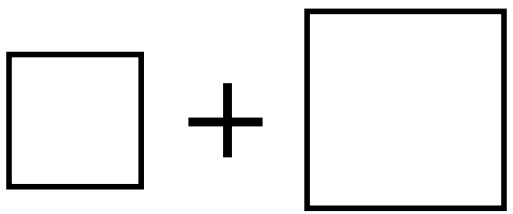
Geometria e Teoria dos Números: somas de quadrados

Tiago J. Fonseca

ICMC - USP

Seminário de Coisas Legais - Outubro 2011



Teorema (Soma de dois quadrados)

Todo primo da forma $p = 4k + 1$ *pode ser escrito como a soma de dois quadrados:* $p = a^2 + b^2$, $a, b \in \mathbb{N}$.

Teorema (Soma de dois quadrados)

Todo primo da forma $p = 4k + 1$ *pode ser escrito como a soma de dois quadrados:* $p = a^2 + b^2$, $a, b \in \mathbb{N}$.

Teorema (Soma de quatro quadrados)

Todo *número natural n pode ser escrito como a soma de quatro quadrados:* $n = a^2 + b^2 + c^2 + d^2$, $a, b, c, d \in \mathbb{N}$.

- (Divisão euclidiana) Dados dois inteiros a e $b \neq 0$, existe um único $r \geq 0$, com $r < |b|$ tal que $a = qb + r$, para algum $q \in \mathbb{Z}$. O inteiro r é o **resto** da divisão de a por b. Dizemos que b **divide** a (ou a é divisível por b) se $r = 0$. Neste caso, denotamos $b \mid a$.

- (Divisão euclidiana) Dados dois inteiros a e $b \neq 0$, existe um único $r \geq 0$, com $r < |b|$ tal que $a = qb + r$, para algum $q \in \mathbb{Z}$. O inteiro r é o **resto** da divisão de a por b. Dizemos que b **divide** a (ou a é divisível por b) se $r = 0$. Neste caso, denotamos $b \mid a$.
- (Congruência módulo n) Dizemos que a é **congruente** b módulo n se $n \mid a - b$. Denotamos $a \equiv b \pmod{n}$. Pode-se mostrar que congruência é uma "relação de equivalência".

- (Divisão euclidiana) Dados dois inteiros a e $b \neq 0$, existe um único $r \geq 0$, com $r < |b|$ tal que $a = qb + r$, para algum $q \in \mathbb{Z}$. O inteiro r é o **resto** da divisão de a por b. Dizemos que b **divide** a (ou a é divisível por b) se $r = 0$. Neste caso, denotamos $b \mid a$.
- (Congruência módulo n) Dizemos que a é **congruente** b módulo n se $n \mid a - b$. Denotamos $a \equiv b \pmod{n}$. Pode-se mostrar que congruência é uma "relação de equivalência".
- Um número inteiro a sempre é congruente a algum número em $\{0, 1, 2, \ldots, n-1\}$ módulo n.

As congruências podem (devem!) ser pensadas como se fossem igualdades. Pode-se mostrar que:

1. $a \equiv b \pmod{n} \Longrightarrow a + c \equiv b + c \pmod{n}$;
2. $a \equiv b \pmod{n} \Longrightarrow ac \equiv bc \pmod{n}$;
3. $a \equiv b \pmod{n} \Longrightarrow a^m \equiv b^m \pmod{n}$, $m \geq 0$.

As congruências podem (devem!) ser pensadas como se fossem igualdades. Pode-se mostrar que:

1. $a \equiv b \pmod{n} \Longrightarrow a + c \equiv b + c \pmod{n}$;
2. $a \equiv b \pmod{n} \Longrightarrow ac \equiv bc \pmod{n}$;
3. $a \equiv b \pmod{n} \Longrightarrow a^m \equiv b^m \pmod{n}$, $m \geq 0$.

Um problema simples e legal: Qual é a menor quantidade dentre os números abaixo que somam 50?

$$4,\ 6,\ 9,\ 12,\ 15,\ 19,\ 27,\ 30,\ 39,\ 42$$

As congruências podem (devem!) ser pensadas como se fossem igualdades. Pode-se mostrar que:

1. $a \equiv b \pmod{n} \Longrightarrow a + c \equiv b + c \pmod{n}$;
2. $a \equiv b \pmod{n} \Longrightarrow ac \equiv bc \pmod{n}$;
3. $a \equiv b \pmod{n} \Longrightarrow a^m \equiv b^m \pmod{n}$, $m \geq 0$.

Um problema simples e legal: Qual é a menor quantidade dentre os números abaixo que somam 50?

$$4,\ 6,\ 9,\ 12,\ 15,\ 19,\ 27,\ 30,\ 39,\ 42$$

Outro: nenhum primo da forma $4k + 3$ é soma de dois quadrados.

Quem foi Minkowski?

Quem foi Minkowski? 1864 - 1909

- Inicialmente, estudou formas quadráticas;

Quem foi Minkowski? 1864 - 1909

- Inicialmente, estudou formas quadráticas;
- Colega de graduação de David Hilbert;

Quem foi Minkowski? 1864 - 1909

- Inicialmente, estudou formas quadráticas;
- Colega de graduação de David Hilbert;
- Professor bastante influente de Einstein;

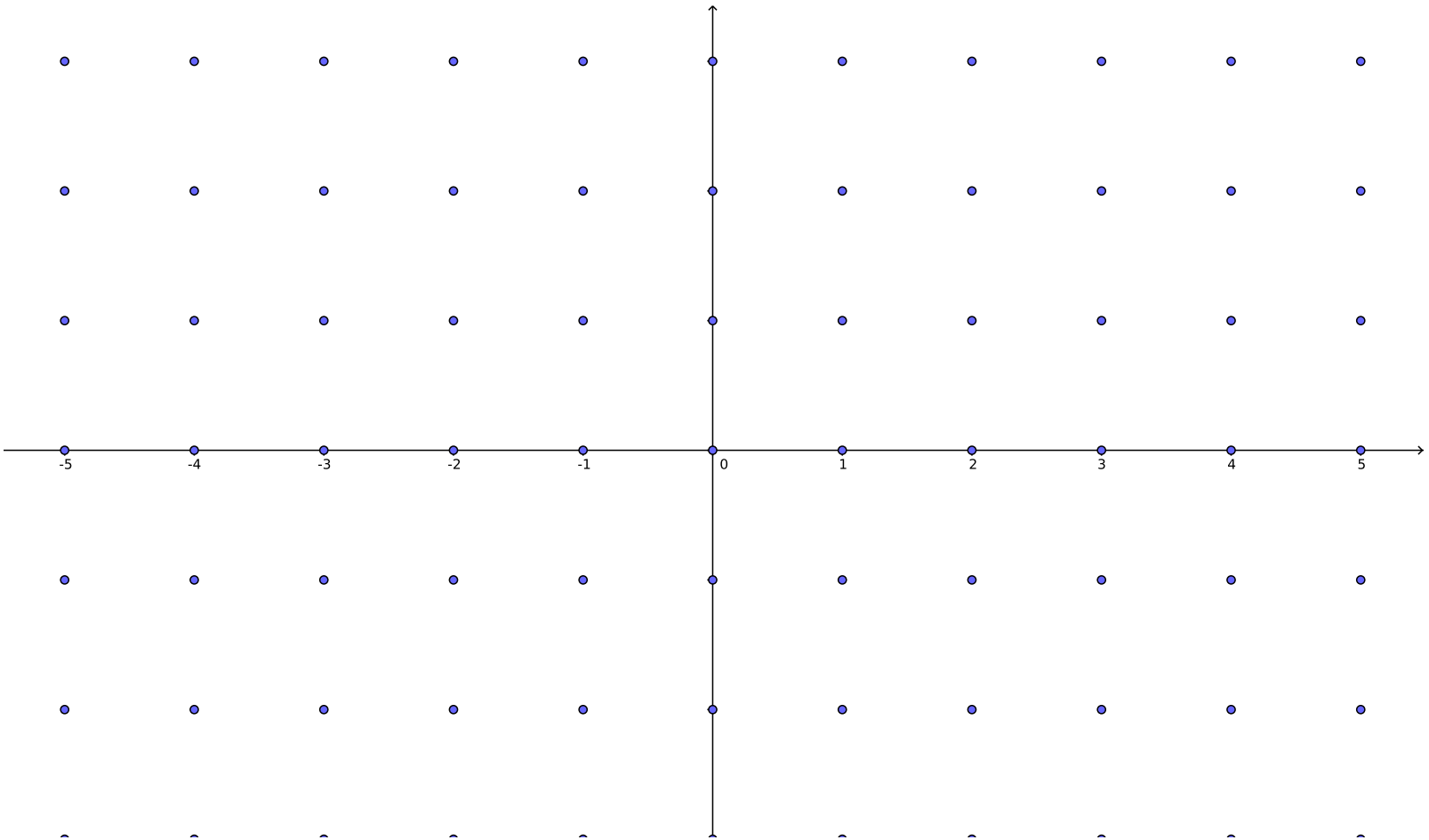
Quem foi Minkowski? 1864 - 1909

- Inicialmente, estudou formas quadráticas;
- Colega de graduação de David Hilbert;
- Professor bastante influente de Einstein;
- Minkowski também se interessou pela teoria da relatividade e formulou o Espaço de Minkowski.

