A Fermat–Euler-tétel

11. évfolyam

9. Matektábor

2012. október

Bevezetés

Mely prímek írhatók fel két négyzetszám összegeként?

Bevezetés

Mely prímek írhatók fel két négyzetszám összegeként?

$$2 = 1^2 + 1^2,$$
$$5 = 1^2 + 2^2,$$
$$13 = 2^2 + 3^2,$$
$$\ldots$$

A tétel

Tétel (Fermat–Euler-tétel)

Egy kettőnél nagyobb prímszám akkor és csak akkor bontható fel két négyzetszám összegére, ha 4-gyel osztva 1 maradékot ad.

A tétel

Tétel (Fermat–Euler-tétel)

Egy kettőnél nagyobb prímszám akkor és csak akkor bontható fel két négyzetszám összegére, ha 4-gyel osztva 1 maradékot ad.

- Pierre Fermat (1640) $\rightarrow$ bizonyításvázlat

A tétel

Tétel (Fermat–Euler-tétel)

Egy kettőnél nagyobb prímszám akkor és csak akkor bontható fel két négyzetszám összegére, ha 4-gyel osztva 1 maradékot ad.

- Pierre Fermat (1640) $\rightarrow$ bizonyításvázlat
- Első teljes bizonyítás: Leonhard Euler (1740-es évek)

A „csak akkor” irány bizonyítása

Ha egy 2-nél nagyobb prím felbontható két négyzetszám összegére, akkor 4-gyel osztva 1 maradékot ad.

A „csak akkor” irány bizonyítása

Ha egy 2-nél nagyobb prím felbontható két négyzetszám összegére, akkor 4-gyel osztva 1 maradékot ad.

- $p = a^2 + b^2 \implies$ a és b egyike páratlan, a másik páros

A „csak akkor” irány bizonyítása

Ha egy 2-nél nagyobb prím felbontható két négyzetszám összegére, akkor 4-gyel osztva 1 maradékot ad.

- $p = a^2 + b^2 \implies$ a és b egyike páratlan, a másik páros: $a = 2k$, $b = 2l + 1$

A „csak akkor” irány bizonyítása

Ha egy 2-nél nagyobb prím felbontható két négyzetszám összegére, akkor 4-gyel osztva 1 maradékot ad.

- $p = a^2 + b^2 \implies$ a és b egyike páratlan, a másik páros: $a = 2k$, $b = 2l + 1$
- $p = (2k)^2 + (2l + 1)^2 =$

A „csak akkor” irány bizonyítása

Ha egy 2-nél nagyobb prím felbontható két négyzetszám összegére, akkor 4-gyel osztva 1 maradékot ad.

- $p = a^2 + b^2 \implies$ a és b egyike páratlan, a másik páros: $a = 2k$, $b = 2l + 1$
- $p = (2k)^2 + (2l + 1)^2 =$
  $4k^2 + 4l^2 + 4l + 1 =$

A „csak akkor” irány bizonyítása

Ha egy 2-nél nagyobb prím felbontható két négyzetszám összegére, akkor 4-gyel osztva 1 maradékot ad.

- $p = a^2 + b^2 \implies$ a és b egyike páratlan, a másik páros: $a = 2k$, $b = 2l + 1$
- $p = (2k)^2 + (2l + 1)^2 =$
  $4k^2 + 4l^2 + 4l + 1 = 4\left(k^2 + l^2 + l\right) + 1$ □

Az „akkor” irány bizonyításai

Minden $p = 4n + 1$ prímszám felbontható két négyzetszám összegére.

Lagrange bizonyítása

Lemma (Wilson-tétel)

Ha p prím, $(p-1)!+1$ osztható p-vel.

Következmény

Ha $p = 4n+1$ prím, akkor $p \mid ((2n)!)^2 + 1$.

Ha $p = 4n + 1$ prím, akkor $p \mid ((2n)!)^2 + 1$.

Ha $p = 4n + 1$ prím, akkor $p \mid ((2n)!)^2 + 1$.

$$p \mid (p-1)! + 1 \implies p \mid (4n)! + 1$$

Ha $p = 4n + 1$ prím, akkor $p \mid ((2n)!)^2 + 1$.

$$p \mid (p-1)! + 1 \implies p \mid (4n)! + 1$$

$$(4n)! + 1 = (1 \cdot 2 \cdot \ldots \cdot (2n) \cdot (2n+1) \cdot \\ \cdot (2n+2) \cdot \ldots (4n)) + 1$$

Ha $p = 4n + 1$ prím, akkor $p \mid ((2n)!)^2 + 1$.

$$p \mid (p-1)! + 1 \implies p \mid (4n)! + 1$$

$$\begin{aligned}(4n)! + 1 &= (1 \cdot 2 \cdot \ldots \cdot (2n) \cdot (2n+1) \cdot \\ &\quad \cdot (2n+2) \cdot \ldots (4n)) + 1 \\ &= (1 \cdot 2 \cdot \ldots \cdot (2n) \cdot (p-2n) \cdot \\ &\quad \cdot (p-(2n-1)) \cdot \ldots (p-1)) + 1\end{aligned}$$

Ha $p = 4n + 1$ prím, akkor $p \mid ((2n)!)^2 + 1$.

$$p \mid (p-1)! + 1 \implies p \mid (4n)! + 1$$

$$\begin{aligned}
(4n)! + 1 &= (1 \cdot 2 \cdot \ldots \cdot (2n) \cdot (2n+1) \cdot \\
&\quad \cdot (2n+2) \cdot \ldots (4n)) + 1 \\
&= (1 \cdot 2 \cdot \ldots \cdot (2n) \cdot (p-2n) \cdot \\
&\quad \cdot (p-(2n-1)) \cdot \ldots (p-1)) + 1 \\
&\equiv \Big((2n)! \cdot (-1)^{2n} \cdot (2n)!\Big) + 1 \quad (p)
\end{aligned}$$

Ha $p = 4n + 1$ prím, akkor $p \mid ((2n)!)^2 + 1$.

$$p \mid (p-1)! + 1 \implies p \mid (4n)! + 1$$

$$\begin{aligned}
(4n)! + 1 &= (1 \cdot 2 \cdot \ldots \cdot (2n) \cdot (2n+1) \cdot \\
&\quad \cdot (2n+2) \cdot \ldots (4n)) + 1 \\
&= (1 \cdot 2 \cdot \ldots \cdot (2n) \cdot (p-2n) \cdot \\
&\quad \cdot (p-(2n-1)) \cdot \ldots (p-1)) + 1 \\
&\equiv \left((2n)! \cdot (-1)^{2n} \cdot (2n)!\right) + 1 \quad (p) \\
&\equiv ((2n)!)^2 + 1 \pmod{p}
\end{aligned}$$

- $N = (2n)! \implies N^2 \equiv -1 \pmod{p}$

- $N = (2n)! \implies N^2 \equiv -1 \pmod{p}$
- $(k; m)$ rendezett párok
  $k, m \in \mathbb{Z}^+ \cup \{0\}$; $k, m \leq \sqrt{p}$

- $N = (2n)! \implies N^2 \equiv -1 \pmod{p}$
- $(k; m)$ rendezett párok
  $k, m \in \mathbb{Z}^+ \cup \{0\}$; $k, m \leq \sqrt{p}$
- $\max k, \max m > \sqrt{p} - 1$
  $\implies$ párok száma $> ((\sqrt{p} - 1) + 1)^2 = p$

- $N = (2n)! \implies N^2 \equiv -1 \pmod{p}$
- $(k; m)$ rendezett párok
  $k, m \in \mathbb{Z}^+ \cup \{0\}$; $k, m \leq \sqrt{p}$
- $\max k, \max m > \sqrt{p} - 1$
  $\implies$ párok száma $> ((\sqrt{p} - 1) + 1)^2 = p$
- $(k; m) \to k + Nm$

- $N = (2n)! \implies N^2 \equiv -1 \pmod{p}$
- $(k; m)$ rendezett párok
  $k, m \in \mathbb{Z}^+ \cup \{0\}$; $k, m \leq \sqrt{p}$
- $\max k, \max m > \sqrt{p} - 1$
  $\implies$ párok száma $> ((\sqrt{p} - 1) + 1)^2 = p$
- $(k; m) \to k + Nm$
- Skatulyaelv miatt van két pár, amire

$$k_1 + Nm_1 \equiv k_2 + Nm_2 \pmod{p}$$

$$\begin{array}{rr} & k_1 + Nm_1 \\ - & k_2 + Nm_2 \\ \hline & a + Nb \end{array}$$

$$\begin{array}{r} k_1 + Nm_1 \\ -\quad k_2 + Nm_2 \\ \hline a + Nb \end{array} \qquad \begin{aligned} a &= k_1 - k_2 \\ b &= m_1 - m_2 \end{aligned}$$

$$\begin{array}{r} k_1 + Nm_1 \\ -\quad k_2 + Nm_2 \\ \hline a + Nb \end{array} \qquad \begin{aligned} a &= k_1 - k_2 \\ b &= m_1 - m_2 \end{aligned} \qquad \begin{aligned} |a| &< \sqrt{p} \\ |b| &< \sqrt{p} \end{aligned}$$

