Notre Dame Journal of Formal Logic
Volume 59, Number 2, 2018

A Problem in Pythagorean Arithmetic

Victor Pambuccian

Meinem Lehrer, Stefan Kleitsch, in Dankbarkeit gewidmet

Abstract Problem 2 at the 56th International Mathematical Olympiad (2015) asks for all triples (a, b, c) of positive integers for which $ab - c$, $bc - a$, and $ca - b$ are all powers of 2. We show that this problem requires only a primitive form of arithmetic, going back to the Pythagoreans, which is the arithmetic of the even and the odd.

1 Introduction

Problem 2 at the 56th International Mathematical Olympiad (2015), proposed by Dušan Djukić, asked contestants to find all triples (a, b, c) of positive integers for which $ab - c$, $bc - a$, and $ca - b$ are all powers of 2. Here a power of 2 is understood to be 2^n with n a nonnegative integer.

As is well known, problems at the International Mathematical Olympiad should be solvable with *elementary* means, and our aim is to find out just how elementary a formal theory is needed to solve Problem 2. Since it speaks about positive integers and the operations of addition and multiplication, an axiom system for a theory in which it holds will need to contain the binary operations $+$ and $\cdot$, the binary relation $<$, and the constants 0 (both $<$ and 0 are needed so we can express the fact that all the numbers we deal with are nonnegative) and 1 (so that we can express the fact that the successor of a number n in the order determined by $<$ is $n + 1$).

2 The Axiom System for PA$^-$ and Its Extensions

Thus, we need axioms for the usual rules for addition $+$ and multiplication $\cdot$, for 1 and 0, that is:

A 1 $\quad (x + y) + z = x + (y + z)$,

Received October 22, 2015; accepted December 2, 2015
First published online January 9, 2018
2010 Mathematics Subject Classification: Primary 03C62, 11U99; Secondary 11A99
Keywords: Pythagorean arithmetic, elementary number theory
 10.1215/00294527-2017-0028

A 2 $x + y = y + x$,

A 3 $(x \cdot y) \cdot z = x \cdot (y \cdot z)$,

A 4 $x \cdot y = y \cdot x$,

A 5 $x \cdot (y + z) = x \cdot y + x \cdot z$,

A 6 $x + 0 = x \wedge x \cdot 0 = 0$,

A 7 $x \cdot 1 = x$.

We also need axioms for inequality $<$ and a binary operation $-$, so that we can express the difference between two numbers if the result is positive. These are

A 8 $(x < y \wedge y < z) \rightarrow x < z$,

A 9 $\neg x < x$,

A 10 $x < y \vee x = y \vee y < x$,

A 11 $x < y \rightarrow x + z < y + z$,

A 12 $(0 < z \wedge x < y) \rightarrow x \cdot z < y \cdot z$,

A 13 $x < y \rightarrow x + (y - x) = y$,

A 14 $0 < 1 \wedge (x > 0 \rightarrow (x > 1 \vee x = 1))$,

A 15 $x > 0 \vee x = 0$.

A1–A15 represent an axiom system for what is referred to as PA^- in Kaye [1, pp. 16–18]. Models of PA^- consist of *numerals*; that is, $\overline{n} = (1 + (1 + \cdots + 1))$ with 1 occurring n times, and, possibly, of *nonstandard* elements, which are greater than all numerals. The structures satisfying the axioms of PA^- are the sets of nonnegative elements of what are referred to as *discretely ordered rings*.

By referring to powers of 2, our problem seems to require more, for we do not have the exponential function in our vocabulary. It turns out that we do not need it, for we can express the fact that a is a power of 2 simply by defining a unary predicate PT which stipulates that a positive number a is a power of 2 if and only if all of its divisors, except 1, are even. Formally, this amounts to (the divisibility predicate $\mid$ being defined as usual, $a \mid b :\Leftrightarrow (\exists c)\, a \cdot c = b$):

$$PT(n) :\Leftrightarrow n > 0 \wedge (\forall d)\,(d \mid n \wedge d > 1 \rightarrow \overline{2} \mid d). \tag{1}$$

This definition certainly corresponds to our intuitions regarding powers of 2, but it may not satisfy properties we find to be intrinsic to the notion of power of 2, properties which can be formalized as follows:

$$PT(a) \wedge PT(b) \rightarrow PT(ab), \tag{2}$$

$$PT(a) \wedge PT(b) \wedge a < b \rightarrow a \mid b, \tag{3}$$

$$PT(a) \wedge a < b \wedge b < \overline{2} \cdot a \rightarrow \neg PT(b). \tag{4}$$