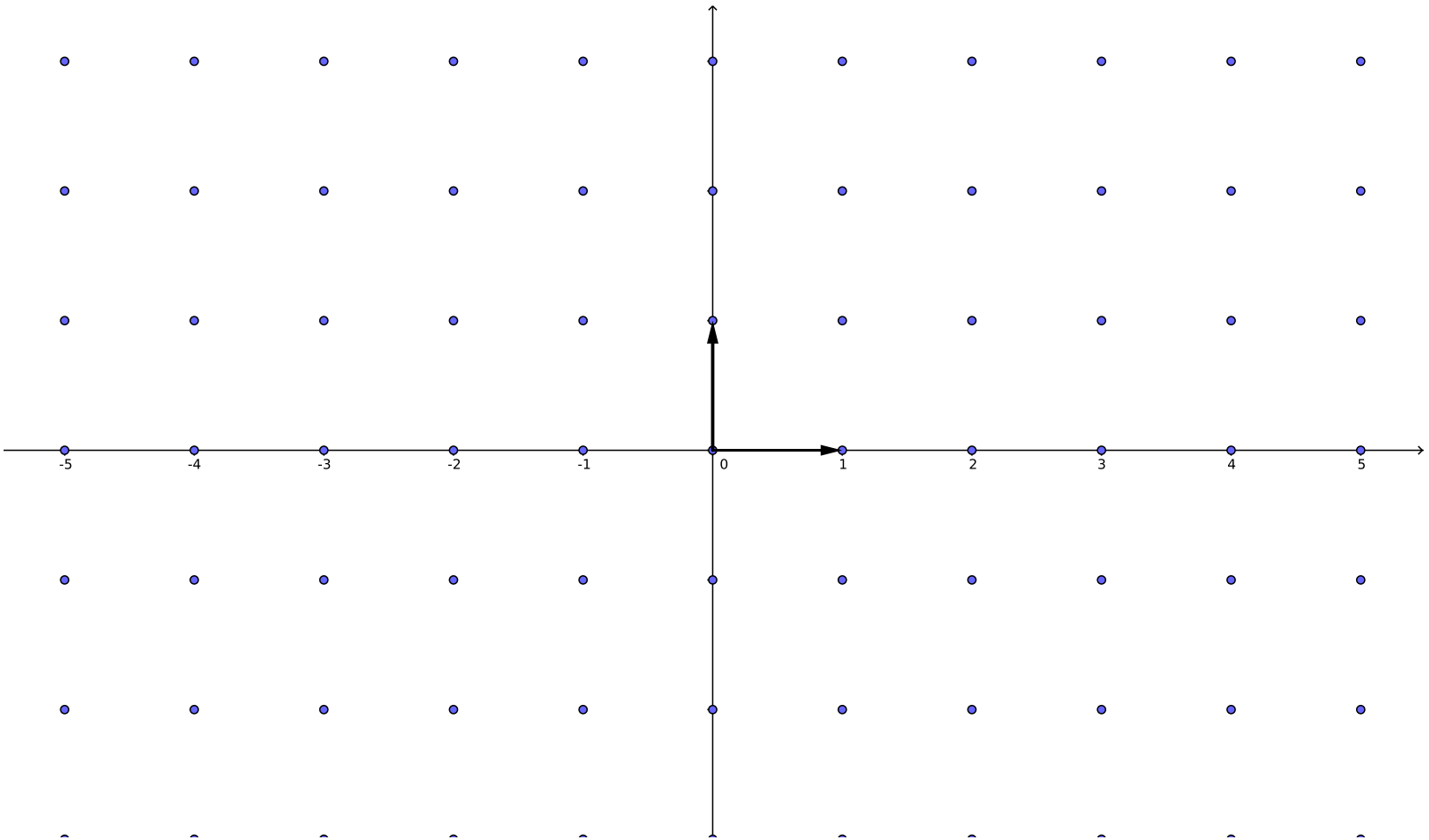
Quem foi Minkowski? 1864 - 1909

- Inicialmente, estudou formas quadráticas;
- Colega de graduação de David Hilbert;
- Professor bastante influente de Einstein;
- Minkowski também se interessou pela teoria da relatividade e formulou o Espaço de Minkowski.
- Inventou a **Geometria dos Números**.