$$\begin{array}{r} k_1 + Nm_1 \\ -\ k_2 + Nm_2 \\ \hline a + Nb \end{array}$$

$$a = k_1 - k_2 \qquad |a| < \sqrt{p}$$
$$b = m_1 - m_2 \qquad |b| < \sqrt{p}$$

$$p \mid a + Nb$$

$$\begin{array}{r} k_1 + Nm_1 \\ -\ k_2 + Nm_2 \\ \hline a + Nb \end{array} \qquad \begin{array}{l} a = k_1 - k_2 \\ b = m_1 - m_2 \end{array} \qquad \begin{array}{l} |a| < \sqrt{p} \\ |b| < \sqrt{p} \end{array}$$

$$p|a + Nb \implies p|(a + Nb)(a - Nb) =$$

$$\begin{array}{r} k_1 + Nm_1 \\ -\ k_2 + Nm_2 \\ \hline a + Nb \end{array} \qquad \begin{array}{l} a = k_1 - k_2 \\ b = m_1 - m_2 \end{array} \qquad \begin{array}{l} |a| < \sqrt{p} \\ |b| < \sqrt{p} \end{array}$$

$$p|a + Nb \implies p|(a + Nb)(a - Nb) =$$
$$a^2 - N^2b^2 \equiv a^2 + b^2 \pmod{p}$$

$$\begin{array}{r} k_1 + Nm_1 \\ -\ k_2 + Nm_2 \\ \hline a + Nb \end{array} \qquad \begin{array}{l} a = k_1 - k_2 \\ b = m_1 - m_2 \end{array} \qquad \begin{array}{l} |a| < \sqrt{p} \\ |b| < \sqrt{p} \end{array}$$

$$p|a + Nb \implies p|(a + Nb)(a - Nb) =$$
$$a^2 - N^2b^2 \equiv a^2 + b^2 \pmod{p} \implies p|a^2 + b^2$$

$$\begin{array}{r} k_1 + Nm_1 \\ -\ k_2 + Nm_2 \\ \hline a + Nb \end{array} \qquad \begin{array}{l} a = k_1 - k_2 \\ b = m_1 - m_2 \end{array} \qquad \begin{array}{l} |a| < \sqrt{p} \\ |b| < \sqrt{p} \end{array}$$

$$p|a + Nb \implies p|(a + Nb)(a - Nb) =$$

$$a^2 - N^2b^2 \equiv a^2 + b^2 \pmod{p} \implies p|a^2 + b^2$$

$$0 < a^2 + b^2$$

$$\begin{array}{r} k_1 + Nm_1 \\ -\ k_2 + Nm_2 \\ \hline a + Nb \end{array} \qquad \begin{array}{l} a = k_1 - k_2 \\ b = m_1 - m_2 \end{array} \qquad \begin{array}{l} |a| < \sqrt{p} \\ |b| < \sqrt{p} \end{array}$$

$$p|a + Nb \implies p|(a + Nb)(a - Nb) =$$

$$a^2 - N^2b^2 \equiv a^2 + b^2 \pmod{p} \implies p|a^2 + b^2$$

$$0 < a^2 + b^2 < 2p$$

$$\begin{array}{r} k_1 + Nm_1 \\ -\ k_2 + Nm_2 \\ \hline a + Nb \end{array} \qquad \begin{array}{l} a = k_1 - k_2 \\ b = m_1 - m_2 \end{array} \qquad \begin{array}{l} |a| < \sqrt{p} \\ |b| < \sqrt{p} \end{array}$$

$$p|a + Nb \implies p|(a + Nb)(a - Nb) =$$
$$a^2 - N^2b^2 \equiv a^2 + b^2 \pmod{p} \implies p|a^2 + b^2$$

$$0 < a^2 + b^2 < 2p \implies p = a^2 + b^2 \qquad \square$$

Zagier bizonyítása

$$x^2 + 4yz = p = 4n + 1$$

Zagier bizonyítása

$$x^2 + 4yz = p = 4n + 1$$

Fermat–Euler-tétel $\Leftrightarrow$ az egyenletnek van olyan (x, y, z) megoldása, ahol $y = z$ $(x, y, z \in \mathbb{Z}^+)$

Zagier bizonyítása

$$x^2 + 4yz = p = 4n + 1$$

Fermat–Euler-tétel $\Leftrightarrow$ az egyenletnek van olyan (x, y, z) megoldása, ahol $y = z$ $(x, y, z \in \mathbb{Z}^+)$

- S a megoldások halmaza

Zagier bizonyítása

$$x^2 + 4yz = p = 4n + 1$$

Fermat–Euler-tétel $\Leftrightarrow$ az egyenletnek van olyan (x, y, z) megoldása, ahol $y = z$ $(x, y, z \in \mathbb{Z}^+)$

- S a megoldások halmaza
- $x, y, z < p \implies |S|$ véges

Zagier bizonyítása

$$x^2 + 4yz = p = 4n + 1$$

Fermat–Euler-tétel $\Leftrightarrow$ az egyenletnek van olyan (x, y, z) megoldása, ahol $y = z$ $(x, y, z \in \mathbb{Z}^+)$

- S a megoldások halmaza
- $x, y, z < p \implies |S|$ véges
- Ha $y \neq z$: $(x, y, z) \leftrightarrow (x, z, y)$

Zagier bizonyítása

$$x^2 + 4yz = p = 4n + 1$$

Fermat–Euler-tétel $\Leftrightarrow$ az egyenletnek van olyan (x, y, z) megoldása, ahol $y = z$ $(x, y, z \in \mathbb{Z}^+)$

- S a megoldások halmaza
- $x, y, z < p \implies |S|$ véges
- Ha $y \neq z$: $(x, y, z) \leftrightarrow (x, z, y)$
- $|S|$ páratlan $\implies$ Fermat–Euler-tétel

A bizonyítás eszköze: involúció

A bizonyítás eszköze: involúció

Definíció

Az $F : H \to H$ függvényt involúciónak nevezzük, ha

$$\forall x \in H : \quad F(F(x)) = x.$$

A bizonyítás eszköze: involúció

Definíció

Az $F : H \to H$ függvényt involúciónak nevezzük, ha

$$\forall x \in H : \quad F(F(x)) = x.$$

Tulajdonság

Bármely involúció nemfix pontjainak száma páros.

A bizonyítás eszköze: involúció

Definíció

Az $F : H \to H$ függvényt involúciónak nevezzük, ha

$$\forall x \in H : \quad F(F(x)) = x.$$

Tulajdonság

Bármely involúció nemfix pontjainak száma páros.

$\Longrightarrow$ *Ha F-nek páratlan sok fixpontja van és H véges, akkor $|H|$ páratlan.*

Megfelelő involúció?

Megfelelő involúció?

$$B(x, y, z) = (x', y', z')$$

x'	y'	z'	Feltétel
$x+2z$	z	$y-x-z$	$x<y-z$
$2y-x$	y	$x-y+z$	$y-z\leq x\leq 2y$
$x-2y$	$x-y+z$	y	$2y<x$

Megfelelő involúció?

$$B(x,y,z)=(x',y',z')$$

x'	y'	z'	Feltétel
$x+2z$	z	$y-x-z$	$x < y-z$
$2y-x$	y	$x-y+z$	$y-z \leq x \leq 2y$
$x-2y$	$x-y+z$	y	$2y < x$

Megfelelő involúció?

$$B(x,y,z) = (x',y',z')$$

S-ről S-re képez?

x'	y'	z'	Feltétel
$x+2z$	z	$y-x-z$	$x<y-z$
$2y-x$	y	$x-y+z$	$y-z\leq x\leq 2y$
$x-2y$	$x-y+z$	y	$2y<x$

Megfelelő involúció?

$$B(x,y,z)=(x',y',z')$$

S-ről S-re képez? Involúció?

x'	y'	z'	Feltétel
$x+2z$	z	$y-x-z$	$x<y-z$
$2y-x$	y	$x-y+z$	$y-z\leq x\leq 2y$
$x-2y$	$x-y+z$	y	$2y<x$

B S-ről S-re képez $(x<y-z)$

x'	y'	z'	Feltétel
$x+2z$	z	$y-x-z$	$x<y-z$
$2y-x$	y	$x-y+z$	$y-z\leq x\leq 2y$
$x-2y$	$x-y+z$	y	$2y<x$

B S-ről S-re képez $(x<y-z)$

$$x'^2+4y'z'=(x+2z)^2+4z\cdot(y-x-z)$$

x'	y'	z'	Feltétel
$x+2z$	z	$y-x-z$	$x<y-z$
$2y-x$	y	$x-y+z$	$y-z\leq x\leq 2y$
$x-2y$	$x-y+z$	y	$2y<x$

B S-ről S-re képez $(x<y-z)$

$$\begin{aligned} x'^2+4y'z' &= (x+2z)^2+4z\cdot(y-x-z) \\ &= x^2+4xz+4z^2+4yz- \\ &\quad -4xz-4z^2 \end{aligned}$$

x'	y'	z'	Feltétel
$x+2z$	z	$y-x-z$	$x<y-z$
$2y-x$	y	$x-y+z$	$y-z\leq x\leq 2y$
$x-2y$	$x-y+z$	y	$2y<x$

B S-ről S-re képez $(x<y-z)$

$$\begin{aligned} x'^2+4y'z' &= (x+2z)^2+4z\cdot(y-x-z) \\ &= x^2+4xz+4z^2+4yz- \\ &\quad -4xz-4z^2=x^2+4yz \end{aligned}$$

x'	y'	z'	Feltétel
$x+2z$	z	$y-x-z$	$x<y-z$
$2y-x$	y	$x-y+z$	$y-z\leq x\leq 2y$
$x-2y$	$x-y+z$	y	$2y<x$

