Building the Biggest Box: Three-factor Polynomials and a Diophantine Equation

Author(s): GREGORY CONVERTITO and DAVID CRUZ-URIBE, OFS

Source: *Mathematics Magazine*, Vol. 89, No. 3 (June 2016), pp. 201-211
Published by: Taylor & Francis, Ltd. on behalf of the Mathematical Association of America
Stable URL: https://www.jstor.org/stable/10.4169/math.mag.89.3.201

Building the Biggest Box: Three-factor Polynomials and a Diophantine Equation

GREGORY CONVERTITO
Trinity College
gregory.convertito@trincoll.edu

DAVID CRUZ-URIBE, OFS
University of Alabama
dcruzuribe@ua.edu

As every instructor knows, and as most students come to realize, optimization problems are the bread and butter of introductory calculus. The following problem is ubiquitous.

> A box with an open top is to be constructed from a square piece of cardboard, 3 ft. wide, by cutting out a square from each of the four corners and bending up the sides. Find the largest volume that such a box can have. [**18**, Section 3.7]

From a pedagogical point of view this problem is nice since it requires optimizing a third degree polynomial: the first derivative has two critical points and a careful student will have to justify which one yields the solution to the problem.

Thinking pragmatically (e.g., with an eye to grading an exam question), the problem as stated above has the added benefit that the dimensions of the box with largest volume are rational. This leads to the following question: if we take the sheet of cardboard to be a rectangle, what other integer dimensions yield an answer which is rational? As the second author discovered (under the pressure of setting a make-up exam), it is not easy to find such examples, though they do exist. In this paper we give a complete answer to this question.

Theorem 1. *Let u and v be natural numbers with $u \geq v$ and $\gcd(u, v) = 1$. Then the equation*

$$\frac{A}{B} = \frac{1}{2} + \frac{3u^2 - v^2}{4uv}$$

gives all ratios $\frac{A}{B}$ such that a rectangle with integer side lengths A and B, $A \geq B$, will yield a rational solution to the box problem.

While the problem of rational solutions has been studied before (see the last section), we have not found this generating formula anywhere in the literature. Surprisingly, the proof of Theorem 1 reduces to a problem in elementary number theory: find all the solutions of the Diophantine equation

$$a^2 + 3b^2 = c^2, \quad a, b, c \in \mathbb{N}.$$

Math. Mag. **89** (2016) 201–211. doi:10.4169/math.mag.89.3.201.
MSC: Primary 11D09, Secondary 26A06.

*The results of this paper are research done by the first author and supervised by the second author as part of the Interdisciplinary Science Program of Trinity College. This research was partially supported by NSF grant 1362425. The authors would also like to thank President Berger-Sweeney of Trinity for her support during the final stages of this project.

This equation resembles the more famous Pythagorean equation

$$a^2 + b^2 = c^2,$$

and our proof is based on one of the many approaches to finding the integer solutions of this equation. The factor of 3, however, introduces some interesting difficulties into the proof.

However, rather than concentrating on the box problem, we want to consider a more general calculus problem that in turn leads to a more general Diophantine equation. We have not encountered this calculus problem before, and we hope that it will be a small but useful addition to the calculus repertoire.

To motivate this generalization, we start with the calculus part of the box problem. Given a cardboard rectangle with dimensions A and B, $A \geq B > 0$, maximizing the volume of the open top box requires finding the local maxima of the third degree polynomial

$$V = x(2x - A)(2x - B), \quad 0 < x < B/2.$$

Since maximizing V is the same as maximizing $2V$, we can replace $2x$ by x and consider instead the polynomial

$$y = x(x - A)(x - B). \tag{1}$$

The box problem imposes the natural constraint that A, B are positive, but in the abstract we can take $A, B \in \mathbb{Z}$.

We generalize this cubic polynomial by replacing x with x^m, $m \in \mathbb{N}$:

$$y = x(x^m - A)(x^m - B) = x^{2m+1} - (A + B)x^{m+1} + ABx, \quad A, B \in \mathbb{Z}. \tag{2}$$

By a small abuse of terminology we will call these three-factor polynomials. Geometrically, the graphs of these polynomials have some interesting properties depending on the parity of m and the signs of A and B. For example, suppose $m = 2$. If $A, B > 0$, the graph has five real roots; if $B < 0 < A$ then the graph has three real roots and three consecutive inflection points. See Figure 1.

