

Example

Let $R = \mathbb{C}[x^2, x^3]$.

1. x^2 and x^3 are irreducible.
2. $x^6 = x^3 \cdot x^3 = x^2 \cdot x^2 \cdot x^2$.

Factorial domains

Definition

An integral domain R is *atomic* if for each non-unit $r \in R$,

1. there is a *factorization* $r = u_1 \cdots u_k$ as a product of irreducibles, ~~and~~
2. ~~this factorization is unique (up to reordering and unit multiple~~).

Example

$\mathbb{Z}$ is factorial: each $z = p_1 \cdots p_k$ for primes $p_1 \cdots p_k$.

Observation

Factorial domains

Definition

An integral domain R is *atomic* if for each non-unit $r \in R$,

1. there is a *factorization* $r = u_1 \cdots u_k$ as a product of irreducibles, ~~and~~
2. ~~this factorization is unique (up to reordering and unit multiple~~).

Example

$\mathbb{Z}$ is factorial: each $z = p_1 \cdots p_k$ for primes $p_1 \cdots p_k$.

Observation

- Where's the addition?

Factorial domains

Definition

An integral domain R is *atomic* if for each non-unit $r \in R$,

1. there is a *factorization* $r = u_1 \cdots u_k$ as a product of irreducibles, ~~and~~
2. ~~this factorization is unique (up to reordering and unit multiple)~~.

Example

$\mathbb{Z}$ is factorial: each $z = p_1 \cdots p_k$ for primes $p_1 \cdots p_k$.

Observation

- Where's the addition?
- Factorization in (cancellative comutative) monoids:

Factorial domains

Definition

An integral domain R is *atomic* if for each non-unit $r \in R$,

1. there is a *factorization* $r = u_1 \cdots u_k$ as a product of irreducibles, ~~and~~
2. ~~this factorization is unique (up to reordering and unit multiple)~~.

Example

$\mathbb{Z}$ is factorial: each $z = p_1 \cdots p_k$ for primes $p_1 \cdots p_k$.

Observation

- Where's the addition?
- Factorization in (cancellative comutative) monoids:

$$(R, +, \cdot) \quad \rightsquigarrow \quad (R \setminus \{0\}, \cdot)$$

Factorial domains

Definition

An integral domain R is *atomic* if for each non-unit $r \in R$,

1. there is a *factorization* $r = u_1 \cdots u_k$ as a product of irreducibles, ~~and~~
2. ~~this factorization is unique (up to reordering and unit multiple~~).

Example

$\mathbb{Z}$ is factorial: each $z = p_1 \cdots p_k$ for primes $p_1 \cdots p_k$.

Observation

- Where's the addition?
- Factorization in (cancellative comutative) monoids:

$$\begin{array}{rcl} (R, +, \cdot) & \rightsquigarrow & (R \setminus \{0\}, \cdot) \\ (\mathbb{C}[M], +, \cdot) & \rightsquigarrow & (M, \cdot) \end{array}$$

Interesting monoids

Definition

An *arithmetical congruence monoid* is a multiplicative submonoid

$$M_{a,b} = \{n : n \equiv a \bmod b\} \subset \mathbb{Z}_{>0}$$

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

Interesting monoids

Definition

An *arithmetical congruence monoid* is a multiplicative submonoid

$$M_{a,b} = \{n : n \equiv a \bmod b\} \subset \mathbb{Z}_{>0}$$

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

Example

The *Hilbert monoid* $M_{1,4}$.

Interesting monoids

Definition

An *arithmetical congruence monoid* is a multiplicative submonoid

$$M_{a,b} = \{n : n \equiv a \bmod b\} \subset \mathbb{Z}_{>0}$$

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

Example

The *Hilbert monoid* $M_{1,4}$.

- Every product in $M_{1,4}$ is a product in $\mathbb{Z}$.

Interesting monoids

Definition

An *arithmetical congruence monoid* is a multiplicative submonoid

$$M_{a,b} = \{n : n \equiv a \bmod b\} \subset \mathbb{Z}_{>0}$$

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

Example

The *Hilbert monoid* $M_{1,4}$.

