# Formal Proof of the Cannonball Problem

int-y1

October 22, 2023

The cannonball problem asks for all positive integers that are both square and square pyramidal. Square numbers are of the form $x^2$, and square pyramidal numbers are of the form $1^2+2^2+\cdots+x^2 = x(x+1)(2x+1)/6$.

This Lean 4 proof shows that the only positive integer solutions to $x(x+1)(2x+1) = 6y^2$ are $(x, y) = (1, 1), (24, 70)$. As a corollary, 1 and 4900 are the only positive integers that are both square and square pyramidal.

The Lean 4 proof follows W. S. Anglin's proof, which I have copy-pasted below. However, I changed parts of the proof to make it easier to translate to Lean 4. The additions are highlighted in teal and the deletions contain a strikethrough. There are 2 notable changes that I made to Anglin's proof:

- In Lemma 1.1, I added the fact that $w/\gcd(x, y)$ needs to be an integer.
- In Lemma 2.5, I rewrote the statement of this lemma.

## 1 Solutions where $x$ is even

Suppose, then, that $x$ is even. Under this assumption we can solve the equation with the help of the following three lemmas which were probably all known to Fermat.

**Lemma 1.1.** *The area of a Pythagorean triangle is never a square.*

*Proof.* Suppose, on the contrary, there are Pythagorean triangles with square areas. Let $w^2$ be the smallest area for which such a triangle exists. Let $x$ and $y$ be the legs of a Pythagorean triangle with area $w^2$. Then $x^2 + y^2 = z^2$ for some integer $z$, and $xy/2 = w^2$. Note that $x/\gcd(x, y)$ and $y/\gcd(x, y)$ are the legs of a Pythagorean triangle with area $(w/\gcd(x, y))^2$. Also note that $w/\gcd(x, y)$ is an integer because $\gcd(x, y)^2 \mid xy = 2w^2$, and $a^2 \mid 2b^2$ implies $a \mid b$. Since $w$ is minimal, $x$ and $y$ are relatively prime (i.e. $\gcd(x, y) = 1$). ~~and, without loss of generality, we may take $x$ odd and $y$ even. (It follows by a congruence consideration modulo 4 that $x$ and $y$ are not both odd.)~~ By the well-known theorem for Pythagorean triangles, there are relatively prime positive integers $r$ and $s$ of different parity such that, without loss of generality, $x = r^2 - s^2$ and $y = 2rs$. Hence $(r^2 - s^2)rs = w^2$ and $s/4 < s \le w^2$. From $r > 0$, $s > 0$, and $x = r^2 - s^2 > 0$, it follows that $r - s > 0$. Since $r$, $s$, $r - s$ and $r + s$ are positive and pairwise relatively prime, and since $(r - s)(r + s)rs = w^2$, it follows that there are positive integers $a$, $b$, $c$ and $d$ such that $r = a^2$, $s = b^2$, $a^2 - b^2 = r - s = c^2$ and $a^2 + b^2 = r + s = d^2$. ~~Note that $c$ and $d$ are relatively prime since $r - s$ and $r + s$ are relatively prime.~~ Noting also that $c$ and $d$ are odd (because $r$ and $s$ have different parity), let $X = (c + d)/2$ and $Y = (d - c)/2$. Then $X^2 + Y^2 = a^2$. From $2XY = b^2$, it follows that $2 \mid b$, so $XY/2 = (b/2)^2 = s/4$ is a square. ~~Then $X$ and $Y$ are relatively prime and $X^2 + Y^2 = a^2$. Hence one of $X$ and $Y$ is even, and $XY/2 = (d^2 - c^2)/8 = b^2/4 = s/4$ is a square integer.~~ Since the triangle with sides $X$, $Y$ and $a$ is a Pythagorean triangle with square area $s/4$, it follows from the minimality of $w^2$ that $w^2 \le s/4$. Contradiction. □

**Corollary 1.2.** *Let $(x, y, z, w)$ be an integer solution to $x^2 + y^2 = z^2$ and $xy/2 = w^2$. Then either $x = 0$ or $y = 0$.*

