POTI
POLOS OLÍMPICOS DE TREINAMENTO INTENSIVO

Problemas Resolvidos

Nível 2

Equações diofantinas II

Material elaborado por Valentino Amadeus Sichinel

Problemas

Problema 1. Mostre que se a, b e x são inteiros positivos tais que $a \cdot b = x^2$ e $\text{mdc}(a, b) = 1$, então existem inteiros r e s tais que $a = r^2$ e $b = s^2$.

Problema 2. Prove que todas as soluções positivas da equação

$$\frac{1}{x^2} + \frac{1}{y^2} = \frac{1}{z^2}$$

com $\text{mdc}(x, y, z) = 1$ são ou da forma

$$(x, y, z) = \Big(r^4 - s^4,\ 2rs(r^2 + s^2),\ rs(r^2 - s^2)\Big),$$

ou da forma

$$(x, y, z) = \Big(2rs(r^2 + s^2),\ r^4 - s^4,\ rs(r^2 - s^2)\Big),$$

onde $r > s > 0$, $\text{mdc}(r, s) = 1$ e r e s têm paridades distintas.

Problema 3. Encontre todos os pares de racionais positivos (x, y) tais que $x^2 + y^2 = 1$.

Problema 4. Encontre todas as quádruplas (a, b, c, d) de inteiros positivos tais que

$$\begin{cases} a^2 + b^2 = c^2 \\ a^2 + c^2 = d^2 \end{cases}.$$

Problema 5 (Torneio das Cidades)**.** Prove que a equação

$$x^2 + y^2 - z^2 = 1997$$

tem infinitas soluções inteiras (x, y, z).

Problema 6. Encontre todas as soluções inteiras de

$$5m^2 + n^2 = 5^{2020}.$$

Problema 7. Encontre todas as triplas (a, b, c) de inteiros positivos tais que

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

Soluções

1. Sejam

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}, \qquad b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k} \qquad \text{e} \qquad x = p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_k^{\gamma_k}$$

as fatorações em primos de a, b e x, respectivamente.

Temos

$$x^2 = p_1^{2\gamma_1} p_2^{2\gamma_2} \cdots p_k^{2\gamma_k} \qquad \text{e} \qquad a \cdot b = p_1^{\alpha_1+\beta_1} p_2^{\alpha_2+\beta_2} \cdots p_k^{\alpha_k+\beta_k}.$$

Logo,

$$\alpha_i + \beta_i = 2\gamma_i \quad \forall\ i \in \{1, 2, \ldots, k\}. \tag{1}$$

Observe, no entanto, que se, para algum i, $\alpha_i > 0$ e $\beta_i > 0$, tanto a quanto b teriam p_i como fator primo. Daí, nesse caso, mdc(a, b) não seria igual a 1. Assim, para todo i, ou $\alpha_i = 0$, ou $\beta_i = 0$. Por (1), isso é o mesmo que

$$\alpha_i = 2\gamma_i \quad \text{ou} \quad \beta_i = 2\gamma_i \qquad \forall\ i \in \{1, 2, \ldots, k\}.$$

Podemos reescrever esse fenômeno da seguinte maneira: para todo i, se $p_i \mid a$, então $\alpha_i = 2\gamma_i$ e $p_i \nmid b$; por outro lado, se $p_i \mid b$, então $\beta_i = 2\gamma_i$ e $p_i \nmid a$. Dessa maneira, podemos reescrever as fatorações em primos de a e b da seguinte forma:

$$a = \prod_{i;\ p_i|a} p_i^{2\gamma_i} \qquad \text{e} \qquad b = \prod_{i;\ p_i|b} p_i^{2\gamma_i}.$$

Isso nos permite escrever

$$a = \Big(\prod_{i;\ p_i|a} p_i^{\gamma_i} \Big)^2 \qquad \text{e} \qquad b = \Big(\prod_{i;\ p_i|b} p_i^{\gamma_i} \Big)^2.$$

Portanto, $a = r^2$ e $b = s^2$, onde

$$r = \prod_{i;\ p_i|a} p_i^{\gamma_i} \qquad \text{e} \qquad s = \prod_{i;\ p_i|b} p_i^{\gamma_i}.$$

