Algebra és számelmélet

ELTE Algebra és Számelmélet Tanszék

Konzultáció: Kiss Emil
http://ewkiss.web.elte.hu/wp/wordpress
ewwkiss@gmail.com

31. előadás

Algebrai és transzcendens számok

Definíció (FGy9.1.1, K5.10.8)

Az $\alpha \in \mathbb{C}$ algebrai szám, ha gyöke egy nem nulla, racionális együtthatós polinomnak.

Algebrai és transzcendens számok

Definíció (FGy9.1.1, K5.10.8)

Az $\alpha \in \mathbb{C}$ algebrai szám, ha gyöke egy nem nulla, racionális együtthatós polinomnak. A többi komplex szám transzcendens.

Algebrai és transzcendens számok

Definíció (FGy9.1.1, K5.10.8)

Az $\alpha \in \mathbb{C}$ algebrai szám, ha gyöke egy nem nulla, racionális együtthatós polinomnak. A többi komplex szám transzcendens.

Például 3,

Algebrai és transzcendens számok

Definíció (FGy9.1.1, K5.10.8)

Az $\alpha \in \mathbb{C}$ algebrai szám, ha gyöke egy nem nulla, racionális együtthatós polinomnak. A többi komplex szám transzcendens.

Például 3, $\sqrt{2}$,

Algebrai és transzcendens számok

Definíció (FGy9.1.1, K5.10.8)

Az $\alpha \in \mathbb{C}$ algebrai szám, ha gyöke egy nem nulla, racionális együtthatós polinomnak. A többi komplex szám transzcendens.

Például 3, $\sqrt{2}$, $\sqrt[5]{7} + 4$,

Algebrai és transzcendens számok

Definíció (FGy9.1.1, K5.10.8)

Az $\alpha \in \mathbb{C}$ algebrai szám, ha gyöke egy nem nulla, racionális együtthatós polinomnak. A többi komplex szám transzcendens.

Például 3, $\sqrt{2}$, $\sqrt[5]{7}+4$, $\sqrt[6]{5+3\sqrt[9]{7}}+\sqrt[5]{4+2\sqrt{3}}$ algebrai számok.

Algebrai és transzcendens számok

Definíció (FGy9.1.1, K5.10.8)

Az $\alpha \in \mathbb{C}$ algebrai szám, ha gyöke egy nem nulla, racionális együtthatós polinomnak. A többi komplex szám transzcendens.

Például 3, $\sqrt{2}$, $\sqrt[5]{7}+4$, $\sqrt[6]{5+3\sqrt[9]{7}}+\sqrt[5]{4+2\sqrt{3}}$ algebrai számok. Utóbbihoz már nehézkes lenne megkeresni azt a polinomot, amelynek gyöke, de a következő tétel a segítségünkre van.

Algebrai és transzcendens számok

Definíció (FGy9.1.1, K5.10.8)

Az $\alpha \in \mathbb{C}$ algebrai szám, ha gyöke egy nem nulla, racionális együtthatós polinomnak. A többi komplex szám transzcendens.

Például 3, $\sqrt{2}$, $\sqrt[5]{7}+4$, $\sqrt[6]{5+3\sqrt[9]{7}}+\sqrt[5]{4+2\sqrt{3}}$ algebrai számok. Utóbbihoz már nehézkes lenne megkeresni azt a polinomot, amelynek gyöke, de a következő tétel a segítségünkre van.

Tétel (FGy9.3.1, 9.3.6, K6.2.12, 6.2.13, NB)

Algebrai számok összege, különbsége, szorzata, hányadosa és n-edik gyöke is algebrai szám.

Algebrai és transzcendens számok

Definíció (FGy9.1.1, K5.10.8)

Az $\alpha \in \mathbb{C}$ algebrai szám, ha gyöke egy nem nulla, racionális együtthatós polinomnak. A többi komplex szám transzcendens.

Például 3, $\sqrt{2}$, $\sqrt[5]{7}+4$, $\sqrt[6]{5+3\sqrt[9]{7}}+\sqrt[5]{4+2\sqrt{3}}$ algebrai számok. Utóbbihoz már nehézkes lenne megkeresni azt a polinomot, amelynek gyöke, de a következő tétel a segítségünkre van.

Tétel (FGy9.3.1, 9.3.6, K6.2.12, 6.2.13, NB)

Algebrai számok összege, különbsége, szorzata, hányadosa és n-edik gyöke is algebrai szám. Sőt algebrai együtthatós polinom gyöke is algebrai.

Algebrai és transzcendens számok

Definíció (FGy9.1.1, K5.10.8)

Az $\alpha \in \mathbb{C}$ algebrai szám, ha gyöke egy nem nulla, racionális együtthatós polinomnak. A többi komplex szám transzcendens.

Például 3, $\sqrt{2}$, $\sqrt[5]{7}+4$, $\sqrt[6]{5+3\sqrt[9]{7}}+\sqrt[5]{4+2\sqrt{3}}$ algebrai számok. Utóbbihoz már nehézkes lenne megkeresni azt a polinomot, amelynek gyöke, de a következő tétel a segítségünkre van.

Tétel (FGy9.3.1, 9.3.6, K6.2.12, 6.2.13, NB)

Algebrai számok összege, különbsége, szorzata, hányadosa és n-edik gyöke is algebrai szám. Sőt algebrai együtthatós polinom gyöke is algebrai. Ezért az algebrai számok algebrailag zárt testet alkotnak.

Algebrai és transzcendens számok

Definíció (FGy9.1.1, K5.10.8)

Az $\alpha \in \mathbb{C}$ algebrai szám, ha gyöke egy nem nulla, racionális együtthatós polinomnak. A többi komplex szám transzcendens.

Például 3, $\sqrt{2}$, $\sqrt[5]{7}+4$, $\sqrt[6]{5+3\sqrt[9]{7}}+\sqrt[5]{4+2\sqrt{3}}$ algebrai számok. Utóbbihoz már nehézkes lenne megkeresni azt a polinomot, amelynek gyöke, de a következő tétel a segítségünkre van.

Tétel (FGy9.3.1, 9.3.6, K6.2.12, 6.2.13, NB)

Algebrai számok összege, különbsége, szorzata, hányadosa és n-edik gyöke is algebrai szám. Sőt algebrai együtthatós polinom gyöke is algebrai. Ezért az algebrai számok algebrailag zárt testet alkotnak.

Ebből következik, hogy ha b algebrai és t transzcendens, akkor $a = b + t$ is transzcendens.

Algebrai és transzcendens számok

Definíció (FGy9.1.1, K5.10.8)

Az $\alpha \in \mathbb{C}$ algebrai szám, ha gyöke egy nem nulla, racionális együtthatós polinomnak. A többi komplex szám transzcendens.

Például 3, $\sqrt{2}$, $\sqrt[5]{7}+4$, $\sqrt[6]{5+3\sqrt[9]{7}}+\sqrt[5]{4+2\sqrt{3}}$ algebrai számok. Utóbbihoz már nehézkes lenne megkeresni azt a polinomot, amelynek gyöke, de a következő tétel a segítségünkre van.

Tétel (FGy9.3.1, 9.3.6, K6.2.12, 6.2.13, NB)

Algebrai számok összege, különbsége, szorzata, hányadosa és n-edik gyöke is algebrai szám. Sőt algebrai együtthatós polinom gyöke is algebrai. Ezért az algebrai számok algebrailag zárt testet alkotnak.

Ebből következik, hogy ha b algebrai és t transzcendens, akkor $a = b + t$ is transzcendens. Ha ugyanis a algebrai lenne,

Algebrai és transzcendens számok

Definíció (FGy9.1.1, K5.10.8)

Az $\alpha \in \mathbb{C}$ algebrai szám, ha gyöke egy nem nulla, racionális együtthatós polinomnak. A többi komplex szám transzcendens.

Például 3, $\sqrt{2}$, $\sqrt[5]{7}+4$, $\sqrt[6]{5+3\sqrt[9]{7}}+\sqrt[5]{4+2\sqrt{3}}$ algebrai számok. Utóbbihoz már nehézkes lenne megkeresni azt a polinomot, amelynek gyöke, de a következő tétel a segítségünkre van.

Tétel (FGy9.3.1, 9.3.6, K6.2.12, 6.2.13, NB)

Algebrai számok összege, különbsége, szorzata, hányadosa és n-edik gyöke is algebrai szám. Sőt algebrai együtthatós polinom gyöke is algebrai. Ezért az algebrai számok algebrailag zárt testet alkotnak.

Ebből következik, hogy ha b algebrai és t transzcendens, akkor $a = b + t$ is transzcendens. Ha ugyanis a algebrai lenne, akkor $t = a - b$ is algebrai lenne a tétel miatt,

Algebrai és transzcendens számok

Definíció (FGy9.1.1, K5.10.8)

Az $\alpha \in \mathbb{C}$ algebrai szám, ha gyöke egy nem nulla, racionális együtthatós polinomnak. A többi komplex szám transzcendens.

Például 3, $\sqrt{2}$, $\sqrt[5]{7}+4$, $\sqrt[6]{5+3\sqrt[9]{7}}+\sqrt[5]{4+2\sqrt{3}}$ algebrai számok. Utóbbihoz már nehézkes lenne megkeresni azt a polinomot, amelynek gyöke, de a következő tétel a segítségünkre van.

Tétel (FGy9.3.1, 9.3.6, K6.2.12, 6.2.13, NB)

Algebrai számok összege, különbsége, szorzata, hányadosa és n-edik gyöke is algebrai szám. Sőt algebrai együtthatós polinom gyöke is algebrai. Ezért az algebrai számok algebrailag zárt testet alkotnak.

Ebből következik, hogy ha b algebrai és t transzcendens, akkor $a = b + t$ is transzcendens. Ha ugyanis a algebrai lenne, akkor $t = a - b$ is algebrai lenne a tétel miatt, ami ellentmondás.

Példák transzcendens számra

Tétel (FGy9.1.3, NB)

Az algebrai számok halmaza megszámlálható,

Példák transzcendens számra

Tétel (FGy9.1.3, NB)

Az algebrai számok halmaza megszámlálható, tehát a komplex számok „döntő része” transzcendens.

Példák transzcendens számra

Tétel (FGy9.1.3, NB)

Az algebrai számok halmaza megszámlálható, tehát a komplex számok „döntő része” transzcendens.

Konkrét transzcendens számot találni mégis nehéz.

Példák transzcendens számra

Tétel (FGy9.1.3, NB)

Az algebrai számok halmaza megszámlálható, tehát a komplex számok „döntő része” transzcendens.

Konkrét transzcendens számot találni mégis nehéz. Az alábbi példák transzcendensek, de ennek bizonyítása igen bonyolult.

Példák transzcendens számra

Tétel (FGy9.1.3, NB)

Az algebrai számok halmaza megszámlálható, tehát a komplex számok „döntő része” transzcendens.

Konkrét transzcendens számot találni mégis nehéz. Az alábbi példák transzcendensek, de ennek bizonyítása igen bonyolult.

(1) π (Lindemann-Weierstrass, 1882),

Példák transzcendens számra

Tétel (FGy9.1.3, NB)

Az algebrai számok halmaza megszámlálható, tehát a komplex számok „döntő része” transzcendens.

Konkrét transzcendens számot találni mégis nehéz. Az alábbi példák transzcendensek, de ennek bizonyítása igen bonyolult.

(1) π (Lindemann-Weierstrass, 1882), $\zeta(2k)$,

Példák transzcendens számra

Tétel (FGy9.1.3, NB)

Az algebrai számok halmaza megszámlálható, tehát a komplex számok „döntő része” transzcendens.

Konkrét transzcendens számot találni mégis nehéz. Az alábbi példák transzcendensek, de ennek bizonyítása igen bonyolult.

(1) π (Lindemann-Weierstrass, 1882), $\zeta(2k)$, itt ζ a Riemann-függvény.

Példák transzcendens számra

Tétel (FGy9.1.3, NB)

Az algebrai számok halmaza megszámlálható, tehát a komplex számok „döntő része” transzcendens.

Konkrét transzcendens számot találni mégis nehéz. Az alábbi példák transzcendensek, de ennek bizonyítása igen bonyolult.

(1) π (Lindemann-Weierstrass, 1882), $\zeta(2k)$, itt ζ a Riemann-függvény. (Oka: $\zeta(2k)/\pi^{2k}$ racionális.)

Példák transzcendens számra

Tétel (FGy9.1.3, NB)

Az algebrai számok halmaza megszámlálható, tehát a komplex számok „döntő része” transzcendens.

Konkrét transzcendens számot találni mégis nehéz. Az alábbi példák transzcendensek, de ennek bizonyítása igen bonyolult.

(1) π (Lindemann-Weierstrass, 1882), $\zeta(2k)$, itt ζ a Riemann-függvény. (Oka: $\zeta(2k)/\pi^{2k}$ racionális.)

(2) e (lásd FGy9.5.2)

Példák transzcendens számra

Tétel (FGy9.1.3, NB)

Az algebrai számok halmaza megszámlálható, tehát a komplex számok „döntő része” transzcendens.

Konkrét transzcendens számot találni mégis nehéz. Az alábbi példák transzcendensek, de ennek bizonyítása igen bonyolult.

(1) π (Lindemann-Weierstrass, 1882), $\zeta(2k)$, itt ζ a Riemann-függvény. (Oka: $\zeta(2k)/\pi^{2k}$ racionális.)

(2) e (lásd FGy9.5.2)

(3) a^b, ahol $\alpha \neq 0, 1$, a és b algebrai, b irracionális

Példák transzcendens számra

Tétel (FGy9.1.3, NB)

Az algebrai számok halmaza megszámlálható, tehát a komplex számok „döntő része” transzcendens.

Konkrét transzcendens számot találni mégis nehéz. Az alábbi példák transzcendensek, de ennek bizonyítása igen bonyolult.

(1) π (Lindemann-Weierstrass, 1882), $\zeta(2k)$, itt ζ a Riemann-függvény. (Oka: $\zeta(2k)/\pi^{2k}$ racionális.)

(2) e (lásd FGy9.5.2)

(3) a^b, ahol $\alpha \neq 0, 1$, a és b algebrai, b irracionális (Gelfond-Schneider-tétel, 1934, FGy9.3.5).

Példák transzcendens számra

Tétel (FGy9.1.3, NB)

Az algebrai számok halmaza megszámlálható, tehát a komplex számok „döntő része” transzcendens.

Konkrét transzcendens számot találni mégis nehéz. Az alábbi példák transzcendensek, de ennek bizonyítása igen bonyolult.

(1) π (Lindemann-Weierstrass, 1882), $\zeta(2k)$, itt ζ a Riemann-függvény. (Oka: $\zeta(2k)/\pi^{2k}$ racionális.)

(2) e (lásd FGy9.5.2)

(3) a^b, ahol $\alpha \neq 0, 1$, a és b algebrai, b irracionális, pl. $2^{\sqrt{2}}$ (Gelfond-Schneider-tétel, 1934, FGy9.3.5).

Példák transzcendens számra

Tétel (FGy9.1.3, NB)

Az algebrai számok halmaza megszámlálható, tehát a komplex számok „döntő része” transzcendens.

Konkrét transzcendens számot találni mégis nehéz. Az alábbi példák transzcendensek, de ennek bizonyítása igen bonyolult.

(1) π (Lindemann-Weierstrass, 1882), $\zeta(2k)$, itt ζ a Riemann-függvény. (Oka: $\zeta(2k)/\pi^{2k}$ racionális.)

(2) e (lásd FGy9.5.2)

(3) a^b, ahol $\alpha \neq 0, 1$, a és b algebrai, b irracionális, pl. $2^{\sqrt{2}}$ és $e^{\pi} = (-1)^{-i}$ (Gelfond-Schneider-tétel, 1934, FGy9.3.5).

Példák transzcendens számra

Tétel (FGy9.1.3, NB)

Az algebrai számok halmaza megszámlálható, tehát a komplex számok „döntő része” transzcendens.

Konkrét transzcendens számot találni mégis nehéz. Az alábbi példák transzcendensek, de ennek bizonyítása igen bonyolult.

(1) π (Lindemann-Weierstrass, 1882), $\zeta(2k)$, itt ζ a Riemann-függvény. (Oka: $\zeta(2k)/\pi^{2k}$ racionális.)

(2) e (lásd FGy9.5.2)

(3) a^b, ahol $\alpha \neq 0, 1$, a és b algebrai, b irracionális, pl. $2^{\sqrt{2}}$ és $e^{\pi} = (-1)^{-i}$ (Gelfond-Schneider-tétel, 1934, FGy9.3.5).

(4) $\sin 1$ (ívmértékben, nem 1°),

Példák transzcendens számra

Tétel (FGy9.1.3, NB)

Az algebrai számok halmaza megszámlálható, tehát a komplex számok „döntő része” transzcendens.

Konkrét transzcendens számot találni mégis nehéz. Az alábbi példák transzcendensek, de ennek bizonyítása igen bonyolult.

(1) π (Lindemann-Weierstrass, 1882), $\zeta(2k)$, itt ζ a Riemann-függvény. (Oka: $\zeta(2k)/\pi^{2k}$ racionális.)

(2) e (lásd FGy9.5.2)

(3) a^b, ahol $\alpha \neq 0, 1$, a és b algebrai, b irracionális, pl. $2^{\sqrt{2}}$ és $e^{\pi} = (-1)^{-i}$ (Gelfond-Schneider-tétel, 1934, FGy9.3.5).

(4) $\sin 1$ (ívmértékben, nem 1°), $\log_{10}(2)$,

Példák transzcendens számra

Tétel (FGy9.1.3, NB)

Az algebrai számok halmaza megszámlálható, tehát a komplex számok „döntő része” transzcendens.

Konkrét transzcendens számot találni mégis nehéz. Az alábbi példák transzcendensek, de ennek bizonyítása igen bonyolult.

(1) π (Lindemann-Weierstrass, 1882), $\zeta(2k)$, itt ζ a Riemann-függvény. (Oka: $\zeta(2k)/\pi^{2k}$ racionális.)

(2) e (lásd FGy9.5.2)

(3) a^b, ahol $\alpha \neq 0, 1$, a és b algebrai, b irracionális, pl. $2^{\sqrt{2}}$ és $e^{\pi} = (-1)^{-i}$ (Gelfond-Schneider-tétel, 1934, FGy9.3.5).

(4) $\sin 1$ (ívmértékben, nem 1°), $\log_{10}(2)$, $e^{\sqrt{2}\pi}$.

Példák transzcendens számra

Tétel (FGy9.1.3, NB)

Az algebrai számok halmaza megszámlálható, tehát a komplex számok „döntő része” transzcendens.

Konkrét transzcendens számot találni mégis nehéz. Az alábbi példák transzcendensek, de ennek bizonyítása igen bonyolult.

(1) π (Lindemann-Weierstrass, 1882), $\zeta(2k)$, itt ζ a Riemann-függvény. (Oka: $\zeta(2k)/\pi^{2k}$ racionális.)

(2) e (lásd FGy9.5.2)

(3) a^b, ahol $\alpha \neq 0, 1$, a és b algebrai, b irracionális, pl. $2^{\sqrt{2}}$ és $e^{\pi} = (-1)^{-i}$ (Gelfond-Schneider-tétel, 1934, FGy9.3.5).

(4) $\sin 1$ (ívmértékben, nem 1°), $\log_{10}(2)$, $e^{\sqrt{2}\pi}$.

Megoldatlan, hogy transzcendens-e: $e \pm \pi$

Példák transzcendens számra

Tétel (FGy9.1.3, NB)

Az algebrai számok halmaza megszámlálható, tehát a komplex számok „döntő része” transzcendens.

Konkrét transzcendens számot találni mégis nehéz. Az alábbi példák transzcendensek, de ennek bizonyítása igen bonyolult.

(1) π (Lindemann-Weierstrass, 1882), $\zeta(2k)$, itt ζ a Riemann-függvény. (Oka: $\zeta(2k)/\pi^{2k}$ racionális.)

(2) e (lásd FGy9.5.2)

(3) a^b, ahol $\alpha \neq 0, 1$, a és b algebrai, b irracionális, pl. $2^{\sqrt{2}}$ és $e^{\pi} = (-1)^{-i}$ (Gelfond-Schneider-tétel, 1934, FGy9.3.5).

(4) $\sin 1$ (ívmértékben, nem 1°), $\log_{10}(2)$, $e^{\sqrt{2}\pi}$.

Megoldatlan, hogy transzcendens-e: $e \pm \pi$ (az egyik biztos),

Példák transzcendens számra

Tétel (FGy9.1.3, NB)

Az algebrai számok halmaza megszámlálható, tehát a komplex számok „döntő része” transzcendens.

Konkrét transzcendens számot találni mégis nehéz. Az alábbi példák transzcendensek, de ennek bizonyítása igen bonyolult.

(1) π (Lindemann-Weierstrass, 1882), $\zeta(2k)$, itt ζ a Riemann-függvény. (Oka: $\zeta(2k)/\pi^{2k}$ racionális.)

(2) e (lásd FGy9.5.2)

(3) a^b, ahol $\alpha \neq 0, 1$, a és b algebrai, b irracionális, pl. $2^{\sqrt{2}}$ és $e^{\pi} = (-1)^{-i}$ (Gelfond-Schneider-tétel, 1934, FGy9.3.5).

(4) $\sin 1$ (ívmértékben, nem 1°), $\log_{10}(2)$, $e^{\sqrt{2}\pi}$.

Megoldatlan, hogy transzcendens-e: $e \pm \pi$ (az egyik biztos), π^e,

Példák transzcendens számra

Tétel (FGy9.1.3, NB)

Az algebrai számok halmaza megszámlálható, tehát a komplex számok „döntő része” transzcendens.

Konkrét transzcendens számot találni mégis nehéz. Az alábbi példák transzcendensek, de ennek bizonyítása igen bonyolult.

(1) π (Lindemann-Weierstrass, 1882), $\zeta(2k)$, itt ζ a Riemann-függvény. (Oka: $\zeta(2k)/\pi^{2k}$ racionális.)

(2) e (lásd FGy9.5.2)

(3) a^b, ahol $\alpha \neq 0, 1$, a és b algebrai, b irracionális, pl. $2^{\sqrt{2}}$ és $e^{\pi} = (-1)^{-i}$ (Gelfond-Schneider-tétel, 1934, FGy9.3.5).

(4) $\sin 1$ (ívmértékben, nem 1°), $\log_{10}(2)$, $e^{\sqrt{2}\pi}$.

Megoldatlan, hogy transzcendens-e: $e \pm \pi$ (az egyik biztos), π^e, $\zeta(3)$,

Példák transzcendens számra

Tétel (FGy9.1.3, NB)

Az algebrai számok halmaza megszámlálható, tehát a komplex számok „döntő része” transzcendens.

Konkrét transzcendens számot találni mégis nehéz. Az alábbi példák transzcendensek, de ennek bizonyítása igen bonyolult.

(1) π (Lindemann-Weierstrass, 1882), $\zeta(2k)$, itt ζ a Riemann-függvény. (Oka: $\zeta(2k)/\pi^{2k}$ racionális.)

(2) e (lásd FGy9.5.2)

(3) a^b, ahol $\alpha \neq 0, 1$, a és b algebrai, b irracionális, pl. $2^{\sqrt{2}}$ és $e^{\pi} = (-1)^{-i}$ (Gelfond-Schneider-tétel, 1934, FGy9.3.5).

(4) $\sin 1$ (ívmértékben, nem 1°), $\log_{10}(2)$, $e^{\sqrt{2}\pi}$.

Megoldatlan, hogy transzcendens-e: $e \pm \pi$ (az egyik biztos), π^e, $\zeta(3)$, $\zeta(5)$.

Példák transzcendens számra

Tétel (FGy9.1.3, NB)

Az algebrai számok halmaza megszámlálható, tehát a komplex számok „döntő része” transzcendens.

Konkrét transzcendens számot találni mégis nehéz. Az alábbi példák transzcendensek, de ennek bizonyítása igen bonyolult.

(1) π (Lindemann-Weierstrass, 1882), $\zeta(2k)$, itt ζ a Riemann-függvény. (Oka: $\zeta(2k)/\pi^{2k}$ racionális.)

(2) e (lásd FGy9.5.2)

(3) a^b, ahol $\alpha \neq 0, 1$, a és b algebrai, b irracionális, pl. $2^{\sqrt{2}}$ és $e^{\pi} = (-1)^{-i}$ (Gelfond-Schneider-tétel, 1934, FGy9.3.5).

(4) $\sin 1$ (ívmértékben, nem 1°), $\log_{10}(2)$, $e^{\sqrt{2}\pi}$.

Megoldatlan, hogy transzcendens-e: $e \pm \pi$ (az egyik biztos), π^e, $\zeta(3)$, $\zeta(5)$. A $\zeta(3)$ irracionális.

e és π irracionális

Tétel (FGy9.5.1)

Az $e = \sum_{n=0}^{\infty}(1/n!)$ szám irracionális.

e és π irracionális

Tétel (FGy9.5.1)

Az $e = \sum_{n=0}^{\infty}(1/n!)$ szám irracionális.

Valóban, tegyük föl, hogy $e = a/b$.

e és π irracionális

Tétel (FGy9.5.1)

Az $e = \sum_{n=0}^{\infty}(1/n!)$ szám irracionális.

Valóban, tegyük föl, hogy $e = a/b$. Ekkor $b!$-sal szorozva az egész $eb!$ szám

e és π irracionális

Tétel (FGy9.5.1)

Az $e = \sum_{n=0}^{\infty}(1/n!)$ szám irracionális.

Valóban, tegyük föl, hogy $e = a/b$. Ekkor $b!$-sal szorozva az egész $eb!$ szám (egész) $+ \sum_{k=1}^{\infty} \frac{1}{(b+1)\ldots(b+k)}$-val egyenlő.

e és π irracionális

Tétel (FGy9.5.1)

Az $e = \sum_{n=0}^{\infty}(1/n!)$ szám irracionális.

Valóban, tegyük föl, hogy $e = a/b$. Ekkor $b!$-sal szorozva az egész $eb!$ szám (egész) $+ \sum_{k=1}^{\infty} \frac{1}{(b+1)\ldots(b+k)}$-val egyenlő.

De ez az S szumma kisebb, mint $\sum_{k=1}^{\infty} \frac{1}{(b+1)^k}$

e és π irracionális

Tétel (FGy9.5.1)

Az $e = \sum_{n=0}^{\infty}(1/n!)$ szám irracionális.

Valóban, tegyük föl, hogy $e = a/b$. Ekkor $b!$-sal szorozva az egész $eb!$ szám (egész) $+ \sum_{k=1}^{\infty} \frac{1}{(b+1)\ldots(b+k)}$-val egyenlő.

De ez az S szumma kisebb, mint $\sum_{k=1}^{\infty} \frac{1}{(b+1)^k} = \frac{1}{b}$

e és π irracionális

Tétel (FGy9.5.1)

Az $e = \sum_{n=0}^{\infty}(1/n!)$ szám irracionális.

Valóban, tegyük föl, hogy $e = a/b$. Ekkor $b!$-sal szorozva az egész $eb!$ szám (egész) $+ \sum_{k=1}^{\infty} \frac{1}{(b+1)\ldots(b+k)}$-val egyenlő. De ez az S szumma kisebb, mint $\sum_{k=1}^{\infty} \frac{1}{(b+1)^k} = \frac{1}{b}$ (mértani sor).

e és π irracionális

Tétel (FGy9.5.1)

Az $e = \sum_{n=0}^{\infty}(1/n!)$ szám irracionális.

Valóban, tegyük föl, hogy $e = a/b$. Ekkor $b!$-sal szorozva az egész $eb!$ szám (egész) $+ \sum_{k=1}^{\infty} \frac{1}{(b+1)\ldots(b+k)}$-val egyenlő. De ez az S szumma kisebb, mint $\sum_{k=1}^{\infty} \frac{1}{(b+1)^k} = \frac{1}{b} \leq 1$ (mértani sor).

e és π irracionális

Tétel (FGy9.5.1)

Az $e = \sum_{n=0}^{\infty}(1/n!)$ szám irracionális.

Valóban, tegyük föl, hogy $e = a/b$. Ekkor $b!$-sal szorozva az egész $eb!$ szám (egész) $+ \sum_{k=1}^{\infty} \frac{1}{(b+1)\ldots(b+k)}$-val egyenlő. De ez az S szumma kisebb, mint $\sum_{k=1}^{\infty} \frac{1}{(b+1)^k} = \frac{1}{b} \leq 1$ (mértani sor). Vagyis S egész szám,

e és π irracionális

Tétel (FGy9.5.1)

Az $e = \sum_{n=0}^{\infty}(1/n!)$ szám irracionális.

Valóban, tegyük föl, hogy $e = a/b$. Ekkor $b!$-sal szorozva az egész $eb!$ szám (egész) $+ \sum_{k=1}^{\infty} \frac{1}{(b+1)\ldots(b+k)}$-val egyenlő. De ez az S szumma kisebb, mint $\sum_{k=1}^{\infty} \frac{1}{(b+1)^k} = \frac{1}{b} \leq 1$ (mértani sor). Vagyis S egész szám, mégis $0 < S < 1$. □

e és π irracionális

Tétel (FGy9.5.1)

Az $e = \sum_{n=0}^{\infty}(1/n!)$ szám irracionális.

Valóban, tegyük föl, hogy $e = a/b$. Ekkor $b!$-sal szorozva az egész $eb!$ szám (egész) $+ \sum_{k=1}^{\infty} \frac{1}{(b+1)\ldots(b+k)}$-val egyenlő. De ez az S szumma kisebb, mint $\sum_{k=1}^{\infty} \frac{1}{(b+1)^k} = \frac{1}{b} \leq 1$ (mértani sor). Vagyis S egész szám, mégis $0 < S < 1$. □

Tétel (FGy9.5.2)

Az π szám irracionális.

e és π irracionális

Tétel (FGy9.5.1)

Az $e = \sum_{n=0}^{\infty}(1/n!)$ szám irracionális.

