O Problema da Pirâmide de Base Quadrada

Jaime E. A. Rodriguez [1], **Felipe D. C. Fidalgo** [2]
[1] Depto de Matemática, FEIS, UNESP, Ilha Solteira, SP, E-mail: jaime@mat.feis.unesp.br
[2] UFSC, Campus Blumenau, SC, E-mail: felipe.fidalgo@ufsc.br

Resumo: *A arte de resolver problemas envolvendo equações diofantinas é muito antiga e até hoje existem problemas sem solução, ou com soluções parciais e, em outros casos, com soluções diversas. Em* 1875, *Edouard Lucas apresentou o seguinte problema desafiador: "Considere uma coleção de balas de canhão empilhadas em forma de pirâmide de base quadrada com uma bala na camada superior, quatro balas na segunda camada, nove balas na terceira camada e assim por diante. Se o empilhamento colapsar, é possível reorganizar as balas em uma base quadrada?". Por longas décadas diversos matemáticos têm tentado fornecer uma solução completa (acessível) a esse problema. Em* 1985, *De Gang Ma, usando idéias de Kanagasabapathy e Ponnudurai, foi o primeiro a fornecer uma solução simples e completa do problema. Neste trabalho apresentamos uma outra solução do problema de Lucas, usando as idéias de De Gang Ma.*

Palavras-Chave: Equação Diofantina, Reciprocidade Quadrática, Congruência.

Abstract: *The art of solving problems involving Diophantine equations it is very old and even today there are unsolved problems or partial solutions and in other cases with different solutions. At* 1875, *Edouard Lucas presented the following challenging problem: "Consider a collection of cannonballs stacked shaped square pyramidal with a bullet in the upper layer, four balls in the second layer nine balls in the third layer and so on. If the stacking collapse is can rearrange the bullets in a square base?". For many long decades the mathematicians have tried to provide a complete solution (accessible) to this issue. At* 1985, *De Gang Ma, by using ideas of Kanagasabapathy and Ponnudurai, was the first to provide a simple and complete solution of the problem. We present another solution to the problem of Luke, using the ideas of De Gang Ma.*

Keywords: Diophantine equations, Quadratic Reciprocity, Congruence.

1 Introdução

Imaginemos uma coleção de balas de canhão empilhadas em forma de pirâmide de base quadrada com uma bala na camada superior, quatro balas na segunda camada, nove balas na terceira camada e assim por diante. Se o empilhamento colapsar, é possível reorganizar as balas em uma base quadrada?

Vamos analisar primeiro os casos mais simples. Se não existir nenhuma bala, se tem uma pirâmide de altura zero e um quadrado zero por zero. Se existir uma única bala, esta forma uma pirâmide de altura um e é um quadrado um por um. Além destes casos triviais, existirão outros? Se a pirâmide tiver três camadas, então o rearranjo não é possível já que existirão $1+4+9=14$ balas e 14 não é um número quadrado perfeito. Assim, o objetivo deste trabalho é apresentar uma solução geral accessível a este problema.

Em 1875, E. Lucas [7], desafiou aos leitores da revista Nouvelles Annales de Mathématique a resolver o seguinte problema:

"Uma pirâmide (de base) quadrada de balas de canhão contém um número quadrado perfeito de balas de canhão unicamente se tem 24 balas de canhão ao longo de cada fileira (camada) em sua base".

Em outras palavras, Lucas afirmou que a única solução (em números naturais) da equação

$$1^2 + 2^2 + 3^2 + \cdots + x^2 = y^2$$

é $x = 24$ e $y = 70$. Aqui x representa a número de balas de canhão na camada da base da pirámide e y o número total de balas.

Observe que a equação acima é equivalente à cúbica

$$x(x+1)(2x+1) = 2x^3 + 3x^2 + x = 6y^2,$$

a qual representa uma Curva Elíptica [11].

Para introduzir o problema e discutir sua solução, apresentamos a seguir uma breve história dessa equação Diofantina e na próxima seção apresentaremos a solução mencionada linhas acima.