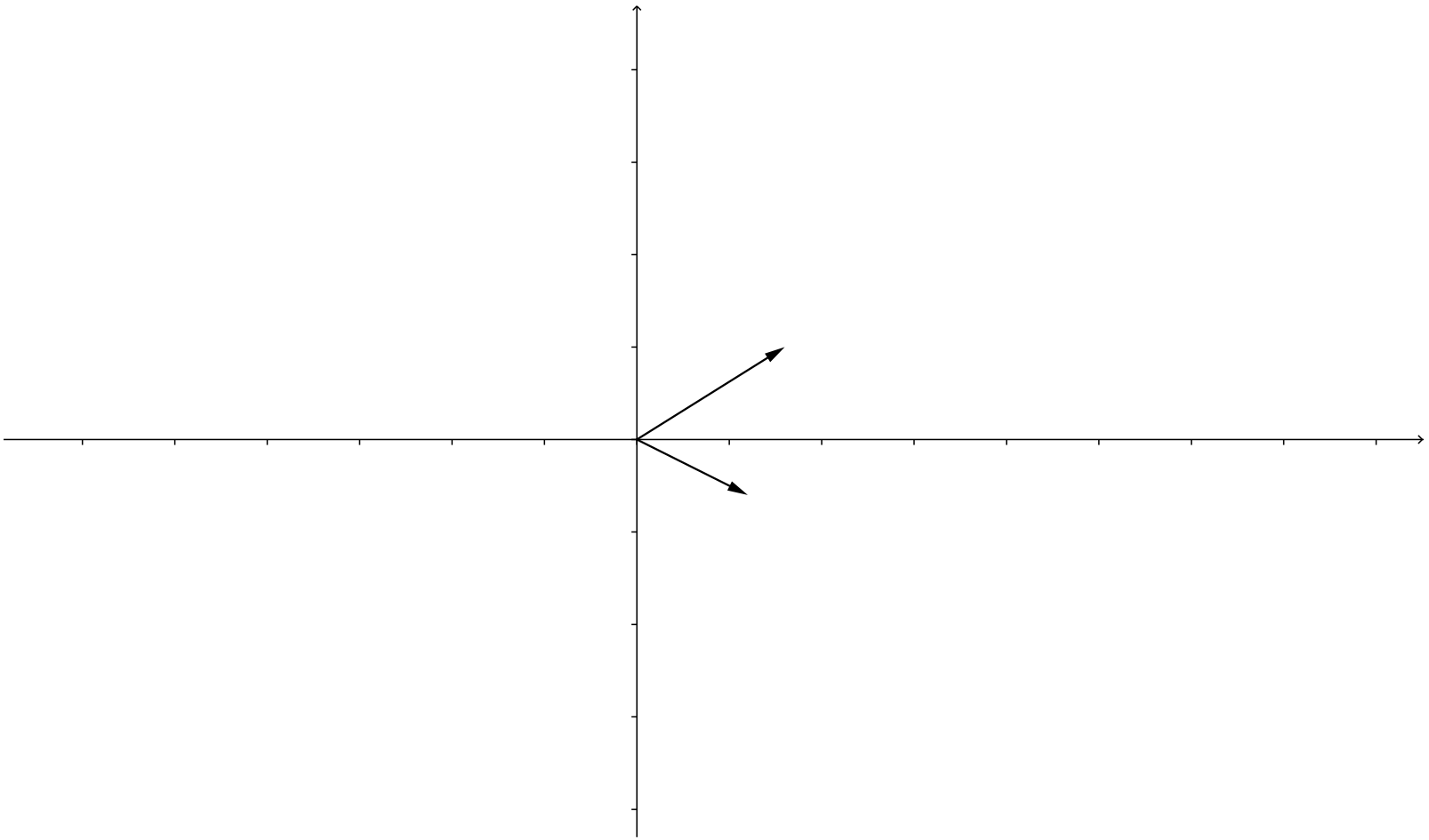
Reticulados no $\mathbb{R}^2$



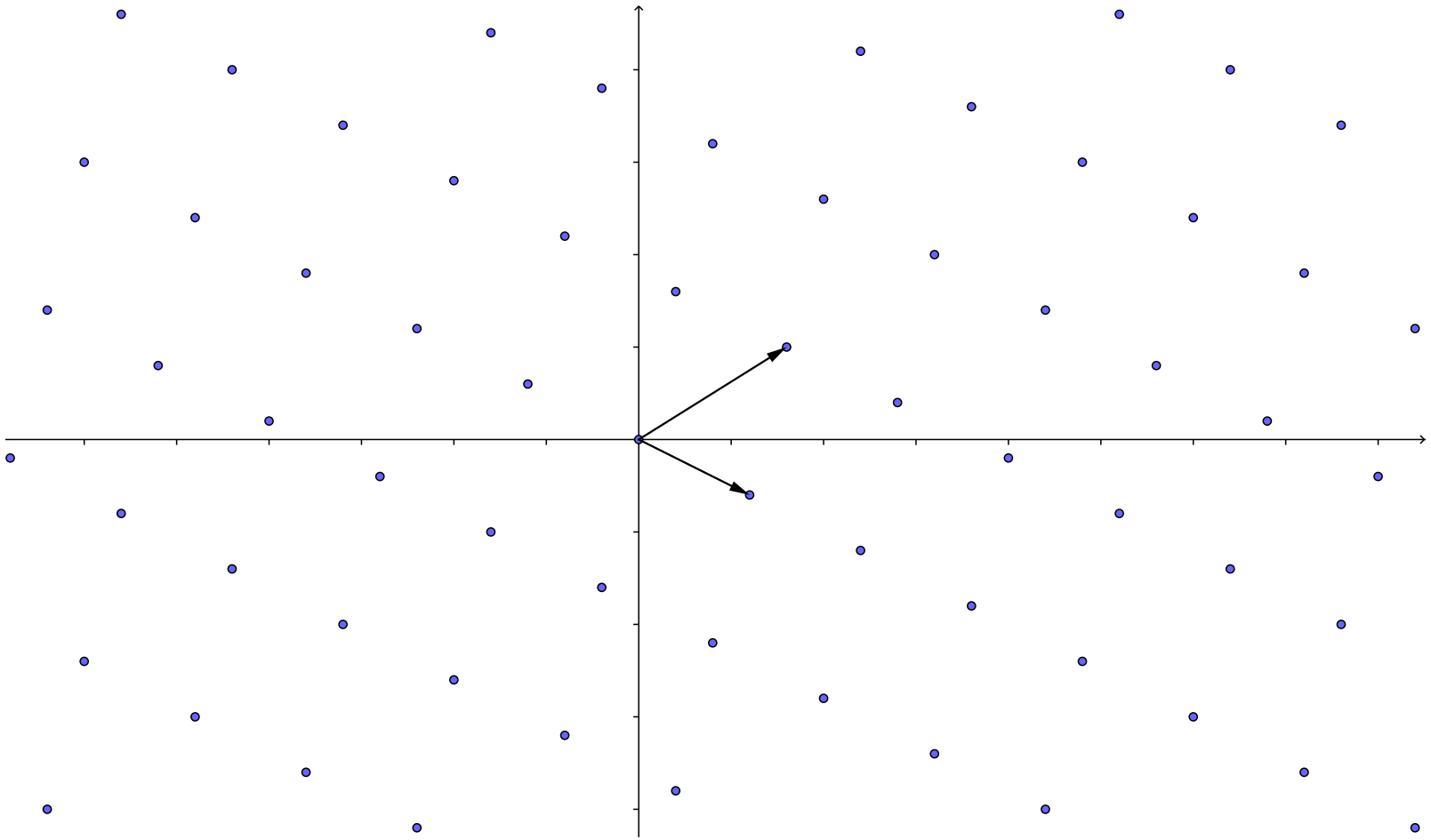
Reticulados no $\mathbb{R}^2$



Reticulados no $\mathbb{R}^2$



Reticulados no $\mathbb{R}^2$



Definições

Definição

Um **reticulado** *no* $\mathbb{R}^n$ *é um conjunto* $\Lambda \subset \mathbb{R}^n$ *gerado por todas as combinações* $\mathbb{Z}$*-lineares de* n *vetores linearmente independentes, i.e.,* $\Lambda = \mathbb{Z}v_1 + \cdots + \mathbb{Z}v_n$*. Diremos que* $v_1, \ldots, v_n$ *formam uma* **base** *do reticulado* Λ*.*

Definições

Definição

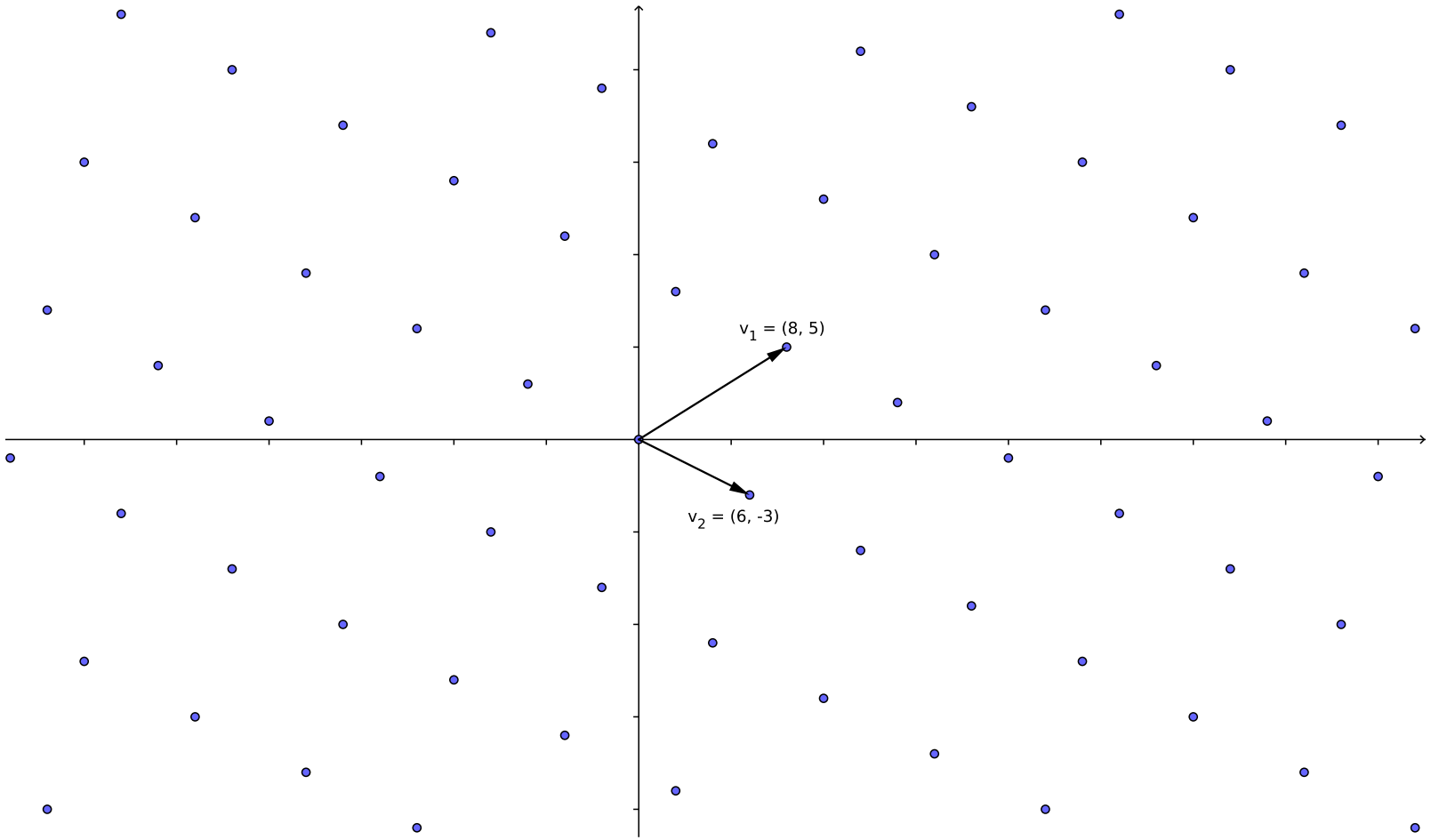
Um **reticulado** *no* $\mathbb{R}^n$ *é um conjunto* $\Lambda \subset \mathbb{R}^n$ *gerado por todas as combinações* $\mathbb{Z}$*-lineares de* n *vetores linearmente independentes, i.e.,* $\Lambda = \mathbb{Z}v_1 + \cdots + \mathbb{Z}v_n$*. Diremos que* $v_1, \ldots, v_n$ *formam uma* **base** *do reticulado* Λ*.*

Definição

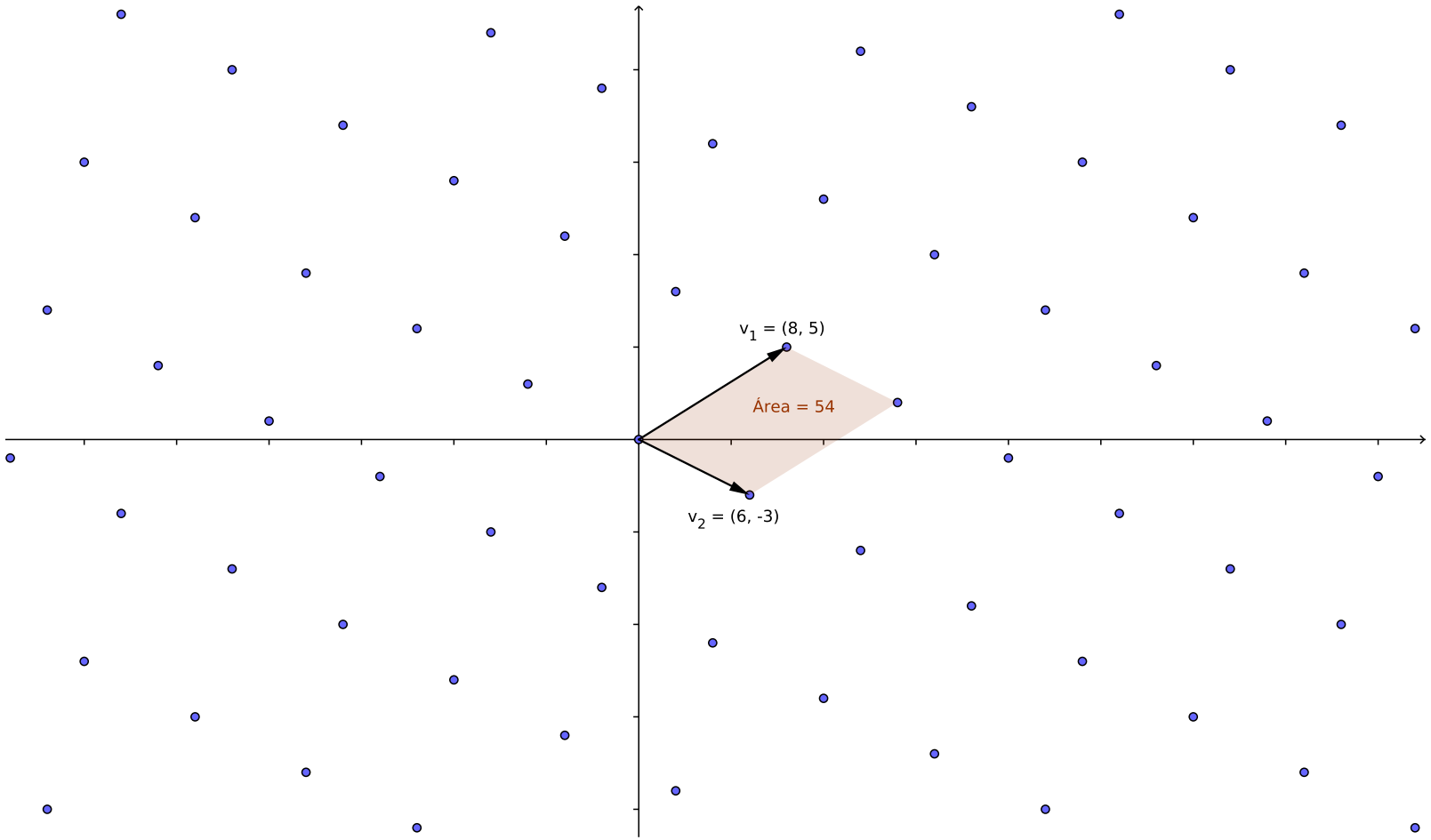
Seja Λ *um reticulado com base* $\{v_1, \ldots, v_n\}$*. O* **volume** *(ou* **área***, se* $n = 2$*) de* Λ *é definido como o módulo do determinante de* $v_1, \ldots, v_n$*:*

$$\mathrm{Vol}(\Lambda) = |\det(v_1, \ldots, v_n)|.$$

De volta ao exemplo no $\mathbb{R}^2$



De volta ao exemplo no $\mathbb{R}^2$



- Note que a escolha da base não é única. Ou seja, duas bases diferentes podem gerar o mesmo reticulado. Por exemplo, $\mathbb{Z}(1,0) + \mathbb{Z}(0,1) = \mathbb{Z}(-1,0) + \mathbb{Z}(0,1)$.