B involúció $(x<y-z)$

x'	y'	z'	Feltétel
$x+2z$	z	$y-x-z$	$x<y-z$
$2y-x$	y	$x-y+z$	$y-z\leq x\leq 2y$
$x-2y$	$x-y+z$	y	$2y<x$

B involúció $(x<y-z)$

$$x' = x+2z$$
$$y' = z$$
$$z' = y-x-z$$

x'	y'	z'	Feltétel
$x+2z$	z	$y-x-z$	$x<y-z$
$2y-x$	y	$x-y+z$	$y-z\le x\le 2y$
$x-2y$	$x-y+z$	y	$2y<x$

B involúció $(x<y-z)$ $\qquad$ $x'>2y'$

$$x' = x+2z$$
$$y' = z$$
$$z' = y-x-z$$

x'	y'	z'	Feltétel
$x+2z$	z	$y-x-z$	$x < y-z$
$2y-x$	y	$x-y+z$	$y-z \le x \le 2y$
$x-2y$	$x-y+z$	y	$2y < x$

B involúció $(x < y-z)$ $\qquad$ $x' > 2y'$

$$x' = x+2z \qquad x'' = x'-2y' = x$$
$$y' = z$$
$$z' = y-x-z$$

x'	y'	z'	Feltétel
$x+2z$	z	$y-x-z$	$x<y-z$
$2y-x$	y	$x-y+z$	$y-z\le x\le 2y$
$x-2y$	$x-y+z$	y	$2y<x$

B involúció $(x<y-z)$ $\qquad$ $x'>2y'$

$$x'=x+2z \qquad x''=x'-2y'=x$$
$$y'=z \qquad y''=x'-y'+z'=y$$
$$z'=y-x-z$$

x'	y'	z'	Feltétel
$x+2z$	z	$y-x-z$	$x < y-z$
$2y-x$	y	$x-y+z$	$y-z \le x \le 2y$
$x-2y$	$x-y+z$	y	$2y < x$

B involúció $(x < y-z)$ $\qquad$ $x' > 2y'$

$$x' = x+2z \qquad x'' = x'-2y' = x$$
$$y' = z \qquad y'' = x'-y'+z' = y$$
$$z' = y-x-z \qquad z'' = y' = z$$

x'	y'	z'	Feltétel
$x+2z$	z	$y-x-z$	$x < y-z$
$2y-x$	y	$x-y+z$	$y-z \leq x \leq 2y$
$x-2y$	$x-y+z$	y	$2y < x$

B fixpontjai?

x'	y'	z'	Feltétel
$x+2z$	z	$y-x-z$	$x<y-z$
$2y-x$	y	$x-y+z$	$y-z\leq x\leq 2y$
$x-2y$	$x-y+z$	y	$2y<x$

B fixpontjai?

$$x=x'=2y-x$$

x'	y'	z'	Feltétel
$x+2z$	z	$y-x-z$	$x<y-z$
$2y-x$	y	$x-y+z$	$y-z\leq x\leq 2y$
$x-2y$	$x-y+z$	y	$2y<x$

B fixpontjai?

$$x=x'=2y-x \implies x=y$$

x'	y'	z'	Feltétel
$x+2z$	z	$y-x-z$	$x<y-z$
$2y-x$	y	$x-y+z$	$y-z\leq x\leq 2y$
$x-2y$	$x-y+z$	y	$2y<x$

B fixpontjai?

$$x=x'=2y-x \implies x=y$$

$$B(x,x,z)=(x,x,z)$$

x'	y'	z'	Feltétel
$x+2z$	z	$y-x-z$	$x<y-z$
$2y-x$	y	$x-y+z$	$y-z\leq x\leq 2y$
$x-2y$	$x-y+z$	y	$2y<x$

B fixpontjai?

$$x=x'=2y-x \implies x=y$$

$$B(x,x,z)=(x,x,z)$$

$$x^2+4xz=p$$

x'	y'	z'	Feltétel
$x+2z$	z	$y-x-z$	$x<y-z$
$2y-x$	y	$x-y+z$	$y-z\le x\le 2y$
$x-2y$	$x-y+z$	y	$2y<x$

B fixpontjai?

$$x = x' = 2y - x \implies x = y$$

$$B(x,x,z) = (x,x,z)$$

$$x^2 + 4xz = p$$

$p = 4n+1$, prím $\implies x = 1$

x'	y'	z'	Feltétel
$x+2z$	z	$y-x-z$	$x<y-z$
$2y-x$	y	$x-y+z$	$y-z\leq x\leq 2y$
$x-2y$	$x-y+z$	y	$2y<x$

B fixpontjai?

$$x = x' = 2y - x \implies x = y$$

$$B(x, x, z) = (x, x, z)$$

$$x^2 + 4xz = p$$

$p = 4n + 1$, prím $\implies x = 1,\ z = n$

Egyetlen fixpont: $(1, 1, n)$

Egyetlen fixpont: $(1, 1, n)$

$\Longrightarrow$ $|S|$ páratlan

Egyetlen fixpont: $(1, 1, n)$

$\Longrightarrow$ $|S|$ páratlan

$\Longrightarrow$ $x^2 + 4yz = p$-nek van (x, z, z) megoldása

Egyetlen fixpont: $(1, 1, n)$

$\Longrightarrow$ $|S|$ páratlan

$\Longrightarrow$ $x^2 + 4yz = p$-nek van (x, z, z) megoldása

$\Longrightarrow$ $x^2 + (2z)^2 = p$: Fermat–Euler-tétel $\square$

Minkowski bizonyítása

Tétel

Legyenek a, b és c egészek úgy, hogy $a > 0$ és $ac - b^2 = 1$ teljesüljön. Ekkor az

$$ax^2 + 2bxy + cy^2 = 1$$

egyenletnek van $(x; y)$ megoldása ($x, y \in \mathbb{Z}$).

Koszinusztétel-jelleg

Minkowski bizonyítása

Tétel

Legyenek a, b és c egészek úgy, hogy $a > 0$ és $ac - b^2 = 1$ teljesüljön. Ekkor az

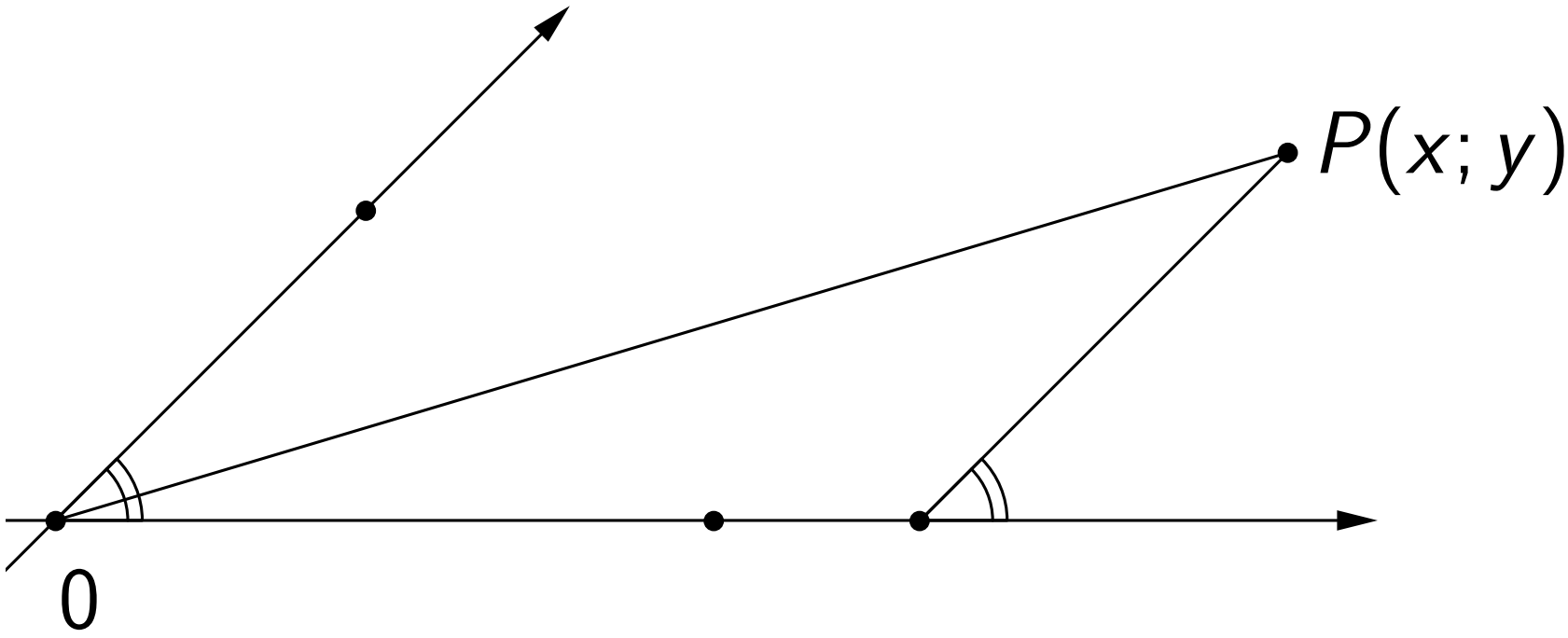
$$ax^2 + 2bxy + cy^2 = 1$$

egyenletnek van $(x; y)$ megoldása ($x, y \in \mathbb{Z}$).

