Properties of Arithmetic Congruence Monoids

Bruce Zheng

July 31, 2014

Atoms and Primes

The natural numbers under multiplication form a monoid. $\mathbb{N} = \{1, 2, \dots\}$. The nonunits of $\mathbb{N}$ are $\{2, 3, \dots\}$.

Definition

Let M be a commutative, cancellative monoid and let x be a nonunit of M. Then

- *If x is not a product of two nonunits, x is irreducible, or an atom.*
- *If for any $y, z \in M$, $x \mid yz$ implies $x \mid y$ or $x \mid z$, then x is prime.*
- *If all nonunits of M have an atomic factorization, M is atomic.*

It is easy to see that all primes are atoms. In $(\mathbb{N}, \times)$, all atoms are prime (Euclid's Lemma).

Hilbert's Monoid

Let $\mathbf{H} = 1 + 4\mathbb{N}_0 = \{1, 5, 9, \dots\}$.
$\mathbf{H}$ is closed under multiplication (so it is a monoid), and any nonunit of $\mathbf{H}$ has an atomic factorization. However, atoms are not necessarily primes.
We have that 9 is an atom of $\mathbf{H}$ with

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

Then $9 \mid 21 \cdot 33$ even though clearly $9 \nmid 21$ and $9 \nmid 33$, so Euclid's Lemma does not hold for $\mathbf{H}$!

Omega-Primality

Definition

Let M be a commutative, cancellative monoid and $x \in M$ a nonunit.

- *If $x_1, \ldots, x_n \in M$ are nonunits with $x \mid x_1 \ldots x_n$ but x divides no subproduct of $x_1 \ldots x_n$, then $x_1 \cdots x_n$ is a bullet for x of length n.*
- *$\omega_M(x)$ is the suprema of the set of bullet lengths for x.*

x is a prime of M if and only if $\omega_M(x) = 1$. As an extension of Euclid's Lemma, we have the following:

Theorem

If $x = p_1 p_2 \cdots p_n \in \mathbb{N}$ for primes p_i, $\omega_{\mathbb{N}}(x) = n$.

$21 \cdot 33$ is a bullet for 9 in $\mathbf{H}$, so $\omega_{\mathbf{H}}(9) \geq 2$ despite the fact that 9 is irreducible.

Arithmetic Congruence Monoids

The fact that **H** is closed under multiplication is equivalent to the fact that $1 \equiv 1^2 \mod 4$.

Definition

Let $a, b \in \mathbb{N}$ with $a \leq b$ and $a^2 \equiv a \mod b$. The Arithmetic Congruence Monoid (ACM) defined on a and b is

$$M(a, b) = \{1\} \cup (a + b\mathbb{N}_0) = \{1, a, a + b, a + 2b, \dots\}$$

Given an ACM $M = M(a, b)$ and $x \in M$, what is $\omega(x)$?

Decomposition of ACM

For $x \in \mathbb{N}$, $x \in M(a,b)$ if and only if $x \equiv a \mod b$. Since modular congruence classes an integer are decomposeable, we may also decompose ACM.

Theorem

Let $M(a,b)$ be an ACM. Suppose $d = \gcd(a,b)$ and set $n = b/d$. Then

$$M(a,b) = M(d,d) \cap M(1,n).$$

If $x \in M(a,b)$, let $r_x \in \mathbb{N}$ be the largest factor of x which is relatively prime to d. Furthermore, let $s_x = x/r_x$. Let $\delta(x)$ be the largest power of d of x that divides s_x in $\mathbb{N}$.

Example

Let $M = M(4,6)$ and $x = 136 \in M$. Then $d = 2$, $r_x = 17$, $s_x = 8$ and $\delta(x) = 3$.

Omega-Primality of ACM

Theorem

Let M be an ACM and $x \in M$. Let $x = s_x p_1 \cdots p_m$ for primes p_i. Then $\omega_M(x) = \max(\delta(x) + 1, m)$.

There is one case when the omega-primality of $M(a, b)$ simplifies greatly:

Example

Let $M = M(1, n)$ be an ACM and $x \in M$. Then let $r_x = p_1 \cdots p_m$. Since $\gcd(1, n) = 1$, $r_x = x$ and $s_x = 1$. Then $\delta(x) = 0$, hence $\omega_M(x) = m = \omega_{\mathbb{N}}(x)$.

Elasticities

Definition

Let M be a commutative, cancellative, atomic monoid and x be a nonunit of M.

- $\mathcal{L}(x) = \{k \in \mathbb{N} : x = a_1 \cdots a_k \text{ for atoms } a_i\}$
- $\rho(x) = \sup\{\mathcal{L}(x)\}/\min\{\mathcal{L}(x)\}$
- $\rho(M) = \sup\{\rho(x) : x \in M\}$
- $\rho_k(M) = \sup\{\sup\{\mathcal{L}(x) : k \in \mathcal{L}(x)\}\}$

The elasticity of M is accepted if there exists some $x \in M$ such that $\rho(x) = \rho(M)$.

Elasticities of ACM

Theorem

Let $M(a, b)$ be an ACM and let $d = \gcd(a, b)$.

- *If $d = 1$, then $\rho(M)$ is always accepted.*
- *If d is divsible by more than 1 prime, $\rho(M) = \infty$, so $\rho(M)$ is never accepted.*

If $d = p^{\alpha}$ for a prime p, then letting $p^{\beta} \in M$ such that β is minimal. Then $\rho(M) = (\alpha + \beta - 1)/\alpha$. We do not know in general whether or not the elasticity is accepted in this case!

$\gcd(a, b) = p$

Let ϕ denote the euler totient function.
Since $|\mathbb{Z}_n^\times| = \phi(n)$, we have that $o(d) \mid \phi(n)$. When d is a prime, $o(p) = \beta$.

Theorem

Let $M = M(p, p) \cap M(1, n)$ for a prime p. Set β to be the smallest power of p such that $p^\beta \in M$.

- *If $\beta > \phi(n)^{2/3}$, then $\rho(M)$ is not accepted.*
- *If $\beta = \phi(n)$, then $\rho_k(M) = (k-1)\beta + 1$.*

Further Reading

[1] S.T. Chapman.
A Tale of Two Monoids: A Friendly Introduction to Nonunique Factorizations.

[2] P. Baginski and S. T. Chapman.
Arithmetic Congruence Monoids: A Survey.