

THE PROPOSITIONAL LATTICE OF DIVISIBILITY AND BEAL'S CONJECTURE

Alexander Bolotin*

Open University of Israel

Abstract

This article is devoted to the lattice-theoretic analysis of Beal's conjecture. We discuss whether this conjecture is deducible from the laws of logic of divisibility.

Keywords: Beal's conjecture, Diophantine equation, Propositional logic, Lattice of divisibility.

1. Introduction

Usually, when Beal's conjecture is formulated by asserting that the Diophantine equation $A^p + B^q = C^r$ in positive integers A, B, C, p, q, r with A, B and C being coprime and all p, q, r being greater than 2 has no solution (see papers [1], [2], [3], just to name a few), the coprime condition is there merely to avoid trivialities.

But one may naturally raise the question whether the demanded simultaneous or pairwise coprimality of positive integers A, B and C has more intrinsic relation to the resolution of this conjecture. Particularly, can the concept of a lattice of divisibility and the corresponding logic based on such a lattice play more important role in proving or disproving this conjecture?

This article will be devoted to the lattice-theoretic analysis of Beal's conjecture.

2. Lattice of divisibility

Let us begin considering a bounded lattice $\mathcal{L} = (\mathbb{N}, \wedge, \vee, 1, 0)$ formed by the natural numbers under the operations of taking the greatest common divisor (gcd) and least common multiple (lcm), with divisibility as the order relation, namely,¹

* Email: arkady_bolotin@hotmail.com

¹ See for detail papers [4], [5].

$$\forall a, b \in \mathbb{N}: a \leq b \text{ if } a \text{ divides } b \quad . \quad (1)$$

The lattice meet $\wedge$ is given by gcd and the lattice join $\vee$ is given by lcm as follows:

$$\begin{aligned} a \leq b &\leftrightarrow a = a \wedge b \equiv gcd(a, b) = a \\ a \leq b &\leftrightarrow b = a \vee b \equiv lcm(a, b) = b \quad , \end{aligned} \quad (2)$$

The crucial observation in the proof of (2) is that the greatest common divisor and least common multiple satisfy the axioms for the lattice meet and join. To be sure, axiomatic identities hold for all elements a, b, c of the lattice of divisibility $\mathcal{L} = (\mathbb{N}, \wedge, \vee, \top, \perp)$ obtained by switching gcd and lcm with the lattice operations $\wedge$ and $\vee$ preserve true, namely,

$$\begin{aligned} a \wedge b &= b \wedge a \equiv gcd(a, b) = gcd(b, a) \\ a \vee b &= b \vee a \equiv lcm(a, b) = lcm(b, a) \quad , \end{aligned} \quad (3)$$

$$\begin{aligned} a \wedge (b \wedge c) &= (a \wedge b) \wedge c \equiv gcd(a, gcd(b, c)) = gcd(gcd(a, b), c) \\ a \vee (b \vee c) &= (a \vee b) \vee c \equiv lcm(a, gcd(b, c)) = lcm(gcd(a, b), c) \quad , \end{aligned} \quad (4)$$

$$\begin{aligned} a \vee (a \wedge b) &= a \equiv lcm(a, gcd(a, b)) = a \\ a \wedge (a \vee b) &= a \equiv gcd(a, lcm(a, b)) = a \quad , \end{aligned} \quad (5)$$

$$\begin{aligned} a \vee a &= a \equiv lcm(a, a) = a \\ a \wedge a &= a \equiv gcd(a, a) = a \quad , \end{aligned} \quad (6)$$

where (3), (4), (5), and (6) present commutative laws, associative laws, absorption laws, and idempotent laws, respectively.

From the expressions (2), it immediately follows that for each $a \in \mathbb{N}$

$$\begin{aligned} 1 \leq a &\leftrightarrow 1 = a \wedge 1 \equiv gcd(a, 1) = 1 \\ 1 \leq a &\leftrightarrow a = a \vee 1 \equiv lcm(a, 1) = a \quad , \end{aligned} \quad (7)$$

which makes 1 the bottom of the lattice of divisibility $\mathcal{L}$.