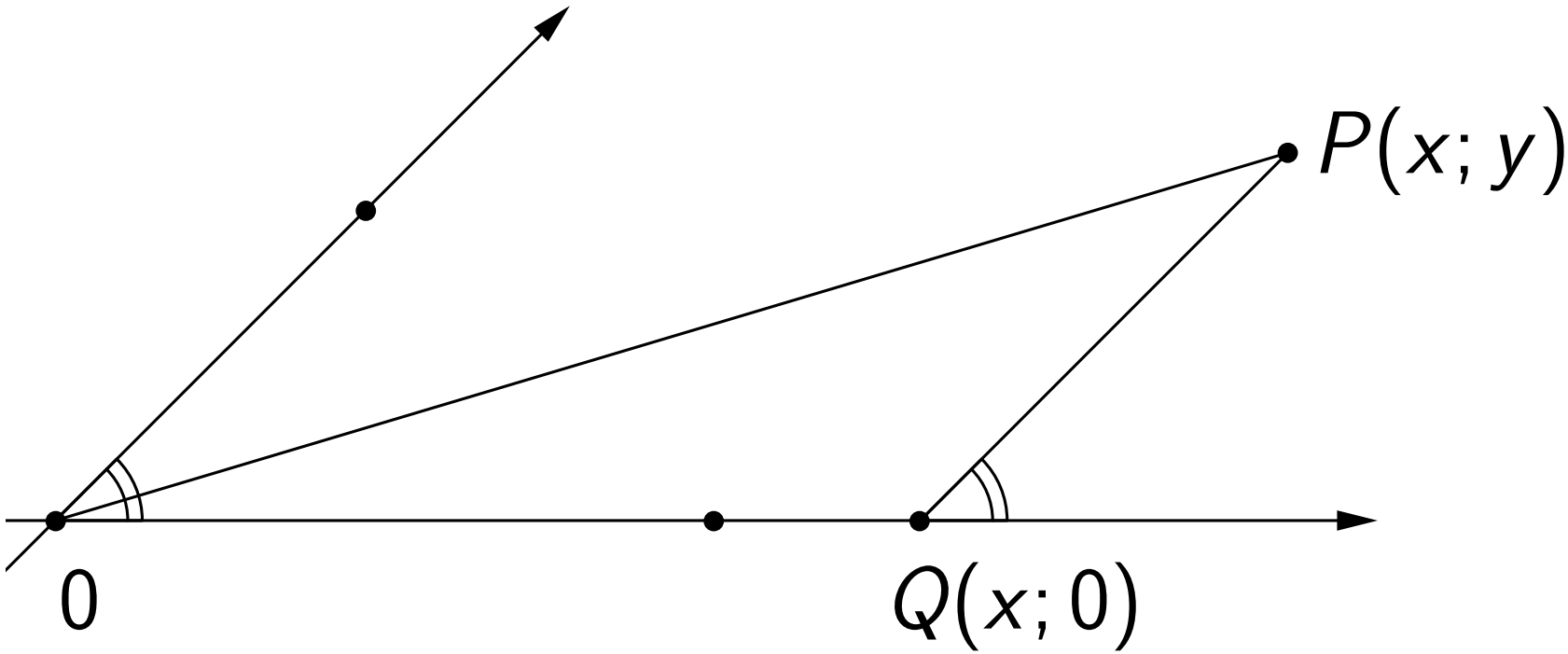
Koszinusztétel-jelleg $\rightarrow$ megfelelő háromszög?

$$ax^2 + 2bxy + cy^2 = 1$$

$$ax^2 + 2bxy + cy^2 = 1$$

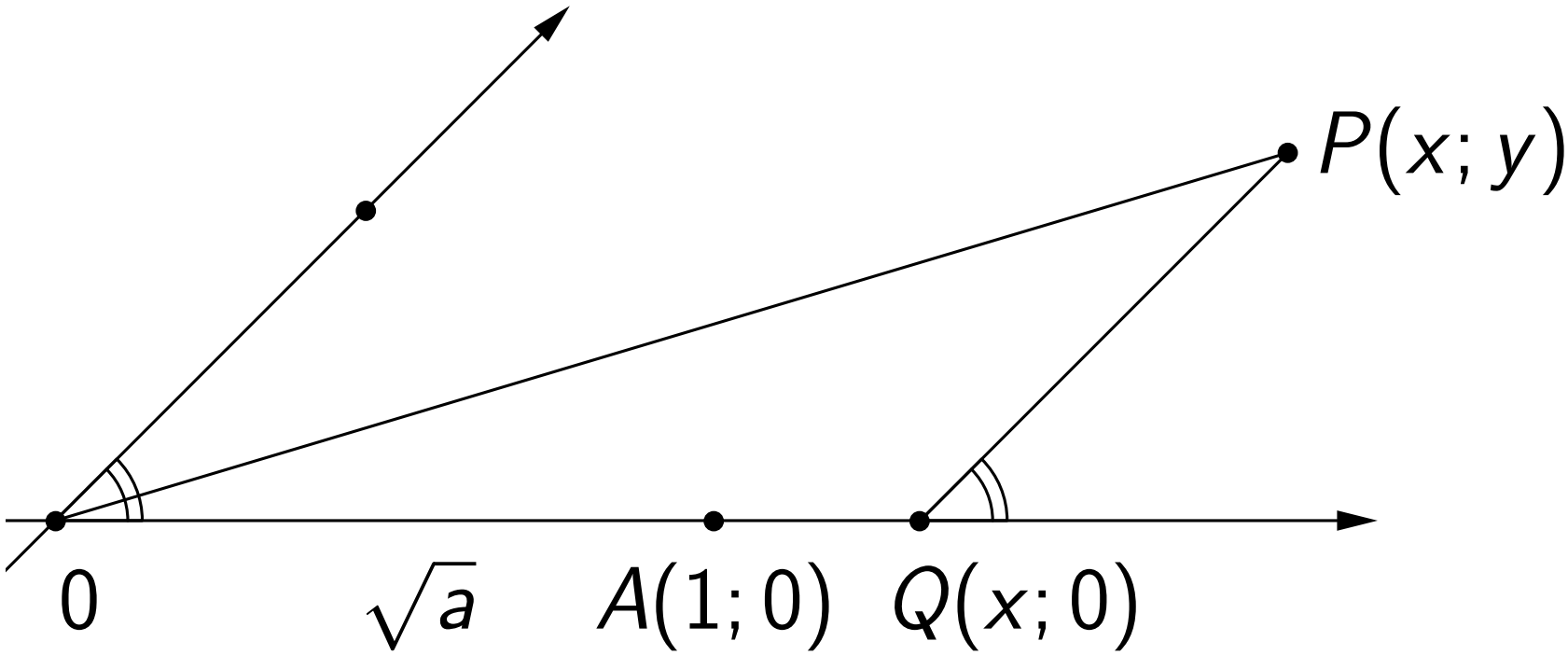


$$ax^2 + 2bxy + cy^2 = 1$$



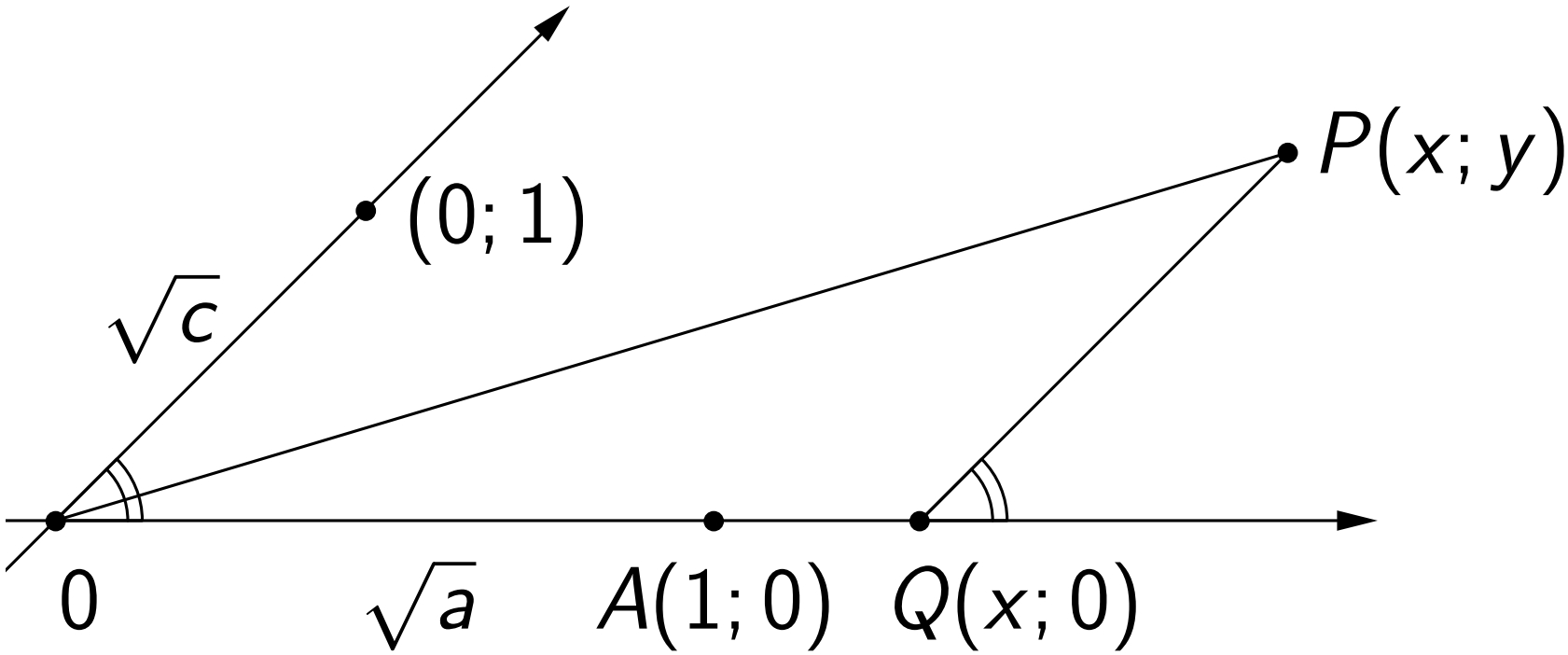
$$\begin{aligned} OP^2 &= OQ^2 - 2OQ \cdot QP \cos(Q\angle) + QP^2 \\ &= ax^2 + 2bxy + cy^2 \end{aligned}$$