- Note que a escolha da base não é única. Ou seja, duas bases diferentes podem gerar o mesmo reticulado. Por exemplo, $\mathbb{Z}(1,0)+\mathbb{Z}(0,1)=\mathbb{Z}(-1,0)+\mathbb{Z}(0,1)$.
- Então é preciso verificar que o volume de um reticulado $\Lambda \subset \mathbb{R}^n$ está bem definido, i.e., não depende da escolha da base.

- Note que a escolha da base não é única. Ou seja, duas bases diferentes podem gerar o mesmo reticulado. Por exemplo, $\mathbb{Z}(1,0)+\mathbb{Z}(0,1)=\mathbb{Z}(-1,0)+\mathbb{Z}(0,1)$.
- Então é preciso verificar que o volume de um reticulado $\Lambda \subset \mathbb{R}^n$ está bem definido, i.e., não depende da escolha da base.
- Mas isto é fácil: se $\Lambda = \mathbb{Z}v_1 + \cdots + \mathbb{Z}v_n = \mathbb{Z}u_1 + \cdots + \mathbb{Z}u_n$, então existem inteiros a_{ij} tais que

$$v_i = a_{i1}u_1 + \cdots + a_{in}u_n,\ i = 1, \ldots, n.$$

Analogamente, existem inteiros b_{ij} tais que

$$u_i = b_{i1}v_1 + \cdots + b_{in}v_n,\ i = 1, \ldots, n.$$

Como cada $a_{ij}, b_{ij} \in \mathbb{Z}$, então $\det(a_{ij}), \det(b_{ij}) \in \mathbb{Z}$. Mas (a_{ij}) é uma matriz de mudança de base (pois os vetores são l.i.) e (b_{ij}) é a matriz de mudança de base inversa. Em particular $\det(a_{ij}) \det(b_{ij}) = 1$ e isto implica $\det(a_{ij}) = \det(b_{ij}) = \pm 1$, pois ambos são inteiros.
Além disso, podemos escrever

$$\begin{pmatrix} \leftarrow v_1 \rightarrow \\ \cdots \\ \leftarrow v_n \rightarrow \end{pmatrix} = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \cdots & \cdots & \cdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix} \begin{pmatrix} \leftarrow u_1 \rightarrow \\ \cdots \\ \leftarrow u_n \rightarrow \end{pmatrix}$$

Aplicando o determinante nos dois lados da equação matricial acima, concluímos que

$$|\det(v_1, \ldots, v_n)| = |\det(u_1, \ldots, u_n)|.$$

O Teorema de Minkowski

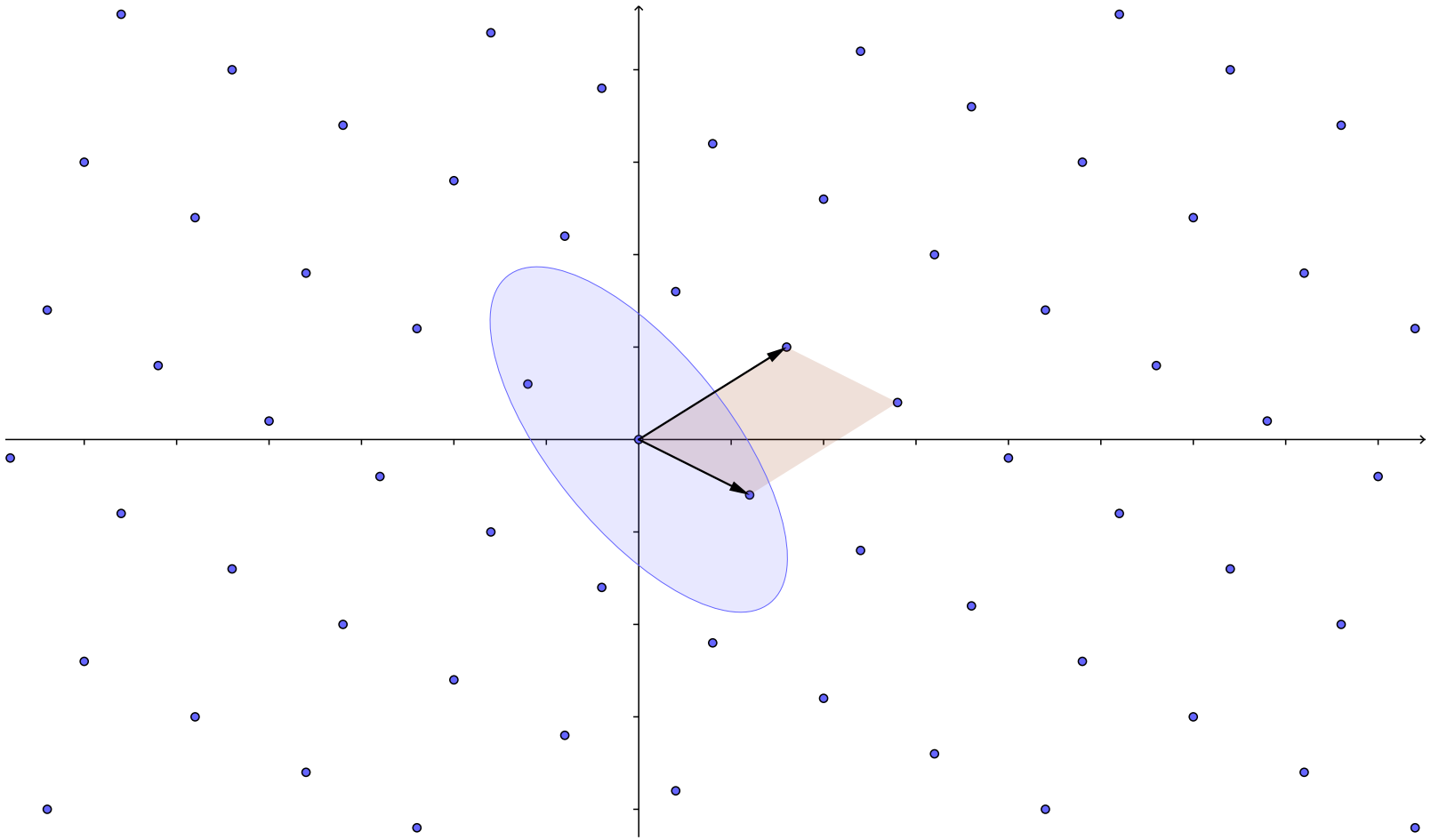
Teorema

Seja $\Lambda \subset \mathbb{R}^n$ um reticulado com volume λ. Se $S \subset \mathbb{R}^n$ é um conjunto convexo, simétrico com relação à origem (isto é, se $x \in S$, então $-x \in S$), e satisfaz

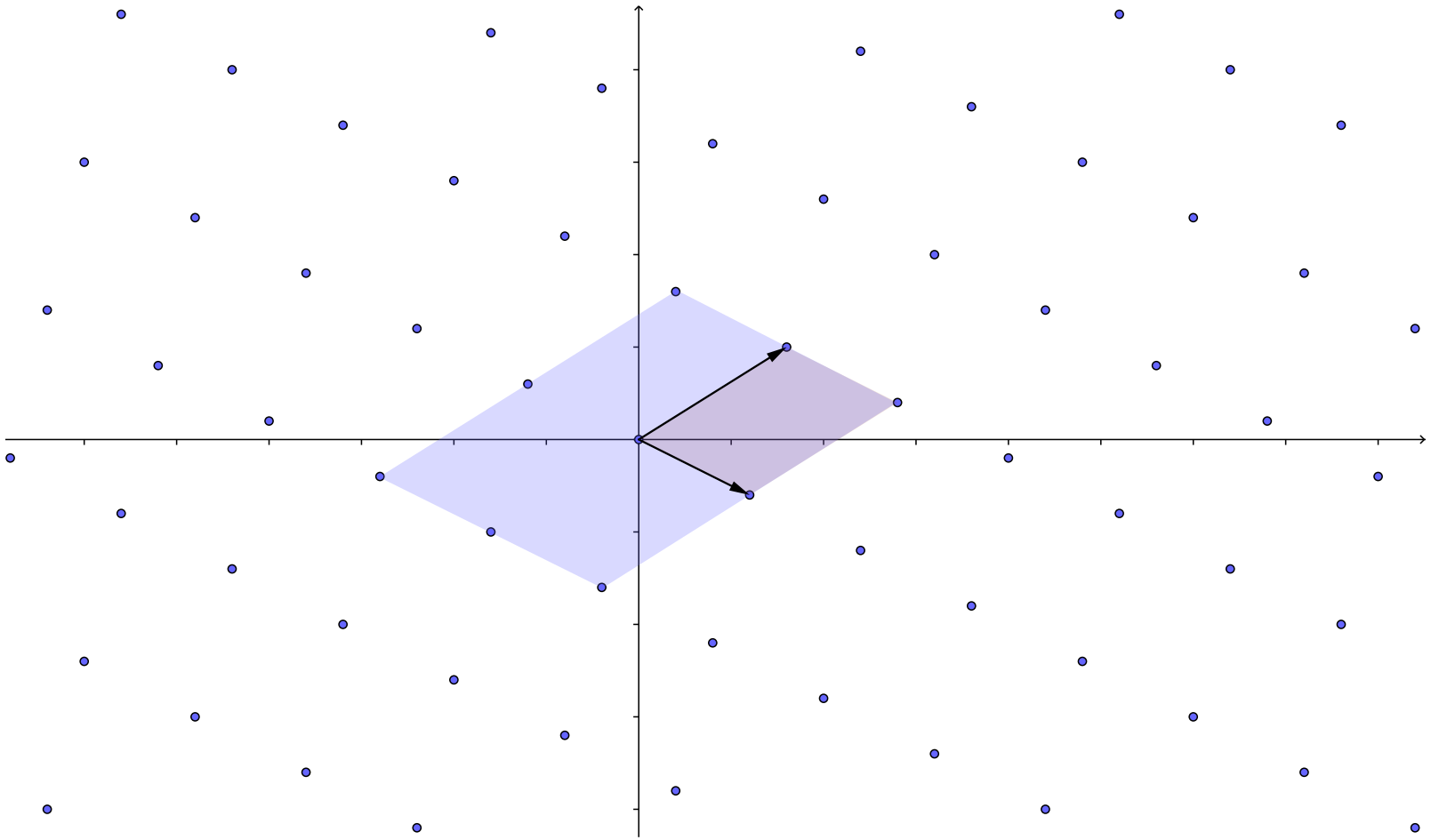
$$\mathrm{Vol}(S) > 2^n \lambda$$

Então existe pelo menos um ponto, diferente da origem, $x \in \Lambda \cap S$.

