Embrace Multisets: prime factorization (part I)

Navid Roux

Last updated on Jan 1, 2021 · 18 min read ·

Abstract

On natural numbers, the concepts of prime factorization, divisibility, greatest common divisor (gcd), and least common multiple (lcm) are all fundamental to discrete math. Mathematics and Computer Science students learn about them in their first semesters; if not even earlier at school. Usually lesser known are multisets and their applications. This article is the first of a series devoted to highlighting multisets. Here, we define multisets from the ground up, and show the usefulness of identifying natural number with their multiset of prime factors. That way, multiplication/division become multiset union/difference, and gcd/lcm become multiset intersection/symmetric difference.

To express these correspondences algebraically, we recap the theory of lattices and obtain a lattice-isomorphism $L_{\mathbb{N}} \cong M_{\mathbb{P}^+}$ between the division lattice on natural numbers and the lattice of finite multisets over prime numbers with multiplicities in $\mathbb{N}_{\geq 0}$. By generalizing the right-hand side to the superlattice $M_{\mathbb{P}}$, now multiplicities in $\mathbb{Z}$, we recover a useful generalization of the left-hand side: a division lattice on $\mathbb{Q}^+$. In particular, we prove the meet and join operations on $M_{\mathbb{P}}$ to correspond on $\mathbb{Q}^+$ to generalized variants of gcd and lcm fulfilling

$$\gcd\left(\frac{a}{b}, \frac{c}{d}\right) = \frac{\gcd(a,c)}{\operatorname{lcm}(b,d)}$$

$$\operatorname{lcm}\left(\frac{a}{b}, \frac{c}{d}\right) = \frac{\operatorname{lcm}(a,c)}{\gcd(b,d)}$$

for reduced fraction representations $\frac{a}{b}$ and $\frac{c}{d}$.

Table of Contents

1 Introduction

The central idea is the following. Every natural number $n \geq 2$ can be factored into its prime factors. Since multiplicity of prime factors is crucial, but order is not, the prime factorization of a natural number forms a multiset. For example, we have $18 = 2 \cdot 3^2$ and can thus identify 18 with the multiset $\{2^{(1)}, 3^2\}$, where the exponents denote multiplicities, i.e., 2 occurs once and 3 occurs twice. We can identify 0 with the empty multiset. Overall, this identification gives rise to the bijections below between the natural numbers $\mathbb{N} = \{1, 2, \ldots\}$ and the set $M_{\mathbb{P}^+}$ of finite multisets with multiplicities in $\mathbb{N}_{\geq 0}$:

$$\mathrm{fact}\colon \mathbb{N} \to M_{\mathbb{P}^+}$$
$$\mathrm{mult}\colon M_{\mathbb{P}^+} \to \mathbb{N}$$

Here, fact maps every natural number to its prime factorization, and mult maps every multiset of primes to a natural number by multiplying, counting multplicities.

The article is driven by the following questions: How do common operations like multiplication, division, greatest common divisor (gcd), and least common multiple (lcm) look like on the side of $M_{\mathbb{P}^+}$? Which operations/what kind of algebraic structure does fact preserve?

We will see that gcd, lcm of natural numbers correspond to multiset intersection, and symmetric difference; all counting multiplicities in a suitable manner. Algebraically, both operation pairs induce lattice structures: $(\mathbb{N}, \gcd, \mathrm{lcm})$ is known as the "division lattice", and $(M_{\mathbb{P}^+}, \cap, \Delta)$ with intersection and symmetric difference is also a lattice, which we will introduce. Our main theorem proves these lattices to be isomorphic by means of the bijections above.

Overview. We rigorously define multisets and their operations in Section 2.1. In Section 2.2 we introduce lattices generally and especially the division lattice on $\mathbb{N}$, and variants of multiset lattices. Our main theorem in Section 3 proves the lattices to be isomorphic, and in Section 4 we generalize the result. We conclude in Section 5.

2 Preliminaries

We work in the usual metamathematical layer and remain vague about our foundation. However, we presuppose some kind of set theory, e.g. ZF. To avoid confusion with multisets later, let us refer to sets from that set theory as *classical sets*, and to multisets always as *multisets*.

2.1 Multisets

2.1.1 Definitions

Classical sets are "collections of objects" without duplicates and without order. Multisets, which have been folklore for long time, lift the first requirement and instead attach to every element a *multiplicity*. Classical sets only allow multiplicities in $\{0, 1\}$ to occur, i.e., either an object is an element of a classical set or it is not. When we generalize to multiplicities in $\mathbb{N}$, $\mathbb{Z}$, or even $\mathbb{R}$, we get different variations. For this article, the integers are sufficient.