Valóban, tegyük föl, hogy $e = a/b$. Ekkor $b!$-sal szorozva az egész $eb!$ szám (egész) $+ \sum_{k=1}^{\infty} \frac{1}{(b+1)\ldots(b+k)}$-val egyenlő. De ez az S szumma kisebb, mint $\sum_{k=1}^{\infty} \frac{1}{(b+1)^k} = \frac{1}{b} \leq 1$ (mértani sor). Vagyis S egész szám, mégis $0 < S < 1$. □

Tétel (FGy9.5.2)

Az π szám irracionális.

A bizonyítás ötlete: Ha $\pi = a/b$, ahol a, b egész,

e és π irracionális

Tétel (FGy9.5.1)

Az $e = \sum_{n=0}^{\infty}(1/n!)$ szám irracionális.

Valóban, tegyük föl, hogy $e = a/b$. Ekkor $b!$-sal szorozva az egész $eb!$ szám (egész) $+ \sum_{k=1}^{\infty} \frac{1}{(b+1)\ldots(b+k)}$-val egyenlő. De ez az S szumma kisebb, mint $\sum_{k=1}^{\infty} \frac{1}{(b+1)^k} = \frac{1}{b} \leq 1$ (mértani sor). Vagyis S egész szám, mégis $0 < S < 1$. □

Tétel (FGy9.5.2)

Az π szám irracionális.

A bizonyítás ötlete: Ha $\pi = a/b$, ahol a, b egész, akkor legyen $P = a^{2n+1} \int_0^1 \sin(\pi x) f(x) dx$,

e és π irracionális

Tétel (FGy9.5.1)

Az $e = \sum_{n=0}^{\infty}(1/n!)$ szám irracionális.

Valóban, tegyük föl, hogy $e = a/b$. Ekkor $b!$-sal szorozva az egész $eb!$ szám (egész) $+ \sum_{k=1}^{\infty} \frac{1}{(b+1)\ldots(b+k)}$-val egyenlő. De ez az S szumma kisebb, mint $\sum_{k=1}^{\infty} \frac{1}{(b+1)^k} = \frac{1}{b} \leq 1$ (mértani sor). Vagyis S egész szám, mégis $0 < S < 1$. □

Tétel (FGy9.5.2)

Az π szám irracionális.

A bizonyítás ötlete: Ha $\pi = a/b$, ahol a, b egész, akkor legyen $P = a^{2n+1} \int_0^1 \sin(\pi x) f(x) dx$, ahol $f(x) = x^n(1-x)^n/n!$.

e és π irracionális

Tétel (FGy9.5.1)

Az $e = \sum_{n=0}^{\infty}(1/n!)$ szám irracionális.

Valóban, tegyük föl, hogy $e = a/b$. Ekkor $b!$-sal szorozva az egész $eb!$ szám (egész) $+ \sum_{k=1}^{\infty} \frac{1}{(b+1)\ldots(b+k)}$-val egyenlő. De ez az S szumma kisebb, mint $\sum_{k=1}^{\infty} \frac{1}{(b+1)^k} = \frac{1}{b} \leq 1$ (mértani sor). Vagyis S egész szám, mégis $0 < S < 1$. □

Tétel (FGy9.5.2)

Az π szám irracionális.

A bizonyítás ötlete: Ha $\pi = a/b$, ahol a, b egész, akkor legyen $P = a^{2n+1} \int_0^1 \sin(\pi x) f(x) dx$, ahol $f(x) = x^n(1-x)^n/n!$. Parciális integrálások sorozatával látható, hogy P egész.

e és π irracionális

Tétel (FGy9.5.1)

Az $e = \sum_{n=0}^{\infty}(1/n!)$ szám irracionális.

Valóban, tegyük föl, hogy $e = a/b$. Ekkor $b!$-sal szorozva az egész $eb!$ szám (egész) $+ \sum_{k=1}^{\infty} \frac{1}{(b+1)\ldots(b+k)}$-val egyenlő. De ez az S szumma kisebb, mint $\sum_{k=1}^{\infty} \frac{1}{(b+1)^k} = \frac{1}{b} \leq 1$ (mértani sor). Vagyis S egész szám, mégis $0 < S < 1$. □

Tétel (FGy9.5.2)

Az π szám irracionális.

A bizonyítás ötlete: Ha $\pi = a/b$, ahol a, b egész, akkor legyen $P = a^{2n+1} \int_0^1 \sin(\pi x) f(x) dx$, ahol $f(x) = x^n(1-x)^n/n!$. Parciális integrálások sorozatával látható, hogy P egész. Másrészt egyszerű becslés adja, hogy $0 < P < 1$.

Transzcendens szám konstrukciója

Algebrai számokat nem lehet kis nevezőjű törtekkel túl jól közelíteni (FGy9.4.1),

Transzcendens szám konstrukciója

Algebrai számokat nem lehet kis nevezőjű törtekkel túl jól közelíteni (FGy9.4.1), de az alábbi α-t lehet,

Transzcendens szám konstrukciója

Algebrai számokat nem lehet kis nevezőjű törtekkel túl jól közelíteni (FGy9.4.1), de az alábbi α-t lehet, mert a sora gyorsan konvergál.

Transzcendens szám konstrukciója

Algebrai számokat nem lehet kis nevezőjű törtekkel túl jól közelíteni (FGy9.4.1), de az alábbi α-t lehet, mert a sora gyorsan konvergál.

FGy9.4.2: Az $\alpha = \sum_{k=1}^{\infty} \frac{1}{10^{k!}}$ Liouville-szám transzcendens.

Transzcendens szám konstrukciója

Algebrai számokat nem lehet kis nevezőjű törtekkel túl jól közelíteni (FGy9.4.1), de az alábbi α-t lehet, mert a sora gyorsan konvergál.

FGy9.4.2: Az $\alpha = \sum_{k=1}^{\infty} \frac{1}{10^{k!}}$ Liouville-szám transzcendens.
$\alpha = 0{,}110001000000000000000001000\ldots$

Transzcendens szám konstrukciója

Algebrai számokat nem lehet kis nevezőjű törtekkel túl jól közelíteni (FGy9.4.1), de az alábbi α-t lehet, mert a sora gyorsan konvergál.

FGy9.4.2: Az $\alpha = \sum_{k=1}^{\infty} \frac{1}{10^{k!}}$ Liouville-szám transzcendens.
$\alpha = 0{,}110001000000000000000001000\ldots$

Tegyük föl, hogy $f(\alpha) = 0$, ahol $f(x) = a_0 + \ldots + a_n x^n \in \mathbb{Q}[x]$,

Transzcendens szám konstrukciója

Algebrai számokat nem lehet kis nevezőjű törtekkel túl jól közelíteni (FGy9.4.1), de az alábbi α-t lehet, mert a sora gyorsan konvergál.

FGy9.4.2: Az $\alpha = \sum_{k=1}^{\infty} \frac{1}{10^{k!}}$ Liouville-szám transzcendens.
$\alpha = 0{,}110001000000000000000001000\ldots$

Tegyük föl, hogy $f(\alpha) = 0$, ahol $f(x) = a_0 + \ldots + a_n x^n \in \mathbb{Q}[x]$, és $a_n \neq 0$.

Transzcendens szám konstrukciója

Algebrai számokat nem lehet kis nevezőjű törtekkel túl jól közelíteni (FGy9.4.1), de az alábbi α-t lehet, mert a sora gyorsan konvergál.

FGy9.4.2: Az $\alpha = \sum_{k=1}^{\infty} \frac{1}{10^{k!}}$ Liouville-szám transzcendens.
$\alpha = 0{,}110001000000000000000001000\ldots$

Tegyük föl, hogy $f(\alpha) = 0$, ahol $f(x) = a_0 + \ldots + a_n x^n \in \mathbb{Q}[x]$, (a nevezőkkel felszorozva feltehető, hogy a_i egész), és $a_n \neq 0$.

Transzcendens szám konstrukciója

Algebrai számokat nem lehet kis nevezőjű törtekkel túl jól közelíteni (FGy9.4.1), de az alábbi α-t lehet, mert a sora gyorsan konvergál.

FGy9.4.2: Az $\alpha = \sum_{k=1}^{\infty} \frac{1}{10^{k!}}$ Liouville-szám transzcendens.
$\alpha = 0{,}110001000000000000000001000\ldots$

Tegyük föl, hogy $f(\alpha) = 0$, ahol $f(x) = a_0 + \ldots + a_n x^n \in \mathbb{Q}[x]$, (a nevezőkkel felszorozva feltehető, hogy a_i egész), és $a_n \neq 0$.
Legyen $\alpha_N = \sum_{k=1}^{N} \frac{1}{10^{k!}}$,

Transzcendens szám konstrukciója

Algebrai számokat nem lehet kis nevezőjű törtekkel túl jól közelíteni (FGy9.4.1), de az alábbi α-t lehet, mert a sora gyorsan konvergál.

FGy9.4.2: Az $\alpha = \sum_{k=1}^{\infty} \frac{1}{10^{k!}}$ Liouville-szám transzcendens.
$\alpha = 0{,}110001000000000000000001000\ldots$

Tegyük föl, hogy $f(\alpha) = 0$, ahol $f(x) = a_0 + \ldots + a_n x^n \in \mathbb{Q}[x]$, (a nevezőkkel felszorozva feltehető, hogy a_i egész), és $a_n \neq 0$.
Legyen $\alpha_N = \sum_{k=1}^{N} \frac{1}{10^{k!}}$, és $\beta_N = \alpha - \alpha_N$.

Transzcendens szám konstrukciója

Algebrai számokat nem lehet kis nevezőjű törtekkel túl jól közelíteni (FGy9.4.1), de az alábbi α-t lehet, mert a sora gyorsan konvergál.

FGy9.4.2: Az $\alpha = \sum_{k=1}^{\infty} \frac{1}{10^{k!}}$ Liouville-szám transzcendens.
$\alpha = 0{,}110001000000000000000001000\ldots$

Tegyük föl, hogy $f(\alpha) = 0$, ahol $f(x) = a_0 + \ldots + a_n x^n \in \mathbb{Q}[x]$, (a nevezőkkel felszorozva feltehető, hogy a_i egész), és $a_n \neq 0$.
Legyen $\alpha_N = \sum_{k=1}^{N} \frac{1}{10^{k!}}$, és $\beta_N = \alpha - \alpha_N$. Ekkor
$10^{(N+1)!-1}\beta_N < 1$,

Transzcendens szám konstrukciója

Algebrai számokat nem lehet kis nevezőjű törtekkel túl jól közelíteni (FGy9.4.1), de az alábbi α-t lehet, mert a sora gyorsan konvergál.

FGy9.4.2: Az $\alpha = \sum_{k=1}^{\infty} \frac{1}{10^{k!}}$ Liouville-szám transzcendens.
$\alpha = 0{,}110001000000000000000001000\ldots$

Tegyük föl, hogy $f(\alpha) = 0$, ahol $f(x) = a_0 + \ldots + a_n x^n \in \mathbb{Q}[x]$, (a nevezőkkel felszorozva feltehető, hogy a_i egész), és $a_n \neq 0$.
Legyen $\alpha_N = \sum_{k=1}^{N} \frac{1}{10^{k!}}$, és $\beta_N = \alpha - \alpha_N$. Ekkor
$10^{(N+1)!-1}\beta_N < 1$, mert ez egy 0-val kezdődő végtelen tizedestört.

Transzcendens szám konstrukciója

Algebrai számokat nem lehet kis nevezőjű törtekkel túl jól közelíteni (FGy9.4.1), de az alábbi α-t lehet, mert a sora gyorsan konvergál.

FGy9.4.2: Az $\alpha = \sum_{k=1}^{\infty} \frac{1}{10^{k!}}$ Liouville-szám transzcendens.
$\alpha = 0{,}110001000000000000000001000\ldots$

Tegyük föl, hogy $f(\alpha) = 0$, ahol $f(x) = a_0 + \ldots + a_n x^n \in \mathbb{Q}[x]$, (a nevezőkkel felszorozva feltehető, hogy a_i egész), és $a_n \neq 0$.
Legyen $\alpha_N = \sum_{k=1}^{N} \frac{1}{10^{k!}}$, és $\beta_N = \alpha - \alpha_N$. Ekkor
$10^{(N+1)!-1}\beta_N < 1$, mert ez egy 0-val kezdődő végtelen tizedestört.
$\alpha^m - \alpha_N^m = (\alpha - \alpha_N)(\sum_{i=0}^{m} \alpha^i \alpha_N^{m-i})$

Transzcendens szám konstrukciója

Algebrai számokat nem lehet kis nevezőjű törtekkel túl jól közelíteni (FGy9.4.1), de az alábbi α-t lehet, mert a sora gyorsan konvergál.

FGy9.4.2: Az $\alpha = \sum_{k=1}^{\infty} \frac{1}{10^{k!}}$ Liouville-szám transzcendens.
$\alpha = 0{,}110001000000000000000001000\ldots$

Tegyük föl, hogy $f(\alpha) = 0$, ahol $f(x) = a_0 + \ldots + a_n x^n \in \mathbb{Q}[x]$, (a nevezőkkel felszorozva feltehető, hogy a_i egész), és $a_n \neq 0$.
Legyen $\alpha_N = \sum_{k=1}^{N} \frac{1}{10^{k!}}$, és $\beta_N = \alpha - \alpha_N$. Ekkor
$10^{(N+1)!-1}\beta_N < 1$, mert ez egy 0-val kezdődő végtelen tizedestört.
$\alpha^m - \alpha_N^m = (\alpha - \alpha_N)(\sum_{i=0}^{m} \alpha^i \alpha_N^{m-i}) \leq (\alpha - \alpha_N)(m+1)$,

Transzcendens szám konstrukciója

Algebrai számokat nem lehet kis nevezőjű törtekkel túl jól közelíteni (FGy9.4.1), de az alábbi α-t lehet, mert a sora gyorsan konvergál.

FGy9.4.2: Az $\alpha = \sum_{k=1}^{\infty} \frac{1}{10^{k!}}$ Liouville-szám transzcendens.
$\alpha = 0{,}110001000000000000000001000\ldots$

Tegyük föl, hogy $f(\alpha) = 0$, ahol $f(x) = a_0 + \ldots + a_n x^n \in \mathbb{Q}[x]$, (a nevezőkkel felszorozva feltehető, hogy a_i egész), és $a_n \neq 0$.
Legyen $\alpha_N = \sum_{k=1}^{N} \frac{1}{10^{k!}}$, és $\beta_N = \alpha - \alpha_N$. Ekkor $10^{(N+1)!-1}\beta_N < 1$, mert ez egy 0-val kezdődő végtelen tizedestört.
$\alpha^m - \alpha_N^m = (\alpha - \alpha_N)(\sum_{i=0}^{m} \alpha^i \alpha_N^{m-i}) \leq (\alpha - \alpha_N)(m+1)$, hiszen $0 < \alpha, \alpha_N < 1$.

Transzcendens szám konstrukciója

Algebrai számokat nem lehet kis nevezőjű törtekkel túl jól közelíteni (FGy9.4.1), de az alábbi α-t lehet, mert a sora gyorsan konvergál.

FGy9.4.2: Az $\alpha = \sum_{k=1}^{\infty} \frac{1}{10^{k!}}$ Liouville-szám transzcendens.
$\alpha = 0{,}110001000000000000000001000\ldots$

Tegyük föl, hogy $f(\alpha) = 0$, ahol $f(x) = a_0 + \ldots + a_n x^n \in \mathbb{Q}[x]$, (a nevezőkkel felszorozva feltehető, hogy a_i egész), és $a_n \neq 0$.
Legyen $\alpha_N = \sum_{k=1}^{N} \frac{1}{10^{k!}}$, és $\beta_N = \alpha - \alpha_N$. Ekkor $10^{(N+1)!-1}\beta_N < 1$, mert ez egy 0-val kezdődő végtelen tizedestört.
$\alpha^m - \alpha_N^m = (\alpha - \alpha_N)(\sum_{i=0}^{m} \alpha^i \alpha_N^{m-i}) \leq (\alpha - \alpha_N)(m+1)$, hiszen $0 < \alpha, \alpha_N < 1$. Ezért a háromszög-egyenlőtlenség miatt

Transzcendens szám konstrukciója

Algebrai számokat nem lehet kis nevezőjű törtekkel túl jól közelíteni (FGy9.4.1), de az alábbi α-t lehet, mert a sora gyorsan konvergál.

FGy9.4.2: Az $\alpha = \sum_{k=1}^{\infty} \frac{1}{10^{k!}}$ Liouville-szám transzcendens.
$\alpha = 0{,}110001000000000000000001000\ldots$

Tegyük föl, hogy $f(\alpha) = 0$, ahol $f(x) = a_0 + \ldots + a_n x^n \in \mathbb{Q}[x]$, (a nevezőkkel felszorozva feltehető, hogy a_i egész), és $a_n \neq 0$.
Legyen $\alpha_N = \sum_{k=1}^{N} \frac{1}{10^{k!}}$, és $\beta_N = \alpha - \alpha_N$. Ekkor $10^{(N+1)!-1}\beta_N < 1$, mert ez egy 0-val kezdődő végtelen tizedestört.
$\alpha^m - \alpha_N^m = (\alpha - \alpha_N)(\sum_{i=0}^{m} \alpha^i \alpha_N^{m-i}) \leq (\alpha - \alpha_N)(m+1)$, hiszen $0 < \alpha, \alpha_N < 1$. Ezért a háromszög-egyenlőtlenség miatt $|f(\alpha) - f(\alpha_N)| \leq |\alpha - \alpha_N| K$,

Transzcendens szám konstrukciója

Algebrai számokat nem lehet kis nevezőjű törtekkel túl jól közelíteni (FGy9.4.1), de az alábbi α-t lehet, mert a sora gyorsan konvergál.

FGy9.4.2: Az $\alpha = \sum_{k=1}^{\infty} \frac{1}{10^{k!}}$ Liouville-szám transzcendens.
$\alpha = 0{,}110001000000000000000001000\ldots$

Tegyük föl, hogy $f(\alpha) = 0$, ahol $f(x) = a_0 + \ldots + a_n x^n \in \mathbb{Q}[x]$, (a nevezőkkel felszorozva feltehető, hogy a_i egész), és $a_n \neq 0$.
Legyen $\alpha_N = \sum_{k=1}^{N} \frac{1}{10^{k!}}$, és $\beta_N = \alpha - \alpha_N$. Ekkor $10^{(N+1)!-1}\beta_N < 1$, mert ez egy 0-val kezdődő végtelen tizedestört.
$\alpha^m - \alpha_N^m = (\alpha - \alpha_N)(\sum_{i=0}^{m} \alpha^i \alpha_N^{m-i}) \leq (\alpha - \alpha_N)(m+1)$, hiszen $0 < \alpha, \alpha_N < 1$. Ezért a háromszög-egyenlőtlenség miatt $|f(\alpha) - f(\alpha_N)| \leq |\alpha - \alpha_N| K$, ahol $K = \sum_{i=0}^{n} |a_i|(i+1)$.

Transzcendens szám konstrukciója

Algebrai számokat nem lehet kis nevezőjű törtekkel túl jól közelíteni (FGy9.4.1), de az alábbi α-t lehet, mert a sora gyorsan konvergál.

FGy9.4.2: Az $\alpha = \sum_{k=1}^{\infty} \frac{1}{10^{k!}}$ Liouville-szám transzcendens.
$\alpha = 0{,}110001000000000000000001000\ldots$

Tegyük föl, hogy $f(\alpha) = 0$, ahol $f(x) = a_0 + \ldots + a_n x^n \in \mathbb{Q}[x]$, (a nevezőkkel felszorozva feltehető, hogy a_i egész), és $a_n \neq 0$.
Legyen $\alpha_N = \sum_{k=1}^{N} \frac{1}{10^{k!}}$, és $\beta_N = \alpha - \alpha_N$. Ekkor $10^{(N+1)!-1}\beta_N < 1$, mert ez egy 0-val kezdődő végtelen tizedestört.
$\alpha^m - \alpha_N^m = (\alpha - \alpha_N)(\sum_{i=0}^{m} \alpha^i \alpha_N^{m-i}) \leq (\alpha - \alpha_N)(m+1)$, hiszen $0 < \alpha, \alpha_N < 1$. Ezért a háromszög-egyenlőtlenség miatt $|f(\alpha) - f(\alpha_N)| \leq |\alpha - \alpha_N| K$, ahol $K = \sum_{i=0}^{n} |a_i|(i+1)$.
Itt $f(\alpha) = 0$

Transzcendens szám konstrukciója

Algebrai számokat nem lehet kis nevezőjű törtekkel túl jól közelíteni (FGy9.4.1), de az alábbi α-t lehet, mert a sora gyorsan konvergál.

FGy9.4.2: Az $\alpha = \sum_{k=1}^{\infty} \frac{1}{10^{k!}}$ Liouville-szám transzcendens.
$\alpha = 0{,}110001000000000000000001000\ldots$

Tegyük föl, hogy $f(\alpha) = 0$, ahol $f(x) = a_0 + \ldots + a_n x^n \in \mathbb{Q}[x]$, (a nevezőkkel felszorozva feltehető, hogy a_i egész), és $a_n \neq 0$.
Legyen $\alpha_N = \sum_{k=1}^{N} \frac{1}{10^{k!}}$, és $\beta_N = \alpha - \alpha_N$. Ekkor $10^{(N+1)!-1}\beta_N < 1$, mert ez egy 0-val kezdődő végtelen tizedestört.
$\alpha^m - \alpha_N^m = (\alpha - \alpha_N)(\sum_{i=0}^{m} \alpha^i \alpha_N^{m-i}) \leq (\alpha - \alpha_N)(m+1)$, hiszen $0 < \alpha, \alpha_N < 1$. Ezért a háromszög-egyenlőtlenség miatt $|f(\alpha) - f(\alpha_N)| \leq |\alpha - \alpha_N| K$, ahol $K = \sum_{i=0}^{n} |a_i|(i+1)$.
Itt $f(\alpha) = 0$ és $10^{nN!} f(\alpha_N)$ egész szám.

Transzcendens szám konstrukciója

Algebrai számokat nem lehet kis nevezőjű törtekkel túl jól közelíteni (FGy9.4.1), de az alábbi α-t lehet, mert a sora gyorsan konvergál.

FGy9.4.2: Az $\alpha = \sum_{k=1}^{\infty} \frac{1}{10^{k!}}$ Liouville-szám transzcendens.
$\alpha = 0{,}110001000000000000000001000\ldots$

Tegyük föl, hogy $f(\alpha) = 0$, ahol $f(x) = a_0 + \ldots + a_n x^n \in \mathbb{Q}[x]$, (a nevezőkkel felszorozva feltehető, hogy a_i egész), és $a_n \neq 0$.
Legyen $\alpha_N = \sum_{k=1}^{N} \frac{1}{10^{k!}}$, és $\beta_N = \alpha - \alpha_N$. Ekkor $10^{(N+1)!-1}\beta_N < 1$, mert ez egy 0-val kezdődő végtelen tizedestört.
$\alpha^m - \alpha_N^m = (\alpha - \alpha_N)(\sum_{i=0}^{m} \alpha^i \alpha_N^{m-i}) \leq (\alpha - \alpha_N)(m+1)$, hiszen $0 < \alpha, \alpha_N < 1$. Ezért a háromszög-egyenlőtlenség miatt $|f(\alpha) - f(\alpha_N)| \leq |\alpha - \alpha_N| K$, ahol $K = \sum_{i=0}^{n} |a_i|(i+1)$.
Itt $f(\alpha) = 0$ és $10^{nN!} f(\alpha_N)$ egész szám. Vagyis $10^{nN!}|f(\alpha_N)| \leq 10^{nN!}\beta_N K$

Transzcendens szám konstrukciója

Algebrai számokat nem lehet kis nevezőjű törtekkel túl jól közelíteni (FGy9.4.1), de az alábbi α-t lehet, mert a sora gyorsan konvergál.

FGy9.4.2: Az $\alpha = \sum_{k=1}^{\infty} \frac{1}{10^{k!}}$ Liouville-szám transzcendens.
$\alpha = 0{,}110001000000000000000001000\ldots$

Tegyük föl, hogy $f(\alpha) = 0$, ahol $f(x) = a_0 + \ldots + a_n x^n \in \mathbb{Q}[x]$, (a nevezőkkel felszorozva feltehető, hogy a_i egész), és $a_n \neq 0$.
Legyen $\alpha_N = \sum_{k=1}^{N} \frac{1}{10^{k!}}$, és $\beta_N = \alpha - \alpha_N$. Ekkor $10^{(N+1)!-1}\beta_N < 1$, mert ez egy 0-val kezdődő végtelen tizedestört.
$\alpha^m - \alpha_N^m = (\alpha - \alpha_N)(\sum_{i=0}^{m} \alpha^i \alpha_N^{m-i}) \leq (\alpha - \alpha_N)(m+1)$, hiszen $0 < \alpha, \alpha_N < 1$. Ezért a háromszög-egyenlőtlenség miatt $|f(\alpha) - f(\alpha_N)| \leq |\alpha - \alpha_N| K$, ahol $K = \sum_{i=0}^{n} |a_i|(i+1)$.
Itt $f(\alpha) = 0$ és $10^{nN!} f(\alpha_N)$ egész szám. Vagyis $10^{nN!}|f(\alpha_N)| \leq 10^{nN!}\beta_N K \leq \frac{K}{10^{(N+1)!-nN!-1}} < 1$ elég nagy N-re.

Transzcendens szám konstrukciója

Algebrai számokat nem lehet kis nevezőjű törtekkel túl jól közelíteni (FGy9.4.1), de az alábbi α-t lehet, mert a sora gyorsan konvergál.

FGy9.4.2: Az $\alpha = \sum_{k=1}^{\infty} \frac{1}{10^{k!}}$ Liouville-szám transzcendens.
$\alpha = 0{,}110001000000000000000001000\ldots$

Tegyük föl, hogy $f(\alpha) = 0$, ahol $f(x) = a_0 + \ldots + a_n x^n \in \mathbb{Q}[x]$, (a nevezőkkel felszorozva feltehető, hogy a_i egész), és $a_n \neq 0$.
Legyen $\alpha_N = \sum_{k=1}^{N} \frac{1}{10^{k!}}$, és $\beta_N = \alpha - \alpha_N$. Ekkor $10^{(N+1)!-1}\beta_N < 1$, mert ez egy 0-val kezdődő végtelen tizedestört.
$\alpha^m - \alpha_N^m = (\alpha - \alpha_N)(\sum_{i=0}^{m} \alpha^i \alpha_N^{m-i}) \leq (\alpha - \alpha_N)(m+1)$, hiszen $0 < \alpha, \alpha_N < 1$. Ezért a háromszög-egyenlőtlenség miatt $|f(\alpha) - f(\alpha_N)| \leq |\alpha - \alpha_N| K$, ahol $K = \sum_{i=0}^{n} |a_i|(i+1)$.
Itt $f(\alpha) = 0$ és $10^{nN!} f(\alpha_N)$ egész szám. Vagyis $10^{nN!}|f(\alpha_N)| \leq 10^{nN!}\beta_N K \leq \frac{K}{10^{(N+1)!-nN!-1}} < 1$ elég nagy N-re.
Azaz $f(\alpha_N) = 0$,

Transzcendens szám konstrukciója

Algebrai számokat nem lehet kis nevezőjű törtekkel túl jól közelíteni (FGy9.4.1), de az alábbi α-t lehet, mert a sora gyorsan konvergál.

FGy9.4.2: Az $\alpha = \sum_{k=1}^{\infty} \frac{1}{10^{k!}}$ Liouville-szám transzcendens.
$\alpha = 0{,}110001000000000000000001000\ldots$

Tegyük föl, hogy $f(\alpha) = 0$, ahol $f(x) = a_0 + \ldots + a_n x^n \in \mathbb{Q}[x]$, (a nevezőkkel felszorozva feltehető, hogy a_i egész), és $a_n \neq 0$.
Legyen $\alpha_N = \sum_{k=1}^{N} \frac{1}{10^{k!}}$, és $\beta_N = \alpha - \alpha_N$. Ekkor $10^{(N+1)!-1}\beta_N < 1$, mert ez egy 0-val kezdődő végtelen tizedestört.
$\alpha^m - \alpha_N^m = (\alpha - \alpha_N)(\sum_{i=0}^{m} \alpha^i \alpha_N^{m-i}) \leq (\alpha - \alpha_N)(m+1)$, hiszen $0 < \alpha, \alpha_N < 1$. Ezért a háromszög-egyenlőtlenség miatt $|f(\alpha) - f(\alpha_N)| \leq |\alpha - \alpha_N| K$, ahol $K = \sum_{i=0}^{n} |a_i|(i+1)$.
Itt $f(\alpha) = 0$ és $10^{nN!} f(\alpha_N)$ egész szám. Vagyis $10^{nN!}|f(\alpha_N)| \leq 10^{nN!}\beta_N K \leq \frac{K}{10^{(N+1)!-nN!-1}} < 1$ elég nagy N-re.
Azaz $f(\alpha_N) = 0$, ami nem teljesülhet végtelen sok N-re. □

Négyzetszámok összege

Hány négyzetszám összegeként áll elő egy (pozitív) egész szám?

Négyzetszámok összege

Hány négyzetszám összegeként áll elő egy (pozitív) egész szám?
Négyzetszám 8-cal osztva 0-t, 1-et vagy 4-et ad maradékul.

Négyzetszámok összege

Hány négyzetszám összegeként áll elő egy (pozitív) egész szám?
Négyzetszám 8-cal osztva 0-t, 1-et vagy 4-et ad maradékul.
Ezért három nem elég a $8k + 7$ alakúakhoz.

Négyzetszámok összege

Hány négyzetszám összegeként áll elő egy (pozitív) egész szám?
Négyzetszám 8-cal osztva 0-t, 1-et vagy 4-et ad maradékul.
Ezért három nem elég a $8k + 7$ alakúakhoz.

Lagrange és Jacobi tétele (FGy7.5.3, NB)

Minden $n > 0$ egész előáll négy négyzetszám összegeként.

Négyzetszámok összege

Hány négyzetszám összegeként áll elő egy (pozitív) egész szám?
Négyzetszám 8-cal osztva 0-t, 1-et vagy 4-et ad maradékul.
Ezért három nem elég a $8k + 7$ alakúakhoz.