Em 1876, M. Moret-Blanc [9], apresentou uma "prova" da afirmação de Lucas e, embora incompleta, forneceu uma certa base para resolvê-la. M. Moret-Blanc dividiu o problema em dois casos: x par e x ímpar (que é o que faremos neste trabalho). Em 1877, tendo observado que existia uma "lacuna" na prova de Moret-Blanc, Lucas [8], publicou uma outra prova, a qual tinha também outra "lacuna" pois ele conseguiu lidar com o caso x par mas não com o caso x ímpar. Em 1918, G. N. Watson [10], conseguiu prencher a lacuna de Lucas com cerca de 14 páginas de uma Teoria Estendida de Funções Elípticas Jacobianas. Esta foi a primeira prova completa da afirmação de Lucas, mas resultou sendo muito complicada e difícil de entender na época. Em 1952, W. Ljunggren [6], usou o Método de Skolem para fornecer uma simples solução aritmética para o problema da pirâmide de base quadrada. Em 1966 [2], Baker e Davenport, usando um teorema da Teoria dos Números, conseguiram resolver as diofantinas simultâneas $3x^2 - 2 = y^2$ e $8x - 7 = z^2$. Seu método, recentemente melhorado por M. Waldschmidt, pode ser adaptado para demonstrar a proposição de Lucas. Em 1975 [5], Kanagasabapathy e Ponnudurai forneceram um solução elementar para as equações diofantinas simultâneas $3x^2 - 2 = y^2$ e $8x - 7 = z^2$. Em 1985, De Gang Ma [4], obteve uma solução elementar do problema de Lucas, a primeira prova completa acessível a nível de graduação.

Neste trabalho usamos as idéias de Ma para fornecer uma outra prova da afirmação de Lucas. Na seção 2, dividida em duas partes, apresentamos a solução ao problema de Lucas.

2 O Problema: Teoria e Resultados

Nesta seção apresentamos uma outra solução do Problema da pirâmide de base Quadrada, dado pela equação

$$1^2 + 2^2 + 3^2 + \cdots + x^2 = y^2,$$

com $x, y \in \mathbb{N}$. Para tal efeito dividimos o problema em dois casos bem definidos.

2.1 Caso I: Quando x é par

A equação original

$$1^2 + 2^2 + 3^2 + \cdots + x^2 = y^2,$$

é equivalente a

$$x(x+1)(2x+1) = 6y^2.$$

Nesta subseção vamos considerar o caso x par. Analisaremos e resolveremos o problema com o auxílio dos seguintes lemas.

Lema 2.1 *A área de um triàngulo (retângulo) pitagórico nunca é um quadrado perfeito.*

Demonstração: Suponha, por absurdo, que existe um triângulo pitagórico cuja área é um quadrado perfeito. Seja w^2 a menor área para a qual tal triângulo existe. Sejam x e y os catetos do triângulo pitagórico com área w^2. Então $x^2+y^2=z^2$, para algum inteiro z e $\frac{xy}{2}=w^2$.

Considere a terna pitagórica (x,y,z). Como w é minimal, então x e y são primos relativos e, sem perda de generalidade, podemos assumir x ímpar e y par (e portanto, z ímpar). De fato, se ambos, x e y, fossem ímpares, então z seria par e, portanto,

$$z^2 \equiv 0(mod\ 4) \quad e \quad x^2 \equiv y^2 \equiv 1(mod\ 4)$$

o que contraria a igualdade $x^2+y^2=z^2$.

Agora afirmamos que existem inteiros primos relativos r e s, de paridade diferente, tais que

$$x = r^2 - s^2 \quad e \quad y = 2rs.$$

De fato, dado que temos um triângulo pitagórico primitivo (pois $mdc(x,y)=1$), então da igualdade $x^2+y^2=z^2$ obtemos $y^2=(z+x)(z-x)$, ou seja, $(\frac{y}{2})^2=(\frac{z+x}{2})(\frac{z-x}{2})$. Observe que $z+x$ e $z-x$ são números pares.

Vamos mostrar que $mdc(\frac{z+x}{2},\frac{z-x}{2})=1$. Seja $d=mdc(\frac{z+x}{2},\frac{z-x}{2})$. Então

$$\begin{cases} \text{d divide } \dfrac{z+x}{2} \\ \\ \text{d divide } \dfrac{z-x}{2}, \end{cases}$$

e portanto

$$\begin{cases} \text{d divide } \dfrac{z+x}{2}+\dfrac{z-x}{2}=z \\ \\ \text{d divide } \dfrac{z+x}{2}-\dfrac{z-x}{2}=x. \end{cases}$$

Assim, dado que $mdc(z,x)=1$, temos que $d=1$. Segue então que existem inteiros positivos r e s tais que $\frac{z+x}{2}=r^2$ e $\frac{z-x}{2}=s^2$, de onde obtemos que $y=2rs$ e $x=r^2-s^2$ (subtraindo as duas igualdades acima). Assim mostramos a afirmação mencionada linhas acima.