> **Definition 2.1 [1]:** A **multiset** is a pair (U, κ_U), where U is a classical set and $\kappa_U\colon U \to \mathbb{Z}$ a function.
>
> For $x \in U$, we say x has multiplicity $\kappa_U(x)$, or equivalently, x occurs $\kappa_U(x)$ times in (U, κ_U).
>
> If it is clear from context, we write U instead of (U, κ_U).

Every classical set S can be identified with the multiset $(S, s \mapsto 1)$.

Consider the multiset on $U = a, b, c$ in which a occurs once, b twice, and c -4 times. Formally, we have $\kappa_U = \{a \mapsto 1, b \mapsto 2, c \mapsto -4\}$. In the following we adopt an easier notation and write $\{a^{(1)}, b^{(2)}, c^{(-4)}\}$. For convenience and formal correctness of later proofs, we identify multisets U_1 and U_2 if κ_1 and κ_2 agree on those elements where at least one of them is non-zero. For instance, this makes $\{a^{(0)}\} = \{x^{(0)} \mid x \in \mathbb{R}\} = \varnothing$.

Definition 2.2: Given two multisets U_1, U_2, we define

- the union

$$U_1 \cup U_2 := (U_1 \cup U_2, x \mapsto \kappa_1(x) + \kappa_2(x))$$

- the intersection

$$U_1 \cap U_2 := (U_1 \cup U_2, x \mapsto \min\{\kappa_1(x), \kappa_2(x)\})$$

- the symmetric difference

$$U_1 \Delta U_2 := (U_1 \cup U_2, x \mapsto \max\{\kappa_1(x), \kappa_2(x)\})$$

- the negative

$$-U_1 := (U_1, x \mapsto -\kappa_1(x))$$

- the difference

$$U_1 - U_2 := (U_1 \cup U_2, x \mapsto \kappa_1(x) - \kappa_2(x))$$

where we take $\kappa_1(x)$ and $\kappa_2(x)$ to be 0 if x lies outside their domain, respectively.

For example, suppose a, b, c are pairwise distinct urelements from our set theory. Then,

- $\{a^{(2)}, b^{(4)}\} \cup \{a^{(-5)}\} = \{a^{(-3)}, b^{(4)}\}$
- $\{a^{(2)}, b^{(3)}\} \cap \{a^{(10)}, b^{(-5)}\} = \{a^{(2)}, b^{(-5)}\}$
- $\{a^{(2)}, b^{(3)}\} \Delta \{a^{(10)}\} = \{a^{(10)}, b^{(3)}\}$

Definition 2.3: We say U is finite if $\kappa_U(x) \neq 0$ only for finitely many x.

Definition 2.4 (Multisets on a Universe): Let X be a classical set. Define M_X be the classical set of all finite multisets on X. Define M_{X^+} be the classical set of all finite multisets on X with only non-negative multiplicities.

2.1.2 Prime Factorization as a Multiset

For the rest of this article, let $\mathbb{N} = \{1, 2, \ldots\}$ denote the natural numbers *without* zero and $\mathbb{P} = \{2, 3, 5, \ldots\}$ the prime numbers. Prime factorization allows us to factor every natural number $n \geq 2$ into its prime factors. For example, we can factor $18 = 2 \cdot 3^2$ and since this representation is unique up to order, we can see it as the multiset $\{2^{(1)}, 3^{(2)}\}$.

Overall, this gives rise to bijections

$$\mathrm{fact}: \mathbb{N} \to M_{\mathbb{P}^+}$$
$$\mathrm{mult}: M_{\mathbb{P}^+} \to \mathbb{N}$$

where fact maps every natural number to its prime factorization, and mult maps every multiset of primes to a natural number by multiplying, counting multplicities. By convention, we set $\mathrm{fact}(0) = \varnothing$ and $\mathrm{mult}(\varnothing) = 1$.

As an example, consider $6 \sim \{2^{(1)}, 3^{(1)}\} = \mathrm{fact}(6)$ and $14 \sim \{2^{(1)}, 7^{(1)}\} = \mathrm{fact}(14)$. We have the following identities:

- multiplication corresponds to multiset union:

$$\mathrm{fact}(6 \cdot 14) = \mathrm{fact}(6) \cup \mathrm{fact}(14) \sim 84$$

- gcd corresponds to multiset intersection:

$$\mathrm{fact}(\gcd(6, 14)) = \mathrm{fact}(6) \cap \mathrm{fact}(14) \sim 2$$

- lcm corresponds to multiset symmetric difference:

$$\mathrm{fact}(\mathrm{lcm}(6, 14)) = \mathrm{fact}(6) \Delta \mathrm{fact}(14) \sim 42$$

These identities hold in general for all natural numbers. They express that fact respects multiplication, gcd, and lcm as operations (on $\mathbb{N}$), and translates them into union, intersection, and symmetric difference, respectively.

