

Algebra3, elemző szakirány

ELTE Algebra és Számelmélet Tanszék

Előadó: Kiss Emil
ewkiss@cs.elte.hu

4. előadás

Két négyzetszám különbsége

Freud-Gyarmati: Számelmélet, 7.3.1. Tétel

Egy szám akkor áll elő **két négyzetszám különbségeként**,

Két négyzetszám különbsége

Freud-Gyarmati: Számelmélet, 7.3.1. Tétel

Egy szám akkor áll elő **két négyzetszám különbségeként**, ha 4-gyel osztva **nem 2** maradékot ad.

Két négyzetszám különbsége

Freud-Gyarmati: Számelmélet, 7.3.1. Tétel

Egy szám akkor áll elő **két négyzetszám különbségé**ként, ha 4-gyel osztva **nem 2** maradékot ad.

Bizonyítás

Ötlet: **szorzattá alakítás.**

Két négyzetszám különbsége

Freud-Gyarmati: Számelmélet, 7.3.1. Tétel

Egy szám akkor áll elő **két négyzetszám különbségeként**, ha 4-gyel osztva **nem 2** maradékot ad.

Bizonyítás

Ötlet: **szorzattá alakítás**. $n = x^2 - y^2$

Két négyzetszám különbsége

Freud-Gyarmati: Számelmélet, 7.3.1. Tétel

Egy szám akkor áll elő **két négyzetszám különbségeként**, ha 4-gyel osztva **nem 2** maradékot ad.

Bizonyítás

Ötlet: **szorzattá alakítás**. $n = x^2 - y^2 = (x - y)(x + y)$.

Két négyzetszám különbsége

Freud-Gyarmati: Számelmélet, 7.3.1. Tétel

Egy szám akkor áll elő **két négyzetszám különbségeként**, ha 4-gyel osztva **nem 2** maradékot ad.

Bizonyítás

Ötlet: **szorzattá alakítás**. $n = x^2 - y^2 = (x - y)(x + y)$.

Legyen $x - y = a$ és $x + y = b$.

Két négyzetszám különbsége

Freud-Gyarmati: Számelmélet, 7.3.1. Tétel

Egy szám akkor áll elő **két négyzetszám különbségeként**, ha 4-gyel osztva **nem 2** maradékot ad.

Bizonyítás

Ötlet: **szorzattá alakítás**. $n = x^2 - y^2 = (x - y)(x + y)$.

Legyen $x - y = a$ és $x + y = b$. Ekkor a és b paritása ugyanaz,

Két négyzetszám különbsége

Freud-Gyarmati: Számelmélet, 7.3.1. Tétel

Egy szám akkor áll elő **két négyzetszám különbségeként**, ha 4-gyel osztva **nem 2** maradékot ad.

Bizonyítás

Ötlet: **szorzattá alakítás**. $n = x^2 - y^2 = (x - y)(x + y)$.

Legyen $x - y = a$ és $x + y = b$. Ekkor a és b paritása ugyanaz, mert $b = a + 2y$,

Két négyzetszám különbsége

Freud-Gyarmati: Számelmélet, 7.3.1. Tétel

Egy szám akkor áll elő **két négyzetszám különbségeként**, ha 4-gyel osztva **nem 2** maradékot ad.

Bizonyítás

Ötlet: **szorzattá alakítás**. $n = x^2 - y^2 = (x - y)(x + y)$.

Legyen $x - y = a$ és $x + y = b$. Ekkor a és b paritása ugyanaz, mert $b = a + 2y$, tehát n vagy páratlan, vagy 4-gyel osztható.

Két négyzetszám különbsége

Freud-Gyarmati: Számelmélet, 7.3.1. Tétel

Egy szám akkor áll elő **két négyzetszám különbségeként**, ha 4-gyel osztva **nem 2** maradékot ad.

Bizonyítás

Ötlet: **szorzattá alakítás**. $n = x^2 - y^2 = (x - y)(x + y)$.

Legyen $x - y = a$ és $x + y = b$. Ekkor a és b paritása ugyanaz, mert $b = a + 2y$, tehát n vagy páratlan, vagy 4-gyel osztható.

Megfordítva: nyilván $x = (a + b)/2$

Két négyzetszám különbsége

Freud-Gyarmati: Számelmélet, 7.3.1. Tétel

Egy szám akkor áll elő **két négyzetszám különbségeként**, ha 4-gyel osztva **nem 2** maradékot ad.

Bizonyítás

Ötlet: **szorzattá alakítás**. $n = x^2 - y^2 = (x - y)(x + y)$.

Legyen $x - y = a$ és $x + y = b$. Ekkor a és b paritása ugyanaz, mert $b = a + 2y$, tehát n vagy páratlan, vagy 4-gyel osztható.

Megfordítva: nyilván $x = (a + b)/2$ és $y = (b - a)/2$.

Két négyzetszám különbsége

Freud-Gyarmati: Számelmélet, 7.3.1. Tétel

Egy szám akkor áll elő **két négyzetszám különbségeként**, ha 4-gyel osztva **nem 2** maradékot ad.

Bizonyítás

Ötlet: **szorzattá alakítás**. $n = x^2 - y^2 = (x - y)(x + y)$.

Legyen $x - y = a$ és $x + y = b$. Ekkor a és b paritása ugyanaz, mert $b = a + 2y$, tehát n vagy páratlan, vagy 4-gyel osztható.

Megfordítva: nyilván $x = (a + b)/2$ és $y = (b - a)/2$.

Ha n páratlan, legyen $a = 1$ és $b = n$,

Két négyzetszám különbsége

Freud-Gyarmati: Számelmélet, 7.3.1. Tétel

Egy szám akkor áll elő **két négyzetszám különbségeként**, ha 4-gyel osztva **nem 2** maradékot ad.

Bizonyítás

Ötlet: **szorzattá alakítás**. $n = x^2 - y^2 = (x - y)(x + y)$.

Legyen $x - y = a$ és $x + y = b$. Ekkor a és b paritása ugyanaz, mert $b = a + 2y$, tehát n vagy páratlan, vagy 4-gyel osztható.

Megfordítva: nyilván $x = (a + b)/2$ és $y = (b - a)/2$.

Ha n páratlan, legyen $a = 1$ és $b = n$, ekkor x, y egész.

Két négyzetszám különbsége

Freud-Gyarmati: Számelmélet, 7.3.1. Tétel

Egy szám akkor áll elő **két négyzetszám különbségeként**, ha 4-gyel osztva **nem 2** maradékot ad.

Bizonyítás

Ötlet: **szorzattá alakítás**. $n = x^2 - y^2 = (x - y)(x + y)$.

Legyen $x - y = a$ és $x + y = b$. Ekkor a és b paritása ugyanaz, mert $b = a + 2y$, tehát n vagy páratlan, vagy 4-gyel osztható.

Megfordítva: nyilván $x = (a + b)/2$ és $y = (b - a)/2$.

Ha n páratlan, legyen $a = 1$ és $b = n$, ekkor x, y egész.

Ha $4 \mid n$, akkor legyen $a = 2$ és $b = n/2$. □

Két négyzetszám különbsége

Freud-Gyarmati: Számelmélet, 7.3.1. Tétel

Egy szám akkor áll elő **két négyzetszám különbségeként**, ha 4-gyel osztva **nem 2** maradékot ad.

Bizonyítás

Ötlet: **szorzattá alakítás**. $n = x^2 - y^2 = (x - y)(x + y)$.

Legyen $x - y = a$ és $x + y = b$. Ekkor a és b paritása ugyanaz, mert $b = a + 2y$, tehát n vagy páratlan, vagy 4-gyel osztható.

Megfordítva: nyilván $x = (a + b)/2$ és $y = (b - a)/2$.

Ha n páratlan, legyen $a = 1$ és $b = n$, ekkor x, y egész.

Ha $4 \mid n$, akkor legyen $a = 2$ és $b = n/2$. □

HF: A megoldásszám $2d(n)$ ha n páratlan

Két négyzetszám különbsége

Freud-Gyarmati: Számelmélet, 7.3.1. Tétel

Egy szám akkor áll elő **két négyzetszám különbségeként**, ha 4-gyel osztva **nem 2** maradékot ad.

Bizonyítás

Ötlet: **szorzattá alakítás**. $n = x^2 - y^2 = (x - y)(x + y)$.

Legyen $x - y = a$ és $x + y = b$. Ekkor a és b paritása ugyanaz, mert $b = a + 2y$, tehát n vagy páratlan, vagy 4-gyel osztható.

Megfordítva: nyilván $x = (a + b)/2$ és $y = (b - a)/2$.

Ha n páratlan, legyen $a = 1$ és $b = n$, ekkor x, y egész.

Ha $4 \mid n$, akkor legyen $a = 2$ és $b = n/2$. □

HF: A megoldásszám $2d(n)$ ha n páratlan és $2d(n/4)$ ha $4 \mid n$.

Két négyzetszám különbsége

Freud-Gyarmati: Számelmélet, 7.3.1. Tétel

Egy szám akkor áll elő **két négyzetszám különbségeként**, ha 4-gyel osztva **nem 2** maradékot ad.

Bizonyítás

Ötlet: **szorzattá alakítás**. $n = x^2 - y^2 = (x - y)(x + y)$.

Legyen $x - y = a$ és $x + y = b$. Ekkor a és b paritása ugyanaz, mert $b = a + 2y$, tehát n vagy páratlan, vagy 4-gyel osztható.

Megfordítva: nyilván $x = (a + b)/2$ és $y = (b - a)/2$.

Ha n páratlan, legyen $a = 1$ és $b = n$, ekkor x, y egész.

Ha $4 \mid n$, akkor legyen $a = 2$ és $b = n/2$. □

HF: A megoldásszám $2d(n)$ ha n páratlan és $2d(n/4)$ ha $4 \mid n$.
(Ez a megfelelő $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ számpárok száma.)

Két négyzetszám összege

Freud-Gyarmati: Számelmélet, 7.4. Szakasz

Egy szám mikor áll elő két négyzetszám összegeként?

Két négyzetszám összege

Freud-Gyarmati: Számelmélet, 7.4. Szakasz

Egy szám mikor áll elő két négyzetszám összegeként?

Ötlet

$$n = x^2 + y^2$$

Két négyzetszám összege

Freud-Gyarmati: Számelmélet, 7.4. Szakasz

Egy szám mikor áll elő **két négyzetszám összegeként?**

Ötlet

$$n = x^2 + y^2 = (x - iy)(x + iy).$$

Két négyzetszám összege

Freud-Gyarmati: Számelmélet, 7.4. Szakasz

Egy szám mikor áll elő **két négyzetszám összegeként?**

Ötlet

$$n = x^2 + y^2 = (x - iy)(x + iy).$$

Itt $x + iy$ Gauss-egész,

Két négyzetszám összege

Freud-Gyarmati: Számelmélet, 7.4. Szakasz

Egy szám mikor áll elő **két négyzetszám összegeként?**

Ötlet

$$n = x^2 + y^2 = (x - iy)(x + iy).$$

Itt $x + iy$ Gauss-egész, ki kell építeni a számelméletüket.

Két négyzetszám összege

Freud-Gyarmati: Számelmélet, 7.4. Szakasz

Egy szám mikor áll elő **két négyzetszám összegeként?**

Ötlet

$$n = x^2 + y^2 = (x - iy)(x + iy).$$

Itt $x + iy$ Gauss-egész, ki kell építeni a számelméletüket.

Hasonló problémák

$$n = x^2 + 5y^2 =$$

Két négyzetszám összege

Freud-Gyarmati: Számelmélet, 7.4. Szakasz

Egy szám mikor áll elő **két négyzetszám összegeként?**

Ötlet

$$n = x^2 + y^2 = (x - iy)(x + iy).$$

Itt $x + iy$ Gauss-egész, ki kell építeni a számelméletüket.

Hasonló problémák

$$n = x^2 + 5y^2 = (x - \sqrt{5}iy)(x + \sqrt{5}iy).$$

Két négyzetszám összege

Freud-Gyarmati: Számelmélet, 7.4. Szakasz

Egy szám mikor áll elő **két négyzetszám összegeként?**

Ötlet

$$n = x^2 + y^2 = (x - iy)(x + iy).$$

Itt $x + iy$ Gauss-egész, ki kell építeni a számelméletüket.

Hasonló problémák

$$n = x^2 + 5y^2 = (x - \sqrt{5}iy)(x + \sqrt{5}iy).$$

Ehhez az $x + \sqrt{5}iy$ alakú számok számelmélete kell.

Két négyzetszám összege

Freud-Gyarmati: Számelmélet, 7.4. Szakasz

Egy szám mikor áll elő **két négyzetszám összegeként?**

Ötlet

$$n = x^2 + y^2 = (x - iy)(x + iy).$$

Itt $x + iy$ Gauss-egész, ki kell építeni a számelméletüket.

Hasonló problémák

$$n = x^2 + 5y^2 = (x - \sqrt{5}iy)(x + \sqrt{5}iy).$$

Ehhez az $x + \sqrt{5}iy$ alakú számok számelmélete kell.

$$z^3 = x^3 + y^3$$

Két négyzetszám összege

Freud-Gyarmati: Számelmélet, 7.4. Szakasz

Egy szám mikor áll elő **két négyzetszám összegeként?**

Ötlet

$$n = x^2 + y^2 = (x - iy)(x + iy).$$

Itt $x + iy$ Gauss-egész, ki kell építeni a számelméletüket.

Hasonló problémák

$$n = x^2 + 5y^2 = (x - \sqrt{5}iy)(x + \sqrt{5}iy).$$

Ehhez az $x + \sqrt{5}iy$ alakú számok számelmélete kell.

$$z^3 = x^3 + y^3 = (x + y)(x + \varepsilon y)(x + \varepsilon^2 y),$$

Két négyzetszám összege

Freud-Gyarmati: Számelmélet, 7.4. Szakasz

Egy szám mikor áll elő **két négyzetszám összegeként?**

Ötlet

$$n = x^2 + y^2 = (x - iy)(x + iy).$$

Itt $x + iy$ Gauss-egész, ki kell építeni a számelméletüket.

Hasonló problémák

$$n = x^2 + 5y^2 = (x - \sqrt{5}iy)(x + \sqrt{5}iy).$$

Ehhez az $x + \sqrt{5}iy$ alakú számok számelmélete kell.

$$z^3 = x^3 + y^3 = (x + y)(x + \varepsilon y)(x + \varepsilon^2 y),$$

ahol $\varepsilon = (1 + \sqrt{3}i)/2$ primitív harmadik egységgyök.

Két négyzetszám összege

Freud-Gyarmati: Számelmélet, 7.4. Szakasz

Egy szám mikor áll elő **két négyzetszám összegeként?**

Ötlet

$$n = x^2 + y^2 = (x - iy)(x + iy).$$

Itt $x + iy$ Gauss-egész, ki kell építeni a számelméletüket.

Hasonló problémák

$$n = x^2 + 5y^2 = (x - \sqrt{5}iy)(x + \sqrt{5}iy).$$

Ehhez az $x + \sqrt{5}iy$ alakú számok számelmélete kell.

$$z^3 = x^3 + y^3 = (x + y)(x + \varepsilon y)(x + \varepsilon^2 y),$$

ahol $\varepsilon = (1 + \sqrt{3}i)/2$ primitív harmadik egységgyök.

Újabb gyűri: **Euler-egészek.**

Két négyzetszám összege

Freud-Gyarmati: Számelmélet, 7.4. Szakasz

Egy szám mikor áll elő **két négyzetszám összegeként?**

Ötlet

$$n = x^2 + y^2 = (x - iy)(x + iy).$$

Itt $x + iy$ Gauss-egész, ki kell építeni a számelméletüket.

Hasonló problémák

$$n = x^2 + 5y^2 = (x - \sqrt{5}iy)(x + \sqrt{5}iy).$$

Ehhez az $x + \sqrt{5}iy$ alakú számok számelmélete kell.

$$z^3 = x^3 + y^3 = (x + y)(x + \varepsilon y)(x + \varepsilon^2 y),$$

ahol $\varepsilon = (1 + \sqrt{3}i)/2$ primitív harmadik egységgyök.