- Every product in $M_{1,4}$ is a product in $\mathbb{Z}$.
- $9, 21, 49 \in M_{1,4}$ are irreducible.

Interesting monoids

Definition

An *arithmetical congruence monoid* is a multiplicative submonoid

$$M_{a,b} = \{n : n \equiv a \bmod b\} \subset \mathbb{Z}_{>0}$$

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

Example

The *Hilbert monoid* $M_{1,4}$.

- Every product in $M_{1,4}$ is a product in $\mathbb{Z}$.
- $9, 21, 49 \in M_{1,4}$ are irreducible.
- $441 = 9 \cdot 49 = 21 \cdot 21$.

Interesting monoids

Definition

A *numerical monoid* S is an **additive** submonoid of $\mathbb{N}$ with $|\mathbb{N} \setminus S| < \infty$.

Definition

A *numerical monoid* S is an **additive** submonoid of $\mathbb{N}$ with $|\mathbb{N} \setminus S| < \infty$.

Example

Let $S = \langle 2, 3 \rangle = \{2, 3, 4, 5, \ldots\}$ under **addition**.

Interesting monoids

Definition

A *numerical monoid* S is an **additive** submonoid of $\mathbb{N}$ with $|\mathbb{N} \setminus S| < \infty$.

Example

Let $S = \langle 2, 3 \rangle = \{2, 3, 4, 5, \ldots\}$ under **addition**.

- $\mathbb{C}[S] = \mathbb{C}[x^2, x^3]$.

Interesting monoids

Definition

A *numerical monoid* S is an **additive** submonoid of $\mathbb{N}$ with $|\mathbb{N} \setminus S| < \infty$.

Example

Let $S = \langle 2, 3 \rangle = \{2, 3, 4, 5, \ldots\}$ under **addition**.

- $\mathbb{C}[S] = \mathbb{C}[x^2, x^3]$.
- $6 = 2 + 2 + 2 = 3 + 3$.

Interesting monoids

Definition

A *numerical monoid* S is an **additive** submonoid of $\mathbb{N}$ with $|\mathbb{N} \setminus S| < \infty$.

Example

Let $S = \langle 2, 3 \rangle = \{2, 3, 4, 5, \ldots\}$ under **addition**.

- $\mathbb{C}[S] = \mathbb{C}[x^2, x^3]$.
- $6 = 2 + 2 + 2 = 3 + 3$. Factorizations are additive!

Interesting monoids

Definition

A *numerical monoid* S is an **additive** submonoid of $\mathbb{N}$ with $|\mathbb{N} \setminus S| < \infty$.

Example

Let $S = \langle 2, 3 \rangle = \{2, 3, 4, 5, \ldots\}$ under **addition**.

- $\mathbb{C}[S] = \mathbb{C}[x^2, x^3]$.
- $6 = 2 + 2 + 2 = 3 + 3$. Factorizations are additive!

Example

$McN = \langle 6, 9, 20 \rangle = \{0, 6, 9, 12, 15, 18, 20, 21, \ldots\}$.

Interesting monoids

Definition

A *numerical monoid* S is an **additive** submonoid of $\mathbb{N}$ with $|\mathbb{N} \setminus S| < \infty$.

Example

Let $S = \langle 2, 3 \rangle = \{2, 3, 4, 5, \ldots\}$ under **addition**.

- $\mathbb{C}[S] = \mathbb{C}[x^2, x^3]$.
- $6 = 2 + 2 + 2 = 3 + 3$. Factorizations are additive!

Example

$McN = \langle 6, 9, 20 \rangle = \{0, 6, 9, 12, 15, 18, 20, 21, \ldots\}$. "McNugget Monoid"

Factorization invariants

Factorization invariants

Definition

Fix a commutative, cancellative monoid $(M, \cdot)$. For non-unit $m \in M$,

$$\mathsf{Z}_M(m) = \{u_1 \cdots u_k = m : u_1, \ldots, u_k \text{ irreducible}\}$$

denotes the *set of factorizations* of m.