When $m > 1$ this equation need not have rational roots, but its roots will all be "nice" in the sense that they are mth roots of integers; for brevity we call these m-rationals. We generalize the box problem by asking which values of A and B are such that the first and second derivatives of this polynomial also have m-rational roots. (In the box problem, the second derivative is linear and so always has rational roots.) The following theorem completely characterizes these values.

Theorem 2. *Given $m \in \mathbb{N}$, let u and v be natural numbers such that* $\gcd(u, v) = 1$ *and $u \geq \frac{v}{\sqrt{2m+1}}$. Then the equation*

$$\frac{A}{B} = \frac{1 + 2m - m^2}{(m+1)^2} \pm \frac{2m}{(m+1)^2}\sqrt{\left(\frac{(2m+1)u^2 + v^2}{2uv}\right)^2 - (2m+1)} \tag{3}$$

gives all ratios $\frac{A}{B}$, $A, B \in \mathbb{Z}$, such that the zeros of the first and second derivatives of the polynomial

$$y = x(x^m - A)(x^m - B)$$

are m-rational.

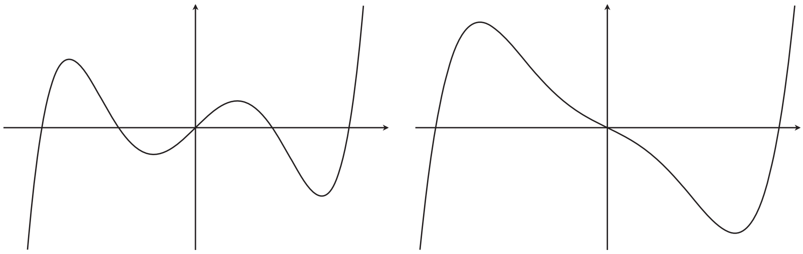

Figure 1 Graphs of three-factor polynomials with $m = 2$ (i.e., degree 5). The graph on the left has five distinct zeros and four local extrema. The graph on the right has three consecutive inflection points with no local extrema between.

The proof of Theorem 2 reduces to the solution of another Diophantine equation,

$$a^2 + kb^2 = c^2, \quad k,\ a,\ b,\ c \in \mathbb{N}, \tag{4}$$

and again the solution is similar to that of the classical Pythagorean equation. The interesting new facets of the proof come when we consider the role played by the prime factors of k.

In the remainder of this paper we first show how the problem of finding m-rational roots for a three-factor polynomial and its derivatives reduces to finding the solutions of (4). We will then derive the complete solution to this equation; for clarity we split the solution into three parts, which we give as Theorems 3, 4, and 5. We then work backwards to prove Theorems 1 and 2. Finally, we will briefly survey the history of the box problem and the underlying Diophantine equations. Both have been considered multiple times in the literature, though our solution employs some elegant number theory, especially with respect to Equation (4). Dickson [**6**] gives a solution, but ours is more detailed in its treatment of the generating formula.

It would be interesting to find other calculus examples that lead to interesting problems in number theory. We looked at a number of other optimization problems in Stewart [**18**] but for each one it was either trivial to determine when the solutions were rational or m-rational, or the solutions were never "nice."

From three-factor polynomials to $a^2 + kb^2 = c^2$

If we take the first and second derivatives of Equation (2), we get

$$\begin{aligned}
\frac{dy}{dx} &= (2m+1)x^{2m} - (A+B)(m+1)x^m + AB,\\
\frac{d^2y}{dx^2} &= 2m(2m+1)x^{2m-1} - m(A+B)x^{m-1}\\
&= x^{m-1}\big(2m(2m+1)x^m - m(A+B)\big).
\end{aligned}$$

It is immediate that the second derivative has zeros when $x = 0$ or when x is the mth root of a rational number. On the other hand, the first derivative is a quadratic in x^m and so its roots will be mth roots of rational numbers only when this quadratic has rational roots.