2. Sejam x, y e z inteiros positivos tais que mdc$(x, y, z) = 1$ e

$$\frac{1}{x^2} + \frac{1}{y^2} = \frac{1}{z^2}.$$

Temos

$$x^2 + y^2 = \Big(\frac{xy}{z}\Big)^2.$$

Sendo um racional cujo quadrado é inteiro, $\frac{xy}{z}$ deve ser inteiro[1]. Logo, x, y e $\frac{xy}{z}$ formam uma terna pitagórica. Daí, existem $r > s > 0$ inteiros positivos primos entre si e de paridades distintas e $d > 0$ um inteiro positivo tais que

$$(x,\ y,\ \frac{xy}{z}) = \Big(d(r^2 - s^2),\ \ d \cdot 2rs,\ \ d(r^2 + s^2)\Big) \tag{1}$$

[1]Prove isto: que, se $q \in \mathbb{Q}$ e $q^2 \in \mathbb{Z}$, então $q \in \mathbb{Z}$.

ou

$$(x,\, y,\, \frac{xy}{z}) = \Big(d \cdot 2rs,\ \ d(r^2 - s^2),\ \ d(r^2 + s^2)\Big). \tag{2}$$

Consideremos o caso (1). Temos, nesse cenário,

$$\begin{aligned}\frac{xy}{z} = d(r^2 + s^2) &\iff xy = d(r^2 + s^2)z \\ &\iff d(r^2 - s^2) \cdot d2rs = d(r^2 + s^2)z \\ &\iff d \cdot 2rs(r^2 - s^2) = (r^2 + s^2)z.\end{aligned}$$

Afirmo que $\text{mdc}(2rs(r^2 - s^2),\, r^2 + s^2) = 1$. De fato,

• $\text{mdc}(2,\, r^2 + s^2) = 1$, pois r e s têm paridades distintas;

• $\text{mdc}(r,\, r^2 + s^2) = 1$, pois se p é primo, $p \mid r$ e $p \mid (r^2 + s^2)$, então $p \mid r^2$ e $p \mid (r^2 + s^2)$, donde $p \mid s^2$ e, daí, $p \mid s$. Assim, $p \mid r$ e $p \mid s$, o que é um absurdo, pois $\text{mdc}(r,\, s) = 1$;

• $\text{mdc}(s,\, r^2 + s^2) = 1$, pois se p é primo, $p \mid s$ e $p \mid (r^2 + s^2)$, então $p \mid s^2$ e $p \mid (r^2 + s^2)$, donde $p \mid r^2$ e, daí, $p \mid r$. Assim, $p \mid s$ e $p \mid r$, o que é um absurdo, pois $\text{mdc}(r,\, s) = 1$;

• $\text{mdc}(r^2 - s^2,\, r^2 + s^2) = 1$, já que, se $p \mid (r^2 - s^2)$ e $p \mid (r^2 + s^2)$, então $p \mid (r^2 - s^2) + (r^2 + s^2) = 2r^2$ e $p \mid (r^2 + s^2)$, o que é um absurdo pois, como vimos, $\text{mdc}(2,\, r^2 + s^2) = \text{mdc}(r,\, r^2 + s^2) = 1$, o que implica $\text{mdc}(2r^2,\, r^2 + s^2) = 1$.

Dessa forma, como $d \cdot 2rs(r^2 - s^2) = (r^2 + s^2)z$, todos os fatores primos de $(r^2 + s^2)$ devem pertencer a d. Por outro lado, se d tivesse algum dos fatores primos de z, esse fator primo seria comum a x, y e z, já que tanto x quanto y são divisíveis por d. Mas isso é absurdo, pois $\text{mdc}(x,\, y,\, z) = 1$. Logo, d contém todos os fatores primos de $(r^2 + s^2)$, e nada além deles. Em outras palavras, $d = r^2 + s^2$. Daí,

$$d \cdot 2rs(r^2 - s^2) = (r^2 + s^2)z \quad \Rightarrow \quad (r^2 + s^2) \cdot 2rs(r^2 - s^2) = (r^2 + s^2)z \quad \Rightarrow \quad 2rs(r^2 - s^2) = z.$$

Assim, temos

$$\begin{aligned}x &= d(r^2 - s^2) = (r^2 + s^2)(r^2 - s^2) = r^4 - s^4, \\ y &= d \cdot 2rs = 2rs(r^2 + s^2), \\ z &= 2rs(r^2 - s^2),\end{aligned}$$

onde r e s são inteiros positivos primos entre si e de paridades distintas, tais que $r > s > 0$.