Mais exemplos



Mais exemplos



Teorema (Soma de dois quadrados)

Todo primo da forma $p = 4k + 1$ pode ser escrito como a soma de dois quadrados.

Teorema (Soma de dois quadrados)

Todo primo da forma $p = 4k + 1$ pode ser escrito como a soma de dois quadrados.

- Conhecido como um teorema de Fermat, mas a primeira demonstração de que se tem notícia é de Euler. Dedekind demonstrou o teorema de forma muito elegante utilizando o anel $\mathbb{Z}[i]$. Há também uma demonstração utilizando funções Θ (Análise Complexa). Outra legal é uma demonstração de uma frase só (no final).

Teorema (Soma de dois quadrados)

Todo primo da forma $p = 4k + 1$ pode ser escrito como a soma de dois quadrados.

- Conhecido como um teorema de Fermat, mas a primeira demonstração de que se tem notícia é de Euler. Dedekind demonstrou o teorema de forma muito elegante utilizando o anel $\mathbb{Z}[i]$. Há também uma demonstração utilizando funções Θ (Análise Complexa). Outra legal é uma demonstração de uma frase só (no final).
- A demonstração que iremos fazer aqui surgiu a partir do trabalho de Minkowski (fim do século 19).

Teorema (Soma de dois quadrados)

Todo primo da forma $p = 4k + 1$ pode ser escrito como a soma de dois quadrados.

- Conhecido como um teorema de Fermat, mas a primeira demonstração de que se tem notícia é de Euler. Dedekind demonstrou o teorema de forma muito elegante utilizando o anel $\mathbb{Z}[i]$. Há também uma demonstração utilizando funções Θ (Análise Complexa). Outra legal é uma demonstração de uma frase só (no final).
- A demonstração que iremos fazer aqui surgiu a partir do trabalho de Minkowski (fim do século 19).
- Antes de demonstrar de forma geral, façamos um caso particular, $p = 5$.

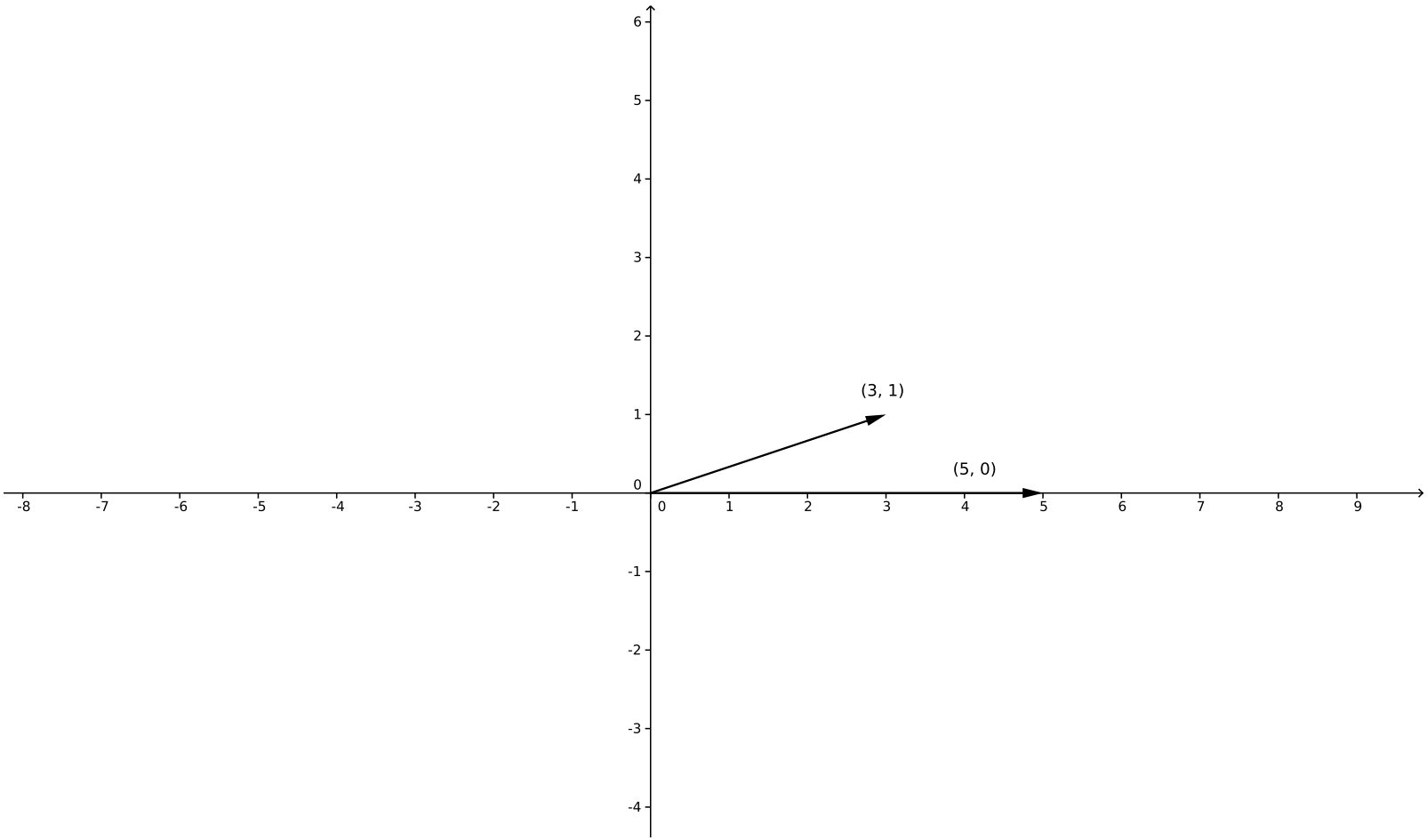
Exemplo: $p = 5$

- Primeiramente, devemos encontrar algum $u \in \mathbb{N}$ tal que $u^2 \equiv -1 \pmod 5$. Note que $u = 3$ satisfaz esta condição: $u^2 = 9 \equiv -1 \pmod 5$.

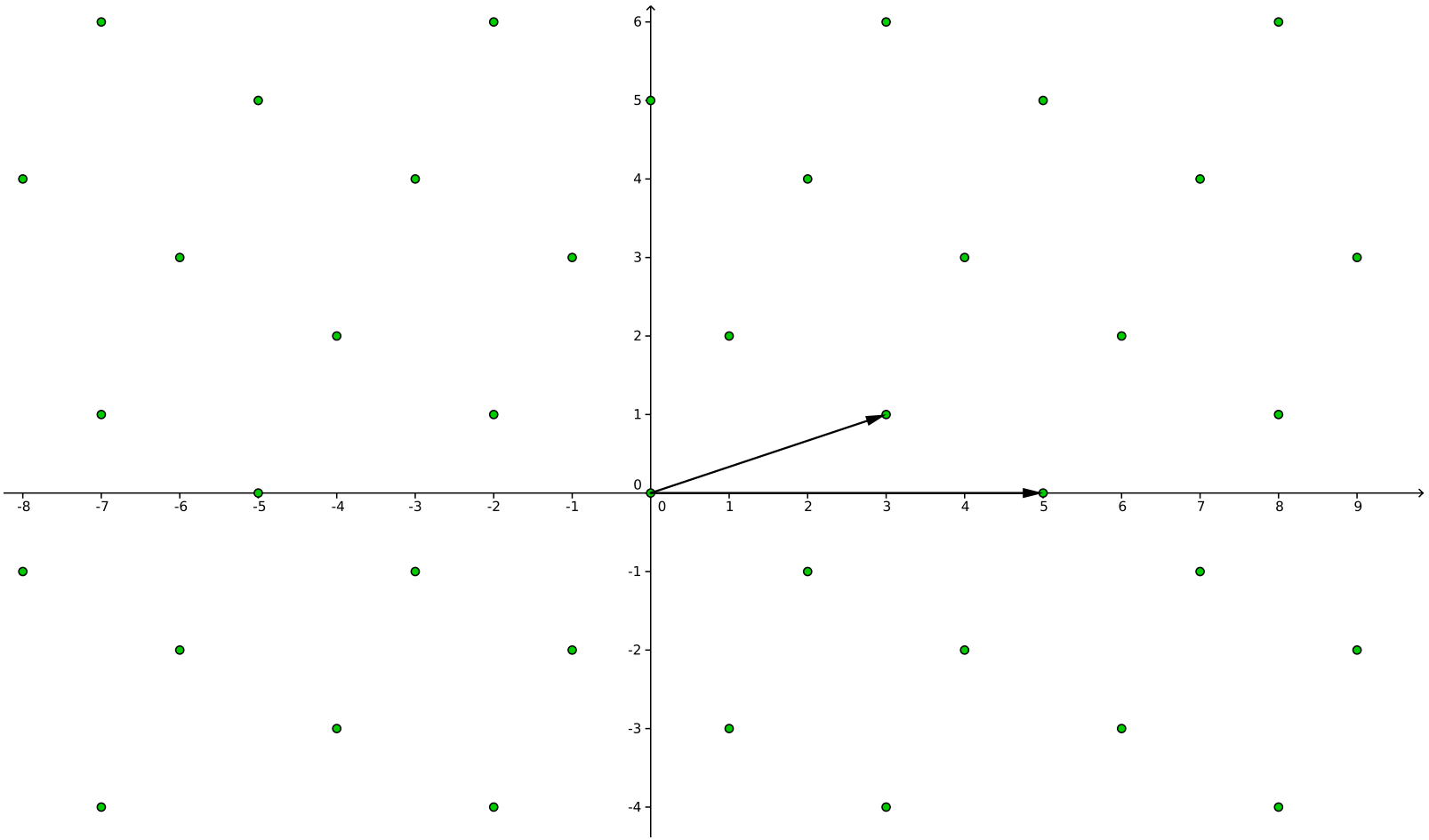
Exemplo: $p = 5$

- Primeiramente, devemos encontrar algum $u \in \mathbb{N}$ tal que $u^2 \equiv -1 \pmod 5$. Note que $u = 3$ satisfaz esta condição: $u^2 = 9 \equiv -1 \pmod 5$.
- Agora, note que o conjunto dos pares de inteiros (a, b) que satisfazem $a \equiv 3b \pmod 5$ formam um reticulado no $\mathbb{R}^2$. *Uma* possível base é $(3, 1)$ e $(5, 0)$.