Újabb gyűrű: **Euler-egészek**. És így tovább!

Gauss-egész normája

A **Gauss-egészek** az $a + bi$ alakú számok, ahol $a, b \in \mathbb{Z}$.

Gauss-egész normája

A **Gauss-egészek** az $a + bi$ alakú számok, ahol $a, b \in \mathbb{Z}$.
Ezek egy \mathbb{G} szokásos gyűrűt alkotnak. (HF)

Gauss-egész normája

A **Gauss-egészek** az $a + bi$ alakú számok, ahol $a, b \in \mathbb{Z}$.

Ezek egy \mathbb{G} szokásos gyűrűt alkotnak. (HF)

Az $\alpha = a + bi$ **normája** $N(\alpha)$

Gauss-egész normája

A **Gauss-egészek** az $a + bi$ alakú számok, ahol $a, b \in \mathbb{Z}$.

Ezek egy \mathbb{G} szokásos gyűrűt alkotnak. (HF)

Az $\alpha = a + bi$ **normája** $N(\alpha) = \alpha\bar{\alpha}$

Gauss-egész normája

A **Gauss-egészek** az $a + bi$ alakú számok, ahol $a, b \in \mathbb{Z}$.

Ezek egy \mathbb{G} szokásos gyűrűt alkotnak. (HF)

Az $\alpha = a + bi$ **normája** $N(\alpha) = \alpha\bar{\alpha} = a^2 + b^2$

Gauss-egész normája

A **Gauss-egészek** az $a + bi$ alakú számok, ahol $a, b \in \mathbb{Z}$.

Ezek egy \mathbb{G} szokásos gyűrűt alkotnak. (HF)

Az $\alpha = a + bi$ **normája** $N(\alpha) = \alpha\bar{\alpha} = a^2 + b^2 = |\alpha|^2$.

Gauss-egész normája

A **Gauss-egészek** az $a + bi$ alakú számok, ahol $a, b \in \mathbb{Z}$.

Ezek egy \mathbb{G} szokásos gyűrűt alkotnak. (HF)

Az $\alpha = a + bi$ **normája** $N(\alpha) = \alpha\bar{\alpha} = a^2 + b^2 = |\alpha|^2$.

Freud-Gyarmati: 7.4.3, 7.4.5. Tétel

Tetszőleges α, β Gauss-egészekre

Gauss-egész normája

A **Gauss-egészek** az $a + bi$ alakú számok, ahol $a, b \in \mathbb{Z}$.

Ezek egy \mathbb{G} szokásos gyűrűt alkotnak. (HF)

Az $\alpha = a + bi$ **normája** $N(\alpha) = \alpha\bar{\alpha} = a^2 + b^2 = |\alpha|^2$.

Freud-Gyarmati: 7.4.3, 7.4.5. Tétel

Tetszőleges α, β Gauss-egészekre

- (1) $N(\alpha)$ nemnegatív egész.

Gauss-egész normája

A **Gauss-egészek** az $a + bi$ alakú számok, ahol $a, b \in \mathbb{Z}$.

Ezek egy \mathbb{G} szokásos gyűrűt alkotnak. (HF)

Az $\alpha = a + bi$ **normája** $N(\alpha) = \alpha\bar{\alpha} = a^2 + b^2 = |\alpha|^2$.

Freud-Gyarmati: 7.4.3, 7.4.5. Tétel

Tetszőleges α, β Gauss-egészekre

- (1) $N(\alpha)$ nemnegatív egész.
- (2) $N(\alpha) = 0 \iff \alpha = 0$.

Gauss-egész normája

A **Gauss-egészek** az $a + bi$ alakú számok, ahol $a, b \in \mathbb{Z}$.

Ezek egy \mathbb{G} szokásos gyűrűt alkotnak. (HF)

Az $\alpha = a + bi$ **normája** $N(\alpha) = \alpha\bar{\alpha} = a^2 + b^2 = |\alpha|^2$.

Freud-Gyarmati: 7.4.3, 7.4.5. Tétel

Tetszőleges α, β Gauss-egészekre

- (1) $N(\alpha)$ nemnegatív egész.
- (2) $N(\alpha) = 0 \iff \alpha = 0$.
- (3) $N(\alpha\beta) = N(\alpha)N(\beta)$.

Gauss-egész normája

A **Gauss-egészek** az $a + bi$ alakú számok, ahol $a, b \in \mathbb{Z}$.

Ezek egy \mathbb{G} szokásos gyűrűt alkotnak. (HF)

Az $\alpha = a + bi$ **normája** $N(\alpha) = \alpha\bar{\alpha} = a^2 + b^2 = |\alpha|^2$.

Freud-Gyarmati: 7.4.3, 7.4.5. Tétel

Tetszőleges α, β Gauss-egészekre

- (1) $N(\alpha)$ nemnegatív egész.
- (2) $N(\alpha) = 0 \iff \alpha = 0$.
- (3) $N(\alpha\beta) = N(\alpha)N(\beta)$.
- (4) $\alpha \mid_{\mathbb{G}} \beta \implies N(\alpha) \mid_{\mathbb{Z}} N(\beta)$.

Gauss-egész normája

A **Gauss-egészek** az $a + bi$ alakú számok, ahol $a, b \in \mathbb{Z}$.

Ezek egy \mathbb{G} szokásos gyűrűt alkotnak. (HF)

Az $\alpha = a + bi$ **normája** $N(\alpha) = \alpha\bar{\alpha} = a^2 + b^2 = |\alpha|^2$.

Freud-Gyarmati: 7.4.3, 7.4.5. Tétel

Tetszőleges α, β Gauss-egészekre

- (1) $N(\alpha)$ nemnegatív egész.
- (2) $N(\alpha) = 0 \iff \alpha = 0$.
- (3) $N(\alpha\beta) = N(\alpha)N(\beta)$.
- (4) $\alpha \mid_{\mathbb{G}} \beta \implies N(\alpha) \mid_{\mathbb{Z}} N(\beta)$.

A (4)-ben $\mid_{\mathbb{G}}$ a \mathbb{G} -beli,

Gauss-egész normája

A **Gauss-egészek** az $a + bi$ alakú számok, ahol $a, b \in \mathbb{Z}$.

Ezek egy \mathbb{G} szokásos gyűrűt alkotnak. (HF)

Az $\alpha = a + bi$ **normája** $N(\alpha) = \alpha\bar{\alpha} = a^2 + b^2 = |\alpha|^2$.

Freud-Gyarmati: 7.4.3, 7.4.5. Tétel

Tetszőleges α, β Gauss-egészekre

- (1) $N(\alpha)$ nemnegatív egész.
- (2) $N(\alpha) = 0 \iff \alpha = 0$.
- (3) $N(\alpha\beta) = N(\alpha)N(\beta)$.
- (4) $\alpha \mid_{\mathbb{G}} \beta \implies N(\alpha) \mid_{\mathbb{Z}} N(\beta)$.

A (4)-ben $\mid_{\mathbb{G}}$ a \mathbb{G} -beli, $\mid_{\mathbb{Z}}$ a \mathbb{Z} -beli oszthatóságot jelöli.

Gauss-egész normája

A **Gauss-egészek** az $a + bi$ alakú számok, ahol $a, b \in \mathbb{Z}$.

Ezek egy \mathbb{G} szokásos gyűrűt alkotnak. (HF)

Az $\alpha = a + bi$ **normája** $N(\alpha) = \alpha\bar{\alpha} = a^2 + b^2 = |\alpha|^2$.

Freud-Gyarmati: 7.4.3, 7.4.5. Tétel

Tetszőleges α, β Gauss-egészekre

- (1) $N(\alpha)$ nemnegatív egész.
- (2) $N(\alpha) = 0 \iff \alpha = 0$.
- (3) $N(\alpha\beta) = N(\alpha)N(\beta)$.
- (4) $\alpha \mid_{\mathbb{G}} \beta \implies N(\alpha) \mid_{\mathbb{Z}} N(\beta)$.

A (4)-ben $\mid_{\mathbb{G}}$ a \mathbb{G} -beli, $\mid_{\mathbb{Z}}$ a \mathbb{Z} -beli oszthatóságot jelöli.

Bizonyítás: (1) és (2) HF.

Gauss-egész normája

A **Gauss-egészek** az $a + bi$ alakú számok, ahol $a, b \in \mathbb{Z}$.

Ezek egy \mathbb{G} szokásos gyűrűt alkotnak. (HF)

Az $\alpha = a + bi$ **normája** $N(\alpha) = \alpha\bar{\alpha} = a^2 + b^2 = |\alpha|^2$.

Freud-Gyarmati: 7.4.3, 7.4.5. Tétel

Tetszőleges α, β Gauss-egészekre

- (1) $N(\alpha)$ nemnegatív egész.
- (2) $N(\alpha) = 0 \iff \alpha = 0$.
- (3) $N(\alpha\beta) = N(\alpha)N(\beta)$.
- (4) $\alpha \mid_{\mathbb{G}} \beta \implies N(\alpha) \mid_{\mathbb{Z}} N(\beta)$.

A (4)-ben $\mid_{\mathbb{G}}$ a \mathbb{G} -beli, $\mid_{\mathbb{Z}}$ a \mathbb{Z} -beli oszthatóságot jelöli.

Bizonyítás: (1) és (2) HF.

(3): $N(\alpha\beta) = |\alpha\beta|^2$

Gauss-egész normája

A **Gauss-egészek** az $a + bi$ alakú számok, ahol $a, b \in \mathbb{Z}$.

Ezek egy \mathbb{G} szokásos gyűrűt alkotnak. (HF)

Az $\alpha = a + bi$ **normája** $N(\alpha) = \alpha\bar{\alpha} = a^2 + b^2 = |\alpha|^2$.

Freud-Gyarmati: 7.4.3, 7.4.5. Tétel

Tetszőleges α, β Gauss-egészekre

- (1) $N(\alpha)$ nemnegatív egész.
- (2) $N(\alpha) = 0 \iff \alpha = 0$.
- (3) $N(\alpha\beta) = N(\alpha)N(\beta)$.
- (4) $\alpha \mid_{\mathbb{G}} \beta \implies N(\alpha) \mid_{\mathbb{Z}} N(\beta)$.

A (4)-ben $\mid_{\mathbb{G}}$ a \mathbb{G} -beli, $\mid_{\mathbb{Z}}$ a \mathbb{Z} -beli oszthatóságot jelöli.

Bizonyítás: (1) és (2) HF.

(3): $N(\alpha\beta) = |\alpha\beta|^2 = (|\alpha||\beta|)^2$

Gauss-egész normája

A **Gauss-egészek** az $a + bi$ alakú számok, ahol $a, b \in \mathbb{Z}$.

Ezek egy \mathbb{G} szokásos gyűrűt alkotnak. (HF)

Az $\alpha = a + bi$ **normája** $N(\alpha) = \alpha\bar{\alpha} = a^2 + b^2 = |\alpha|^2$.

Freud-Gyarmati: 7.4.3, 7.4.5. Tétel

Tetszőleges α, β Gauss-egészekre

- (1) $N(\alpha)$ nemnegatív egész.
- (2) $N(\alpha) = 0 \iff \alpha = 0$.
- (3) $N(\alpha\beta) = N(\alpha)N(\beta)$.
- (4) $\alpha \mid_{\mathbb{G}} \beta \implies N(\alpha) \mid_{\mathbb{Z}} N(\beta)$.

A (4)-ben $\mid_{\mathbb{G}}$ a \mathbb{G} -beli, $\mid_{\mathbb{Z}}$ a \mathbb{Z} -beli oszthatóságot jelöli.

Bizonyítás: (1) és (2) HF.

(3): $N(\alpha\beta) = |\alpha\beta|^2 = (|\alpha||\beta|)^2 = N(\alpha)N(\beta)$.

Gauss-egész normája

A **Gauss-egészek** az $a + bi$ alakú számok, ahol $a, b \in \mathbb{Z}$.

Ezek egy \mathbb{G} szokásos gyűrűt alkotnak. (HF)

Az $\alpha = a + bi$ **normája** $N(\alpha) = \alpha\bar{\alpha} = a^2 + b^2 = |\alpha|^2$.

Freud-Gyarmati: 7.4.3, 7.4.5. Tétel

Tetszőleges α, β Gauss-egészekre

- (1) $N(\alpha)$ nemnegatív egész.
- (2) $N(\alpha) = 0 \iff \alpha = 0$.
- (3) $N(\alpha\beta) = N(\alpha)N(\beta)$.
- (4) $\alpha \mid_{\mathbb{G}} \beta \implies N(\alpha) \mid_{\mathbb{Z}} N(\beta)$.

A (4)-ben $\mid_{\mathbb{G}}$ a \mathbb{G} -beli, $\mid_{\mathbb{Z}}$ a \mathbb{Z} -beli oszthatóságot jelöli.

Bizonyítás: (1) és (2) HF.

$$(3): N(\alpha\beta) = |\alpha\beta|^2 = (|\alpha||\beta|)^2 = N(\alpha)N(\beta).$$

$$(4): \beta = \alpha\gamma \implies N(\beta) = N(\alpha)N(\gamma).$$

Az egységek a Gauss-egészek között

Freud-Gyarmati: 7.4.7. Tétel

A Gauss-egészek egységei a ± 1 , $\pm i$ számok.

Az egységek a Gauss-egészek között

Freud-Gyarmati: 7.4.7. Tétel

A Gauss-egészek egységei a ± 1 , $\pm i$ számok.

Ezek pontosan azok a Gauss-egészek, melyek normája 1.

Az egységek a Gauss-egészek között

Freud-Gyarmati: 7.4.7. Tétel

A Gauss-egészek egységei a ± 1 , $\pm i$ számok.
Ezek pontosan azok a Gauss-egészek, melyek normája 1.

Bizonyítás

Ha $\varepsilon \mid 1$, akkor $N(\varepsilon) \mid N(1) = 1$.

Az egységek a Gauss-egészek között

Freud-Gyarmati: 7.4.7. Tétel

A Gauss-egészek egységei a ± 1 , $\pm i$ számok.
Ezek pontosan azok a Gauss-egészek, melyek normája 1.

Bizonyítás

Ha $\varepsilon \mid 1$, akkor $N(\varepsilon) \mid N(1) = 1$.

Vagyis ha ε egység, akkor normája 1 vagy -1 .

Az egységek a Gauss-egészek között

Freud-Gyarmati: 7.4.7. Tétel

A Gauss-egészek egységei a ± 1 , $\pm i$ számok.
Ezek pontosan azok a Gauss-egészek, melyek normája 1.

Bizonyítás

Ha $\varepsilon \mid 1$, akkor $N(\varepsilon) \mid N(1) = 1$.

Vagyis ha ε egység, akkor normája 1 vagy -1 .

Legyen $\varepsilon = a + bi$, akkor $a^2 + b^2 = \pm 1$.

Az egységek a Gauss-egészek között

Freud-Gyarmati: 7.4.7. Tétel

A Gauss-egészek egységei a ± 1 , $\pm i$ számok.
Ezek pontosan azok a Gauss-egészek, melyek normája 1.

Bizonyítás

Ha $\varepsilon \mid 1$, akkor $N(\varepsilon) \mid N(1) = 1$.

Vagyis ha ε egység, akkor normája 1 vagy -1 .

Legyen $\varepsilon = a + bi$, akkor $a^2 + b^2 = \pm 1$.

Mivel a^2 és b^2 nemnegatív egészek, az egyik 1, a másik 0.

Az egységek a Gauss-egészek között

Freud-Gyarmati: 7.4.7. Tétel

A Gauss-egészek egységei a ± 1 , $\pm i$ számok.
Ezek pontosan azok a Gauss-egészek, melyek normája 1.

Bizonyítás

Ha $\varepsilon \mid 1$, akkor $N(\varepsilon) \mid N(1) = 1$.

Vagyis ha ε egység, akkor normája 1 vagy -1 .

Legyen $\varepsilon = a + bi$, akkor $a^2 + b^2 = \pm 1$.

Mivel a^2 és b^2 nemnegatív egészek, az egyik 1, a másik 0.