*Proof.* For the sake of contradiction, suppose $x \neq 0$ and $y \neq 0$. If $x$ and $y$ have the same sign, then $(|x|, |y|)$ violates Lemma 1.1. If $x$ and $y$ have different signs, then $w^2 = xy/2 < 0$ has no solutions in $w$. □

**Lemma 1.3.** *There are no positive integers $x$ such that $2x^4 + 1$ is a square.*

*Proof.* To obtain a contradiction, suppose that $(x, y)$ is the least positive integer solution of $2x^4 + 1 = y^2$. Then for some positive integer $s$, $y = 2s + 1$ and $x^4 = 2s(s + 1)$. If $s$ is odd then $s$ and $2(s + 1)$ are relatively prime and, for some integers $u$ and $v$, $s = u^4$ and $2(s + 1) = v^4$. This gives $2(u^4 + 1) = v^4$ ~~with $u$ odd and $v$ even. Hence we have $2(1 + 1) \equiv 0 \pmod 8$~~. However, $2(u^4 + 1) \bmod 8 \in \{2, 4\}$ and $v^4 \bmod 8 \in \{0, 1\}$. Since this is impossible, $s$ cannot be odd. Since $s$ is even, $2s$ and $s + 1$ are relatively prime, and there are integers $u$ and $v$, both greater than 1, such that $2s = u^4$ and $s + 1 = v^4$. Let $w$ be the positive integer such that $u = 2w$. Let $a$ be the positive integer such that $v^2 = 2a + 1$. Then $u^4/2 + 1 = s + 1 = v^4$ so that $2w^4 = (v^4 - 1)/4 = a(a + 1)$. Since $v^2 = 2a + 1$, it follows from congruence considerations modulo 4 that $a$ is even. Since $2w^4 = a(a + 1)$, it follows that there are positive integers $b$ and $c$ such that $a = 2b^4$ and $a + 1 = c^4$. However, this implies that $2b^4 + 1 = (c^2)^2$ and hence $y \le c^2$ (by the minimality of $(x, y)$). On the other hand, $c^2 \le a + 1 < v^2 \le s + 1 < y$. Contradiction. □

**Corollary 1.4.** *Let $(x, y)$ be an integer solution to $2x^4 + 1 = y^2$. Then $x = 0$.*

**Lemma 1.5.** *There is exactly one positive integer $x$, namely, 1, such that $8x^4 + 1$ is a square.*

*Proof.* Firstly, $8x^4 + 1 \ne (2s)^2$ because $8x^4 + 1$ is odd and $(2s)^2$ is even. Suppose $8x^4 + 1 = (2s + 1)^2$. Then $2x^4 = s(s + 1)$. If $s$ is even then there are integers $u$ and $v$ such that $s = 2u^4$ and $s + 1 = v^4$. In that case, $2u^4 + 1 = s + 1 = v^4$ and, by Corollary 1.4 ~~Lemma 1.3~~, $u = 0$ and, hence, $x = 0$. If $s$ is odd then there are integers $u$ and $v$ such that $s = u^4$ and $s + 1 = 2v^4$. In that case, $u^4 + 1 = 2v^4$, and so, $u$ is odd. Using $v^4 = (u^4 + 1)/2$ and $u = 2u' + 1$, we have $(v^4 - u^2)/2 = (2u'^2 + 2u')^2$ and $(v^4 + u^2)/2 = (2u'^2 + 2u' + 1)^2$. ~~Since $u$ is odd, a congruence consideration modulo 4 shows that $v$ is odd. Squaring both sides of $u^4 + 1 = 2v^4$, we obtain $4v^8 - 4u^4 = u^8 - 2u^4 + 1$ and hence $(v^4 - u^2)(v^4 + u^2) = ((u^4 - 1)/2)^2$, an integer square. Since $v^4$ and $u^2$ are relatively prime,~~ it follows that both $(v^4 - u^2)/2$ and $(v^4 + u^2)/2$ are integer squares. Now $(v^2 - u)^2 + (v^2 + u)^2 = 4(v^4 + u^2)/2 = A^2$ and $(v^2 - u)(v^2 + u)/2 = (v^4 - u^2)/2 = B^2$. By Corollary 1.2, ~~Lemma 1.1, this is impossible unless~~ $v^2 = \pm u$. Since $u^4 + 1 = 2v^4$, we obtain $u^4 - 2u^2 + 1 = 0$ and $u^2 = 1$. From this it follows that $s = 1$ and $x = \pm 1$. □