Let us assume that for each $a \in \mathbb{N}$ the following definitions hold

$$\begin{aligned}gcd(a, 0) &\equiv a \\lcm(a, 0) &\equiv 0\end{aligned}\quad . \tag{8}$$

Then these definitions readily imply

$$\begin{aligned}a \leq 0 &\leftrightarrow a = a \wedge 0 \equiv gcd(a, 0) = a \\a \leq 0 &\leftrightarrow 0 = a \vee 0 \equiv lcm(a, 0) = 0\end{aligned}\quad , \tag{9}$$

which makes 0 the top of the lattice of divisibility $\mathcal{L}$. Thus, for every a in $\mathbb{N}$

$$1 \leq a \leq 0 \quad . \tag{10}$$

3. Pseudo-complements

Now, let us take into consideration coprime natural numbers a and b , i.e., ones whose greatest common divisor being 1, namely, $gcd(a, b) = 1$.

In the lattice-theoretic terms, the elements a and b identified with coprime natural numbers can be regarded as *pseudo-complements* of each other (analogous to pseudo-complements in a Heyting algebra, see, for example [6]). Indeed, for such elements one gets

$$a \wedge b = 1 \leftrightarrow gcd(a, b) = 1 \quad , \tag{11}$$

while

$$a \vee b \neq 0 \leftrightarrow lcm(a, b) = ab \quad . \tag{12}$$

Let us denote a *pseudo-complement* of the element a as the unary operation $\neg a$, then $b = \neg a$ and equivalently, $a = \neg b$. This gives us the following involution law: Since the pseudo-complement is not unique, $\neg\neg a$ need not be equivalent to a .

Along these lines, the lattice of divisibility $\mathcal{L} = (\mathbb{N} = \{1, 2, 3, \dots\}, \wedge, \vee, \neg, 0, 1)$ is an *algebra with two binary operations (i.e., the meet $\wedge$ and the join $\vee$), one unary operation ($\neg$), and two nullary operations (1 and 0).*

4. Finite sublattices of divisibility

Consider the partially ordered by divisibility set $\mathcal{L}_a = (a, \neg a, +)$:

$$\begin{aligned} \mathcal{L}_a &= (a, \neg a, +) \\ &\equiv \{1, a, \neg a, a + \neg a, a \neg a, a^2 + a \neg a, \neg a^2 + a \neg a, a^2 \neg a + a \neg a^2\}, \end{aligned} \quad (13)$$

where $a, \neg a \in \mathbb{N}$ and a^2 and $\neg a^2$ denote $a \cdot a$ and $\neg a \cdot \neg a$, respectively.²

Using Euclid's algorithm [7] one can find

$$\begin{aligned} \gcd(b, a) &= \gcd(b - a, a) \\ \text{lcm}(b, a) &= \frac{b \cdot a}{\gcd(b, a)}. \end{aligned} \quad (14)$$

So, it is readily can be proved that

$$\begin{aligned} &a \wedge \neg a = 1 \\ &a \wedge (a + \neg a) = 1 \\ &a \wedge a \neg a = a \\ &a \wedge (a^2 + a \neg a) = a \\ &a \wedge (\neg a^2 + a \neg a) = 1 \\ &a \wedge (a^2 \neg a + a \neg a^2) = a \\ & \\ &a \vee \neg a = a \neg a \\ &a \vee (a + \neg a) = a^2 + a \neg a \\ &a \vee a \neg a = a \neg a \\ &a \vee (a^2 + a \neg a) = a^2 + a \neg a \\ &a \vee (\neg a^2 + a \neg a) = a \neg a^2 + a^2 \neg a \\ &a \vee (a^2 \neg a + a \neg a^2) = a^2 \neg a + a \neg a^2 \end{aligned}, \quad (15)$$

² Let us note that due to the definition of set equality (see, for example [8]), all the sets mentioned in this paper do not contain repetitions, e.g., neither $a \neq 1$, $\neg a \neq 1$ nor $a \neq \neg a$.