$$ax^2 + 2bxy + cy^2 = 1$$



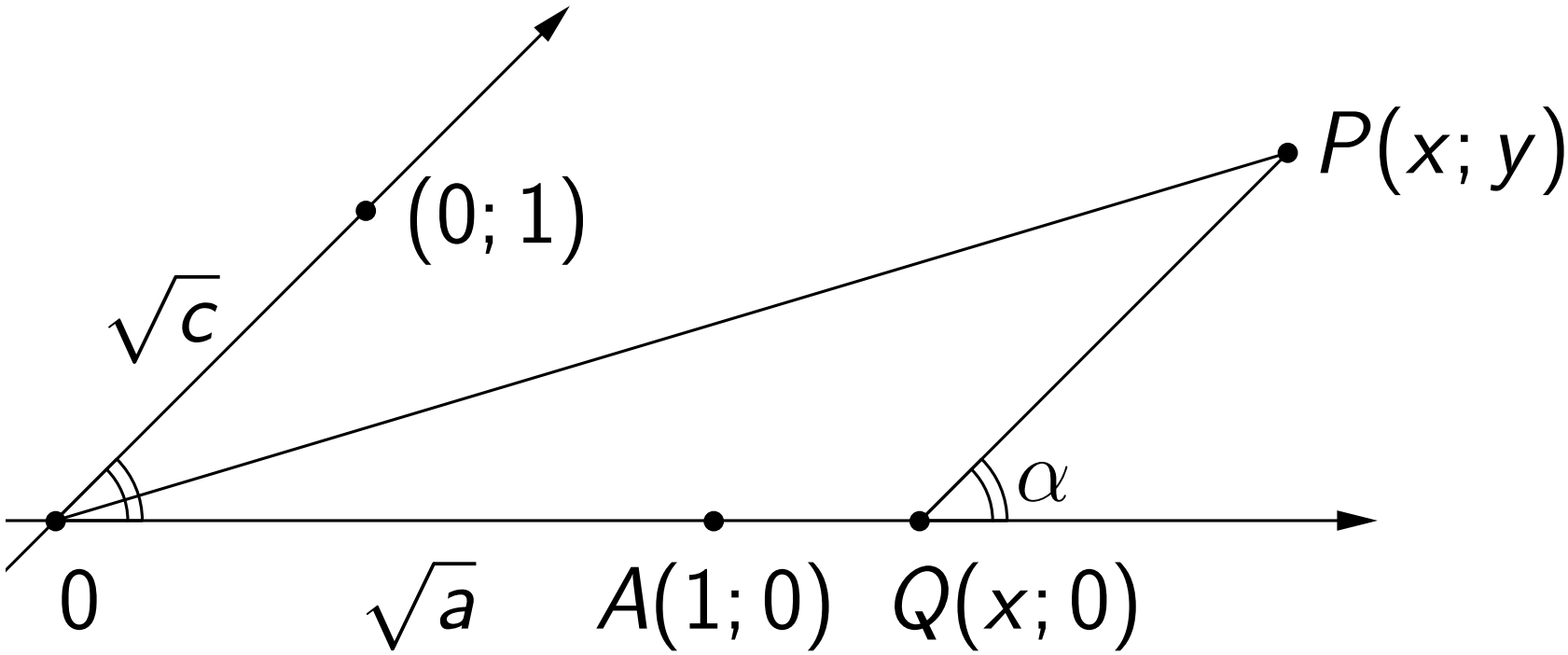
$$\begin{aligned} OP^2 &= OQ^2 - 2OQ \cdot QP \cos(Q\angle) + QP^2 \\ &= ax^2 + 2bxy + cy^2 \end{aligned}$$

$$ax^2 + 2bxy + cy^2 = 1$$



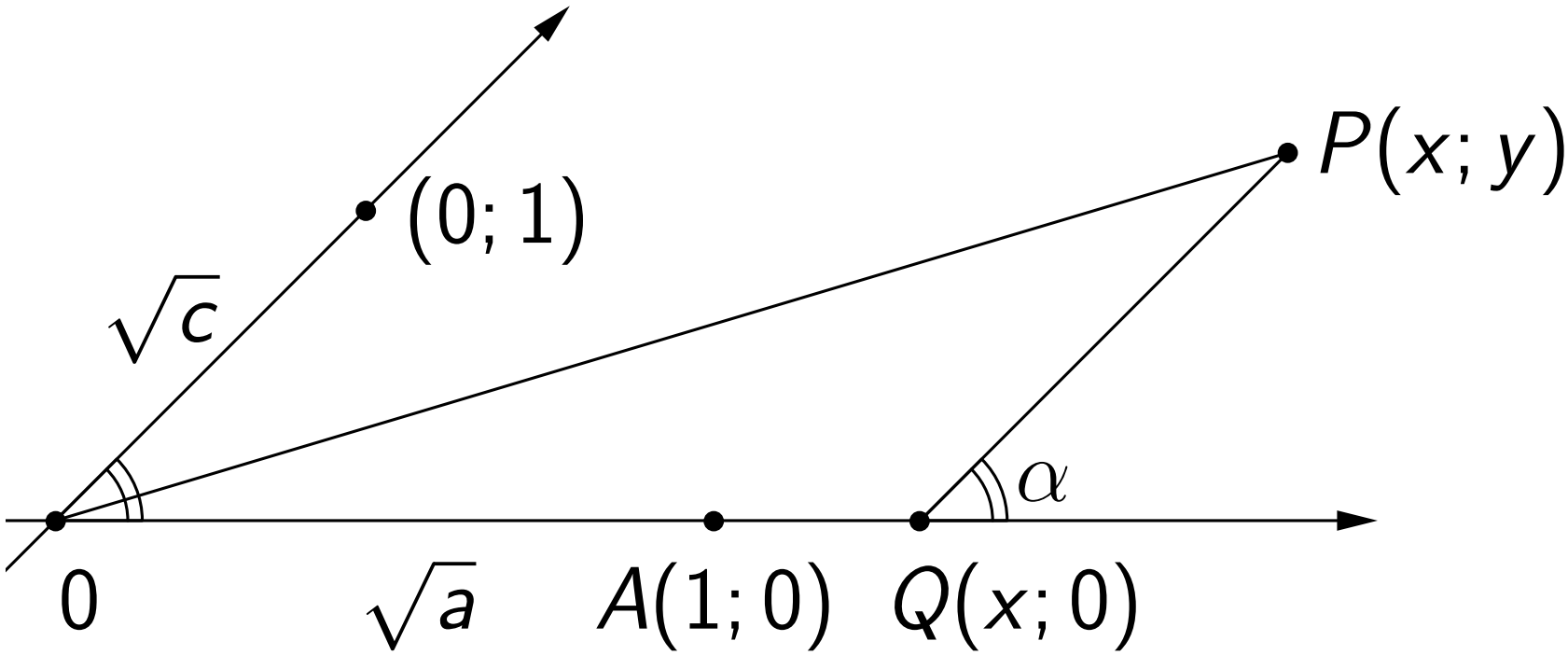
$$\begin{aligned} OP^2 &= OQ^2 - 2OQ \cdot QP \cos(Q\angle) + QP^2 \\ &= ax^2 + 2bxy + cy^2 \end{aligned}$$

$$ax^2 + 2bxy + cy^2 = 1$$



$$\begin{aligned} OP^2 &= OQ^2 - 2OQ \cdot QP \cos(Q\angle) + QP^2 \\ &= ax^2 + 2bxy + cy^2 \end{aligned}$$

$$ax^2 + 2bxy + cy^2 = 1$$



$$\cos\alpha = b/\sqrt{ac}$$

$$\begin{aligned} OP^2 &= OQ^2 - 2OQ \cdot QP \cos(Q\angle) + QP^2 \\ &= ax^2 + 2bxy + cy^2 \end{aligned}$$