Segue desta afirmação que $(r^2-s^2)rs=w^2$ e que $s/4<s\leq w^2$. Já que $r,s,r-s$ e $r+s$ são primos relativos dois a dois e como $(r-s)(r+s)rs=w^2$, segue que existem inteiros positivos a,b,c,d tais que $r=a^2$, $s=b^2$, $a^2-b^2=r-s=c^2$ e $a^2+b^2=r+s=d^2$. Observar que $mdc(c,d)=1$, pois $mdc(r-s,r+s)=1$. Observe também que c e d são ímpares pois r e s tem paridade diferente.

Agora, consideremos $X=\frac{d+c}{2}$ e $Y=\frac{d-c}{2}$. Então X e Y são primos relativos e $X^2+Y^2=a^2$. Portanto ou X ou Y é par e $\frac{XY}{2}=\frac{d^2-c^2}{8}=\frac{b^2}{4}=\frac{s}{4}$ é um quadrado. Dado que o triângulo de lados X,Y e a é um triângulo pitagórico com área $s/4$, segue da minimalidade de w^2 que $w^2\leq s/4$, o qual é uma contradição. Assim fica demonstrado o lema.

Lema 2.2 *Não existe nenhum inteiro positivo x tal que $2x^4+1$ seja um quadrado.*

Demonstraçâo: Por absurdo, suponha que (x,y) seja a menor solução inteira da equação $2x^4+1=y^2$. Então para algum inteiro positivo s temos que $y=2s+1$, de onde obtemos que $x^4=2s(s+1)$. Se s for ímpar então $mdc(s,2(s+1))=1$ e assim, para alguns inteiros u e v temos que $s=u^4$ e $2(s+1)=v^4$. Segue então que $2(u^4+1)=v^4$, com u ímpar e v par. Portanto, temos $2(1+1)\equiv 0\ (mod\ 8)$, o que é impossível. Sendo assim s não pode ser ímpar. Logo s é par. Segue então que $mdc(2s,s+1)=1$ e portanto existem inteiros u e v, ambos maiores do que 1, tais que $2s \quad u^4$ e $s+1=v^4$

Seja w o inteiro positivo tal que $u = 2w$. Seja a o inteiro positivo tal que $v^2 = 2a+1$. Então $\frac{u^4}{2} + 1 = s + 1 = v^4$, de modo que $2w^4 = \frac{v^4-1}{4} = a(a+1)$. Como $v^2 = 2a+1$, segue que a é par. Agora, como $2w^4 = a(a+1)$, segue-se que existem inteiros positivos b e c tais que $a = 2b^4$ e $a+1 = c^4$. Porém isto implica que $2b^4 + 1 = (c^2)^2$ (ou seja, c^2 é uma solução da equação $2x^4 + 1 = y^2$) e portanto $y \leq c^2$, pela minimalidade de (x, y). Por outro lado temos que $c^2 \leq a + 1 < v^2 \leq s + 1 < y$, o que é uma contradição. Assim fica mostrado o lema.

Lema 2.3 *Existe exatamente um único inteiro positivo, $(x = 1)$, tal que $8x^4+1$ é um quadrado.*

Demonstração: Suponha que $8x^4 + 1 = (2s + 1)^2$, para algum s inteiro positivo. Então obtemos que $2x^4 = s(s + 1)$.

Se s for par então existem inteiros u e v tais que $s = 2u^4$ e $s + 1 = v^4$. Neste caso $2u^4 + 1 = v^4$ e pelo Lema 2.2, se tem $u = 0$ e portanto, $x = 0$.

Se s for ímpar então existem inteiros positivos u e v tais que $s = u^4$ e $s+1 = 2v^4$. Neste caso $u^4 + 1 = 2v^4$. Como u é ímpar, resulta v ímpar. Elevando ao quadrado ambos os lados da expressão $u^4 + 1 = 2v^4$ obtemos $4v^8 - 4u^4 = u^8 - 2u^4 + 1$ e portanto

$$(v^4 - u^2)(v^4 + u^2) = \left(\frac{u^4 - 1}{2}\right)^2,$$

que é um quadrado perfeito.

