

Algebra és számelmélet

ELTE Algebra és Számelmélet Tanszék

Konzultáció: Kiss Emil

<http://ewkiss.web.elte.hu/wp/wordpress>

ewkiss@gmail.com

12. előadás

Teljes maradékrendszer

Definíció (FGy2.2.2)

Ha $m > 0$ egész, és mindegyik mod m maradékosztályból kivesszünk pontosan 1 számot,

Teljes maradékrendszer

Definíció (FGy2.2.2)

Ha $m > 0$ egész, és mindegyik mod m maradékosztályból kivesszünk pontosan 1 számot, akkor **teljes maradékrendszert** kapunk mod m .

Teljes maradérendszer

Definíció (FGy2.2.2)

Ha $m > 0$ egész, és mindegyik mod m maradékosztályból kivesszünk pontosan 1 számot, akkor **teljes maradérendszert** kapunk mod m .

Például $0, 1, 2, 3$

teljes maradérendszer mod 4 .

Teljes maradérendszer

Definíció (FGy2.2.2)

Ha $m > 0$ egész, és mindegyik mod m maradékosztályból kivesszünk pontosan 1 számot, akkor **teljes maradékrendszert** kapunk mod m .

Például $0, 1, 2, 3$ is, $1, 2, 3, 4$ is,
teljes maradérendszer mod 4 .

Teljes maradékrendszer

Definíció (FGy2.2.2)

Ha $m > 0$ egész, és mindegyik mod m maradékosztályból kivesszünk pontosan 1 számot, akkor **teljes maradékrendszert** kapunk mod m .

Például $0, 1, 2, 3$ is, $1, 2, 3, 4$ is, $-2, -1, 0, 1$ is,
teljes maradékrendszer mod 4 .

Teljes maradékrendszer

Definíció (FGy2.2.2)

Ha $m > 0$ egész, és mindegyik mod m maradékosztályból kivesszünk pontosan 1 számot, akkor **teljes maradékrendszert** kapunk mod m .

Például $0, 1, 2, 3$ is, $1, 2, 3, 4$ is, $-2, -1, 0, 1$ is, $13, 26, 56, 75$ is teljes maradékrendszer mod 4 .

Teljes maradékrendszer

Definíció (FGy2.2.2)

Ha $m > 0$ egész, és mindegyik mod m maradékosztályból kivesszünk pontosan 1 számot, akkor **teljes maradékrendszert** kapunk mod m .

Például $0, 1, 2, 3$ is, $1, 2, 3, 4$ is, $-2, -1, 0, 1$ is, $13, 26, 56, 75$ is teljes maradékrendszer mod 4 .

Tétel (FGy2.2.3)

Adott m szám pontosan akkor alkot teljes maradékrendszert mod m , ha páronként inkongruensek mod m .

Teljes maradékrendszer

Definíció (FGy2.2.2)

Ha $m > 0$ egész, és mindegyik mod m maradékosztályból kivesszünk pontosan 1 számot, akkor **teljes maradékrendszert** kapunk mod m .

Például $0, 1, 2, 3$ is, $1, 2, 3, 4$ is, $-2, -1, 0, 1$ is, $13, 26, 56, 75$ is teljes maradékrendszer mod 4 .

Tétel (FGy2.2.3)

Adott m szám pontosan akkor alkot teljes maradékrendszert mod m , ha páronként inkongruensek mod m .

Valóban, ha páronként inkongruensek, és m darab van,

Teljes maradékrendszer

Definíció (FGy2.2.2)

Ha $m > 0$ egész, és mindegyik mod m maradékosztályból kivesszünk pontosan 1 számot, akkor **teljes maradékrendszert** kapunk mod m .

Például $0, 1, 2, 3$ is, $1, 2, 3, 4$ is, $-2, -1, 0, 1$ is, $13, 26, 56, 75$ is teljes maradékrendszer mod 4 .

Tétel (FGy2.2.3)

Adott m szám pontosan akkor alkot teljes maradékrendszert mod m , ha páronként inkongruensek mod m .

Valóban, ha páronként inkongruensek, és m darab van, akkor minden maradékosztályba kell, hogy jusson.

Teljes maradékrendszer

Definíció (FGy2.2.2)

Ha $m > 0$ egész, és mindegyik mod m maradékosztályból kivesszünk pontosan 1 számot, akkor **teljes maradékrendszert** kapunk mod m .

Például $0, 1, 2, 3$ is, $1, 2, 3, 4$ is, $-2, -1, 0, 1$ is, $13, 26, 56, 75$ is teljes maradékrendszer mod 4 .

Tétel (FGy2.2.3)

Adott m szám pontosan akkor alkot teljes maradékrendszert mod m , ha páronként inkongruensek mod m .

Valóban, ha páronként inkongruensek, és m darab van, akkor minden maradékosztályba kell, hogy jusson.