**Lemma 1.6.** *Suppose $x$ and $y$ are nonnegative and coprime. Suppose $xy/3$ is a square. Then $x \not\equiv 2 \pmod 3$.*

*Proof.* Firstly, $3 \mid xy$. If $3 \mid x$ then $x \equiv 0 \pmod 3$. Otherwise, suppose $3 \mid y$ and $y = 3k$. Then $x$ and $k$ are coprime and $xk$ is a square. It follows that $x$ is a square, and therefore, $x \bmod 3 \in \{0, 1\}$. □

With the above three lemmas, we are now in a position to solve $x(x + 1)(2x + 1) = 6y^2$ under the assumption that $x$ is even. Suppose, then, that $x$ is even. Then $x + 1$ is odd. Since $x/2$ ~~$x$~~, $x + 1$ and $2x + 1$ are relatively prime in pairs, it follows from Lemma 1.6 that ~~that $x + 1$ and $2x + 1$ (both being odd) are either squares or triples of squares. Thus~~ $x + 1 \not\equiv 2 \pmod 3$ and $2x + 1 \not\equiv 2 \pmod 3$. Hence $x \equiv 0 \pmod 3$, and for some nonnegative integers $p$, $q$ and $r$, we have $x = 6q^2$, $x + 1 = p^2$ and $2x + 1 = r^2$. Thus $6q^2 = (r - p)(r + p)$. Since $p$ and $r$ are both odd, 4 is a factor of $(r - p)(r + p) = 6q^2$ and thus $q$ is even. Let $q'$ be the integer such that $q = 2q'$. We now have $6q'^2 = ((r - p)/2)((r + p)/2)$ and, since $(r - p)/2$ and $(r + p)/2$ are relatively prime (because $r^2$ and $p^2$ are relatively prime), we obtain one of the following two cases.

Case (i). One of $(r - p)/2$ and $(r + p)/2$ has the form $6A^2$ and the other has the form $B^2$ (where $B$ is positive ~~$A$ and $B$ are nonnegative integers~~). Then $p = \pm(6A^2 - B^2)$ and $6q^2 = 4(6q'^2) = 4(6A^2B^2)$ $\cancel{q = 2AB}$. Since $6q^2 + 1 = x + 1 = p^2$, we have $24A^2B^2 + 1 = (6A^2 - B^2)^2$ or $(6A^2 - 3B^2)^2 - 8B^4 = 1$. By Lemma 1.5, $B = 1$ ~~$B = 0$ or $1$~~ and, hence, $A^2 \in \{0, 1\}$ and $x = 6q^2 = 0$ or 24. The only nontrivial solution is thus with $x = 24$.

Case (ii). One of $(r - p)/2$ and $(r + p)/2$ has the form $3A^2$ and the other has the form $2B^2$ (where $B$ is positive ~~$A$ and $B$ are nonnegative integers~~). Then $p = (3A^2 - 2B^2)$ and $6q^2 = 4(6q'^2) = 4(6A^2B^2)$ $\cancel{q = 2AB}$. This gives $24A^2B^2 + 1 = (3A^2 - 2B^2)^2$ and hence $(3A^2 - 6B^2)^2 - 2(2B)^4 = 1$. This contradicts Lemma 1.3. ~~By Lemma 1.3, $B = 0$ and hence $x = 6q^2 = 0$.~~

Thus when $x$ is even, the only solution to Lucas's puzzle is $x = 24$ cannonballs along the base of the square pyramid.