Como $mdc(u^2, v^4) = 1$, segue que $\frac{v^4 - u^2}{2}$ e $\frac{v^4 + u^2}{2}$ são quadrados perfeitos. Agora sejam

$$(v^2 - u)^2 + (v^2 + u)^2 = 4\frac{v^4 + u^2}{2} = A^2 \quad e \quad \frac{(v^2 - u)(v^2 + u)}{2} = \frac{v^4 - u^2}{2} = B^2.$$

Mas pelo lema 2.1 isto é impossível, a menos que $v^2 = u$. E como $u^4 + 1 = 2v^4$, obtemos $u^4 - 2u^2 + 1 = (u^2 - 1)^2 = 0$, de onde $u^2 = 1$. Daqui segue que $s = 1$ e assim $x = 1$. Desta forma fica demonstrado o lema.

Agora, com o auxílio dos três lemas acima, estamos em condições de resolver a equação

$$x(x + 1)(2x + 1) = 6y^2,$$

sob a hipótese de x ser par.

Se x é par então $x + 1$ é ímpar. Como x, $x + 1$ e $2x + 1$ são primos relativos dois a dois, segue que $x + 1$ e $2x + 1$ (sendo ambos ímpares) são ou quadrados perfeitos ou três vezes um quadrado perfeito. Assim

$$x + 1 \ncong 2(mod\ 3) \qquad e \qquad 2x + 1 \ncong 2(mod\ 3).$$

Portanto $x \equiv 0(mod\ 3)$, e existem inteiros não negativos $p, q\ e\ r$ tais que

$$x = 6q^2,\ x + 1 = p^2 \ \ e \ \ 2x + 1 = r^2.$$

Assim $6q^2 = (r-p)(r+p)$. Como p e r são ambos ímpares, então 4 é um fator de $(r-p)(r+p) = 6q^2$ e assim q é par. Seja q_0 um inteiro tal que $q = 2q_0$. Agora se tem

$$6q_0^2 = (\frac{r-p}{2})(\frac{r+p}{2}),$$

e como $mdc(\frac{r-p}{2}, \frac{r+p}{2}) = 1$ (pois $mdc(r^2, p^2) = 1$), obtemos um dos seguintes casos:

Caso 1: Das expressões $\frac{r-p}{2}$ e $\frac{r+p}{2}$, uma é da forma $6A^2$ e a outra da forma B^2, onde A e B são inteiros não negativos. Então $p = \pm(6A^2 - B^2)$ e $q = 2AB$. Como $6q^2 + 1 = x + 1 = p^2$,

temos $24A^2B^2 + 1 = (6A^2 - B^2)^2$ ou $(6A^2 - 3B^2)^2 - 8B^4 = 1$. Logo, pelo Lema 2.3, $B = 0$ ou $B = 1$ e, portanto, $x = 6q^2 = 0$ ou $x = 24$. Assim a única solução não trivial é $x = 24$.

Caso 2: Das expressões $\frac{r-p}{2}$ e $\frac{r+p}{2}$, uma é da forma $3A^2$ e a outra da forma $2B^2$, onde A e B são inteiros não negativos. Então $p = \pm(3A^2 - 2B^2)$ e $q = 2AB$. Isto dá $24A^2B^2 + 1 = (3A^2 - 2B^2)^2$ e, portanto, $(3A^2 - 6B^2)^2 - 2(2B)^4 = 1$. Logo, pelo Lema 2.2 se tem $B = 0$ e assim $x = 6q^2 = 0$.

Desta forma, quando x é par, a única solução do enigma de Lucas é $x = 24$ balas de canhão ao longo da base da pirâmide quadrada e, portanto, $y = 70$.

2.2 Caso II: Quando x é ímpar

Para resolver o problema nesta segunda parte, primeiro investigaremos as soluções da equação Diofantina $X^2 - 3Y^2 = 1$. Para isso sejam $a = 2 + \sqrt{3}$ e $b = 2 - \sqrt{3}$. Observar que $ab = 1$. Para qualquer n inteiro não-negativo, sejam

$$u_n = \frac{a^n + b^n}{2} \quad e \quad v_n = \frac{a^n - b^n}{2\sqrt{3}}.$$

Então u_n e v_n são inteiros e, quando $n \geq 1$, (u_n, v_n) é a n-ésima solução inteira da equação $X^2 - 3Y^2 = 1$. De fato, quando $n = 0$, temos a solução $X = 1$ e $Y = 0$.