If we apply the quadratic equation, we see that $\frac{dy}{dx} = 0$ when

$$x^m = \frac{(A+B)(m+1) \pm \sqrt{(m+1)^2A^2 + (2m^2 - 4m - 2)AB + (m+1)^2B^2}}{2(2m+1)}.$$

Therefore, x^m is rational exactly when the discriminant

$$\sqrt{(m+1)^2A^2 + (2m^2 - 4m - 2)AB + (m+1)^2B^2}$$

is rational. If we remove a factor of B^2, then beneath the radical we get

$$(m+1)^2\left(\frac{A}{B}\right)^2 + (2m^2 - 4m - 2)\frac{A}{B} + (m+1)^2.$$

For this quantity to be the square of a rational number there must exist $f,\ g \in \mathbb{N}$, f and g coprime, such that

$$(m+1)^2\left(\frac{A}{B}\right)^2 + (2m^2 - 4m - 2)\frac{A}{B} + (m+1)^2 - \left(\frac{f}{g}\right)^2 = 0.$$

We again apply the quadratic formula to solve for the ratio $\frac{A}{B}$:

$$\frac{A}{B} = \frac{1 + 2m - m^2 \pm \sqrt{(m^2 - 2m - 1)^2 - (m+1)^2\left[(m+1)^2 - \left(\frac{f}{g}\right)^2\right]}}{(m+1)^2}. \tag{5}$$

The right-hand side is rational when there exist $p,\ q \in \mathbb{N}$ coprime such that

$$(m+1)^2\left(\frac{f}{g}\right)^2 - 4m^2(2m+1) = \left(\frac{p}{q}\right)^2;$$

equivalently,

$$p^2g^2 + 4(2m+1)m^2g^2q^2 = q^2f^2(m+1)^2.$$

In other words, we have shown that if the solution to $\frac{dy}{dx} = 0$ is m-rational, then we get a solution to the Diophantine equation

$$a^2 + (2m+1)b^2 = c^2, \quad a,\ b,\ c \in \mathbb{N}. \tag{6}$$

The general Diophantine equation

Though $2m + 1$ is odd, we will consider the Diophantine equation

$$a^2 + kb^2 = c^2, \quad a,\ b,\ c \in \mathbb{N}, \tag{7}$$

for any $k \in \mathbb{N}$. To find all solutions of this equation it will suffice to find all triples with no common factor; thus we define a primitive triple (a, b, c) to be any solution of (7) such that a, b, c are coprime.

Theorem 3. *Given $k \in \mathbb{N}$, let u and v be natural numbers such that* $\gcd(u, v) = 1$ *and $u \geq \frac{v}{\sqrt{k}}$, and let r be the greatest common divisor of $ku^2 - v^2$ and $2uv$. Then*

$$a = \frac{ku^2 - v^2}{r}, \quad b = \frac{2uv}{r}, \quad c = \frac{ku^2 + v^2}{r},$$

give all primitive triples (a, b, c) to Equation (7).

An interesting, hidden feature of this generating formula is that the factor r can only take on a limited number of values. When $k \equiv 1, 2, 3 \pmod 4$, we have the following elegant result.

Theorem 4. *Let $k \equiv 1, 2, 3 \pmod 4$ and let u and v be as in Theorem 3. Then r can only be equal to either $\gcd(v, k)$ or $2\gcd(v, k)$; the exact value depends on the parity of u and v and is given in Table 1.*

TABLE 1: Possible values for r when $k \equiv 1, 2, 3$.

	Value of r		
parity	$k \equiv 1$	$k \equiv 2$	$k \equiv 3$
u odd, v odd	$2\gcd(v, k)$	$\gcd(v, k)$	$2\gcd(v, k)$
u odd, v even	$\gcd(v, k)$	$\gcd(v, k)$	$\gcd(v, k)$
u even, v odd	$\gcd(v, k)$	$\gcd(v, k)$	$\gcd(v, k)$

We illustrate these cases with some examples of primitive triples (a, b, c) for various values of k and the generating triple $\langle u, v, r\rangle$. See Table 2.

TABLE 2: Primitive triples when $k \equiv 1,\ 2,\ 3$.

parity	$k \equiv 1$	$k \equiv 2$	$k \equiv 3$
u odd, v odd	$k = 5$	$k = 2$,	$k = 3$
	$\langle 3, 1, 2\rangle$,	$\langle 5, 1, 1\rangle$,	$\langle 3, 1, 2\rangle$,
	$(22, 3, 23)$	$(49, 10, 51)$	$(13, 3, 14)$
u odd, v even	$k = 5$	$k = 6$	$k = 7$
	$\langle 3, 4, 1\rangle$	$\langle 3, 2, 2\rangle$	$\langle 1, 2, 1\rangle$
	$(29, 24, 61)$	$(25, 6, 29)$	$(3, 4, 11)$
u even, v odd	$k = 9$	$k = 2$	$k = 3$
	$\langle 2, 3, 3\rangle$	$\langle 4, 3, 1\rangle$	$\langle 4, 3, 3\rangle$
	$(9, 4, 15)$	$(23, 24, 41)$	$(13, 8, 19)$