$$\begin{aligned}
& \neg a \wedge (a + \neg a) = 1 \\
& \neg a \wedge a \neg a = \neg a \\
& \neg a \wedge (a^2 + a \neg a) = 1 \\
& \neg a \wedge (\neg a^2 + a \neg a) = \neg a \\
& \neg a \wedge (a^2 \neg a + a \neg a^2) = \neg a \\
& \neg a \vee (a + \neg a) = \neg a^2 + a \neg a \\
& \neg a \vee a \neg a = a \neg a \\
& \neg a \vee (a^2 + a \neg a) = a^2 \neg a + a \neg a^2 \\
& \neg a \vee (\neg a^2 + a \neg a) = \neg a^2 + a \neg a \\
& \neg a \vee (a^2 \neg a + a \neg a^2) = a^2 \neg a + a \neg a^2
\end{aligned} \tag{16}$$

$$\begin{aligned}
& (a + \neg a) \wedge a \neg a = 1 \\
& (a + \neg a) \wedge (a^2 + a \neg a) = a + \neg a \\
& (a + \neg a) \wedge (\neg a^2 + a \neg a) = a + \neg a \\
& (a + \neg a) \wedge (a^2 \neg a + a \neg a^2) = a + \neg a \\
& (a + \neg a) \vee a \neg a = a^2 \neg a + a \neg a^2 \\
& (a + \neg a) \vee (a^2 + a \neg a) = a^2 \neg a + a \neg a^2 \\
& (a + \neg a) \vee (\neg a^2 + a \neg a) = a^2 \neg a + a \neg a^2 \\
& (a + \neg a) \vee (a^2 \neg a + a \neg a^2) = a^2 \neg a + a \neg a^2
\end{aligned} \tag{17}$$

$$\begin{aligned}
& a \neg a \wedge (a^2 + a \neg a) = a \\
& a \neg a \wedge (\neg a^2 + a \neg a) = \neg a \\
& a \neg a \wedge (a^2 \neg a + a \neg a^2) = a \neg a \\
& a \neg a \vee (a^2 + a \neg a) = a^2 \neg a + a \neg a^2 \\
& a \neg a \vee (\neg a^2 + a \neg a) = a^2 \neg a + a \neg a^2 \\
& a \neg a \vee (a^2 \neg a + a \neg a^2) = a^2 \neg a + a \neg a^2
\end{aligned} \tag{18}$$

$$\begin{aligned}
& (a^2 + a \neg a) \wedge (\neg a^2 + a \neg a) = a + \neg a \\
& (a^2 + a \neg a) \wedge (a^2 \neg a + a \neg a^2) = a + \neg a \\
& (a^2 + a \neg a) \vee (\neg a^2 + a \neg a) = a^2 \neg a + a \neg a^2 \\
& (a^2 + a \neg a) \vee (a^2 \neg a + a \neg a^2) = a^2 \neg a + a \neg a^2
\end{aligned} \tag{19}$$

Thus, every pair of the elements of $\mathcal{L}_a$ has an upper bound and a lower bound within $\mathcal{L}_a$, which means that the set $\mathcal{L}_a$ is a finite sublattice of divisibility, specifically,

$$\forall a^2, \neg a^2: \mathcal{L}_a = (a, \neg a, +) \subset \mathcal{L} = (\mathbb{N} = \{1, 2, 3, \dots\}, \wedge, \vee, \neg, 1, 0) \quad . \tag{20}$$

Equally stated, the solutions to the Diophantine equation in positive coprime integers, that is,

$$c = a + \neg a \quad (21)$$

make the lattice of divisibility $\mathcal{L}$.

5. Squared lattices of divisibility

Let us take the lattice of divisibility $\mathcal{L}^2 = (\mathbb{N}^2 = \{1^2, 2^2, 3^2, \dots\}, \wedge, \vee, \neg, 1, 0)$ created by the squared natural numbers and consider the following set partially ordered by divisibility $\mathcal{L}_{a^2} = (a^2, \neg a^2, +)$:

$$\begin{aligned} \mathcal{L}_{a^2} &= (a^2, \neg a^2, +) \\ &\equiv \{1^2, a^2, \neg a^2, a^2 + \neg a^2, a^2 \neg a^2, a^4 + a^2 \neg a^2, \neg a^4 + a^2 \neg a^2, a^4 \neg a^2 \\ &\quad + a^2 \neg a^4\} \quad , \end{aligned} \quad (22)$$

where $a^2, \neg a^2 \in \mathbb{N}^2$.