Agora, a fim de mostrar que $x = 1$ é o único inteiro positivo ímpar tal que $x(x+1)(2x+1)$ é da forma $6y^2$, faremos uso dos seguintes resultados.

Lema 2.4 *Se m e n são inteiros não-negativos, então:*

(a) $u_{m+n} = u_m u_n + 3v_m v_n$ *e* $v_{m+n} = u_m v_n + u_n v_m$.

(b) Se $m - n \geq 0$, *então* $u_{m-n} = u_m u_n - 3v_m v_n$ *e* $v_{m-n} = -u_m v_n + u_n v_m$.

Demonstração: Ambas as partes seguem de cálculos diretos das definições de u_n e v_n (veja-se [4], [6]).

Usando o lema acima, não é difícil obter o seguinte resultado.

Lema 2.5 *Se m é um inteiro não-negativo, então* $u_{m+2} = 2u_1 u_{m+1} - u_m$ *e* $v_{m+2} = 2u_1 v_{m+1} - v_m$.

Demonstração: Veja-se [4], [6].

Agora, usando o fato de que (u_m, v_m) é a solução da equação $X^2 - 3Y^2 = 1$, temos também o seguinte resultado.

Lema 2.6 *Se m é um inteiro não-negativo, então* $u_{2m} = 2u_m^2 - 1 = 6v_m^2 + 1$ *e* $v_{2m} = 2u_m v_m$.

Demonstração: Veja-se [4], [6].

Lema 2.7 *Sejam m, n e r inteiros não-negativos tais que $2rm - n$ seja também inteiro não-negativo. Então* $u_{2rm \pm n} \equiv (-1)^r u_n \ (mod\ u_m)$.

Demonstração: Aplicando indução sobre r e o Lema 2.4, verifica-se que

$$u_{(2r+1)m} \equiv 0 \pmod{u_m} \quad e \quad v_{2rm} \equiv 0 \pmod{u_m}.$$

Ja que o lema 2.6 implica que $u_{2rm} = 2u_{rm}^2 - 1 = 6v_{rm}^2 + 1$, segue que $u_{2rm} \equiv (-1)^r \pmod{u_m}$. Desta forma, pelo Lema 2.4, obtemos

$$u_{2rm \pm n} = u_{2rm} u_n \pm 3v_{2rm} v_n \equiv (-1)^r \pmod{u_m}.$$

Observação 2.1 *Consideremos alguns dos primeiros valores de u_n. Começando por $n = 0$, temos 1, 2, 7, 26, 97, 362, $\cdots$ e assim por diante. Se consideramos estes valores, módulo 5, teremos $1, 2, 2, 1, 2, 2, \cdots$. Pelo Lema 2.5, esta é uma sequência periódica. Se consideramos os valores de u_n módulo 8, obtemos $1, 2, 7, 2, 1, 2, 7, 2, \cdots$, a qual é uma sequência puramente periódica de comprimento 4. Observe que quando n é par, u_n é ímpar.*

2.3 A Lei de Reciprocidade Quadrática

A Lei de Reciprocidade Quadrática é um teorema acerca da Aritmética Modular que fornece condições para a resolubilidade de equações quadráticas módulo números primos. Dado p primo, essa lei fornece uma bela descrição de quais números primos são quadrados módulo p. Casos especiais desta lei se devem a Fermat, Euler e Legendre, mas foi Gauss quem apresentou a primeira prova completa. Explicitamente, a Lei da Reciprocidade Quadrática estabelece que se p e q são primos (ímpares) distintos, sendo pelo menos um deles congruente a 1 módulo 4, então p é um quadrado módulo q se, e somente se, q é um quadrado módulo p. Para estabelecer tal lei usa-se o Símbolo de Legendre (veja-se [12], [13]).

Definição 2.1 *(Símbolo de Legendre) Seja p um número primo e a um número inteiro tal que $mdc(a, p) = 1$. Então o símbolo $\left(\frac{a}{p}\right)$ é definido por:*

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{se } a \text{ é um resíduo quadrático mod } p, \\ -1, & \text{se } a \text{ é um não-resíduo quadrático mod } p, \\ 0, & \text{se } p|a. \end{cases}$$

Proposição 2.1 *(Critério de Euler) Seja $p > 2$ primo e a inteiro qualquer. Então*

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \ (mod \ \ p).$$

O critério de Euler fornece uma maneira de identificar resíduos quadráticos. Mas o resultado a seguir é muito mais forte.