When $k \equiv 0 \pmod 4$, the restrictions on r, u, and v are slightly more complicated. Rewrite $k = 2^{2i}\lambda$, where $\lambda \equiv 1, 2, 3 \pmod 4$ and $i \in \mathbb{N}$. Then finding all primitive solutions to (7) is equivalent to finding all primitive solutions to the equation

$$a^2 + \lambda\beta^2 = c^2, \tag{8}$$

where $\beta = 2^i b$. We can do this by applying Theorem 4; however, to express our solution it is easier to modify the generating formulas.

Theorem 5. *Let $k \equiv 0 \pmod 4$, and fix $\lambda \equiv 1, 2, 3 \pmod 4$ and $i \in \mathbb{N}$ such that $k = 2^{2i}\lambda$. Then*

$$a = \frac{\lambda u^2 - v^2}{\gcd(v, \lambda)}, \quad b = \frac{2uv}{2^i \gcd(v, \lambda)}, \quad c = \frac{\lambda u^2 + v^2}{\gcd(v, \lambda)}$$

give all primitive triples to Equation (7) for k as given and for u and v coprime, $u \geq \frac{v}{\sqrt{\lambda}}$, subject to the restrictions in Table 3.

TABLE 3: Additional restrictions on u and v when $k \equiv 0$. N/A denotes a case which does not occur. The restrictions on u and v may give no extra information if $i = 1, 2$.

	$k \equiv 0$	
parity	$\lambda \equiv 1, 3$	$\lambda \equiv 2$
u, v odd	N/A	i=1 only
u odd, v even	$2^{i-1}\|v$	$2^{i}\|v$
u even, v odd	$2^{i-1}\|u$	$2^{i-1}\|u$

We now prove Theorems 3 through 5. To prove the generating formula in Theorem 3 we start with a given primitive triple and proceed in a fashion similar to that used to find all Pythagorean triples (cf. Courant & Robbins [**5**]).

Proof of Theorem 3. Let (a, b, c) be a primitive triple. Rewrite (7) as $\frac{c+a}{kb} = \frac{b}{c-a}$, and set this equal to $\frac{u}{v}$, where $u, v \in \mathbb{N}$ are coprime. We can then solve for the ratios $\frac{a}{b}$ and $\frac{c}{b}$:

$$\frac{a}{b} = \frac{ku^2 - v^2}{2uv} \quad \text{and} \quad \frac{c}{b} = \frac{ku^2 + v^2}{2uv}.$$

Note that this implies that $u \geq \frac{v}{\sqrt{k}}$.

The left-hand side of each equation is a fraction in lowest terms, and if the right-hand side were also in lowest terms, then we could equate numerators and denominators. However, in general this will not be the case. Let r be the greatest common factor of $ku^2 - v^2$ and $2uv$; then, since both fractions have denominator b on the left-hand side, we must also have that $r = \gcd(2uv, ku^2 + v^2)$. Therefore, we have the relation

$$a = \frac{ku^2 - v^2}{r}, \quad b = \frac{2uv}{r}, \quad c = \frac{ku^2 + v^2}{r}. \tag{9}$$

Conversely, given any choice of u and v with $\gcd(u, v) = 1$ and $u \geq \frac{v}{\sqrt{k}}$, define r as above. Then it is straightforward to show that (a, b, c) is a primitive triple. Therefore, the parameterization (9) completely characterizes the primitive solutions of the Diophantine Equation (7). ∎

The proof of Theorem 4 is a rather involved argument that looks at the prime factors of r modulo 4 to determine the possible values of r.

Proof of Theorem 4. We will show that r must always be equal to $\gcd(v, k)$ or $2\gcd(v, k)$ and then consider the relationship between the parity of u and v and the values of r. For brevity, let $(v, k) = \gcd(v, k)$, and define k_0 and v_0 by $k = k_0(v, k)$ and $v = v_0(v, k)$. Then $\gcd(v_0, k_0) = 1$ and we have that

$$r = \gcd\left(k_0(v, k)u^2 - v_0^2(v, k)^2, 2uv_0(v, k), k_0(v, k)u^2 + v_0^2(v, k)^2\right). \tag{10}$$

Hence, $(v, k)|r$ and so we can rewrite r as $r = r_0(v, k)$. Suppose first that $r_0 \neq 2^j$, $j \geq 0$. Then there exists a prime $q \neq 2$ that divides r_0; in particular, a larger power of q must divide r than divides (v, k). Therefore, by (10) we must have that $q|2uv_0$; since $q \neq 2$, $q|u$ or $q|v_0$. Suppose $q|u$; since we also have that $q|k_0u^2 \pm v_0^2(v, k)$, we have that q divides $v_0^2(v, k)$ which is impossible since u and v are coprime. On the other hand, suppose $q|v_0$. Then, since $q|2k_0u^2$, and v_0 and k_0 are relatively prime, $q|u$ which contradicts the fact that u and v are coprime.