Lagrange és Jacobi tétele (FGy7.5.3, NB)

Minden $n > 0$ egész előáll négy négyzetszám összegeként.
A megoldások száma páratlan n esetén $8\sigma(n)$,

Négyzetszámok összege

Hány négyzetszám összegeként áll elő egy (pozitív) egész szám?
Négyzetszám 8-cal osztva 0-t, 1-et vagy 4-et ad maradékul.
Ezért három nem elég a $8k + 7$ alakúakhoz.

Lagrange és Jacobi tétele (FGy7.5.3, NB)

Minden $n > 0$ egész előáll négy négyzetszám összegeként.
A megoldások száma páratlan n esetén $8\sigma(n)$,
páros n-re pedig 24-szer az n páratlan osztóinak összege.

Négyzetszámok összege

Hány négyzetszám összegeként áll elő egy (pozitív) egész szám?
Négyzetszám 8-cal osztva 0-t, 1-et vagy 4-et ad maradékul.
Ezért három nem elég a $8k + 7$ alakúakhoz.

Lagrange és Jacobi tétele (FGy7.5.3, NB)

Minden $n > 0$ egész előáll négy négyzetszám összegeként.
A megoldások száma páratlan n esetén $8\sigma(n)$,
páros n-re pedig 24-szer az n páratlan osztóinak összege.

Három négyzetszám tétel (FGy7.5.2, NB)

A $4^m(8k + 7)$ alakú számok nem állnak elő három négyzetszám összegeként,

Négyzetszámok összege

Hány négyzetszám összegeként áll elő egy (pozitív) egész szám?
Négyzetszám 8-cal osztva 0-t, 1-et vagy 4-et ad maradékul.
Ezért három nem elég a $8k + 7$ alakúakhoz.

Lagrange és Jacobi tétele (FGy7.5.3, NB)

Minden $n > 0$ egész előáll négy négyzetszám összegeként.
A megoldások száma páratlan n esetén $8\sigma(n)$,
páros n-re pedig 24-szer az n páratlan osztóinak összege.

Három négyzetszám tétel (FGy7.5.2, NB)

A $4^m(8k + 7)$ alakú számok nem állnak elő három négyzetszám összegeként, a többiek igen.

Négyzetszámok összege

Hány négyzetszám összegeként áll elő egy (pozitív) egész szám?
Négyzetszám 8-cal osztva 0-t, 1-et vagy 4-et ad maradékul.
Ezért három nem elég a $8k + 7$ alakúakhoz.

Lagrange és Jacobi tétele (FGy7.5.3, NB)

Minden $n > 0$ egész előáll négy négyzetszám összegeként.
A megoldások száma páratlan n esetén $8\sigma(n)$,
páros n-re pedig 24-szer az n páratlan osztóinak összege.

Három négyzetszám tétel (FGy7.5.2, NB)

A $4^m(8k + 7)$ alakú számok nem állnak elő három négyzetszám összegeként, a többiek igen.

Azt, hogy a $4^m(8k + 7)$ alakú számok nem állnak elő,

Négyzetszámok összege

Hány négyzetszám összegeként áll elő egy (pozitív) egész szám?
Négyzetszám 8-cal osztva 0-t, 1-et vagy 4-et ad maradékul.
Ezért három nem elég a $8k + 7$ alakúakhoz.

Lagrange és Jacobi tétele (FGy7.5.3, NB)

Minden $n > 0$ egész előáll négy négyzetszám összegeként.
A megoldások száma páratlan n esetén $8\sigma(n)$,
páros n-re pedig 24-szer az n páratlan osztóinak összege.

Három négyzetszám tétel (FGy7.5.2, NB)

A $4^m(8k + 7)$ alakú számok nem állnak elő három négyzetszám összegeként, a többiek igen.

Azt, hogy a $4^m(8k + 7)$ alakú számok nem állnak elő,
a 8-cal való osztási maradékok vizsgálatával láthatjuk (HF).

Négyzetszámok összege

Hány négyzetszám összegeként áll elő egy (pozitív) egész szám?
Négyzetszám 8-cal osztva 0-t, 1-et vagy 4-et ad maradékul.
Ezért három nem elég a $8k + 7$ alakúakhoz.

Lagrange és Jacobi tétele (FGy7.5.3, NB)

Minden $n > 0$ egész előáll négy négyzetszám összegeként.
A megoldások száma páratlan n esetén $8\sigma(n)$,
páros n-re pedig 24-szer az n páratlan osztóinak összege.

Három négyzetszám tétel (FGy7.5.2, NB)

A $4^m(8k + 7)$ alakú számok nem állnak elő három négyzetszám összegeként, a többiek igen.

Azt, hogy a $4^m(8k + 7)$ alakú számok nem állnak elő,
a 8-cal való osztási maradékok vizsgálatával láthatjuk (HF).
A másik irány bizonyítása nagyon nehéz.

A két négyzetszám tétel

Tétel (FGy7.5.1)

Az $n > 0$ pontosan akkor áll elő két négyzetszám összegeként, ha a kanonikus alakjában a $4k - 1$ alakú prímek kitevője páros.

A két négyzetszám tétel

Tétel (FGy7.5.1)

Az $n > 0$ pontosan akkor áll elő két négyzetszám összegeként, ha a kanonikus alakjában a $4k - 1$ alakú prímek kitevője páros.

Mivel egy négyzetszám 4-gyel osztva csak 0 vagy 1 maradékot adhat,

A két négyzetszám tétel

Tétel (FGy7.5.1)

Az $n > 0$ pontosan akkor áll elő két négyzetszám összegeként, ha a kanonikus alakjában a $4k - 1$ alakú prímek kitevője páros.

Mivel egy négyzetszám 4-gyel osztva csak 0 vagy 1 maradékot adhat, egy $4k - 1$ alakú szám nem lehet két négyzetszám összege.

A két négyzetszám tétel

Tétel (FGy7.5.1)

Az $n > 0$ pontosan akkor áll elő két négyzetszám összegeként, ha a kanonikus alakjában a $4k - 1$ alakú prímek kitevője páros.

Mivel egy négyzetszám 4-gyel osztva csak 0 vagy 1 maradékot adhat, egy $4k - 1$ alakú szám nem lehet két négyzetszám összege. De a 21 sem áll elő,

A két négyzetszám tétel

Tétel (FGy7.5.1)

Az $n > 0$ pontosan akkor áll elő két négyzetszám összegeként, ha a kanonikus alakjában a $4k - 1$ alakú prímek kitevője páros.

Mivel egy négyzetszám 4-gyel osztva csak 0 vagy 1 maradékot adhat, egy $4k - 1$ alakú szám nem lehet két négyzetszám összege. De a 21 sem áll elő, pedig $4k + 1$ alakú.

A két négyzetszám tétel

Tétel (FGy7.5.1)

Az $n > 0$ pontosan akkor áll elő két négyzetszám összegeként, ha a kanonikus alakjában a $4k - 1$ alakú prímek kitevője páros.

Mivel egy négyzetszám 4-gyel osztva csak 0 vagy 1 maradékot adhat, egy $4k - 1$ alakú szám nem lehet két négyzetszám összege. De a 21 sem áll elő, pedig $4k + 1$ alakú. Mi ennek az oka?

A két négyzetszám tétel

Tétel (FGy7.5.1)

Az $n > 0$ pontosan akkor áll elő két négyzetszám összegeként, ha a kanonikus alakjában a $4k - 1$ alakú prímek kitevője páros.

Mivel egy négyzetszám 4-gyel osztva csak 0 vagy 1 maradékot adhat, egy $4k - 1$ alakú szám nem lehet két négyzetszám összege. De a 21 sem áll elő, pedig $4k + 1$ alakú. Mi ennek az oka?

Tegyük föl, hogy p páratlan prím,

A két négyzetszám tétel

Tétel (FGy7.5.1)

Az $n > 0$ pontosan akkor áll elő két négyzetszám összegeként, ha a kanonikus alakjában a $4k - 1$ alakú prímek kitevője páros.

Mivel egy négyzetszám 4-gyel osztva csak 0 vagy 1 maradékot adhat, egy $4k - 1$ alakú szám nem lehet két négyzetszám összege. De a 21 sem áll elő, pedig $4k + 1$ alakú. Mi ennek az oka?

Tegyük föl, hogy p páratlan prím, és $p \mid n = a^2 + b^2$.

A két négyzetszám tétel

Tétel (FGy7.5.1)

Az $n > 0$ pontosan akkor áll elő két négyzetszám összegeként, ha a kanonikus alakjában a $4k - 1$ alakú prímek kitevője páros.

Mivel egy négyzetszám 4-gyel osztva csak 0 vagy 1 maradékot adhat, egy $4k - 1$ alakú szám nem lehet két négyzetszám összege. De a 21 sem áll elő, pedig $4k + 1$ alakú. Mi ennek az oka?

Tegyük föl, hogy p páratlan prím, és $p \mid n = a^2 + b^2$. Ekkor $a^2 \equiv -b^2 \ (p)$.

A két négyzetszám tétel

Tétel (FGy7.5.1)

Az $n > 0$ pontosan akkor áll elő két négyzetszám összegeként, ha a kanonikus alakjában a $4k - 1$ alakú prímek kitevője páros.

Mivel egy négyzetszám 4-gyel osztva csak 0 vagy 1 maradékot adhat, egy $4k - 1$ alakú szám nem lehet két négyzetszám összege. De a 21 sem áll elő, pedig $4k + 1$ alakú. Mi ennek az oka?

Tegyük föl, hogy p páratlan prím, és $p \mid n = a^2 + b^2$. Ekkor $a^2 \equiv -b^2 \ (p)$. Ha $p \nmid a, b$, akkor b-nek van egy c inverze mod p.

A két négyzetszám tétel

Tétel (FGy7.5.1)

Az $n > 0$ pontosan akkor áll elő két négyzetszám összegeként, ha a kanonikus alakjában a $4k-1$ alakú prímek kitevője páros.

Mivel egy négyzetszám 4-gyel osztva csak 0 vagy 1 maradékot adhat, egy $4k-1$ alakú szám nem lehet két négyzetszám összege. De a 21 sem áll elő, pedig $4k+1$ alakú. Mi ennek az oka?

Tegyük föl, hogy p páratlan prím, és $p \mid n = a^2 + b^2$. Ekkor $a^2 \equiv -b^2 \ (p)$. Ha $p \nmid a, b$, akkor b-nek van egy c inverze mod p. Ezzel szorozva $(ac)^2 \equiv -(bc)^2 \equiv -1 \ (p)$.

A két négyzetszám tétel

Tétel (FGy7.5.1)

Az $n > 0$ pontosan akkor áll elő két négyzetszám összegeként, ha a kanonikus alakjában a $4k-1$ alakú prímek kitevője páros.

Mivel egy négyzetszám 4-gyel osztva csak 0 vagy 1 maradékot adhat, egy $4k-1$ alakú szám nem lehet két négyzetszám összege. De a 21 sem áll elő, pedig $4k+1$ alakú. Mi ennek az oka?

Tegyük föl, hogy p páratlan prím, és $p \mid n = a^2 + b^2$. Ekkor $a^2 \equiv -b^2 \ (p)$. Ha $p \nmid a, b$, akkor b-nek van egy c inverze mod p. Ezzel szorozva $(ac)^2 \equiv -(bc)^2 \equiv -1 \ (p)$. Ezért -1 kvadratikus maradék mod p,

A két négyzetszám tétel

Tétel (FGy7.5.1)

Az $n > 0$ pontosan akkor áll elő két négyzetszám összegeként, ha a kanonikus alakjában a $4k-1$ alakú prímek kitevője páros.

Mivel egy négyzetszám 4-gyel osztva csak 0 vagy 1 maradékot adhat, egy $4k-1$ alakú szám nem lehet két négyzetszám összege. De a 21 sem áll elő, pedig $4k+1$ alakú. Mi ennek az oka?

Tegyük föl, hogy p páratlan prím, és $p \mid n = a^2 + b^2$. Ekkor $a^2 \equiv -b^2 \ (p)$. Ha $p \nmid a, b$, akkor b-nek van egy c inverze mod p. Ezzel szorozva $(ac)^2 \equiv -(bc)^2 \equiv -1 \ (p)$. Ezért -1 kvadratikus maradék mod p, és többféleképpen is láttuk, hogy p szükségképpen $4k+1$ alakú.

A két négyzetszám tétel

Tétel (FGy7.5.1)

Az $n > 0$ pontosan akkor áll elő két négyzetszám összegeként, ha a kanonikus alakjában a $4k-1$ alakú prímek kitevője páros.

Mivel egy négyzetszám 4-gyel osztva csak 0 vagy 1 maradékot adhat, egy $4k-1$ alakú szám nem lehet két négyzetszám összege. De a 21 sem áll elő, pedig $4k+1$ alakú. Mi ennek az oka?

Tegyük föl, hogy p páratlan prím, és $p \mid n = a^2 + b^2$. Ekkor $a^2 \equiv -b^2 \ (p)$. Ha $p \nmid a, b$, akkor b-nek van egy c inverze mod p. Ezzel szorozva $(ac)^2 \equiv -(bc)^2 \equiv -1 \ (p)$. Ezért -1 kvadratikus maradék mod p, és többféleképpen is láttuk, hogy p szükségképpen $4k+1$ alakú. Ezért $4k-1$ alakú p esetén p osztja a és b valamelyikét.

A két négyzetszám tétel

Tétel (FGy7.5.1)

Az $n > 0$ pontosan akkor áll elő két négyzetszám összegeként, ha a kanonikus alakjában a $4k-1$ alakú prímek kitevője páros.

Mivel egy négyzetszám 4-gyel osztva csak 0 vagy 1 maradékot adhat, egy $4k-1$ alakú szám nem lehet két négyzetszám összege. De a 21 sem áll elő, pedig $4k+1$ alakú. Mi ennek az oka?

Tegyük föl, hogy p páratlan prím, és $p \mid n = a^2 + b^2$. Ekkor $a^2 \equiv -b^2 \ (p)$. Ha $p \nmid a, b$, akkor b-nek van egy c inverze mod p. Ezzel szorozva $(ac)^2 \equiv -(bc)^2 \equiv -1 \ (p)$. Ezért -1 kvadratikus maradék mod p, és többféleképpen is láttuk, hogy p szükségképpen $4k+1$ alakú. Ezért $4k-1$ alakú p esetén p osztja a és b valamelyikét. De ha pl. $p \mid a$,

A két négyzetszám tétel

Tétel (FGy7.5.1)

Az $n > 0$ pontosan akkor áll elő két négyzetszám összegeként, ha a kanonikus alakjában a $4k-1$ alakú prímek kitevője páros.

Mivel egy négyzetszám 4-gyel osztva csak 0 vagy 1 maradékot adhat, egy $4k-1$ alakú szám nem lehet két négyzetszám összege. De a 21 sem áll elő, pedig $4k+1$ alakú. Mi ennek az oka?

Tegyük föl, hogy p páratlan prím, és $p \mid n = a^2 + b^2$. Ekkor $a^2 \equiv -b^2 \ (p)$. Ha $p \nmid a, b$, akkor b-nek van egy c inverze mod p. Ezzel szorozva $(ac)^2 \equiv -(bc)^2 \equiv -1 \ (p)$. Ezért -1 kvadratikus maradék mod p, és többféleképpen is láttuk, hogy p szükségképpen $4k+1$ alakú. Ezért $4k-1$ alakú p esetén p osztja a és b valamelyikét. De ha pl. $p \mid a$, akkor $p \mid b^2$,

A két négyzetszám tétel

Tétel (FGy7.5.1)

Az $n > 0$ pontosan akkor áll elő két négyzetszám összegeként, ha a kanonikus alakjában a $4k-1$ alakú prímek kitevője páros.

Mivel egy négyzetszám 4-gyel osztva csak 0 vagy 1 maradékot adhat, egy $4k-1$ alakú szám nem lehet két négyzetszám összege. De a 21 sem áll elő, pedig $4k+1$ alakú. Mi ennek az oka?

Tegyük föl, hogy p páratlan prím, és $p \mid n = a^2 + b^2$. Ekkor $a^2 \equiv -b^2 \ (p)$. Ha $p \nmid a, b$, akkor b-nek van egy c inverze mod p. Ezzel szorozva $(ac)^2 \equiv -(bc)^2 \equiv -1 \ (p)$. Ezért -1 kvadratikus maradék mod p, és többféleképpen is láttuk, hogy p szükségképpen $4k+1$ alakú. Ezért $4k-1$ alakú p esetén p osztja a és b valamelyikét. De ha pl. $p \mid a$, akkor $p \mid b^2$, ezért $p \mid b$,

A két négyzetszám tétel

Tétel (FGy7.5.1)

Az $n > 0$ pontosan akkor áll elő két négyzetszám összegeként, ha a kanonikus alakjában a $4k-1$ alakú prímek kitevője páros.

Mivel egy négyzetszám 4-gyel osztva csak 0 vagy 1 maradékot adhat, egy $4k-1$ alakú szám nem lehet két négyzetszám összege. De a 21 sem áll elő, pedig $4k+1$ alakú. Mi ennek az oka?

Tegyük föl, hogy p páratlan prím, és $p \mid n = a^2 + b^2$. Ekkor $a^2 \equiv -b^2 \ (p)$. Ha $p \nmid a, b$, akkor b-nek van egy c inverze mod p. Ezzel szorozva $(ac)^2 \equiv -(bc)^2 \equiv -1 \ (p)$. Ezért -1 kvadratikus maradék mod p, és többféleképpen is láttuk, hogy p szükségképpen $4k+1$ alakú. Ezért $4k-1$ alakú p esetén p osztja a és b valamelyikét. De ha pl. $p \mid a$, akkor $p \mid b^2$, ezért $p \mid b$, azaz $p^2 \mid n$,

A két négyzetszám tétel

Tétel (FGy7.5.1)

Az $n > 0$ pontosan akkor áll elő két négyzetszám összegeként, ha a kanonikus alakjában a $4k-1$ alakú prímek kitevője páros.

Mivel egy négyzetszám 4-gyel osztva csak 0 vagy 1 maradékot adhat, egy $4k-1$ alakú szám nem lehet két négyzetszám összege. De a 21 sem áll elő, pedig $4k+1$ alakú. Mi ennek az oka?

Tegyük föl, hogy p páratlan prím, és $p \mid n = a^2 + b^2$. Ekkor $a^2 \equiv -b^2 \ (p)$. Ha $p \nmid a, b$, akkor b-nek van egy c inverze mod p. Ezzel szorozva $(ac)^2 \equiv -(bc)^2 \equiv -1 \ (p)$. Ezért -1 kvadratikus maradék mod p, és többféleképpen is láttuk, hogy p szükségképpen $4k+1$ alakú. Ezért $4k-1$ alakú p esetén p osztja a és b valamelyikét. De ha pl. $p \mid a$, akkor $p \mid b^2$, ezért $p \mid b$, azaz $p^2 \mid n$, és egyszerűsíthetünk p^2-tel.

A két négyzetszám tétel

Tétel (FGy7.5.1)

Az $n > 0$ pontosan akkor áll elő két négyzetszám összegeként, ha a kanonikus alakjában a $4k-1$ alakú prímek kitevője páros.

Mivel egy négyzetszám 4-gyel osztva csak 0 vagy 1 maradékot adhat, egy $4k-1$ alakú szám nem lehet két négyzetszám összege. De a 21 sem áll elő, pedig $4k+1$ alakú. Mi ennek az oka?

Tegyük föl, hogy p páratlan prím, és $p \mid n = a^2 + b^2$. Ekkor $a^2 \equiv -b^2 \ (p)$. Ha $p \nmid a, b$, akkor b-nek van egy c inverze mod p. Ezzel szorozva $(ac)^2 \equiv -(bc)^2 \equiv -1 \ (p)$. Ezért -1 kvadratikus maradék mod p, és többféleképpen is láttuk, hogy p szükségképpen $4k+1$ alakú. Ezért $4k-1$ alakú p esetén p osztja a és b valamelyikét. De ha pl. $p \mid a$, akkor $p \mid b^2$, ezért $p \mid b$, azaz $p^2 \mid n$, és egyszerűsíthetünk p^2-tel. Az eljárást folytatva látjuk, hogy p kitevője páros n-ben.

A két négyzetszám tétel

Tétel (FGy7.5.1)

Az $n > 0$ pontosan akkor áll elő két négyzetszám összegeként, ha a kanonikus alakjában a $4k-1$ alakú prímek kitevője páros.

Mivel egy négyzetszám 4-gyel osztva csak 0 vagy 1 maradékot adhat, egy $4k-1$ alakú szám nem lehet két négyzetszám összege. De a 21 sem áll elő, pedig $4k+1$ alakú. Mi ennek az oka?

Tegyük föl, hogy p páratlan prím, és $p \mid n = a^2 + b^2$. Ekkor $a^2 \equiv -b^2 \ (p)$. Ha $p \nmid a, b$, akkor b-nek van egy c inverze mod p. Ezzel szorozva $(ac)^2 \equiv -(bc)^2 \equiv -1 \ (p)$. Ezért -1 kvadratikus maradék mod p, és többféleképpen is láttuk, hogy p szükségképpen $4k+1$ alakú. Ezért $4k-1$ alakú p esetén p osztja a és b valamelyikét. De ha pl. $p \mid a$, akkor $p \mid b^2$, ezért $p \mid b$, azaz $p^2 \mid n$, és egyszerűsíthetünk p^2-tel. Az eljárást folytatva látjuk, hogy p kitevője páros n-ben. Ezzel a feltétel szükségességét beláttuk.

Gauss-prímek

A tétel megfordítása a Gauss-egészek $\mathbb{G}$ gyűrűjének vizsgálatával igazolható,

Gauss-prímek

A tétel megfordítása a Gauss-egészek $\mathbb{G}$ gyűrűjének vizsgálatával igazolható, megkapjuk a felbontások számát is.

Gauss-prímek

A tétel megfordítása a Gauss-egészek $\mathbb{G}$ gyűrűjének vizsgálatával igazolható, megkapjuk a felbontások számát is. Vázoljuk a főbb gondolatokat, részletek a FGy-könyv 7.4. szakaszában olvashatók.

Gauss-prímek

A tétel megfordítása a Gauss-egészek $\mathbb{G}$ gyűrűjének vizsgálatával igazolható, megkapjuk a felbontások számát is. Vázoljuk a főbb gondolatokat, részletek a FGy-könyv 7.4. szakaszában olvashatók.

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

Gauss-prímek

A tétel megfordítása a Gauss-egészek $\mathbb{G}$ gyűrűjének vizsgálatával igazolható, megkapjuk a felbontások számát is. Vázoljuk a főbb gondolatokat, részletek a FGy-könyv 7.4. szakaszában olvashatók.

(1) A Gauss-egészek az $a + bi$ alakú számok, ahol $a, b \in \mathbb{Z}$. Euklideszi gyűrűt alkotnak az $N(a + bi) = a^2 + b^2$ „normára” nézve.

Gauss-prímek

A tétel megfordítása a Gauss-egészek $\mathbb{G}$ gyűrűjének vizsgálatával igazolható, megkapjuk a felbontások számát is. Vázoljuk a főbb gondolatokat, részletek a FGy-könyv 7.4. szakaszában olvashatók.

(1) A Gauss-egészek az $a + bi$ alakú számok, ahol $a, b \in \mathbb{Z}$. Euklideszi gyűrűt alkotnak az $N(a + bi) = a^2 + b^2$ „normára" nézve. Az $\alpha : \beta$ maradékos osztás elvégzésekor a hányados az α/β számhoz legközelebbi Gauss-egész lesz.

Gauss-prímek

A tétel megfordítása a Gauss-egészek $\mathbb{G}$ gyűrűjének vizsgálatával igazolható, megkapjuk a felbontások számát is. Vázoljuk a főbb gondolatokat, részletek a FGy-könyv 7.4. szakaszában olvashatók.

(1) A Gauss-egészek az $a+bi$ alakú számok, ahol $a, b \in \mathbb{Z}$. Euklideszi gyűrűt alkotnak az $N(a+bi) = a^2+b^2$ „normára" nézve. Az $\alpha : \beta$ maradékos osztás elvégzésekor a hányados az α/β számhoz legközelebbi Gauss-egész lesz.

(2) A norma multiplikatív: $N(\alpha\beta) = N(\alpha)N(\beta)$.

Gauss-prímek

A tétel megfordítása a Gauss-egészek $\mathbb{G}$ gyűrűjének vizsgálatával igazolható, megkapjuk a felbontások számát is. Vázoljuk a főbb gondolatokat, részletek a FGy-könyv 7.4. szakaszában olvashatók.

(1) A Gauss-egészek az $a+bi$ alakú számok, ahol $a, b \in \mathbb{Z}$. Euklideszi gyűrűt alkotnak az $N(a+bi) = a^2+b^2$ „normára" nézve. Az $\alpha : \beta$ maradékos osztás elvégzésekor a hányados az α/β számhoz legközelebbi Gauss-egész lesz.

(2) A norma multiplikatív: $N(\alpha\beta) = N(\alpha)N(\beta)$. Az egységek ± 1, $\pm i$;

Gauss-prímek

A tétel megfordítása a Gauss-egészek $\mathbb{G}$ gyűrűjének vizsgálatával igazolható, megkapjuk a felbontások számát is. Vázoljuk a főbb gondolatokat, részletek a FGy-könyv 7.4. szakaszában olvashatók.

(1) A Gauss-egészek az $a+bi$ alakú számok, ahol $a, b \in \mathbb{Z}$. Euklideszi gyűrűt alkotnak az $N(a+bi) = a^2+b^2$ „normára" nézve. Az $\alpha : \beta$ maradékos osztás elvégzésekor a hányados az α/β számhoz legközelebbi Gauss-egész lesz.

(2) A norma multiplikatív: $N(\alpha\beta) = N(\alpha)N(\beta)$. Az egységek ± 1, $\pm i$; azon elemei $\mathbb{G}$-nek, melyek normája 1.

Gauss-prímek

A tétel megfordítása a Gauss-egészek $\mathbb{G}$ gyűrűjének vizsgálatával igazolható, megkapjuk a felbontások számát is. Vázoljuk a főbb gondolatokat, részletek a FGy-könyv 7.4. szakaszában olvashatók.

(1) A Gauss-egészek az $a+bi$ alakú számok, ahol $a, b \in \mathbb{Z}$. Euklideszi gyűrűt alkotnak az $N(a+bi) = a^2+b^2$ „normára" nézve. Az $\alpha : \beta$ maradékos osztás elvégzésekor a hányados az α/β számhoz legközelebbi Gauss-egész lesz.

(2) A norma multiplikatív: $N(\alpha\beta) = N(\alpha)N(\beta)$. Az egységek ± 1, $\pm i$; azon elemei $\mathbb{G}$-nek, melyek normája 1.

(3) Ha p egy $4k+1$ alakú prím, akkor -1 kvadratikus maradék mod p,

Gauss-prímek

A tétel megfordítása a Gauss-egészek $\mathbb{G}$ gyűrűjének vizsgálatával igazolható, megkapjuk a felbontások számát is. Vázoljuk a főbb gondolatokat, részletek a FGy-könyv 7.4. szakaszában olvashatók.

(1) A Gauss-egészek az $a+bi$ alakú számok, ahol $a, b \in \mathbb{Z}$. Euklideszi gyűrűt alkotnak az $N(a+bi) = a^2+b^2$ „normára" nézve. Az $\alpha : \beta$ maradékos osztás elvégzésekor a hányados az α/β számhoz legközelebbi Gauss-egész lesz.

(2) A norma multiplikatív: $N(\alpha\beta) = N(\alpha)N(\beta)$. Az egységek ± 1, $\pm i$; azon elemei $\mathbb{G}$-nek, melyek normája 1.

(3) Ha p egy $4k+1$ alakú prím, akkor -1 kvadratikus maradék mod p, ezért $p \mid a^2+1 = (a+i)(a-i)$ alkalmas a-ra.

Gauss-prímek

A tétel megfordítása a Gauss-egészek $\mathbb{G}$ gyűrűjének vizsgálatával igazolható, megkapjuk a felbontások számát is. Vázoljuk a főbb gondolatokat, részletek a FGy-könyv 7.4. szakaszában olvashatók.

(1) A Gauss-egészek az $a+bi$ alakú számok, ahol $a, b \in \mathbb{Z}$. Euklideszi gyűrűt alkotnak az $N(a+bi) = a^2+b^2$ „normára" nézve. Az $\alpha : \beta$ maradékos osztás elvégzésekor a hányados az α/β számhoz legközelebbi Gauss-egész lesz.

(2) A norma multiplikatív: $N(\alpha\beta) = N(\alpha)N(\beta)$. Az egységek ± 1, $\pm i$; azon elemei $\mathbb{G}$-nek, melyek normája 1.

(3) Ha p egy $4k+1$ alakú prím, akkor -1 kvadratikus maradék mod p, ezért $p \mid a^2+1 = (a+i)(a-i)$ alkalmas a-ra. De $p \nmid a \pm i$,

Gauss-prímek

A tétel megfordítása a Gauss-egészek $\mathbb{G}$ gyűrűjének vizsgálatával igazolható, megkapjuk a felbontások számát is. Vázoljuk a főbb gondolatokat, részletek a FGy-könyv 7.4. szakaszában olvashatók.

(1) A Gauss-egészek az $a+bi$ alakú számok, ahol $a, b \in \mathbb{Z}$. Euklideszi gyűrűt alkotnak az $N(a+bi) = a^2+b^2$ „normára" nézve. Az $\alpha : \beta$ maradékos osztás elvégzésekor a hányados az α/β számhoz legközelebbi Gauss-egész lesz.

(2) A norma multiplikatív: $N(\alpha\beta) = N(\alpha)N(\beta)$. Az egységek ± 1, $\pm i$; azon elemei $\mathbb{G}$-nek, melyek normája 1.

(3) Ha p egy $4k+1$ alakú prím, akkor -1 kvadratikus maradék mod p, ezért $p \mid a^2+1 = (a+i)(a-i)$ alkalmas a-ra. De $p \nmid a \pm i$, ezért p nem prím a Gauss-egészek között.

Gauss-prímek

A tétel megfordítása a Gauss-egészek $\mathbb{G}$ gyűrűjének vizsgálatával igazolható, megkapjuk a felbontások számát is. Vázoljuk a főbb gondolatokat, részletek a FGy-könyv 7.4. szakaszában olvashatók.