This is perhaps not so surprising if one thinks that PA^- is a very weak theory in which one cannot even show that among two consecutive numbers one is even and the other one is odd. In fact, for any natural number n, there may be sequences of n consecutive numbers, none of which are odd and none of which are even. For the positive cone of $\mathbb{Z}[X]$ (here $\mathbb{Z}[X]$ is ordered by $\sum_{i=0}^{n} c_i X^i > 0$ if and only if $c_n > 0$)

is a model of PA^-, and the sequence $X+1, \dots, X+\overline{n}$ has no even element and no odd element. Yet none of (2)–(4) hold in $\mathrm{PA}^- + \mathrm{A}16$ either, where A16 is the axiom expressed in a language enriched with the unary operation symbol $[\frac{\cdot}{2}]$, stating that every number is odd or even:

A 16 $\quad x = 2[\frac{x}{2}] \vee x = 2[\frac{x}{2}] + 1.$

To see this, denote by $K_D[X]$ the ring of polynomials in X with free term in D and with all other coefficients in K, ordered by $\sum_{i=0}^{n} c_i X^i > 0$ if and only if $c_n > 0$ (here $c_0 \in D$, and $c_i \in K$ for all $1 \leq i \leq n$, with $c_n \neq 0$), and denote by $\mathcal{C}(K_D[X])$ the positive cone of $K_D[X]$. Let $\mathbb{Z}_{\frac{1}{2}}$ stand for the ring of dyadic numbers, that is, all rational numbers of the form $\frac{m}{2^n}$, with $m, n \in \mathbb{Z}$ and $n \geq 0$, and let $R = \mathbb{Z}_{\frac{1}{2}}[\sqrt{3}]$ stand for the ring whose elements are of the form $a + b\sqrt{3}$, with $a, b \in \mathbb{Z}_{\frac{1}{2}}$. Then $\mathcal{C}(R_{\mathbb{Z}}[X])$ with $[\frac{\sum_{i=1}^{n} a_i X^i + a_0}{2}] = \sum_{i=1}^{n} \frac{a_i}{2} X^i + [\frac{a_0}{2}]$ is a model of $\mathrm{PA}^- + \mathrm{A}16$. However, given that $PT(\sqrt{3}X)$, but $\neg PT(3X^2)$, (2) does not hold, and given that $PT(X)$, $PT(\sqrt{3}X)$, $X < \sqrt{3}X$, yet $X \nmid \sqrt{3}X$, (3) does not hold either, and the fact that $X < \sqrt{3}X < 2X$, with X, $\sqrt{3}X$, and $2X$ powers of 2, shows that (4) does not hold.

What $\mathrm{PA}^- + \mathrm{A}16$ lacks is an axiom stating that every fraction can be brought into a form in which the numerator and denominator are not both even. It is an axiom needed for the proof based on considerations of parity of the fact that $\sqrt{2}$ is irrational (but, as pointed out in Pambuccian [3] (see also Menn and Pambuccian [2]), too weak to prove that $\sqrt{17}$ is irrational). This was, apparently, the oldest form of number theory, as practiced by the Pythagoreans, about which Aristotle tells us in his *Metaphysics*, 986a, "Evidently, then, these thinkers also consider that number is the principle both as matter for things and as forming both their modifications and their permanent states, and hold that the elements of number are the even and the odd" (translated by W. D. Ross).

To state the axiom, we need two more binary operations, κ and μ (so the language in which our *Pythagorean arithmetic* is expressed consists of 0, 1, $+$, $-$, $\cdot$, $<$, $[\frac{\cdot}{2}]$, κ, μ), together with the following axiom:

A 17 $$m = \kappa(m,n) \cdot \mu(m,n) \wedge n = \kappa(m,n) \cdot \mu(n,m)$$
$$\wedge (\mu(m,n) = 2[\tfrac{\mu(m,n)}{2}] + 1 \vee \mu(n,m) = 2[\tfrac{\mu(n,m)}{2}] + 1).$$

With our modest means, A17 accomplishes what the fact that, for any positive integer n, there are nonnegative integers $p(n)$ and $q(n)$ such that $n = 2^{p(n)}(2q(n)+1)$ does for natural numbers. Our $\kappa(m,n)$ here plays the role of $2^{\min\{p(n),p(m)\}}$, whereas $\mu(m,n)$ and $\mu(n,m)$ stand for $2^{p(m)-\min\{p(n),p(m)\}}(2q(m)+1)$ and $2^{p(n)-\min\{p(n),p(m)\}}(2q(n)+1)$, respectively.