Therefore, we must have that $r_0 = 2^j$, $j \geq 0$. We will now show that $j = 0, 1$. Suppose to the contrary that $j \geq 2$. Then arguing as before we must have that $r_0|2uv_0$, so $2|u$ or $2|v_0$. If $2|u$, then we get $2|v$, a contradiction. If $2|v_0$ we get $2|k_0u^2$, and since $\gcd(v_0, k_0) = 1$, $2|u$ which is again a contradiction. Therefore, $r_0 = 1,\ 2$.

We now show that the value of r_0 depends on the parity of u and v. We consider the three cases $k \equiv 1, 2, 3 \pmod 4$ in turn. For brevity, all equivalences should be read as modulo 4. First suppose that $k \equiv 1$. If u and v are both odd, then $ku^2 - v^2 \equiv 0$, $ku^2 + v^2 \equiv 2$, and $2uv \equiv 2$. Each is divisible by 2, but (v, k) is odd. Hence, $r = 2(v, k)$. If u is odd and v is even, then, $ku^2 - v^2 \equiv 1$, $ku^2 + v^2 \equiv 1$, and $2uv \equiv 0$. There is no common factor of 2, so $r = (v, k)$. Finally, if u is even and v odd, then $ku^2 - v^2 \equiv 3$, $ku^2 + v^2 \equiv 1$, and $2uv \equiv 0$. There is again no common factor of 2, and so $r = (v, k)$.

Now suppose $k \equiv 2$. If u and v are both odd, then, $ku^2 - v^2 \equiv 1$, $ku^2 + v^2 \equiv 3$, and $2uv \equiv 2$, and so $r = (v, k)$. If u is odd and v is even, then $ku^2 - v^2 \equiv 2$, $ku^2 + v^2 \equiv 2$, and $2uv \equiv 0$. There is a common factor of 2, but (v, k) is even, and since not all of the terms are divisible by 4, we must have $r = (v, k)$. If u is even and v is odd, then $ku^2 - v^2 \equiv 3$, $ku^2 + v^2 \equiv 1$, and $2uv \equiv 0$, so $r = (v, k)$.

Finally, suppose $k \equiv 3$. If u and v are both odd, then, $ku^2 - v^2 \equiv 2$, $ku^2 + v^2 \equiv 0$, and $2uv \equiv 2$. There is a common factor of 2 and (v, k) is odd, so we have $r = 2(v, k)$. If u is odd and v is even, then $ku^2 - v^2 \equiv 3$, $ku^2 + v^2 \equiv 3$, and $2uv \equiv 0$, so $r = (v, k)$. And if u is even and v is odd, then, $ku^2 - v^2 \equiv 3$, $ku^2 + v^2 \equiv 1$, and $2uv \equiv 0$, so again, $r = (v, k)$. ■

Finally, we prove Theorem 5, which covers the case in which $k \equiv 0 \pmod 4$. The heart of the proof is determining how many powers of 2 can be present in u, v, and r when $k = 2^{2i}\lambda$.

Proof of Theorem 5. Let k, λ, and i be as given. Then by Theorems 3 and 4, all the primitive triples a, β, c for Equation (8) are given by

$$a = \frac{\lambda u^2 - v^2}{r}, \quad \beta = \frac{2uv}{r}, \quad c = \frac{\lambda u^2 + v^2}{r},$$

where u and v are coprime, $u \geq \frac{v}{\sqrt{\lambda}}$, and r is from Table 1. To get the desired solutions to Equation (7) we need to account for the additional restrictions imposed by the fact that $2^i b = \beta$.