(1) A Gauss-egészek az $a+bi$ alakú számok, ahol $a, b \in \mathbb{Z}$. Euklideszi gyűrűt alkotnak az $N(a+bi) = a^2+b^2$ „normára" nézve. Az $\alpha : \beta$ maradékos osztás elvégzésekor a hányados az α/β számhoz legközelebbi Gauss-egész lesz.

(2) A norma multiplikatív: $N(\alpha\beta) = N(\alpha)N(\beta)$. Az egységek ± 1, $\pm i$; azon elemei $\mathbb{G}$-nek, melyek normája 1.

(3) Ha p egy $4k+1$ alakú prím, akkor -1 kvadratikus maradék mod p, ezért $p \mid a^2+1 = (a+i)(a-i)$ alkalmas a-ra. De $p \nmid a \pm i$, ezért p nem prím a Gauss-egészek között. Két konjugált prímre bomlik.

Gauss-prímek

A tétel megfordítása a Gauss-egészek $\mathbb{G}$ gyűrűjének vizsgálatával igazolható, megkapjuk a felbontások számát is. Vázoljuk a főbb gondolatokat, részletek a FGy-könyv 7.4. szakaszában olvashatók.

(1) A Gauss-egészek az $a+bi$ alakú számok, ahol $a, b \in \mathbb{Z}$. Euklideszi gyűrűt alkotnak az $N(a+bi) = a^2+b^2$ „normára" nézve. Az $\alpha : \beta$ maradékos osztás elvégzésekor a hányados az α/β számhoz legközelebbi Gauss-egész lesz.

(2) A norma multiplikatív: $N(\alpha\beta) = N(\alpha)N(\beta)$. Az egységek ± 1, $\pm i$; azon elemei $\mathbb{G}$-nek, melyek normája 1.

(3) Ha p egy $4k+1$ alakú prím, akkor -1 kvadratikus maradék mod p, ezért $p \mid a^2+1 = (a+i)(a-i)$ alkalmas a-ra. De $p \nmid a \pm i$, ezért p nem prím a Gauss-egészek között. Két konjugált prímre bomlik. Példa: $5 = (2+i)(2-i)$.

Gauss-prímek

A tétel megfordítása a Gauss-egészek $\mathbb{G}$ gyűrűjének vizsgálatával igazolható, megkapjuk a felbontások számát is. Vázoljuk a főbb gondolatokat, részletek a FGy-könyv 7.4. szakaszában olvashatók.

(1) A Gauss-egészek az $a+bi$ alakú számok, ahol $a, b \in \mathbb{Z}$. Euklideszi gyűrűt alkotnak az $N(a+bi) = a^2+b^2$ „normára" nézve. Az $\alpha : \beta$ maradékos osztás elvégzésekor a hányados az α/β számhoz legközelebbi Gauss-egész lesz.

(2) A norma multiplikatív: $N(\alpha\beta) = N(\alpha)N(\beta)$. Az egységek ± 1, $\pm i$; azon elemei $\mathbb{G}$-nek, melyek normája 1.

(3) Ha p egy $4k+1$ alakú prím, akkor -1 kvadratikus maradék mod p, ezért $p \mid a^2+1 = (a+i)(a-i)$ alkalmas a-ra. De $p \nmid a \pm i$, ezért p nem prím a Gauss-egészek között. Két konjugált prímre bomlik. Példa: $5 = (2+i)(2-i)$.

(4) A $4k-1$ alakú pozitív prímek, mint pl. a 3, a Gauss-egészek között is prímek.

Gauss-prímek

A tétel megfordítása a Gauss-egészek $\mathbb{G}$ gyűrűjének vizsgálatával igazolható, megkapjuk a felbontások számát is. Vázoljuk a főbb gondolatokat, részletek a FGy-könyv 7.4. szakaszában olvashatók.

(1) A Gauss-egészek az $a+bi$ alakú számok, ahol $a, b \in \mathbb{Z}$. Euklideszi gyűrűt alkotnak az $N(a+bi) = a^2+b^2$ „normára" nézve. Az $\alpha : \beta$ maradékos osztás elvégzésekor a hányados az α/β számhoz legközelebbi Gauss-egész lesz.

(2) A norma multiplikatív: $N(\alpha\beta) = N(\alpha)N(\beta)$. Az egységek ± 1, $\pm i$; azon elemei $\mathbb{G}$-nek, melyek normája 1.

(3) Ha p egy $4k+1$ alakú prím, akkor -1 kvadratikus maradék mod p, ezért $p \mid a^2+1 = (a+i)(a-i)$ alkalmas a-ra. De $p \nmid a \pm i$, ezért p nem prím a Gauss-egészek között. Két konjugált prímre bomlik. Példa: $5 = (2+i)(2-i)$.

(4) A $4k-1$ alakú pozitív prímek, mint pl. a 3, a Gauss-egészek között is prímek. Prím még az $1+i$,

Gauss-prímek

A tétel megfordítása a Gauss-egészek $\mathbb{G}$ gyűrűjének vizsgálatával igazolható, megkapjuk a felbontások számát is. Vázoljuk a főbb gondolatokat, részletek a FGy-könyv 7.4. szakaszában olvashatók.

(1) A Gauss-egészek az $a+bi$ alakú számok, ahol $a, b \in \mathbb{Z}$. Euklideszi gyűrűt alkotnak az $N(a+bi) = a^2+b^2$ „normára" nézve. Az $\alpha : \beta$ maradékos osztás elvégzésekor a hányados az α/β számhoz legközelebbi Gauss-egész lesz.

(2) A norma multiplikatív: $N(\alpha\beta) = N(\alpha)N(\beta)$. Az egységek ± 1, $\pm i$; azon elemei $\mathbb{G}$-nek, melyek normája 1.

(3) Ha p egy $4k+1$ alakú prím, akkor -1 kvadratikus maradék mod p, ezért $p \mid a^2+1 = (a+i)(a-i)$ alkalmas a-ra. De $p \nmid a \pm i$, ezért p nem prím a Gauss-egészek között. Két konjugált prímre bomlik. Példa: $5 = (2+i)(2-i)$.

(4) A $4k-1$ alakú pozitív prímek, mint pl. a 3, a Gauss-egészek között is prímek. Prím még az $1+i$, és az eddig felsoroltak asszociáltjai.

Gauss-prímek

A tétel megfordítása a Gauss-egészek $\mathbb{G}$ gyűrűjének vizsgálatával igazolható, megkapjuk a felbontások számát is. Vázoljuk a főbb gondolatokat, részletek a FGy-könyv 7.4. szakaszában olvashatók.

(1) A Gauss-egészek az $a+bi$ alakú számok, ahol $a, b \in \mathbb{Z}$. Euklideszi gyűrűt alkotnak az $N(a+bi) = a^2+b^2$ „normára" nézve. Az $\alpha : \beta$ maradékos osztás elvégzésekor a hányados az α/β számhoz legközelebbi Gauss-egész lesz.

(2) A norma multiplikatív: $N(\alpha\beta) = N(\alpha)N(\beta)$. Az egységek ± 1, $\pm i$; azon elemei $\mathbb{G}$-nek, melyek normája 1.

(3) Ha p egy $4k+1$ alakú prím, akkor -1 kvadratikus maradék mod p, ezért $p \mid a^2+1 = (a+i)(a-i)$ alkalmas a-ra. De $p \nmid a \pm i$, ezért p nem prím a Gauss-egészek között. Két konjugált prímre bomlik. Példa: $5 = (2+i)(2-i)$.

(4) A $4k-1$ alakú pozitív prímek, mint pl. a 3, a Gauss-egészek között is prímek. Prím még az $1+i$, és az eddig felsoroltak asszociáltjai. Más Gauss-prím nincs.

A megoldások száma

Az $n = x^2 + y^2 = (x + yi)(x - yi)$ összefüggésbe helyettesítsük $x + iy$ kanonikus alakját a Gauss-egészek között.

A megoldások száma

Az $n = x^2 + y^2 = (x + yi)(x - yi)$ összefüggésbe helyettesítsük $x + iy$ kanonikus alakját a Gauss-egészek között. Konjugálással $x - iy$ kanonikus alakja is megkapható.

A megoldások száma

Az $n = x^2 + y^2 = (x + yi)(x - yi)$ összefüggésbe helyettesítsük $x + iy$ kanonikus alakját a Gauss-egészek között. Konjugálással $x - iy$ kanonikus alakja is megkapható. A kettőt összeszorozva,

A megoldások száma

Az $n = x^2 + y^2 = (x + yi)(x - yi)$ összefüggésbe helyettesítsük $x + iy$ kanonikus alakját a Gauss-egészek között. Konjugálással $x - iy$ kanonikus alakja is megkapható. A kettőt összeszorozva, és n kanonikus alakjával összevetve a következő tételt kapjuk.

A megoldások száma

Az $n = x^2 + y^2 = (x + yi)(x - yi)$ összefüggésbe helyettesítsük $x + iy$ kanonikus alakját a Gauss-egészek között. Konjugálással $x - iy$ kanonikus alakja is megkapható. A kettőt összeszorozva, és n kanonikus alakjával összevetve a következő tételt kapjuk.

Tétel (FGy7.5.1)

Legyen n kanonikus alakja $2^\alpha p_1^{\beta_1} \dots p_r^{\beta_r} q_1^{\gamma_1} \dots q_s^{\gamma_s}$,

A megoldások száma

Az $n = x^2 + y^2 = (x + yi)(x - yi)$ összefüggésbe helyettesítsük $x + iy$ kanonikus alakját a Gauss-egészek között. Konjugálással $x - iy$ kanonikus alakja is megkapható. A kettőt összeszorozva, és n kanonikus alakjával összevetve a következő tételt kapjuk.

Tétel (FGy7.5.1)

Legyen n kanonikus alakja $2^\alpha p_1^{\beta_1} \dots p_r^{\beta_r} q_1^{\gamma_1} \dots q_s^{\gamma_s}$, ahol $p_i \equiv 1\ (4)$

A megoldások száma

Az $n = x^2 + y^2 = (x + yi)(x - yi)$ összefüggésbe helyettesítsük $x + iy$ kanonikus alakját a Gauss-egészek között. Konjugálással $x - iy$ kanonikus alakja is megkapható. A kettőt összeszorozva, és n kanonikus alakjával összevetve a következő tételt kapjuk.

Tétel (FGy7.5.1)

Legyen n kanonikus alakja $2^\alpha p_1^{\beta_1} \dots p_r^{\beta_r} q_1^{\gamma_1} \dots q_s^{\gamma_s}$, ahol $p_i \equiv 1\ (4)$ és $q_j \equiv -1\ (4)$.

A megoldások száma

Az $n = x^2 + y^2 = (x + yi)(x - yi)$ összefüggésbe helyettesítsük $x + iy$ kanonikus alakját a Gauss-egészek között. Konjugálással $x - iy$ kanonikus alakja is megkapható. A kettőt összeszorozva, és n kanonikus alakjával összevetve a következő tételt kapjuk.

Tétel (FGy7.5.1)

Legyen n kanonikus alakja $2^\alpha p_1^{\beta_1} \dots p_r^{\beta_r} q_1^{\gamma_1} \dots q_s^{\gamma_s}$, ahol $p_i \equiv 1\ (4)$ és $q_j \equiv -1\ (4)$. Ekkor $n = x^2 + y^2$ megoldásainak száma

A megoldások száma

Az $n = x^2 + y^2 = (x + yi)(x - yi)$ összefüggésbe helyettesítsük $x + iy$ kanonikus alakját a Gauss-egészek között. Konjugálással $x - iy$ kanonikus alakja is megkapható. A kettőt összeszorozva, és n kanonikus alakjával összevetve a következő tételt kapjuk.

Tétel (FGy7.5.1)

Legyen n kanonikus alakja $2^\alpha p_1^{\beta_1} \dots p_r^{\beta_r} q_1^{\gamma_1} \dots q_s^{\gamma_s}$, ahol $p_i \equiv 1\ (4)$ és $q_j \equiv -1\ (4)$. Ekkor $n = x^2 + y^2$ megoldásainak száma $4(\beta_1 + 1) \dots (\beta_r + 1)$ ha mindegyik γ_j páros,

A megoldások száma

Az $n = x^2 + y^2 = (x + yi)(x - yi)$ összefüggésbe helyettesítsük $x + iy$ kanonikus alakját a Gauss-egészek között. Konjugálással $x - iy$ kanonikus alakja is megkapható. A kettőt összeszorozva, és n kanonikus alakjával összevetve a következő tételt kapjuk.

Tétel (FGy7.5.1)

Legyen n kanonikus alakja $2^\alpha p_1^{\beta_1} \dots p_r^{\beta_r} q_1^{\gamma_1} \dots q_s^{\gamma_s}$, ahol $p_i \equiv 1\ (4)$ és $q_j \equiv -1\ (4)$. Ekkor $n = x^2 + y^2$ megoldásainak száma $4(\beta_1 + 1) \dots (\beta_r + 1)$ ha mindegyik γ_j páros, és 0 egyébként.

A megoldások száma

Az $n = x^2 + y^2 = (x + yi)(x - yi)$ összefüggésbe helyettesítsük $x + iy$ kanonikus alakját a Gauss-egészek között. Konjugálással $x - iy$ kanonikus alakja is megkapható. A kettőt összeszorozva, és n kanonikus alakjával összevetve a következő tételt kapjuk.

Tétel (FGy7.5.1)

Legyen n kanonikus alakja $2^\alpha p_1^{\beta_1} \dots p_r^{\beta_r} q_1^{\gamma_1} \dots q_s^{\gamma_s}$, ahol $p_i \equiv 1\ (4)$ és $q_j \equiv -1\ (4)$. Ekkor $n = x^2 + y^2$ megoldásainak száma $4(\beta_1 + 1) \dots (\beta_r + 1)$ ha mindegyik γ_j páros, és 0 egyébként.

A megoldásszám az (x, y) párok száma, ahol $x^2 + y^2 = n$.

A megoldások száma

Az $n = x^2 + y^2 = (x + yi)(x - yi)$ összefüggésbe helyettesítsük $x + iy$ kanonikus alakját a Gauss-egészek között. Konjugálással $x - iy$ kanonikus alakja is megkapható. A kettőt összeszorozva, és n kanonikus alakjával összevetve a következő tételt kapjuk.

Tétel (FGy7.5.1)

Legyen n kanonikus alakja $2^\alpha p_1^{\beta_1} \dots p_r^{\beta_r} q_1^{\gamma_1} \dots q_s^{\gamma_s}$, ahol $p_i \equiv 1\ (4)$ és $q_j \equiv -1\ (4)$. Ekkor $n = x^2 + y^2$ megoldásainak száma $4(\beta_1 + 1) \dots (\beta_r + 1)$ ha mindegyik γ_j páros, és 0 egyébként.

A megoldásszám az (x, y) párok száma, ahol $x^2 + y^2 = n$.
Pl. $n = 90 = 2 \cdot 3^2 \cdot 5$ esetén

A megoldások száma

Az $n = x^2 + y^2 = (x + yi)(x - yi)$ összefüggésbe helyettesítsük $x + iy$ kanonikus alakját a Gauss-egészek között. Konjugálással $x - iy$ kanonikus alakja is megkapható. A kettőt összeszorozva, és n kanonikus alakjával összevetve a következő tételt kapjuk.

Tétel (FGy7.5.1)

Legyen n kanonikus alakja $2^\alpha p_1^{\beta_1} \dots p_r^{\beta_r} q_1^{\gamma_1} \dots q_s^{\gamma_s}$, ahol $p_i \equiv 1\ (4)$ és $q_j \equiv -1\ (4)$. Ekkor $n = x^2 + y^2$ megoldásainak száma $4(\beta_1 + 1) \dots (\beta_r + 1)$ ha mindegyik γ_j páros, és 0 egyébként.

A megoldásszám az (x, y) párok száma, ahol $x^2 + y^2 = n$. Pl. $n = 90 = 2 \cdot 3^2 \cdot 5$ esetén a $4 \cdot (1 + 1) = 8$ megoldás valójában csak egy megoldás:

A megoldások száma

Az $n = x^2 + y^2 = (x + yi)(x - yi)$ összefüggésbe helyettesítsük $x + iy$ kanonikus alakját a Gauss-egészek között. Konjugálással $x - iy$ kanonikus alakja is megkapható. A kettőt összeszorozva, és n kanonikus alakjával összevetve a következő tételt kapjuk.

Tétel (FGy7.5.1)

Legyen n kanonikus alakja $2^\alpha p_1^{\beta_1} \dots p_r^{\beta_r} q_1^{\gamma_1} \dots q_s^{\gamma_s}$, ahol $p_i \equiv 1\ (4)$ és $q_j \equiv -1\ (4)$. Ekkor $n = x^2 + y^2$ megoldásainak száma $4(\beta_1 + 1) \dots (\beta_r + 1)$ ha mindegyik γ_j páros, és 0 egyébként.

A megoldásszám az (x, y) párok száma, ahol $x^2 + y^2 = n$.
Pl. $n = 90 = 2 \cdot 3^2 \cdot 5$ esetén a $4 \cdot (1 + 1) = 8$ megoldás valójában csak egy megoldás: $90 = 81 + 9$.

A megoldások száma

Az $n = x^2 + y^2 = (x + yi)(x - yi)$ összefüggésbe helyettesítsük $x + iy$ kanonikus alakját a Gauss-egészek között. Konjugálással $x - iy$ kanonikus alakja is megkapható. A kettőt összeszorozva, és n kanonikus alakjával összevetve a következő tételt kapjuk.

Tétel (FGy7.5.1)

Legyen n kanonikus alakja $2^\alpha p_1^{\beta_1} \dots p_r^{\beta_r} q_1^{\gamma_1} \dots q_s^{\gamma_s}$, ahol $p_i \equiv 1\ (4)$ és $q_j \equiv -1\ (4)$. Ekkor $n = x^2 + y^2$ megoldásainak száma $4(\beta_1 + 1) \dots (\beta_r + 1)$ ha mindegyik γ_j páros, és 0 egyébként.

A megoldásszám az (x, y) párok száma, ahol $x^2 + y^2 = n$. Pl. $n = 90 = 2 \cdot 3^2 \cdot 5$ esetén a $4 \cdot (1 + 1) = 8$ megoldás valójában csak egy megoldás: $90 = 81 + 9$. Ebből nyolc úgy keletkezik, hogy a sorrendet és az előjeleket változtatjuk:

A megoldások száma

Az $n = x^2 + y^2 = (x + yi)(x - yi)$ összefüggésbe helyettesítsük $x + iy$ kanonikus alakját a Gauss-egészek között. Konjugálással $x - iy$ kanonikus alakja is megkapható. A kettőt összeszorozva, és n kanonikus alakjával összevetve a következő tételt kapjuk.

Tétel (FGy7.5.1)

Legyen n kanonikus alakja $2^\alpha p_1^{\beta_1} \dots p_r^{\beta_r} q_1^{\gamma_1} \dots q_s^{\gamma_s}$, ahol $p_i \equiv 1\ (4)$ és $q_j \equiv -1\ (4)$. Ekkor $n = x^2 + y^2$ megoldásainak száma $4(\beta_1 + 1) \dots (\beta_r + 1)$ ha mindegyik γ_j páros, és 0 egyébként.

A megoldásszám az (x, y) párok száma, ahol $x^2 + y^2 = n$. Pl. $n = 90 = 2 \cdot 3^2 \cdot 5$ esetén a $4 \cdot (1 + 1) = 8$ megoldás valójában csak egy megoldás: $90 = 81 + 9$. Ebből nyolc úgy keletkezik, hogy a sorrendet és az előjeleket változtatjuk: $(\pm 9, \pm 3)$ is,

A megoldások száma

Az $n = x^2 + y^2 = (x + yi)(x - yi)$ összefüggésbe helyettesítsük $x + iy$ kanonikus alakját a Gauss-egészek között. Konjugálással $x - iy$ kanonikus alakja is megkapható. A kettőt összeszorozva, és n kanonikus alakjával összevetve a következő tételt kapjuk.

Tétel (FGy7.5.1)

Legyen n kanonikus alakja $2^\alpha p_1^{\beta_1} \dots p_r^{\beta_r} q_1^{\gamma_1} \dots q_s^{\gamma_s}$, ahol $p_i \equiv 1\ (4)$ és $q_j \equiv -1\ (4)$. Ekkor $n = x^2 + y^2$ megoldásainak száma $4(\beta_1 + 1) \dots (\beta_r + 1)$ ha mindegyik γ_j páros, és 0 egyébként.

A megoldásszám az (x, y) párok száma, ahol $x^2 + y^2 = n$. Pl. $n = 90 = 2 \cdot 3^2 \cdot 5$ esetén a $4 \cdot (1 + 1) = 8$ megoldás valójában csak egy megoldás: $90 = 81 + 9$. Ebből nyolc úgy keletkezik, hogy a sorrendet és az előjeleket változtatjuk: $(\pm 9, \pm 3)$ is, $(\pm 3, \pm 9)$ is $4 - 4$ megoldás.

A Waring problémakör

Definíció (FGy7.6.1, 7.6.3)

Legyen $g(k)$ a legkisebb olyan r, hogy minden pozitív egész felírható legfeljebb r darab teljes k-adik hatvány összegeként,

A Waring problémakör

Definíció (FGy7.6.1, 7.6.3)

Legyen $g(k)$ a legkisebb olyan r, hogy minden pozitív egész felírható legfeljebb r darab teljes k-adik hatvány összegeként, $G(k)$ pedig a legkisebb olyan r, hogy minden elég nagy pozitív egész felírható így.

A Waring problémakör

Definíció (FGy7.6.1, 7.6.3)

Legyen $g(k)$ a legkisebb olyan r, hogy minden pozitív egész felírható legfeljebb r darab teljes k-adik hatvány összegeként, $G(k)$ pedig a legkisebb olyan r, hogy minden elég nagy pozitív egész felírható így.

Például $g(2) = G(2) = 4$,

A Waring problémakör

Definíció (FGy7.6.1, 7.6.3)

Legyen $g(k)$ a legkisebb olyan r, hogy minden pozitív egész felírható legfeljebb r darab teljes k-adik hatvány összegeként, $G(k)$ pedig a legkisebb olyan r, hogy minden elég nagy pozitív egész felírható így.

Például $g(2) = G(2) = 4$, hiszen 4 négyzetszám minden számhoz elegendő,

A Waring problémakör

Definíció (FGy7.6.1, 7.6.3)

Legyen $g(k)$ a legkisebb olyan r, hogy minden pozitív egész felírható legfeljebb r darab teljes k-adik hatvány összegeként, $G(k)$ pedig a legkisebb olyan r, hogy minden elég nagy pozitív egész felírható így.

Például $g(2) = G(2) = 4$, hiszen 4 négyzetszám minden számhoz elegendő, 3 viszont végtelen sokhoz nem elegendő.

A Waring problémakör

Definíció (FGy7.6.1, 7.6.3)

Legyen $g(k)$ a legkisebb olyan r, hogy minden pozitív egész felírható legfeljebb r darab teljes k-adik hatvány összegeként, $G(k)$ pedig a legkisebb olyan r, hogy minden elég nagy pozitív egész felírható így.

Például $g(2) = G(2) = 4$, hiszen 4 négyzetszám minden számhoz elegendő, 3 viszont végtelen sokhoz nem elegendő.
Az sem nyilvánvaló, de igaz, hogy $G(k)$ létezik,

A Waring problémakör

Definíció (FGy7.6.1, 7.6.3)

Legyen $g(k)$ a legkisebb olyan r, hogy minden pozitív egész felírható legfeljebb r darab teljes k-adik hatvány összegeként, $G(k)$ pedig a legkisebb olyan r, hogy minden elég nagy pozitív egész felírható így.

Például $g(2) = G(2) = 4$, hiszen 4 négyzetszám minden számhoz elegendő, 3 viszont végtelen sokhoz nem elegendő.
Az sem nyilvánvaló, de igaz, hogy $G(k)$ létezik, előfordulhatna, hogy egyre nagyobb számokat

A Waring problémakör

Definíció (FGy7.6.1, 7.6.3)

Legyen $g(k)$ a legkisebb olyan r, hogy minden pozitív egész felírható legfeljebb r darab teljes k-adik hatvány összegeként, $G(k)$ pedig a legkisebb olyan r, hogy minden elég nagy pozitív egész felírható így.

Például $g(2) = G(2) = 4$, hiszen 4 négyzetszám minden számhoz elegendő, 3 viszont végtelen sokhoz nem elegendő.
Az sem nyilvánvaló, de igaz, hogy $G(k)$ létezik, előfordulhatna, hogy egyre nagyobb számokat csak egyre több k-adik hatvány összegeként lehet felírni.

A Waring problémakör

Definíció (FGy7.6.1, 7.6.3)

Legyen $g(k)$ a legkisebb olyan r, hogy minden pozitív egész felírható legfeljebb r darab teljes k-adik hatvány összegeként, $G(k)$ pedig a legkisebb olyan r, hogy minden elég nagy pozitív egész felírható így.

Például $g(2) = G(2) = 4$, hiszen 4 négyzetszám minden számhoz elegendő, 3 viszont végtelen sokhoz nem elegendő.
Az sem nyilvánvaló, de igaz, hogy $G(k)$ létezik, előfordulhatna, hogy egyre nagyobb számokat csak egyre több k-adik hatvány összegeként lehet felírni.
A $G(k)$ értékek meghatározása kis k esetén is igen nehéz.

A Waring problémakör

Definíció (FGy7.6.1, 7.6.3)

Legyen $g(k)$ a legkisebb olyan r, hogy minden pozitív egész felírható legfeljebb r darab teljes k-adik hatvány összegeként, $G(k)$ pedig a legkisebb olyan r, hogy minden elég nagy pozitív egész felírható így.

Például $g(2) = G(2) = 4$, hiszen 4 négyzetszám minden számhoz elegendő, 3 viszont végtelen sokhoz nem elegendő.
Az sem nyilvánvaló, de igaz, hogy $G(k)$ létezik, előfordulhatna, hogy egyre nagyobb számokat csak egyre több k-adik hatvány összegeként lehet felírni.
A $G(k)$ értékek meghatározása kis k esetén is igen nehéz.
Például csak azt tudjuk, hogy $4 \leq G(3) \leq 7$,

A Waring problémakör

Definíció (FGy7.6.1, 7.6.3)

Legyen $g(k)$ a legkisebb olyan r, hogy minden pozitív egész felírható legfeljebb r darab teljes k-adik hatvány összegeként, $G(k)$ pedig a legkisebb olyan r, hogy minden elég nagy pozitív egész felírható így.

Például $g(2) = G(2) = 4$, hiszen 4 négyzetszám minden számhoz elegendő, 3 viszont végtelen sokhoz nem elegendő.
Az sem nyilvánvaló, de igaz, hogy $G(k)$ létezik, előfordulhatna, hogy egyre nagyobb számokat csak egyre több k-adik hatvány összegeként lehet felírni.
A $G(k)$ értékek meghatározása kis k esetén is igen nehéz.
Például csak azt tudjuk, hogy $4 \leq G(3) \leq 7$, viszont $G(4) = 16$.

A Waring problémakör

Definíció (FGy7.6.1, 7.6.3)

Legyen $g(k)$ a legkisebb olyan r, hogy minden pozitív egész felírható legfeljebb r darab teljes k-adik hatvány összegeként, $G(k)$ pedig a legkisebb olyan r, hogy minden elég nagy pozitív egész felírható így.

Például $g(2) = G(2) = 4$, hiszen 4 négyzetszám minden számhoz elegendő, 3 viszont végtelen sokhoz nem elegendő.
Az sem nyilvánvaló, de igaz, hogy $G(k)$ létezik, előfordulhatna, hogy egyre nagyobb számokat csak egyre több k-adik hatvány összegeként lehet felírni.
A $G(k)$ értékek meghatározása kis k esetén is igen nehéz.
Például csak azt tudjuk, hogy $4 \leq G(3) \leq 7$, viszont $G(4) = 16$.
Elemien látható, hogy $G(k) \geq k + 1$,

A Waring problémakör

Definíció (FGy7.6.1, 7.6.3)

Legyen $g(k)$ a legkisebb olyan r, hogy minden pozitív egész felírható legfeljebb r darab teljes k-adik hatvány összegeként, $G(k)$ pedig a legkisebb olyan r, hogy minden elég nagy pozitív egész felírható így.

Például $g(2) = G(2) = 4$, hiszen 4 négyzetszám minden számhoz elegendő, 3 viszont végtelen sokhoz nem elegendő.
Az sem nyilvánvaló, de igaz, hogy $G(k)$ létezik, előfordulhatna, hogy egyre nagyobb számokat csak egyre több k-adik hatvány összegeként lehet felírni.
A $G(k)$ értékek meghatározása kis k esetén is igen nehéz.
Például csak azt tudjuk, hogy $4 \leq G(3) \leq 7$, viszont $G(4) = 16$.
Elemien látható, hogy $G(k) \geq k + 1$, de pl. $G(6) \geq 9$ (FGy7.6.4-5).

A Waring problémakör

Definíció (FGy7.6.1, 7.6.3)

Legyen $g(k)$ a legkisebb olyan r, hogy minden pozitív egész felírható legfeljebb r darab teljes k-adik hatvány összegeként, $G(k)$ pedig a legkisebb olyan r, hogy minden elég nagy pozitív egész felírható így.

Például $g(2) = G(2) = 4$, hiszen 4 négyzetszám minden számhoz elegendő, 3 viszont végtelen sokhoz nem elegendő.
Az sem nyilvánvaló, de igaz, hogy $G(k)$ létezik, előfordulhatna, hogy egyre nagyobb számokat csak egyre több k-adik hatvány összegeként lehet felírni.
A $G(k)$ értékek meghatározása kis k esetén is igen nehéz.
Például csak azt tudjuk, hogy $4 \leq G(3) \leq 7$, viszont $G(4) = 16$.
Elemien látható, hogy $G(k) \geq k + 1$, de pl. $G(6) \geq 9$ (FGy7.6.4-5).
Sejtés: $g(k) = 2^k + \lfloor (3/2)^k \rfloor - 2$ (vö. FGy7.6.2).