Ha $a^2 = 1$, akkor tehát $\varepsilon = \pm 1$,

Az egységek a Gauss-egészek között

Freud-Gyarmati: 7.4.7. Tétel

A Gauss-egészek egységei a ± 1 , $\pm i$ számok.
Ezek pontosan azok a Gauss-egészek, melyek normája 1.

Bizonyítás

Ha $\varepsilon \mid 1$, akkor $N(\varepsilon) \mid N(1) = 1$.

Vagyis ha ε egység, akkor normája 1 vagy -1 .

Legyen $\varepsilon = a + bi$, akkor $a^2 + b^2 = \pm 1$.

Mivel a^2 és b^2 nemnegatív egészek, az egyik 1, a másik 0.

Ha $a^2 = 1$, akkor tehát $\varepsilon = \pm 1$, különben $\varepsilon = \pm i$.

Az egységek a Gauss-egészek között

Freud-Gyarmati: 7.4.7. Tétel

A Gauss-egészek egységei a ± 1 , $\pm i$ számok.
Ezek pontosan azok a Gauss-egészek, melyek normája 1.

Bizonyítás

Ha $\varepsilon \mid 1$, akkor $N(\varepsilon) \mid N(1) = 1$.

Vagyis ha ε egység, akkor normája 1 vagy -1 .

Legyen $\varepsilon = a + bi$, akkor $a^2 + b^2 = \pm 1$.

Mivel a^2 és b^2 nemnegatív egészek, az egyik 1, a másik 0.

Ha $a^2 = 1$, akkor tehát $\varepsilon = \pm 1$, különben $\varepsilon = \pm i$.

Megfordítva: ± 1 és $\pm i$ invertálhatók \mathbb{G} -ben,

Az egységek a Gauss-egészek között

Freud-Gyarmati: 7.4.7. Tétel

A Gauss-egészek egységei a ± 1 , $\pm i$ számok.
Ezek pontosan azok a Gauss-egészek, melyek normája 1.

Bizonyítás

Ha $\varepsilon \mid 1$, akkor $N(\varepsilon) \mid N(1) = 1$.

Vagyis ha ε egység, akkor normája 1 vagy -1 .

Legyen $\varepsilon = a + bi$, akkor $a^2 + b^2 = \pm 1$.

Mivel a^2 és b^2 nemnegatív egészek, az egyik 1, a másik 0.

Ha $a^2 = 1$, akkor tehát $\varepsilon = \pm 1$, különben $\varepsilon = \pm i$.

Megfordítva: ± 1 és $\pm i$ invertálhatók \mathbb{G} -ben, hiszen

$$1 = 1 \cdot 1$$

Az egységek a Gauss-egészek között

Freud-Gyarmati: 7.4.7. Tétel

A Gauss-egészek egységei a ± 1 , $\pm i$ számok.
Ezek pontosan azok a Gauss-egészek, melyek normája 1.

Bizonyítás

Ha $\varepsilon \mid 1$, akkor $N(\varepsilon) \mid N(1) = 1$.

Vagyis ha ε egység, akkor normája 1 vagy -1 .

Legyen $\varepsilon = a + bi$, akkor $a^2 + b^2 = \pm 1$.

Mivel a^2 és b^2 nemnegatív egészek, az egyik 1, a másik 0.

Ha $a^2 = 1$, akkor tehát $\varepsilon = \pm 1$, különben $\varepsilon = \pm i$.

Megfordítva: ± 1 és $\pm i$ invertálhatók \mathbb{G} -ben, hiszen

$$1 = 1 \cdot 1 = (-1) \cdot (-1)$$

Az egységek a Gauss-egészek között

Freud-Gyarmati: 7.4.7. Tétel

A Gauss-egészek egységei a ± 1 , $\pm i$ számok.
Ezek pontosan azok a Gauss-egészek, melyek normája 1.

Bizonyítás

Ha $\varepsilon \mid 1$, akkor $N(\varepsilon) \mid N(1) = 1$.

Vagyis ha ε egység, akkor normája 1 vagy -1 .

Legyen $\varepsilon = a + bi$, akkor $a^2 + b^2 = \pm 1$.

Mivel a^2 és b^2 nemnegatív egészek, az egyik 1, a másik 0.

Ha $a^2 = 1$, akkor tehát $\varepsilon = \pm 1$, különben $\varepsilon = \pm i$.

Megfordítva: ± 1 és $\pm i$ invertálhatók \mathbb{G} -ben, hiszen

$$1 = 1 \cdot 1 = (-1) \cdot (-1) = i \cdot (-i).$$

Az egységek a Gauss-egészek között

Freud-Gyarmati: 7.4.7. Tétel

A Gauss-egészek egységei a ± 1 , $\pm i$ számok.
Ezek pontosan azok a Gauss-egészek, melyek normája 1.

Bizonyítás

Ha $\varepsilon \mid 1$, akkor $N(\varepsilon) \mid N(1) = 1$.

Vagyis ha ε egység, akkor normája 1 vagy -1 .

Legyen $\varepsilon = a + bi$, akkor $a^2 + b^2 = \pm 1$.

Mivel a^2 és b^2 nemnegatív egészek, az egyik 1, a másik 0.

Ha $a^2 = 1$, akkor tehát $\varepsilon = \pm 1$, különben $\varepsilon = \pm i$.

Megfordítva: ± 1 és $\pm i$ invertálhatók \mathbb{G} -ben, hiszen

$$1 = 1 \cdot 1 = (-1) \cdot (-1) = i \cdot (-i).$$

Ezért ezek minden Gauss-egésznek osztói. □

Maradékos osztás Gauss-egészekre

Freud-Gyarmati: 7.4.8. Tétel

Tetszőleges α és $\beta \neq 0$ Gauss-egészekhez léteznek olyan γ és ρ Gauss-egészek, hogy

Maradékös osztás Gauss-egészekre

Freud-Gyarmati: 7.4.8. Tétel

Tetszőleges α és $\beta \neq 0$ Gauss-egészekhez léteznek olyan γ és ρ Gauss-egészek, hogy $\alpha = \beta\gamma + \rho$

Maradékos osztás Gauss-egészekre

Freud-Gyarmati: 7.4.8. Tétel

Tetszőleges α és $\beta \neq 0$ Gauss-egészekhez léteznek olyan γ és ρ Gauss-egészek, hogy $\alpha = \beta\gamma + \rho$ és $N(\rho) < N(\beta)$.

Maradékos osztás Gauss-egészekre

Freud-Gyarmati: 7.4.8. Tétel

Tetszőleges α és $\beta \neq 0$ Gauss-egészekhez léteznek olyan γ és ρ Gauss-egészek, hogy $\alpha = \beta\gamma + \rho$ és $N(\rho) < N(\beta)$.

Bizonyítás

Az egyenletet átalakítva $(\alpha/\beta) - \gamma = \rho/\beta$.

Maradékos osztás Gauss-egészekre

Freud-Gyarmati: 7.4.8. Tétel

Tetszőleges α és $\beta \neq 0$ Gauss-egészekhez léteznek olyan γ és ρ Gauss-egészek, hogy $\alpha = \beta\gamma + \rho$ és $N(\rho) < N(\beta)$.

Bizonyítás

Az egyenletet átalakítva $(\alpha/\beta) - \gamma = \rho/\beta$.

Nyilván $N(\rho) < N(\beta) \iff |\rho|^2 < |\beta|^2$

Maradékös osztás Gauss-egészekre

Freud-Gyarmati: 7.4.8. Tétel

Tetszőleges α és $\beta \neq 0$ Gauss-egészekhez léteznek olyan γ és ρ Gauss-egészek, hogy $\alpha = \beta\gamma + \rho$ és $N(\rho) < N(\beta)$.

Bizonyítás

Az egyenletet átalakítva $(\alpha/\beta) - \gamma = \rho/\beta$.

Nyilván $N(\rho) < N(\beta) \iff |\rho|^2 < |\beta|^2 \iff |\rho/\beta|^2 < 1$.

Maradékös osztás Gauss-egészekre

Freud-Gyarmati: 7.4.8. Tétel

Tetszőleges α és $\beta \neq 0$ Gauss-egészekhez léteznek olyan γ és ρ Gauss-egészek, hogy $\alpha = \beta\gamma + \rho$ és $N(\rho) < N(\beta)$.

Bizonyítás

Az egyenletet átalakítva $(\alpha/\beta) - \gamma = \rho/\beta$.

Nyilván $N(\rho) < N(\beta) \iff |\rho|^2 < |\beta|^2 \iff |\rho/\beta|^2 < 1$.

Vagyis olyan γ kell, hogy $|(\alpha/\beta) - \gamma|^2 < 1$.

Maradékos osztás Gauss-egészekre

Freud-Gyarmati: 7.4.8. Tétel

Tetszőleges α és $\beta \neq 0$ Gauss-egészekhez léteznek olyan γ és ρ Gauss-egészek, hogy $\alpha = \beta\gamma + \rho$ és $N(\rho) < N(\beta)$.

Bizonyítás

Az egyenletet átalakítva $(\alpha/\beta) - \gamma = \rho/\beta$.

Nyilván $N(\rho) < N(\beta) \iff |\rho|^2 < |\beta|^2 \iff |\rho/\beta|^2 < 1$.

Vagyis olyan γ kell, hogy $|(\alpha/\beta) - \gamma|^2 < 1$.

Ilyet elég találni, mert akkor $\rho = (\alpha/\beta) - \gamma$ jó lesz.

Maradékös osztás Gauss-egészekre

Freud-Gyarmati: 7.4.8. Tétel

Tetszőleges α és $\beta \neq 0$ Gauss-egészekhez léteznek olyan γ és ρ Gauss-egészek, hogy $\alpha = \beta\gamma + \rho$ és $N(\rho) < N(\beta)$.

Bizonyítás

Az egyenletet átalakítva $(\alpha/\beta) - \gamma = \rho/\beta$.

Nyilván $N(\rho) < N(\beta) \iff |\rho|^2 < |\beta|^2 \iff |\rho/\beta|^2 < 1$.

Vagyis olyan γ kell, hogy $|(\alpha/\beta) - \gamma|^2 < 1$.

Ilyet elég találni, mert akkor $\rho = (\alpha/\beta) - \gamma$ jó lesz.

Legyen $\alpha/\beta = c + di$,

Maradékos osztás Gauss-egészekre

Freud-Gyarmati: 7.4.8. Tétel

Tetszőleges α és $\beta \neq 0$ Gauss-egészekhez léteznek olyan γ és ρ Gauss-egészek, hogy $\alpha = \beta\gamma + \rho$ és $N(\rho) < N(\beta)$.

Bizonyítás

Az egyenletet átalakítva $(\alpha/\beta) - \gamma = \rho/\beta$.

Nyilván $N(\rho) < N(\beta) \iff |\rho|^2 < |\beta|^2 \iff |\rho/\beta|^2 < 1$.

Vagyis olyan γ kell, hogy $|(\alpha/\beta) - \gamma|^2 < 1$.

Ilyet elég találni, mert akkor $\rho = (\alpha/\beta) - \gamma$ jó lesz.

Legyen $\alpha/\beta = c + di$, c' a c -hez legközelebbi egész.

Maradékös osztás Gauss-egészekre

Freud-Gyarmati: 7.4.8. Tétel

Tetszőleges α és $\beta \neq 0$ Gauss-egészekhez léteznek olyan γ és ρ Gauss-egészek, hogy $\alpha = \beta\gamma + \rho$ és $N(\rho) < N(\beta)$.

Bizonyítás

Az egyenletet átalakítva $(\alpha/\beta) - \gamma = \rho/\beta$.

Nyilván $N(\rho) < N(\beta) \iff |\rho|^2 < |\beta|^2 \iff |\rho/\beta|^2 < 1$.

Vagyis olyan γ kell, hogy $|(\alpha/\beta) - \gamma|^2 < 1$.

Ilyet elég találni, mert akkor $\rho = (\alpha/\beta) - \gamma$ jó lesz.

Legyen $\alpha/\beta = c + di$, c' a c -hez, d' a d -hez legközelebbi egész.

Maradékös osztás Gauss-egészekre

Freud-Gyarmati: 7.4.8. Tétel

Tetszőleges α és $\beta \neq 0$ Gauss-egészekhez léteznek olyan γ és ρ Gauss-egészek, hogy $\alpha = \beta\gamma + \rho$ és $N(\rho) < N(\beta)$.

Bizonyítás

Az egyenletet átalakítva $(\alpha/\beta) - \gamma = \rho/\beta$.

Nyilván $N(\rho) < N(\beta) \iff |\rho|^2 < |\beta|^2 \iff |\rho/\beta|^2 < 1$.

Vagyis olyan γ kell, hogy $|(\alpha/\beta) - \gamma|^2 < 1$.

Ilyet elég találni, mert akkor $\rho = (\alpha/\beta) - \gamma$ jó lesz.

Legyen $\alpha/\beta = c + di$, c' a c -hez, d' a d -hez legközelebbi egész.

Ekkor $|c - c'| \leq 1/2$

Maradékös osztás Gauss-egészekre

Freud-Gyarmati: 7.4.8. Tétel

Tetszőleges α és $\beta \neq 0$ Gauss-egészekhez léteznek olyan γ és ρ Gauss-egészek, hogy $\alpha = \beta\gamma + \rho$ és $N(\rho) < N(\beta)$.

Bizonyítás

Az egyenletet átalakítva $(\alpha/\beta) - \gamma = \rho/\beta$.

Nyilván $N(\rho) < N(\beta) \iff |\rho|^2 < |\beta|^2 \iff |\rho/\beta|^2 < 1$.

Vagyis olyan γ kell, hogy $|(\alpha/\beta) - \gamma|^2 < 1$.

Ilyet elég találni, mert akkor $\rho = (\alpha/\beta) - \gamma$ jó lesz.

Legyen $\alpha/\beta = c + di$, c' a c -hez, d' a d -hez legközelebbi egész.

Ekkor $|c - c'| \leq 1/2$ és $|d - d'| \leq 1/2$.

Maradékos osztás Gauss-egészekre

Freud-Gyarmati: 7.4.8. Tétel

Tetszőleges α és $\beta \neq 0$ Gauss-egészekhez léteznek olyan γ és ρ Gauss-egészek, hogy $\alpha = \beta\gamma + \rho$ és $N(\rho) < N(\beta)$.

Bizonyítás

Az egyenletet átalakítva $(\alpha/\beta) - \gamma = \rho/\beta$.

Nyilván $N(\rho) < N(\beta) \iff |\rho|^2 < |\beta|^2 \iff |\rho/\beta|^2 < 1$.

Vagyis olyan γ kell, hogy $|(\alpha/\beta) - \gamma|^2 < 1$.

Ilyet elég találni, mert akkor $\rho = (\alpha/\beta) - \gamma$ jó lesz.

Legyen $\alpha/\beta = c + di$, c' a c -hez, d' a d -hez legközelebbi egész.

Ekkor $|c - c'| \leq 1/2$ és $|d - d'| \leq 1/2$.

Tehát a $\gamma = c' + d'i$ megfelelő Gauss-egész,

Maradékös osztás Gauss-egészekre

Freud-Gyarmati: 7.4.8. Tétel

Tetszőleges α és $\beta \neq 0$ Gauss-egészekhez léteznek olyan γ és ρ Gauss-egészek, hogy $\alpha = \beta\gamma + \rho$ és $N(\rho) < N(\beta)$.

Bizonyítás

Az egyenletet átalakítva $(\alpha/\beta) - \gamma = \rho/\beta$.

Nyilván $N(\rho) < N(\beta) \iff |\rho|^2 < |\beta|^2 \iff |\rho/\beta|^2 < 1$.

Vagyis olyan γ kell, hogy $|(\alpha/\beta) - \gamma|^2 < 1$.

Ilyet elég találni, mert akkor $\rho = (\alpha/\beta) - \gamma$ jó lesz.

Legyen $\alpha/\beta = c + di$, c' a c -hez, d' a d -hez legközelebbi egész.

Ekkor $|c - c'| \leq 1/2$ és $|d - d'| \leq 1/2$.