We first consider the case $\lambda \equiv 1, 3 \pmod 4$. Let u and v be odd. Then

$$2^i b = \beta = \frac{2uv}{2\gcd(v, \lambda)} = \frac{uv}{\gcd(v, \lambda)}.$$

Hence, $2^i|uv$. However, u and v are both odd, so this is impossible. Therefore, when $\lambda \equiv 1, 3$ we must have that $r = \gcd(v, \lambda)$. Now, let u be odd and v even. Then

$$2^i b = \beta = \frac{2uv}{\gcd(v, \lambda)},$$

and so $2^i|2uv$ which gives $2^{i-1}|v$. (When $i = 1,\ 2$ we get no additional information about v.) Finally, let u be even and v odd. Then, $2^i|2uv$, so $2^{i-1}|u$. (Again, we get no additional information when $i = 1,\ 2$.)

Next we consider the case $\lambda \equiv 2 \pmod 4$. By Theorem 4, $r = \gcd(v, \lambda)$. Let u and v odd; then

$$2^i b = \beta = \frac{2uv}{\gcd(v, \lambda)}.$$

Since $\gcd(v, \lambda)$ is odd, $2^{i-1}|uv$, but this is only possible when $i = 1$. Now let u be odd and v even. Then

$$2^i b = \beta = \frac{2uv}{\gcd(v, \lambda)} = \frac{uv}{\gcd(v/2, \lambda/2)}.$$

Hence, $2^i|uv$, so $2^i|v$. Finally, let u be even and v odd. Then

$$2^i b = \beta = \frac{2uv}{\gcd(v, \lambda)},$$

so $2^{i-1}|u$. If we combine the results from both cases, we get the desired conclusion. ■

Solving the original problem

Given Theorems 3 and 4, we can now reverse the steps of our analysis and find all three-factor polynomials whose first derivatives have m-rational roots, thus proving Theorem 2. Since $k = 2m + 1$ we only need to consider the cases $k \equiv 1, 3 \pmod 4$ from Theorem 4. We will then take $m = 1$ and prove Theorem 1 and so characterize the rational solutions of the box problem.

Proof of Theorem 2. Recall that in our original reduction to the Diophantine Equation (6) we set $b = 2gmq$ and $c = (m + 1)fq$. If we solve for the ratio $\frac{f}{g}$ and combine this with our generating formulas (9) from Theorem 3 we get

$$\frac{f}{g} = \left(\frac{c}{b}\right)\left(\frac{2m}{m+1}\right) = \left(\frac{(2m+1)u^2 + v^2}{2uv}\right)\left(\frac{2m}{m+1}\right).$$

If we substitute this into (5) and simplify, then we have Equation (3):

$$\frac{A}{B} = \frac{1 + 2m - m^2}{(m+1)^2} \pm \frac{2m}{(m+1)^2}\sqrt{\left(\frac{(2m+1)u^2 + v^2}{2uv}\right)^2 - (2m+1)}.$$

Note that since we are concerned with ratios, the factor r disappears and our formula only depends on m and our choices of u and v. Theorem 3 gives us the restrictions $\gcd(u, v) = 1$ and $u \geq \frac{v}{\sqrt{2m+1}}$. This completes the proof. ■

The following refinement of Theorem 2 is useful to prove Theorem 1.

Corollary 6. *If we restrict $A, B > 0$ or $A, B < 0$, then it suffices to choose $u \geq v$, $\gcd(u, v) = 1$, and the negative branch of Equation* (3) *is impossible.*

Proof. Since A and B must have the same sign, without loss of generality we may assume $\frac{A}{B} \geq 1$. Given this, if we denote the expression under the radical by R, then we must have that

$$1 + 2m - m^2 \pm 2m\sqrt{R} \geq (m+1)^2,$$

which implies that $\pm\sqrt{R} \geq m$, so the negative branch is impossible. Moreover, $R \geq m^2$ which implies

$$(2m+1)u^2 + v^2 \geq 2(m+1)uv.$$

Since $u \geq \frac{v}{\sqrt{2m+1}}$, if we fix a, $0 < a \leq \sqrt{2m+1}$ such that $u = \frac{v}{a}$, then we may rewrite the above inequality as the quadratic expression

$$a^2 - 2(m+1)a + (2m+1) \geq 0.$$

This holds provided that a is not between the two roots of the quadratic:

$$a = \frac{2(m+1) \pm \sqrt{4(m+1)^2 - 4(2m+1)}}{2} = 1,\ 2m+1.$$

Since $a \leq \sqrt{2m+1}$, we must have $a \leq 1$. In other words, to find ratios $\frac{A}{B} \geq 1$, we should take $u \geq v$. ■

Theorem 1 now emerges as a corollary to the work done above by setting $m = 1$.