Note that, as shown in Schacht [4], in the presence of A17, the requirement made by A16 can be replaced by the weaker assumption

A 18 $\quad x = [\frac{2x}{2}].$

Pythagorean arithmetic can thus be axiomatized by {A1–A15, A17, A18}. Throughout the paper, we will use the symbols $\leq$ and $\geq$ with their usual meanings. All of (2)–(4) hold in Pythagorean arithmetic. To see this, note first that additive cancellation holds, that is, Pythagorean arithmetic satisfies the following:

$$a + x = a + y \rightarrow x = y. \tag{5}$$

Proof Suppose $a + x = a + y$. By A10, one of $x < y$, $x = y$, or $y < x$ must hold. Suppose $x = y$ does not hold. Given the symmetry in x and y of our hypothesis, we may assume without loss of generality that $x < y$. Then, by A11, we have $a + x < a + y$ as well; thus, $a + y < a + y$, which contradicts A9. □

Multiplicative cancellation is also allowed in Pythagorean arithmetic, that is,

$$a \neq 0 \wedge a \cdot x = a \cdot y \rightarrow x = y. \tag{6}$$

Proof By A10, we have $x < y$ or $x = y$, or $y < x$. If $x = y$ does not hold, then one of $x < y$ or $y < x$ must hold. Suppose $x < y$. By A15 and A12, we have $a \cdot x < a \cdot y$, which, together with our hypothesis $a \cdot x = a \cdot y$, contradicts A9. We obtain the same contradiction by assuming $y < x$. □

Distributivity of multiplication holds over subtraction as well, that is,

$$b < a \wedge c \neq 0 \rightarrow c \cdot a - c \cdot b = c \cdot (a - b). \tag{7}$$

Proof By A13, $b+(a-b) = a$; thus, by A5, $c \cdot a = c \cdot (b+(a-b)) = c \cdot b + c \cdot (a-b)$. Since, by A15, $c > 0$, by A6 and A9, $a - b \neq 0$, and thus, by A15, $a - b > 0$, we have, by A12, $c \cdot (a-b) > 0$. Thus, $c \cdot a > c \cdot b$ so, by A13, $c \cdot b + (c \cdot a - c \cdot b) = c \cdot a$. Together with $c \cdot a = c \cdot b + c \cdot (a-b)$, this implies, by (5), $c \cdot (a-b) = c \cdot a - c \cdot b$. □

Also, odd numbers are never even in Pythagorean arithmetic, that is,

$$\overline{2} \cdot n + 1 \neq \overline{2} \cdot m. \tag{8}$$

Proof Suppose $\overline{2} \cdot n + 1 = \overline{2} \cdot m$. By A14 and A11, $\overline{2} \cdot n < \overline{2} \cdot n + 1$; thus, $\overline{2} \cdot n < \overline{2} \cdot m$ and also $n < m$ (by A8, A9, A10, and A12), so, by A13, $\overline{2} \cdot n + (\overline{2} \cdot m - \overline{2} \cdot n) = \overline{2} \cdot m$. Thus, $\overline{2} \cdot n + (\overline{2} \cdot m - \overline{2} \cdot n) = \overline{2} \cdot n + 1$, and thus, by (5), $\overline{2} \cdot m - \overline{2} \cdot n = 1$, that is, by (7), $\overline{2} \cdot (m - n) = 1$. Since $m - n > 0$, we have, by A14, $m - n > 1$ or $m - n = 1$. Thus, by A7, $\overline{2} \cdot (m - n) > \overline{2}$ or $\overline{2} \cdot (m - n) = \overline{2}$, that is, $1 > \overline{2}$ or $1 = \overline{2}$, none of which can hold, for, by A14 and A11, $0 < 1$ and $1 < 1 + 1$. □

We also have

$$\overline{2} \cdot m + 1 \mid a \cdot b \wedge PT(a) \rightarrow \overline{2} \cdot m + 1 \mid b. \tag{9}$$

