British Journal of Mathematics & Computer Science
18(1): 1-5, 2016, Article no.BJMCS.27581
ISSN: 2231-0851

SCIENCEDOMAIN *international*
www.sciencedomain.org

An Example of the Application of Provability Logic to Unsolved Problems in Number Theory: The Cullen Numbers and Conway's Supposition

Alexander Bolotin[1*]

[1] *Open University of Israel, Beersheba, Israel.*

Author's contribution

The sole author designed, analyzed, interpreted and prepared the manuscript.

Article Information

DOI: 10.9734/BJMCS/2016/27581
Editor(s):
(1) Fangfei Li, Department of Mathematics, East China University of Science and Technology, Shanghai, China.
(2) Paul Bracken, Department of Mathematics, The University of Texas-Pan American
Edinburg, TX 78539, USA.
Reviewers:
(1) I. V. Nikolaev, The Fields Institute for Research in Mathematical Sciences, Ontario, Canada.
(2) Anonymous, Hasan Kalyoncu University, Turkey.
(3) Fethi Soltani, Jazan University, Jazan, Saudi Arabia.
Complete Peer review History: http://www.sciencedomain.org/review-history/15662

Original Research Article

Received: 8th June 2016
Accepted: 27th July 2016
Published: 5th August 2016

Abstract

This short paper offers an example of possibly fruitful interactions between modal logic and number theory. In the paper, Conway's remark that p and $p \cdot 2^p + 1$ can both be prime numbers is formulated as a formula of modal logic and then analyzed for its decidability.

Keywords: Modal logic; provability logic; Fermat's last theorem; Cullen numbers; Conway's remark; decidability.

1 Introduction

The importance of the applications of modal logic to mathematics and computer science is difficult to overestimate. Provability logic is the only one example of such applications [1].

It is so because modal logic is a valuable tool in clarifying our understanding of central results concerning provability in the foundations of mathematics. For example, using code numbers for arithmetic sentences,

[*] *Corresponding author: E-mail: arkady_bolotin@hotmail.com;*

Gödel was able to demonstrate a correspondence between sentences of mathematics and facts about which sentences are and are not provable in Peano's system for arithmetic.

However, by some reason, modal logic (or provability logic) has been never tried in number theory. Meanwhile, the use of modal logic would allow testing the decidability of unsolved problems in number theory; in particular, it might allow answering the important question whether a modal logic formula of a given problem *is a theorem or not.*

So, this short paper offers an example of possibly fruitful interactions between modal logic and number theory.

2 Fermat's Last Theorem

Let us first consider the situation with the last theorem of Fermat before 1994. In the terms of propositional calculus, this theorem can be presented as the negation.

$$\neg A = (\forall\, n, x, y, z \in \mathbb{N} \mid z^n \neq x^n + y^n \ \vee\ n \leq 2) \tag{1}$$

of the following proposition A

$$A = (\exists\, n, x, y, z \in \mathbb{N} \mid z^n = x^n + y^n \ \wedge\ n > 2) \ \ . \tag{2}$$

As the negation (1) contains the universal quantification $\forall$, in order to prove (1) a witness for $\neg A(K)$ must be provided when any allowed input $K = (n, x, y, z) \in \mathbb{N}$ is given. But, despite the fact that there exist proofs of $\neg A$ for specific subsets of conditions (e.g., $n = 3, 4, 5$), given an infinite amount of inputs K, the general proof of $\neg A$ would be impossible to achieve from the constructivist point of view.

So, instead, one may try to prove the proposition A itself. Since this proposition contains the existential quantification $\exists$, the proof of $A(K)$ must provide K and a witness for $A(K)$. However, it is clear that the proposition A is *possibly* false. In terms of modal logic, this can be written as the formula

$$\Diamond\, A(K) = \perp \ \ , \tag{3}$$

which assigns the truth value "false", $\perp$, to the proposition "it is possible that $A(K)$". Mathematically, this modal formula corresponds to the impossibility of certain Diophantine equations and systems of equations (see, for example [2]).

Using the modal operator of necessity $\Box$ and the analogy of de Morgan's laws [3,4].

$$\neg\, \Diamond\, A(K) \Leftrightarrow\ \Box\neg A(K) \ \ , \tag{4}$$

One can write the negation of the assumption (3) as the following propositional expression

$$\Box\neg A(K) = \top \ \ . \tag{5}$$

Next, making use of the characteristic axiom of modal logic

$$\Box\neg A(K) \rightarrow \neg A(K) \tag{6}$$

that reads "if $\neg A(K)$ is necessary, then $\neg A(K)$ is the case", one can get

$$\neg A(K) = \top \ \ . \tag{7}$$

This propositional formula means that the negation $\neg A(K)$ is a logical truth for any allowable input $K = (n, x, y, z) \in \mathbb{N}$.

Consider the predicate of this formula, $P(K)$:

$$P(K) = \left((z^n \neq x^n + y^n) \lor (n \leq 2)\right) \quad . \tag{8}$$

Since $\neg A(K)$ is a logical truth, the logical value of $P(K)$ must be $\top$ for any n and x, y, z. On the other hand, the expression

$$\left((n > 2) \lor (n \leq 2)\right) \tag{9}$$

must be a logical truth too. Comparing two expressions (8) and (9) one can assert the following statement of equivalency

$$(z^n \neq x^n + y^n) \Leftrightarrow (n > 2) \tag{10}$$

that means two logical implications: the implication $(z^n \neq x^n + y^n) \Rightarrow (n > 2)$ (equivalent to the phrase "if $z^n = x^n + y^n$ has no non-trivial solutions then $n > 2$") and the implication $(n > 2) \Rightarrow (z^n \neq x^n + y^n)$ (equivalent to the phrase "if $n > 2$ then the equation $z^n = x^n + y^n$ has no non-trivial solutions").

