A NOTE ON MASS COLLOQUIUM: MONOIDS AND MCNUGGETS

WILLIAM CHUANG

Abstract. The big picture, big idea (question) of this talk is to ask what numbers we can't order for a McNuggets, and what's the largest number of the set of these numbers? Furthermore, to find out the generalized solution of this question.

Contents

MASS Colloquium Meeting Details:
Speaker: Scott Chapman, Sam Houston State University
Room Number: 113 McAllister
Date: 11/16/2017
Time: 1:30pm - 2:30pm

1. Notations.

- $\mathbb{Z} = \{... - 3, -2, -1, 0, 1, 2, 3, ...\}$ these are integers.
- $\mathbb{N} = \{1, 2, 3, ...\}$ these are natural numbers.
- $\mathbb{N}_0 = \{0, 1, 2, 3, ...\}$ these are natural numbers with zero in a set.

Date: 11/16/2017.

So, those would be the three sets we are talking about.

2. Definitions.

These are two things that were covered in the Day one Number Theory. We will learn two things. The first thing we learn in number theory is prime numbers, and it's a very simple definition. Although the version of the definition we can use for the algebraic number theory is not the definition if we probably think of on top of our head. One meaning of prime which is probably we thought about in high schools is: positive integer greater than one is prime if and only if its only factors are one and itself. Now, the version of this the one that are going to more freely to be used in this talk is the second version of the definition which goes like this:

Definition

Prime. A positive integer $p > 1$ is *prime* if whenever $p|xy$ then either $p|x$ or $p|y$.

Here is a simplest version to write out the Fundamental Theorem of Arithmetic:

Theorem

The Fundamental Theorem of Arithmetic. Every integer $x > 1$ can be factored uniquely up to order as a product of prime integers.

We got to show two things: a. to show the integer can be factored as a product of primes which is a very good example of "well-ordering theorem". Then we got to argue that that factorization is prime up to order as a product of primes. That means there is a unique list of prime factors which is monotonically increasing such that that integer is a product of the list of primes.

The Fundamental Theorem of Arithmetic

Given a positive integer $x > 1$ there is a unique list of prime integers $p_1, p_2, p_3, ..., p_k$ with $p_1 \leq p_2 \leq ... \leq p_{k-1} \leq p_k$ such that

$$x = p_1 \cdot p_2 \cdot p_3 \cdot ... \cdot p_k.$$

Examples are our friends. So, here is an example

$$30 = 2 \cdot 3 \cdot 5 = 2 \cdot 5 \cdot 3 = 5 \cdot 2 \cdot 3 = 5 \cdot 3 \cdot 2 = 3 \cdot 2 \cdot 5 = 3 \cdot 5 \cdot 2.$$

My question: Is there is a unique factorization if the number field is not $\mathbb{Z}$, but like a set of all positive even integers.

The answer from the speaker: Yes, if you go to different system, you may not have a unique factorization. So, my advice is just hang on.

So, good we haven't done anything harder, so we just done number theory. In the following 2/3 of the talk we are going to take intergers and smash them down and look at the subsets of them. Talk about how will it look like to factor an integer in one of those subsets. Now, in order to do that, we are going to use a really simple number theory idea. So, the first part of the talk is based on the **congruence relations**. We will use the simple congruence relation over $\mathbb{Z}$ defined by

$$a \equiv b (\mod n)$$

if and only if

$$n | a - b \text{ in } \mathbb{Z}$$

Now, again there is a lot of different ways we can write this. For our purpose today, we will keep focusing on integers mod 4, and mod 6. So, again our goal is to keep things simple. We're not going to look at any thing mod 3193, or whatnot. To show something may go wrong with factorization, but at the same time it made things become interesting as well.

We are going to look at these two things: Let's consider two simple arithmetic sequences. This could be Day 1 in discrete math. We are looking two very simple arithmetic sequences (What does it mean for a sequence to be arithmetic? We start with a number, and we got everything else by adding every successor number by the same amount).

But there are not just an arithmetic sequences. They have some stronger properties. If we take any two elements of the first sequence, and multiply them together, we get back another element in this sequence. Why?

Well, assumed that we already knew a little bit about congruence. So, we take a number that is congruence, let's call it a, suppose it's congruent to 1 mod 4, now we take another number b which is also congruent 1 mod 4, so the result is still 1 mod 4. **So, that set of the**

sequence is multiplicative closed. This is also true for the second sequence. However, this is not always the case if we randomly write down an arithmetic sequence, it's not going to be arithmetic closed.