Exemplo: $p = 5$



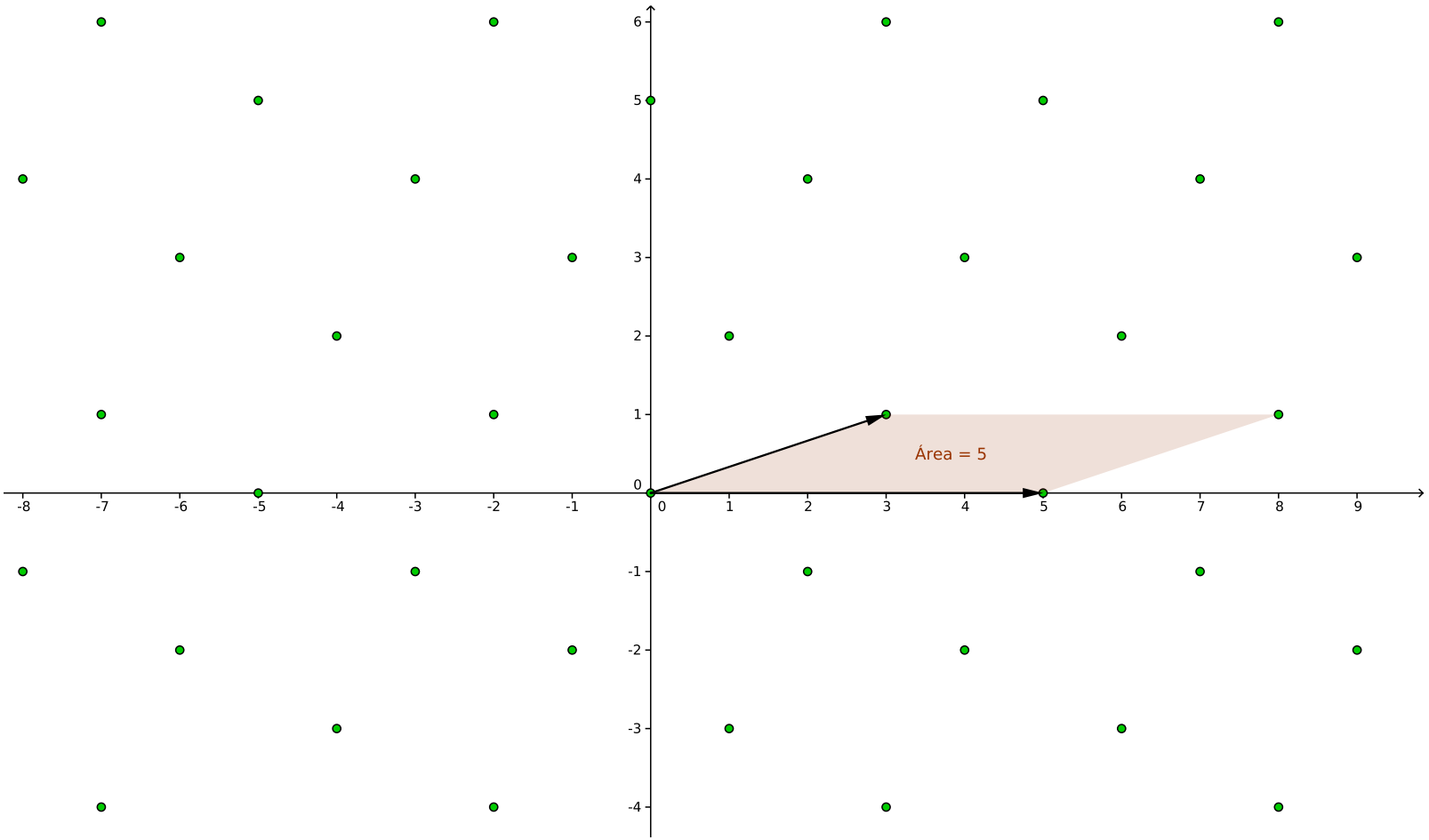
Exemplo: $p = 5$



Exemplo: $p = 5$

- Primeiramente, devemos encontrar algum $u \in \mathbb{N}$ tal que $u^2 \equiv -1 \pmod 5$. Note que $u = 3$ satisfaz esta condição: $u^2 = 9 \equiv -1 \pmod 5$.
- Agora, note que o conjunto dos pares de inteiros (a, b) que satisfazem $a \equiv 3b \pmod 5$ formam um reticulado no $\mathbb{R}^2$. *Uma* possível base é $(3, 1)$ e $(5, 0)$.
- A área deste reticulado é, portanto, igual a 5.