Illusztráció: Tekintsük a $\cos(2r_j\pi/n) + i\sin(2r_j\pi/n)$ számokat, ahol $r_1, \dots, r_n \in \mathbb{Z}$.

Teljes maradékrendszer

Definíció (FGy2.2.2)

Ha $m > 0$ egész, és mindegyik mod m maradékosztályból kivesszünk pontosan 1 számot, akkor **teljes maradékrendszert** kapunk mod m .

Például $0, 1, 2, 3$ is, $1, 2, 3, 4$ is, $-2, -1, 0, 1$ is, $13, 26, 56, 75$ is teljes maradékrendszer mod 4 .

Tétel (FGy2.2.3)

Adott m szám pontosan akkor alkot teljes maradékrendszert mod m , ha páronként inkongruensek mod m .

Valóban, ha páronként inkongruensek, és m darab van, akkor minden maradékosztályba kell, hogy jusson.

Illusztráció: Tekintsük a $\cos(2r_j\pi/n) + i\sin(2r_j\pi/n)$ számokat, ahol $r_1, \dots, r_n \in \mathbb{Z}$. Ezek pontosan akkor sorolják fel az n -edik egységgyököket,

Teljes maradékrendszer

Definíció (FGy2.2.2)

Ha $m > 0$ egész, és mindegyik mod m maradékosztályból kivesszünk pontosan 1 számot, akkor **teljes maradékrendszert** kapunk mod m .

Például $0, 1, 2, 3$ is, $1, 2, 3, 4$ is, $-2, -1, 0, 1$ is, $13, 26, 56, 75$ is teljes maradékrendszer mod 4 .

Tétel (FGy2.2.3)

Adott m szám pontosan akkor alkot teljes maradékrendszert mod m , ha páronként inkongruensek mod m .

Valóban, ha páronként inkongruensek, és m darab van, akkor minden maradékosztályba kell, hogy jusson.

Illusztráció: Tekintsük a $\cos(2r_j\pi/n) + i\sin(2r_j\pi/n)$ számokat, ahol $r_1, \dots, r_n \in \mathbb{Z}$. Ezek pontosan akkor sorolják fel az n -edik egységgyököket, ha r_1, \dots, r_n teljes maradékrendszer mod n .

Összeadás és szorzás

Tétel (FGy2.2.4)

Legyen r_1, \dots, r_m teljes maradékrendszer mod m .

Összeadás és szorzás

Tétel (FGy2.2.4)

Legyen r_1, \dots, r_m teljes maradékrendszer mod m .

Ha $(a, m) = 1$, és b tetszőleges, akkor $ar_1 + b, \dots, ar_m + b$ is az.

Összeadás és szorzás

Tétel (FGy2.2.4)

Legyen r_1, \dots, r_m teljes maradékkérendszér mod m .

Ha $(a, m) = 1$, és b tetszőleges, akkor $ar_1 + b, \dots, ar_m + b$ is az.

Mivel ez m szám, elég megmutatni, hogy páronként inkongruensek mod m .

Összeadás és szorzás

Tétel (FGy2.2.4)

Legyen r_1, \dots, r_m teljes maradékkérendszér mod m .

Ha $(a, m) = 1$, és b tetszőleges, akkor $ar_1 + b, \dots, ar_m + b$ is az.

Mivel ez m szám, elég megmutatni, hogy páronként inkongruensek mod m . Ez következik abból, hogy minden kongruencia egyszerűsíthető a modulushoz relatív prím számmal. □

Összeadás és szorzás

Tétel (FGy2.2.4)

Legyen r_1, \dots, r_m teljes maradékrendszer mod m .

Ha $(a, m) = 1$, és b tetszőleges, akkor $ar_1 + b, \dots, ar_m + b$ is az.

Mivel ez m szám, elég megmutatni, hogy páronként inkongruensek mod m . Ez következik abból, hogy minden kongruencia egyszerűsíthető a modulushoz relatív prím számmal. \square

Tétel (FGy2.2.5)

Ha $a \equiv b \pmod{m}$, akkor $(a, m) = (b, m)$.

Összeadás és szorzás

Tétel (FGy2.2.4)

Legyen r_1, \dots, r_m teljes maradékkendszer mod m .

Ha $(a, m) = 1$, és b tetszőleges, akkor $ar_1 + b, \dots, ar_m + b$ is az.

Mivel ez m szám, elég megmutatni, hogy páronként inkongruensek mod m . Ez következik abból, hogy minden kongruencia egyszerűsíthető a modulushoz relatív prím számmal. \square

Tétel (FGy2.2.5)

Ha $a \equiv b \pmod{m}$, akkor $(a, m) = (b, m)$. Így ha egy maradékosztály egy eleme relatív prím a modulushoz, akkor mindegyik eleme az.

Összeadás és szorzás

Tétel (FGy2.2.4)

Legyen r_1, \dots, r_m teljes maradékrendszer mod m .