Remark 2.5: The division $\frac{a}{b}_{\mathbb{N}}$ of two natural numbers *over* $\mathbb{N}$ corresponds to multiset difference only if its result is a natural number again. For example,

$$\mathrm{fact}\left(\frac{14}{2}\right) = \mathrm{fact}(14) - \mathrm{fact}(2)$$

but, depending on your definition, $\frac{14}{6}_{\mathbb{N}} = 2$, whereas $\mathrm{fact}(14) - \mathrm{fact}(6)$ would even contain elements with negative multiplicities.

The rest of this article can be understood as an algebraic description of how nicely behaved these bijections are. In Section 2.2, we introduce lattices and equip $\mathbb{N}$ and $M_{\mathbb{P}^+}$ with lattice structures. Then, our main theorem in Section 3 shows that the resulting lattices are isomorphic by the very maps from above. Finally, we generalize the theorem in Section 4 to the case where we allow negative multiplicities in our multisets.

2.1.3 Technical Lemmas

In the following, we collect some technical lemmas we later need to prove our main theorems. (If you are interested in algebra, you might like the below lemma on sign decomposition.)

Lemma 2.6:

1. Union, intersection, symmetric difference are commutative and associative operations.
2. The negative is an involution.
3. $U_1 - U_2 = U_1 \cup (-U_2)$
4. $U_1 \Delta U_2 = (U_1 \cup U_2) - (U_1 \cap U_2)$

Click for proof

1. Immediate by definition.
2. Immediate by definition.
3. Immediate by definition.
4. We have to show

$$\max\{\kappa_1(x), \kappa_2(x)\} = (\kappa_1(x) + \kappa_2(x)) - \min\{\kappa_1(x), \kappa_2(x)\}.$$

This follows by case analysis with cases $\kappa_1(x) < \kappa_2(x)$, $\kappa_1(x) \geq \kappa_2(x)$.

Generally in mathematics, [involutions often go hand-in-hand with “decomposition” theorems](), as is the case here:

Lemma 2.7 (Sign Decomposition): Let U be a multiset, then

$$U = U^+ - U^-$$

where $U^+ = \{x \in U \mid \kappa_U(x) > 0\}$ is the positive part and $U^- = \{x \in U \mid \kappa_U(x) < 0\}$ the negative part.

Lemma 2.8: 1. $U_1 \cap U_2 = -(-U_1 \Delta - U_2)$ and $U_1 \Delta U_2 = -(-U_1 \cap -U_2)$ 2. $U_1 \cap (U_2 \Delta U_3) = (U_1 \cap U_2) \Delta (U_1 \cap U_3)$ 3. $U_1 \Delta (U_2 \cap U_3) = (U_1 \Delta U_2) \cap (U_1 \Delta U_3)$

Click for proof

1. Immediate by general property $\min\{a, b\} = -\max\{-a, -b\}$.
2. We have to show

$$\begin{aligned}&\min\{\kappa_1(x), \max\{\kappa_2(x), \kappa_3(x)\}\}\\ =&\max\{\min\{\kappa_1(x), \kappa_2(x)\}, \min\{\kappa_1(x), \kappa_3(x)\}\}.\end{aligned}$$

   This follows by case analysis on the 6 cases of all total orders possible on $\{\kappa_1(x), \kappa_2(x), \kappa_3(x)\}$.
3. This following by "dualizing" exploiting property 4, applying property 5, and transporting back using property 4 again:

$$\begin{aligned}&U_1\Delta(U_2 \cap U_3)\\ =&-(-U_1 \cap -(U_2 \cap U_3)) \quad \text{by prop. 4}\\ =&-(-U_1 \cap (-U_2\Delta - U_3)) \quad \text{by prop. 4}\\ =&-((-U_1 \cap -U_2)\Delta(-U_1 \cap -U_3)) \quad \text{by prop. 5}\\ =&-(-(U_1\Delta U_2)\Delta - (U_1\Delta U_3)) \quad \text{by prop. 4}\\ =&(U_1\Delta U_2) \cap (U_1\Delta U_3) \quad \text{by prop. 4 and - involution}\end{aligned}$$

■

We do *not* have a a distributive law between operations $\cup$ and $\cap$, however, we have one for them in case of sign decompositions:

Lemma 2.9: Let U and V be multisets, then

- $$U \cap V = (U^+ \cap V^+) - (U^-\Delta V^-)$$
- $$U\Delta V = (U^+\Delta V^+) - (U^- \cap V^-)$$

Proof: to be done, the second claim follows by duality. ■

2.2 Lattices

Lattices are algebraic structures that, intuitively, resemble real-world lattices. Figure 1 depicts one exemplary lattice, which we will use to motivate the formal definition of mathematical lattices.