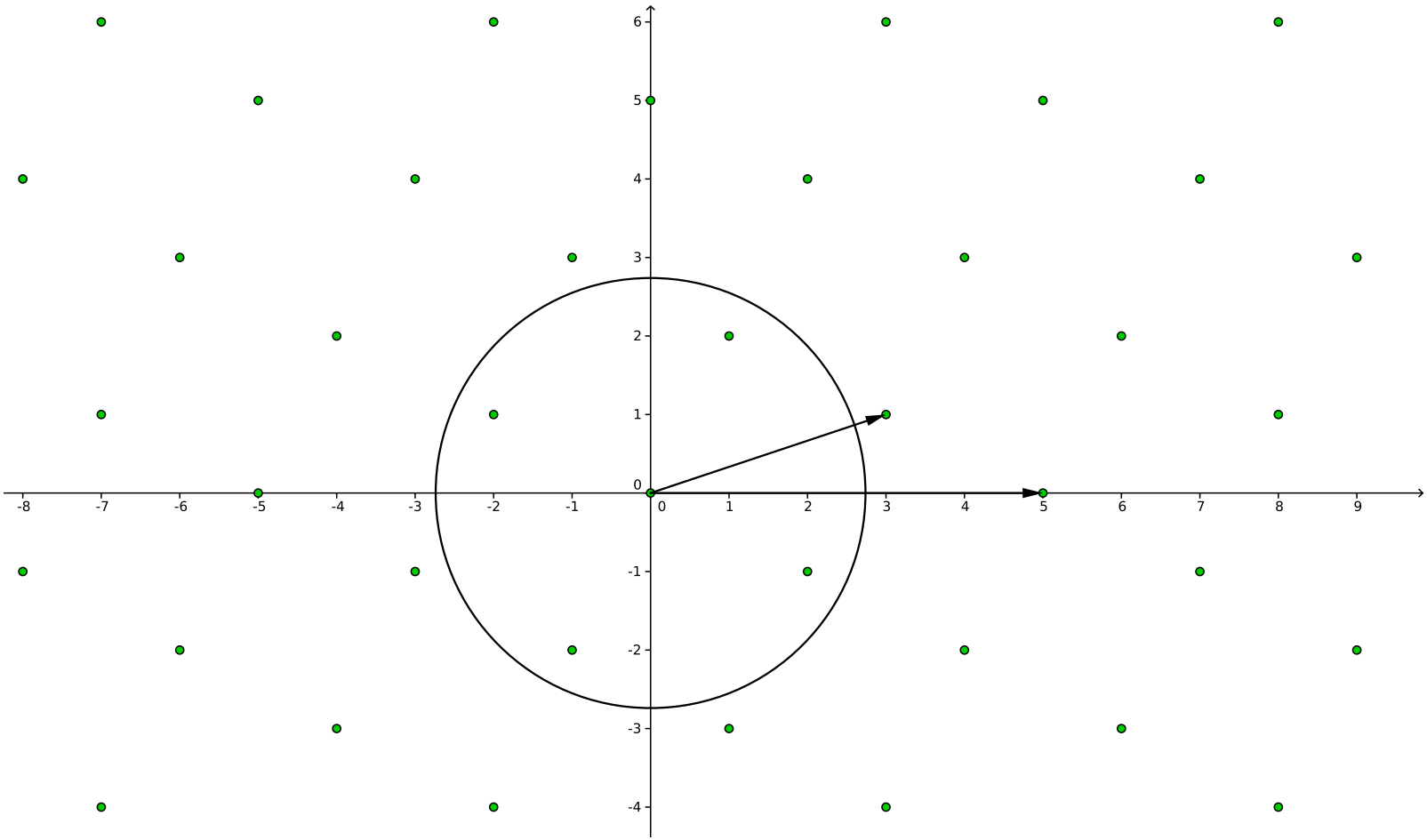
Exemplo: $p = 5$



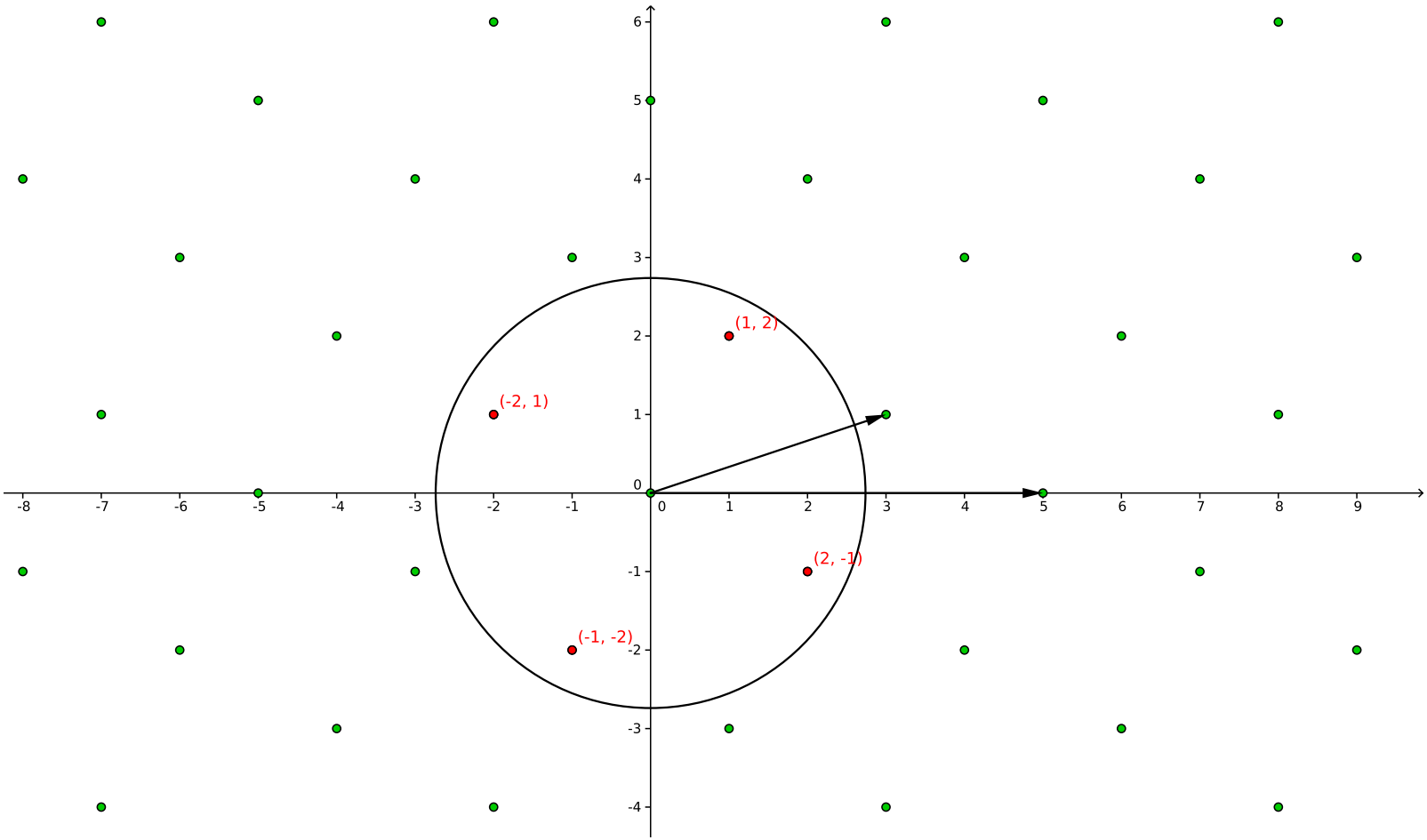
Exemplo: $p = 5$

- Primeiramente, devemos encontrar algum $u \in \mathbb{N}$ tal que $u^2 \equiv -1 \pmod 5$. Note que $u = 3$ satisfaz esta condição: $u^2 = 9 \equiv -1 \pmod 5$.
- Agora, note que o conjunto dos pares de inteiros (a, b) que satisfazem $a \equiv 3b \pmod 5$ formam um reticulado no $\mathbb{R}^2$. *Uma* possível base é $(3, 1)$ e $(5, 0)$.
- A área deste reticulado é, portanto, igual a 5.
- O truque consiste em tomar um círculo centrado na origem de raio $\sqrt{\frac{3p}{2}} = \sqrt{\frac{15}{2}} \simeq 2.73\ldots$.

Exemplo: $p = 5$



Exemplo: $p = 5$



Pré-requisitos

Lema

Se $p = 4k + 1$ é primo, então existe $u \in \mathbb{N}$ tal que $u^2 \equiv -1 \pmod{p}$.

Pré-requisitos

Lema

Se $p = 4k + 1$ é primo, então existe $u \in \mathbb{N}$ tal que $u^2 \equiv -1 \pmod{p}$.

Para a prova do lema, iremos usar o fato de que, se p é primo, então $\mathbb{Z}/(p) = \{\bar{0}, \bar{1}, \ldots, \overline{p-1}\}$ é um corpo. Ou seja, se $a \not\equiv 0 \pmod{p}$, então existe $b \in \mathbb{Z}$ tal que $ab \equiv 1 \pmod{p}$.

Pré-requisitos

Lema

Se $p = 4k + 1$ é primo, então existe $u \in \mathbb{N}$ tal que $u^2 \equiv -1 \pmod{p}$.

Para a prova do lema, iremos usar o fato de que, se p é primo, então $\mathbb{Z}/(p) = \{\bar{0}, \bar{1}, \ldots, \overline{p-1}\}$ é um corpo. Ou seja, se $a \not\equiv 0 \pmod{p}$, então existe $b \in \mathbb{Z}$ tal que $ab \equiv 1 \pmod{p}$.

Demonstração.

Por um lado, $(p-1)! = (p-1)(p-2)\cdots 2\cdot 1 \equiv -1 \pmod{p}$ pois, como o inverso módulo p de um inteiro em $\{2, 3, \ldots, p-2\}$ também está neste conjunto, podemos parear cada elemento com seu inverso na equação acima de forma que todo mundo se cancela e só sobra $(p-1)! \equiv p-1 \equiv -1 \pmod{p}$.

Demonstração.

Por um lado, $(p-1)! = (p-1)(p-2)\cdots 2\cdot 1 \equiv -1 \pmod{p}$ pois, como o inverso módulo p de um inteiro em $\{2, 3, \ldots, p-2\}$ também está neste conjunto, podemos parear cada elemento com seu inverso na equação acima de forma que todo mundo se cancela e só sobra $(p-1)! \equiv p-1 \equiv -1 \pmod{p}$. Por outro lado, como $p-1 = 4k$, podemos parear os inteiros da seguinte maneira

$$\begin{aligned}(p-1)! &\equiv 1(p-1)2(p-2)\cdots 2k(p-2k) \\ &\equiv 1(-1)2(-2)\cdots 2k(-2k) \equiv [(2k)!]^2 \pmod{p}\end{aligned}$$

Demonstração.

Por um lado, $(p-1)! = (p-1)(p-2)\cdots 2\cdot 1 \equiv -1 \pmod{p}$ pois, como o inverso módulo p de um inteiro em $\{2, 3, \ldots, p-2\}$ também está neste conjunto, podemos parear cada elemento com seu inverso na equação acima de forma que todo mundo se cancela e só sobra $(p-1)! \equiv p-1 \equiv -1 \pmod{p}$. Por outro lado, como $p-1 = 4k$, podemos parear os inteiros da seguinte maneira

$$\begin{aligned}(p-1)! &\equiv 1(p-1)2(p-2)\cdots 2k(p-2k) \\ &\equiv 1(-1)2(-2)\cdots 2k(-2k) \equiv [(2k)!]^2 \pmod{p}\end{aligned}$$

Tomando $u = (2k)!$, temos $u^2 \equiv -1 \pmod{p}$. □

Demonstração do Teorema

Fixe u qualquer tal que $u^2 \equiv -1 \pmod{p}$ e considere o conjunto Λ de todos os pares $(a, b) \in \mathbb{Z}^2$ tais que

$$a \equiv ub \pmod{p}.$$

Demonstração do Teorema

Fixe u qualquer tal que $u^2 \equiv -1 \pmod{p}$ e considere o conjunto Λ de todos os pares $(a, b) \in \mathbb{Z}^2$ tais que

$$a \equiv ub \pmod{p}.$$

É fácil mostrar que $\Lambda \subset \mathbb{R}^2$ é um reticulado.

Demonstração do Teorema

Fixe u qualquer tal que $u^2 \equiv -1 \pmod{p}$ e considere o conjunto Λ de todos os pares $(a, b) \in \mathbb{Z}^2$ tais que

$$a \equiv ub \pmod{p}.$$

É fácil mostrar que $\Lambda \subset \mathbb{R}^2$ é um reticulado. De fato, basta notar que $\Lambda = \mathbb{Z}(p, 0) + \mathbb{Z}(u, 1)$: a inclusão $\mathbb{Z}(p, 0) + \mathbb{Z}(u, 1) \subset \Lambda$ é imediata. Se $(a, b) \in \Lambda$, então a e b satisfazem a congruência acima, i.e., $a = ub + pk$, $k \in \mathbb{Z}$. Logo $(a, b) = k(p, 0) + b(u, 1)$, o que mostra a outra inclusão.

Demonstração do Teorema

Fixe u qualquer tal que $u^2 \equiv -1 \pmod{p}$ e considere o conjunto Λ de todos os pares $(a, b) \in \mathbb{Z}^2$ tais que

$$a \equiv ub \pmod{p}.$$

É fácil mostrar que $\Lambda \subset \mathbb{R}^2$ é um reticulado. De fato, basta notar que $\Lambda = \mathbb{Z}(p, 0) + \mathbb{Z}(u, 1)$: a inclusão $\mathbb{Z}(p, 0) + \mathbb{Z}(u, 1) \subset \Lambda$ é imediata. Se $(a, b) \in \Lambda$, então a e b satisfazem a congruência acima, i.e., $a = ub + pk$, $k \in \mathbb{Z}$. Logo $(a, b) = k(p, 0) + b(u, 1)$, o que mostra a outra inclusão.
A área de Λ é, portanto,

$$\lambda = \begin{vmatrix} p & 0 \\ u & 1 \end{vmatrix} = p.$$

Demonstração do Teorema

Seja $\mathcal{C}$ um círculo de raio $\sqrt{\frac{3p}{2}}$ centrado na origem. A área deste círculo é $\frac{3}{2}p\pi$ e, portanto, estritamente maior que $4p$.