## 2 Solutions where $x$ is odd

We have solved Lucas's problem under the assumption that $x$ is even. In this section we solve it under the assumption that $x$ is odd. To do this, we first investigate the solutions of the Diophantine equation $X^2 - 3Y^2 = 1$.

Let $a = 2+\sqrt{3}$ and $b = 2-\sqrt{3}$. Note that $ab = 1$. Where $n$ is any nonnegative integer, let $u_n = (a^n+b^n)/2$ and $v_n = (a^n - b^n)/(2\sqrt{3})$. Then $u_n$ and $v_n$ are integers, and it is a well-known result (from the theory of the Pell equation) that when $n \geq 1$, $(u_n, v_n)$ is the $n$th positive integer solution of $X^2 - 3Y^2 = 1$. Of course, when $n = 0$, we have the solution $X = 1$ and $Y = 0$.

In order to show that $x = 1$ is the only odd positive integer such that $x(x+1)(2x+1)$ has the form $6y^2$, we use the following lemmas.

**Lemma 2.1.** *Where $m$ and $n$ are nonnegative integers, $u_{m+n} = u_m u_n + 3v_m v_n$ and $v_{m+n} = u_m v_n + u_n v_m$. Also if $m - n \geq 0$, then $u_{m-n} = u_m u_n - 3v_m v_n$ and $v_{m-n} = -u_m v_n + u_n v_m$.*

*Proof.* This follows from results already in mathlib4 $\ddot\smile$ ~~by straight calculation from the definitions of $u_n$ and $v_n$~~. □

Using Lemma 2.1, it is not hard to obtain the following result.

**Lemma 2.2.** *Where $m$ is a nonnegative integer, $u_{m+2} = 4\cancel{2u_1}u_{m+1} - u_m$ and $v_{m+2} = 4\cancel{2u_1}v_{m+1} - v_m$.*

Using the fact that $(u_m, v_m)$ is a solution of $X^2 - 3Y^2 = 1$, we also have the following.

**Lemma 2.3.** *Where $m$ is a nonnegative integer, $u_{2m} = 2u_m^2 - 1 = 6v_m^2 + 1$ and $v_{2m} = 2u_m v_m$.*

**Lemma 2.4.** *Let $m$, $n$ and $r$ be nonnegative integers such that $2rm - n$ is nonnegative. Then $u_{2rm\pm n} \equiv (-1)^r u_n \pmod{u_m}$.*

*Proof.* Using mathematical induction on $r$ together with Lemma 2.1, we can show that $u_{(2r+1)m} \equiv 0 \pmod{u_m}$ and $v_{2rm} \equiv 0 \pmod{u_m}$. Since, by Lemma 2.3, $u_{2rm} = 2u_{rm}^2 - 1 = 6v_{rm}^2 + 1$, it follows that $u_{2rm} \equiv (-1)^r \pmod{u_m}$. Thus $u_{2rm\pm n} = u_{2rm}u_n \pm 3v_{2rm}v_n \equiv (-1)^r u_n \pmod{u_m}$ (using Lemma 2.1). □

Let us consider the first few values of $u_n$. Starting with $n = 0$, we have $1, 2, 7, 26, 97, 362$, and so on. If we consider these values modulo 5, we have $1, 2, 2, 1, 2, 2, \ldots$. By Lemma 2.2 it follows that this sequence is periodic. If we consider the values of $u_n$ modulo 8, we obtain $1, 2, 7, 2, 1, 2, \ldots$. By Lemma 2.2, this is a purely periodic sequence with period length 4. Note that when $n$ is even, $u_n$ is odd. Using the laws of quadratic reciprocity, the above comments lead us to the following two lemmas.