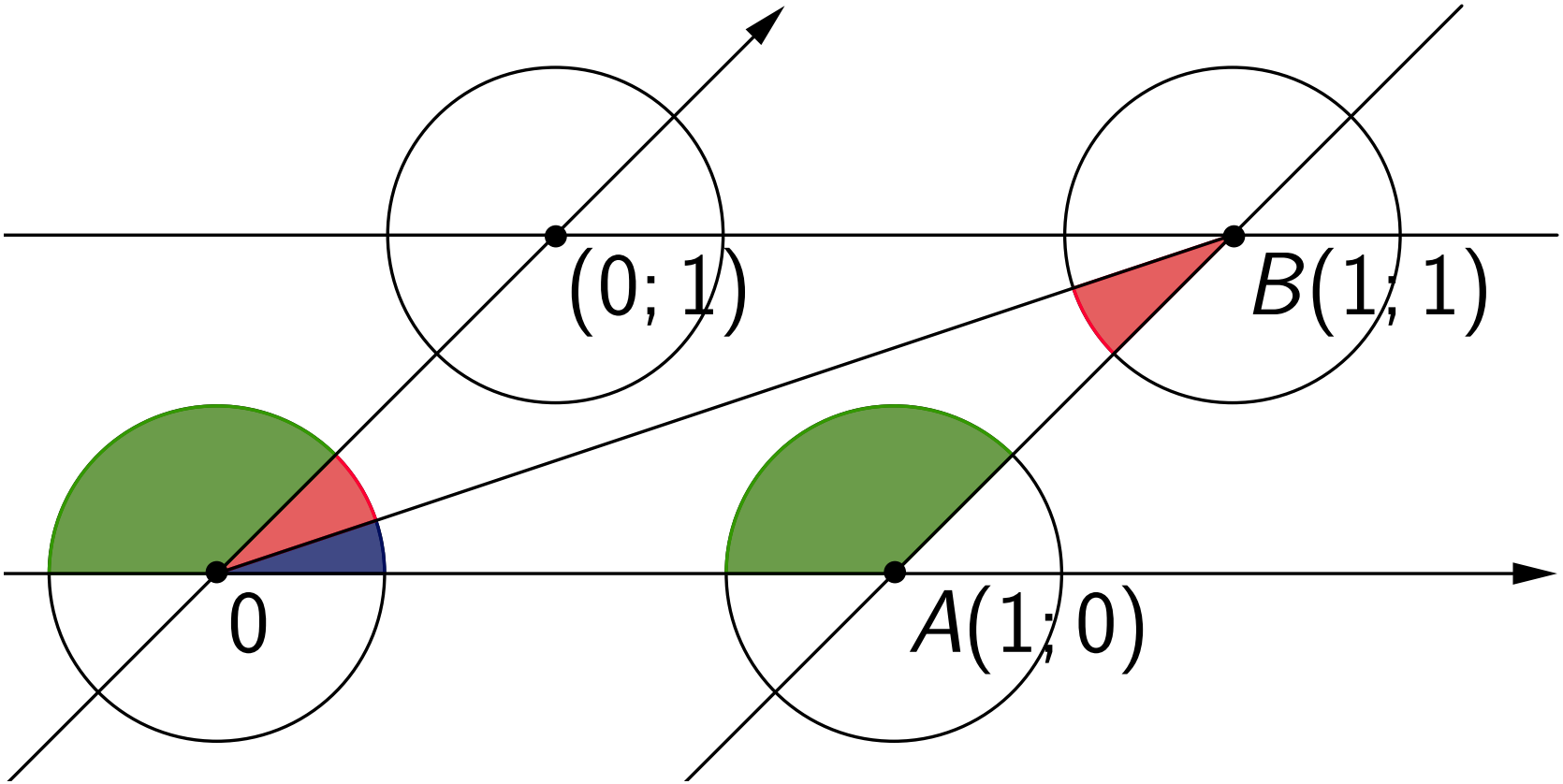
- $ax^2 + 2bxy + cy^2 = 1$ egész megoldása $\leftrightarrow$ $(0;0)$-tól 1 távolságra lévő rácspont

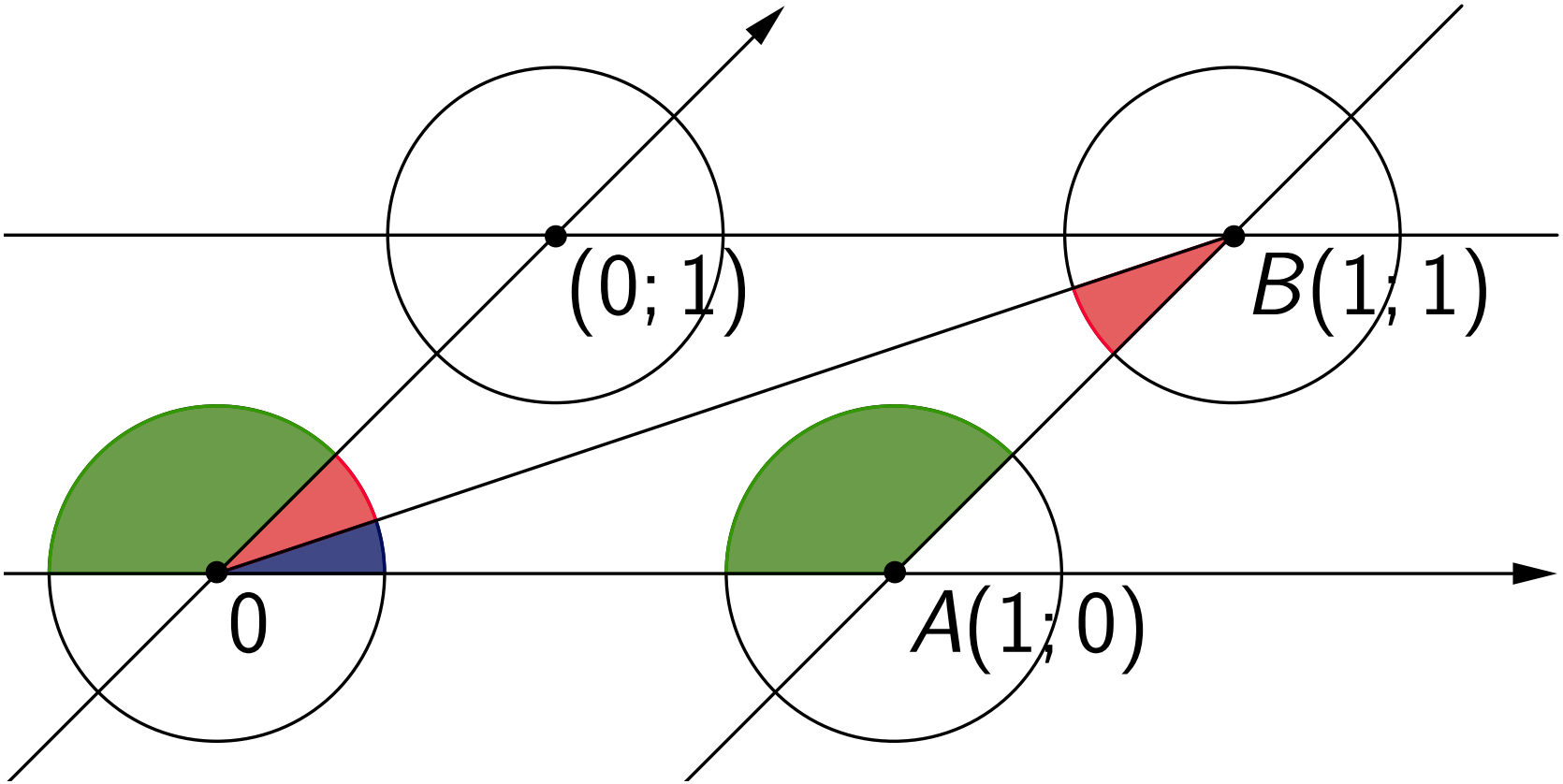
- $ax^2 + 2bxy + cy^2 = 1$ egész megoldása $\leftrightarrow$ $(0;0)$-tól 1 távolságra lévő rácspont
- d a minimális távolság két rácspont között

- $ax^2 + 2bxy + cy^2 = 1$ egész megoldása $\leftrightarrow$ $(0;0)$-tól 1 távolságra lévő rácspont
- d a minimális távolság két rácspont között
- (m, n) az origótól d távolságban lévő rácspont