Euler-egységek és norma*

A Fermat-sejtés $n = 3$ esete az Euler-egészek $\mathbb{E}$ gyűrűjének vizsgálatával igazolható, lásd a FGy-könyv 7.7. szakaszát.

Euler-egységek és norma*

A Fermat-sejtés $n = 3$ esete az Euler-egészek $\mathbb{E}$ gyűrűjének vizsgálatával igazolható, lásd a FGy-könyv 7.7. szakaszát.

(1) Az Euler-egészek az $a + b\omega$ alakú számok, ahol $a, b \in \mathbb{Z}$ és $\omega = (-1 + i\sqrt{3})/2$ primitív harmadik egységgyök.

Euler-egységek és norma*

A Fermat-sejtés $n = 3$ esete az Euler-egészek $\mathbb{E}$ gyűrűjének vizsgálatával igazolható, lásd a FGy-könyv 7.7. szakaszát.

(1) Az Euler-egészek az $a + b\omega$ alakú számok, ahol $a, b \in \mathbb{Z}$ és $\omega = (-1 + i\sqrt{3})/2$ primitív harmadik egységgyök. Euklideszi gyűrűt alkotnak az $N(a + b\omega) = |a + b\omega|^2 = a^2 - ab + b^2$ normára nézve.

Euler-egységek és norma*

A Fermat-sejtés $n = 3$ esete az Euler-egészek $\mathbb{E}$ gyűrűjének vizsgálatával igazolható, lásd a FGy-könyv 7.7. szakaszát.

(1) Az Euler-egészek az $a + b\omega$ alakú számok, ahol $a, b \in \mathbb{Z}$ és $\omega = (-1 + i\sqrt{3})/2$ primitív harmadik egységgyök. Euklideszi gyűrűt alkotnak az $N(a + b\omega) = |a + b\omega|^2 = a^2 - ab + b^2$ normára nézve. Az $\alpha : \beta$ maradékos osztás elvégzésekor a hányados az α/β számhoz legközelebbi Euler-egész lesz.

Euler-egységek és norma*

A Fermat-sejtés $n = 3$ esete az Euler-egészek $\mathbb{E}$ gyűrűjének vizsgálatával igazolható, lásd a FGy-könyv 7.7. szakaszát.

(1) Az Euler-egészek az $a + b\omega$ alakú számok, ahol $a, b \in \mathbb{Z}$ és $\omega = (-1 + i\sqrt{3})/2$ primitív harmadik egységgyök. Euklideszi gyűrűt alkotnak az $N(a + b\omega) = |a + b\omega|^2 = a^2 - ab + b^2$ normára nézve. Az $\alpha : \beta$ maradékos osztás elvégzésekor a hányados az α/β számhoz legközelebbi Euler-egész lesz.

(2) A norma multiplikatív: $N(\alpha\beta) = N(\alpha)N(\beta)$.

Euler-egységek és norma*

A Fermat-sejtés $n = 3$ esete az Euler-egészek $\mathbb{E}$ gyűrűjének vizsgálatával igazolható, lásd a FGy-könyv 7.7. szakaszát.

(1) Az Euler-egészek az $a + b\omega$ alakú számok, ahol $a, b \in \mathbb{Z}$ és $\omega = (-1 + i\sqrt{3})/2$ primitív harmadik egységgyök. Euklideszi gyűrűt alkotnak az $N(a + b\omega) = |a + b\omega|^2 = a^2 - ab + b^2$ normára nézve. Az $\alpha : \beta$ maradékos osztás elvégzésekor a hányados az α/β számhoz legközelebbi Euler-egész lesz.

(2) A norma multiplikatív: $N(\alpha\beta) = N(\alpha)N(\beta)$.
Az egységek $\mathbb{E}$ azon elemei, melyek normája 1,

Euler-egységek és norma*

A Fermat-sejtés $n = 3$ esete az Euler-egészek $\mathbb{E}$ gyűrűjének vizsgálatával igazolható, lásd a FGy-könyv 7.7. szakaszát.

(1) Az Euler-egészek az $a + b\omega$ alakú számok, ahol $a, b \in \mathbb{Z}$ és $\omega = (-1 + i\sqrt{3})/2$ primitív harmadik egységgyök. Euklideszi gyűrűt alkotnak az $N(a + b\omega) = |a + b\omega|^2 = a^2 - ab + b^2$ normára nézve. Az $\alpha : \beta$ maradékos osztás elvégzésekor a hányados az α/β számhoz legközelebbi Euler-egész lesz.

(2) A norma multiplikatív: $N(\alpha\beta) = N(\alpha)N(\beta)$.
Az egységek $\mathbb{E}$ azon elemei, melyek normája 1, ezek a hatodik egységgyökök:

Euler-egységek és norma*

A Fermat-sejtés $n = 3$ esete az Euler-egészek $\mathbb{E}$ gyűrűjének vizsgálatával igazolható, lásd a FGy-könyv 7.7. szakaszát.

(1) Az Euler-egészek az $a + b\omega$ alakú számok, ahol $a, b \in \mathbb{Z}$ és $\omega = (-1 + i\sqrt{3})/2$ primitív harmadik egységgyök. Euklideszi gyűrűt alkotnak az $N(a + b\omega) = |a + b\omega|^2 = a^2 - ab + b^2$ normára nézve. Az $\alpha : \beta$ maradékos osztás elvégzésekor a hányados az α/β számhoz legközelebbi Euler-egész lesz.

(2) A norma multiplikatív: $N(\alpha\beta) = N(\alpha)N(\beta)$.
Az egységek $\mathbb{E}$ azon elemei, melyek normája 1, ezek a hatodik egységgyökök: ± 1,

Euler-egységek és norma*

A Fermat-sejtés $n = 3$ esete az Euler-egészek $\mathbb{E}$ gyűrűjének vizsgálatával igazolható, lásd a FGy-könyv 7.7. szakaszát.

(1) Az Euler-egészek az $a + b\omega$ alakú számok, ahol $a, b \in \mathbb{Z}$ és $\omega = (-1 + i\sqrt{3})/2$ primitív harmadik egységgyök. Euklideszi gyűrűt alkotnak az $N(a + b\omega) = |a + b\omega|^2 = a^2 - ab + b^2$ normára nézve. Az $\alpha : \beta$ maradékos osztás elvégzésekor a hányados az α/β számhoz legközelebbi Euler-egész lesz.

(2) A norma multiplikatív: $N(\alpha\beta) = N(\alpha)N(\beta)$.
Az egységek $\mathbb{E}$ azon elemei, melyek normája 1, ezek a hatodik egységgyökök: ± 1, $\pm\omega$,

Euler-egységek és norma*

A Fermat-sejtés $n = 3$ esete az Euler-egészek $\mathbb{E}$ gyűrűjének vizsgálatával igazolható, lásd a FGy-könyv 7.7. szakaszát.

(1) Az Euler-egészek az $a + b\omega$ alakú számok, ahol $a, b \in \mathbb{Z}$ és $\omega = (-1 + i\sqrt{3})/2$ primitív harmadik egységgyök. Euklideszi gyűrűt alkotnak az $N(a + b\omega) = |a + b\omega|^2 = a^2 - ab + b^2$ normára nézve. Az $\alpha : \beta$ maradékos osztás elvégzésekor a hányados az α/β számhoz legközelebbi Euler-egész lesz.

(2) A norma multiplikatív: $N(\alpha\beta) = N(\alpha)N(\beta)$.
Az egységek $\mathbb{E}$ azon elemei, melyek normája 1, ezek a hatodik egységgyökök: ± 1, $\pm\omega$, $\pm\overline{\omega}$

Euler-egységek és norma*

A Fermat-sejtés $n = 3$ esete az Euler-egészek $\mathbb{E}$ gyűrűjének vizsgálatával igazolható, lásd a FGy-könyv 7.7. szakaszát.

(1) Az Euler-egészek az $a + b\omega$ alakú számok, ahol $a, b \in \mathbb{Z}$ és $\omega = (-1 + i\sqrt{3})/2$ primitív harmadik egységgyök. Euklideszi gyűrűt alkotnak az $N(a + b\omega) = |a + b\omega|^2 = a^2 - ab + b^2$ normára nézve. Az $\alpha : \beta$ maradékos osztás elvégzésekor a hányados az α/β számhoz legközelebbi Euler-egész lesz.

(2) A norma multiplikatív: $N(\alpha\beta) = N(\alpha)N(\beta)$.
Az egységek $\mathbb{E}$ azon elemei, melyek normája 1, ezek a hatodik egységgyökök: ± 1, $\pm\omega$, $\pm\overline{\omega} = \pm\omega^2$.

Euler-egységek és norma*

A Fermat-sejtés $n = 3$ esete az Euler-egészek $\mathbb{E}$ gyűrűjének vizsgálatával igazolható, lásd a FGy-könyv 7.7. szakaszát.

(1) Az Euler-egészek az $a + b\omega$ alakú számok, ahol $a, b \in \mathbb{Z}$ és $\omega = (-1 + i\sqrt{3})/2$ primitív harmadik egységgyök. Euklideszi gyűrűt alkotnak az $N(a + b\omega) = |a + b\omega|^2 = a^2 - ab + b^2$ normára nézve. Az $\alpha : \beta$ maradékos osztás elvégzésekor a hányados az α/β számhoz legközelebbi Euler-egész lesz.

(2) A norma multiplikatív: $N(\alpha\beta) = N(\alpha)N(\beta)$.
Az egységek $\mathbb{E}$ azon elemei, melyek normája 1, ezek a hatodik egységgyökök: ± 1, $\pm\omega$, $\pm\overline{\omega} = \pm\omega^2$.

Legyen p páratlan prím. Az $x^2 - x + 1 \equiv 0\ (p)$ megoldásához alkalmazzuk a másodfokú egyenlet megoldóképletét $\mathbb{Z}_p$-ben.

Euler-egységek és norma*

A Fermat-sejtés $n = 3$ esete az Euler-egészek $\mathbb{E}$ gyűrűjének vizsgálatával igazolható, lásd a FGy-könyv 7.7. szakaszát.

(1) Az Euler-egészek az $a + b\omega$ alakú számok, ahol $a, b \in \mathbb{Z}$ és $\omega = (-1 + i\sqrt{3})/2$ primitív harmadik egységgyök. Euklideszi gyűrűt alkotnak az $N(a + b\omega) = |a + b\omega|^2 = a^2 - ab + b^2$ normára nézve. Az $\alpha : \beta$ maradékos osztás elvégzésekor a hányados az α/β számhoz legközelebbi Euler-egész lesz.

(2) A norma multiplikatív: $N(\alpha\beta) = N(\alpha)N(\beta)$.
Az egységek $\mathbb{E}$ azon elemei, melyek normája 1, ezek a hatodik egységgyökök: ± 1, $\pm\omega$, $\pm\overline{\omega} = \pm\omega^2$.

Legyen p páratlan prím. Az $x^2 - x + 1 \equiv 0\ (p)$ megoldásához alkalmazzuk a másodfokú egyenlet megoldóképletét $\mathbb{Z}_p$-ben.
A négyzetgyök alatt -3 áll,

Euler-egységek és norma*

A Fermat-sejtés $n = 3$ esete az Euler-egészek $\mathbb{E}$ gyűrűjének vizsgálatával igazolható, lásd a FGy-könyv 7.7. szakaszát.

(1) Az Euler-egészek az $a + b\omega$ alakú számok, ahol $a, b \in \mathbb{Z}$ és $\omega = (-1 + i\sqrt{3})/2$ primitív harmadik egységgyök. Euklideszi gyűrűt alkotnak az $N(a + b\omega) = |a + b\omega|^2 = a^2 - ab + b^2$ normára nézve. Az $\alpha : \beta$ maradékos osztás elvégzésekor a hányados az α/β számhoz legközelebbi Euler-egész lesz.

(2) A norma multiplikatív: $N(\alpha\beta) = N(\alpha)N(\beta)$.
Az egységek $\mathbb{E}$ azon elemei, melyek normája 1, ezek a hatodik egységgyökök: ± 1, $\pm\omega$, $\pm\overline{\omega} = \pm\omega^2$.

Legyen p páratlan prím. Az $x^2 - x + 1 \equiv 0\ (p)$ megoldásához alkalmazzuk a másodfokú egyenlet megoldóképletét $\mathbb{Z}_p$-ben.
A négyzetgyök alatt -3 áll, tehát pontosan akkor van megoldás, ha -3 kvadratikus maradék mod p.

Euler-egységek és norma*

A Fermat-sejtés $n = 3$ esete az Euler-egészek $\mathbb{E}$ gyűrűjének vizsgálatával igazolható, lásd a FGy-könyv 7.7. szakaszát.

(1) Az Euler-egészek az $a + b\omega$ alakú számok, ahol $a, b \in \mathbb{Z}$ és $\omega = (-1 + i\sqrt{3})/2$ primitív harmadik egységgyök. Euklideszi gyűrűt alkotnak az $N(a + b\omega) = |a + b\omega|^2 = a^2 - ab + b^2$ normára nézve. Az $\alpha : \beta$ maradékos osztás elvégzésekor a hányados az α/β számhoz legközelebbi Euler-egész lesz.

(2) A norma multiplikatív: $N(\alpha\beta) = N(\alpha)N(\beta)$.
Az egységek $\mathbb{E}$ azon elemei, melyek normája 1, ezek a hatodik egységgyökök: ± 1, $\pm\omega$, $\pm\overline{\omega} = \pm\omega^2$.

Legyen p páratlan prím. Az $x^2 - x + 1 \equiv 0\ (p)$ megoldásához alkalmazzuk a másodfokú egyenlet megoldóképletét $\mathbb{Z}_p$-ben. A négyzetgyök alatt -3 áll, tehát pontosan akkor van megoldás, ha -3 kvadratikus maradék mod p. A reciprocitási tétel szerint ez azzal ekvivalens, hogy $p \equiv 1\ (3)$.

Euler-prímek*

Az Euler-prímek leírása a következő (FGy7.7.7).

Euler-prímek*

Az Euler-prímek leírása a következő (FGy7.7.7).

(3) Ha p egy $3k+1$ alakú prím, akkor alkalmas a-ra $p \mid a^2 - a + 1 = (a+\omega)(a+\overline{\omega})$.

Euler-prímek*

Az Euler-prímek leírása a következő (FGy7.7.7).

(3) Ha p egy $3k+1$ alakú prím, akkor alkalmas a-ra $p \mid a^2 - a + 1 = (a+\omega)(a+\overline{\omega})$. De p nem osztója egyik tényezőnek sem,

Euler-prímek*

Az Euler-prímek leírása a következő (FGy7.7.7).

(3) Ha p egy $3k+1$ alakú prím, akkor alkalmas a-ra $p \mid a^2 - a + 1 = (a+\omega)(a+\overline{\omega})$. De p nem osztója egyik tényezőnek sem, ezért nem prím az Euler-egészek között.

Euler-prímek*

Az Euler-prímek leírása a következő (FGy7.7.7).

(3) Ha p egy $3k+1$ alakú prím, akkor alkalmas a-ra $p \mid a^2 - a + 1 = (a+\omega)(a+\overline{\omega})$. De p nem osztója egyik tényezőnek sem, ezért nem prím az Euler-egészek között. Két konjugált prímre bomlik.

Euler-prímek*

Az Euler-prímek leírása a következő (FGy7.7.7).

(3) Ha p egy $3k+1$ alakú prím, akkor alkalmas a-ra $p \mid a^2 - a + 1 = (a+\omega)(a+\overline{\omega})$. De p nem osztója egyik tényezőnek sem, ezért nem prím az Euler-egészek között. Két konjugált prímre bomlik. Példa: $7 = (3+\omega)(2-\omega)$.

Euler-prímek*

Az Euler-prímek leírása a következő (FGy7.7.7).

(3) Ha p egy $3k+1$ alakú prím, akkor alkalmas a-ra $p \mid a^2 - a + 1 = (a+\omega)(a+\overline{\omega})$. De p nem osztója egyik tényezőnek sem, ezért nem prím az Euler-egészek között. Két konjugált prímre bomlik. Példa: $7 = (3+\omega)(2-\omega)$.

(4) A $3k+2$ alakú pozitív prímek az Euler-egészek között is prímek.

Euler-prímek*

Az Euler-prímek leírása a következő (FGy7.7.7).

(3) Ha p egy $3k+1$ alakú prím, akkor alkalmas a-ra $p \mid a^2 - a + 1 = (a+\omega)(a+\overline{\omega})$. De p nem osztója egyik tényezőnek sem, ezért nem prím az Euler-egészek között. Két konjugált prímre bomlik. Példa: $7 = (3+\omega)(2-\omega)$.

(4) A $3k+2$ alakú pozitív prímek az Euler-egészek között is prímek. Prím még $\lambda = i\sqrt{3}$

Euler-prímek*

Az Euler-prímek leírása a következő (FGy7.7.7).

(3) Ha p egy $3k+1$ alakú prím, akkor alkalmas a-ra $p \mid a^2 - a + 1 = (a+\omega)(a+\overline{\omega})$. De p nem osztója egyik tényezőnek sem, ezért nem prím az Euler-egészek között. Két konjugált prímre bomlik. Példa: $7 = (3+\omega)(2-\omega)$.

(4) A $3k+2$ alakú pozitív prímek az Euler-egészek között is prímek. Prím még $\lambda = i\sqrt{3} = 1 + 2\omega$,

Euler-prímek*

Az Euler-prímek leírása a következő (FGy7.7.7).

(3) Ha p egy $3k+1$ alakú prím, akkor alkalmas a-ra $p \mid a^2 - a + 1 = (a+\omega)(a+\overline{\omega})$. De p nem osztója egyik tényezőnek sem, ezért nem prím az Euler-egészek között. Két konjugált prímre bomlik. Példa: $7 = (3+\omega)(2-\omega)$.

(4) A $3k+2$ alakú pozitív prímek az Euler-egészek között is prímek. Prím még $\lambda = i\sqrt{3} = 1 + 2\omega$, és az eddig felsoroltak asszociáltjai.

Euler-prímek*

Az Euler-prímek leírása a következő (FGy7.7.7).

(3) Ha p egy $3k+1$ alakú prím, akkor alkalmas a-ra $p \mid a^2 - a + 1 = (a+\omega)(a+\overline{\omega})$. De p nem osztója egyik tényezőnek sem, ezért nem prím az Euler-egészek között. Két konjugált prímre bomlik. Példa: $7 = (3+\omega)(2-\omega)$.

(4) A $3k+2$ alakú pozitív prímek az Euler-egészek között is prímek. Prím még $\lambda = i\sqrt{3} = 1 + 2\omega$, és az eddig felsoroltak asszociáltjai. Más Euler-prím nincs.

Euler-prímek*

Az Euler-prímek leírása a következő (FGy7.7.7).

(3) Ha p egy $3k+1$ alakú prím, akkor alkalmas a-ra $p \mid a^2 - a + 1 = (a+\omega)(a+\overline{\omega})$. De p nem osztója egyik tényezőnek sem, ezért nem prím az Euler-egészek között. Két konjugált prímre bomlik. Példa: $7 = (3+\omega)(2-\omega)$.

(4) A $3k+2$ alakú pozitív prímek az Euler-egészek között is prímek. Prím még $\lambda = i\sqrt{3} = 1+2\omega$, és az eddig felsoroltak asszociáltjai. Más Euler-prím nincs.

Tétel (FGy7.7.9)

Az egységek páronként inkongruensek mod $\lambda^2 = -3$,

Euler-prímek*

Az Euler-prímek leírása a következő (FGy7.7.7).

(3) Ha p egy $3k+1$ alakú prím, akkor alkalmas a-ra $p \mid a^2 - a + 1 = (a+\omega)(a+\overline{\omega})$. De p nem osztója egyik tényezőnek sem, ezért nem prím az Euler-egészek között. Két konjugált prímre bomlik. Példa: $7 = (3+\omega)(2-\omega)$.

(4) A $3k+2$ alakú pozitív prímek az Euler-egészek között is prímek. Prím még $\lambda = i\sqrt{3} = 1 + 2\omega$, és az eddig felsoroltak asszociáltjai. Más Euler-prím nincs.

Tétel (FGy7.7.9)

Az egységek páronként inkongruensek mod $\lambda^2 = -3$, de $\omega, \omega^2 \equiv 1\ (\lambda)$.

Euler-prímek*

Az Euler-prímek leírása a következő (FGy7.7.7).

(3) Ha p egy $3k+1$ alakú prím, akkor alkalmas a-ra $p \mid a^2 - a + 1 = (a+\omega)(a+\overline{\omega})$. De p nem osztója egyik tényezőnek sem, ezért nem prím az Euler-egészek között. Két konjugált prímre bomlik. Példa: $7 = (3+\omega)(2-\omega)$.

(4) A $3k+2$ alakú pozitív prímek az Euler-egészek között is prímek. Prím még $\lambda = i\sqrt{3} = 1 + 2\omega$, és az eddig felsoroltak asszociáltjai. Más Euler-prím nincs.

Tétel (FGy7.7.9)

Az egységek páronként inkongruensek mod $\lambda^2 = -3$, de $\omega, \omega^2 \equiv 1\ (\lambda)$. Az $n_0 + n_1\lambda + \ldots + n_{k-1}\lambda^{k-1}$ számok teljes maradékrendszert alkotnak mod λ^k,

Euler-prímek*

Az Euler-prímek leírása a következő (FGy7.7.7).

(3) Ha p egy $3k+1$ alakú prím, akkor alkalmas a-ra $p \mid a^2 - a + 1 = (a+\omega)(a+\overline{\omega})$. De p nem osztója egyik tényezőnek sem, ezért nem prím az Euler-egészek között. Két konjugált prímre bomlik. Példa: $7 = (3+\omega)(2-\omega)$.

(4) A $3k+2$ alakú pozitív prímek az Euler-egészek között is prímek. Prím még $\lambda = i\sqrt{3} = 1 + 2\omega$, és az eddig felsoroltak asszociáltjai. Más Euler-prím nincs.

Tétel (FGy7.7.9)

Az egységek páronként inkongruensek mod $\lambda^2 = -3$, de $\omega, \omega^2 \equiv 1\ (\lambda)$. Az $n_0 + n_1\lambda + \ldots + n_{k-1}\lambda^{k-1}$ számok teljes maradékrendszert alkotnak mod λ^k, ahol $n_j \in \{-1, 0, 1\}$.

Euler-prímek*

Az Euler-prímek leírása a következő (FGy7.7.7).

(3) Ha p egy $3k+1$ alakú prím, akkor alkalmas a-ra $p \mid a^2 - a + 1 = (a+\omega)(a+\overline{\omega})$. De p nem osztója egyik tényezőnek sem, ezért nem prím az Euler-egészek között. Két konjugált prímre bomlik. Példa: $7 = (3+\omega)(2-\omega)$.

(4) A $3k+2$ alakú pozitív prímek az Euler-egészek között is prímek. Prím még $\lambda = i\sqrt{3} = 1 + 2\omega$, és az eddig felsoroltak asszociáltjai. Más Euler-prím nincs.

Tétel (FGy7.7.9)

Az egységek páronként inkongruensek mod $\lambda^2 = -3$, de $\omega, \omega^2 \equiv 1\ (\lambda)$. Az $n_0 + n_1\lambda + \ldots + n_{k-1}\lambda^{k-1}$ számok teljes maradékrendszert alkotnak mod λ^k, ahol $n_j \in \{-1, 0, 1\}$. Ha $n_0 \neq 0$, akkor redukált maradékrendszert kapunk.

Euler-prímek*

Az Euler-prímek leírása a következő (FGy7.7.7).

(3) Ha p egy $3k+1$ alakú prím, akkor alkalmas a-ra $p \mid a^2 - a + 1 = (a+\omega)(a+\overline{\omega})$. De p nem osztója egyik tényezőnek sem, ezért nem prím az Euler-egészek között. Két konjugált prímre bomlik. Példa: $7 = (3+\omega)(2-\omega)$.

(4) A $3k+2$ alakú pozitív prímek az Euler-egészek között is prímek. Prím még $\lambda = i\sqrt{3} = 1 + 2\omega$, és az eddig felsoroltak asszociáltjai. Más Euler-prím nincs.

Tétel (FGy7.7.9)

Az egységek páronként inkongruensek mod $\lambda^2 = -3$, de $\omega, \omega^2 \equiv 1\ (\lambda)$. Az $n_0 + n_1\lambda + \ldots + n_{k-1}\lambda^{k-1}$ számok teljes maradékrendszert alkotnak mod λ^k, ahol $n_j \in \{-1, 0, 1\}$.
Ha $n_0 \neq 0$, akkor redukált maradékrendszert kapunk.
Ha $(\alpha, \lambda^4) = 1$, akkor $\alpha^3 \equiv \pm 1\ (\lambda^4)$.

Számolás mod λ^k *

Bizonyításvázlat. Az első állítás közvetlen számolás,

Számolás mod λ^k *

Bizonyításvázlat. Az első állítás közvetlen számolás, például $\lambda = \omega - \overline{\omega}$

Számolás mod λ^k *

Bizonyításvázlat. Az első állítás közvetlen számolás, például $\lambda = \omega - \overline{\omega} = \omega - \omega^2$

Számolás mod λ^k *

Bizonyításvázlat. Az első állítás közvetlen számolás, például
$\lambda = \omega - \overline{\omega} = \omega - \omega^2 = \omega(1 - \omega)$,

Számolás mod λ^k *

Bizonyításvázlat. Az első állítás közvetlen számolás, például $\lambda = \omega - \overline{\omega} = \omega - \omega^2 = \omega(1-\omega)$, de ω egység. □

Számolás mod λ^k *

Bizonyításvázlat. Az első állítás közvetlen számolás, például $\lambda = \omega - \overline{\omega} = \omega - \omega^2 = \omega(1-\omega)$, de ω egység. □

Ezért $\alpha = a + b\omega \equiv a + b\ (\lambda)$,

Számolás mod λ^k *

Bizonyításvázlat. Az első állítás közvetlen számolás, például $\lambda = \omega - \overline{\omega} = \omega - \omega^2 = \omega(1-\omega)$, de ω egység. □

Ezért $\alpha = a + b\omega \equiv a + b\ (\lambda)$, vagyis minden Euler-egész kongruens egy egész számmal,

Számolás mod λ^k *

Bizonyításvázlat. Az első állítás közvetlen számolás, például $\lambda = \omega - \overline{\omega} = \omega - \omega^2 = \omega(1-\omega)$, de ω egység. □

Ezért $\alpha = a + b\omega \equiv a + b\ (\lambda)$, vagyis minden Euler-egész kongruens egy egész számmal, és $\lambda \mid \lambda^2 = -3$ miatt $\{-1, 0, 1\}$ egyikével is.

Számolás mod λ^k *

Bizonyításvázlat. Az első állítás közvetlen számolás, például $\lambda = \omega - \overline{\omega} = \omega - \omega^2 = \omega(1-\omega)$, de ω egység. □

Ezért $\alpha = a + b\omega \equiv a + b\ (\lambda)$, vagyis minden Euler-egész kongruens egy egész számmal, és $\lambda \mid \lambda^2 = -3$ miatt $\{-1, 0, 1\}$ egyikével is. Megfordítva, ha $\lambda \mid n \in \mathbb{Z}$, akkor $3 = N(\lambda) \mid N(n) = n^2$,

Számolás mod λ^k *

Bizonyításvázlat. Az első állítás közvetlen számolás, például $\lambda = \omega - \overline{\omega} = \omega - \omega^2 = \omega(1-\omega)$, de ω egység. □

Ezért $\alpha = a + b\omega \equiv a + b\ (\lambda)$, vagyis minden Euler-egész kongruens egy egész számmal, és $\lambda \mid \lambda^2 = -3$ miatt $\{-1, 0, 1\}$ egyikével is. Megfordítva, ha $\lambda \mid n \in \mathbb{Z}$, akkor $3 = N(\lambda) \mid N(n) = n^2$, azaz $3 \mid n$.

Számolás mod λ^k *

Bizonyításvázlat. Az első állítás közvetlen számolás, például $\lambda = \omega - \overline{\omega} = \omega - \omega^2 = \omega(1-\omega)$, de ω egység. □

Ezért $\alpha = a + b\omega \equiv a + b\ (\lambda)$, vagyis minden Euler-egész kongruens egy egész számmal, és $\lambda \mid \lambda^2 = -3$ miatt $\{-1, 0, 1\}$ egyikével is. Megfordítva, ha $\lambda \mid n \in \mathbb{Z}$, akkor $3 = N(\lambda) \mid N(n) = n^2$, azaz $3 \mid n$. Vagyis $\alpha = n_0 + \beta\lambda$,

Számolás mod λ^k *

Bizonyításvázlat. Az első állítás közvetlen számolás, például $\lambda = \omega - \overline{\omega} = \omega - \omega^2 = \omega(1-\omega)$, de ω egység. □

Ezért $\alpha = a + b\omega \equiv a + b\ (\lambda)$, vagyis minden Euler-egész kongruens egy egész számmal, és $\lambda \mid \lambda^2 = -3$ miatt $\{-1, 0, 1\}$ egyikével is. Megfordítva, ha $\lambda \mid n \in \mathbb{Z}$, akkor $3 = N(\lambda) \mid N(n) = n^2$, azaz $3 \mid n$. Vagyis $\alpha = n_0 + \beta\lambda$, ahol $n_0 \in \{-1, 0, 1\}$ egyértelmű,

Számolás mod λ^k *

Bizonyításvázlat. Az első állítás közvetlen számolás, például $\lambda = \omega - \overline{\omega} = \omega - \omega^2 = \omega(1-\omega)$, de ω egység. □

Ezért $\alpha = a + b\omega \equiv a + b\ (\lambda)$, vagyis minden Euler-egész kongruens egy egész számmal, és $\lambda \mid \lambda^2 = -3$ miatt $\{-1, 0, 1\}$ egyikével is. Megfordítva, ha $\lambda \mid n \in \mathbb{Z}$, akkor $3 = N(\lambda) \mid N(n) = n^2$, azaz $3 \mid n$. Vagyis $\alpha = n_0 + \beta\lambda$, ahol $n_0 \in \{-1, 0, 1\}$ egyértelmű, és így $\beta \in \mathbb{E}$ is egyértelmű.