O caso (2) é totalmente análogo; mudando apenas os papeis de x e de y. Portanto, temos ou

$$(x,\, y,\, z) = \Big(r^4 - s^4,\ \ 2rs(r^2 + s^2),\ \ rs(r^2 - s^2)\Big),$$

ou

$$(x,\, y,\, z) = \Big(2rs(r^2 + s^2),\ \ r^4 - s^4,\ \ rs(r^2 - s^2)\Big),$$

onde $r > s > 0$, $\text{mdc}(r,\, s) = 1$ e r e s têm paridades distintas.

3. Sejam x e y racionais positivos tais que

$$x^2 + y^2 = 1.$$

Escrevamos

$$x = \frac{a}{b} \qquad \text{e} \qquad y = \frac{p}{q},$$

com

$$\text{mdc}(a,\, b) = \text{mdc}(p,\, q) = 1.$$

Observe que

$$\left(\frac{a}{b}\right)^2 + \left(\frac{p}{q}\right)^2 = 1 \quad \Rightarrow \quad a^2 + \left(\frac{bp}{q}\right)^2 = b^2.$$

Daí, $\left(\frac{bp}{q}\right)^2$ é inteiro. Sendo racional cujo quadrado é inteiro, $\frac{bp}{q}$ é inteiro[1]. Logo, $q \mid bp$. Como $\text{mdc}(p,\, q) = 1$, segue que $q \mid b$.

Por outro lado,

$$\left(\frac{a}{b}\right)^2 + \left(\frac{p}{q}\right)^2 = 1 \quad \Rightarrow \quad \left(\frac{aq}{b}\right)^2 + p^2 = q^2$$

e, por um raciocínio totalmente análogo, concluímos que $b \mid q$.

Como b e q são inteiros positivos tais que $q \mid b$ e $b \mid q$, $b = q$. Para não haver confusão, denotaremos, daqui para frente, b e q por m.

O que queremos, então, é encontrar inteiros positivos a, p e m tais que $\text{mdc}(a,\, m) = 1$, $\text{mdc}(p,\, m) = 1$ e

$$\left(\frac{a}{m}\right)^2 + \left(\frac{q}{m}\right)^2 = 1, \qquad \text{isto é,} \qquad a^2 + q^2 = m^2.$$

Em outras palavras, queremos que $(a,\, q,\, m)$ seja uma terna pitagórica primitiva. Sabemos que isso acontece se, e somente se, existem inteiros positivos $r > s > 0$, primos entre si e de paridades distintas, tais que ou

$$(a,\, q,\, m) = (r^2 - s^2,\ 2rs,\ r^2 + s^2),$$

ou

$$(a,\, q,\, m) = (2rs,\ r^2 - s^2,\ r^2 + s^2).$$

Portanto, os racionais positivos x e y são tais que $x^2 + y^2 = 1$ se, e somente se,

$$(x,\, y) = \left(\frac{r^2 - s^2}{r^2 + s^2},\ \frac{2rs}{r^2 + s^2}\right)$$

ou

$$(x,\, y) = \left(\frac{2rs}{r^2 + s^2},\ \frac{r^2 - s^2}{r^2 + s^2}\right),$$

onde r e s são inteiros positivos de paridades distintas tais que $r > s > 0$ e $\text{mdc}(r,\, s) = 1$.

4. Dentre todas as quádruplas que satisfazem as equações do enunciado, consideremos uma cujo valor de d é o menor possível. Afirmamos que tanto $(a,\, b,\, c)$ quanto $(a,\, c,\, d)$ são ternas pitagóricas primitivas. Para ver isso, como a e c são elementos de ambas as ternas, é suficiente que mostremos que $\text{mdc}(a,\, c) = 1$. E isto, de fato, ocorre: se p é um primo tal que $p \mid a$ e $p \mid c$, vem da primeira equação do enunciado que $p \mid b$ e, da segunda, que $p \mid d$. Assim, $\left(\frac{a}{p}\right)$, $\left(\frac{b}{p}\right)$, $\left(\frac{c}{p}\right)$, e $\left(\frac{d}{p}\right)$ são todos inteiros. Dividindo cada uma das equações por p^2, ficamos com

