Computing Factorizations in Arithmetical Congruence Monoids

Presenter: Jacob Hartzer
JMHartzer@tamu.edu

Abstract

Let $\mathbb{N}$ represent the set of all positive integers. Fix $a < b \in \mathbb{N}$, and let $M_{a,b} = \{n \in \mathbb{N} : n \equiv a \mod b\}$. If the set $M_{a,b}$ is closed under multiplication (that is if $a^2 \equiv a \mod b$), then it is known as an Arithmetical Congruence Monoid or ACM. In this poster, we present software for computing factorizations in ACMs. Using this software we provide examples of ACMs that exhibit periodic reducibility as well as some that don't

Introduction to ACMs

ACMs are defined as follows

- A set of all numbers that are $a \mod b$
- $a^2 \equiv a \mod b$

For example: the Hilbert Monoid $M_{1,4}$

$$1, 5, 9, 13, 17, 21, 25$$

There exist both prime and composite elements that are irreducible

prime	nonprime
13	49
53	121
997	933

Also, there exist elements that are uniquely factorable

$$25 = 5 \cdot 5$$
$$189 = 9 \cdot 21$$

Finally, ACMs lead to nonuniqe factorization

$$441 = 21 \cdot 21 = 9 \cdot 49$$

$$693 = 21 \cdot 33 = 9 \cdot 77$$

Elements that can be factored by elements are termed reducible

Sample Code

```
N = ArithmeticCongruenceMonoid([1,4])
N.ArithmeticFactorizations(10^25 + 1)
    [[100001, 1267801, 78875943472201],
     [55561, 2281841, 78875943472201],
     [2761, 45918641, 78875943472201]]
N = ArithmeticCongruenceMonoid([4,6])
N.MaxElasticityToElement(10^6)
    1.6666666666666667
N.PercentIrreducible(10^6)
    0.6272987454025092
```

The Program

To understand the program, take 441^2, with the following factorization:

$$441^2 = 3^4 \cdot 7^4$$

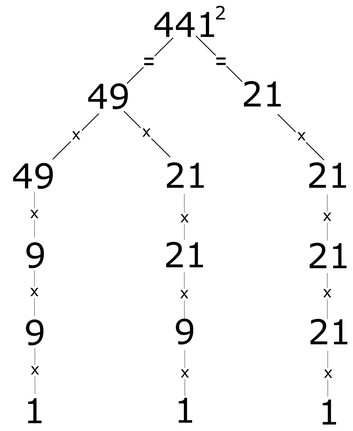
It then finds every combination of these primes

$$3^1 7^0, 3^2 7^0, 3^3 7^0, 3^4 7^0, 3^1 7^1 ... 3^4 7^4$$

It then removes all factors that aren't in the monoid

$$[1, 9, 21, 49, 441] \equiv 1 \mod 4$$

A recursive program then finds every way to multiply these numbers to the original, by branching lists.

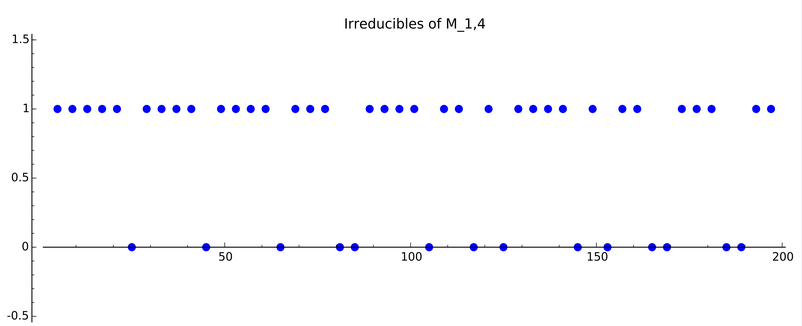


The Question

Nonunique factorization leads us to ask the question:
Is there is any pattern in element reducibility?

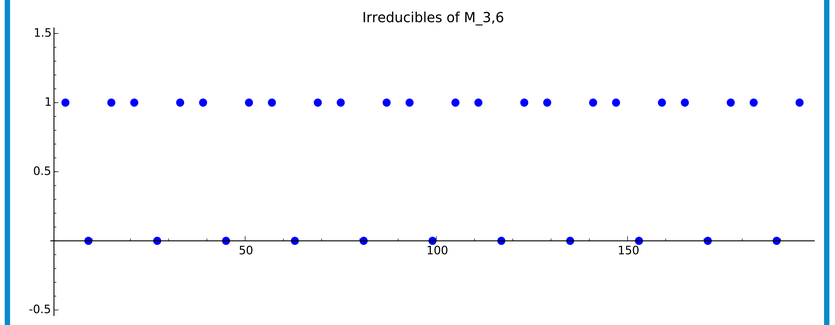
Aperiodic ACMs

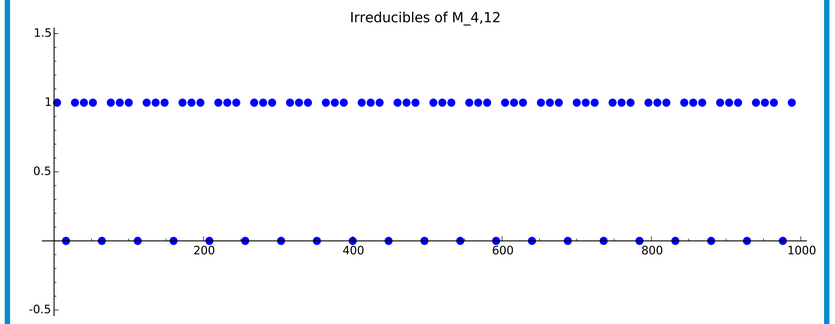
Below is an example graph of an aperiodic ACM

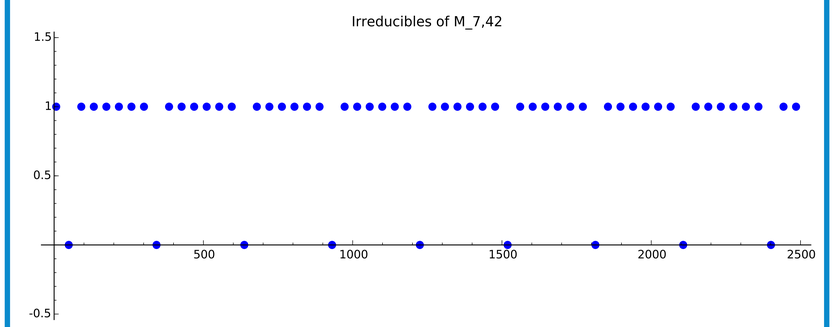


Periodic ACMs

Here are a few examples of periodic ACMs







As can be seen, all periodic ACMs follow the following conditions

- $a \neq 1$
- $b = k \cdot a$ where $k \in \mathbb{Z}^+$

Theorem

Theorem: $M_{a,b}$ is periodic if and only if $b = k \cdot a$ for some $k \in \mathbb{Z}^+$

References

[1] W. A. Stein et al., *Sage Mathematics Software (Version 5.3)*, The Sage Development Team, 2013, http://www.sagemath.org.