Teorema 2.1 *(Lei de Reciprocidade Quadrática)*

(1) Sejam p e q primos ímpares distintos. Então

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$$

(2) Seja p um primo ímpar. Então

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1, & \text{se } p \equiv \pm 1 \ mod \ 8 \\ -1, & \text{se } p \equiv \pm 3 \ mod \ 8. \end{cases}$$

Da Lei da Reciprocidade Quadrática e do comentário na observação 2.1 acima são obtidos os seguintes dois resultados.

Lema 2.8 *Se n é par, então:*

(a) *u_n é um ímpar não múltiplo de 5.*

(b) $\left(\frac{5}{u_n}\right) = 1$ *se, e somente se, n é um múltiplo de 3.*

Demonstração: (a) Ao supor que u_n é par e múltiplo de 5, obtemos um absurdo. A parte (b) segue da Lei da Reciprocidade Quadrática.

Lema 2.9 *Se n é par então u_n é ímpar e* $\left(\frac{-2}{u_n}\right) = 1$ *se, e somente se, n é um múltiplo de* 4.

A seguinte proposição é resultado principal deste trabalho. Aqui apresentamos uma simples demonstração, usando os resultados acima apresentados.

Proposição 2.2 *Se n é um inteiro não negativo então $u_n = 4\alpha^2 + 3$, para algum α, inteiro não-negativo, unicamente quando $u_n = 7$.*

Demonstração: Supondo $u_n = 4\alpha^2 + 3$, se tem que $u_n \equiv 3 \pmod 8$ ou $u_n \equiv 7 \pmod 8$. Da sequência de valores de u_n, módulo 8, segue que n é da forma $n = 8k \pm 2$. Agora suponha que $n \neq 2$ (e, portanto, $u_n \neq 7$). Então podemos escrever n na forma $2q2^s \pm 2$, onde q é ímpar e $s \geq 2$. Assim, pelo Lema 2.7, se tem $u_n = u_{2q2^s \pm 2} \equiv (-1)^q u_2 \ (\ u_{2^s})$ e portanto

$$\left(\frac{-2}{u_{2^s}}\right)\left(\frac{5}{u_{2^s}}\right) = \left(\frac{-10}{u_{2^s}}\right)\left(\frac{4\alpha^2}{u_{2^s}}\right) = 1.$$

Do Lema 2.9 segue que $\left(\frac{-2}{u_{2^s}}\right) = 1$ e do Lema 2.8 segue que $\left(\frac{5}{u_{2^s}}\right) = -1$. Como isto é impossível, concluímos que $n = 2$ e, portanto, $u_n = 7$.

Exemplo 2.1 *Determinar se -90 é resíduo quadrático módulo* 1019.

$$\left(\frac{-90}{1019}\right) = \left(\frac{-1}{1019}\right)\left(\frac{-2}{1019}\right)\left(\frac{3^2}{1019}\right)\left(\frac{5}{1019}\right) = (-1)(-1)\cdot 1 \cdot \left(\frac{1019}{5}\right) = \left(\frac{4}{5}\right) = \left(\frac{2^2}{5}\right) = 1.$$

Assim -90 é resíduo quadrático módulo 1019.

Agora, suponha que x é inteiro ímpar positivo e $x(x+1)(2x+1) = 6y^2$, para algum inteiro y. Dado que $x,\ x+1$ *e* $2x+1$ são primos relativos dois a dois, segue que x é um quadrado ou o triplo de um quadrado, e portanto, $x \ncong 2 \pmod 3$. Mais ainda, como $x+1$ é par, então é o dobro de um quadrado perfeito ou seis vezes um quadrado perfeito e, portanto, $x+1 \ncong 1 \pmod 3$. Sendo assim temos que $x \equiv 1 \pmod 3$ e, portanto, $x+1 \equiv 2 \pmod 3$ e $2x+1 \equiv 0 \pmod 3$. Assim, para alguns inteiros não negativos $u,\ v$ *e* w se tem que $x = u^2,\ x+1 = 2v^2$ e $2x+1 = 3w^2$. Segue que $6w^2 + 1 = 4x + 3 = 4u^2 + 3$. Também temos que

$$(6w^2+1)^2 - 3(4vw)^2 = 12w^2(3w^2 + 1 - 4v^2) + 1 = 12w^2(2x + 1 + 1 - 2(x+1)) + 1 = 1.$$

Logo, pela proposição 2.2, se tem que $6w^2 + 1 = 7$. Assim $w = 1$ e portanto $x = 1$. Isto fornece a solução trivial ($x = 1$) de balas de canhão para o problema de Lucas.