$$\begin{cases} \left(\frac{a}{p}\right)^2 + \left(\frac{b}{p}\right)^2 = \left(\frac{c}{p}\right)^2 \\ \left(\frac{a}{p}\right)^2 + \left(\frac{c}{p}\right)^2 = \left(\frac{d}{p}\right)^2 \end{cases},$$

o que é um absurdo, pois o último elemento da quádrupla $\left(\left(\frac{a}{p}\right),\, \left(\frac{b}{p}\right),\, \left(\frac{c}{p}\right),\, \left(\frac{d}{p}\right)\right)$ é menor que d, que supomos ser mínimo. Dessa forma, $(a,\, b,\, c,\, d)$, que é uma quádrupla que estamos supondo satisfazer

[1]Prove isto: que, se um número racional é tal que seu quadrado é inteiro, então o número é inteiro.

as condições do enunciado e ter o valor de d mínimo, é tal que o mdc entre quaisquer dois de seus elementos é igual a 1.

Isolando c^2 nas duas equações do enunciado e somando, ficamos com

$$2c^2 = d^2 + b^2 = \frac{(d+b)^2}{2} + \frac{(d-b)^2}{2}. \tag{1}$$

Veja que, como as ternas são primitivas, c e d são ímpares. Como c é ímpar, vem da segunda equação que a é par. Daí, pela primeira equação, b também é ímpar. Usaremos mais tarde que a é par. Por hora, precisamos somente do fato de que b e d têm a mesma paridade. Isso implica que $\frac{b+d}{2}$ e $\frac{b-d}{2}$ são ambos inteiros. (1) pode ser reescrita como

$$c^2 = \left(\frac{d+b}{2}\right)^2 + \left(\frac{d-b}{2}\right)^2.$$

A terna pitagórica $\left(\left(\frac{d+b}{2}\right), \left(\frac{d-b}{2}\right), c\right)$ é primitiva. De fato, se p divide tanto $\left(\frac{d+b}{2}\right)$ quanto $\left(\frac{d-b}{2}\right)$, p divide

$$\left(\frac{d+b}{2}\right) + \left(\frac{d-b}{2}\right) = d$$

e

$$\left(\frac{d+b}{2}\right) - \left(\frac{d-b}{2}\right) = b,$$

e $\text{mdc}(b, d) = 1$. Assim, existem r e s inteiros positivos primos entre si e de paridades distintas tais que

$$\left(\left(\frac{d+b}{2}\right), \left(\frac{d-b}{2}\right), c\right) = (r^2 - s^2, 2rs, r^2 + s^2) \tag{2}$$

ou

$$\left(\left(\frac{d+b}{2}\right), \left(\frac{d-b}{2}\right), c\right) = (2rs, r^2 - s^2, r^2 + s^2). \tag{3}$$

Voltemos às equações do enunciado. Isolando a^2 nas duas e somando, encontramos

$$2a^2 = d^2 - b^2 = (d+b)(d-b).$$

Independentemente de estarmos em (2) ou em (3), isso é o mesmo que

$$2a^2 = 8rs(r^2 - s^2).$$

Como a é par, $\frac{a}{2}$ é inteiro. Podemos reescrever a última equação como

$$\left(\frac{a}{2}\right)^2 = rs(r^2 - s^2) = rs(r-s)(r+s).$$

Observe agora que, como $\text{mdc}(r, s) = 1$ e r e s têm paridades distintas, r, s, $(r-s)$ e $(r+s)$ são dois a dois primos entre si. De fato:

- se $p \mid r$ e $p \mid s$, $p = 1$, pois $\text{mdc}(r, s) = 1$;
- se $p \mid r$ e $p \mid (r-s)$, então $p \mid r - (r-s) = s$; daí, $p = 1$, já que $\text{mdc}(r, s) = 1$;
- se $p \mid r$ e $p \mid (r+s)$, então $p \mid (r+s) - r = s$; daí, $p = 1$, já que $\text{mdc}(r, s) = 1$;
- se $p \mid s$ e $p \mid (r-s)$, então $p \mid (r-s) + s = r$; daí, $p = 1$, já que $\text{mdc}(r, s) = 1$;
- se $p \mid s$ e $p \mid (r+s)$, então $p \mid (r+s) - s = r$; daí, $p = 1$, já que $\text{mdc}(r, s) = 1$;