Számolás mod λ^k *

Bizonyításvázlat. Az első állítás közvetlen számolás, például $\lambda = \omega - \overline{\omega} = \omega - \omega^2 = \omega(1-\omega)$, de ω egység. □

Ezért $\alpha = a + b\omega \equiv a + b\ (\lambda)$, vagyis minden Euler-egész kongruens egy egész számmal, és $\lambda \mid \lambda^2 = -3$ miatt $\{-1, 0, 1\}$ egyikével is. Megfordítva, ha $\lambda \mid n \in \mathbb{Z}$, akkor $3 = N(\lambda) \mid N(n) = n^2$, azaz $3 \mid n$. Vagyis $\alpha = n_0 + \beta\lambda$, ahol $n_0 \in \{-1, 0, 1\}$ egyértelmű, és így $\beta \in \mathbb{E}$ is egyértelmű. Az eljárást β-val folytatva a második állítást kapjuk:

Számolás mod λ^k *

Bizonyításvázlat. Az első állítás közvetlen számolás, például $\lambda = \omega - \overline{\omega} = \omega - \omega^2 = \omega(1-\omega)$, de ω egység. □

Ezért $\alpha = a + b\omega \equiv a + b\ (\lambda)$, vagyis minden Euler-egész kongruens egy egész számmal, és $\lambda \mid \lambda^2 = -3$ miatt $\{-1, 0, 1\}$ egyikével is. Megfordítva, ha $\lambda \mid n \in \mathbb{Z}$, akkor $3 = N(\lambda) \mid N(n) = n^2$, azaz $3 \mid n$. Vagyis $\alpha = n_0 + \beta\lambda$, ahol $n_0 \in \{-1, 0, 1\}$ egyértelmű, és így $\beta \in \mathbb{E}$ is egyértelmű. Az eljárást β-val folytatva a második állítást kapjuk: $\alpha \equiv n_0 + n_1\lambda + \ldots + n_{k-1}\lambda^{k-1}\ (\lambda^k)$,

Számolás mod λ^k *

Bizonyításvázlat. Az első állítás közvetlen számolás, például $\lambda = \omega - \overline{\omega} = \omega - \omega^2 = \omega(1-\omega)$, de ω egység. □

Ezért $\alpha = a + b\omega \equiv a + b\ (\lambda)$, vagyis minden Euler-egész kongruens egy egész számmal, és $\lambda \mid \lambda^2 = -3$ miatt $\{-1, 0, 1\}$ egyikével is. Megfordítva, ha $\lambda \mid n \in \mathbb{Z}$, akkor $3 = N(\lambda) \mid N(n) = n^2$, azaz $3 \mid n$. Vagyis $\alpha = n_0 + \beta\lambda$, ahol $n_0 \in \{-1, 0, 1\}$ egyértelmű, és így $\beta \in \mathbb{E}$ is egyértelmű. Az eljárást β-val folytatva a második állítást kapjuk: $\alpha \equiv n_0 + n_1\lambda + \ldots + n_{k-1}\lambda^{k-1}\ (\lambda^k)$, és az n_j egyértelmű. □

Számolás mod λ^k *

Bizonyításvázlat. Az első állítás közvetlen számolás, például $\lambda = \omega - \overline{\omega} = \omega - \omega^2 = \omega(1-\omega)$, de ω egység. □

Ezért $\alpha = a + b\omega \equiv a + b\ (\lambda)$, vagyis minden Euler-egész kongruens egy egész számmal, és $\lambda \mid \lambda^2 = -3$ miatt $\{-1, 0, 1\}$ egyikével is. Megfordítva, ha $\lambda \mid n \in \mathbb{Z}$, akkor $3 = N(\lambda) \mid N(n) = n^2$, azaz $3 \mid n$. Vagyis $\alpha = n_0 + \beta\lambda$, ahol $n_0 \in \{-1, 0, 1\}$ egyértelmű, és így $\beta \in \mathbb{E}$ is egyértelmű. Az eljárást β-val folytatva a második állítást kapjuk: $\alpha \equiv n_0 + n_1\lambda + \ldots + n_{k-1}\lambda^{k-1}\ (\lambda^k)$, és az n_j egyértelmű. □

Ha $n_0 = 0$, akkor $\lambda \mid \alpha$.

Számolás mod λ^k *

Bizonyításvázlat. Az első állítás közvetlen számolás, például $\lambda = \omega - \overline{\omega} = \omega - \omega^2 = \omega(1-\omega)$, de ω egység. □

Ezért $\alpha = a + b\omega \equiv a + b\ (\lambda)$, vagyis minden Euler-egész kongruens egy egész számmal, és $\lambda \mid \lambda^2 = -3$ miatt $\{-1, 0, 1\}$ egyikével is. Megfordítva, ha $\lambda \mid n \in \mathbb{Z}$, akkor $3 = N(\lambda) \mid N(n) = n^2$, azaz $3 \mid n$. Vagyis $\alpha = n_0 + \beta\lambda$, ahol $n_0 \in \{-1, 0, 1\}$ egyértelmű, és így $\beta \in \mathbb{E}$ is egyértelmű. Az eljárást β-val folytatva a második állítást kapjuk: $\alpha \equiv n_0 + n_1\lambda + \ldots + n_{k-1}\lambda^{k-1}\ (\lambda^k)$, és az n_j egyértelmű. □

Ha $n_0 = 0$, akkor $\lambda \mid \alpha$. Ha $n_0 = \pm 1$, akkor az ismert azonosság miatt $n_0^k \equiv n_0^k - (\lambda\beta)^k$

Számolás mod λ^k *

Bizonyításvázlat. Az első állítás közvetlen számolás, például $\lambda = \omega - \overline{\omega} = \omega - \omega^2 = \omega(1-\omega)$, de ω egység. □

Ezért $\alpha = a + b\omega \equiv a + b\ (\lambda)$, vagyis minden Euler-egész kongruens egy egész számmal, és $\lambda \mid \lambda^2 = -3$ miatt $\{-1, 0, 1\}$ egyikével is. Megfordítva, ha $\lambda \mid n \in \mathbb{Z}$, akkor $3 = N(\lambda) \mid N(n) = n^2$, azaz $3 \mid n$. Vagyis $\alpha = n_0 + \beta\lambda$, ahol $n_0 \in \{-1, 0, 1\}$ egyértelmű, és így $\beta \in \mathbb{E}$ is egyértelmű. Az eljárást β-val folytatva a második állítást kapjuk: $\alpha \equiv n_0 + n_1\lambda + \ldots + n_{k-1}\lambda^{k-1}\ (\lambda^k)$, és az n_j egyértelmű. □

Ha $n_0 = 0$, akkor $\lambda \mid \alpha$. Ha $n_0 = \pm 1$, akkor az ismert azonosság miatt $n_0^k \equiv n_0^k - (\lambda\beta)^k = (n_0 - \lambda\beta)\gamma\ (\lambda^k)$,

Számolás mod λ^k *

Bizonyításvázlat. Az első állítás közvetlen számolás, például $\lambda = \omega - \overline{\omega} = \omega - \omega^2 = \omega(1-\omega)$, de ω egység. □

Ezért $\alpha = a + b\omega \equiv a + b\ (\lambda)$, vagyis minden Euler-egész kongruens egy egész számmal, és $\lambda \mid \lambda^2 = -3$ miatt $\{-1, 0, 1\}$ egyikével is. Megfordítva, ha $\lambda \mid n \in \mathbb{Z}$, akkor $3 = N(\lambda) \mid N(n) = n^2$, azaz $3 \mid n$. Vagyis $\alpha = n_0 + \beta\lambda$, ahol $n_0 \in \{-1, 0, 1\}$ egyértelmű, és így $\beta \in \mathbb{E}$ is egyértelmű. Az eljárást β-val folytatva a második állítást kapjuk: $\alpha \equiv n_0 + n_1\lambda + \ldots + n_{k-1}\lambda^{k-1}\ (\lambda^k)$, és az n_j egyértelmű. □

Ha $n_0 = 0$, akkor $\lambda \mid \alpha$. Ha $n_0 = \pm 1$, akkor az ismert azonosság miatt $n_0^k \equiv n_0^k - (\lambda\beta)^k = (n_0 - \lambda\beta)\gamma\ (\lambda^k)$, ahol $\gamma \in \mathbb{E}$,

Számolás mod λ^k *

Bizonyításvázlat. Az első állítás közvetlen számolás, például $\lambda = \omega - \overline{\omega} = \omega - \omega^2 = \omega(1-\omega)$, de ω egység. □

Ezért $\alpha = a + b\omega \equiv a + b\ (\lambda)$, vagyis minden Euler-egész kongruens egy egész számmal, és $\lambda \mid \lambda^2 = -3$ miatt $\{-1, 0, 1\}$ egyikével is. Megfordítva, ha $\lambda \mid n \in \mathbb{Z}$, akkor $3 = N(\lambda) \mid N(n) = n^2$, azaz $3 \mid n$. Vagyis $\alpha = n_0 + \beta\lambda$, ahol $n_0 \in \{-1, 0, 1\}$ egyértelmű, és így $\beta \in \mathbb{E}$ is egyértelmű. Az eljárást β-val folytatva a második állítást kapjuk: $\alpha \equiv n_0 + n_1\lambda + \ldots + n_{k-1}\lambda^{k-1}\ (\lambda^k)$, és az n_j egyértelmű. □

Ha $n_0 = 0$, akkor $\lambda \mid \alpha$. Ha $n_0 = \pm 1$, akkor az ismert azonosság miatt $n_0^k \equiv n_0^k - (\lambda\beta)^k = (n_0 - \lambda\beta)\gamma\ (\lambda^k)$, ahol $\gamma \in \mathbb{E}$, ezért $(n_0 - \lambda\beta, \lambda^k) = 1$. □

Számolás mod λ^k *

Bizonyításvázlat. Az első állítás közvetlen számolás, például $\lambda = \omega - \overline{\omega} = \omega - \omega^2 = \omega(1-\omega)$, de ω egység. □

Ezért $\alpha = a + b\omega \equiv a + b\ (\lambda)$, vagyis minden Euler-egész kongruens egy egész számmal, és $\lambda \mid \lambda^2 = -3$ miatt $\{-1, 0, 1\}$ egyikével is. Megfordítva, ha $\lambda \mid n \in \mathbb{Z}$, akkor $3 = N(\lambda) \mid N(n) = n^2$, azaz $3 \mid n$. Vagyis $\alpha = n_0 + \beta\lambda$, ahol $n_0 \in \{-1, 0, 1\}$ egyértelmű, és így $\beta \in \mathbb{E}$ is egyértelmű. Az eljárást β-val folytatva a második állítást kapjuk: $\alpha \equiv n_0 + n_1\lambda + \ldots + n_{k-1}\lambda^{k-1}\ (\lambda^k)$, és az n_j egyértelmű. □

Ha $n_0 = 0$, akkor $\lambda \mid \alpha$. Ha $n_0 = \pm 1$, akkor az ismert azonosság miatt $n_0^k \equiv n_0^k - (\lambda\beta)^k = (n_0 - \lambda\beta)\gamma\ (\lambda^k)$, ahol $\gamma \in \mathbb{E}$, ezért $(n_0 - \lambda\beta, \lambda^k) = 1$. □

Végül ha $\alpha = a + b\lambda + \beta\lambda^2$,

Számolás mod λ^k *

Bizonyításvázlat. Az első állítás közvetlen számolás, például $\lambda = \omega - \overline{\omega} = \omega - \omega^2 = \omega(1-\omega)$, de ω egység. □

Ezért $\alpha = a + b\omega \equiv a + b\ (\lambda)$, vagyis minden Euler-egész kongruens egy egész számmal, és $\lambda \mid \lambda^2 = -3$ miatt $\{-1, 0, 1\}$ egyikével is. Megfordítva, ha $\lambda \mid n \in \mathbb{Z}$, akkor $3 = N(\lambda) \mid N(n) = n^2$, azaz $3 \mid n$. Vagyis $\alpha = n_0 + \beta\lambda$, ahol $n_0 \in \{-1, 0, 1\}$ egyértelmű, és így $\beta \in \mathbb{E}$ is egyértelmű. Az eljárást β-val folytatva a második állítást kapjuk: $\alpha \equiv n_0 + n_1\lambda + \ldots + n_{k-1}\lambda^{k-1}\ (\lambda^k)$, és az n_j egyértelmű. □

Ha $n_0 = 0$, akkor $\lambda \mid \alpha$. Ha $n_0 = \pm 1$, akkor az ismert azonosság miatt $n_0^k \equiv n_0^k - (\lambda\beta)^k = (n_0 - \lambda\beta)\gamma\ (\lambda^k)$, ahol $\gamma \in \mathbb{E}$, ezért $(n_0 - \lambda\beta, \lambda^k) = 1$. □

Végül ha $\alpha = a + b\lambda + \beta\lambda^2$, ahol $a, b \in \{0, \pm 1\}$, $a \neq 0$ és $\beta \in \mathbb{E}$,

Számolás mod λ^k *

Bizonyításvázlat. Az első állítás közvetlen számolás, például $\lambda = \omega - \overline{\omega} = \omega - \omega^2 = \omega(1-\omega)$, de ω egység. □

Ezért $\alpha = a + b\omega \equiv a + b\ (\lambda)$, vagyis minden Euler-egész kongruens egy egész számmal, és $\lambda \mid \lambda^2 = -3$ miatt $\{-1, 0, 1\}$ egyikével is. Megfordítva, ha $\lambda \mid n \in \mathbb{Z}$, akkor $3 = N(\lambda) \mid N(n) = n^2$, azaz $3 \mid n$. Vagyis $\alpha = n_0 + \beta\lambda$, ahol $n_0 \in \{-1, 0, 1\}$ egyértelmű, és így $\beta \in \mathbb{E}$ is egyértelmű. Az eljárást β-val folytatva a második állítást kapjuk: $\alpha \equiv n_0 + n_1\lambda + \ldots + n_{k-1}\lambda^{k-1}\ (\lambda^k)$, és az n_j egyértelmű. □

Ha $n_0 = 0$, akkor $\lambda \mid \alpha$. Ha $n_0 = \pm 1$, akkor az ismert azonosság miatt $n_0^k \equiv n_0^k - (\lambda\beta)^k = (n_0 - \lambda\beta)\gamma\ (\lambda^k)$, ahol $\gamma \in \mathbb{E}$, ezért $(n_0 - \lambda\beta, \lambda^k) = 1$. □

Végül ha $\alpha = a + b\lambda + \beta\lambda^2$, ahol $a, b \in \{0, \pm 1\}$, $a \neq 0$ és $\beta \in \mathbb{E}$, akkor $\alpha^3 \equiv (a + b\lambda)^3$

Számolás mod λ^k *

Bizonyításvázlat. Az első állítás közvetlen számolás, például $\lambda = \omega - \overline{\omega} = \omega - \omega^2 = \omega(1-\omega)$, de ω egység. □

Ezért $\alpha = a + b\omega \equiv a + b\ (\lambda)$, vagyis minden Euler-egész kongruens egy egész számmal, és $\lambda \mid \lambda^2 = -3$ miatt $\{-1, 0, 1\}$ egyikével is. Megfordítva, ha $\lambda \mid n \in \mathbb{Z}$, akkor $3 = N(\lambda) \mid N(n) = n^2$, azaz $3 \mid n$. Vagyis $\alpha = n_0 + \beta\lambda$, ahol $n_0 \in \{-1, 0, 1\}$ egyértelmű, és így $\beta \in \mathbb{E}$ is egyértelmű. Az eljárást β-val folytatva a második állítást kapjuk: $\alpha \equiv n_0 + n_1\lambda + \ldots + n_{k-1}\lambda^{k-1}\ (\lambda^k)$, és az n_j egyértelmű. □

Ha $n_0 = 0$, akkor $\lambda \mid \alpha$. Ha $n_0 = \pm 1$, akkor az ismert azonosság miatt $n_0^k \equiv n_0^k - (\lambda\beta)^k = (n_0 - \lambda\beta)\gamma\ (\lambda^k)$, ahol $\gamma \in \mathbb{E}$, ezért $(n_0 - \lambda\beta, \lambda^k) = 1$. □

Végül ha $\alpha = a + b\lambda + \beta\lambda^2$, ahol $a, b \in \{0, \pm 1\}$, $a \neq 0$ és $\beta \in \mathbb{E}$, akkor $\alpha^3 \equiv (a + b\lambda)^3 \equiv a^3 + 3a^2b\lambda + (b\lambda)^3\ (\lambda^4)$,

Számolás mod λ^k *

Bizonyításvázlat. Az első állítás közvetlen számolás, például $\lambda = \omega - \overline{\omega} = \omega - \omega^2 = \omega(1-\omega)$, de ω egység. □

Ezért $\alpha = a + b\omega \equiv a + b\ (\lambda)$, vagyis minden Euler-egész kongruens egy egész számmal, és $\lambda \mid \lambda^2 = -3$ miatt $\{-1, 0, 1\}$ egyikével is. Megfordítva, ha $\lambda \mid n \in \mathbb{Z}$, akkor $3 = N(\lambda) \mid N(n) = n^2$, azaz $3 \mid n$. Vagyis $\alpha = n_0 + \beta\lambda$, ahol $n_0 \in \{-1, 0, 1\}$ egyértelmű, és így $\beta \in \mathbb{E}$ is egyértelmű. Az eljárást β-val folytatva a második állítást kapjuk: $\alpha \equiv n_0 + n_1\lambda + \ldots + n_{k-1}\lambda^{k-1}\ (\lambda^k)$, és az n_j egyértelmű. □

Ha $n_0 = 0$, akkor $\lambda \mid \alpha$. Ha $n_0 = \pm 1$, akkor az ismert azonosság miatt $n_0^k \equiv n_0^k - (\lambda\beta)^k = (n_0 - \lambda\beta)\gamma\ (\lambda^k)$, ahol $\gamma \in \mathbb{E}$, ezért $(n_0 - \lambda\beta, \lambda^k) = 1$. □

Végül ha $\alpha = a + b\lambda + \beta\lambda^2$, ahol $a, b \in \{0, \pm 1\}$, $a \neq 0$ és $\beta \in \mathbb{E}$, akkor $\alpha^3 \equiv (a + b\lambda)^3 \equiv a^3 + 3a^2b\lambda + (b\lambda)^3\ (\lambda^4)$, felhasználva, hogy $\lambda^2 = -3$.

Számolás mod λ^k *

Bizonyításvázlat. Az első állítás közvetlen számolás, például $\lambda = \omega - \overline{\omega} = \omega - \omega^2 = \omega(1-\omega)$, de ω egység. □

Ezért $\alpha = a + b\omega \equiv a + b\ (\lambda)$, vagyis minden Euler-egész kongruens egy egész számmal, és $\lambda \mid \lambda^2 = -3$ miatt $\{-1, 0, 1\}$ egyikével is. Megfordítva, ha $\lambda \mid n \in \mathbb{Z}$, akkor $3 = N(\lambda) \mid N(n) = n^2$, azaz $3 \mid n$. Vagyis $\alpha = n_0 + \beta\lambda$, ahol $n_0 \in \{-1, 0, 1\}$ egyértelmű, és így $\beta \in \mathbb{E}$ is egyértelmű. Az eljárást β-val folytatva a második állítást kapjuk: $\alpha \equiv n_0 + n_1\lambda + \ldots + n_{k-1}\lambda^{k-1}\ (\lambda^k)$, és az n_j egyértelmű. □

Ha $n_0 = 0$, akkor $\lambda \mid \alpha$. Ha $n_0 = \pm 1$, akkor az ismert azonosság miatt $n_0^k \equiv n_0^k - (\lambda\beta)^k = (n_0 - \lambda\beta)\gamma\ (\lambda^k)$, ahol $\gamma \in \mathbb{E}$, ezért $(n_0 - \lambda\beta, \lambda^k) = 1$. □

Végül ha $\alpha = a + b\lambda + \beta\lambda^2$, ahol $a, b \in \{0, \pm 1\}$, $a \neq 0$ és $\beta \in \mathbb{E}$, akkor $\alpha^3 \equiv (a + b\lambda)^3 \equiv a^3 + 3a^2b\lambda + (b\lambda)^3\ (\lambda^4)$, felhasználva, hogy $\lambda^2 = -3$. De $a^2 = 1$

Számolás mod λ^k *

Bizonyításvázlat. Az első állítás közvetlen számolás, például $\lambda = \omega - \overline{\omega} = \omega - \omega^2 = \omega(1-\omega)$, de ω egység. □

Ezért $\alpha = a + b\omega \equiv a + b\ (\lambda)$, vagyis minden Euler-egész kongruens egy egész számmal, és $\lambda \mid \lambda^2 = -3$ miatt $\{-1, 0, 1\}$ egyikével is. Megfordítva, ha $\lambda \mid n \in \mathbb{Z}$, akkor $3 = N(\lambda) \mid N(n) = n^2$, azaz $3 \mid n$. Vagyis $\alpha = n_0 + \beta\lambda$, ahol $n_0 \in \{-1, 0, 1\}$ egyértelmű, és így $\beta \in \mathbb{E}$ is egyértelmű. Az eljárást β-val folytatva a második állítást kapjuk: $\alpha \equiv n_0 + n_1\lambda + \ldots + n_{k-1}\lambda^{k-1}\ (\lambda^k)$, és az n_j egyértelmű. □

Ha $n_0 = 0$, akkor $\lambda \mid \alpha$. Ha $n_0 = \pm 1$, akkor az ismert azonosság miatt $n_0^k \equiv n_0^k - (\lambda\beta)^k = (n_0 - \lambda\beta)\gamma\ (\lambda^k)$, ahol $\gamma \in \mathbb{E}$, ezért $(n_0 - \lambda\beta, \lambda^k) = 1$. □

Végül ha $\alpha = a + b\lambda + \beta\lambda^2$, ahol $a, b \in \{0, \pm 1\}$, $a \neq 0$ és $\beta \in \mathbb{E}$, akkor $\alpha^3 \equiv (a + b\lambda)^3 \equiv a^3 + 3a^2b\lambda + (b\lambda)^3\ (\lambda^4)$, felhasználva, hogy $\lambda^2 = -3$. De $a^2 = 1$ és $b^3 = b$,

Számolás mod λ^k *

Bizonyításvázlat. Az első állítás közvetlen számolás, például $\lambda = \omega - \overline{\omega} = \omega - \omega^2 = \omega(1-\omega)$, de ω egység. □

Ezért $\alpha = a + b\omega \equiv a + b\ (\lambda)$, vagyis minden Euler-egész kongruens egy egész számmal, és $\lambda \mid \lambda^2 = -3$ miatt $\{-1, 0, 1\}$ egyikével is. Megfordítva, ha $\lambda \mid n \in \mathbb{Z}$, akkor $3 = N(\lambda) \mid N(n) = n^2$, azaz $3 \mid n$. Vagyis $\alpha = n_0 + \beta\lambda$, ahol $n_0 \in \{-1, 0, 1\}$ egyértelmű, és így $\beta \in \mathbb{E}$ is egyértelmű. Az eljárást β-val folytatva a második állítást kapjuk: $\alpha \equiv n_0 + n_1\lambda + \ldots + n_{k-1}\lambda^{k-1}\ (\lambda^k)$, és az n_j egyértelmű. □

Ha $n_0 = 0$, akkor $\lambda \mid \alpha$. Ha $n_0 = \pm 1$, akkor az ismert azonosság miatt $n_0^k \equiv n_0^k - (\lambda\beta)^k = (n_0 - \lambda\beta)\gamma\ (\lambda^k)$, ahol $\gamma \in \mathbb{E}$, ezért $(n_0 - \lambda\beta, \lambda^k) = 1$. □

Végül ha $\alpha = a + b\lambda + \beta\lambda^2$, ahol $a, b \in \{0, \pm 1\}$, $a \neq 0$ és $\beta \in \mathbb{E}$, akkor $\alpha^3 \equiv (a + b\lambda)^3 \equiv a^3 + 3a^2b\lambda + (b\lambda)^3\ (\lambda^4)$, felhasználva, hogy $\lambda^2 = -3$. De $a^2 = 1$ és $b^3 = b$, ezért $\alpha^3 \equiv a\ (\lambda^4)$. □

Fermat-sejtés, $n = 3$ eset*

Köbszám 9-cel osztva, 0-t, 1-et, vagy -1-et adhat maradékul.

Fermat-sejtés, $n = 3$ eset*

Köbszám 9-cel osztva, 0-t, 1-et, vagy -1-et adhat maradékul.
Vagyis ha $x^3 + y^3 = z^3$, akkor van közöttük 9-cel osztható.

Fermat-sejtés, $n = 3$ eset*

Köbszám 9-cel osztva, 0-t, 1-et, vagy -1-et adhat maradékul.
Vagyis ha $x^3 + y^3 = z^3$, akkor van közöttük 9-cel osztható.
Feltehető, hogy x, y, z páronként relatív prímek,

Fermat-sejtés, $n = 3$ eset*

Köbszám 9-cel osztva, 0-t, 1-et, vagy -1-et adhat maradékul.
Vagyis ha $x^3 + y^3 = z^3$, akkor van közöttük 9-cel osztható.
Feltehető, hogy x, y, z páronként relatív prímek, ahogy a pitagoraszi számhármasoknál is, azaz alapmegoldásokat keresünk.

Fermat-sejtés, $n = 3$ eset*

Köbszám 9-cel osztva, 0-t, 1-et, vagy -1-et adhat maradékul.
Vagyis ha $x^3 + y^3 = z^3$, akkor van közöttük 9-cel osztható.
Feltehető, hogy x, y, z páronként relatív prímek, ahogy a pitagoraszi számhármasoknál is, azaz alapmegoldásokat keresünk.

Miért hasznosak az Euler-egészek a Fermat-sejtés megoldásakor?

Fermat-sejtés, $n = 3$ eset*

Köbszám 9-cel osztva, 0-t, 1-et, vagy -1-et adhat maradékul.
Vagyis ha $x^3 + y^3 = z^3$, akkor van közöttük 9-cel osztható.
Feltehető, hogy x, y, z páronként relatív prímek, ahogy a pitagoraszi számhármasoknál is, azaz alapmegoldásokat keresünk.

Miért hasznosak az Euler-egészek a Fermat-sejtés megoldásakor?
Ha $x^3 + y^3 = z^3$, akkor $u^3 - 1 = (u-1)(u-\omega)(u-\omega^2)$ miatt

Fermat-sejtés, $n = 3$ eset*

Köbszám 9-cel osztva, 0-t, 1-et, vagy -1-et adhat maradékul. Vagyis ha $x^3 + y^3 = z^3$, akkor van közöttük 9-cel osztható. Feltehető, hogy x, y, z páronként relatív prímek, ahogy a pitagoraszi számhármasoknál is, azaz alapmegoldásokat keresünk.

Miért hasznosak az Euler-egészek a Fermat-sejtés megoldásakor? Ha $x^3 + y^3 = z^3$, akkor $u^3 - 1 = (u-1)(u-\omega)(u-\omega^2)$ miatt $x^3 = (z-y)(z-\omega y)(z-\omega^2 y)$.

Fermat-sejtés, $n = 3$ eset*

Köbszám 9-cel osztva, 0-t, 1-et, vagy -1-et adhat maradékul. Vagyis ha $x^3 + y^3 = z^3$, akkor van közöttük 9-cel osztható. Feltehető, hogy x, y, z páronként relatív prímek, ahogy a pitagoraszi számhármasoknál is, azaz alapmegoldásokat keresünk.

Miért hasznosak az Euler-egészek a Fermat-sejtés megoldásakor? Ha $x^3 + y^3 = z^3$, akkor $u^3 - 1 = (u-1)(u-\omega)(u-\omega^2)$ miatt $x^3 = (z-y)(z-\omega y)(z-\omega^2 y)$. Ha ezek relatív prímek lennének, akkor köbszámok lennének $\mathbb{E}$-ben (egységtényezőtől eltekintve).

Fermat-sejtés, $n = 3$ eset*

Köbszám 9-cel osztva, 0-t, 1-et, vagy -1-et adhat maradékul. Vagyis ha $x^3 + y^3 = z^3$, akkor van közöttük 9-cel osztható. Feltehető, hogy x, y, z páronként relatív prímek, ahogy a pitagoraszi számhármasoknál is, azaz alapmegoldásokat keresünk.

Miért hasznosak az Euler-egészek a Fermat-sejtés megoldásakor? Ha $x^3 + y^3 = z^3$, akkor $u^3 - 1 = (u-1)(u-\omega)(u-\omega^2)$ miatt $x^3 = (z-y)(z-\omega y)(z-\omega^2 y)$. Ha ezek relatív prímek lennének, akkor köbszámok lennének $\mathbb{E}$-ben (egységtényezőtől eltekintve).

$(z-y)$, $(z-\omega y)$, $(z-\omega^2 y)$ közül bármely kettő legnagyobb közös osztója 1 vagy λ,

Fermat-sejtés, $n = 3$ eset*

Köbszám 9-cel osztva, 0-t, 1-et, vagy -1-et adhat maradékul. Vagyis ha $x^3 + y^3 = z^3$, akkor van közöttük 9-cel osztható. Feltehető, hogy x, y, z páronként relatív prímek, ahogy a pitagoraszi számhármasoknál is, azaz alapmegoldásokat keresünk.

Miért hasznosak az Euler-egészek a Fermat-sejtés megoldásakor? Ha $x^3 + y^3 = z^3$, akkor $u^3 - 1 = (u-1)(u-\omega)(u-\omega^2)$ miatt $x^3 = (z-y)(z-\omega y)(z-\omega^2 y)$. Ha ezek relatív prímek lennének, akkor köbszámok lennének $\mathbb{E}$-ben (egységtényezőtől eltekintve).

$(z-y)$, $(z-\omega y)$, $(z-\omega^2 y)$ közül bármely kettő legnagyobb közös osztója 1 vagy λ, és e számok páronként kongruensek mod λ.

Fermat-sejtés, $n = 3$ eset*

Köbszám 9-cel osztva, 0-t, 1-et, vagy -1-et adhat maradékul. Vagyis ha $x^3 + y^3 = z^3$, akkor van közöttük 9-cel osztható. Feltehető, hogy x, y, z páronként relatív prímek, ahogy a pitagoraszi számhármasoknál is, azaz alapmegoldásokat keresünk.