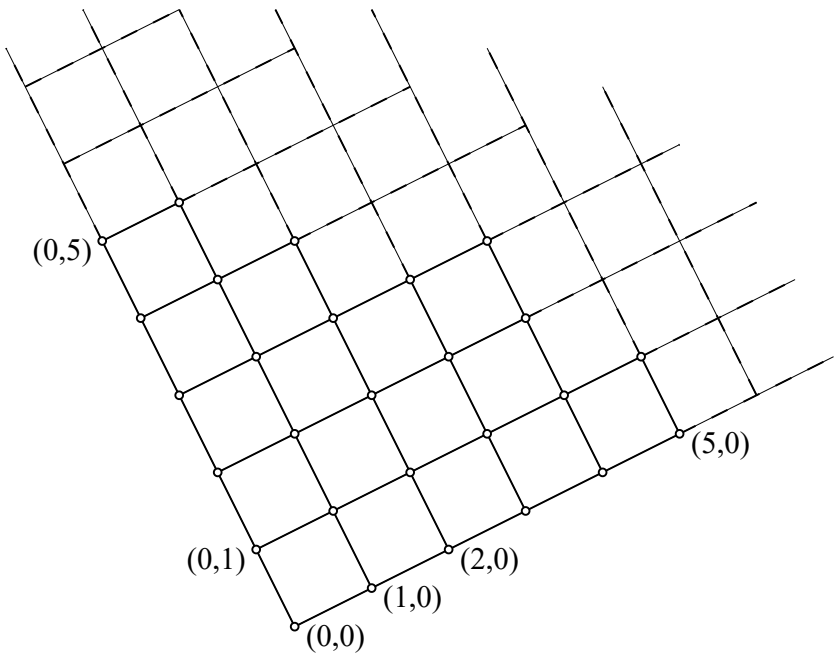

Fig. 1: An exemplary lattice (taken from here under CC0 license)

Intuitively, a real-world lattice has two characteristics: its collection of nodal points and its mesh structure. How we encode this in mathematics? We can encode the former as a classical set L, and in Figure 1 we have $L = \mathbb{N}_0 \times \mathbb{N}_0$. To represent the mesh structure, we could pick graphs on L, however real-world lattices usually fulfill much more structure, as elaborated on below. Hence, picking graphs would be too generous, and we instead encode the mesh structure by two commutative and associative operations $\vee, \wedge\colon L \times L \to L$ called *meet* and *join*. We motivate their semantics in context of Figure 1 next.

Imagine you are standing on $(0, 1)$ and your friend on $(5, 0)$. You both would like to gather at a common point, but both of you can only walk downwards. What is the *greatest lower bound* (point) suitable to gather at such that both of you only travel the minimum distance necessary? It is $(5, 0)$, and that would be the meet $(0, 1) \vee (5, 0)$. Now on the contrary, imagine you both could only walk upwards from $(0, 1)$ and $(5, 0)$ on, respectively. What is the *lowest upper bound* (point) suitable to gather at such that both of you only travel the minimum distance necessary? It is $(5, 1)$, and that would be the join $(0, 1) \wedge (5, 0)$. Formally we define $(a, b) \vee (c, d) = (\min\{a, c\}, \min\{b, d\})$ and $(a, b) \wedge (c, d) = (\max\{a, c\}, \max\{b, d\})$.

With this imaginery, it is clear that the meet and join should be commutative operations. Perhaps slightly less clear is that we demand associativity, too. For that, imagine three people p_1, p_2, p_3 would like to gather, e.g., by only walking upwards. Then they should be a unique gathering point, independent of whether they gather up "in parallel" ($p_1 \wedge p_2 \wedge p_3$), by the first two people gathering first ($(p_1 \wedge p_2) \wedge p_3$), or by the latter two people gathering first ($p_1 \wedge (p_2 \wedge p_3)$).

Thus, in contrast to directed graphs, lattices possesses meets and joins *for all* two points.