3 Conclusão

O problema colocado inicialmente foi de considerar uma coleção de balas de canhão empilhadas em forma de pirâmide de base quadrada com uma bala na camada superior, quatro balas na segunda camada, nove balas na terceira camada e assim por diante. Perguntava-se, caso o empilhamento colapsar, se era possível reorganizar as balas em uma base quadrada?. Observamos que se temos 4900 balas de canhão, podemos arranjar elas em uma pirámide em uma pirámide de altura 24 ou colocar elas em um quadrado 70×70.

Lembramos que o problema acima, se traduziu em determinar soluções naturais para a equação cúbica

$$1^2 + 2^2 + 3^2 + \cdots + x^2 = y^2 \quad \text{ou} \quad x(x+1)(2x+1) = 2x^3 + 3x^2 + x = 6y^2.$$

Tal como *E. Lucas* tinha afirmado, tem se mostrado que $(24, 70)$ é a única solução para a equação cúbica acima (ou seja, para o problema inicialmente colocado), além da solução trivial $(1, 1)$.

Embora o Método de Diofantus permita obter tal solução (veja-se [11]), o procedimento mostrado neste trabalho usa técnicas mais sofisticadas para determinar a solução ao problema, além de permitir ilustrar o uso de ferramentas da Teoría dos Números para resolver uma situação de natureza geométrica. Também observamos como que o problema estudado tem uma íntima relação com uma classe de certas curvas cúbicas (as curvas elípticas), as quais são úteis na Criptografia, entre outras aplicações (veja-se [11]).

Referências Bibliográficas

[**1**] W. S. Anglin, *The Square Pyramid Puzzle*, The American Mathematical Monthly, Vol. 97, No. 2, 1990, pp. 120-124.

[**2**] A. Baker and H. Davenport, *The equations* $3x^2 - 2 = y^2$ *and* $8x^2 - 7 = z^2$, Quaterly Journal of Mathematics, ser. 2, 20 (1969), 129-37.

[**3**] I, Cucurezeanu, *An Elementary Solution of Luca's Problem*, Journal of Number Theory, 44, 9-12 (1993).

[**4**] De Gang Ma, *An Elementary proof of the solution to the Diophantine Equation* $6y^2 = x(x+1)(2x+1)$, Sichuan Daxue Xuebao, 4 (1985), 107-16.

[**5**] P. kanagasabapathy and T. Ponnudurai, *The simultaneous Diophantine equations* $y^2 - 3x^2 = -2$ *and* $z^2 - 8x^2 = -7$, Quarterly Journal of Mathematics, ser. 2, 26 (1975), 275-78.

[**6**] W. Ljunggren, *New Solution of a Problem proposed by E. Lucas*, Norsk Mat. Tidsskrift, 34 (1952), 65-72.

[**7**] E. Lucas, *Question 1180*, Nouvelles Annales de Mathématiques, ser. 2, 14 (1875), 336.

[**8**] E. Lucas, *Question 1180*, Nouvelles Annales de Mathématiques, ser. 2, 16 (1877), 429-32.

[**9**] M. Moret-Blanc, *Question 1180*, Nouvelles Annales de Mathématiques, ser. 2, 15 (1876) 46-48.

[**10**] G. N. Watson, *The problem of the square pyramid*, Messenger of Mathematics, 48 (1918-19), 1-22.

[**11**] L. C. Washington, *Elliptic Curves, Number Theory and Cryptography*, CRC Press, Taylor and Francis Group, Second Edition, 2008.

[**12**] J. P. de O. Santos, *Introdução à Teoria dos Números*, Coleção Matemática Universitária IMPA 1998.

[**13**] F. B. Martinez, C. G. Moreira, N. Saldanha e E. Tengan, *Teoría dos Números, um passeio com os primos e outros números familiares pelo mundo inteiro*, Projeto Euclides, IMPA, 2010.