**Lemma 2.5.** ~~*If $n$ is even then $u_n$ is an odd nonmultiple of 5 and $\left(\frac{5}{u_n}\right) = 1$ iff $n$ is a multiple of 3.*~~ *Suppose $n$ is even. Firstly, $u_n$ is odd. Secondly, $u_n$ is not a multiple of 5. Thirdly, $\left(\frac{5}{u_n}\right) = -1$ iff $n$ is not a multiple of 3. (This lemma was rewritten so that it can be used in Lemma 2.7)*

**Lemma 2.6.** *If $n$ is even then $u_n$ is odd and $\left(\frac{-2}{u_n}\right) = 1$ iff $n$ is a multiple of 4.*

The following and final lemma was first proved by Ma.

**Lemma 2.7.** *Where $n$ is a nonnegative integer, $u_n$ has the form $4M^2 + 3$ only when $u_n = 7$.*

*Proof.* Suppose $u_n = 4M^2 + 3$. Then $u_n \equiv 3$ or $7 \pmod 8$ and, from the sequence of values of $u_n$ modulo 8, it follows that $n$ has the form $8k \pm 2$. If $k = 0$, then $n = 2$ and $u_n = 7$ and we're done. Otherwise, suppose $k > 0$ so that ~~Suppose~~ $n \neq 2$ (and hence $u_n \neq 7$). Then we can write $n$ in the form $2k'2^s \pm 2$ where $k'$ is odd and $s \geq 2$. By Lemma 2.4, $u_n = u_{2k'2^s\pm 2} \equiv (-1)^{k'} u_2 \pmod{u_{2^s}}$. Since $k'$ is odd and $u_2 = 7$, it follows that $4M^2 = u_n - 3 \equiv -10 \pmod{u_{2^s}}$ and, hence,

$$\left(\frac{-2}{u_{2^s}}\right)\left(\frac{5}{u_{2^s}}\right) = \left(\frac{-10}{u_{2^s}}\right) = \left(\frac{4M^2}{u_{2^s}}\right) \cancel{= 1} = \left(\frac{2M}{u_{2^s}}\right)^2 \geq 0$$

By Lemma 2.6 it follows that the first factor on the left is 1. By Lemma 2.5 it follows that the second factor on the left is $-1$. Since this is impossible, we may conclude that $n = 2$ and hence $u_n = 7$. □

Suppose now that $x$ is an odd positive integer and $x(x+1)(2x+1) = 6y^2$ for some integer $y$. Since $x+1$ is even, we have $x((x+1)/2)(2x+1) = 3y^2$. Since $x$, $(x+1)/2$ and $2x+1$ are relatively prime in pairs, by Lemma 1.6, we have $x \not\equiv 2 \pmod 3$ and $(x+1)/2 \not\equiv 2 \pmod 3$. ~~Since $x$, $x+1$ and $2x+1$ are relatively prime in pairs, it follows that $x$ is either a square or a triple of a square, and hence $x \neq 2 \pmod 3$. Moreover, $x+1$, being even, is either double a square or six times a square, and, hence, $x+1 \not\equiv 1 \pmod 3$.~~ Thus $x \equiv 1 \pmod 3$ and hence ~~$x+1 \equiv 2 \pmod 3$ and~~ $2x+1 \equiv 0 \pmod 3$. Thus for some nonnegative integers $u$, $v$ and $w$, we have $x = u^2$, $x+1 = 2v^2$ and $2x+1 = 3w^2$. From this we obtain $6w^2+1 = 4x+3 = 4u^2+3$. Also $(6w^2+1)^2 - 3(4vw)^2 = 12w^2(3w^2+1-4v^2)+1 = 12w^2(2x+1+1-2(x+1))+1 = 1$. Thus $u_n = 6w^2+1 = 4u^2+3$ for some $n$. Hence, by Lemma 2.7, $4u^2+3 = 7$ ~~$6w^2+1=7$~~. Thus $x = u^2 = 1$ ~~$w=1$ and $x=1$~~. This gives us the trivial 1 cannonball solution to Lucas's problem.

We may conclude that if a square number of cannonballs are stacked in a square pyramid then there are exactly 4900 of them.