Definition 2.10: A lattice is a structure $(L, \vee, \wedge)$ consisting of a classical set L and two commutative and associative operations $\vee, \wedge \colon L \times L \to L$ fulfilling the absorption laws

$$a \vee (a \wedge b) = a$$
$$a \wedge (a \vee b) = a$$

We leave it to the reader to motivate and prove the absorption laws in context of Figure 1. TODO: other variable names.

Remark 2.11: Lattices can be equivalently described from an order-theoretical perspective: lattices are partially ordered sets where each two-element subset $\{a, b\}$ has a lowest upper bound (join) and a greatest lower bound (meet). We refer to Wikipedia for an axiomatization of these bounds. It often helps to think of a lattice in terms of both the meet and join operations as well as the partial order associated to it. The example lattice from above corresponds to $\mathbb{N}_0 \times \mathbb{N}_0$ partially ordered by

$$(a, b) \sqsubseteq (c, d) \Leftrightarrow (a \sqsubseteq c) \text{ and } (b \sqsubseteq d).$$

In particular, lattices are usually drawn as Hasse diagrams as is done in Figure 1: every upwards edge $x - y$ stands for $x \sqsubseteq y$.

2.2.1 Divison Lattice on $\mathbb{N}$

By $\mathbb{N} = \{1, 2, \ldots\}$ let us abbreviate the natural numbers *without 0*. Given two natural numbers n and m, we define the well-known divisibility relation

$$n \mid m \Leftrightarrow \exists q \in \mathbb{N}. n \cdot q = m$$

This is a partial order, and moreover for every two-element subset, the greatest common divisor and the least common multiple serve as meets and joins, respectively.

Lemma 2.12 (Division Lattice on $\mathbb{N}$): $L_{\mathbb{N}} = (\mathbb{N}, \gcd, \operatorname{lcm})$ is a lattice.

See Figure 2 for a partial visualization of $L_{\mathbb{N}}$ as a Hasse diagram. For example, the meet of 18 and 12 is $6 = \operatorname{lcm}(18, 12)$, and 6 is precisely the nearest point you can reach from both 18 and 12 by only walking downards. Also, the join of 2 and 5 is $10 = \gcd(2, 5)$, and 10 is precisely the nearest point you can reach from both 2 and 5 by only walking the edges upwards.

Remark 2.13: In the division lattice on $\mathbb{N}$, the element 1 has the property that it divides every other number, i.e., order-theoretically $1 \sqsubseteq n$ for all n. Lattices that possess such a *bottom element* are called *lower-bounded lattices*.