Tehát a $\gamma = c' + d'i$ megfelelő Gauss-egész, mert

$$|(\alpha/\beta) - \gamma|^2 = (c - c')^2 + (d - d')^2$$

Maradékös osztás Gauss-egészekre

Freud-Gyarmati: 7.4.8. Tétel

Tetszőleges α és $\beta \neq 0$ Gauss-egészekhez léteznek olyan γ és ρ Gauss-egészek, hogy $\alpha = \beta\gamma + \rho$ és $N(\rho) < N(\beta)$.

Bizonyítás

Az egyenletet átalakítva $(\alpha/\beta) - \gamma = \rho/\beta$.

Nyilván $N(\rho) < N(\beta) \iff |\rho|^2 < |\beta|^2 \iff |\rho/\beta|^2 < 1$.

Vagyis olyan γ kell, hogy $|(\alpha/\beta) - \gamma|^2 < 1$.

Ilyet elég találni, mert akkor $\rho = (\alpha/\beta) - \gamma$ jó lesz.

Legyen $\alpha/\beta = c + di$, c' a c -hez, d' a d -hez legközelebbi egész.

Ekkor $|c - c'| \leq 1/2$ és $|d - d'| \leq 1/2$.

Tehát a $\gamma = c' + d'i$ megfelelő Gauss-egész, mert

$$|(\alpha/\beta) - \gamma|^2 = (c - c')^2 + (d - d')^2 \leq (1/2)^2 + (1/2)^2$$

Maradékös osztás Gauss-egészekre

Freud-Gyarmati: 7.4.8. Tétel

Tetszőleges α és $\beta \neq 0$ Gauss-egészekhez léteznek olyan γ és ρ Gauss-egészek, hogy $\alpha = \beta\gamma + \rho$ és $N(\rho) < N(\beta)$.

Bizonyítás

Az egyenletet átalakítva $(\alpha/\beta) - \gamma = \rho/\beta$.

Nyilván $N(\rho) < N(\beta) \iff |\rho|^2 < |\beta|^2 \iff |\rho/\beta|^2 < 1$.

Vagyis olyan γ kell, hogy $|(\alpha/\beta) - \gamma|^2 < 1$.

Ilyet elég találni, mert akkor $\rho = (\alpha/\beta) - \gamma$ jó lesz.

Legyen $\alpha/\beta = c + di$, c' a c -hez, d' a d -hez legközelebbi egész.

Ekkor $|c - c'| \leq 1/2$ és $|d - d'| \leq 1/2$.

Tehát a $\gamma = c' + d'i$ megfelelő Gauss-egész, mert

$|(\alpha/\beta) - \gamma|^2 = (c - c')^2 + (d - d')^2 \leq (1/2)^2 + (1/2)^2 < 1$. \square

Maradékös osztás Gauss-egészekre

Freud-Gyarmati: 7.4.8. Tétel

Tetszőleges α és $\beta \neq 0$ Gauss-egészekhez léteznek olyan γ és ρ Gauss-egészek, hogy $\alpha = \beta\gamma + \rho$ és $N(\rho) < N(\beta)$.

Bizonyítás

Az egyenletet átalakítva $(\alpha/\beta) - \gamma = \rho/\beta$.

Nyilván $N(\rho) < N(\beta) \iff |\rho|^2 < |\beta|^2 \iff |\rho/\beta|^2 < 1$.

Vagyis olyan γ kell, hogy $|(\alpha/\beta) - \gamma|^2 < 1$.

Ilyet elég találni, mert akkor $\rho = (\alpha/\beta) - \gamma$ jó lesz.

Legyen $\alpha/\beta = c + di$, c' a c -hez, d' a d -hez legközelebbi egész.

Ekkor $|c - c'| \leq 1/2$ és $|d - d'| \leq 1/2$.

Tehát a $\gamma = c' + d'i$ megfelelő Gauss-egész, mert

$|(\alpha/\beta) - \gamma|^2 = (c - c')^2 + (d - d')^2 \leq (1/2)^2 + (1/2)^2 < 1$. \square

Tehát \mathbb{G} **euklideszi** gyűrű,

Maradékös osztás Gauss-egészekre

Freud-Gyarmati: 7.4.8. Tétel

Tetszőleges α és $\beta \neq 0$ Gauss-egészekhez léteznek olyan γ és ρ Gauss-egészek, hogy $\alpha = \beta\gamma + \rho$ és $N(\rho) < N(\beta)$.

Bizonyítás

Az egyenletet átalakítva $(\alpha/\beta) - \gamma = \rho/\beta$.

Nyilván $N(\rho) < N(\beta) \iff |\rho|^2 < |\beta|^2 \iff |\rho/\beta|^2 < 1$.

Vagyis olyan γ kell, hogy $|(\alpha/\beta) - \gamma|^2 < 1$.

Ilyet elég találni, mert akkor $\rho = (\alpha/\beta) - \gamma$ jó lesz.

Legyen $\alpha/\beta = c + di$, c' a c -hez, d' a d -hez legközelebbi egész.

Ekkor $|c - c'| \leq 1/2$ és $|d - d'| \leq 1/2$.

Tehát a $\gamma = c' + d'i$ megfelelő Gauss-egész, mert

$|(\alpha/\beta) - \gamma|^2 = (c - c')^2 + (d - d')^2 \leq (1/2)^2 + (1/2)^2 < 1$. \square

Tehát \mathbb{G} **euklideszi** gyűrű, és így **alaptételes**.

A Gauss-prímek

Freud-Gyarmati: 7.4.15. Tétel

A Gauss-egészek között a prímek (azaz a felbonthatatlanok) az alább felsorolt számok, valamint **egységszereseik**.

A Gauss-prímek

Freud-Gyarmati: 7.4.15. Tétel

A Gauss-egészek között a prímek (azaz a felbonthatatlanok) az alább felsorolt számok, valamint **egységszereseik**.

(1) $1 + i$.

A Gauss-prímek

Freud-Gyarmati: 7.4.15. Tétel

A Gauss-egészek között a prímek (azaz a felbonthatatlanok) az alább felsorolt számok, valamint **egységszereseik**.

- (1) $1 + i$.
- (2) Minden pozitív, \mathbb{Z} -beli, $4k + 3$ alakú prímszám.

A Gauss-prímek

Freud-Gyarmati: 7.4.15. Tétel

A Gauss-egészek között a prímek (azaz a felbonthatatlanok) az alább felsorolt számok, valamint **egységszereseik**.

- (1) $1 + i$.
- (2) Minden pozitív, \mathbb{Z} -beli, $4k + 3$ alakú prímszám.
- (3) Minden pozitív, \mathbb{Z} -beli, $4k + 1$ alakú p prímszám esetén a $p = \pi_1 \pi_2$ felbontásból kapott **p normájú** π_1 és π_2 .

A Gauss-prímek

Freud-Gyarmati: 7.4.15. Tétel

A Gauss-egészek között a prímek (azaz a felbonthatatlanok) az alább felsorolt számok, valamint **egységszereseik**.

- (1) $1 + i$.
- (2) Minden pozitív, \mathbb{Z} -beli, $4k + 3$ alakú prímszám.
- (3) Minden pozitív, \mathbb{Z} -beli, $4k + 1$ alakú p prímszám esetén a $p = \pi_1 \pi_2$ felbontásból kapott **p normájú** π_1 és π_2 .

Példák

$$2 = (1 + i)(1 - i)$$

A Gauss-prímek

Freud-Gyarmati: 7.4.15. Tétel

A Gauss-egészek között a prímek (azaz a felbonthatatlanok) az alább felsorolt számok, valamint **egységszereseik**.

- (1) $1 + i$.
- (2) Minden pozitív, \mathbb{Z} -beli, $4k + 3$ alakú prímszám.
- (3) Minden pozitív, \mathbb{Z} -beli, $4k + 1$ alakú p prímszám esetén a $p = \pi_1 \pi_2$ felbontásból kapott **p normájú** π_1 és π_2 .

Példák

$$2 = (1 + i)(1 - i) = (-i)(1 + i)^2$$

A Gauss-prímek

Freud-Gyarmati: 7.4.15. Tétel

A Gauss-egészek között a prímek (azaz a felbonthatatlanok) az alább felsorolt számok, valamint **egységszereseik**.

- (1) $1 + i$.
- (2) Minden pozitív, \mathbb{Z} -beli, $4k + 3$ alakú prímszám.
- (3) Minden pozitív, \mathbb{Z} -beli, $4k + 1$ alakú p prímszám esetén a $p = \pi_1 \pi_2$ felbontásból kapott **p normájú** π_1 és π_2 .

Példák

$2 = (1 + i)(1 - i) = (-i)(1 + i)^2$ a 2 kanonikus alakja \mathbb{G} -ben.

A Gauss-prímek

Freud-Gyarmati: 7.4.15. Tétel

A Gauss-egészek között a prímek (azaz a felbonthatatlanok) az alább felsorolt számok, valamint **egységszereseik**.

- (1) $1 + i$.
- (2) Minden pozitív, \mathbb{Z} -beli, $4k + 3$ alakú prímszám.
- (3) Minden pozitív, \mathbb{Z} -beli, $4k + 1$ alakú p prímszám esetén a $p = \pi_1 \pi_2$ felbontásból kapott **p normájú** π_1 és π_2 .

Példák

$2 = (1 + i)(1 - i) = (-i)(1 + i)^2$ a 2 kanonikus alakja \mathbb{G} -ben.
 3 , -3 , $3i$, $-3i$ mind prímek a Gauss-egészek között.

A Gauss-prímek

Freud-Gyarmati: 7.4.15. Tétel

A Gauss-egészek között a prímek (azaz a felbonthatatlanok) az alább felsorolt számok, valamint **egységszereseik**.

- (1) $1 + i$.
- (2) Minden pozitív, \mathbb{Z} -beli, $4k + 3$ alakú prímszám.
- (3) Minden pozitív, \mathbb{Z} -beli, $4k + 1$ alakú p prímszám esetén a $p = \pi_1 \pi_2$ felbontásból kapott **p normájú** π_1 és π_2 .

Példák

$2 = (1 + i)(1 - i) = (-i)(1 + i)^2$ a 2 kanonikus alakja \mathbb{G} -ben.

$3, -3, 3i, -3i$ mind prímek a Gauss-egészek között.

$5 = (2 + i)(2 - i)$

A Gauss-prímek

Freud-Gyarmati: 7.4.15. Tétel

A Gauss-egészek között a prímek (azaz a felbonthatatlanok) az alább felsorolt számok, valamint **egységsszereseik**.

- (1) $1 + i$.
- (2) Minden pozitív, \mathbb{Z} -beli, $4k + 3$ alakú prímszám.
- (3) Minden pozitív, \mathbb{Z} -beli, $4k + 1$ alakú p prímszám esetén a $p = \pi_1 \pi_2$ felbontásból kapott **p normájú** π_1 és π_2 .

Példák

$2 = (1 + i)(1 - i) = (-i)(1 + i)^2$ a 2 kanonikus alakja \mathbb{G} -ben.

$3, -3, 3i, -3i$ mind prímek a Gauss-egészek között.

$5 = (2 + i)(2 - i) = (1 + 2i)(1 - 2i)$.

A Gauss-prímek

Freud-Gyarmati: 7.4.15. Tétel

A Gauss-egészek között a prímek (azaz a felbonthatatlanok) az alább felsorolt számok, valamint **egységszereseik**.

- (1) $1 + i$.
- (2) Minden pozitív, \mathbb{Z} -beli, $4k + 3$ alakú prímszám.
- (3) Minden pozitív, \mathbb{Z} -beli, $4k + 1$ alakú p prímszám esetén a $p = \pi_1 \pi_2$ felbontásból kapott **p normájú** π_1 és π_2 .

Példák

$2 = (1 + i)(1 - i) = (-i)(1 + i)^2$ a 2 kanonikus alakja \mathbb{G} -ben.

3 , -3 , $3i$, $-3i$ mind prímek a Gauss-egészek között.

$5 = (2 + i)(2 - i) = (1 + 2i)(1 - 2i)$. A $2 + i$ egységszeresei $2 + i$,

A Gauss-prímek

Freud-Gyarmati: 7.4.15. Tétel

A Gauss-egészek között a prímek (azaz a felbonthatatlanok) az alább felsorolt számok, valamint **egységszereseik**.

- (1) $1 + i$.
- (2) Minden pozitív, \mathbb{Z} -beli, $4k + 3$ alakú prímszám.
- (3) Minden pozitív, \mathbb{Z} -beli, $4k + 1$ alakú p prímszám esetén a $p = \pi_1 \pi_2$ felbontásból kapott **p normájú** π_1 és π_2 .

Példák

$2 = (1 + i)(1 - i) = (-i)(1 + i)^2$ a 2 kanonikus alakja \mathbb{G} -ben.

3 , -3 , $3i$, $-3i$ mind prímek a Gauss-egészek között.

$5 = (2 + i)(2 - i) = (1 + 2i)(1 - 2i)$. A $2 + i$ egységszeresei

$2 + i$, $-2 - i$,

A Gauss-prímek

Freud-Gyarmati: 7.4.15. Tétel

A Gauss-egészek között a prímek (azaz a felbonthatatlanok) az alább felsorolt számok, valamint **egységszereseik**.

- (1) $1 + i$.
- (2) Minden pozitív, \mathbb{Z} -beli, $4k + 3$ alakú prímszám.
- (3) Minden pozitív, \mathbb{Z} -beli, $4k + 1$ alakú p prímszám esetén a $p = \pi_1 \pi_2$ felbontásból kapott **p normájú** π_1 és π_2 .

Példák

$2 = (1 + i)(1 - i) = (-i)(1 + i)^2$ a 2 kanonikus alakja \mathbb{G} -ben.

3 , -3 , $3i$, $-3i$ mind prímek a Gauss-egészek között.

$5 = (2 + i)(2 - i) = (1 + 2i)(1 - 2i)$. A $2 + i$ egységszeresei $2 + i$, $-2 - i$, $-1 + 2i$,

A Gauss-prímek

Freud-Gyarmati: 7.4.15. Tétel

A Gauss-egészek között a prímek (azaz a felbonthatatlanok) az alább felsorolt számok, valamint **egységszereseik**.

- (1) $1 + i$.
- (2) Minden pozitív, \mathbb{Z} -beli, $4k + 3$ alakú prímszám.
- (3) Minden pozitív, \mathbb{Z} -beli, $4k + 1$ alakú p prímszám esetén a $p = \pi_1 \pi_2$ felbontásból kapott **p normájú** π_1 és π_2 .

Példák

$2 = (1 + i)(1 - i) = (-i)(1 + i)^2$ a 2 kanonikus alakja \mathbb{G} -ben.

3 , -3 , $3i$, $-3i$ mind prímek a Gauss-egészek között.

$5 = (2 + i)(2 - i) = (1 + 2i)(1 - 2i)$. A $2 + i$ egységszeresei $2 + i$, $-2 - i$, $-1 + 2i$, $1 - 2i$

A Gauss-prímek

Freud-Gyarmati: 7.4.15. Tétel

A Gauss-egészek között a prímek (azaz a felbonthatatlanok) az alább felsorolt számok, valamint **egységszereseik**.

- (1) $1 + i$.
- (2) Minden pozitív, \mathbb{Z} -beli, $4k + 3$ alakú prímszám.
- (3) Minden pozitív, \mathbb{Z} -beli, $4k + 1$ alakú p prímszám esetén a $p = \pi_1 \pi_2$ felbontásból kapott **p normájú** π_1 és π_2 .

Példák

$2 = (1 + i)(1 - i) = (-i)(1 + i)^2$ a 2 kanonikus alakja \mathbb{G} -ben.
 3 , -3 , $3i$, $-3i$ mind prímek a Gauss-egészek között.
 $5 = (2 + i)(2 - i) = (1 + 2i)(1 - 2i)$. A $2 + i$ egységszeresei $2 + i$, $-2 - i$, $-1 + 2i$, $1 - 2i$ (de $2 - i$ és $1 + 2i$ nem).

A Gauss-prímek: elégséges feltételek

Állítás

Ha $N(\alpha)$ prím \mathbb{Z} -ben,

A Gauss-prímek: elégséges feltételek

Állítás

Ha $N(\alpha)$ prím \mathbb{Z} -ben, akkor α prím

\mathbb{G} -ben.