Since

$$\begin{aligned} a^2 \wedge b^2 &\equiv \gcd(a^2, b^2) = [\gcd(a, b)]^2 \equiv (a \wedge b)^2 \\ a^2 \vee b^2 &\equiv \text{lcm}(a^2, b^2) = [\text{lcm}(a, b)]^2 \equiv (a \vee b)^2 \quad , \end{aligned} \quad (23)$$

it is not hard to demonstrate that all the relations (15) - (19) will hold if one formally replaces a and $\neg a$ with a^2 and $\neg a^2$.

What is more, by the Pythagorean theorem there is a sublattice of $\mathcal{L}^2$ that is closed under the binary operation $a^2 + \neg a^2$, namely,

$$\exists a^2, \neg a^2: (a^2 + \neg a^2) \in \mathcal{L}^2 \quad . \quad (24)$$

This implies that set (22) can be a sublattice of divisibility

$$\exists a^2, \neg a^2: \mathcal{L}_{a^2} = (a^2, \neg a^2, +) \subset \mathcal{L}^2 = (\mathbb{N}^2 = \{1^2, 2^2, 3^2, \dots\}, \wedge, \vee, \neg, 1, 0) \quad , \quad (25)$$

or, in other words, the solutions to the squared Diophantine equation in coprime integers

$$c^2 = a^2 + \neg a^2 \quad (26)$$

can form the squared lattice of divisibility $\mathcal{L}^2$.

6. Cubed lattices of divisibility

In similar manner, let us introduce the lattice $\mathcal{L}^3 = (\mathbb{N}^3 = \{1^3, 2^3, 3^3, \dots\}, \wedge, \vee, \neg, 1, 0)$ whose members are cubed natural numbers partially ordered by divisibility. Let us take into consideration the set $\mathcal{L}_{a^3} = (a^3, \neg a^3, +)$:

$$\begin{aligned} \mathcal{L}_{a^3} &= (a^3, \neg a^3, +) \\ &\equiv \{1^3, a^3, \neg a^3, a^3 + \neg a^3, a^3 \neg a^3, a^6 + a^3 \neg a^3, \neg a^6 + a^3 \neg a^3, a^6 \neg a^3 \\ &\quad + a^3 \neg a^6\} \quad , \end{aligned} \quad (27)$$

where $a^3, \neg a^3 \in \mathbb{N}^3$.

Again, given that

$$\begin{aligned} a^3 \wedge b^3 &= (a \wedge b)^3 \\ a^3 \vee b^3 &= (a \vee b)^3 \quad , \end{aligned} \quad (28)$$

it is easy to see that replacing a and $\neg a$ with a^3 and $\neg a^3$ all the relations (15) - (19) would hold true.

However, the peculiarity of this case is that according to Beal's conjecture, the cubed lattice of divisibility $\mathcal{L}^3 = (\mathbb{N}^3 = \{1^3, 2^3, 3^3, \dots\}, \wedge, \vee, \neg, 1, 0)$ cannot be closed under the binary operation $a^3 + \neg a^3$, explicitly,

$$\nexists a^3, \neg a^3: (a^3 + \neg a^3) \in \mathcal{L}^3 \quad . \quad (29)$$

This implies that the set $\mathcal{L}_{a^3}$ cannot be a sublattice of the cubed lattice of divisibility, that is,

$$\nexists a^3, \neg a^3: \mathcal{L}_{a^3} = (a^3, \neg a^3, +) \subset \mathcal{L}^3 = (\mathbb{N}^3 = \{1^3, 2^3, 3^3, \dots\}, \wedge, \vee, \neg, 1, 0) \quad . \quad (30)$$

Thus, the solutions to the cubed Diophantine equation in coprime integers

$$c^3 = a^3 + \neg a^3 \quad (31)$$

cannot form the cubed lattice of divisibility $\mathcal{L}^3$.

Equivalently speaking, Beal's conjecture surmises that the lattice of divisibility induced by natural numbers raised to the third (or higher) power cannot be endowed with the binary operation $a^3 + \neg a^3$ on its elements.