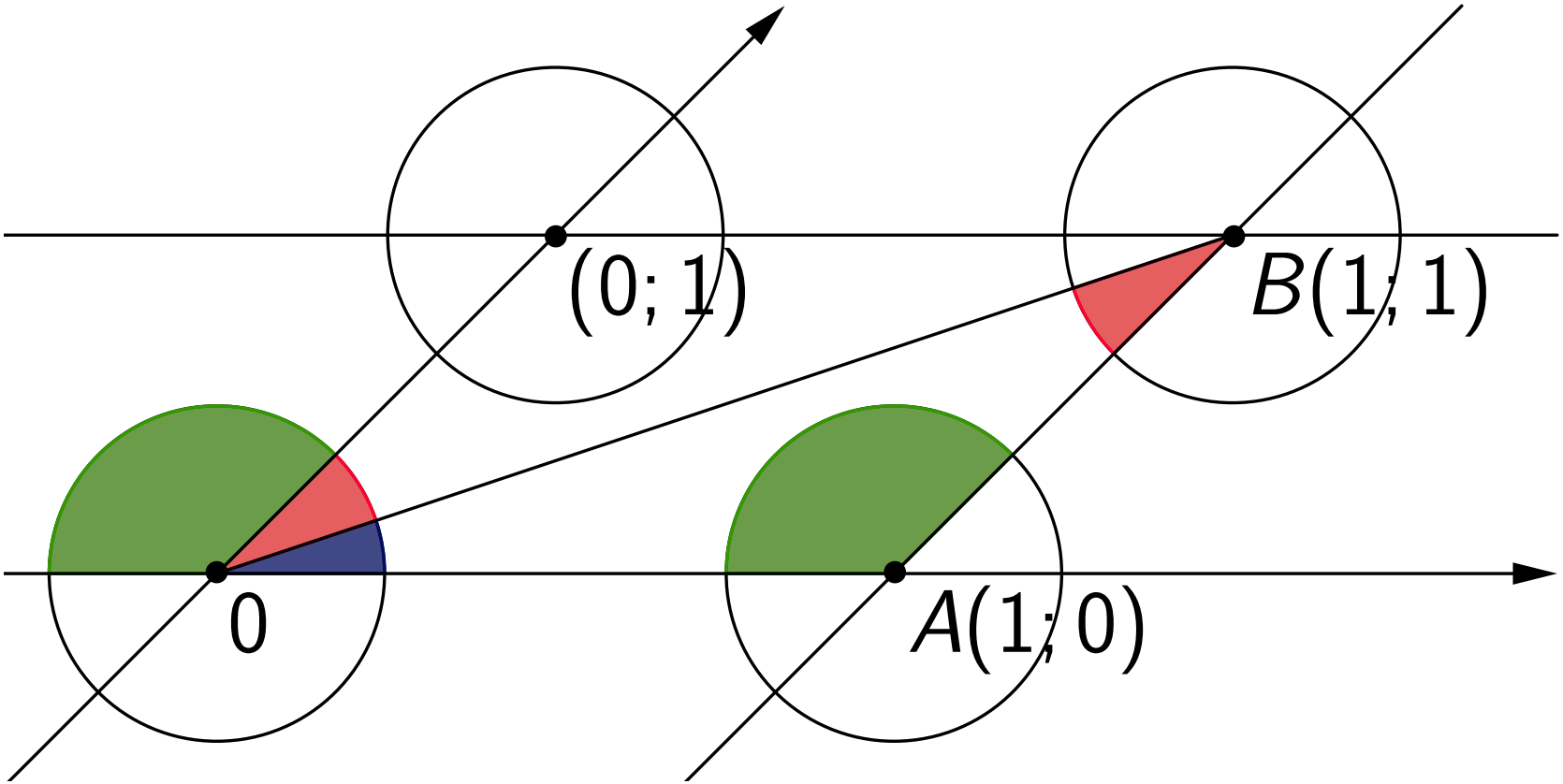
- $ax^2 + 2bxy + cy^2 = 1$ egész megoldása $\leftrightarrow$ $(0;0)$-tól 1 távolságra lévő rácspont
- d a minimális távolság két rácspont között
- (m, n) az origótól d távolságban lévő rácspont
- rácspont középpontú, $\frac{d}{2}$ sugarú köröknek nincs közös belső pontja

- $ax^2 + 2bxy + cy^2 = 1$ egész megoldása $\leftrightarrow$ $(0;0)$-tól 1 távolságra lévő rácspont
- d a minimális távolság két rácspont között
- (m, n) az origótól d távolságban lévő rácspont
- rácspont középpontú, $\frac{d}{2}$ sugarú köröknek nincs közös belső pontja
  Indirekten: $AB < AC + CB < \frac{d}{2} + \frac{d}{2} = d$
  $\rightarrow$ ellentmondás!

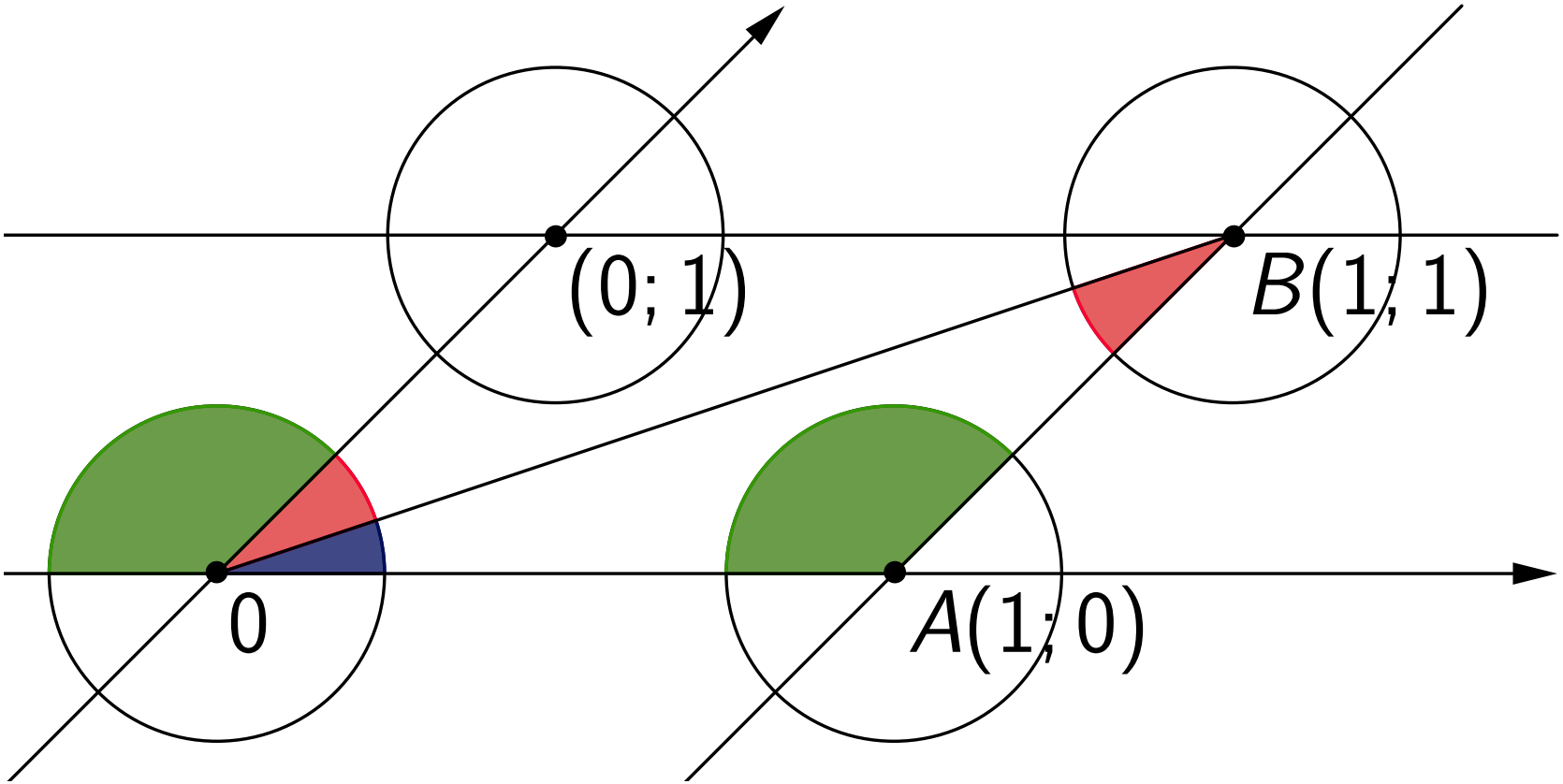

(0; 1)
B(1; 1)
0
A(1; 0)



$$\frac{d^2}{8}\pi$$



$$\frac{d^2}{8}\pi <$$



$$\frac{d^2}{8}\pi < \frac{1}{2} \cdot OA \cdot AB \cdot \sin(A\angle)$$

$$\frac{1}{2} \cdot OA \cdot AB \cdot \sin(A\angle) = \frac{1}{2}\sqrt{a}\sqrt{c}\sin(A\angle)$$

$$\frac{1}{2} \cdot OA \cdot AB \cdot \sin(A\angle) = \frac{1}{2}\sqrt{a}\sqrt{c}\sin(A\angle)$$
$$= \frac{1}{2}\sqrt{ac \cdot (1 - \cos^2 \alpha)}$$

$$\begin{aligned}\frac{1}{2}\cdot OA\cdot AB\cdot \sin(A\angle) &= \frac{1}{2}\sqrt{a}\sqrt{c}\sin(A\angle)\\ &= \frac{1}{2}\sqrt{ac\cdot(1-\cos^2\alpha)}\\ &= \frac{1}{2}\sqrt{ac-b^2}\end{aligned}$$

$$\frac{1}{2} \cdot OA \cdot AB \cdot \sin(A\angle) = \frac{1}{2}\sqrt{a}\sqrt{c}\sin(A\angle)$$
$$= \frac{1}{2}\sqrt{ac \cdot (1 - \cos^2 \alpha)}$$
$$= \frac{1}{2}\sqrt{ac - b^2} = \frac{1}{2}$$

$$\frac{d^2}{8}\pi < \frac{1}{2}$$

$$\frac{1}{2} \cdot OA \cdot AB \cdot \sin(A\angle) = \frac{1}{2}\sqrt{a}\sqrt{c}\sin(A\angle)$$
$$= \frac{1}{2}\sqrt{ac \cdot (1 - \cos^2 \alpha)}$$
$$= \frac{1}{2}\sqrt{ac - b^2} = \frac{1}{2}$$

$$\frac{d^2}{8}\pi < \frac{1}{2} \implies d^2 < \frac{4}{\pi} < 2$$

$$\frac{1}{2} \cdot OA \cdot AB \cdot \sin(A\angle) = \frac{1}{2}\sqrt{a}\sqrt{c}\sin(A\angle)$$
$$= \frac{1}{2}\sqrt{ac \cdot (1 - \cos^2 \alpha)}$$
$$= \frac{1}{2}\sqrt{ac - b^2} = \frac{1}{2}$$

$$\frac{d^2}{8}\pi < \frac{1}{2} \implies d^2 < \frac{4}{\pi} < 2$$

$$d^2 = am^2 + 2bmn + cn^2 \implies d = 1$$

Wilson-tétel: $p|N^2+1$, ahol $N=\left(\frac{p-1}{2}\right)!$

Wilson-tétel: $p|N^2+1$, ahol $N=\left(\frac{p-1}{2}\right)!$

Minkowski-tételben $a=p$, $b=N$, $c=\frac{b^2+1}{a}$

Wilson-tétel: $p|N^2+1$, ahol $N=\left(\frac{p-1}{2}\right)!$

Minkowski-tételben $a=p$, $b=N$, $c=\frac{b^2+1}{a}$

$$1=am^2+2bmn+cn^2$$

Wilson-tétel: $p|N^2+1$, ahol $N=\left(\frac{p-1}{2}\right)!$

Minkowski-tételben $a=p$, $b=N$, $c=\frac{b^2+1}{a}$

$$1 = am^2 + 2bmn + cn^2$$

$$p = a^2m^2 + 2abmn + \left(b^2+1\right)n^2$$

Wilson-tétel: $p|N^2+1$, ahol $N=\left(\frac{p-1}{2}\right)!$

Minkowski-tételben $a=p$, $b=N$, $c=\frac{b^2+1}{a}$

$$\begin{aligned} 1 &= am^2+2bmn+cn^2 \\ p &= a^2m^2+2abmn+\left(b^2+1\right)n^2 \\ &= (am+bn)^2+n^2 \end{aligned}$$

A felbontás egyértelműségének bizonyítása

Indirekt feltevés

Legyen $p = 4n + 1$ prímszám. Tegyük fel, hogy

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

ahol $a > b > 0$ és $c > d > 0$; $a \neq c$ és $b \neq d$.