Proof of Theorem 1. Since we assume that $A \geq B > 0$, by Corollary 6, we need only take $u \geq v$ and we eliminate the negative branch of Equation (3). Thus, if we set $m = 1$, we get that all solutions to (1) are given by

$$\frac{A}{B} = \frac{1}{2} + \frac{3u^2 - v^2}{4uv}.$$

The change of variables that yielded (1) does not change the ratio of solutions, so this equation gives all the solutions to the original box problem. ■

A brief history of the problem

As we noted at the beginning, the box problem itself is now a staple of calculus textbooks. Besides Stewart [**18**], a random check of current books showed that it is also in Larson and Edwards [**12**], Rogawski [**17**], and Varberg, Purcell and Rigdon [**21**]. Going back in time, it is in the classic calculus book by Thomas [**19**]. Going further back, it can be found in books from 1917 [**14**], 1909 [**13**], and 1875 [**16**]. The earliest appearance we could find was in the 1852 text *A Treatise on the Differential Calculus* by Isaac Todhunter [**20**]. However, we suspect the problem was considered even earlier in some form.

The problem of finding dimensions for the rectangle that yields rational solutions has also been considered by several different authors: see Dundas [**9**], Coll *et al.* [**4**] (who give the same solution as Dickson [**6**]); Graham and Roberts [**11**], Duemmel [**8**] (who confronted the same problem writing an exam as did the second author); Buddenhagen *et al.* [**2**]. (Hereafter, we adopt the notation of our sources for ease of reference). The last three papers all begin their analysis in a way similar to us but focus on the Diophantine equation $a^2 + b^2 - ab = c^2$, though Graham and Roberts transform this equation to the same form as ours: $n^2 + 3m^2 = c^2$. All of these authors generalized their results in a variety of ways, but none considered the general Diophantine Equation (4). Dundas's exhaustive treatment of differently shaped boxes was the initial inspiration for our generalization to three-factor polynomials.

Three-factor polynomials do not seem to have appeared in the literature, at least in this form. However, a much deeper generalization of the original question is the problem of finding polynomials with integer coefficients such that they and all their derivatives have rational roots. For a survey of this problem with extensive references, see Buchholz and MacDougall [**1**].

Equation (4) has a long and interesting history. One of the earliest treatments of this specific equation is found in the work of the Japanese mathematician Matsunaga from the first half of the eighteenth century [**15**] (pp. 229–232). He dealt with the equation $rx^2 + y^2 = z^2$, and gave the infinite family of solutions $x = 2mn$, $y = rm^2 - n^2$, $z = rm^2 + n^2$, where n is "even or odd according as r is odd or even," and not divisible by r. This is similar to our solutions, but he apparently did not analyze the subtleties of the different cases. The historical context for Matsunaga's work on the problem is intriguing: he was part of the *Rangaku* ("Dutch Study") movement during the Tokugawa shogunate: a group of Japanese scholars who kept up with Western science through contact with the Dutch at the trading post of Dejima, the only foreigners allowed in Japan during this isolationist period [**10**].

In Europe, Equation (4) was probably studied by the early 18th century. More general equations were treated, at least in part, by Lagrange ($Ar^2 = p^2 - Bq^2$), Euler ($\alpha f^2 + \beta g^2 = \gamma h^2$), Minding ($x^2 = Ay^2 + Bz^2$), and Dirichlet ($ax^2 + by^2 + cz^2 = 0$): see Dickson, *History of the Theory of Numbers, Vol. 2* (pp. 420–423) [**7**]. Solutions of this exact equation can be found in Carmichael, *Diophantine Analysis* [**3**] and Dickson, *Introduction to the Theory of Numbers* [**6**]. Carmichael, through other methods, shows that

$$x = mn^2 + Dn^2, \quad y = 2mn, \quad z = m^2 - Dn^2$$

is *a* set of solutions, but then proceeds to prove it is the general set of solutions in a rather roundabout way: he first solves $x^2 - Dy^2 = 1$ for rational solutions, then introduces a number of auxiliary variables and uses them to find the special cases when these solutions are integers. Then he arrives at a method of generating solutions to $x^2 - Dy^2 = \sigma^2$ for a chosen σ, and explains that "In order to apply the theorem in a particular case it is necessary first to find, by inspection or otherwise, the least positive integral solution." Dickson gives a solution similar to ours. Neither author, however, gives the analysis of the generating terms that we give in Theorems 4 and 5.