A Gauss-prímek: elégséges feltételek

Állítás

Ha $N(\alpha)$ prím \mathbb{Z} -ben, akkor α prím (felbonthatatlan) \mathbb{G} -ben.

A Gauss-prímek: elégséges feltételek

Állítás

Ha $N(\alpha)$ prím \mathbb{Z} -ben, akkor α prím (felbonthatatlan) \mathbb{G} -ben.

Bizonyítás: $\alpha = \beta\gamma \implies N(\alpha) = N(\beta)N(\gamma) = p.$

A Gauss-prímek: elégséges feltételek

Állítás

Ha $N(\alpha)$ prím \mathbb{Z} -ben, akkor α prím (felbonthatatlan) \mathbb{G} -ben.

Bizonyítás: $\alpha = \beta\gamma \implies N(\alpha) = N(\beta)N(\gamma) = p$.

Így $N(\beta)$ és $N(\gamma)$ egyike 1,

A Gauss-prímek: elégséges feltételek

Állítás

Ha $N(\alpha)$ prím \mathbb{Z} -ben, akkor α prím (felbonthatatlan) \mathbb{G} -ben.

Bizonyítás: $\alpha = \beta\gamma \implies N(\alpha) = N(\beta)N(\gamma) = p$.

Így $N(\beta)$ és $N(\gamma)$ egyike 1, vagyis β és γ egyike egység. \square

A Gauss-prímek: elégséges feltételek

Állítás

Ha $N(\alpha)$ prím \mathbb{Z} -ben, akkor α prím (felbonthatatlan) \mathbb{G} -ben.

Bizonyítás: $\alpha = \beta\gamma \implies N(\alpha) = N(\beta)N(\gamma) = p$.

Így $N(\beta)$ és $N(\gamma)$ egyike 1, vagyis β és γ egyike egység. \square

Állítás

Ha $N(\alpha) = p^2$,

A Gauss-prímek: elégséges feltételek

Állítás

Ha $N(\alpha)$ prím \mathbb{Z} -ben, akkor α prím (felbonthatatlan) \mathbb{G} -ben.

Bizonyítás: $\alpha = \beta\gamma \implies N(\alpha) = N(\beta)N(\gamma) = p$.

Így $N(\beta)$ és $N(\gamma)$ egyike 1, vagyis β és γ egyike egység. \square

Állítás

Ha $N(\alpha) = p^2$, ahol p egy $4k + 3$ alakú prím \mathbb{Z} -ben,

A Gauss-prímek: elégséges feltételek

Állítás

Ha $N(\alpha)$ prím \mathbb{Z} -ben, akkor α prím (felbonthatatlan) \mathbb{G} -ben.

Bizonyítás: $\alpha = \beta\gamma \implies N(\alpha) = N(\beta)N(\gamma) = p$.

Így $N(\beta)$ és $N(\gamma)$ egyike 1, vagyis β és γ egyike egység. \square

Állítás

Ha $N(\alpha) = p^2$, ahol p egy $4k + 3$ alakú prím \mathbb{Z} -ben,
akkor α prím \mathbb{G} -ben.

A Gauss-prímek: elégséges feltételek

Állítás

Ha $N(\alpha)$ prím \mathbb{Z} -ben, akkor α prím (felbonthatatlan) \mathbb{G} -ben.

Bizonyítás: $\alpha = \beta\gamma \implies N(\alpha) = N(\beta)N(\gamma) = p$.

Így $N(\beta)$ és $N(\gamma)$ egyike 1, vagyis β és γ egyike egység. \square

Állítás

Ha $N(\alpha) = p^2$, ahol p egy $4k + 3$ alakú prím \mathbb{Z} -ben, akkor α prím (felbonthatatlan) \mathbb{G} -ben.

A Gauss-prímek: elégséges feltételek

Állítás

Ha $N(\alpha)$ prím \mathbb{Z} -ben, akkor α prím (felbonthatatlan) \mathbb{G} -ben.

Bizonyítás: $\alpha = \beta\gamma \implies N(\alpha) = N(\beta)N(\gamma) = p$.

Így $N(\beta)$ és $N(\gamma)$ egyike 1, vagyis β és γ egyike egység. \square

Állítás

Ha $N(\alpha) = p^2$, ahol p egy $4k + 3$ alakú prím \mathbb{Z} -ben, akkor α prím (felbonthatatlan) \mathbb{G} -ben.

Bizonyítás: $\alpha = \beta\gamma \implies N(\alpha) = N(\beta)N(\gamma) = p^2$.

A Gauss-prímek: elégséges feltételek

Állítás

Ha $N(\alpha)$ prím \mathbb{Z} -ben, akkor α prím (felbonthatatlan) \mathbb{G} -ben.

Bizonyítás: $\alpha = \beta\gamma \implies N(\alpha) = N(\beta)N(\gamma) = p$.

Így $N(\beta)$ és $N(\gamma)$ egyike 1, vagyis β és γ egyike egység. \square

Állítás

Ha $N(\alpha) = p^2$, ahol p egy $4k + 3$ alakú prím \mathbb{Z} -ben, akkor α prím (felbonthatatlan) \mathbb{G} -ben.

Bizonyítás: $\alpha = \beta\gamma \implies N(\alpha) = N(\beta)N(\gamma) = p^2$.

Ha $N(\beta)$ és $N(\gamma)$ egyike 1, akkor β és γ egyike egység.

A Gauss-prímek: elégséges feltételek

Állítás

Ha $N(\alpha)$ prím \mathbb{Z} -ben, akkor α prím (felbonthatatlan) \mathbb{G} -ben.

Bizonyítás: $\alpha = \beta\gamma \implies N(\alpha) = N(\beta)N(\gamma) = p$.

Így $N(\beta)$ és $N(\gamma)$ egyike 1, vagyis β és γ egyike egység. \square

Állítás

Ha $N(\alpha) = p^2$, ahol p egy $4k + 3$ alakú prím \mathbb{Z} -ben, akkor α prím (felbonthatatlan) \mathbb{G} -ben.

Bizonyítás: $\alpha = \beta\gamma \implies N(\alpha) = N(\beta)N(\gamma) = p^2$.

Ha $N(\beta)$ és $N(\gamma)$ egyike 1, akkor β és γ egyike egység.

Ha nem, akkor $N(\beta) = N(\gamma) = p$.

A Gauss-prímek: elégséges feltételek

Állítás

Ha $N(\alpha)$ prím \mathbb{Z} -ben, akkor α prím (felbonthatatlan) \mathbb{G} -ben.

Bizonyítás: $\alpha = \beta\gamma \implies N(\alpha) = N(\beta)N(\gamma) = p$.

Így $N(\beta)$ és $N(\gamma)$ egyike 1, vagyis β és γ egyike egység. \square

Állítás

Ha $N(\alpha) = p^2$, ahol p egy $4k + 3$ alakú prím \mathbb{Z} -ben, akkor α prím (felbonthatatlan) \mathbb{G} -ben.

Bizonyítás: $\alpha = \beta\gamma \implies N(\alpha) = N(\beta)N(\gamma) = p^2$.

Ha $N(\beta)$ és $N(\gamma)$ egyike 1, akkor β és γ egyike egység.

Ha nem, akkor $N(\beta) = N(\gamma) = p$. Legyen $\beta = u + vi$,

A Gauss-prímek: elégséges feltételek

Állítás

Ha $N(\alpha)$ prím \mathbb{Z} -ben, akkor α prím (felbonthatatlan) \mathbb{G} -ben.

Bizonyítás: $\alpha = \beta\gamma \implies N(\alpha) = N(\beta)N(\gamma) = p$.

Így $N(\beta)$ és $N(\gamma)$ egyike 1, vagyis β és γ egyike egység. \square

Állítás

Ha $N(\alpha) = p^2$, ahol p egy $4k + 3$ alakú prím \mathbb{Z} -ben, akkor α prím (felbonthatatlan) \mathbb{G} -ben.

Bizonyítás: $\alpha = \beta\gamma \implies N(\alpha) = N(\beta)N(\gamma) = p^2$.

Ha $N(\beta)$ és $N(\gamma)$ egyike 1, akkor β és γ egyike egység.

Ha nem, akkor $N(\beta) = N(\gamma) = p$. Legyen $\beta = u + vi$, akkor $u^2 + v^2 = p$.

A Gauss-prímek: elégséges feltételek

Állítás

Ha $N(\alpha)$ prím \mathbb{Z} -ben, akkor α prím (felbonthatatlan) \mathbb{G} -ben.

Bizonyítás: $\alpha = \beta\gamma \implies N(\alpha) = N(\beta)N(\gamma) = p$.

Így $N(\beta)$ és $N(\gamma)$ egyike 1, vagyis β és γ egyike egység. \square

Állítás

Ha $N(\alpha) = p^2$, ahol p egy $4k + 3$ alakú prím \mathbb{Z} -ben, akkor α prím (felbonthatatlan) \mathbb{G} -ben.

Bizonyítás: $\alpha = \beta\gamma \implies N(\alpha) = N(\beta)N(\gamma) = p^2$.

Ha $N(\beta)$ és $N(\gamma)$ egyike 1, akkor β és γ egyike egység.

Ha nem, akkor $N(\beta) = N(\gamma) = p$. Legyen $\beta = u + vi$,

akkor $u^2 + v^2 = p$. Négyzetszám 4-gyel osztva

0 vagy 1 maradékot ad,

A Gauss-prímek: elégséges feltételek

Állítás

Ha $N(\alpha)$ prím \mathbb{Z} -ben, akkor α prím (felbonthatatlan) \mathbb{G} -ben.

Bizonyítás: $\alpha = \beta\gamma \implies N(\alpha) = N(\beta)N(\gamma) = p$.

Így $N(\beta)$ és $N(\gamma)$ egyike 1, vagyis β és γ egyike egység. \square

Állítás

Ha $N(\alpha) = p^2$, ahol p egy $4k + 3$ alakú prím \mathbb{Z} -ben, akkor α prím (felbonthatatlan) \mathbb{G} -ben.

Bizonyítás: $\alpha = \beta\gamma \implies N(\alpha) = N(\beta)N(\gamma) = p^2$.

Ha $N(\beta)$ és $N(\gamma)$ egyike 1, akkor β és γ egyike egység.

Ha nem, akkor $N(\beta) = N(\gamma) = p$. Legyen $\beta = u + vi$,

akkor $u^2 + v^2 = p$. Négyzetszám 4-gyel osztva

0 vagy 1 maradékot ad, p pedig 3-at,

A Gauss-prímek: elégséges feltételek

Állítás

Ha $N(\alpha)$ prím \mathbb{Z} -ben, akkor α prím (felbonthatatlan) \mathbb{G} -ben.

Bizonyítás: $\alpha = \beta\gamma \implies N(\alpha) = N(\beta)N(\gamma) = p$.

Így $N(\beta)$ és $N(\gamma)$ egyike 1, vagyis β és γ egyike egység. \square

Állítás

Ha $N(\alpha) = p^2$, ahol p egy $4k + 3$ alakú prím \mathbb{Z} -ben, akkor α prím (felbonthatatlan) \mathbb{G} -ben.

Bizonyítás: $\alpha = \beta\gamma \implies N(\alpha) = N(\beta)N(\gamma) = p^2$.

Ha $N(\beta)$ és $N(\gamma)$ egyike 1, akkor β és γ egyike egység.

Ha nem, akkor $N(\beta) = N(\gamma) = p$. Legyen $\beta = u + vi$,

akkor $u^2 + v^2 = p$. Négyzetszám 4-gyel osztva

0 vagy 1 maradékot ad, p pedig 3-at, ez ellentmondás. \square

A Gauss-prímek: elégséges feltételek

Állítás

Ha $N(\alpha)$ prím \mathbb{Z} -ben, akkor α prím (felbonthatatlan) \mathbb{G} -ben.

Bizonyítás: $\alpha = \beta\gamma \implies N(\alpha) = N(\beta)N(\gamma) = p$.

Így $N(\beta)$ és $N(\gamma)$ egyike 1, vagyis β és γ egyike egység. \square

Állítás

Ha $N(\alpha) = p^2$, ahol p egy $4k + 3$ alakú prím \mathbb{Z} -ben, akkor α prím (felbonthatatlan) \mathbb{G} -ben.

Bizonyítás: $\alpha = \beta\gamma \implies N(\alpha) = N(\beta)N(\gamma) = p^2$.

Ha $N(\beta)$ és $N(\gamma)$ egyike 1, akkor β és γ egyike egység.

Ha nem, akkor $N(\beta) = N(\gamma) = p$. Legyen $\beta = u + vi$,

akkor $u^2 + v^2 = p$. Négyzetszám 4-gyel osztva

0 vagy 1 maradékot ad, p pedig 3-at, ez ellentmondás. \square

Beláttuk: a tételbeli számok Gauss-prímek.

A Gauss-prímek: a Wilson-tétel felhasználása

Wilson tétele (FGy: 2.7.1. Tétel)

Ha $p > 0$ prímszám \mathbb{Z} -ben, akkor $(p - 1)! \equiv -1 \pmod{p}$.

A Gauss-prímek: a Wilson-tétel felhasználása

Wilson tétele (FGy: 2.7.1. Tétel)

Ha $p > 0$ prímszám \mathbb{Z} -ben, akkor $(p - 1)! \equiv -1 \pmod{p}$.

Állítás

Ha p egy $4k + 1$ alakú prím \mathbb{Z} -ben,

A Gauss-prímek: a Wilson-tétel felhasználása

Wilson tétele (FGy: 2.7.1. Tétel)

Ha $p > 0$ prímszám \mathbb{Z} -ben, akkor $(p - 1)! \equiv -1 \pmod{p}$.

Állítás

Ha p egy $4k + 1$ alakú prím \mathbb{Z} -ben, akkor p **nem** prím \mathbb{G} -ben.

A Gauss-prímek: a Wilson-tétel felhasználása

Wilson tétele (FGy: 2.7.1. Tétel)

Ha $p > 0$ prímszám \mathbb{Z} -ben, akkor $(p - 1)! \equiv -1 \pmod{p}$.

Állítás

Ha p egy $4k + 1$ alakú prím \mathbb{Z} -ben, akkor p **nem** prím \mathbb{G} -ben.

Bizonyítás

Párosítsuk j -t $p-j$ -vel.

A Gauss-prímek: a Wilson-tétel felhasználása

Wilson tétele (FGy: 2.7.1. Tétel)

Ha $p > 0$ prímszám \mathbb{Z} -ben, akkor $(p - 1)! \equiv -1 \pmod{p}$.

Állítás

Ha p egy $4k + 1$ alakú prím \mathbb{Z} -ben, akkor p **nem** prím \mathbb{G} -ben.

Bizonyítás

Párosítsuk j -t $p-j$ -vel. Mivel $4 \mid p - 1$, senki sem önmaga párja.

A Gauss-prímek: a Wilson-tétel felhasználása

Wilson tétele (FGy: 2.7.1. Tétel)

Ha $p > 0$ prímszám \mathbb{Z} -ben, akkor $(p - 1)! \equiv -1 \pmod{p}$.

Állítás

Ha p egy $4k + 1$ alakú prím \mathbb{Z} -ben, akkor p **nem** prím \mathbb{G} -ben.

Bizonyítás

Párosítsuk j -t $p-j$ -vel. Mivel $4 \mid p - 1$, senki sem önmaga párja.

$$(p - 1)! \equiv ((p - 1)/2)! \cdot ((p - 1)/2)! \cdot (-1)^{(p-1)/2} \pmod{p}$$

A Gauss-prímek: a Wilson-tétel felhasználása

Wilson tétele (FGy: 2.7.1. Tétel)

Ha $p > 0$ prímszám \mathbb{Z} -ben, akkor $(p - 1)! \equiv -1 \pmod{p}$.

Állítás

Ha p egy $4k + 1$ alakú prím \mathbb{Z} -ben, akkor p **nem** prím \mathbb{G} -ben.