So, the first sequence start at one, and every successor number add up a four.

$$1, 5, 9, 13, 17, 21, 25, 29, 33, 37, 41, 45, 49, ...$$

It's a set of sequence congruence to 1 mod 4. It;s also called the **Hilber Monoid:**

$$= \{1 + 4k | k \in \mathbb{N}_0\} = 1 + 4\mathbb{N}_0.$$

What is a monoid?

> Definition
>
> **Monoid:** which is (1) closed under an associative binary operation and (2) has an identity element $I \in S$ such that for all $a \in S$, $Ia = aI = a$. But its elements don't need to have inverses.

There is a legend that "Hilbert used this monoid when he taught courses in Elementary Number Theory to convince students of the necessity of proving the unique factorization property of the integers."

In $1 + 4\mathbb{N}_0$ we have

$$21 \cdot 33 = 9 \cdot 77$$
$$(3 \cdot 7) \cdot (3 \cdot 11) = (3 \cdot 3) \cdot (7 \cdot 11)$$

It's clear that 9, 21, 33, and 77 can't be factored in $1 + 4\mathbb{N}_0$. However, 9, 21, 33, and 77 are not prime in the usual sense of the definition in $\mathbb{Z}$.

And the second sequence start at four, and every successor number add up a six.

$$4, 10, 16, 22, 28, 34, 40, 46, 52, 58, 64, 70, 76, 82, ... = 4 + 6\mathbb{N}_0$$

It's a set of sequence congruence to 0 mod 4. We obtain

$$70 \cdot 22 = 154 \cdot 10$$
$$(2 \cdot 5 \cdot 7) \cdot (2 \cdot 11) = (2 \cdot 7 \cdot 11) \cdot (2 \cdot 5)$$

It's clear that 70, 22, 154, and 10 can't be factored in $4+6\mathbb{N}_0$. However, 70, 22, 154, and 10 are not prime in the usual sense of the definition in $\mathbb{Z}$. By appending 1 to this sequence we derive a monoid **M**$= 4 + 6\mathbb{N}_0 \cup \{1\}$ which is known as **Meyerson's Monoid**.

It follows a basic observation: Both of these examples are extremely elementary in nature.

Additionally, we have a big goal: To convince you that factorization of elements into irreducibles in the second example is far more complicated similar factorizations in the first.

3. An Example in Almost Every Basic Abstract Algebra Textbook

Let $D = \mathbb{Z}[\sqrt{5}]$. In D, $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ represents a nonunique factorization into products of irreducibles in D. In order to understand this, we must understand units and noms in$D$. The previous examples avoid this problem.

4. New Notation

Let M be a commutative cancellative monoid written multiplicatively with identity element 1 and associated group of units $M^{\times}$. Let $M^{*} = M \setminus M^{\times}$. We use the usual conventions involving divisibility:

$$x|yM \iff xz = y \text{ for some } z \in M.$$

Definition

If $x|y$ and $y|x$ in M, then x and y are associates.

Let $x \in M^{*}$. Then we have: (1) **prime** if whenever $x|yz$ for x, y, and z in M, then either $x|y$ or $x|z$. (2) **irreducible (or an atom)** if whenever $x = yz$ for x, y, and z in M, then either $y \in M^{\times}$ or $z \in M^{\times}$.

$$x \text{ prime in } M \Rightarrow x \text{ irreducible in } M$$

but not conversely.

Definition

Set $A(M)$ = the set of irreducibles of M. If $M^{*} =< A(M) >$, then$M$ is called atomic.

Not all integral domains are atomic. For instance,

$$\mathbb{Z} + X\mathbb{Q}[X] = \{f(X) \in \mathbb{Q}[X] | f(0) \in \mathbb{Z}\}.$$

In this case, X cannot be factored as a product of irreducibles.

$$X = 2 \cdot \left(\frac{1}{2}X\right) = 2 \cdot 3 \cdot \left(\frac{1}{6}X\right) = \ldots$$

5. How Things Factor in $1 + 4\mathbb{N}_0$

Lemma

The element x is irreducible in $1 + 4\mathbb{N}_0$ if and only if x is either

- p where p is a prime and $p \equiv 1(\mod 4)$, or
- $p_1 p_2$ where p_1 and p_2 are primes congruent to $3 \mod 4$.

x is prime if and only if it is of type 1.

Definition

In general, a monoid with this property, i.e.,

$$x = \alpha_1 ... \alpha_s = \beta_1 ... \beta_t$$

for α_i and β_j in $A(M)$, then $s = t$, is called half-factorial.