• se $p \mid (r-s)$ e $p \mid (r+s)$, então $p \mid (r-s)+(r+s) = 2r$ e $p \mid (r+s)-(r-s) = 2s$; daí, $p \mid 2$, já que $\text{mdc}(r,\, s) = 1$; como r e s têm paridades distintas, no entanto, $(r-s)$ é ímpar; logo, $p \mid 2$ e p divide um número ímpar, donde $p = 1$.

Dessa forma, segue do problema 1[1] que r, s, $(r-s)$ e $(r+s)$ são quadrados perfeitos. Escrevendo $r = x^2$, $s = y^2$, $r - s = z^2$ e $r + s = w^2$, encontramos as igualdades

$$\begin{cases} y^2 + z^2 = x^2 \\ y^2 + x^2 = w^2 \end{cases}.$$

Voilà: $(y,\, z,\, x,\, w)$ é uma das quádruplas que satisfazem as condições do enunciado. Mas

$$w^2 = r + s < 2r \leq 2rs \leq \frac{d+b}{2} < d \leq d^2,$$

ou seja, $w < d$. Absurdo, pois supomos que d era mínimo!

Dessa maneira, concluímos que não há quádrupla $(a,\, b,\, c,\, d)$ de inteiros positivos que satisfaz

$$\begin{cases} a^2 + b^2 = c^2 \\ a^2 + c^2 = d^2 \end{cases}.$$

5. Queremos encontrar triplas $(x,\, y,\, z)$ tais que

$$y^2 - z^2 = 1997 - x^2 \iff (y-z)(y+z) = 1997 - x^2.$$

É suficiente que encontremos triplas tais que

$$y - z = 1 \qquad \text{e} \qquad y + z = 1997 - x^2.$$

Estas duas igualdades se verificam se, e somente se,

$$y = \frac{1998 - x^2}{2} \qquad \text{e} \qquad z = \frac{1996 - x^2}{2}.$$

Precisamos que x seja par. Por outro lado, se x for par, digamos, igual a $2t$, podemos definir

$$y = \frac{1998 - 4t^2}{2} = 999 - 2t^2 \qquad \text{e} \qquad z = \frac{1996 - 4t^2}{2} = 998 - 2t^2,$$

e a equação será satisfeita.

Dessa forma, as soluções inteiras de

$$x^2 + y^2 - z^2 = 1997$$

são as triplas da forma

$$(2t,\ 999 - 2t^2,\ 998 - 2t^2),$$

onde t é inteiro. Como cada valor de t gera uma tripla distinta, concluímos que existem infinitas triplas que satisfazem a equação do enunciado.

[1] Na verdade, não tão diretamente. Mas, dado o resultado do problema 1, é fácil de provar por indução que, se os inteiros positivos a_1, a_2, ..., a_n são dois a dois primos entre si e tais que $\prod_{i=1}^{n} a_i$ é um quadrado perfeito, então cada um dos a_i é um quadrado perfeito - fica o exercício!

6. Suponhamos, por um instante, que $m, n \neq 0$.

Seja α o maior inteiro tal que $5^\alpha \mid n$ e β o maior inteiro tal que $5^\beta \mid m$. A maior potência de 5 que divide $5m^2$ é $5^{2\beta+1}$, enquanto que a maior potência de 5 que divide n^2 é $5^{2\alpha}$. Dessa forma, o expoente da maior potência de 5 que divide $5m^2+n^2$ é $\min(2\beta+1,\, 2\alpha)$. Como, por hipótese, $5m^2+n^2 = 5^{2020}$, esse expoente deve ser igual a 2020. Como $2\beta+1$ é ímpar, só podemos ter, então, $2\alpha = 2020$ e $2\beta+1 > 2\alpha$, isto é, $\beta \geq \alpha = 1010$.