Proof Since $\overline{2} \cdot m + 1 \mid a \cdot b$, there is a c such that $(\overline{2} \cdot m + 1) \cdot c = a \cdot b$. By A17 with c instead of m and a instead of n we get that $c = \kappa(c,a) \cdot \mu(c,a)$ and $a = \kappa(c,a) \cdot \mu(a,c)$, with at least one of $\mu(c,a)$ and $\mu(a,c)$ odd. Plugging these in to $(\overline{2} \cdot m + 1) \cdot c = ab$, using the associativity and commutativity of multiplication and canceling $\kappa(a,c)$, we get $(\overline{2} \cdot m + 1) \cdot \mu(c,a) = \mu(a,c) \cdot b$. Now $\mu(a,c)$ must be odd, for, if it were even, $(\overline{2} \cdot m + 1) \cdot \mu(c,a)$ would have to be even as well, forcing $\mu(c,a)$ to be even (it has to be even or odd, since A16 holds, and if it were odd, $(\overline{2} \cdot m + 1) \cdot \mu(c,a)$ would be odd, a contradiction, for a number cannot be both odd and even, by (8)), but one of $\mu(a,c)$ and $\mu(c,a)$ must be odd. Since $\mu(a,c)$ is odd, $\mu(a,c) \mid a$, and $PT(a)$, we must have $\mu(a,c) = 1$, so we have $(\overline{2} \cdot m + 1) \cdot \mu(c,a) = b$, so $\overline{2} \cdot m + 1 \mid b$. □

We can now show that (2)–(4) hold in Pythagorean arithmetic. Suppose $PT(a)$ and $PT(b)$, and let $d \mid ab$ with $d > 1$. If d were odd, then, by (9), bearing in mind that $PT(a)$, we would have $d \mid b$, but that would contradict the fact that $PT(b)$. This proves (2). Suppose now $a < b$, $PT(a)$, and $PT(b)$. By A17 we have $a = \kappa(a,b) \cdot \mu(a,b)$ and $b = \kappa(a,b) \cdot \mu(b,a)$. Since a and b cannot have odd divisors greater than 1 and one of $\mu(a,b)$ and $\mu(b,a)$ has to be odd, the odd one has to be 1 (both cannot be 1, for else $a = b$). Since we cannot have $\mu(b,a) = 1$, as that would entail $b < a$ or $b = a$, we must have $\mu(a,b) = 1$, and thus $a \mid b$, proving (3). Suppose now $a < b$, $b < \overline{2} \cdot a$, and $PT(a)$. By A17, we have $a = \kappa(a,b) \cdot \mu(a,b)$ and $b = \kappa(a,b) \cdot \mu(b,a)$. Given that a can have no odd divisor except for 1, $\mu(a,b)$ is either even or 1. If it were 1, then $b = a \cdot \mu(b,a)$, and thus $1 < \mu(b,a) < \overline{2}$, contradicting A14, which asks for $\mu(b,a) - 1$ to be 1 or > 1, that is, $\mu(b,a) = \overline{2}$ or $\mu(b,a) > \overline{2}$, which is a contradiction. Thus, $\mu(a,b)$ is even, so $\mu(b,a)$ must be odd. It cannot be 1, or else we would have $b \leq a$, so $\mu(b,a)$ is an odd number greater than 1. Thus, $\neg PT(b)$, proving (4).

3 Problem 2 Holds in Pythagorean Arithmetic

To turn Problem 2 into a statement that can be proved inside Pythagorean arithmetic, we need to express it not as a question but rather as a solved problem, one that states what the solutions are and implicitly that there are no other solutions. In this form, its statement is—with $S = \{(2,2,2), (3,2,2), \&, (11,6,2), \&, (7,5,3), \&\}$, where by $(x, y, z), \&$ we have denoted the sequence of all triples obtained by permuting x, y, and z—

$$a \cdot b > c \wedge b \cdot c > a \wedge c \cdot a > b \wedge PT(a \cdot b - c) \wedge PT(b \cdot c - a)$$
$$\wedge PT(c \cdot a - b) \to \bigvee_{(i,j,k) \in S} a = \overline{i} \wedge b = \overline{j} \wedge c = \overline{k}. \tag{10}$$

Now (10) can be shown to hold in Pythagorean arithmetic, the proof being what one expects it to be.