Bizonyítás

Párosítsuk j -t $p-j$ -vel. Mivel $4 \mid p - 1$, senki sem önmaga párja.

$$(p - 1)! \equiv ((p - 1)/2)! \cdot ((p - 1)/2)! \cdot (-1)^{(p-1)/2} \pmod{p}$$

Legyen $x = ((p - 1)/2)!$,

A Gauss-prímek: a Wilson-tétel felhasználása

Wilson tétele (FGy: 2.7.1. Tétel)

Ha $p > 0$ prímszám \mathbb{Z} -ben, akkor $(p - 1)! \equiv -1 \pmod{p}$.

Állítás

Ha p egy $4k + 1$ alakú prím \mathbb{Z} -ben, akkor p **nem** prím \mathbb{G} -ben.

Bizonyítás

Párosítsuk j -t $p-j$ -vel. Mivel $4 \mid p - 1$, senki sem önmaga párja.

$$(p - 1)! \equiv ((p - 1)/2)! \cdot ((p - 1)/2)! \cdot (-1)^{(p-1)/2} \pmod{p}$$

Legyen $x = ((p - 1)/2)!$, akkor tehát $p \mid x^2 + 1 = (x + i)(x - i)$.

A Gauss-prímek: a Wilson-tétel felhasználása

Wilson tétele (FGy: 2.7.1. Tétel)

Ha $p > 0$ prímszám \mathbb{Z} -ben, akkor $(p - 1)! \equiv -1 \pmod{p}$.

Állítás

Ha p egy $4k + 1$ alakú prím \mathbb{Z} -ben, akkor p **nem** prím \mathbb{G} -ben.

Bizonyítás

Párosítsuk j -t $p-j$ -vel. Mivel $4 \mid p - 1$, senki sem önmaga párja.

$$(p - 1)! \equiv ((p - 1)/2)! \cdot ((p - 1)/2)! \cdot (-1)^{(p-1)/2} \pmod{p}$$

Legyen $x = ((p - 1)/2)!$, akkor tehát $p \mid x^2 + 1 = (x + i)(x - i)$.

Ha p Gauss-prím lenne, akkor innen $p \mid x + i$ vagy $p \mid x - i$.

A Gauss-prímek: a Wilson-tétel felhasználása

Wilson tétele (FGy: 2.7.1. Tétel)

Ha $p > 0$ prímszám \mathbb{Z} -ben, akkor $(p - 1)! \equiv -1 \pmod{p}$.

Állítás

Ha p egy $4k + 1$ alakú prím \mathbb{Z} -ben, akkor p **nem** prím \mathbb{G} -ben.

Bizonyítás

Párosítsuk j -t $p-j$ -vel. Mivel $4 \mid p - 1$, senki sem önmaga párja.

$$(p - 1)! \equiv ((p - 1)/2)! \cdot ((p - 1)/2)! \cdot (-1)^{(p-1)/2} \pmod{p}$$

Legyen $x = ((p - 1)/2)!$, akkor tehát $p \mid x^2 + 1 = (x + i)(x - i)$.

Ha p Gauss-prím lenne, akkor innen $p \mid x + i$ vagy $p \mid x - i$.

Egyik sem igaz, mert $p(a + bi) = x \pm i$ -ből $pb = \pm 1$ következne.

A Gauss-prímek: a Wilson-tétel felhasználása

Wilson tétele (FGy: 2.7.1. Tétel)

Ha $p > 0$ prímszám \mathbb{Z} -ben, akkor $(p - 1)! \equiv -1 \pmod{p}$.

Állítás

Ha p egy $4k + 1$ alakú prím \mathbb{Z} -ben, akkor p **nem** prím \mathbb{G} -ben.

Bizonyítás

Párosítsuk j -t $p-j$ -vel. Mivel $4 \mid p - 1$, senki sem önmaga párja.

$$(p - 1)! \equiv ((p - 1)/2)! \cdot ((p - 1)/2)! \cdot (-1)^{(p-1)/2} \pmod{p}$$

Legyen $x = ((p - 1)/2)!$, akkor tehát $p \mid x^2 + 1 = (x + i)(x - i)$.

Ha p Gauss-prím lenne, akkor innen $p \mid x + i$ vagy $p \mid x - i$.

Egyik sem igaz, mert $p(a + bi) = x \pm i$ -ből $pb = \pm 1$ következne.

Azaz $p \mid \pm 1$, ez ellentmondás. □

A Gauss-prímek: a szükségesség bizonyítása

Tegyük föl, hogy α Gauss-prím.

A Gauss-prímek: a szükségesség bizonyítása

Tegyük föl, hogy α Gauss-prím. Ekkor $\alpha \mid \alpha\bar{\alpha} = N(\alpha) \in \mathbb{Z}$.

A Gauss-prímek: a szükségesség bizonyítása

Tegyük föl, hogy α Gauss-prím. Ekkor $\alpha \mid \alpha\bar{\alpha} = N(\alpha) \in \mathbb{Z}$.
Bontsuk $N(\alpha)$ -t \mathbb{Z} -ben prímszámok szorzatára.

A Gauss-prímek: a szükségesség bizonyítása

Tegyük föl, hogy α Gauss-prím. Ekkor $\alpha \mid \alpha\bar{\alpha} = N(\alpha) \in \mathbb{Z}$.
Bontsuk $N(\alpha)$ -t \mathbb{Z} -ben prímszámok szorzatára.
Mivel α Gauss-prím, valamelyik tényezőnek osztója lesz.

A Gauss-prímek: a szükségesség bizonyítása

Tegyük föl, hogy α Gauss-prím. Ekkor $\alpha \mid \alpha\bar{\alpha} = N(\alpha) \in \mathbb{Z}$.
Bontsuk $N(\alpha)$ -t \mathbb{Z} -ben prímszámok szorzatára.
Mivel α Gauss-prím, valamelyik tényezőnek osztója lesz.
Azaz $\alpha \mid p$ alkalmas \mathbb{Z} -beli pozitív p prímre.

A Gauss-prímek: a szükségesség bizonyítása

Tegyük föl, hogy α Gauss-prím. Ekkor $\alpha \mid \alpha\bar{\alpha} = N(\alpha) \in \mathbb{Z}$.

Bontsuk $N(\alpha)$ -t \mathbb{Z} -ben prímszámok szorzatára.

Mivel α Gauss-prím, valamelyik tényezőnek osztója lesz.

Azaz $\alpha \mid p$ alkalmas \mathbb{Z} -beli pozitív p prímre.

Ha $p = 2$

A Gauss-prímek: a szükségesség bizonyítása

Tegyük föl, hogy α Gauss-prím. Ekkor $\alpha \mid \alpha\bar{\alpha} = N(\alpha) \in \mathbb{Z}$.

Bontsuk $N(\alpha)$ -t \mathbb{Z} -ben prímszámok szorzatára.

Mivel α Gauss-prím, valamelyik tényezőnek osztója lesz.

Azaz $\alpha \mid p$ alkalmas \mathbb{Z} -beli pozitív p prímre.

Ha $p = 2 = (1 + i)(1 - i)$

A Gauss-prímek: a szükségesség bizonyítása

Tegyük föl, hogy α Gauss-prím. Ekkor $\alpha \mid \alpha\bar{\alpha} = N(\alpha) \in \mathbb{Z}$.

Bontsuk $N(\alpha)$ -t \mathbb{Z} -ben prímszámok szorzatára.

Mivel α Gauss-prím, valamelyik tényezőnek osztója lesz.

Azaz $\alpha \mid p$ alkalmas \mathbb{Z} -beli pozitív p prímre.

Ha $p = 2 = (1 + i)(1 - i) = (-i)(1 + i)^2$,

A Gauss-prímek: a szükségesség bizonyítása

Tegyük föl, hogy α Gauss-prím. Ekkor $\alpha \mid \alpha\bar{\alpha} = N(\alpha) \in \mathbb{Z}$.

Bontsuk $N(\alpha)$ -t \mathbb{Z} -ben prímszámok szorzatára.

Mivel α Gauss-prím, valamelyik tényezőnek osztója lesz.

Azaz $\alpha \mid p$ alkalmas \mathbb{Z} -beli pozitív p prímre.

Ha $p = 2 = (1 + i)(1 - i) = (-i)(1 + i)^2$, akkor $\alpha \mid 1 + i$.

A Gauss-prímek: a szükségesség bizonyítása

Tegyük föl, hogy α Gauss-prím. Ekkor $\alpha \mid \alpha\bar{\alpha} = N(\alpha) \in \mathbb{Z}$.

Bontsuk $N(\alpha)$ -t \mathbb{Z} -ben prímszámok szorzatára.

Mivel α Gauss-prím, valamelyik tényezőnek osztója lesz.

Azaz $\alpha \mid p$ alkalmas \mathbb{Z} -beli pozitív p prímre.

Ha $p = 2 = (1 + i)(1 - i) = (-i)(1 + i)^2$, akkor $\alpha \mid 1 + i$.

Mivel $1 + i$ Gauss-prím, ezért α az $1 + i$ egységszerese.

A Gauss-prímek: a szükségesség bizonyítása

Tegyük föl, hogy α Gauss-prím. Ekkor $\alpha \mid \alpha\bar{\alpha} = N(\alpha) \in \mathbb{Z}$.

Bontsuk $N(\alpha)$ -t \mathbb{Z} -ben prímszámok szorzatára.

Mivel α Gauss-prím, valamelyik tényezőnek osztója lesz.

Azaz $\alpha \mid p$ alkalmas \mathbb{Z} -beli pozitív p prímre.

Ha $p = 2 = (1 + i)(1 - i) = (-i)(1 + i)^2$, akkor $\alpha \mid 1 + i$.

Mivel $1 + i$ Gauss-prím, ezért α az $1 + i$ egységszerese.

Ha $p \equiv 3 \pmod{4}$, akkor p prím \mathbb{G} -ben,

A Gauss-prímek: a szükségesség bizonyítása

Tegyük föl, hogy α Gauss-prím. Ekkor $\alpha \mid \alpha\bar{\alpha} = N(\alpha) \in \mathbb{Z}$.

Bontsuk $N(\alpha)$ -t \mathbb{Z} -ben prímszámok szorzatára.

Mivel α Gauss-prím, valamelyik tényezőnek osztója lesz.

Azaz $\alpha \mid p$ alkalmas \mathbb{Z} -beli pozitív p prímre.

Ha $p = 2 = (1 + i)(1 - i) = (-i)(1 + i)^2$, akkor $\alpha \mid 1 + i$.

Mivel $1 + i$ Gauss-prím, ezért α az $1 + i$ egységszerese.

Ha $p \equiv 3 \pmod{4}$, akkor p prím \mathbb{G} -ben, és α a p egységszerese.

A Gauss-prímek: a szükségesség bizonyítása

Tegyük föl, hogy α Gauss-prím. Ekkor $\alpha \mid \alpha\bar{\alpha} = N(\alpha) \in \mathbb{Z}$.

Bontsuk $N(\alpha)$ -t \mathbb{Z} -ben prímszámok szorzatára.

Mivel α Gauss-prím, valamelyik tényezőnek osztója lesz.

Azaz $\alpha \mid p$ alkalmas \mathbb{Z} -beli pozitív p prímre.

Ha $p = 2 = (1 + i)(1 - i) = (-i)(1 + i)^2$, akkor $\alpha \mid 1 + i$.

Mivel $1 + i$ Gauss-prím, ezért α az $1 + i$ egységszerese.

Ha $p \equiv 3 \pmod{4}$, akkor p prím \mathbb{G} -ben, és α a p egységszerese.

Ha $p \equiv 1 \pmod{4}$, akkor p **nem** Gauss-prím.

A Gauss-prímek: a szükségesség bizonyítása

Tegyük föl, hogy α Gauss-prím. Ekkor $\alpha \mid \alpha\bar{\alpha} = N(\alpha) \in \mathbb{Z}$.

Bontsuk $N(\alpha)$ -t \mathbb{Z} -ben prímszámok szorzatára.

Mivel α Gauss-prím, valamelyik tényezőnek osztója lesz.

Azaz $\alpha \mid p$ alkalmas \mathbb{Z} -beli pozitív p prímre.

Ha $p = 2 = (1 + i)(1 - i) = (-i)(1 + i)^2$, akkor $\alpha \mid 1 + i$.

Mivel $1 + i$ Gauss-prím, ezért α az $1 + i$ egységszerese.

Ha $p \equiv 3 \pmod{4}$, akkor p prím \mathbb{G} -ben, és α a p egységszerese.

Ha $p \equiv 1 \pmod{4}$, akkor p **nem** Gauss-prím.

Mivel normája p^2 , csakis két Gauss-prím szorzatára bomolhat.

A Gauss-prímek: a szükségesség bizonyítása

Tegyük föl, hogy α Gauss-prím. Ekkor $\alpha \mid \alpha\bar{\alpha} = N(\alpha) \in \mathbb{Z}$.

Bontsuk $N(\alpha)$ -t \mathbb{Z} -ben prímszámok szorzatára.

Mivel α Gauss-prím, valamelyik tényezőnek osztója lesz.

Azaz $\alpha \mid p$ alkalmas \mathbb{Z} -beli pozitív p prímre.

Ha $p = 2 = (1 + i)(1 - i) = (-i)(1 + i)^2$, akkor $\alpha \mid 1 + i$.

Mivel $1 + i$ Gauss-prím, ezért α az $1 + i$ egységszerese.

Ha $p \equiv 3 \pmod{4}$, akkor p prím \mathbb{G} -ben, és α a p egységszerese.

Ha $p \equiv 1 \pmod{4}$, akkor p **nem** Gauss-prím.

Mivel normája p^2 , csakis két Gauss-prím szorzatára bomolhat.

Valóban, ha $p = \pi_1 \dots \pi_k$,

A Gauss-prímek: a szükségesség bizonyítása

Tegyük föl, hogy α Gauss-prím. Ekkor $\alpha \mid \alpha\bar{\alpha} = N(\alpha) \in \mathbb{Z}$.

Bontsuk $N(\alpha)$ -t \mathbb{Z} -ben prímszámok szorzatára.

Mivel α Gauss-prím, valamelyik tényezőnek osztója lesz.

Azaz $\alpha \mid p$ alkalmas \mathbb{Z} -beli pozitív p prímre.

Ha $p = 2 = (1 + i)(1 - i) = (-i)(1 + i)^2$, akkor $\alpha \mid 1 + i$.

Mivel $1 + i$ Gauss-prím, ezért α az $1 + i$ egységszerese.

Ha $p \equiv 3 \pmod{4}$, akkor p prím \mathbb{G} -ben, és α a p egységszerese.

Ha $p \equiv 1 \pmod{4}$, akkor p **nem** Gauss-prím.

Mivel normája p^2 , csakis két Gauss-prím szorzatára bomolhat.

Valóban, ha $p = \pi_1 \dots \pi_k$, akkor $p^2 = N(p) = N(\pi_1) \dots N(\pi_k)$.

A Gauss-prímek: a szükségesség bizonyítása

Tegyük föl, hogy α Gauss-prím. Ekkor $\alpha \mid \alpha\bar{\alpha} = N(\alpha) \in \mathbb{Z}$.
Bontuk $N(\alpha)$ -t \mathbb{Z} -ben prímszámok szorzatára.

Mivel α Gauss-prím, valamelyik tényezőnek osztója lesz.

Azaz $\alpha \mid p$ alkalmas \mathbb{Z} -beli pozitív p prímre.

Ha $p = 2 = (1 + i)(1 - i) = (-i)(1 + i)^2$, akkor $\alpha \mid 1 + i$.

Mivel $1 + i$ Gauss-prím, ezért α az $1 + i$ egységszerese.

Ha $p \equiv 3 \pmod{4}$, akkor p prím \mathbb{G} -ben, és α a p egységszerese.

Ha $p \equiv 1 \pmod{4}$, akkor p **nem** Gauss-prím.

Mivel normája p^2 , csakis két Gauss-prím szorzatára bomolhat.

Valóban, ha $p = \pi_1 \dots \pi_k$, akkor $p^2 = N(p) = N(\pi_1) \dots N(\pi_k)$.

Ezért csak két darab nem egység tényező lehet.

A Gauss-prímek: a szükségesség bizonyítása

Tegyük föl, hogy α Gauss-prím. Ekkor $\alpha \mid \alpha\bar{\alpha} = N(\alpha) \in \mathbb{Z}$.
Bontuk $N(\alpha)$ -t \mathbb{Z} -ben prímszámok szorzatára.