Factorization invariants

Definition

Fix a commutative, cancellative monoid $(M, \cdot)$. For non-unit $m \in M$,

$$\mathsf{Z}_M(m) = \{u_1 \cdots u_k = m : u_1, \ldots, u_k \text{ irreducible}\}$$

denotes the *set of factorizations* of m. The *elasticity* of m is

$$\rho(m) = \frac{\text{max length in } \mathsf{Z}_M(m)}{\text{min length in } \mathsf{Z}_M(m)}.$$

Factorization invariants

Definition

Fix a commutative, cancellative monoid $(M, \cdot)$. For non-unit $m \in M$,

$$\mathsf{Z}_M(m) = \{u_1 \cdots u_k = m : u_1, \ldots, u_k \text{ irreducible}\}$$

denotes the *set of factorizations* of m. The *elasticity* of m is

$$\rho(m) = \frac{\text{max length in } \mathsf{Z}_M(m)}{\text{min length in } \mathsf{Z}_M(m)}.$$

The *elasticity* of M is $\rho(M) = \sup_{m \in M} \rho(m)$.

Factorization invariants

Definition

Fix a commutative, cancellative monoid $(M, \cdot)$. For non-unit $m \in M$,

$$\mathsf{Z}_M(m) = \{u_1 \cdots u_k = m : u_1, \ldots, u_k \text{ irreducible}\}$$

denotes the *set of factorizations* of m. The *elasticity* of m is

$$\rho(m) = \frac{\text{max length in } \mathsf{Z}_M(m)}{\text{min length in } \mathsf{Z}_M(m)}.$$

The *elasticity* of M is $\rho(M) = \sup_{m \in M} \rho(m)$.

Example (The good)

The Hilbert monoid: $\rho(M_{1,4}) = 1$.

Factorization invariants

Definition

Fix a commutative, cancellative monoid $(M, \cdot)$. For non-unit $m \in M$,

$$\mathsf{Z}_M(m) = \{u_1 \cdots u_k = m : u_1, \ldots, u_k \text{ irreducible}\}$$

denotes the *set of factorizations* of m. The *elasticity* of m is

$$\rho(m) = \frac{\text{max length in } \mathsf{Z}_M(m)}{\text{min length in } \mathsf{Z}_M(m)}.$$

The *elasticity* of M is $\rho(M) = \sup_{m \in M} \rho(m)$.

Example (The good)

The Hilbert monoid: $\rho(M_{1,4}) = 1$.

- Every factorization of $m \in M_{1,4}$ has the same length.

Factorization invariants

Definition

Fix a commutative, cancellative monoid $(M, \cdot)$. For non-unit $m \in M$,

$$\mathsf{Z}_M(m) = \{u_1 \cdots u_k = m : u_1, \ldots, u_k \text{ irreducible}\}$$

denotes the *set of factorizations* of m. The *elasticity* of m is

$$\rho(m) = \frac{\text{max length in } \mathsf{Z}_M(m)}{\text{min length in } \mathsf{Z}_M(m)}.$$

The *elasticity* of M is $\rho(M) = \sup_{m \in M} \rho(m)$.

Example (The good)

The Hilbert monoid: $\rho(M_{1,4}) = 1$.

- Every factorization of $m \in M_{1,4}$ has the same length.
- This is (almost) the best we could hope for.

Factorization invariants

Definition

Fix a commutative, cancellative monoid $(M, \cdot)$. For non-unit $m \in M$,

$$\mathsf{Z}_M(m) = \{u_1 \cdots u_k = m : u_1, \ldots, u_k \text{ irreducible}\}$$

denotes the *set of factorizations* of m. The *elasticity* of m is

$$\rho(m) = \frac{\text{max length in } \mathsf{Z}_M(m)}{\text{min length in } \mathsf{Z}_M(m)}.$$

The *elasticity* of M is $\rho(M) = \sup_{m \in M} \rho(m)$.

Example (The bad)

Numerical monoids: $S = \langle n_1 < \ldots < n_k \rangle \subset \mathbb{N}$. $\rho(S) = n_k/n_1$.

Factorization invariants

Definition

Fix a commutative, cancellative monoid $(M, \cdot)$. For non-unit $m \in M$,

$$\mathsf{Z}_M(m) = \{u_1 \cdots u_k = m : u_1, \ldots, u_k \text{ irreducible}\}$$

denotes the *set of factorizations* of m. The *elasticity* of m is

$$\rho(m) = \frac{\text{max length in } \mathsf{Z}_M(m)}{\text{min length in } \mathsf{Z}_M(m)}.$$

The *elasticity* of M is $\rho(M) = \sup_{m \in M} \rho(m)$.