Demonstração do Teorema

Seja $\mathcal{C}$ um círculo de raio $\sqrt{\frac{3p}{2}}$ centrado na origem. A área deste círculo é $\frac{3}{2}p\pi$ e, portanto, estritamente maior que $4p$. Pelo *Teorema de Minkowski*, existe um ponto diferente da origem $(x, y) \in \mathcal{C} \cap \Lambda$. Como $(x, y) \in \Lambda$, então

$$x \equiv uy \pmod{p} \Rightarrow p \mid x^2 + y^2.$$

Demonstração do Teorema

Seja $\mathcal{C}$ um círculo de raio $\sqrt{\frac{3p}{2}}$ centrado na origem. A área deste círculo é $\frac{3}{2}p\pi$ e, portanto, estritamente maior que $4p$. Pelo *Teorema de Minkowski*, existe um ponto diferente da origem $(x, y) \in \mathcal{C} \cap \Lambda$. Como $(x, y) \in \Lambda$, então

$$x \equiv uy \pmod{p} \Rightarrow p \mid x^2 + y^2.$$

Por outro lado, como $(x, y) \in \mathcal{C}$, temos que

$$\sqrt{x^2 + y^2} \leq \sqrt{\frac{3p}{2}} \Rightarrow x^2 + y^2 \leq \frac{3p}{2}$$

Demonstração do Teorema

Seja $\mathcal{C}$ um círculo de raio $\sqrt{\frac{3p}{2}}$ centrado na origem. A área deste círculo é $\frac{3}{2}p\pi$ e, portanto, estritamente maior que $4p$. Pelo *Teorema de Minkowski*, existe um ponto diferente da origem $(x, y) \in \mathcal{C} \cap \Lambda$. Como $(x, y) \in \Lambda$, então

$$x \equiv uy \pmod{p} \Rightarrow p \mid x^2 + y^2.$$

Por outro lado, como $(x, y) \in \mathcal{C}$, temos que

$$\sqrt{x^2 + y^2} \leq \sqrt{\frac{3p}{2}} \Rightarrow x^2 + y^2 \leq \frac{3p}{2}$$

Logo a única possibilidade é $x^2 + y^2 = p$.

Demonstração do Teorema

Seja $\mathcal{C}$ um círculo de raio $\sqrt{\frac{3p}{2}}$ centrado na origem. A área deste círculo é $\frac{3}{2}p\pi$ e, portanto, estritamente maior que $4p$. Pelo *Teorema de Minkowski*, existe um ponto diferente da origem $(x, y) \in \mathcal{C} \cap \Lambda$. Como $(x, y) \in \Lambda$, então

$$x \equiv uy \pmod{p} \Rightarrow p \mid x^2 + y^2.$$

Por outro lado, como $(x, y) \in \mathcal{C}$, temos que

$$\sqrt{x^2 + y^2} \leq \sqrt{\frac{3p}{2}} \Rightarrow x^2 + y^2 \leq \frac{3p}{2}$$

Logo a única possibilidade é $x^2 + y^2 = p$. ☺

Teorema (Soma de quatro quadrados)

Todo *número natural n pode ser escrito como a soma de quatro quadrados.*

Teorema (Soma de quatro quadrados)

Todo *número natural n pode ser escrito como a soma de quatro quadrados.*

Desta vez, sem desenhos. Ainda não aprendi a desenhar em 4 dimensões.

Pré-requisitos

Lema

Se m e n são somas de quatro quadrados, então $m \cdot n$ também o é.

Demonstração.

Faça $\alpha = a + bi, \beta = -c - di, \gamma = w + xi$ e $\delta = y + zi$ e aplique o determinante nos dois lados da equação

$$\begin{pmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{pmatrix} \begin{pmatrix} \gamma & \delta \\ -\overline{\delta} & \overline{\gamma} \end{pmatrix} = \begin{pmatrix} \alpha\gamma - \beta\overline{\delta} & \alpha\delta + \beta\overline{\gamma} \\ -\overline{(\alpha\delta + \beta\overline{\gamma})} & \overline{\alpha\gamma - \beta\overline{\delta}} \end{pmatrix}.$$

Demonstração do Teorema

Pelo lema anterior, basta mostrar esta afirmação para n primo. Então, seja p um primo qualquer e fixe dois inteiros u e v que satisfazem

$$u^2 + v^2 + 1 \equiv 0 \pmod{p}.$$

Demonstração do Teorema

Pelo lema anterior, basta mostrar esta afirmação para n primo. Então, seja p um primo qualquer e fixe dois inteiros u e v que satisfazem

$$u^2 + v^2 + 1 \equiv 0 \pmod{p}.$$

Note que u e v existem pois u^2 percorre $\frac{p+1}{2}$ classes distintas módulo p quando u varia, e o mesmo vale para $-v^2 - 1$, então deve existir algum par (u, v) que satisfaz $u^2 \equiv -v^2 - 1 \pmod{p}$.

Demonstração do Teorema

Pelo lema anterior, basta mostrar esta afirmação para n primo. Então, seja p um primo qualquer e fixe dois inteiros u e v que satisfazem

$$u^2 + v^2 + 1 \equiv 0 \pmod{p}.$$

Note que u e v existem pois u^2 percorre $\frac{p+1}{2}$ classes distintas módulo p quando u varia, e o mesmo vale para $-v^2 - 1$, então deve existir algum par (u, v) que satisfaz $u^2 \equiv -v^2 - 1 \pmod{p}$. Agora, considere o conjunto $\Lambda \subset \mathbb{Z}^4$ de todos as quádruplas (a, b, c, d) onde

$$c \equiv au + bv \pmod{p} \text{ e } d \equiv av - bu \pmod{p}.$$

Demonstração do Teorema

É fácil verificar que Λ é um reticulado e $\{(1,0,1,0),(0,1,1,-1),(0,0,p,0),\ (0,0,0,p)\}$ é uma base para Λ. De imediato também conclui-se que o volume de Λ é p^2.

Demonstração do Teorema

É fácil verificar que Λ é um reticulado e $\{(1,0,1,0),(0,1,1,-1),(0,0,p,0),\ (0,0,0,p)\}$ é uma base para Λ. De imediato também conclui-se que o volume de Λ é p^2. Agora considere uma hiperesfera (de 4 dimensões) S de raio $r = \sqrt{1.9p}$. O volume de uma 4-esfera é dado por

$$\frac{\pi^2 r^4}{2}.$$

Demonstração do Teorema

É fácil verificar que Λ é um reticulado e $\{(1,0,1,0),(0,1,1,-1),(0,0,p,0),(0,0,0,p)\}$ é uma base para Λ. De imediato também conclui-se que o volume de Λ é p^2. Agora considere uma hiperesfera (de 4 dimensões) S de raio $r = \sqrt{1.9p}$. O volume de uma 4-esfera é dado por

$$\frac{\pi^2 r^4}{2}.$$

Então $\mathrm{Vol}(S) > 16p^2$ e, portanto, existe um ponto diferente da origem $(x,y,z,w) \in \Lambda \cap S$. Pelas relações acima,

$$p \mid x^2 + y^2 + z^2 + w^2.$$

Demonstração do Teorema

É fácil verificar que Λ é um reticulado e $\{(1,0,1,0),(0,1,1,-1),(0,0,p,0),\ (0,0,0,p)\}$ é uma base para Λ. De imediato também conclui-se que o volume de Λ é p^2. Agora considere uma hiperesfera (de 4 dimensões) S de raio $r = \sqrt{1.9p}$. O volume de uma 4-esfera é dado por

$$\frac{\pi^2 r^4}{2}.$$

Então $\mathrm{Vol}(S) > 16p^2$ e, portanto, existe um ponto diferente da origem $(x,y,z,w) \in \Lambda \cap S$. Pelas relações acima,

$$p \mid x^2 + y^2 + z^2 + w^2.$$

Mas, como $x^2 + y^2 + z^2 + w^2 < 1.9p$, devemos ter $p = x^2 + y^2 + z^2 + w^2$.

Demonstração do Teorema

É fácil verificar que Λ é um reticulado e $\{(1,0,1,0),(0,1,1,-1),(0,0,p,0),\ (0,0,0,p)\}$ é uma base para Λ. De imediato também conclui-se que o volume de Λ é p^2. Agora considere uma hiperesfera (de 4 dimensões) S de raio $r = \sqrt{1.9p}$. O volume de uma 4-esfera é dado por

$$\frac{\pi^2 r^4}{2}.$$

Então $\mathrm{Vol}(S) > 16p^2$ e, portanto, existe um ponto diferente da origem $(x,y,z,w) \in \Lambda \cap S$. Pelas relações acima,

$$p \mid x^2 + y^2 + z^2 + w^2.$$

Mas, como $x^2 + y^2 + z^2 + w^2 < 1.9p$, devemos ter $p = x^2 + y^2 + z^2 + w^2$. ☺

Demonstração com uma única frase (devida a Don Zagier) do teorema da soma de dois quadrados:

Demonstração.

A involução, no conjunto finito $S = \{(x, y, z) \in \mathbb{N}^3 \mid x^2 + 4yz = p\}$, definida por

$$(x, y, z) \mapsto \begin{cases} (x + 2z, z, y - x - z) & \text{se } x < y - z \\ (2y - x, y, x - y + z) & \text{se } y - z < x < 2y \\ (x - 2y, x - y + z, y) & \text{se } x > 2y \end{cases}$$

tem exatamente um único ponto fixo $(1, 1, k)$, logo $\#S$ é ímpar e a involução definida por $(x, y, z) \mapsto (x, z, y)$ também possui um ponto fixo. □

Referências bibliográficas

- Stewart, Ian e Tall, David; "**Algebraic Number Theory and Fermat's Last Theorem**"; AK Peters, Ltd.; third edition, 2001.
- C.D., Olds e Lax, Anneli; "**The Geometry of Numbers**"; MAA; 2000.
- Conway, J.H. e Sloane, N. "**Sphere packings, lattices, and groups**";
- Wikipedia!