Mivel α Gauss-prím, valamelyik tényezőnek osztója lesz.

Azaz $\alpha \mid p$ alkalmas \mathbb{Z} -beli pozitív p prímre.

Ha $p = 2 = (1 + i)(1 - i) = (-i)(1 + i)^2$, akkor $\alpha \mid 1 + i$.

Mivel $1 + i$ Gauss-prím, ezért α az $1 + i$ egységszerese.

Ha $p \equiv 3 \pmod{4}$, akkor p prím \mathbb{G} -ben, és α a p egységszerese.

Ha $p \equiv 1 \pmod{4}$, akkor p **nem** Gauss-prím.

Mivel normája p^2 , csakis két Gauss-prím szorzatára bomolhat.

Valóban, ha $p = \pi_1 \dots \pi_k$, akkor $p^2 = N(p) = N(\pi_1) \dots N(\pi_k)$.

Ezért csak két darab nem egység tényező lehet.

Ekkor $\alpha \mid p = \pi_1 \pi_2$

A Gauss-prímek: a szükségesség bizonyítása

Tegyük föl, hogy α Gauss-prím. Ekkor $\alpha \mid \alpha\bar{\alpha} = N(\alpha) \in \mathbb{Z}$.
Bontsuk $N(\alpha)$ -t \mathbb{Z} -ben prímszámok szorzatára.

Mivel α Gauss-prím, valamelyik tényezőnek osztója lesz.

Azaz $\alpha \mid p$ alkalmas \mathbb{Z} -beli pozitív p prímre.

Ha $p = 2 = (1 + i)(1 - i) = (-i)(1 + i)^2$, akkor $\alpha \mid 1 + i$.

Mivel $1 + i$ Gauss-prím, ezért α az $1 + i$ egységszerese.

Ha $p \equiv 3 \pmod{4}$, akkor p prím \mathbb{G} -ben, és α a p egységszerese.

Ha $p \equiv 1 \pmod{4}$, akkor p **nem** Gauss-prím.

Mivel normája p^2 , csakis két Gauss-prím szorzatára bomolhat.

Valóban, ha $p = \pi_1 \dots \pi_k$, akkor $p^2 = N(p) = N(\pi_1) \dots N(\pi_k)$.

Ezért csak két darab nem egység tényező lehet.

Ekkor $\alpha \mid p = \pi_1\pi_2$ miatt $\alpha \mid \pi_1$ vagy $\alpha \mid \pi_2$.

A Gauss-prímek: a szükségesség bizonyítása

Tegyük föl, hogy α Gauss-prím. Ekkor $\alpha \mid \alpha\bar{\alpha} = N(\alpha) \in \mathbb{Z}$.
Bontsuk $N(\alpha)$ -t \mathbb{Z} -ben prímszámok szorzatára.

Mivel α Gauss-prím, valamelyik tényezőnek osztója lesz.

Azaz $\alpha \mid p$ alkalmas \mathbb{Z} -beli pozitív p prímre.

Ha $p = 2 = (1 + i)(1 - i) = (-i)(1 + i)^2$, akkor $\alpha \mid 1 + i$.

Mivel $1 + i$ Gauss-prím, ezért α az $1 + i$ egységszerese.

Ha $p \equiv 3 \pmod{4}$, akkor p prím \mathbb{G} -ben, és α a p egységszerese.

Ha $p \equiv 1 \pmod{4}$, akkor p **nem** Gauss-prím.

Mivel normája p^2 , csakis két Gauss-prím szorzatára bomolhat.

Valóban, ha $p = \pi_1 \dots \pi_k$, akkor $p^2 = N(p) = N(\pi_1) \dots N(\pi_k)$.

Ezért csak két darab nem egység tényező lehet.

Ekkor $\alpha \mid p = \pi_1\pi_2$ miatt $\alpha \mid \pi_1$ vagy $\alpha \mid \pi_2$.

Így α a π_1 vagy a π_2 egységszerese. □

A tétel kimondása

Freud-Gyarmati: 7.5.1. Tétel

Egy pozitív egész szám akkor és csak akkor áll elő két négyzetszám összegeként,

A tétel kimondása

Freud-Gyarmati: 7.5.1. Tétel

Egy pozitív egész szám akkor és csak akkor áll elő két négyzetszám összegeként, ha **minden $4k + 3$ alakú prím páros kitevőn** szerepel benne.

A tétel kimondása

Freud-Gyarmati: 7.5.1. Tétel

Egy pozitív egész szám akkor és csak akkor áll elő két négyzetszám összegeként, ha **minden $4k + 3$ alakú prím páros kitevőn** szerepel benne. Ha $n = 2^\alpha p_1^{\beta_1} \dots p_m^{\beta_m} q_1^{\gamma_1} \dots q_\ell^{\gamma_\ell}$,

A tétel kimondása

Freud-Gyarmati: 7.5.1. Tétel

Egy pozitív egész szám akkor és csak akkor áll elő két négyzetszám összegeként, ha **minden $4k + 3$ alakú prím páros kitevőn** szerepel benne. Ha $n = 2^\alpha p_1^{\beta_1} \dots p_m^{\beta_m} q_1^{\gamma_1} \dots q_\ell^{\gamma_\ell}$, ahol $p_i \equiv 1 \pmod{4}$

A tétel kimondása

Freud-Gyarmati: 7.5.1. Tétel

Egy pozitív egész szám akkor és csak akkor áll elő két négyzetszám összegeként, ha **minden $4k + 3$ alakú prím páros kitevőn** szerepel benne. Ha $n = 2^\alpha p_1^{\beta_1} \dots p_m^{\beta_m} q_1^{\gamma_1} \dots q_\ell^{\gamma_\ell}$, ahol $p_i \equiv 1 \pmod{4}$ és $q_j \equiv 3 \pmod{4}$,

A tétel kimondása

Freud-Gyarmati: 7.5.1. Tétel

Egy pozitív egész szám akkor és csak akkor áll elő két négyzetszám összegeként, ha **minden $4k + 3$ alakú prím páros kitevőn** szerepel benne. Ha $n = 2^\alpha p_1^{\beta_1} \dots p_m^{\beta_m} q_1^{\gamma_1} \dots q_\ell^{\gamma_\ell}$, ahol $p_i \equiv 1 \pmod{4}$ és $q_j \equiv 3 \pmod{4}$, akkor a megoldások száma

A tétel kimondása

Freud-Gyarmati: 7.5.1. Tétel

Egy pozitív egész szám akkor és csak akkor áll elő két négyzetszám összegeként, ha **minden $4k + 3$ alakú prím páros kitevőn** szerepel benne. Ha $n = 2^\alpha p_1^{\beta_1} \dots p_m^{\beta_m} q_1^{\gamma_1} \dots q_\ell^{\gamma_\ell}$, ahol $p_i \equiv 1 \pmod{4}$ és $q_j \equiv 3 \pmod{4}$, akkor a megoldások száma (vagyis azon (x, y) számpárok száma, melyekre $x^2 + y^2 = n$)

A tétel kimondása

Freud-Gyarmati: 7.5.1. Tétel

Egy pozitív egész szám akkor és csak akkor áll elő két négyzetszám összegeként, ha **minden $4k + 3$ alakú prím páros kitevőn** szerepel benne. Ha $n = 2^\alpha p_1^{\beta_1} \dots p_m^{\beta_m} q_1^{\gamma_1} \dots q_\ell^{\gamma_\ell}$, ahol $p_i \equiv 1 \pmod{4}$ és $q_j \equiv 3 \pmod{4}$, akkor a megoldások száma (vagyis azon (x, y) számpárok száma, melyekre $x^2 + y^2 = n$) pontosan $4(\beta_1 + 1) \dots (\beta_m + 1)$.

A tétel kimondása

Freud-Gyarmati: 7.5.1. Tétel

Egy pozitív egész szám akkor és csak akkor áll elő két négyzetszám összegeként, ha **minden $4k + 3$ alakú prím páros kitevőn** szerepel benne. Ha $n = 2^\alpha p_1^{\beta_1} \dots p_m^{\beta_m} q_1^{\gamma_1} \dots q_\ell^{\gamma_\ell}$, ahol $p_i \equiv 1 \pmod{4}$ és $q_j \equiv 3 \pmod{4}$, akkor a megoldások száma (vagyis azon (x, y) számpárok száma, melyekre $x^2 + y^2 = n$) pontosan $4(\beta_1 + 1) \dots (\beta_m + 1)$.

Példák

A **15** nem áll elő, mert a 3 az első kitevőn szerepel.

A tétel kimondása

Freud-Gyarmati: 7.5.1. Tétel

Egy pozitív egész szám akkor és csak akkor áll elő két négyzetszám összegeként, ha **minden $4k + 3$ alakú prím páros kitevőn** szerepel benne. Ha $n = 2^\alpha p_1^{\beta_1} \dots p_m^{\beta_m} q_1^{\gamma_1} \dots q_\ell^{\gamma_\ell}$, ahol $p_i \equiv 1 \pmod{4}$ és $q_j \equiv 3 \pmod{4}$, akkor a megoldások száma (vagyis azon (x, y) számpárok száma, melyekre $x^2 + y^2 = n$) pontosan $4(\beta_1 + 1) \dots (\beta_m + 1)$.

Példák

A **15** nem áll elő, mert a 3 az első kitevőn szerepel.
Valóban, $0^2 + 15 = 1^2 + 14 = 2^2 + 11 = 3^2 + 6$ egyike sem jó.

A tétel kimondása

Freud-Gyarmati: 7.5.1. Tétel

Egy pozitív egész szám akkor és csak akkor áll elő két négyzetszám összegeként, ha **minden $4k + 3$ alakú prím páros kitevőn** szerepel benne. Ha $n = 2^\alpha p_1^{\beta_1} \dots p_m^{\beta_m} q_1^{\gamma_1} \dots q_\ell^{\gamma_\ell}$, ahol $p_i \equiv 1 \pmod{4}$ és $q_j \equiv 3 \pmod{4}$, akkor a megoldások száma (vagyis azon (x, y) számpárok száma, melyekre $x^2 + y^2 = n$) pontosan $4(\beta_1 + 1) \dots (\beta_m + 1)$.

Példák

A **15** nem áll elő, mert a 3 az első kitevőn szerepel. Valóban, $0^2 + 15 = 1^2 + 14 = 2^2 + 11 = 3^2 + 6$ egyike sem jó. **90** = $2 \cdot 5 \cdot 3^2$ előállításainak száma $4(1 + 1) = 8$.

A tétel kimondása

Freud-Gyarmati: 7.5.1. Tétel

Egy pozitív egész szám akkor és csak akkor áll elő két négyzetszám összegeként, ha **minden $4k + 3$ alakú prím páros kitevőn** szerepel benne. Ha $n = 2^\alpha p_1^{\beta_1} \dots p_m^{\beta_m} q_1^{\gamma_1} \dots q_\ell^{\gamma_\ell}$, ahol $p_i \equiv 1 \pmod{4}$ és $q_j \equiv 3 \pmod{4}$, akkor a megoldások száma (vagyis azon (x, y) számpárok száma, melyekre $x^2 + y^2 = n$) pontosan $4(\beta_1 + 1) \dots (\beta_m + 1)$.

Példák

A **15** nem áll elő, mert a 3 az első kitevőn szerepel. Valóban, $0^2 + 15 = 1^2 + 14 = 2^2 + 11 = 3^2 + 6$ egyike sem jó. **90** = $2 \cdot 5 \cdot 3^2$ előállításainak száma $4(1 + 1) = 8$. Ezek $(\pm 3)^2 + (\pm 9)^2$ (ez 4 darab),

A tétel kimondása

Freud-Gyarmati: 7.5.1. Tétel

Egy pozitív egész szám akkor és csak akkor áll elő két négyzetszám összegeként, ha **minden $4k + 3$ alakú prím páros kitevőn** szerepel benne. Ha $n = 2^\alpha p_1^{\beta_1} \dots p_m^{\beta_m} q_1^{\gamma_1} \dots q_\ell^{\gamma_\ell}$, ahol $p_i \equiv 1 \pmod{4}$ és $q_j \equiv 3 \pmod{4}$, akkor a megoldások száma (vagyis azon (x, y) számpárok száma, melyekre $x^2 + y^2 = n$) pontosan $4(\beta_1 + 1) \dots (\beta_m + 1)$.

Példák

A **15** nem áll elő, mert a 3 az első kitevőn szerepel. Valóban, $0^2 + 15 = 1^2 + 14 = 2^2 + 11 = 3^2 + 6$ egyike sem jó. **90** $= 2 \cdot 5 \cdot 3^2$ előállításainak száma $4(1 + 1) = 8$. Ezek $(\pm 3)^2 + (\pm 9)^2$ (ez 4 darab), továbbá $(\pm 9)^2 + (\pm 3)^2$ (ez is 4 darab).

A tétel bizonyítása

Ha $n = x^2 + y^2$, akkor írjuk $x + iy$ -t Gauss-prímek szorzataként.

A tétel bizonyítása

Ha $n = x^2 + y^2$, akkor írjuk $x + iy$ -t Gauss-prímek szorzataként.

$$x + iy = \varepsilon(1 + i)^\delta \pi_1^{\theta_1} \dots \pi_u^{\theta_u} r_1^{\sigma_1} \dots r_v^{\sigma_v} .$$

A tétel bizonyítása

Ha $n = x^2 + y^2$, akkor írjuk $x + iy$ -t Gauss-prímek szorzataként.

$$x + iy = \varepsilon(1 + i)^\delta \pi_1^{\theta_1} \dots \pi_u^{\theta_u} r_1^{\sigma_1} \dots r_v^{\sigma_v}.$$

Itt ε egység,

A tétel bizonyítása

Ha $n = x^2 + y^2$, akkor írjuk $x + iy$ -t Gauss-prímek szorzataként.

$$x + iy = \varepsilon(1 + i)^\delta \pi_1^{\theta_1} \dots \pi_u^{\theta_u} r_1^{\sigma_1} \dots r_v^{\sigma_v}.$$

Itt ε egység, $r_j \in \mathbb{Z}$ $4k + 3$ alakú prím,

A tétel bizonyítása

Ha $n = x^2 + y^2$, akkor írjuk $x + iy$ -t Gauss-prímek szorzataként.

$$x + iy = \varepsilon(1 + i)^\delta \pi_1^{\theta_1} \dots \pi_u^{\theta_u} r_1^{\sigma_1} \dots r_v^{\sigma_v}.$$

Itt ε egység, $r_j \in \mathbb{Z}$ $4k + 3$ alakú prím, $N(\pi_j)$ $4k + 1$ alakú prím.

A tétel bizonyítása

Ha $n = x^2 + y^2$, akkor írjuk $x + iy$ -t Gauss-prímek szorzataként.

$$x + iy = \varepsilon(1 + i)^\delta \pi_1^{\theta_1} \dots \pi_u^{\theta_u} r_1^{\sigma_1} \dots r_v^{\sigma_v}.$$

Itt ε egység, $r_j \in \mathbb{Z}$ $4k + 3$ alakú prím, $N(\pi_i)$ $4k + 1$ alakú prím.

Mindkét oldalt konjugálva

$$x - iy = \bar{\varepsilon}(1 - i)^\delta \bar{\pi}_1^{\theta_1} \dots \bar{\pi}_u^{\theta_u} r_1^{\sigma_1} \dots r_v^{\sigma_v}.$$

A tétel bizonyítása

Ha $n = x^2 + y^2$, akkor írjuk $x + iy$ -t Gauss-prímek szorzataként.

$$x + iy = \varepsilon(1 + i)^\delta \pi_1^{\theta_1} \dots \pi_u^{\theta_u} r_1^{\sigma_1} \dots r_v^{\sigma_v}.$$

Itt ε egység, $r_j \in \mathbb{Z}$ $4k + 3$ alakú prím, $N(\pi_i)$ $4k + 1$ alakú prím.

Mindkét oldalt konjugálva

$$x - iy = \bar{\varepsilon}(1 - i)^\delta \bar{\pi}_1^{\theta_1} \dots \bar{\pi}_u^{\theta_u} r_1^{\sigma_1} \dots r_v^{\sigma_v}.$$

Ezeket összeszorozva $n = (x + iy)(x - iy)$ felbontását kapjuk.