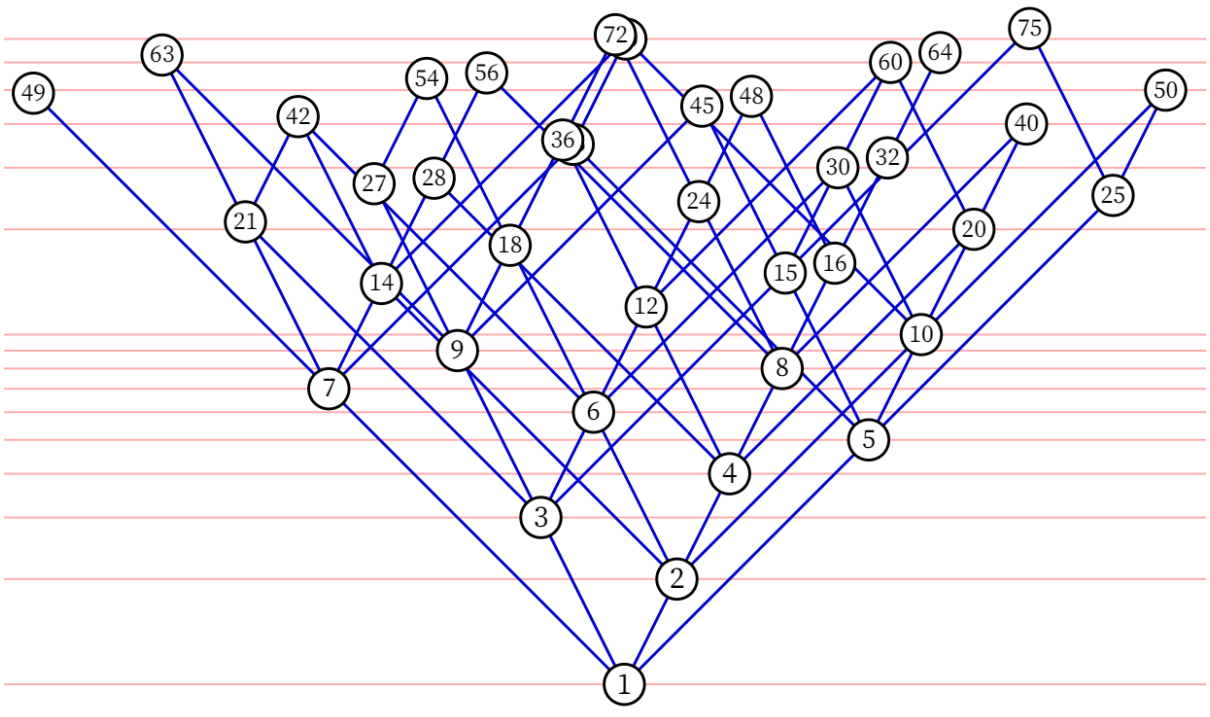

Fig. 2: Parts of the infinite division lattice (taken from this interactive website by Bryan Gin-ge Chen)

2.2.2 Multiset Lattices

Theorem 2.14 (Multiset Lattices): Let X be a classical set.

1. $(M_X, \cap, \Delta)$ is a distributive lattice.
2. $(M_{X^+}, \cap, \Delta) \subseteq M_X$ is a distributive sublattice with bottom $\varnothing$

We leave the proof as an exercise to the reader.

Remark 2.15: We described both M_X and M_{X^+} algebraically. From an order-theoretic perspective, these lattices are ordered via

$$U_1 \sqsubseteq U_2 \Leftrightarrow \forall x \in U_1.\ \kappa_{U_1}(x) \leq \kappa_{U_2}(x)$$

Remark 2.16: Ignoring size issues of the chosen set theory, the class of all multisets would form a lattice, too.

3 Divison Lattice on $\mathbb{N} \cong$ Positive Finite Multisets over $\mathbb{P}$

With the preliminaries done, we can finally state and prove our main theorem that via prime factorization gcd and lcm correspond to multiset intersection and symmetric difference:

Theorem 3.1: $M_{\mathbb{P}^+} \cong L_{\mathbb{N}}$ as lower-bounded lattices, where

- $\mathrm{fact}\colon L_{\mathbb{N}} \to M_{\mathbb{P}^+}$ maps natural numbers to their prime factorization
- $\mathrm{mult}\colon M_{\mathbb{P}^+} \to L_{\mathbb{N}}$ maps multisets of primes to their multiplication

Moreover, multiplication is preserved and reflected as multiset union:

$$\begin{aligned}\mathrm{fact}(a \cdot b) &= \mathrm{fact}(a) \cup \mathrm{fact}(b)\\ \mathrm{mult}(A \cup B) &= \mathrm{mult}(A) \cdot \mathrm{mult}(B)\end{aligned}$$

Click for proof

We noted above that fact and mult are bijections and inverses of each other. Hence, it suffices to show that fact is a homomorphism of lower-bounded lattices and preserves multiplication.

Let us first recall some helper lemmas from elementary number theory. For $a \in \mathbb{N}$, writing $\Pi_{p \in \mathbb{P}}\ p^{p_a}$ to refer to its prime factorization, we have the identities below.

$$\begin{aligned}\gcd(a,b) &= \Pi_{p\in\mathbb{P}}\ p^{\min\{p_a,p_b\}}\\ \operatorname{lcm}(a,b) &= \Pi_{p\in\mathbb{P}}\ p^{\max\{p_a,p_b\}}\\ a\cdot b &= \Pi_{p\in\mathbb{P}}\ p^{p_a+p_b}\end{aligned}$$

It immediately follows that fact preserves multiplication:

$$\begin{aligned}\mathrm{fact}(a\cdot b) &= \mathrm{fact}(\Pi_{p\in\mathbb{P}}\ p^{p_a+p_b})\\ &= (p\colon\mathbb{P})\mapsto p_a+p_b\\ &= \mathrm{fact}(A)\cup\mathrm{fact}(B)\end{aligned}$$

Moreover, it perserves meets,

$$\begin{aligned}\mathrm{fact}(\gcd(a,b)) &= \mathrm{fact}\left(\Pi_{p\in\mathbb{P}}\ p^{\min\{p_a,p_b\}}\right)\\ &= (p\colon\mathbb{P})\mapsto \min\{p_a,p_b\}\\ &= \mathrm{fact}(A)\cap\mathrm{fact}(B)\end{aligned}$$

and joins:

$$\begin{aligned}\mathrm{fact}(\operatorname{lcm}(a,b)) &= \mathrm{fact}\left(\Pi_{p\in\mathbb{P}}\ p^{\max\{p_a,p_b\}}\right)\\ &= (p\colon\mathbb{P})\mapsto \max\{p_a,p_b\}\\ &= \mathrm{fact}(A)\Delta\mathrm{fact}(B)\end{aligned}$$