Vizsgáljuk $(ad + bc)(ad - bc)$-t!

Vizsgáljuk $(ad + bc)(ad - bc)$-t!

$$\begin{aligned}(ad + bc)(ad - bc) &= a^2d^2 - b^2c^2 \\ &= \left(p - b^2\right) d^2 - b^2 \left(p - d^2\right)\end{aligned}$$

Vizsgáljuk $(ad + bc)(ad - bc)$-t!

$$\begin{aligned}(ad + bc)(ad - bc) &= a^2d^2 - b^2c^2 \\ &= \left(p - b^2\right) d^2 - b^2 \left(p - d^2\right) \\ &= pd^2 - b^2d^2 - pb^2 + b^2d^2\end{aligned}$$

Vizsgáljuk $(ad + bc)(ad - bc)$-t!

$$\begin{aligned}(ad + bc)(ad - bc) &= a^2d^2 - b^2c^2 \\ &= \left(p - b^2\right) d^2 - b^2 \left(p - d^2\right) \\ &= pd^2 - b^2d^2 - pb^2 + b^2d^2 \\ &= p\left(d^2 - b^2\right)\end{aligned}$$

Vizsgáljuk $(ad + bc)(ad - bc)$-t!

$$\begin{aligned}(ad + bc)(ad - bc) &= a^2d^2 - b^2c^2 \\ &= \left(p - b^2\right) d^2 - b^2 \left(p - d^2\right) \\ &= pd^2 - b^2d^2 - pb^2 + b^2d^2 \\ &= p\left(d^2 - b^2\right) \\ &\equiv 0 \pmod{p}\end{aligned}$$

Vizsgáljuk $(ad + bc)(ad - bc)$-t!

$$\begin{aligned}(ad + bc)(ad - bc) &= a^2d^2 - b^2c^2 \\ &= \left(p - b^2\right) d^2 - b^2 \left(p - d^2\right) \\ &= pd^2 - b^2d^2 - pb^2 + b^2d^2 \\ &= p\left(d^2 - b^2\right) \\ &\equiv 0 \pmod{p}\end{aligned}$$

$$\implies p|(ad + bc) \vee p|(ad - bc)$$

Tegyük fel, hogy $p|(ad + bc)$.

Tegyük fel, hogy $p|(ad + bc)$.

- $a^2, b^2, c^2, d^2 < p \implies a, b, c, d < \sqrt{p}$

Tegyük fel, hogy $p|(ad + bc)$.

- $a^2, b^2, c^2, d^2 < p \implies a, b, c, d < \sqrt{p}$
- $0 < ad + bc < 2p$

Tegyük fel, hogy $p|(ad+bc)$.

- $a^2, b^2, c^2, d^2 < p \implies a, b, c, d < \sqrt{p}$
- $0 < ad + bc < 2p \implies ad + bc = p$

Tegyük fel, hogy $p|(ad+bc)$.

- $a^2, b^2, c^2, d^2 < p \implies a, b, c, d < \sqrt{p}$
- $0 < ad + bc < 2p \implies ad + bc = p$

$$p^2 = \left(a^2 + b^2\right)\left(c^2 + d^2\right)$$

Tegyük fel, hogy $p|(ad+bc)$.

- $a^2, b^2, c^2, d^2 < p \implies a, b, c, d < \sqrt{p}$
- $0 < ad + bc < 2p \implies ad + bc = p$

$$\begin{aligned} p^2 &= \left(a^2+b^2\right)\left(c^2+d^2\right) \\ &= (ad+bc)^2 + (ac-bd)^2 \end{aligned}$$

Tegyük fel, hogy $p|(ad+bc)$.

- $a^2, b^2, c^2, d^2 < p \implies a, b, c, d < \sqrt{p}$
- $0 < ad + bc < 2p \implies ad + bc = p$

$$\begin{aligned} p^2 &= \left(a^2+b^2\right)\left(c^2+d^2\right) \\ &= (ad+bc)^2 + (ac-bd)^2 \\ &= p^2 + (ac-bd)^2 \end{aligned}$$

Tegyük fel, hogy $p|(ad+bc)$.

- $a^2, b^2, c^2, d^2 < p \implies a, b, c, d < \sqrt{p}$
- $0 < ad + bc < 2p \implies ad + bc = p$

$$\begin{aligned} p^2 &= \left(a^2+b^2\right)\left(c^2+d^2\right) \\ &= (ad+bc)^2 + (ac-bd)^2 \\ &= p^2 + (ac-bd)^2 \end{aligned}$$

- $ac - bd = 0$

Tegyük fel, hogy $p|(ad+bc)$.

- $a^2, b^2, c^2, d^2 < p \implies a, b, c, d < \sqrt{p}$
- $0 < ad + bc < 2p \implies ad + bc = p$

$$\begin{aligned} p^2 &= \left(a^2+b^2\right)\left(c^2+d^2\right) \\ &= (ad+bc)^2 + (ac-bd)^2 \\ &= p^2 + (ac-bd)^2 \end{aligned}$$

- $ac - bd = 0$, de $a > b$ és $c > d$, ezért $ac - bd > 0$, ellentmondás!

Ezért $p|(ad - bc)$

- $0 < a, b, c, d < \sqrt{p}$

Ezért $p|(ad - bc)$

- $0 < a, b, c, d < \sqrt{p}$
- $-p < ad - bc < p$

Ezért $p|(ad - bc)$

- $0 < a, b, c, d < \sqrt{p}$
- $-p < ad - bc < p \implies ad - bc = 0$

Ezért $p|(ad - bc)$

- $0 < a, b, c, d < \sqrt{p}$
- $-p < ad - bc < p \implies ad - bc = 0$
- $ad = bc \implies a|bc$

Ezért $p|(ad - bc)$

- $0 < a, b, c, d < \sqrt{p}$
- $-p < ad - bc < p \implies ad - bc = 0$
- $ad = bc \implies a|bc$
- $(a; b) = 1$

Ezért $p|(ad - bc)$

- $0 < a, b, c, d < \sqrt{p}$
- $-p < ad - bc < p \implies ad - bc = 0$
- $ad = bc \implies a|bc$
- $(a; b) = 1 \implies a|c$

Ezért $p|(ad - bc)$

- $0 < a, b, c, d < \sqrt{p}$
- $-p < ad - bc < p \implies ad - bc = 0$
- $ad = bc \implies a|bc$
- $(a; b) = 1 \implies a|c\colon\ c = ka$

Ezért $p|(ad - bc)$

- $0 < a, b, c, d < \sqrt{p}$
- $-p < ad - bc < p \implies ad - bc = 0$
- $ad = bc \implies a|bc$
- $(a; b) = 1 \implies a|c\colon\ c = ka$
- $ad = bka \implies d = bk$

Ezért $p|(ad-bc)$

- $0 < a, b, c, d < \sqrt{p}$
- $-p < ad - bc < p \implies ad - bc = 0$
- $ad = bc \implies a|bc$
- $(a; b) = 1 \implies a|c\colon\ c = ka$
- $ad = bka \implies d = bk$

$$p = c^2 + d^2 = k^2\left(a^2 + b^2\right) = k^2 p$$

Ezért $p|(ad-bc)$

- $0 < a, b, c, d < \sqrt{p}$
- $-p < ad - bc < p \implies ad - bc = 0$
- $ad = bc \implies a|bc$
- $(a; b) = 1 \implies a|c\colon\ c = ka$
- $ad = bka \implies d = bk$

$$p = c^2 + d^2 = k^2\left(a^2 + b^2\right) = k^2 p$$

- $k = 1$: $a = c$ és $b = d$, ellentmondás!

Források

Vlagyimir Tikhomirov

Three paths to Mt. Fermat–Euler

Quantum, 1994. május–június

ProofWiki

Fermat's Christmas Theorem

proofwiki.org

Készítők

Biri Eszter Daniela 11. c
Braun Márton 11. b
Czövek Márton 11. c
Essig Attila 11. b
Forrás Bence 11. c
Gressai Mánuel 11. b
Hu Jia Lin 11. b
Nguyen Uyen My 11. c
Simon Péter 11. c

Segítőtanár: Nemecskó István