Acknowledgment We are grateful to our colleague Jeffrey Bayliss, a historian of Japan, for calling our attention to the historical setting of Matsunaga's work.

REFERENCES

1. R. H. Buchholz, J. A. MacDougall, When Newton met Diophantus: A study of rational-derived polynomials and their extension to quadratic fields, *J. Number Theory* **81** no. 2 (2000) 210–233.
2. J. Buddenhagen, C. Ford, M. May, Nice cubic polynomials, pythagorean triples, and the law of cosines, *Math. Mag.* **65** no. 4 (1992) 244–249.
3. R. D. Carmichael, *Diophantine Analysis*. Dover, New York, 1915.
4. V. E. Coll, J. Davis, M. Hall, C. Magnant, J. Stankewicz, H. Wang, Integer solutions to box optimization problems, *College Math. J.* **45** no. 3 (2014) 180–190.
5. R. Courant, H. Robbins, *What is Mathematics?* Oxford Univ. Press, Oxford, 1996.
6. L. E. Dickson, *Introduction to the Theory of Numbers*. Univ. of Chicago Press, Chicago, 1929.
7. ———, *History of the Theory of Numbers Vol. 2: Diophantine Analysis*. Carnegie Institution of Washington, Washington, DC, 1920.
8. J. Duemmel, From calculus to number theory, *Amer. Math. Monthly* **96** no. 2 (1989) 140–143.
9. K. Dundas, To build a better box, *College Math. J.* **15** no. 1 (1984) 30–36.
10. G. K. Goodman, *The Dutch Impact on Japan (1640–1853)*. E. J. Brill, Leiden, The Netherlands, 1967.
11. G. P. Graham, C. E. Roberts, A Diophantine equation from calculus, *Math. Mag.* **62** no. 2 (1989) 97–101.
12. R. Larson, B. Edwards, *Calculus*. Cengage Learning, Independence, KY, 2013.
13. A. E. H. Love, *The Elements of the Differential Calculus: Founded on the Method of Rates Or Fluxions*. At the Univ. Press, 1909.
14. H. W. March, H. C. Wolff, *Calculus*. Modern Mathematical Texts. McGraw-Hill, New York, 1917.
15. Y. Mikami, *The Development of Mathematics in China and Japan*. Abhandlungen zur Geschichte der mathematischen Wissenschaften mit Einschluss ihrer Anwendungen. B G. Teubner, Leipzig, 1913, http://name.umdl.umich.edu/acd4271.0008.001.
16. J. M. Rice, W. W. Johnson, *The Elements of the Differential Calculus: Founded on the Method of Rates Or Fluxions*. J. Wiley & Son, New York, 1875.

17. J. Rogawski, *Calculus*. W. H. Freeman, New York, 2011.
18. J. Stewart, *Calculus*. Seventh edition. Cengage Learning, Independence, KY, 2011.
19. G. B. Thomas, *Calculus and Analytic Geometry*. Addison-Wesley Mathematics Series. Addison-Wesley, Reading, MA, 1953.
20. I. Todhunter, *A Treatise on the Differential Calculus and the Elements of the Integral Calculus: With Numerous Examples*. MacMillan, New York, 1852.
21. D. Varberg, E. Purcell, S. Rigdon, *Calculus*. Ninth edition. Prentice Hall, Englewood Cliffs, NJ, 2007.

Summary. We consider a well known calculus question, and show that the solution of this problem is equivalent to finding integer solutions to a Diophantine equation. We generalize the calculus question, which in turn leads to a more general Diophantine equation. We give solutions to all of these and describe some of the historical background.

DAVID CRUZ-URIBE, OFS (MR Author ID: 329597 is professor and chair of mathematics at the University of Alabama in Tuscaloosa, AL. Prior to this, he spent nineteen years on the faculty at Trinity College, Hartford, CT. His research is in harmonic analysis and partial differential equations; this foray into number theory was fascinating but unintended.

GREGORY CONVERTITO (MR Author ID: 1146505 is a senior at Trinity College in Hartford, Connecticut. He studies mathematics and philosophy, and enjoys sailing and sitting on the beach, reading.

Ask Siri . . .

A: What is 4 divided by 0?
S: The answer is definitely . . . undefined.

$$4 \div 0 = \text{undefined}$$

Submitted by Anneliese Jones, Ann Arbor, MI