Finally fact also preserves the bottom element: $\mathrm{fact}(1)=\varnothing$. ■

■

4 Division lattice on $\mathbb{Q}^+ \cong$ Finite Multisets over $\mathbb{P}$

We have seen $M_{\mathbb{P}^+}\cong L_{\mathbb{N}}$, i.e., how the lattice of positive finite multisets over prime numbers is isomorphic to the division lattice on $\mathbb{N}$. What happens if we now relax (extend) the LHS to the superlattice $M_{\mathbb{P}}$ with negative multiplicities allowed? Is there also a corresponding superlattice of $L_{\mathbb{N}}$ that is isomorphic to $M_{\mathbb{P}}$? Indeed there is, and a natural generalization of $L_{\mathbb{N}}$ to a division lattice $L_{\mathbb{Q}^+}$ on $\mathbb{Q}^+$ fits the bill, where $\mathbb{Q}^+=\{q\in\mathbb{Q}\mid q>0\}$ are the positive rational numbers. In particular, this yields *meaningful* extensions of $\gcd$ and lcm to $\mathbb{Q}^+$.

Before defining $L_{\mathbb{Q}^+}$ and proving $M_{\mathbb{P}}\cong L_{\mathbb{Q}^+}$, let us begin with building some intuition as to why that should be the case. Recall how we bijected positive finite multisets over $\mathbb{P}$ with natural numbers: we mapped a multiset A to the multiplication $\Pi_{p\in\mathbb{P}}\ p^{\kappa_A(p)}$. What happens if we allowed negative multiplicities, i.e., $\kappa_A(p)<0$? Nothing, really; multiplying prime factors raised to possibly negative exponents still makes sense. For example, we would map $\{5^{(1)},2^{(-1)},3^{(-2)}\}$ to $5^1\cdot 2^{-1}\cdot 3^{-2}=\frac{5}{18}$. Hence, we represent fractions as multisets with prime factors of their numerator becoming positive elements and prime factors of their denominator becoming negative elements. To ensure uniqueness, we always choose the reduced fraction representation.

Definition 4.1 (Prime Factorization of Rational Numbers): Let $r\in\mathbb{Q}^+$ be a rational number with reduced fraction representation $\frac{a}{b}$ with $a,b\in\mathbb{N}$. Let $a=p_1^{a_1}\cdot\ldots\cdot p_n^{a_n}$ and $b=q_1^{b_1}\cdot\ldots\cdot q_m^{b_m}$ be the prime factorizations of a and b with $n,m\geq 0$. Then, we call

$$r=p_1^{a_1}\cdot\ldots\cdot p_n^{a_n}\cdot q_1^{-b_1}\cdot\ldots\cdot q_m^{-b_m}.$$

the **prime factorization** of r.

By convention, we set $1=\langle\text{empty product}\rangle$.

This allows identifying rational numbers with multisets of their prime factors. In contrast to earlier discussions, we must now allow multiplicities in $\mathbb{Z}$.

Definition 4.2 (Lattice on $\mathbb{Q}^+$): Define the lattice $L_{\mathbb{Q}^+} = (\mathbb{Q}^+, \gcd, \operatorname{lcm})$ with

- $$\gcd\left(\frac{a}{b}, \frac{c}{d}\right) = \frac{\gcd(a,c)}{\operatorname{lcm}(b,d)}$$
- $$\operatorname{lcm}\left(\frac{a}{b}, \frac{c}{d}\right) = \frac{\operatorname{lcm}(a,c)}{\gcd(b,d)}$$

Here, we overload the names of $\gcd$ and lcm as the functions defined here agree with the previously defined functions when restricted to $\mathbb{N}$. We leave proving the lattice properties to the reader.

For example, we have $\gcd(\frac{3}{8}, \frac{2}{5}) = \frac{\gcd(3,2)}{\operatorname{lcm}(8,5)} = \frac{1}{40}$. Moreover, $\operatorname{lcm}(\frac{3}{8}, \frac{2}{5}) = \frac{\operatorname{lcm}(3,2)}{\gcd(8,5)} = \frac{6}{1}$, and indeed, 6 is the first common multiple of both $\frac{3}{8}$ and $\frac{2}{5}$.