Miért hasznosak az Euler-egészek a Fermat-sejtés megoldásakor? Ha $x^3 + y^3 = z^3$, akkor $u^3 - 1 = (u-1)(u-\omega)(u-\omega^2)$ miatt $x^3 = (z-y)(z-\omega y)(z-\omega^2 y)$. Ha ezek relatív prímek lennének, akkor köbszámok lennének $\mathbb{E}$-ben (egységtényezőtől eltekintve).

$(z-y)$, $(z-\omega y)$, $(z-\omega^2 y)$ közül bármely kettő legnagyobb közös osztója 1 vagy λ, és e számok páronként kongruensek mod λ.

A második állítás nyilvánvaló, hiszen láttuk, hogy $\omega \equiv 1 \equiv \omega^2$ (λ).

Fermat-sejtés, $n = 3$ eset*

Köbszám 9-cel osztva, 0-t, 1-et, vagy -1-et adhat maradékul. Vagyis ha $x^3 + y^3 = z^3$, akkor van közöttük 9-cel osztható. Feltehető, hogy x, y, z páronként relatív prímek, ahogy a pitagoraszi számhármasoknál is, azaz alapmegoldásokat keresünk.

Miért hasznosak az Euler-egészek a Fermat-sejtés megoldásakor? Ha $x^3 + y^3 = z^3$, akkor $u^3 - 1 = (u-1)(u-\omega)(u-\omega^2)$ miatt $x^3 = (z-y)(z-\omega y)(z-\omega^2 y)$. Ha ezek relatív prímek lennének, akkor köbszámok lennének $\mathbb{E}$-ben (egységtényezőtől eltekintve).

$(z-y)$, $(z-\omega y)$, $(z-\omega^2 y)$ közül bármely kettő legnagyobb közös osztója 1 vagy λ, és e számok páronként kongruensek mod λ.

A második állítás nyilvánvaló, hiszen láttuk, hogy $\omega \equiv 1 \equiv \omega^2$ (λ). Ha pl. $\pi \mid \big((z-y),(z-\omega y)\big)$,

Fermat-sejtés, $n = 3$ eset*

Köbszám 9-cel osztva, 0-t, 1-et, vagy -1-et adhat maradékul. Vagyis ha $x^3 + y^3 = z^3$, akkor van közöttük 9-cel osztható. Feltehető, hogy x, y, z páronként relatív prímek, ahogy a pitagoraszi számhármasoknál is, azaz alapmegoldásokat keresünk.

Miért hasznosak az Euler-egészek a Fermat-sejtés megoldásakor? Ha $x^3 + y^3 = z^3$, akkor $u^3 - 1 = (u-1)(u-\omega)(u-\omega^2)$ miatt $x^3 = (z-y)(z-\omega y)(z-\omega^2 y)$. Ha ezek relatív prímek lennének, akkor köbszámok lennének $\mathbb{E}$-ben (egységtényezőtől eltekintve).

$(z-y)$, $(z-\omega y)$, $(z-\omega^2 y)$ közül bármely kettő legnagyobb közös osztója 1 vagy λ, és e számok páronként kongruensek mod λ.

A második állítás nyilvánvaló, hiszen láttuk, hogy $\omega \equiv 1 \equiv \omega^2 \ (\lambda)$. Ha pl. $\pi \mid \big((z-y),(z-\omega y)\big)$, ahol π Euler-prím,

Fermat-sejtés, $n = 3$ eset*

Köbszám 9-cel osztva, 0-t, 1-et, vagy -1-et adhat maradékul. Vagyis ha $x^3 + y^3 = z^3$, akkor van közöttük 9-cel osztható. Feltehető, hogy x, y, z páronként relatív prímek, ahogy a pitagoraszi számhármasoknál is, azaz alapmegoldásokat keresünk.

Miért hasznosak az Euler-egészek a Fermat-sejtés megoldásakor? Ha $x^3 + y^3 = z^3$, akkor $u^3 - 1 = (u-1)(u-\omega)(u-\omega^2)$ miatt $x^3 = (z-y)(z-\omega y)(z-\omega^2 y)$. Ha ezek relatív prímek lennének, akkor köbszámok lennének $\mathbb{E}$-ben (egységtényezőtől eltekintve).

$(z-y)$, $(z-\omega y)$, $(z-\omega^2 y)$ közül bármely kettő legnagyobb közös osztója 1 vagy λ, és e számok páronként kongruensek mod λ.

A második állítás nyilvánvaló, hiszen láttuk, hogy $\omega \equiv 1 \equiv \omega^2 \ (\lambda)$. Ha pl. $\pi \mid \big((z-y),(z-\omega y)\big)$, ahol π Euler-prím, akkor $\pi \mid y(\omega - 1)$.

Fermat-sejtés, $n = 3$ eset*

Köbszám 9-cel osztva, 0-t, 1-et, vagy -1-et adhat maradékul. Vagyis ha $x^3 + y^3 = z^3$, akkor van közöttük 9-cel osztható. Feltehető, hogy x, y, z páronként relatív prímek, ahogy a pitagoraszi számhármasoknál is, azaz alapmegoldásokat keresünk.

Miért hasznosak az Euler-egészek a Fermat-sejtés megoldásakor? Ha $x^3 + y^3 = z^3$, akkor $u^3 - 1 = (u-1)(u-\omega)(u-\omega^2)$ miatt $x^3 = (z-y)(z-\omega y)(z-\omega^2 y)$. Ha ezek relatív prímek lennének, akkor köbszámok lennének $\mathbb{E}$-ben (egységtényezőtől eltekintve).

$(z-y)$, $(z-\omega y)$, $(z-\omega^2 y)$ közül bármely kettő legnagyobb közös osztója 1 vagy λ, és e számok páronként kongruensek mod λ.

A második állítás nyilvánvaló, hiszen láttuk, hogy $\omega \equiv 1 \equiv \omega^2$ (λ). Ha pl. $\pi \mid \big((z-y),(z-\omega y)\big)$, ahol π Euler-prím, akkor $\pi \mid y(\omega - 1)$. De $\pi \mid y$ nem lehet,

Fermat-sejtés, $n = 3$ eset*

Köbszám 9-cel osztva, 0-t, 1-et, vagy -1-et adhat maradékul. Vagyis ha $x^3 + y^3 = z^3$, akkor van közöttük 9-cel osztható. Feltehető, hogy x, y, z páronként relatív prímek, ahogy a pitagoraszi számhármasoknál is, azaz alapmegoldásokat keresünk.

Miért hasznosak az Euler-egészek a Fermat-sejtés megoldásakor? Ha $x^3 + y^3 = z^3$, akkor $u^3 - 1 = (u-1)(u-\omega)(u-\omega^2)$ miatt $x^3 = (z-y)(z-\omega y)(z-\omega^2 y)$. Ha ezek relatív prímek lennének, akkor köbszámok lennének $\mathbb{E}$-ben (egységtényezőtől eltekintve).

$(z-y)$, $(z-\omega y)$, $(z-\omega^2 y)$ közül bármely kettő legnagyobb közös osztója 1 vagy λ, és e számok páronként kongruensek mod λ.

A második állítás nyilvánvaló, hiszen láttuk, hogy $\omega \equiv 1 \equiv \omega^2 \ (\lambda)$. Ha pl. $\pi \mid \big((z-y),(z-\omega y)\big)$, ahol π Euler-prím, akkor $\pi \mid y(\omega - 1)$. De $\pi \mid y$ nem lehet, mert akkor $\pi \mid z - y$ miatt $\pi \mid (y, z)$ lenne.

Fermat-sejtés, $n = 3$ eset*

Köbszám 9-cel osztva, 0-t, 1-et, vagy -1-et adhat maradékul. Vagyis ha $x^3 + y^3 = z^3$, akkor van közöttük 9-cel osztható. Feltehető, hogy x, y, z páronként relatív prímek, ahogy a pitagoraszi számhármasoknál is, azaz alapmegoldásokat keresünk.

Miért hasznosak az Euler-egészek a Fermat-sejtés megoldásakor? Ha $x^3 + y^3 = z^3$, akkor $u^3 - 1 = (u-1)(u-\omega)(u-\omega^2)$ miatt $x^3 = (z-y)(z-\omega y)(z-\omega^2 y)$. Ha ezek relatív prímek lennének, akkor köbszámok lennének $\mathbb{E}$-ben (egységtényezőtől eltekintve).

$(z-y)$, $(z-\omega y)$, $(z-\omega^2 y)$ közül bármely kettő legnagyobb közös osztója 1 vagy λ, és e számok páronként kongruensek mod λ.

A második állítás nyilvánvaló, hiszen láttuk, hogy $\omega \equiv 1 \equiv \omega^2$ (λ). Ha pl. $\pi \mid \big((z-y),(z-\omega y)\big)$, ahol π Euler-prím, akkor $\pi \mid y(\omega - 1)$. De $\pi \mid y$ nem lehet, mert akkor $\pi \mid z - y$ miatt $\pi \mid (y, z)$ lenne. Ezért $\pi \mid (1-\omega)$,

Fermat-sejtés, $n = 3$ eset*

Köbszám 9-cel osztva, 0-t, 1-et, vagy -1-et adhat maradékul. Vagyis ha $x^3 + y^3 = z^3$, akkor van közöttük 9-cel osztható. Feltehető, hogy x, y, z páronként relatív prímek, ahogy a pitagoraszi számhármasoknál is, azaz alapmegoldásokat keresünk.

Miért hasznosak az Euler-egészek a Fermat-sejtés megoldásakor? Ha $x^3 + y^3 = z^3$, akkor $u^3 - 1 = (u-1)(u-\omega)(u-\omega^2)$ miatt $x^3 = (z-y)(z-\omega y)(z-\omega^2 y)$. Ha ezek relatív prímek lennének, akkor köbszámok lennének $\mathbb{E}$-ben (egységtényezőtől eltekintve).

$(z-y)$, $(z-\omega y)$, $(z-\omega^2 y)$ közül bármely kettő legnagyobb közös osztója 1 vagy λ, és e számok páronként kongruensek mod λ.

A második állítás nyilvánvaló, hiszen láttuk, hogy $\omega \equiv 1 \equiv \omega^2 \ (\lambda)$. Ha pl. $\pi \mid \big((z-y),(z-\omega y)\big)$, ahol π Euler-prím, akkor $\pi \mid y(\omega - 1)$. De $\pi \mid y$ nem lehet, mert akkor $\pi \mid z - y$ miatt $\pi \mid (y, z)$ lenne. Ezért $\pi \mid (1-\omega)$, ami a λ prímnek asszociáltja. $\square$

A Fermat-tétel $n = 3$ esetének bizonyítása*

Kicsit általánosabban, belátjuk, hogy ha e, f, g Euler-egységek,

A Fermat-tétel $n = 3$ esetének bizonyítása*

Kicsit általánosabban, belátjuk, hogy ha e, f, g Euler-egységek, akkor az $ex^3 + fy^3 + gz^3 = 0$ egyenletnek nincs olyan megoldása $\mathbb{E}$-ben,

A Fermat-tétel $n = 3$ esetének bizonyítása*

Kicsit általánosabban, belátjuk, hogy ha e, f, g Euler-egységek, akkor az $ex^3 + fy^3 + gz^3 = 0$ egyenletnek nincs olyan megoldása $\mathbb{E}$-ben, ahol $\lambda \mid z$,

A Fermat-tétel $n = 3$ esetének bizonyítása*

Kicsit általánosabban, belátjuk, hogy ha e, f, g Euler-egységek, akkor az $ex^3 + fy^3 + gz^3 = 0$ egyenletnek nincs olyan megoldása $\mathbb{E}$-ben, ahol $\lambda \mid z$, de $\lambda \nmid x, y$.

A Fermat-tétel $n = 3$ esetének bizonyítása*

Kicsit általánosabban, belátjuk, hogy ha e, f, g Euler-egységek, akkor az $ex^3 + fy^3 + gz^3 = 0$ egyenletnek nincs olyan megoldása $\mathbb{E}$-ben, ahol $\lambda \mid z$, de $\lambda \nmid x, y$. Most is elég alapmegoldást keresni,

A Fermat-tétel $n = 3$ esetének bizonyítása*

Kicsit általánosabban, belátjuk, hogy ha e, f, g Euler-egységek, akkor az $ex^3 + fy^3 + gz^3 = 0$ egyenletnek nincs olyan megoldása $\mathbb{E}$-ben, ahol $\lambda \mid z$, de $\lambda \nmid x, y$. Most is elég alapmegoldást keresni, tegyük fel, hogy λ kitevője z-ben a fenti megoldásban a legkisebb.

A Fermat-tétel $n = 3$ esetének bizonyítása*

Kicsit általánosabban, belátjuk, hogy ha e, f, g Euler-egységek, akkor az $ex^3 + fy^3 + gz^3 = 0$ egyenletnek nincs olyan megoldása $\mathbb{E}$-ben, ahol $\lambda \mid z$, de $\lambda \nmid x, y$. Most is elég alapmegoldást keresni, tegyük fel, hogy λ kitevője z-ben a fenti megoldásban a legkisebb. Mivel $\lambda \nmid x$, láttuk, hogy $x^3 \equiv \pm 1 \ (\lambda^4)$.

A Fermat-tétel $n = 3$ esetének bizonyítása*

Kicsit általánosabban, belátjuk, hogy ha e, f, g Euler-egységek, akkor az $ex^3 + fy^3 + gz^3 = 0$ egyenletnek nincs olyan megoldása $\mathbb{E}$-ben, ahol $\lambda \mid z$, de $\lambda \nmid x, y$. Most is elég alapmegoldást keresni, tegyük fel, hogy λ kitevője z-ben a fenti megoldásban a legkisebb. Mivel $\lambda \nmid x$, láttuk, hogy $x^3 \equiv \pm 1\ (\lambda^4)$. Az x helyett $-x$-et írva feltehető, hogy $x^3 \equiv 1\ (\lambda^4)$,

A Fermat-tétel $n = 3$ esetének bizonyítása*

Kicsit általánosabban, belátjuk, hogy ha e, f, g Euler-egységek, akkor az $ex^3 + fy^3 + gz^3 = 0$ egyenletnek nincs olyan megoldása $\mathbb{E}$-ben, ahol $\lambda \mid z$, de $\lambda \nmid x, y$. Most is elég alapmegoldást keresni, tegyük fel, hogy λ kitevője z-ben a fenti megoldásban a legkisebb. Mivel $\lambda \nmid x$, láttuk, hogy $x^3 \equiv \pm 1\ (\lambda^4)$. Az x helyett $-x$-et írva feltehető, hogy $x^3 \equiv 1\ (\lambda^4)$, és hasonlóan y-ra is.

A Fermat-tétel $n = 3$ esetének bizonyítása*

Kicsit általánosabban, belátjuk, hogy ha e, f, g Euler-egységek, akkor az $ex^3 + fy^3 + gz^3 = 0$ egyenletnek nincs olyan megoldása $\mathbb{E}$-ben, ahol $\lambda \mid z$, de $\lambda \nmid x, y$. Most is elég alapmegoldást keresni, tegyük fel, hogy λ kitevője z-ben a fenti megoldásban a legkisebb. Mivel $\lambda \nmid x$, láttuk, hogy $x^3 \equiv \pm 1\ (\lambda^4)$. Az x helyett $-x$-et írva feltehető, hogy $x^3 \equiv 1\ (\lambda^4)$, és hasonlóan y-ra is. De $\lambda^3 \mid z^3$,

A Fermat-tétel $n = 3$ esetének bizonyítása*

Kicsit általánosabban, belátjuk, hogy ha e, f, g Euler-egységek, akkor az $ex^3 + fy^3 + gz^3 = 0$ egyenletnek nincs olyan megoldása $\mathbb{E}$-ben, ahol $\lambda \mid z$, de $\lambda \nmid x, y$. Most is elég alapmegoldást keresni, tegyük fel, hogy λ kitevője z-ben a fenti megoldásban a legkisebb. Mivel $\lambda \nmid x$, láttuk, hogy $x^3 \equiv \pm 1\ (\lambda^4)$. Az x helyett $-x$-et írva feltehető, hogy $x^3 \equiv 1\ (\lambda^4)$, és hasonlóan y-ra is. De $\lambda^3 \mid z^3$, így $e + f \equiv 0\ (\lambda^3)$.

A Fermat-tétel $n = 3$ esetének bizonyítása*

Kicsit általánosabban, belátjuk, hogy ha e, f, g Euler-egységek, akkor az $ex^3 + fy^3 + gz^3 = 0$ egyenletnek nincs olyan megoldása $\mathbb{E}$-ben, ahol $\lambda \mid z$, de $\lambda \nmid x, y$. Most is elég alapmegoldást keresni, tegyük fel, hogy λ kitevője z-ben a fenti megoldásban a legkisebb. Mivel $\lambda \nmid x$, láttuk, hogy $x^3 \equiv \pm 1\ (\lambda^4)$. Az x helyett $-x$-et írva feltehető, hogy $x^3 \equiv 1\ (\lambda^4)$, és hasonlóan y-ra is. De $\lambda^3 \mid z^3$, így $e + f \equiv 0\ (\lambda^3)$. Az egységek páronként inkongruensek mod λ^2,

A Fermat-tétel $n = 3$ esetének bizonyítása*

Kicsit általánosabban, belátjuk, hogy ha e, f, g Euler-egységek, akkor az $ex^3 + fy^3 + gz^3 = 0$ egyenletnek nincs olyan megoldása $\mathbb{E}$-ben, ahol $\lambda \mid z$, de $\lambda \nmid x, y$. Most is elég alapmegoldást keresni, tegyük fel, hogy λ kitevője z-ben a fenti megoldásban a legkisebb. Mivel $\lambda \nmid x$, láttuk, hogy $x^3 \equiv \pm 1\ (\lambda^4)$. Az x helyett $-x$-et írva feltehető, hogy $x^3 \equiv 1\ (\lambda^4)$, és hasonlóan y-ra is. De $\lambda^3 \mid z^3$, így $e + f \equiv 0\ (\lambda^3)$. Az egységek páronként inkongruensek mod λ^2, ezért $e = -f$.

A Fermat-tétel $n = 3$ esetének bizonyítása*

Kicsit általánosabban, belátjuk, hogy ha e, f, g Euler-egységek, akkor az $ex^3 + fy^3 + gz^3 = 0$ egyenletnek nincs olyan megoldása $\mathbb{E}$-ben, ahol $\lambda \mid z$, de $\lambda \nmid x, y$. Most is elég alapmegoldást keresni, tegyük fel, hogy λ kitevője z-ben a fenti megoldásban a legkisebb. Mivel $\lambda \nmid x$, láttuk, hogy $x^3 \equiv \pm 1\ (\lambda^4)$. Az x helyett $-x$-et írva feltehető, hogy $x^3 \equiv 1\ (\lambda^4)$, és hasonlóan y-ra is. De $\lambda^3 \mid z^3$, így $e + f \equiv 0\ (\lambda^3)$. Az egységek páronként inkongruensek mod λ^2, ezért $e = -f$. Visszahelyettesítve $e - e + gz^3 \equiv 0\ (\lambda^4)$,

A Fermat-tétel $n = 3$ esetének bizonyítása*

Kicsit általánosabban, belátjuk, hogy ha e, f, g Euler-egységek, akkor az $ex^3 + fy^3 + gz^3 = 0$ egyenletnek nincs olyan megoldása $\mathbb{E}$-ben, ahol $\lambda \mid z$, de $\lambda \nmid x, y$. Most is elég alapmegoldást keresni, tegyük fel, hogy λ kitevője z-ben a fenti megoldásban a legkisebb. Mivel $\lambda \nmid x$, láttuk, hogy $x^3 \equiv \pm 1\ (\lambda^4)$. Az x helyett $-x$-et írva feltehető, hogy $x^3 \equiv 1\ (\lambda^4)$, és hasonlóan y-ra is. De $\lambda^3 \mid z^3$, így $e + f \equiv 0\ (\lambda^3)$. Az egységek páronként inkongruensek mod λ^2, ezért $e = -f$. Visszahelyettesítve $e - e + gz^3 \equiv 0\ (\lambda^4)$, így $\lambda^2 \mid z$,

A Fermat-tétel $n = 3$ esetének bizonyítása*

Kicsit általánosabban, belátjuk, hogy ha e, f, g Euler-egységek, akkor az $ex^3 + fy^3 + gz^3 = 0$ egyenletnek nincs olyan megoldása $\mathbb{E}$-ben, ahol $\lambda \mid z$, de $\lambda \nmid x, y$. Most is elég alapmegoldást keresni, tegyük fel, hogy λ kitevője z-ben a fenti megoldásban a legkisebb. Mivel $\lambda \nmid x$, láttuk, hogy $x^3 \equiv \pm 1\ (\lambda^4)$. Az x helyett $-x$-et írva feltehető, hogy $x^3 \equiv 1\ (\lambda^4)$, és hasonlóan y-ra is. De $\lambda^3 \mid z^3$, így $e + f \equiv 0\ (\lambda^3)$. Az egységek páronként inkongruensek mod λ^2, ezért $e = -f$. Visszahelyettesítve $e - e + gz^3 \equiv 0\ (\lambda^4)$, így $\lambda^2 \mid z$, és $\lambda^6 \mid -(g/e)z^3 = x^3 - y^3$

A Fermat-tétel $n = 3$ esetének bizonyítása*

Kicsit általánosabban, belátjuk, hogy ha e, f, g Euler-egységek, akkor az $ex^3 + fy^3 + gz^3 = 0$ egyenletnek nincs olyan megoldása $\mathbb{E}$-ben, ahol $\lambda \mid z$, de $\lambda \nmid x, y$. Most is elég alapmegoldást keresni, tegyük fel, hogy λ kitevője z-ben a fenti megoldásban a legkisebb. Mivel $\lambda \nmid x$, láttuk, hogy $x^3 \equiv \pm 1\ (\lambda^4)$. Az x helyett $-x$-et írva feltehető, hogy $x^3 \equiv 1\ (\lambda^4)$, és hasonlóan y-ra is. De $\lambda^3 \mid z^3$, így $e + f \equiv 0\ (\lambda^3)$. Az egységek páronként inkongruensek mod λ^2, ezért $e = -f$. Visszahelyettesítve $e - e + gz^3 \equiv 0\ (\lambda^4)$, így $\lambda^2 \mid z$, és $\lambda^6 \mid -(g/e)z^3 = x^3 - y^3 = (x - y)(x - \omega y)(x - \omega^2 y)$.

A Fermat-tétel $n = 3$ esetének bizonyítása*

Kicsit általánosabban, belátjuk, hogy ha e, f, g Euler-egységek, akkor az $ex^3 + fy^3 + gz^3 = 0$ egyenletnek nincs olyan megoldása $\mathbb{E}$-ben, ahol $\lambda \mid z$, de $\lambda \nmid x, y$. Most is elég alapmegoldást keresni, tegyük fel, hogy λ kitevője z-ben a fenti megoldásban a legkisebb. Mivel $\lambda \nmid x$, láttuk, hogy $x^3 \equiv \pm 1\ (\lambda^4)$. Az x helyett $-x$-et írva feltehető, hogy $x^3 \equiv 1\ (\lambda^4)$, és hasonlóan y-ra is. De $\lambda^3 \mid z^3$, így $e + f \equiv 0\ (\lambda^3)$. Az egységek páronként inkongruensek mod λ^2, ezért $e = -f$. Visszahelyettesítve $e - e + gz^3 \equiv 0\ (\lambda^4)$, így $\lambda^2 \mid z$, és $\lambda^6 \mid -(g/e)z^3 = x^3 - y^3 = (x - y)(x - \omega y)(x - \omega^2 y)$.
Láttuk, hogy a három tényező λ-val osztás után páronként relatív prím,

A Fermat-tétel $n = 3$ esetének bizonyítása*

Kicsit általánosabban, belátjuk, hogy ha e, f, g Euler-egységek, akkor az $ex^3 + fy^3 + gz^3 = 0$ egyenletnek nincs olyan megoldása $\mathbb{E}$-ben, ahol $\lambda \mid z$, de $\lambda \nmid x, y$. Most is elég alapmegoldást keresni, tegyük fel, hogy λ kitevője z-ben a fenti megoldásban a legkisebb. Mivel $\lambda \nmid x$, láttuk, hogy $x^3 \equiv \pm 1\ (\lambda^4)$. Az x helyett $-x$-et írva feltehető, hogy $x^3 \equiv 1\ (\lambda^4)$, és hasonlóan y-ra is. De $\lambda^3 \mid z^3$, így $e + f \equiv 0\ (\lambda^3)$. Az egységek páronként inkongruensek mod λ^2, ezért $e = -f$. Visszahelyettesítve $e - e + gz^3 \equiv 0\ (\lambda^4)$, így $\lambda^2 \mid z$, és $\lambda^6 \mid -(g/e)z^3 = x^3 - y^3 = (x - y)(x - \omega y)(x - \omega^2 y)$.
Láttuk, hogy a három tényező λ-val osztás után páronként relatív prím, ezért $x - y = e_1 \lambda x_1^3$,

A Fermat-tétel $n = 3$ esetének bizonyítása*

Kicsit általánosabban, belátjuk, hogy ha e, f, g Euler-egységek, akkor az $ex^3 + fy^3 + gz^3 = 0$ egyenletnek nincs olyan megoldása $\mathbb{E}$-ben, ahol $\lambda \mid z$, de $\lambda \nmid x, y$. Most is elég alapmegoldást keresni, tegyük fel, hogy λ kitevője z-ben a fenti megoldásban a legkisebb. Mivel $\lambda \nmid x$, láttuk, hogy $x^3 \equiv \pm 1\ (\lambda^4)$. Az x helyett $-x$-et írva feltehető, hogy $x^3 \equiv 1\ (\lambda^4)$, és hasonlóan y-ra is. De $\lambda^3 \mid z^3$, így $e + f \equiv 0\ (\lambda^3)$. Az egységek páronként inkongruensek mod λ^2, ezért $e = -f$. Visszahelyettesítve $e - e + gz^3 \equiv 0\ (\lambda^4)$, így $\lambda^2 \mid z$, és $\lambda^6 \mid -(g/e)z^3 = x^3 - y^3 = (x - y)(x - \omega y)(x - \omega^2 y)$.
Láttuk, hogy a három tényező λ-val osztás után páronként relatív prím, ezért $x - y = e_1 \lambda x_1^3$, $x - \omega y = f_1 \lambda y_1^3$,

A Fermat-tétel $n = 3$ esetének bizonyítása*

Kicsit általánosabban, belátjuk, hogy ha e, f, g Euler-egységek, akkor az $ex^3 + fy^3 + gz^3 = 0$ egyenletnek nincs olyan megoldása $\mathbb{E}$-ben, ahol $\lambda \mid z$, de $\lambda \nmid x, y$. Most is elég alapmegoldást keresni, tegyük fel, hogy λ kitevője z-ben a fenti megoldásban a legkisebb. Mivel $\lambda \nmid x$, láttuk, hogy $x^3 \equiv \pm 1\ (\lambda^4)$. Az x helyett $-x$-et írva feltehető, hogy $x^3 \equiv 1\ (\lambda^4)$, és hasonlóan y-ra is. De $\lambda^3 \mid z^3$, így $e + f \equiv 0\ (\lambda^3)$. Az egységek páronként inkongruensek mod λ^2, ezért $e = -f$. Visszahelyettesítve $e - e + gz^3 \equiv 0\ (\lambda^4)$, így $\lambda^2 \mid z$, és $\lambda^6 \mid -(g/e)z^3 = x^3 - y^3 = (x - y)(x - \omega y)(x - \omega^2 y)$.
Láttuk, hogy a három tényező λ-val osztás után páronként relatív prím, ezért $x - y = e_1 \lambda x_1^3$, $x - \omega y = f_1 \lambda y_1^3$, $x - \omega^2 y = g_1 \lambda z_1^3$

A Fermat-tétel $n = 3$ esetének bizonyítása*

Kicsit általánosabban, belátjuk, hogy ha e, f, g Euler-egységek, akkor az $ex^3 + fy^3 + gz^3 = 0$ egyenletnek nincs olyan megoldása $\mathbb{E}$-ben, ahol $\lambda \mid z$, de $\lambda \nmid x, y$. Most is elég alapmegoldást keresni, tegyük fel, hogy λ kitevője z-ben a fenti megoldásban a legkisebb. Mivel $\lambda \nmid x$, láttuk, hogy $x^3 \equiv \pm 1\ (\lambda^4)$. Az x helyett $-x$-et írva feltehető, hogy $x^3 \equiv 1\ (\lambda^4)$, és hasonlóan y-ra is. De $\lambda^3 \mid z^3$, így $e + f \equiv 0\ (\lambda^3)$. Az egységek páronként inkongruensek mod λ^2, ezért $e = -f$. Visszahelyettesítve $e - e + gz^3 \equiv 0\ (\lambda^4)$, így $\lambda^2 \mid z$, és $\lambda^6 \mid -(g/e)z^3 = x^3 - y^3 = (x - y)(x - \omega y)(x - \omega^2 y)$.
Láttuk, hogy a három tényező λ-val osztás után páronként relatív prím, ezért $x - y = e_1 \lambda x_1^3$, $x - \omega y = f_1 \lambda y_1^3$, $x - \omega^2 y = g_1 \lambda z_1^3$ alkalmas e_1, f_1, g_1 egységekre.