A tétel bizonyítása

Ha $n = x^2 + y^2$, akkor írjuk $x + iy$ -t Gauss-prímek szorzataként.

$$x + iy = \varepsilon(1 + i)^\delta \pi_1^{\theta_1} \dots \pi_u^{\theta_u} r_1^{\sigma_1} \dots r_v^{\sigma_v}.$$

Itt ε egység, $r_j \in \mathbb{Z}$ $4k + 3$ alakú prím, $N(\pi_i)$ $4k + 1$ alakú prím.

Mindkét oldalt konjugálva

$$x - iy = \bar{\varepsilon}(1 - i)^\delta \bar{\pi}_1^{\theta_1} \dots \bar{\pi}_u^{\theta_u} r_1^{\sigma_1} \dots r_v^{\sigma_v}.$$

Ezeket összeszorozva $n = (x + iy)(x - iy)$ felbontását kapjuk.

Az n egy másik felbontását az $n = 2^\alpha p_1^{\beta_1} \dots p_m^{\beta_m} q_1^{\gamma_1} \dots q_\ell^{\gamma_\ell}$ -ből kapjuk,

A tétel bizonyítása

Ha $n = x^2 + y^2$, akkor írjuk $x + iy$ -t Gauss-prímek szorzataként.

$$x + iy = \varepsilon(1 + i)^\delta \pi_1^{\theta_1} \dots \pi_u^{\theta_u} r_1^{\sigma_1} \dots r_v^{\sigma_v} .$$

Itt ε egység, $r_j \in \mathbb{Z}$ $4k + 3$ alakú prím, $N(\pi_i)$ $4k + 1$ alakú prím.

Mindkét oldalt konjugálva

$$x - iy = \bar{\varepsilon}(1 - i)^\delta \bar{\pi}_1^{\theta_1} \dots \bar{\pi}_u^{\theta_u} r_1^{\sigma_1} \dots r_v^{\sigma_v} .$$

Ezeket összeszorozva $n = (x + iy)(x - iy)$ felbontását kapjuk.

Az n egy másik felbontását az $n = 2^\alpha p_1^{\beta_1} \dots p_m^{\beta_m} q_1^{\gamma_1} \dots q_\ell^{\gamma_\ell}$ -ből kapjuk, ha 2 -t és p_i -t Gauss-prímek szorzatára bontjuk.

A tétel bizonyítása

Ha $n = x^2 + y^2$, akkor írjuk $x + iy$ -t Gauss-prímek szorzataként.

$$x + iy = \varepsilon(1 + i)^\delta \pi_1^{\theta_1} \dots \pi_u^{\theta_u} r_1^{\sigma_1} \dots r_v^{\sigma_v}.$$

Itt ε egység, $r_j \in \mathbb{Z}$ $4k + 3$ alakú prím, $N(\pi_i)$ $4k + 1$ alakú prím.

Mindkét oldalt konjugálva

$$x - iy = \bar{\varepsilon}(1 - i)^\delta \bar{\pi}_1^{\theta_1} \dots \bar{\pi}_u^{\theta_u} r_1^{\sigma_1} \dots r_v^{\sigma_v}.$$

Ezeket összeszorozva $n = (x + iy)(x - iy)$ felbontását kapjuk.

Az n egy másik felbontását az $n = 2^\alpha p_1^{\beta_1} \dots p_m^{\beta_m} q_1^{\gamma_1} \dots q_\ell^{\gamma_\ell}$ -ből kapjuk, ha 2-t és p_i -t Gauss-prímek szorzatára bontjuk.

Az alaptétel egyértelműségi állítása miatt ez a két felbontás csak egységszeresben és sorrendben térhet el.

A tétel bizonyítása

Ha $n = x^2 + y^2$, akkor írjuk $x + iy$ -t Gauss-prímek szorzataként.

$$x + iy = \varepsilon(1 + i)^\delta \pi_1^{\theta_1} \dots \pi_u^{\theta_u} r_1^{\sigma_1} \dots r_v^{\sigma_v}.$$

Itt ε egység, $r_j \in \mathbb{Z}$ $4k + 3$ alakú prím, $N(\pi_i)$ $4k + 1$ alakú prím.

Mindkét oldalt konjugálva

$$x - iy = \bar{\varepsilon}(1 - i)^\delta \bar{\pi}_1^{\theta_1} \dots \bar{\pi}_u^{\theta_u} r_1^{\sigma_1} \dots r_v^{\sigma_v}.$$

Ezeket összeszorozva $n = (x + iy)(x - iy)$ felbontását kapjuk.

Az n egy másik felbontását az $n = 2^\alpha p_1^{\beta_1} \dots p_m^{\beta_m} q_1^{\gamma_1} \dots q_\ell^{\gamma_\ell}$ -ből kapjuk, ha 2-t és p_i -t Gauss-prímek szorzatára bontjuk.

Az alaptétel egyértelműségi állítása miatt ez a két felbontás csak egységszeresben és sorrendben térhet el.

A q_1 prím normája q_1^2 ,

A tétel bizonyítása

Ha $n = x^2 + y^2$, akkor írjuk $x + iy$ -t Gauss-prímek szorzataként.

$$x + iy = \varepsilon(1 + i)^\delta \pi_1^{\theta_1} \dots \pi_u^{\theta_u} r_1^{\sigma_1} \dots r_v^{\sigma_v}.$$

Itt ε egység, $r_j \in \mathbb{Z}$ $4k + 3$ alakú prím, $N(\pi_i)$ $4k + 1$ alakú prím.

Mindkét oldalt konjugálva

$$x - iy = \bar{\varepsilon}(1 - i)^\delta \bar{\pi}_1^{\theta_1} \dots \bar{\pi}_u^{\theta_u} r_1^{\sigma_1} \dots r_v^{\sigma_v}.$$

Ezeket összeszorozva $n = (x + iy)(x - iy)$ felbontását kapjuk.

Az n egy másik felbontását az $n = 2^\alpha p_1^{\beta_1} \dots p_m^{\beta_m} q_1^{\gamma_1} \dots q_\ell^{\gamma_\ell}$ -ből kapjuk, ha 2-t és p_i -t Gauss-prímek szorzatára bontjuk.

Az alaptétel egyértelműségi állítása miatt ez a két felbontás csak egységszeresben és sorrendben térhet el.

A q_1 prím normája q_1^2 , az $1 + i$, π_i , $\bar{\pi}_i$ normája prím.

A tétel bizonyítása

Ha $n = x^2 + y^2$, akkor írjuk $x + iy$ -t Gauss-prímek szorzataként.

$$x + iy = \varepsilon(1 + i)^\delta \pi_1^{\theta_1} \dots \pi_u^{\theta_u} r_1^{\sigma_1} \dots r_v^{\sigma_v}.$$

Itt ε egység, $r_j \in \mathbb{Z}$ $4k + 3$ alakú prím, $N(\pi_i)$ $4k + 1$ alakú prím.

Mindkét oldalt konjugálva

$$x - iy = \bar{\varepsilon}(1 - i)^\delta \bar{\pi}_1^{\theta_1} \dots \bar{\pi}_u^{\theta_u} r_1^{\sigma_1} \dots r_v^{\sigma_v}.$$

Ezeket összeszorozva $n = (x + iy)(x - iy)$ felbontását kapjuk.

Az n egy másik felbontását az $n = 2^\alpha p_1^{\beta_1} \dots p_m^{\beta_m} q_1^{\gamma_1} \dots q_\ell^{\gamma_\ell}$ -ből kapjuk, ha 2-t és p_i -t Gauss-prímek szorzatára bontjuk.

Az alaptétel egyértelműségi állítása miatt ez a két felbontás csak egységszeresben és sorrendben térhet el.

A q_1 prím normája q_1^2 , az $1 + i$, π_i , $\bar{\pi}_i$ normája prím.

Ezért q_1 csakis valamelyik r_j egységszerese lehet.

A tétel bizonyítása

Ha $n = x^2 + y^2$, akkor írjuk $x + iy$ -t Gauss-prímek szorzataként.

$$x + iy = \varepsilon(1 + i)^\delta \pi_1^{\theta_1} \dots \pi_u^{\theta_u} r_1^{\sigma_1} \dots r_v^{\sigma_v}.$$

Itt ε egység, $r_j \in \mathbb{Z}$ $4k + 3$ alakú prím, $N(\pi_i)$ $4k + 1$ alakú prím.

Mindkét oldalt konjugálva

$$x - iy = \bar{\varepsilon}(1 - i)^\delta \bar{\pi}_1^{\theta_1} \dots \bar{\pi}_u^{\theta_u} r_1^{\sigma_1} \dots r_v^{\sigma_v}.$$

Ezeket összeszorozva $n = (x + iy)(x - iy)$ felbontását kapjuk.

Az n egy másik felbontását az $n = 2^\alpha p_1^{\beta_1} \dots p_m^{\beta_m} q_1^{\gamma_1} \dots q_\ell^{\gamma_\ell}$ -ből kapjuk, ha 2-t és p_i -t Gauss-prímek szorzatára bontjuk.

Az alaptétel egyértelműségi állítása miatt ez a két felbontás csak egységszeresben és sorrendben térhet el.

A q_1 prím normája q_1^2 , az $1 + i$, π_i , $\bar{\pi}_i$ normája prím.

Ezért q_1 csakis valamelyik r_j egységszerese lehet.

De r_j kitevője n -ben $2\sigma_j$,

A tétel bizonyítása

Ha $n = x^2 + y^2$, akkor írjuk $x + iy$ -t Gauss-prímek szorzataként.

$$x + iy = \varepsilon(1 + i)^\delta \pi_1^{\theta_1} \dots \pi_u^{\theta_u} r_1^{\sigma_1} \dots r_v^{\sigma_v}.$$

Itt ε egység, $r_j \in \mathbb{Z}$ $4k + 3$ alakú prím, $N(\pi_i)$ $4k + 1$ alakú prím.

Mindkét oldalt konjugálva

$$x - iy = \bar{\varepsilon}(1 - i)^\delta \bar{\pi}_1^{\theta_1} \dots \bar{\pi}_u^{\theta_u} r_1^{\sigma_1} \dots r_v^{\sigma_v}.$$

Ezeket összeszorozva $n = (x + iy)(x - iy)$ felbontását kapjuk.

Az n egy másik felbontását az $n = 2^\alpha p_1^{\beta_1} \dots p_m^{\beta_m} q_1^{\gamma_1} \dots q_\ell^{\gamma_\ell}$ -ből kapjuk, ha 2-t és p_i -t Gauss-prímek szorzatára bontjuk.

Az alaptétel egyértelműségi állítása miatt ez a két felbontás csak egységszeresben és sorrendben térhet el.

A q_1 prím normája q_1^2 , az $1 + i$, π_i , $\bar{\pi}_i$ normája prím.

Ezért q_1 csakis valamelyik r_j egységszerese lehet.

De r_j kitevője n -ben $2\sigma_j$, ami páros.

A tétel bizonyítása

Ha $n = x^2 + y^2$, akkor írjuk $x + iy$ -t Gauss-prímek szorzataként.

$$x + iy = \varepsilon(1 + i)^\delta \pi_1^{\theta_1} \dots \pi_u^{\theta_u} r_1^{\sigma_1} \dots r_v^{\sigma_v}.$$

Itt ε egység, $r_j \in \mathbb{Z}$ $4k + 3$ alakú prím, $N(\pi_j)$ $4k + 1$ alakú prím.

Mindkét oldalt konjugálva

$$x - iy = \bar{\varepsilon}(1 - i)^\delta \bar{\pi}_1^{\theta_1} \dots \bar{\pi}_u^{\theta_u} r_1^{\sigma_1} \dots r_v^{\sigma_v}.$$

Ezeket összeszorozva $n = (x + iy)(x - iy)$ felbontását kapjuk.

Az n egy másik felbontását az $n = 2^\alpha p_1^{\beta_1} \dots p_m^{\beta_m} q_1^{\gamma_1} \dots q_\ell^{\gamma_\ell}$ -ből kapjuk, ha 2-t és p_i -t Gauss-prímek szorzatára bontjuk.

Az alaptétel egyértelműségi állítása miatt ez a két felbontás csak egységszeresben és sorrendben térhet el.

A q_1 prím normája q_1^2 , az $1 + i$, π_i , $\bar{\pi}_i$ normája prím.

Ezért q_1 csakis valamelyik r_j egységszerese lehet.

De r_j kitevője n -ben $2\sigma_j$, ami páros. Ezért q_1 kitevője

$\gamma_1 = 2\sigma_j$ is páros.

A tétel bizonyítása

Ha $n = x^2 + y^2$, akkor írjuk $x + iy$ -t Gauss-prímek szorzataként.

$$x + iy = \varepsilon(1 + i)^{\delta} \pi_1^{\theta_1} \dots \pi_u^{\theta_u} r_1^{\sigma_1} \dots r_v^{\sigma_v}.$$

Itt ε egység, $r_j \in \mathbb{Z}$ $4k + 3$ alakú prím, $N(\pi_j)$ $4k + 1$ alakú prím.

Mindkét oldalt konjugálva

$$x - iy = \bar{\varepsilon}(1 - i)^{\delta} \bar{\pi}_1^{\theta_1} \dots \bar{\pi}_u^{\theta_u} r_1^{\sigma_1} \dots r_v^{\sigma_v}.$$

Ezeket összeszorozva $n = (x + iy)(x - iy)$ felbontását kapjuk.

Az n egy másik felbontását az $n = 2^{\alpha} p_1^{\beta_1} \dots p_m^{\beta_m} q_1^{\gamma_1} \dots q_{\ell}^{\gamma_{\ell}}$ -ből kapjuk, ha 2-t és p_i -t Gauss-prímek szorzatára bontjuk.

Az alaptétel egyértelműségi állítása miatt ez a két felbontás csak egységszeresben és sorrendben térhet el.

A q_1 prím normája q_1^2 , az $1 + i$, π_i , $\bar{\pi}_i$ normája prím.

Ezért q_1 csakis valamelyik r_j egységszerese lehet.

De r_j kitevője n -ben $2\sigma_j$, ami páros. Ezért q_1 kitevője

$\gamma_1 = 2\sigma_j$ is páros. Hasonlóan q_2, \dots, q_{ℓ} kitevője is páros.

A tétel bizonyítása

Ha $n = x^2 + y^2$, akkor írjuk $x + iy$ -t Gauss-prímek szorzataként.

$$x + iy = \varepsilon(1 + i)^{\delta} \pi_1^{\theta_1} \dots \pi_u^{\theta_u} r_1^{\sigma_1} \dots r_v^{\sigma_v}.$$

Itt ε egység, $r_j \in \mathbb{Z}$ $4k + 3$ alakú prím, $N(\pi_j)$ $4k + 1$ alakú prím.

Mindkét oldalt konjugálva

$$x - iy = \bar{\varepsilon}(1 - i)^{\delta} \bar{\pi}_1^{\theta_1} \dots \bar{\pi}_u^{\theta_u} r_1^{\sigma_1} \dots r_v^{\sigma_v}.$$

Ezeket összeszorozva $n = (x + iy)(x - iy)$ felbontását kapjuk.

Az n egy másik felbontását az $n = 2^{\alpha} p_1^{\beta_1} \dots p_m^{\beta_m} q_1^{\gamma_1} \dots q_{\ell}^{\gamma_{\ell}}$ -ből kapjuk, ha 2-t és p_i -t Gauss-prímek szorzatára bontjuk.

Az alaptétel egyértelműségi állítása miatt ez a két felbontás csak egységszeresben és sorrendben térhet el.

A q_1 prím normája q_1^2 , az $1 + i$, π_i , $\bar{\pi}_i$ normája prím.

Ezért q_1 csakis valamelyik r_j egységszerese lehet.

De r_j kitevője n -ben $2\sigma_j$, ami páros. Ezért q_1 kitevője

$\gamma_1 = 2\sigma_j$ is páros. Hasonlóan q_2, \dots, q_{ℓ} kitevője is páros.

A megoldásszámra vonatkozó képlet **HF**, nem bizonyítjuk.