Theorem 4.3: $M_X \cong L_{\mathbb{Q}^+}$ as lattices, where

- $\operatorname{fact}\colon L_{\mathbb{Q}^+} \to M_{\mathbb{P}}$ maps rational numbers to their prime factorization
- $\operatorname{mult}\colon M_{\mathbb{P}} \to L_{\mathbb{Q}^+}$ maps multisets of primes to their multiplication

Moreover, multiplication and division are preserved and reflected as follows:

$$\begin{aligned}\operatorname{fact}(a \cdot b) &= \operatorname{fact}(a) \cup \operatorname{fact}(b)\\ \operatorname{fact}\left(\frac{a}{b}\right) &= \operatorname{fact}(a) - \operatorname{fact}(b)\end{aligned}$$

$$\operatorname{mult}(A \cup B) = \operatorname{mult}(A) \cdot \operatorname{mult}(B)$$

$$\operatorname{mult}(A - B) = \frac{\operatorname{mult}(A)}{\operatorname{mult}(B)}$$

Again, we overload the names of mult and fact.

Click for proof

We noted above that fact and mult are bijections and inverses of each other. Hence, it suffices to show that fact is a homomorphism of lower-bounded lattices and preserves multiplication as well as division.

Similar to the proof of Theorem 3.1, let us first recall some (generalized) helper lemmas from elementary number theory. For $u \in \mathbb{Q}^+$, writing $\Pi_{p\in\mathbb{P}}\, p^{p_u}$ to refer to its prime factorization, we have the identities below for $u, v \in \mathbb{Q}^+$.

$$\begin{aligned}u \cdot v &= \Pi_{p\in\mathbb{P}}\, p^{p_u + p_v}\\ \frac{u}{v} &= \Pi_{p\in\mathbb{P}}\, p^{p_u - p_v}\end{aligned}$$

From these identities, it immediately follows that fact preserves multiplication and division. Moreover, it preserves meets: let $u, v \in \mathbb{Q}$ with reduced fraction representations $u = \frac{u^+}{u^-}$ and $v = \frac{v^+}{v^-}$. Then we have:

$$\begin{aligned}
& \operatorname{fact}(\gcd(u,v)) \\
=\ & \operatorname{fact}\left(\frac{\gcd(u^+, v^+)}{\operatorname{lcm}(u^-, v^-)}\right) \\
=\ & \operatorname{fact}(\gcd(u^+, v^+)) - \operatorname{fact}(\operatorname{lcm}(u^-, v^-)) \\
=\ & (\operatorname{fact}(u^+) \cap \operatorname{fact}(v^+)) - (\operatorname{fact}(u^-) \Delta \operatorname{fact}(v^-)) && \text{(iv)} \\
=\ & (\operatorname{fact}(u)^+ \cap \operatorname{fact}(v)^+) - (\operatorname{fact}(u)^- \Delta \operatorname{fact}(v)^-) && \text{(v)} \\
=\ & \operatorname{fact}(u) \cap \operatorname{fact}(v) && \text{(vi)}
\end{aligned}$$

To arrive at line (iv), we used that Theorem 3.1 already established fact being a lattice homomorphism on the sublattice $L_{\mathbb{N}}$. For line (v), we used the sign decomposition of multisets from Lemma 2.7, and for line (vi) we used Lemma 2.9.

Preservation of joins is proved analogously. ■

5 Conclusion

Our goal was to identify natural numbers with their multisets of prime factors and to see which algebraic structure transports across this identification.

We defined multisets and recapped lattices. Our main theorem captured…

Future work: what is multiplication and division on top of lattice structure?

TODO

> We note that $(M_{\mathbb{P}}, \cup, -)$ does *not* form a lattice, as one might think from these equations. Is there a name for the structure noted in this remark, though?

TODO: Delta has wrong spacing because it's not a binary operator for tex

TODO: gcd, lcm visually with multisets

Divison Lattice on all Z or Q with negative number == coproduct with lattice somehow?

https://observablehq.com/@bryangingechen/divisibility-lattice

TODO: answer here: https://math.stackexchange.com/questions/151081/gcd-of-rationals

1. D Loeb, "Sets with a negative number of elements" https://www.sciencedirect.com/science/article/pii/0001870892900119?via%3Dihub ^

university math

Navid Roux

Computer Science M. Sc. Student

Academically interested in formal systems for knowledge representation; recreationally in love with sports.

Related

- Embrace Multisets: Lattice-Ordered Multisets
- Leverage Multisets to your Advantage
- Diagram Operators
- FrameIT
- Presentation of "Diagram Operators in a Logical Framework" at LFMTP 2020