Theorem 3.1 *The statement (10) can be proved using only the axioms {A1–A15, A17, A18}, that is, inside Pythagorean arithmetic.*

Proof First, note that each of a, b, and c has to be greater than 1. That none can be 0 is plain, for if, say, $a = 0$, then $a \cdot b > c$ could not hold, given A6 and A15. None of them can be 1 either, for if, say, $a = 1$, then we would have $b > c$ and $c > b$, which, after applying A8, would contradict A9. Suppose now that two of a, b, and c were equal, say, $a = b$. Then we would have $PT(a^2 - c)$ and $PT(a \cdot (c-1))$. The latter implies $PT(a)$ and $PT(c-1)$, and since $a > 1$, $PT(a)$ implies that a is even. If $c > 2$, then $c - 1 > 1$, and thus, $PT(c-1)$ would imply that $c - 1$ is even, that is, c is odd. But then $a^2 - c$ would have to be odd, and since we have $P(a^2 - c)$, we would need to have $a^2 - c = 1$, that is, $a^2 = c + 1$. Since $PT(a)$, we also have, by (2), $PT(a^2)$, so $PT(c+1)$ as well. Given that their difference is $\overline{2}$, both $c - 1$ and $c + 1$, which have to be even as $c > \overline{2}$, cannot be multiples of $\overline{4}$. Since both have only even divisors, one of them must be $\overline{2}$. Since $c + 1 > \overline{3}$, we must have $c - 1 = \overline{2}$, so $c = \overline{3}$, and thus, given $a^2 = c + 1$, $a = \overline{2}$. So $(\overline{2}, \overline{2}, \overline{3})$ is the only solution with $a = b$ and $c > \overline{2}$. If $c = \overline{2}$, then $PT(a^2 - c)$ and $PT(a)$ imply that $\overline{4} \nmid a$, so that $a = \overline{2}$. Thus, $(\overline{2}, \overline{2}, \overline{2})$ is the only solution with $a = b$ and $c = \overline{2}$.

Given the symmetry in a, b, c of the hypothesis in (10) and the fact that we have already dealt with the case in which two among them are equal, we may assume for the moment that $1 < c < b < a$. Let us also denote $a \cdot b - c$ by m, $b \cdot c - a$ by n, and $c \cdot a - b$ by p. Note that $n < p < m$. By (3), we must thus have $n \mid p$, $n \mid m$, and $p \mid m$. Note that $m - p = (b - c) \cdot (a + 1)$ and $m + p = (b + c) \cdot (a - 1)$, so

$$p \mid (b - c) \cdot (a + 1) \qquad \text{and} \qquad p \mid (b + c) \cdot (a - 1). \tag{11}$$

One of $a + 1$ and $a - 1$ cannot be a multiple of $\overline{4}$, for their difference is $\overline{2}$. If $a - 1$ is not a multiple of $\overline{4}$, then, since $p \cdot x = (b + c) \cdot (a - 1)$ for some $x > 0$ and we have either $a - 1 = \overline{2} \cdot (\overline{2} \cdot k + 1)$ or $a - 1 = \overline{2} \cdot k + 1$, we have $p \cdot x = (b + c) \cdot \overline{2} \cdot (\overline{2} \cdot k + 1)$ or $p \cdot x = (b + c) \cdot (\overline{2} \cdot k + 1)$. In both cases, by (9), $\overline{2} \cdot k + 1 \mid x$, that is, $x = (\overline{2} \cdot k + 1) \cdot y$. Thus, the two options are, after canceling $\overline{2} \cdot k + 1$ (by (6)): $p \cdot y = (b + c) \cdot \overline{2}$ or $p \cdot y = b + c$. Thus, in any case, $p \cdot y = \overline{2} \cdot (b + c)$ must hold for some y, and thus

$$p \leq \overline{2} \cdot (b + c). \tag{12}$$

If $a + 1$ is not a multiple of $\overline{4}$, then we arrive analogously to $p \cdot y = \overline{2} \cdot (b - c)$, and thus $p \leq \overline{2} \cdot (b - c)$. So, in this case as well, (12) holds.