Escrevendo

$$n = 5^\alpha \cdot a \qquad \text{e} \qquad m = 5^\beta \cdot b,$$

encontramos de

$$5m^2 + n^2 = 5^{2020}$$

que

$$5^{2\beta+1}a^2 + 5^{2\alpha}b^2 = 5^{2020} \quad \Rightarrow \quad 5^{(2\beta+1)-2\alpha}a^2 + b^2 = 1.$$

Absurdo, pois

$$5^{(2\beta+1)-2\alpha}a^2 + b^2 \;\; \geq \;\; 5a^2 + b^2 \;\; \geq \;\; 5 + 1 \;\; = \;\; 6.$$

Dessa forma, a hipótese que fizemos não se verifica, isto é, não é verdade que $m, n \neq 0$.

Se $n = 0$, devemos ter $5m^2 = 5^{2020} \iff m^2 = 5^{2019}$, o que não pode acontecer, pois 5^{2019} não é quadrado perfeito.

Se $m = 0$, devemos ter $n^2 = 5^{2020} \iff n = 5^{1010}$.

Portanto, o único par de inteiros $(m,\, n)$ para o qual $5m^2 + n^2 = 5^{2020}$ é $(m,\, n) = (0,\, 5^{1010})$.

7. Assim como quando lidamos com terna pitagóricas, é suficiente olharmos para as triplas primitivas, isto é, tais que $\text{mdc}(a,\, b,\, c) = 1$. Seja, então, $(a,\, b,\, c)$ uma tripla de inteiros positivos primos entre si tais que

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

Podemos reescrever a equação acima como

$$\frac{(a+b)^2}{2} + \frac{(a-b)^2}{2} = 2c^2,$$

ou

$$\Big(\frac{a+b}{2}\Big)^2 + \Big(\frac{a-b}{2}\Big)^2 = c^2.$$

Como $a^2 + b^2 = 2c^2$, a e b têm a mesma paridade, donde $\frac{a+b}{2}$ e $\frac{a-b}{2}$ são ambos inteiros. Assim, $\Big(\big(\frac{a+b}{2}\big),\, \big(\frac{a-b}{2}\big),\, c\Big)$ é uma terna pitagórica. Além disso, a terna é primitiva: se

$$p \mid \big(\frac{a+b}{2}\big) \qquad \text{e} \qquad p \mid \big(\frac{a-b}{2}\big),$$

então

$$p \mid \big(\frac{a+b}{2}\big) + \big(\frac{a-b}{2}\big) = a \qquad \text{e} \qquad p \mid \big(\frac{a+b}{2}\big) - \big(\frac{a-b}{2}\big) = b.$$

Daí, se p também divide c, p divide a, b e c e, portanto, $p = 1$ (pois $\text{mdc}(a,\, b,\, c) = 1$).

Dessa forma, existem $r > s > 0$ inteiros primos entre si e de paridades distintas tais que

$$\Big(\Big(\frac{a+b}{2}\Big),\, \Big(\frac{a-b}{2}\Big),\, c\Big) = (r^2 - s^2,\; 2rs,\; r^2 + s^2)$$

ou

$$\Big(\Big(\frac{a+b}{2}\Big),\, \Big(\frac{a-b}{2}\Big),\, c\Big) = (2rs,\; r^2 - s^2,\; r^2 + s^2).$$

O primeiro caso nos dá

$$(a,\, b,\, c) = (r^2 + 2rs - s^2,\ r^2 - 2rs - s^2,\ r^2 + s^2),$$

e o segundo,

$$(a,\, b,\, c) = (r^2 - 2rs - s^2,\ r^2 + 2rs - s^2,\ r^2 + s^2).$$

É fácil verificar que em ambas as situações temos, de fato, uma solução à equação do problema.

Portanto, as triplas $(a,\, b,\, c)$ de inteiros positivos tais que $a^2 + b^2 = 2c^2$ são exatamente as triplas que são ou da forma

$$\big(d(r^2 - 2rs - s^2),\ d(r^2 + 2rs - s^2),\ d(r^2 + s^2)\big),$$

ou da forma

$$\big(d(r^2 + 2rs - s^2),\ d(r^2 - 2rs - s^2),\ d(r^2 + s^2)\big),$$

sendo, em ambos os casos, d um inteiro positivo, e r e s inteiros positivos primos entre si, de paridades distintas e tais que $r^2 - 2rs - s^2 > 0$.