The assertion $\lozenge\, A(K) = \perp$ does not contain a logical contradiction. This upholds the idea that there might exist a general proof witnessing the truth of the negation (1). And indeed, in 1994 such proof was finally found [5].

3 Cullen Numbers

As it is known, the Cullen numbers $C(n)$

$$C(n) = n \cdot 2^n + 1 \tag{11}$$

are all composite for $n \in [2; 1000]$, except for n = 141. Furthermore, even for larger n the Cullen numbers $C(n)$ are very likely to be composite since Fermat's (little) theorem tells us that $(p-1) \cdot 2^{p-1} + 1$ and $(p-2) \cdot 2^{p-2} + 1$ are both divisible by $p \in \mathbb{P}$ (see details in [6]).

Besides, as John Conway observes [6,7], the Cullen numbers $C(n)$ are divisible by $2n - 1$ if that is a prime of shape $8k \pm 3$. He asks if p and $p \cdot 2^p + 1$ can both be prime; for brevity we will call this question "Conway's supposition".

In terms of propositional formulae, Conway's supposition can be written as follows:

$$A(n) = (\exists\, n \in \mathbb{N} \mid n \in \mathbb{P} \land (n \cdot 2^n + 1) \in \mathbb{P}) \quad , \tag{12}$$

where $\mathbb{P}$ denotes the set of all prime numbers.

Let us analyze the decidability of Conway's supposition; for that, we will present this supposition as a modal formula

$$\lozenge\, A(n) = \top \tag{13}$$

asserting that *Conway's supposition is possibly true*. From (13) it follows that

$$\neg A(n) = \perp \quad , \tag{14}$$

where the negation $\neg A(n)$ is defined as

$$\neg A(n) = (\forall\, n \in \mathbb{N} \mid n \notin \mathbb{P} \,\vee\, (n \cdot 2^n + 1) \notin \mathbb{P}) \quad . \tag{15}$$

For the negation $\neg A(n)$ being always false it is necessary that the predicate $P(n)$ must be always false, i.e.,

$$(n \notin \mathbb{P} \,\vee\, (n \cdot 2^n + 1) \notin \mathbb{P}) = \perp \quad . \tag{16}$$

Thus, the following expression must be true for any prime number p

$$\big((p \cdot 2^p + 1) \in \mathbb{P}\big) = \top \quad . \tag{17}$$

However, it is easy to show that the assertion (17) cannot be correct for any arbitrary p: For example, if $p = 3$, one gets $(3 \cdot 2^3 + 1) = 25 \notin \mathbb{P}$. Thus, the hypothesis $\lozenge\, A(n) = \top$ does not hold.

Therefore, let us consider the alternative hypothesis, namely: *Conway's supposition is possibly false*, that is

$$\lozenge\, A(n) = \perp \quad . \tag{18}$$

If Eq. 18 holds then the predicate $P(n)$ must be always true, i.e.,

$$(n \notin \mathbb{P}) \,\vee\, \big((n \cdot 2^n + 1) \notin \mathbb{P}\big) = \top \quad . \tag{19}$$

Comparing this expression with the logically truthful assertion $(n \notin \mathbb{P}) \vee (n \in \mathbb{P})$ immediately gives the following statement of equivalency

$$\big((n \cdot 2^n + 1) \notin \mathbb{P}\big) \Leftrightarrow (n \in \mathbb{P}) \quad . \tag{20}$$

The proposition $(n \in \mathbb{P})$ can be replaced by $(n = p)$, consequently, the alternative hypothesis $\lozenge\, A(n) = \perp$ is logically equivalent to

$$(n = p) \Leftrightarrow \big((n \cdot 2^n + 1) \notin \mathbb{P}\big) \quad . \tag{21}$$

It is easy to see that Eq. 21 leads to the contradiction: Let n be equal to 141, then $(n = p)$ is the true proposition, but at the same time $\big((141 \cdot 2^{141} + 1) \notin \mathbb{P}\big)$ is not. For this reason, the hypothesis $\lozenge\, A(n) = \perp$ causes a logical contradiction.

But then the hypothesis $\lozenge\, A(n)$ is undecidable: it is nether true nor false. This means that Conway's supposition *cannot be a theorem.* i.e., it cannot be proven or disproven analytically or with an algorithm.

4 Conclusion

Unlike the case of the Fermat's last theorem, in which one can get a general proof witnessing the false of the proposition $\lozenge\, A(K)$, the logical structure of Conway's supposition does not admit a general proof of its truth.

This leaves us only with brute-force methods to search for possible Cullen numbers satisfying Conway's supposition.

Acknowledgements

Author wishes to thank anonymous reviewers for their insightful comments.

Competing Interests

Author has declared that no competing interests exist.

References

[1] Boolos G. The logic of provability. Cambridge: Cambridge University Press; 1993.

[2] Carmichael R. On the impossibility of certain Diophantine equations and systems of equations. Amer. Math. Monthly (Mathematical Association of America). 1913;20(7):213–221.

[3] Hughes G, Cresswell M. An introduction to modal logic. London: Methuen; 1968.

[4] Garson J. Modal logic for philosophers, second edition. Cambridge: Cambridge University Press; 2013.

[5] Wiles A. Modular elliptic curves and Fermat's last theorem. Annals of Mathematics. 1995;141(3): 448.

[6] Guy R. Unsolved problems in number theory. Springer Science + Business Media New York; 2004.

[7] Keller W. New Cullen primes, (92-11-20 preprint); 1992.

Peer-review history:
The peer review history for this paper can be accessed here (Please copy paste the total link in your browser address bar)
http://sciencedomain.org/review-history/15662