Now, $b \cdot c + c = (b + 1) \cdot c \leq a \cdot c = p + b \leq \overline{2} \cdot (b + c) + b = \overline{3} \cdot b + \overline{2} \cdot c$. Thus, we have $b \cdot c + c \leq \overline{3} \cdot b + \overline{2} \cdot c$. Thus, by using A8, A9, A10, and A11, $b \cdot c \leq \overline{3} \cdot b + c$, and given that $\overline{3} \cdot b + c < \overline{4} \cdot b$, we get, using A12, $c < \overline{4}$. Thus, we have only two possibilities: (i) $c = \overline{2}$ and (ii) $c = \overline{3}$.

Suppose that (i) holds. Then we need to have $PT(a \cdot b - \overline{2})$, $PT(\overline{2} \cdot a - b)$, and $PT(\overline{2} \cdot b - a)$. If a and b were both even, then $a \cdot b - \overline{2}$ would be a multiple of $\overline{2}$, but not of $\overline{4}$, so we would need to have $a \cdot b - \overline{2} = \overline{2}$, which is impossible, since $b \geq \overline{3}$ and $a \geq \overline{4}$ (as $c < b < a$ and $c = \overline{2}$). One can also easily note that a and b cannot both be odd, for else $a \cdot b - \overline{2}$ would be odd and, thus, would have to be 1, which is impossible for the reasons mentioned above. Thus, the pair (a, b) consists of an even number and an odd number. Suppose a were odd and b were even; then $\overline{2} \cdot b - a$ would be odd and, thus, would have to be 1. Thus, $a = \overline{2} \cdot b - 1$, and thus, $m = a \cdot b - c = \overline{2} \cdot b^2 - b - \overline{2}$ and $p = c \cdot a - b = \overline{3} \cdot b - \overline{2}$. Since $p \mid m$, we have $\overline{3} \cdot b - \overline{2} \mid \overline{2} \cdot b^2 - b - \overline{2}$. Since

$$\overline{9} \cdot (\overline{2} \cdot b^2 - b - \overline{2}) = (\overline{3} \cdot b - \overline{2}) \cdot (\overline{6} \cdot b + 1) - \overline{16}, \tag{13}$$

we must have $\overline{3} \cdot b - \overline{2} \mid \overline{16}$. Thus, $\overline{3} \cdot b - \overline{2} \in \{1, \overline{2}, \overline{4}, \overline{8}, \overline{16}\}$. However, since $b \geq \overline{3}$, we have $\overline{3} \cdot b - \overline{2} \geq 7$, and thus, we can only have $\overline{3} \cdot b - \overline{2} = \overline{8}$, which has no solution b, or $\overline{3} \cdot b - \overline{2} = \overline{16}$, which means $b = \overline{6}$ and $a = \overline{2} \cdot b - 1 = \overline{11}$. So, in the case in which $c = \overline{2}$, we have only $(\overline{11}, \overline{6}, \overline{2})$ as a solution.

Suppose now that (ii) holds. Looking at (11) with $c = \overline{3}$, we note that not both of $b - \overline{3}$ and $b + \overline{3}$ can be multiples of $\overline{4}$ (given that their difference is $\overline{6}$). If $4 \nmid b - \overline{3}$, then $b - \overline{3} = i \cdot (\overline{2} \cdot k + 1)$ with $i \in \{1, \overline{2}\}$, and (11) becomes $p \cdot x = i \cdot (\overline{2} \cdot k + 1) \cdot (a + 1)$. By (9), $x = (\overline{2} \cdot k + 1) \cdot y$, for some y, so we have $p \cdot y = i \cdot (a + 1)$, so $p \leq \overline{2} \cdot (a + 1)$. Similarly, if $4 \nmid b + \overline{3}$, then $p \cdot y = i \cdot (a - 1)$; thus, $p \leq \overline{2} \cdot (a - 1)$. So, in any case, we have $p \leq \overline{2} \cdot (a + 1)$, that is, $\overline{3} \cdot a - b \leq \overline{2} \cdot (a + 1)$, which means $a - b \leq \overline{2}$. Since we also have $1 \leq a - b$, we can have only $a - b = 1$ or $a - b = \overline{2}$. If $a = b + 1$, then $n = \overline{2} \cdot b - 1$, which, being odd and a power of 2, must be 1, which is not possible, as it would imply $b = 1$. If $a = b + \overline{2}$, then $m = (b - 1) \cdot (b + \overline{3})$, and thus we must have $PT(b - 1)$ and $PT(b + \overline{3})$. Since $(b + \overline{3}) - (b - 1) = \overline{4}$, one of them must be $\overline{4}$, and, since $b \geq \overline{4}$, that one cannot be $b + \overline{3}$, so it must be $b - 1$, so $b = \overline{5}$ and $a = \overline{7}$. $\square$

4 Pythagorean Arithmetic Is the Right Setting

We may wonder whether we actually needed all of Pythagorean arithmetic to prove (10). From a methodological point of view, we have argued that, in the absence of A17, the usual properties of powers of 2 would not hold, and thus, the meaning of the terms involved would be altered. In that sense Pythagorean arithmetic is the right theory in which the question regarding the provability of (10) ought to be raised.