Example (The bad)

Numerical monoids: $S = \langle n_1 < \ldots < n_k \rangle \subset \mathbb{N}$. $\rho(S) = n_k/n_1$.

- $n_1 n_k = n_1 + \cdots + n_1 = n_k + \cdots + n_k$, so $\rho(n_1 n_k) = n_k/n_1$.

Factorization invariants

Definition

Fix a commutative, cancellative monoid $(M, \cdot)$. For non-unit $m \in M$,

$$\mathsf{Z}_M(m) = \{u_1 \cdots u_k = m : u_1, \ldots, u_k \text{ irreducible}\}$$

denotes the *set of factorizations* of m. The *elasticity* of m is

$$\rho(m) = \frac{\text{max length in } \mathsf{Z}_M(m)}{\text{min length in } \mathsf{Z}_M(m)}.$$

The *elasticity* of M is $\rho(M) = \sup_{m \in M} \rho(m)$.

Example (The bad)

Numerical monoids: $S = \langle n_1 < \ldots < n_k \rangle \subset \mathbb{N}$. $\rho(S) = n_k/n_1$.

- $n_1 n_k = n_1 + \cdots + n_1 = n_k + \cdots + n_k$, so $\rho(n_1 n_k) = n_k/n_1$.
- $\rho(n) \le n_k/n_1$ for all $n \in S$.

Factorization invariants

Definition

Fix a commutative, cancellative monoid $(M, \cdot)$. For non-unit $m \in M$,

$$\mathsf{Z}_M(m) = \{u_1 \cdots u_k = m : u_1, \ldots, u_k \text{ irreducible}\}$$

denotes the *set of factorizations* of m. The *elasticity* of m is

$$\rho(m) = \frac{\text{max length in } \mathsf{Z}_M(m)}{\text{min length in } \mathsf{Z}_M(m)}.$$

The *elasticity* of M is $\rho(M) = \sup_{m \in M} \rho(m)$.

Example (The ugly)

The Meyerson monoid: $\rho(M_{4,6}) = 2$.

Factorization invariants

Definition

Fix a commutative, cancellative monoid $(M, \cdot)$. For non-unit $m \in M$,

$$\mathsf{Z}_M(m) = \{u_1 \cdots u_k = m : u_1, \ldots, u_k \text{ irreducible}\}$$

denotes the *set of factorizations* of m. The *elasticity* of m is

$$\rho(m) = \frac{\text{max length in } \mathsf{Z}_M(m)}{\text{min length in } \mathsf{Z}_M(m)}.$$

The *elasticity* of M is $\rho(M) = \sup_{m \in M} \rho(m)$.

Example (The ugly)

The Meyerson monoid: $\rho(M_{4,6}) = 2$.

- $\rho(m) < 2$ for all $m \in M_{4,6}$!

Factorization invariants

Definition

Fix a commutative, cancellative monoid $(M, \cdot)$. For non-unit $m \in M$,

$$\mathsf{Z}_M(m) = \{u_1 \cdots u_k = m : u_1, \ldots, u_k \text{ irreducible}\}$$

denotes the *set of factorizations* of m. The *elasticity* of m is

$$\rho(m) = \frac{\text{max length in } \mathsf{Z}_M(m)}{\text{min length in } \mathsf{Z}_M(m)}.$$

The *elasticity* of M is $\rho(M) = \sup_{m \in M} \rho(m)$.

Example (The ugly)

The Meyerson monoid: $\rho(M_{4,6}) = 2$.

- $\rho(m) < 2$ for all $m \in M_{4,6}$!
- Elasticity of $M_{4,6}$ is *not accepted*.

Factorization invariants

Definition (ω-primality)

Fix a cancellative, commutative, atomic monoid M. For $x \in M$, $\omega(x)$ is the smallest positive integer m such that whenever $x \mid \prod_{i=1}^{r} u_i$ for $r > m$, there exists a subset $T \subset \{1, \ldots, r\}$ with $|T| \leq m$ such that $x \mid \prod_{i \in T} u_i$.