Theorem

There is a map, $\phi : \mathbb{Z}\sqrt{-5} \to 1 + 4\mathbb{N}_0$ which preserves lengths of factorizations into products of irreducibles. It follows $\mathbb{Z}[\sqrt{-5}]$ is half-factorial.

Meyerson's Monoid doesn't satisfy the half-factorial property: $100000 = 10^4 = 250 \cdot 10 \cdot 4$. And, $250 = 2 \cdot 5^3 \equiv 4(\mod 6)$ is irreducible in M.

Definition

Let M be an atomic monoid. Define for $x \in M^*$ $L(x) =$ the longest length of an irreducible factorization of x in M, $I(x) =$ the shortest length of an irreducible factorization of x in M, and

$$\rho = \frac{L(x)}{I(x)}$$

to be their quotient. $\rho(x)$ is called the elasticity of x.

Definition

$$\rho(M) = \sup\{\rho(x) | x \in M^*\}$$

is called the elasticity of M. If there exists an $x \in M^*$ such that $\rho(M) = \rho(x) = \frac{L(x)}{I(x)}$, then we say that the elasticity of M is accepted.

Proposition

(W. Meyerson, 2003)

- If $x \in M$, then $1 \leq \rho(x) < 2$.
- $\rho(M) = 2$

The Punch Line

M is an atomic monoid with elasticity 2 and the elasticity is **not accepted**.

6. The Chicken McNugget Problem

What numbers of Chicken McNuggets can be ordered using only packs with 6, 9, or 20 pieces?

Definition

Positive integers that satisfying the Chicken McNugget problem are know as McNugget numbers. In particular, if n is a McNugget number, then there is an ordered triple (a, b, c) of non-negative integers such that

$$6a + 9b + 20c = n$$

(a, b, c) is a McNugget expansion of n. Since both $(3, 0, 0)$ and $(0, 2, 0)$ are McNugget expansions of 18. It's clear that McNugget expansions are not unique. This phenomenon will be the central focus of the remainder of the talk.

The following are positive integers that don't have McNugget expansion:

$$1, 2, 3, 4, 5, 7, 8, 10, 11, 13, 14, 16, 17, 19, 22, 23, 25, 28, 31, 34, 37, 43.$$

Proposition

Any positive integers greater than 43 is a McNuggets number.

So, 43 is the largest McNuggets number we can't order.

7. Generalization

Given a set of k objects with predetermined values $n_1, n_2, ..., n_k,$. WHat possible values of n can have from combinations of these objects?

Thus if a value of n can be derived, then there is an ordered k-tuple of nonnegative integers $(x_1, ..., x_k)$ which satisfy the linear diophatine equation

$$n = x_1n_1 + x_2n_2 + ... + x_kn_k.$$

We view this in a more algebraic manner. Given integers $n_1, ..., n_k > 0$, set

$$< n_1, ..., n_k >= \{x_1n_1 + x_2n_2 + ... + x_kn_k | x_1, ..., x_k \in \mathbb{N}_0\}.$$

Monoids of nonnegative integers under addition, like the one above, are known as numerical monoids, and $n_1, ..., n_k$ are called generators. The numerical monoids $< 6, 9, 20 >$ is called the Chicken McNugget monoid.

Since this talk is a little bit short on time, so the speaker skipped some slides, and only covered the following contents:

8. A General Result.

Proposition

Given $< n_1, n_2, ..., n_k >$, then $\rho(< n_1, n_2, ..., n_k >) = \frac{n_k}{n_1}$.

Proof. Let $n \in < n_1, ..., n_k >$ and suppose $n = x_1n_1 + ... + x_ka_k$. Then

$$\frac{n}{n_k} = \frac{n_1}{n_k}x_1 + ... + \frac{n_k}{n_k}x_k \leq x_1 + ... + x_k \leq \frac{n_1}{n_1}x_1 + ... + \frac{n_k}{n_1}x_k = \frac{n}{n_1}.$$

It follows that $L(n) \leq \frac{n}{n_1}$ and $l(n) \geq \frac{n}{n_k}$ for all $n \in < n_1, ..., n_k >$, from which $\rho(< n_1, ..., n_k >) \leq \frac{n_k}{n_1}$. Also, $\rho(< n_1, ..., n_k >) \geq \rho(n_1n_k) = \frac{n_k}{n_1}$, so we have equality. □

Proposition

The elasticity of the Chicken McNugget Monoid is $\frac{20}{6} = \frac{10}{3}$.

9. References of the talk

[1] A Tale of Two Monoids: A Friendly Introduction to the Theory of Non-unique Factorization, Mathematics Magazine 87(2014), 163173.

[2] Factorization in the Chicken McNugget Monoid, preprint (with Chris ONeill).