From a purely formal point of view, however, one is justified to ask whether (10) does not follow from weaker assumptions. Our proof already shows that it does. All we have used in it is PA^-, A16, and (9). That this is less than what Pythagorean arithmetic asks can be seen by noting that $\mathcal{C}(\mathbb{Q}(\sqrt{2})_{\mathbb{Z}}[X])$ is a model of PA^-, A16, and (9) (as there are no nonstandard powers of 2 in it), but not of Pythagorean arithmetic (which is plain, as A17 fails for $m = X$ and $n = \sqrt{2} \cdot X$).

However, the weak theory of the odd and the even, $PA^- + A16$, is not strong enough to prove (10). In fact, even if enlarged by (2) and (3), it still is not strong enough to prove (10).

Theorem 4.1 *$PA^- + A16 + (2) + (3)$ does not prove (10).*

Proof If D is an ordered integral domain and R is an ordered integral domain containing D, then we denote by $R_D[X, Y, Z]$ the ring of polynomials in X, Y, and Z, with free term in D and with all other coefficients in R, ordered by $\sum_{0 \le i,j,k \le n} c_{(i,j,k)} X^i Y^j Z^k > 0$ (here $c_{(0,0,0)} \in D$, and $c_{(i,j,k)} \in R$ for all $1 \le i, j, k \le n$) if and only if $c_{(u,v,w)} > 0$, where (u, v, w) is the greatest element, in the lexicographic ordering, among all the indices (i, j, k) of the nonzero coefficients $c_{i,j,k}$ of the terms of highest degree, that is, for which $i + j + k$ is maximal (i.e., $(u, v, w) = \max\{(i, j, k) : c_{(i,j,k)} \neq 0; i + j + k = d\}$, where d is the degree of the polynomial $\sum_{0 \le i,j,k \le n} c_{(i,j,k)} X^i Y^j Z^k$ and max is the greatest element in the lexicographic order). Let $\mathcal{C}(R_D[X, Y, Z])$ denote the positive cone of $R_D[X, Y, Z]$.

Then $\mathcal{C}(R_D[X, Y, Z])$, with $R = \mathbb{Z}_{\frac{1}{2}}$ and $D = \mathbb{Z}$, with

$$\left[\frac{\sum_{0 \le i,j,k \le n} c_{(i,j,k)} X^i Y^j Z^k}{2}\right] = \sum_{0 \le i,j,k \le n, i+j+k \neq 0} \frac{c_{(i,j,k)}}{2} X^i Y^j Z^k + \left[\frac{c_{(0,0,0)}}{2}\right],$$

is a model of PA, of A16, of (2), and of (3), but not of (10), for all of $XY - Z$, $YZ - X$, and $ZX - Y$ are positive and are powers of 2. □

References

[1] Kaye, R., *Models of Peano Arithmetic*, vol. 15 of *Oxford Logic Guides*, Oxford University Press, Oxford, 1991. Zbl 0744.03037. MR 1098499. 198

[2] Menn S., and V. Pambuccian, “Addenda et corrigenda to ‘The arithmetic of the even and the odd’,” *Review of Symbolic Logic*, vol. 9 (2016), pp. 638–40. MR 3569173. DOI 10.1017/S1755020316000204. 199

[3] Pambuccian, V. “The arithmetic of the even and the odd,” *Review of Symbolic Logic*, vol. 9 (2016), pp. 359–69. MR 3506912. DOI 10.1017/S1755020315000386. 199

[4] Schacht, C. "Another arithmetic of the even and the odd," *Review of Symbolic Logic*, submitted. 199

School of Mathematical and Natural Sciences
Arizona State University
Phoenix, Arizona 85069-7100
USA
pamb@asu.edu
http://www.public.asu.edu/~pusunac/index.html