Factorization invariants

Definition (ω-primality)

Fix a cancellative, commutative, atomic monoid M. For $x \in M$, $\omega(x)$ is the smallest positive integer m such that whenever $x \mid \prod_{i=1}^{r} u_i$ for $r > m$, there exists a subset $T \subset \{1, \ldots, r\}$ with $|T| \leq m$ such that $x \mid \prod_{i \in T} u_i$.

Fact

$\omega(x) = 1$ if and only if x is prime (i.e. $x \mid ab$ implies $x \mid a$ or $x \mid b$).

Factorization invariants

Definition (ω-primality)

Fix a cancellative, commutative, atomic monoid M. For $x \in M$, $\omega(x)$ is the smallest positive integer m such that whenever $x \mid \prod_{i=1}^{r} u_i$ for $r > m$, there exists a subset $T \subset \{1, \ldots, r\}$ with $|T| \leq m$ such that $x \mid \prod_{i \in T} u_i$.

Fact

$\omega(x) = 1$ if and only if x is prime (i.e. $x \mid ab$ implies $x \mid a$ or $x \mid b$).

Fact

M is factorial if and only if every irreducible element of M is prime. Moreover, $\omega(p_1 \cdots p_r) = r$ for any primes $p_1, \ldots, p_r \in M$.

Quasilinearity for numerical monoids

Theorem (O.–Pelayo, 2013)

Fix a numerical monoid $S = \langle n_1, \ldots, n_k \rangle \subset \mathbb{N}$. *For* $n \gg 0$,

$$\omega_S(n) = \frac{1}{n_1} n + a_0(n)$$

where $a_0(n)$ *periodic with period* n_1.

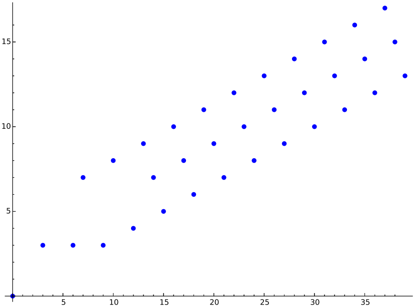
Quasilinearity for numerical monoids

Theorem (O.–Pelayo, 2013)

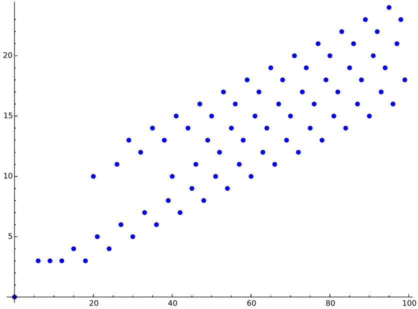
Fix a numerical monoid $S = \langle n_1, \ldots, n_k \rangle \subset \mathbb{N}$. For $n \gg 0$,

$$\omega_S(n) = \frac{1}{n_1} n + a_0(n)$$

where $a_0(n)$ periodic with period n_1.



$S = \langle 3, 7 \rangle$



$McN = \langle 6, 9, 20 \rangle$

References

Alfred Geroldinger, Franz Halter-Koch (2006)
Nonunique factorization: Algebraic, Combinatorial, and Analytic Theory.
Chapman & Hall/CRC, Boca Raton, FL, 2006.

Christopher O'Neill, Roberto Pelayo (2014)
How do you measure primality?
American Mathematical Monthly, forthcoming.

Manuel Delgado, Pedro García-Sánchez, Jose Morais
GAP Numerical Semigroups Package
`http://www.gap-system.org/Packages/numericalsgps.html`.

References

Alfred Geroldinger, Franz Halter-Koch (2006)
Nonunique factorization: Algebraic, Combinatorial, and Analytic Theory.
Chapman & Hall/CRC, Boca Raton, FL, 2006.

Christopher O'Neill, Roberto Pelayo (2014)
How do you measure primality?
American Mathematical Monthly, forthcoming.

Manuel Delgado, Pedro García-Sánchez, Jose Morais
GAP Numerical Semigroups Package
`http://www.gap-system.org/Packages/numericalsgps.html`.

Thanks!