7. Algebra $\mathcal{L}^3$ as applied to logic of divisibility

The lattice $\mathcal{L}^3 = (\mathbb{N}^3 = \{1^3, 2^3, 3^3, \dots\}, \wedge, \vee, \neg, 1, 0)$ is an algebra that satisfies the following conditions:

- 1) $(\mathbb{N}^3, \wedge, \vee)$ is a lattice of divisibility;
- 2) $a^3 \leq b^3 \leftrightarrow a^3 = (a \wedge b)^3, b^3 = (a \vee b)^3$;
- 3) $a \wedge 1 = 1, a \vee 0 = 0$;
- 4) $a \wedge \neg a = 1, a \vee \neg a = a \neg a$.

Let the map $\mathcal{M}: x \rightarrow \{F, T\}$, where x is an element of the lattice $\mathcal{L}^3$, assign a truth value to a proposition X identified with x , specifically,

$$X = \mathcal{M}(x) \quad , \quad (32)$$

such that $\mathcal{M}(1) = F$ (i.e., false) and $\mathcal{M}(0) = T$ (i.e., true).

8. Closing remarks

If the axioms of the propositional logic relating to divisibility are interpreted as terms of an algebra $\mathcal{L}^3 = (\mathbb{N}^3 = \{1^3, 2^3, 3^3, \dots\}, \wedge, \vee, \neg, 1, 0)$, then they will be evaluated to the divisibility lattice's top, i.e., 0, under any assignment of values to the propositional formula's variables.

In other words, if the propositional formula always has the value 0, then it is *deducible* from the laws of *logic of divisibility*, so valid in divisibility logical sense propositional formulas are exactly those that always have a value of 0.

This is similar to the notion that formulas valid in classically logical sense are those that have a value of 1 in the two-element Boolean algebra under any possible assignment of true and false to the formula's variables [9].

In this fashion, the proposition

$$D = \mathcal{M}(c^3 - a^3 - \neg a^3) \quad (33)$$

will be true if $c^3 - a^3 - \neg a^3 = 0$ for any $c^3 \in \mathcal{L}^3$ being the pseudo-complement of both a and $\neg a$, i.e., $c \wedge a = c \wedge \neg a = 1$. However, since it is easy to demonstrate that the lattice expression $c^3 - a^3 - \neg a^3$ is not always 0 (unlike the expression $c - a - \neg a$ which is a tautology in divisibility logical sense), it follows that the Beal's conjecture cannot be proved *logically*, that is, it cannot be derivable by reasoning from the laws of logic of divisibility.

But the fact that the truth of the proposition (33) cannot be **determined** logically means that there does not exist *a general constructive method* of solving the cubed Diophantine equation (31) in coprime natural numbers.

References

- [1] Dilworth R., Peter G. Algebraic Theory of Lattices. Prentice-Hall. 1973, ISBN 978-0-13-022269-5.
- [2] Beukers F. The Diophantine equation $Ax^p + By^q = Cz^r$, Duke Math.J. 91(1998), 61-88.
- [3] Chen I., Siksek S. Perfect powers expressible as sum of two cubes, J.Algebra 322 (2009), 638-656.
- [4] Nation J. Finite sublattices of a free lattice, Trans. Amer. Math. Soc. 269 (1982), 311-337.
- [5] Nation J. On partially ordered sets embeddable in a free lattice, Algebra Universalis **18** (1984), 327-333.
- [6] Yankov, V. Brouwer lattice, in Hazewinkel, Michiel, *Encyclopedia of Mathematics*, Springer, 2001, ISBN 978-1-55608-010-4.
- [7] MacLane S., and Birkhoff G. The Euclidean Algorithm in: A Survey of Modern Algebra, Fourth Edition. MacMillan Publishing Co., 1977. ISBN 0-02-310070-2. 1-7.
- [8] Lévy, A. Basic set theory. Mineola, New York: Dover Publications, 2002, ISBN 978-0-486-42079-0.
- [9] Blyth T. Lattices and ordered algebraic structures. Springer. p. 151, 2005, ISBN 978-1-85233-905-0.