A Fermat-tétel $n = 3$ esetének bizonyítása*

Kicsit általánosabban, belátjuk, hogy ha e, f, g Euler-egységek, akkor az $ex^3 + fy^3 + gz^3 = 0$ egyenletnek nincs olyan megoldása $\mathbb{E}$-ben, ahol $\lambda \mid z$, de $\lambda \nmid x, y$. Most is elég alapmegoldást keresni, tegyük fel, hogy λ kitevője z-ben a fenti megoldásban a legkisebb. Mivel $\lambda \nmid x$, láttuk, hogy $x^3 \equiv \pm 1\ (\lambda^4)$. Az x helyett $-x$-et írva feltehető, hogy $x^3 \equiv 1\ (\lambda^4)$, és hasonlóan y-ra is. De $\lambda^3 \mid z^3$, így $e + f \equiv 0\ (\lambda^3)$. Az egységek páronként inkongruensek mod λ^2, ezért $e = -f$. Visszahelyettesítve $e - e + gz^3 \equiv 0\ (\lambda^4)$, így $\lambda^2 \mid z$, és $\lambda^6 \mid -(g/e)z^3 = x^3 - y^3 = (x - y)(x - \omega y)(x - \omega^2 y)$.
Láttuk, hogy a három tényező λ-val osztás után páronként relatív prím, ezért $x - y = e_1 \lambda x_1^3$, $x - \omega y = f_1 \lambda y_1^3$, $x - \omega^2 y = g_1 \lambda z_1^3$ alkalmas e_1, f_1, g_1 egységekre. Az 1, ω, ω^2 együtthatókkal szorozva és összeadva

A Fermat-tétel $n = 3$ esetének bizonyítása*

Kicsit általánosabban, belátjuk, hogy ha e, f, g Euler-egységek, akkor az $ex^3 + fy^3 + gz^3 = 0$ egyenletnek nincs olyan megoldása $\mathbb{E}$-ben, ahol $\lambda \mid z$, de $\lambda \nmid x, y$. Most is elég alapmegoldást keresni, tegyük fel, hogy λ kitevője z-ben a fenti megoldásban a legkisebb. Mivel $\lambda \nmid x$, láttuk, hogy $x^3 \equiv \pm 1\ (\lambda^4)$. Az x helyett $-x$-et írva feltehető, hogy $x^3 \equiv 1\ (\lambda^4)$, és hasonlóan y-ra is. De $\lambda^3 \mid z^3$, így $e + f \equiv 0\ (\lambda^3)$. Az egységek páronként inkongruensek mod λ^2, ezért $e = -f$. Visszahelyettesítve $e - e + gz^3 \equiv 0\ (\lambda^4)$, így $\lambda^2 \mid z$, és $\lambda^6 \mid -(g/e)z^3 = x^3 - y^3 = (x - y)(x - \omega y)(x - \omega^2 y)$.
Láttuk, hogy a három tényező λ-val osztás után páronként relatív prím, ezért $x - y = e_1 \lambda x_1^3$, $x - \omega y = f_1 \lambda y_1^3$, $x - \omega^2 y = g_1 \lambda z_1^3$ alkalmas e_1, f_1, g_1 egységekre. Az 1, ω, ω^2 együtthatókkal szorozva és összeadva $1 + \omega + \omega^2 = 0$ miatt

A Fermat-tétel $n = 3$ esetének bizonyítása*

Kicsit általánosabban, belátjuk, hogy ha e, f, g Euler-egységek, akkor az $ex^3 + fy^3 + gz^3 = 0$ egyenletnek nincs olyan megoldása $\mathbb{E}$-ben, ahol $\lambda \mid z$, de $\lambda \nmid x, y$. Most is elég alapmegoldást keresni, tegyük fel, hogy λ kitevője z-ben a fenti megoldásban a legkisebb. Mivel $\lambda \nmid x$, láttuk, hogy $x^3 \equiv \pm 1\ (\lambda^4)$. Az x helyett $-x$-et írva feltehető, hogy $x^3 \equiv 1\ (\lambda^4)$, és hasonlóan y-ra is. De $\lambda^3 \mid z^3$, így $e + f \equiv 0\ (\lambda^3)$. Az egységek páronként inkongruensek mod λ^2, ezért $e = -f$. Visszahelyettesítve $e - e + gz^3 \equiv 0\ (\lambda^4)$, így $\lambda^2 \mid z$, és $\lambda^6 \mid -(g/e)z^3 = x^3 - y^3 = (x - y)(x - \omega y)(x - \omega^2 y)$.
Láttuk, hogy a három tényező λ-val osztás után páronként relatív prím, ezért $x - y = e_1 \lambda x_1^3$, $x - \omega y = f_1 \lambda y_1^3$, $x - \omega^2 y = g_1 \lambda z_1^3$ alkalmas e_1, f_1, g_1 egységekre. Az 1, ω, ω^2 együtthatókkal szorozva és összeadva $1 + \omega + \omega^2 = 0$ miatt $0 = e_1 x_1^3 + \omega f_1 y_1^3 + \omega^2 g_1 z_1^3$.

A Fermat-tétel $n = 3$ esetének bizonyítása*

Kicsit általánosabban, belátjuk, hogy ha e, f, g Euler-egységek, akkor az $ex^3 + fy^3 + gz^3 = 0$ egyenletnek nincs olyan megoldása $\mathbb{E}$-ben, ahol $\lambda \mid z$, de $\lambda \nmid x, y$. Most is elég alapmegoldást keresni, tegyük fel, hogy λ kitevője z-ben a fenti megoldásban a legkisebb. Mivel $\lambda \nmid x$, láttuk, hogy $x^3 \equiv \pm 1\ (\lambda^4)$. Az x helyett $-x$-et írva feltehető, hogy $x^3 \equiv 1\ (\lambda^4)$, és hasonlóan y-ra is. De $\lambda^3 \mid z^3$, így $e + f \equiv 0\ (\lambda^3)$. Az egységek páronként inkongruensek mod λ^2, ezért $e = -f$. Visszahelyettesítve $e - e + gz^3 \equiv 0\ (\lambda^4)$, így $\lambda^2 \mid z$, és $\lambda^6 \mid -(g/e)z^3 = x^3 - y^3 = (x - y)(x - \omega y)(x - \omega^2 y)$.
Láttuk, hogy a három tényező λ-val osztás után páronként relatív prím, ezért $x - y = e_1 \lambda x_1^3$, $x - \omega y = f_1 \lambda y_1^3$, $x - \omega^2 y = g_1 \lambda z_1^3$ alkalmas e_1, f_1, g_1 egységekre. Az 1, ω, ω^2 együtthatókkal szorozva és összeadva $1 + \omega + \omega^2 = 0$ miatt $0 = e_1 x_1^3 + \omega f_1 y_1^3 + \omega^2 g_1 z_1^3$.
Ez olyan egyenlet, mint amiből kiindultunk.

A Fermat-tétel $n = 3$ esetének bizonyítása*

Kicsit általánosabban, belátjuk, hogy ha e, f, g Euler-egységek, akkor az $ex^3 + fy^3 + gz^3 = 0$ egyenletnek nincs olyan megoldása $\mathbb{E}$-ben, ahol $\lambda \mid z$, de $\lambda \nmid x, y$. Most is elég alapmegoldást keresni, tegyük fel, hogy λ kitevője z-ben a fenti megoldásban a legkisebb. Mivel $\lambda \nmid x$, láttuk, hogy $x^3 \equiv \pm 1\ (\lambda^4)$. Az x helyett $-x$-et írva feltehető, hogy $x^3 \equiv 1\ (\lambda^4)$, és hasonlóan y-ra is. De $\lambda^3 \mid z^3$, így $e + f \equiv 0\ (\lambda^3)$. Az egységek páronként inkongruensek mod λ^2, ezért $e = -f$. Visszahelyettesítve $e - e + gz^3 \equiv 0\ (\lambda^4)$, így $\lambda^2 \mid z$, és $\lambda^6 \mid -(g/e)z^3 = x^3 - y^3 = (x - y)(x - \omega y)(x - \omega^2 y)$.
Láttuk, hogy a három tényező λ-val osztás után páronként relatív prím, ezért $x - y = e_1 \lambda x_1^3$, $x - \omega y = f_1 \lambda y_1^3$, $x - \omega^2 y = g_1 \lambda z_1^3$ alkalmas e_1, f_1, g_1 egységekre. Az 1, ω, ω^2 együtthatókkal szorozva és összeadva $1 + \omega + \omega^2 = 0$ miatt $0 = e_1 x_1^3 + \omega f_1 y_1^3 + \omega^2 g_1 z_1^3$.
Ez olyan egyenlet, mint amiből kiindultunk. Mivel $\lambda^6 \mid z^3$,

A Fermat-tétel $n = 3$ esetének bizonyítása*

Kicsit általánosabban, belátjuk, hogy ha e, f, g Euler-egységek, akkor az $ex^3 + fy^3 + gz^3 = 0$ egyenletnek nincs olyan megoldása $\mathbb{E}$-ben, ahol $\lambda \mid z$, de $\lambda \nmid x, y$. Most is elég alapmegoldást keresni, tegyük fel, hogy λ kitevője z-ben a fenti megoldásban a legkisebb. Mivel $\lambda \nmid x$, láttuk, hogy $x^3 \equiv \pm 1\ (\lambda^4)$. Az x helyett $-x$-et írva feltehető, hogy $x^3 \equiv 1\ (\lambda^4)$, és hasonlóan y-ra is. De $\lambda^3 \mid z^3$, így $e + f \equiv 0\ (\lambda^3)$. Az egységek páronként inkongruensek mod λ^2, ezért $e = -f$. Visszahelyettesítve $e - e + gz^3 \equiv 0\ (\lambda^4)$, így $\lambda^2 \mid z$, és $\lambda^6 \mid -(g/e)z^3 = x^3 - y^3 = (x - y)(x - \omega y)(x - \omega^2 y)$.
Láttuk, hogy a három tényező λ-val osztás után páronként relatív prím, ezért $x - y = e_1 \lambda x_1^3$, $x - \omega y = f_1 \lambda y_1^3$, $x - \omega^2 y = g_1 \lambda z_1^3$ alkalmas e_1, f_1, g_1 egységekre. Az 1, ω, ω^2 együtthatókkal szorozva és összeadva $1 + \omega + \omega^2 = 0$ miatt $0 = e_1 x_1^3 + \omega f_1 y_1^3 + \omega^2 g_1 z_1^3$.
Ez olyan egyenlet, mint amiből kiindultunk. Mivel $\lambda^6 \mid z^3$, ezért $\lambda \mid x_1 y_1 z_1$,

A Fermat-tétel $n = 3$ esetének bizonyítása*

Kicsit általánosabban, belátjuk, hogy ha e, f, g Euler-egységek, akkor az $ex^3 + fy^3 + gz^3 = 0$ egyenletnek nincs olyan megoldása $\mathbb{E}$-ben, ahol $\lambda \mid z$, de $\lambda \nmid x, y$. Most is elég alapmegoldást keresni, tegyük fel, hogy λ kitevője z-ben a fenti megoldásban a legkisebb. Mivel $\lambda \nmid x$, láttuk, hogy $x^3 \equiv \pm 1\ (\lambda^4)$. Az x helyett $-x$-et írva feltehető, hogy $x^3 \equiv 1\ (\lambda^4)$, és hasonlóan y-ra is. De $\lambda^3 \mid z^3$, így $e + f \equiv 0\ (\lambda^3)$. Az egységek páronként inkongruensek mod λ^2, ezért $e = -f$. Visszahelyettesítve $e - e + gz^3 \equiv 0\ (\lambda^4)$, így $\lambda^2 \mid z$, és $\lambda^6 \mid -(g/e)z^3 = x^3 - y^3 = (x - y)(x - \omega y)(x - \omega^2 y)$.
Láttuk, hogy a három tényező λ-val osztás után páronként relatív prím, ezért $x - y = e_1 \lambda x_1^3$, $x - \omega y = f_1 \lambda y_1^3$, $x - \omega^2 y = g_1 \lambda z_1^3$ alkalmas e_1, f_1, g_1 egységekre. Az 1, ω, ω^2 együtthatókkal szorozva és összeadva $1 + \omega + \omega^2 = 0$ miatt $0 = e_1 x_1^3 + \omega f_1 y_1^3 + \omega^2 g_1 z_1^3$.
Ez olyan egyenlet, mint amiből kiindultunk. Mivel $\lambda^6 \mid z^3$, ezért $\lambda \mid x_1 y_1 z_1$, pl. $\lambda \mid z_1$,

A Fermat-tétel $n = 3$ esetének bizonyítása*

Kicsit általánosabban, belátjuk, hogy ha e, f, g Euler-egységek, akkor az $ex^3 + fy^3 + gz^3 = 0$ egyenletnek nincs olyan megoldása $\mathbb{E}$-ben, ahol $\lambda \mid z$, de $\lambda \nmid x, y$. Most is elég alapmegoldást keresni, tegyük fel, hogy λ kitevője z-ben a fenti megoldásban a legkisebb. Mivel $\lambda \nmid x$, láttuk, hogy $x^3 \equiv \pm 1\ (\lambda^4)$. Az x helyett $-x$-et írva feltehető, hogy $x^3 \equiv 1\ (\lambda^4)$, és hasonlóan y-ra is. De $\lambda^3 \mid z^3$, így $e + f \equiv 0\ (\lambda^3)$. Az egységek páronként inkongruensek mod λ^2, ezért $e = -f$. Visszahelyettesítve $e - e + gz^3 \equiv 0\ (\lambda^4)$, így $\lambda^2 \mid z$, és $\lambda^6 \mid -(g/e)z^3 = x^3 - y^3 = (x - y)(x - \omega y)(x - \omega^2 y)$.
Láttuk, hogy a három tényező λ-val osztás után páronként relatív prím, ezért $x - y = e_1 \lambda x_1^3$, $x - \omega y = f_1 \lambda y_1^3$, $x - \omega^2 y = g_1 \lambda z_1^3$ alkalmas e_1, f_1, g_1 egységekre. Az 1, ω, ω^2 együtthatókkal szorozva és összeadva $1 + \omega + \omega^2 = 0$ miatt $0 = e_1 x_1^3 + \omega f_1 y_1^3 + \omega^2 g_1 z_1^3$.
Ez olyan egyenlet, mint amiből kiindultunk. Mivel $\lambda^6 \mid z^3$, ezért $\lambda \mid x_1 y_1 z_1$, pl. $\lambda \mid z_1$, de akkor $\lambda \nmid x_1$

A Fermat-tétel $n = 3$ esetének bizonyítása*

Kicsit általánosabban, belátjuk, hogy ha e, f, g Euler-egységek, akkor az $ex^3 + fy^3 + gz^3 = 0$ egyenletnek nincs olyan megoldása $\mathbb{E}$-ben, ahol $\lambda \mid z$, de $\lambda \nmid x, y$. Most is elég alapmegoldást keresni, tegyük fel, hogy λ kitevője z-ben a fenti megoldásban a legkisebb. Mivel $\lambda \nmid x$, láttuk, hogy $x^3 \equiv \pm 1\ (\lambda^4)$. Az x helyett $-x$-et írva feltehető, hogy $x^3 \equiv 1\ (\lambda^4)$, és hasonlóan y-ra is. De $\lambda^3 \mid z^3$, így $e + f \equiv 0\ (\lambda^3)$. Az egységek páronként inkongruensek mod λ^2, ezért $e = -f$. Visszahelyettesítve $e - e + gz^3 \equiv 0\ (\lambda^4)$, így $\lambda^2 \mid z$, és $\lambda^6 \mid -(g/e)z^3 = x^3 - y^3 = (x - y)(x - \omega y)(x - \omega^2 y)$.
Láttuk, hogy a három tényező λ-val osztás után páronként relatív prím, ezért $x - y = e_1 \lambda x_1^3$, $x - \omega y = f_1 \lambda y_1^3$, $x - \omega^2 y = g_1 \lambda z_1^3$ alkalmas e_1, f_1, g_1 egységekre. Az 1, ω, ω^2 együtthatókkal szorozva és összeadva $1 + \omega + \omega^2 = 0$ miatt $0 = e_1 x_1^3 + \omega f_1 y_1^3 + \omega^2 g_1 z_1^3$. Ez olyan egyenlet, mint amiből kiindultunk. Mivel $\lambda^6 \mid z^3$, ezért $\lambda \mid x_1 y_1 z_1$, pl. $\lambda \mid z_1$, de akkor $\lambda \nmid x_1$ (és y_1),

A Fermat-tétel $n = 3$ esetének bizonyítása*

Kicsit általánosabban, belátjuk, hogy ha e, f, g Euler-egységek, akkor az $ex^3 + fy^3 + gz^3 = 0$ egyenletnek nincs olyan megoldása $\mathbb{E}$-ben, ahol $\lambda \mid z$, de $\lambda \nmid x, y$. Most is elég alapmegoldást keresni, tegyük fel, hogy λ kitevője z-ben a fenti megoldásban a legkisebb. Mivel $\lambda \nmid x$, láttuk, hogy $x^3 \equiv \pm 1\ (\lambda^4)$. Az x helyett $-x$-et írva feltehető, hogy $x^3 \equiv 1\ (\lambda^4)$, és hasonlóan y-ra is. De $\lambda^3 \mid z^3$, így $e + f \equiv 0\ (\lambda^3)$. Az egységek páronként inkongruensek mod λ^2, ezért $e = -f$. Visszahelyettesítve $e - e + gz^3 \equiv 0\ (\lambda^4)$, így $\lambda^2 \mid z$, és $\lambda^6 \mid -(g/e)z^3 = x^3 - y^3 = (x - y)(x - \omega y)(x - \omega^2 y)$.
Láttuk, hogy a három tényező λ-val osztás után páronként relatív prím, ezért $x - y = e_1 \lambda x_1^3$, $x - \omega y = f_1 \lambda y_1^3$, $x - \omega^2 y = g_1 \lambda z_1^3$ alkalmas e_1, f_1, g_1 egységekre. Az 1, ω, ω^2 együtthatókkal szorozva és összeadva $1 + \omega + \omega^2 = 0$ miatt $0 = e_1 x_1^3 + \omega f_1 y_1^3 + \omega^2 g_1 z_1^3$. Ez olyan egyenlet, mint amiből kiindultunk. Mivel $\lambda^6 \mid z^3$, ezért $\lambda \mid x_1 y_1 z_1$, pl. $\lambda \mid z_1$, de akkor $\lambda \nmid x_1$ (és y_1), hiszen $(z_1, x_1) = 1$.

A Fermat-tétel $n = 3$ esetének bizonyítása*

Kicsit általánosabban, belátjuk, hogy ha e, f, g Euler-egységek, akkor az $ex^3 + fy^3 + gz^3 = 0$ egyenletnek nincs olyan megoldása $\mathbb{E}$-ben, ahol $\lambda \mid z$, de $\lambda \nmid x, y$. Most is elég alapmegoldást keresni, tegyük fel, hogy λ kitevője z-ben a fenti megoldásban a legkisebb. Mivel $\lambda \nmid x$, láttuk, hogy $x^3 \equiv \pm 1\ (\lambda^4)$. Az x helyett $-x$-et írva feltehető, hogy $x^3 \equiv 1\ (\lambda^4)$, és hasonlóan y-ra is. De $\lambda^3 \mid z^3$, így $e + f \equiv 0\ (\lambda^3)$. Az egységek páronként inkongruensek mod λ^2, ezért $e = -f$. Visszahelyettesítve $e - e + gz^3 \equiv 0\ (\lambda^4)$, így $\lambda^2 \mid z$, és $\lambda^6 \mid -(g/e)z^3 = x^3 - y^3 = (x - y)(x - \omega y)(x - \omega^2 y)$.
Láttuk, hogy a három tényező λ-val osztás után páronként relatív prím, ezért $x - y = e_1 \lambda x_1^3$, $x - \omega y = f_1 \lambda y_1^3$, $x - \omega^2 y = g_1 \lambda z_1^3$ alkalmas e_1, f_1, g_1 egységekre. Az 1, ω, ω^2 együtthatókkal szorozva és összeadva $1 + \omega + \omega^2 = 0$ miatt $0 = e_1 x_1^3 + \omega f_1 y_1^3 + \omega^2 g_1 z_1^3$.
Ez olyan egyenlet, mint amiből kiindultunk. Mivel $\lambda^6 \mid z^3$, ezért $\lambda \mid x_1 y_1 z_1$, pl. $\lambda \mid z_1$, de akkor $\lambda \nmid x_1$ (és y_1), hiszen $(z_1, x_1) = 1$.
De ha $\lambda^k \mid z_1$,

A Fermat-tétel $n = 3$ esetének bizonyítása*

Kicsit általánosabban, belátjuk, hogy ha e, f, g Euler-egységek, akkor az $ex^3 + fy^3 + gz^3 = 0$ egyenletnek nincs olyan megoldása $\mathbb{E}$-ben, ahol $\lambda \mid z$, de $\lambda \nmid x, y$. Most is elég alapmegoldást keresni, tegyük fel, hogy λ kitevője z-ben a fenti megoldásban a legkisebb. Mivel $\lambda \nmid x$, láttuk, hogy $x^3 \equiv \pm 1\ (\lambda^4)$. Az x helyett $-x$-et írva feltehető, hogy $x^3 \equiv 1\ (\lambda^4)$, és hasonlóan y-ra is. De $\lambda^3 \mid z^3$, így $e + f \equiv 0\ (\lambda^3)$. Az egységek páronként inkongruensek mod λ^2, ezért $e = -f$. Visszahelyettesítve $e - e + gz^3 \equiv 0\ (\lambda^4)$, így $\lambda^2 \mid z$, és $\lambda^6 \mid -(g/e)z^3 = x^3 - y^3 = (x - y)(x - \omega y)(x - \omega^2 y)$.
Láttuk, hogy a három tényező λ-val osztás után páronként relatív prím, ezért $x - y = e_1 \lambda x_1^3$, $x - \omega y = f_1 \lambda y_1^3$, $x - \omega^2 y = g_1 \lambda z_1^3$ alkalmas e_1, f_1, g_1 egységekre. Az 1, ω, ω^2 együtthatókkal szorozva és összeadva $1 + \omega + \omega^2 = 0$ miatt $0 = e_1 x_1^3 + \omega f_1 y_1^3 + \omega^2 g_1 z_1^3$.
Ez olyan egyenlet, mint amiből kiindultunk. Mivel $\lambda^6 \mid z^3$, ezért $\lambda \mid x_1 y_1 z_1$, pl. $\lambda \mid z_1$, de akkor $\lambda \nmid x_1$ (és y_1), hiszen $(z_1, x_1) = 1$.
De ha $\lambda^k \mid z_1$, akkor $\lambda z_1^3 \mid z^3$ miatt $\lambda^{k+1} \mid z$,

A Fermat-tétel $n = 3$ esetének bizonyítása*

Kicsit általánosabban, belátjuk, hogy ha e, f, g Euler-egységek, akkor az $ex^3 + fy^3 + gz^3 = 0$ egyenletnek nincs olyan megoldása $\mathbb{E}$-ben, ahol $\lambda \mid z$, de $\lambda \nmid x, y$. Most is elég alapmegoldást keresni, tegyük fel, hogy λ kitevője z-ben a fenti megoldásban a legkisebb. Mivel $\lambda \nmid x$, láttuk, hogy $x^3 \equiv \pm 1\ (\lambda^4)$. Az x helyett $-x$-et írva feltehető, hogy $x^3 \equiv 1\ (\lambda^4)$, és hasonlóan y-ra is. De $\lambda^3 \mid z^3$, így $e + f \equiv 0\ (\lambda^3)$. Az egységek páronként inkongruensek mod λ^2, ezért $e = -f$. Visszahelyettesítve $e - e + gz^3 \equiv 0\ (\lambda^4)$, így $\lambda^2 \mid z$, és $\lambda^6 \mid -(g/e)z^3 = x^3 - y^3 = (x - y)(x - \omega y)(x - \omega^2 y)$.
Láttuk, hogy a három tényező λ-val osztás után páronként relatív prím, ezért $x - y = e_1 \lambda x_1^3$, $x - \omega y = f_1 \lambda y_1^3$, $x - \omega^2 y = g_1 \lambda z_1^3$ alkalmas e_1, f_1, g_1 egységekre. Az 1, ω, ω^2 együtthatókkal szorozva és összeadva $1 + \omega + \omega^2 = 0$ miatt $0 = e_1 x_1^3 + \omega f_1 y_1^3 + \omega^2 g_1 z_1^3$.
Ez olyan egyenlet, mint amiből kiindultunk. Mivel $\lambda^6 \mid z^3$, ezért $\lambda \mid x_1 y_1 z_1$, pl. $\lambda \mid z_1$, de akkor $\lambda \nmid x_1$ (és y_1), hiszen $(z_1, x_1) = 1$.
De ha $\lambda^k \mid z_1$, akkor $\lambda z_1^3 \mid z^3$ miatt $\lambda^{k+1} \mid z$, ellentmondás. □

A 31. előadás összefoglalása

Fogalmak

Algebrai és transzcendens szám (FGy9.1.1, K5.10.8).

A 31. előadás összefoglalása

Fogalmak

Algebrai és transzcendens szám (FGy9.1.1, K5.10.8).
Gauss- és Euler-egészek.

A 31. előadás összefoglalása

Fogalmak

Algebrai és transzcendens szám (FGy9.1.1, K5.10.8).
Gauss- és Euler-egészek.

Tételek

Az algebrai számok megszámlálható,

A 31. előadás összefoglalása

Fogalmak

Algebrai és transzcendens szám (FGy9.1.1, K5.10.8).
Gauss- és Euler-egészek.

Tételek

Az algebrai számok megszámlálható, algebrailag zárt testet alkotnak (FGy9.3.1, 9.3.6, 9.1.3, K6.2.12, 6.2.13, NB).

A 31. előadás összefoglalása

Fogalmak

Algebrai és transzcendens szám (FGy9.1.1, K5.10.8).
Gauss- és Euler-egészek.

Tételek

Az algebrai számok megszámlálható, algebrailag zárt testet alkotnak (FGy9.3.1, 9.3.6, 9.1.3, K6.2.12, 6.2.13, NB).
Példák: a Gelfond-Schneider-tétel (FGy9.3.5),

A 31. előadás összefoglalása

Fogalmak

Algebrai és transzcendens szám (FGy9.1.1, K5.10.8).
Gauss- és Euler-egészek.

Tételek

Az algebrai számok megszámlálható, algebrailag zárt testet alkotnak (FGy9.3.1, 9.3.6, 9.1.3, K6.2.12, 6.2.13, NB).
Példák: a Gelfond-Schneider-tétel (FGy9.3.5), e és π irracionális (FGy9.5.1–2),

A 31. előadás összefoglalása

Fogalmak

Algebrai és transzcendens szám (FGy9.1.1, K5.10.8).
Gauss- és Euler-egészek.

Tételek

Az algebrai számok megszámlálható, algebrailag zárt testet alkotnak (FGy9.3.1, 9.3.6, 9.1.3, K6.2.12, 6.2.13, NB).
Példák: a Gelfond-Schneider-tétel (FGy9.3.5), e és π irracionális (FGy9.5.1–2), a Liouville-szám transzcendens (FGy9.4.2).

A 31. előadás összefoglalása

Fogalmak

Algebrai és transzcendens szám (FGy9.1.1, K5.10.8).
Gauss- és Euler-egészek.

Tételek

Az algebrai számok megszámlálható, algebrailag zárt testet alkotnak (FGy9.3.1, 9.3.6, 9.1.3, K6.2.12, 6.2.13, NB).
Példák: a Gelfond-Schneider-tétel (FGy9.3.5), e és π irracionális (FGy9.5.1–2), a Liouville-szám transzcendens (FGy9.4.2).
Négy és három négyzetszám-tétel (FGy7.5.2–3, NB).

A 31. előadás összefoglalása

Fogalmak

Algebrai és transzcendens szám (FGy9.1.1, K5.10.8).
Gauss- és Euler-egészek.

Tételek

Az algebrai számok megszámlálható, algebrailag zárt testet alkotnak (FGy9.3.1, 9.3.6, 9.1.3, K6.2.12, 6.2.13, NB).
Példák: a Gelfond-Schneider-tétel (FGy9.3.5), e és π irracionális (FGy9.5.1–2), a Liouville-szám transzcendens (FGy9.4.2).
Négy és három négyzetszám-tétel (FGy7.5.2–3, NB).
Két négyzetszám-tétel, a megoldások száma (FGy7.5.1).

A 31. előadás összefoglalása

Fogalmak

Algebrai és transzcendens szám (FGy9.1.1, K5.10.8).
Gauss- és Euler-egészek.

Tételek

Az algebrai számok megszámlálható, algebrailag zárt testet alkotnak (FGy9.3.1, 9.3.6, 9.1.3, K6.2.12, 6.2.13, NB).
Példák: a Gelfond-Schneider-tétel (FGy9.3.5), e és π irracionális (FGy9.5.1–2), a Liouville-szám transzcendens (FGy9.4.2).
Négy és három négyzetszám-tétel (FGy7.5.2–3, NB).
Két négyzetszám-tétel, a megoldások száma (FGy7.5.1).
A Waring-problémakör (FGy7.6).

A 31. előadás összefoglalása

Fogalmak

Algebrai és transzcendens szám (FGy9.1.1, K5.10.8).
Gauss- és Euler-egészek.

Tételek

Az algebrai számok megszámlálható, algebrailag zárt testet alkotnak (FGy9.3.1, 9.3.6, 9.1.3, K6.2.12, 6.2.13, NB).
Példák: a Gelfond-Schneider-tétel (FGy9.3.5), e és π irracionális (FGy9.5.1–2), a Liouville-szám transzcendens (FGy9.4.2).
Négy és három négyzetszám-tétel (FGy7.5.2–3, NB).
Két négyzetszám-tétel, a megoldások száma (FGy7.5.1).
A Waring-problémakör (FGy7.6).
A Gauss- és Euler-egészek számelmélete (FGy7.4, 7.7).

A 31. előadás összefoglalása

Fogalmak

Algebrai és transzcendens szám (FGy9.1.1, K5.10.8).
Gauss- és Euler-egészek.

Tételek

Az algebrai számok megszámlálható, algebrailag zárt testet alkotnak (FGy9.3.1, 9.3.6, 9.1.3, K6.2.12, 6.2.13, NB).
Példák: a Gelfond-Schneider-tétel (FGy9.3.5), e és π irracionális (FGy9.5.1–2), a Liouville-szám transzcendens (FGy9.4.2).
Négy és három négyzetszám-tétel (FGy7.5.2–3, NB).
Két négyzetszám-tétel, a megoldások száma (FGy7.5.1).
A Waring-problémakör (FGy7.6).
A Gauss- és Euler-egészek számelmélete (FGy7.4, 7.7).
A Fermat-tétel $n = 3$ esetének bizonyítása.