Ha $(a, m) = 1$, és b tetszőleges, akkor $ar_1 + b, \dots, ar_m + b$ is az.

Mivel ez m szám, elég megmutatni, hogy páronként inkongruensek mod m . Ez következik abból, hogy minden kongruencia egyszerűsíthető a modulushoz relatív prím számmal. \square

Tétel (FGy2.2.5)

Ha $a \equiv b \pmod{m}$, akkor $(a, m) = (b, m)$. Így ha egy maradékosztály egy eleme relatív prím a modulushoz, akkor mindegyik eleme az.

A feltétel szerint $b = a + km$ alkalmas k egészre.

Összeadás és szorzás

Tétel (FGy2.2.4)

Legyen r_1, \dots, r_m teljes maradékrendszer mod m .

Ha $(a, m) = 1$, és b tetszőleges, akkor $ar_1 + b, \dots, ar_m + b$ is az.

Mivel ez m szám, elég megmutatni, hogy páronként inkongruensek mod m . Ez következik abból, hogy minden kongruencia egyszerűsíthető a modulushoz relatív prím számmal. \square

Tétel (FGy2.2.5)

Ha $a \equiv b \pmod{m}$, akkor $(a, m) = (b, m)$. Így ha egy maradékosztály egy eleme relatív prím a modulushoz, akkor mindegyik eleme az.

A feltétel szerint $b = a + km$ alkalmas k egészre.

Ezért ha $c \mid m$,

Összeadás és szorzás

Tétel (FGy2.2.4)

Legyen r_1, \dots, r_m teljes maradékrendszer mod m .

Ha $(a, m) = 1$, és b tetszőleges, akkor $ar_1 + b, \dots, ar_m + b$ is az.

Mivel ez m szám, elég megmutatni, hogy páronként inkongruensek mod m . Ez következik abból, hogy minden kongruencia egyszerűsíthető a modulushoz relatív prím számmal. \square

Tétel (FGy2.2.5)

Ha $a \equiv b \pmod{m}$, akkor $(a, m) = (b, m)$. Így ha egy maradékosztály egy eleme relatív prím a modulushoz, akkor mindegyik eleme az.

A feltétel szerint $b = a + km$ alkalmas k egészre.

Ezért ha $c \mid m$, akkor $c \mid a$ akkor és csak akkor, ha $c \mid b = a + km$.

Összeadás és szorzás

Tétel (FGy2.2.4)

Legyen r_1, \dots, r_m teljes maradékrendszer mod m .

Ha $(a, m) = 1$, és b tetszőleges, akkor $ar_1 + b, \dots, ar_m + b$ is az.

Mivel ez m szám, elég megmutatni, hogy páronként inkongruensek mod m . Ez következik abból, hogy minden kongruencia egyszerűsíthető a modulushoz relatív prím számmal. \square

Tétel (FGy2.2.5)

Ha $a \equiv b \pmod{m}$, akkor $(a, m) = (b, m)$. Így ha egy maradékosztály egy eleme relatív prím a modulushoz, akkor mindegyik eleme az.

A feltétel szerint $b = a + km$ alkalmas k egészre.

Ezért ha $c \mid m$, akkor $c \mid a$ akkor és csak akkor, ha $c \mid b = a + km$.

Tehát a és m közös osztói ugyanazok, mint b és m közös osztói. \square

Redukált maradékosztály, Euler-függvény

Definíció (FGy2.2.6)

Egy mod m maradékosztály **redukált**, ha minden eleme relatív prím az m modulushoz.

Redukált maradékosztály, Euler-függvény

Definíció (FGy2.2.6)

Egy mod m maradékosztály **redukált**, ha minden eleme relatív prím az m modulushoz.

Az előző tétel alapján ehhez elég, hogy a maradékosztálynak legyen olyan eleme, ami relatív prím a modulushoz.

Redukált maradékosztály, Euler-függvény

Definíció (FGy2.2.6)

Egy mod m maradékosztály **redukált**, ha minden eleme relatív prím az m moduluszhoz.

Az előző tétel alapján ehhez elég, hogy a maradékosztálynak legyen olyan eleme, ami relatív prím a moduluszhoz.

Definíció (FGy2.2.7)

A $0, 1, 2, \dots, m - 1$ számok közül az m -hez relatív prímelek számát jelölje $\varphi(m)$.

Redukált maradékosztály, Euler-függvény

Definíció (FGy2.2.6)

Egy mod m maradékosztály **redukált**, ha minden eleme relatív prím az m modulushoz.

Az előző tétel alapján ehhez elég, hogy a maradékosztálynak legyen olyan eleme, ami relatív prím a modulushoz.

Definíció (FGy2.2.7)

A $0, 1, 2, \dots, m - 1$ számok közül az m -hez relatív prímelek számát jelölje $\varphi(m)$. Ez az úgynevezett **Euler-függvény**.

Redukált maradékosztály, Euler-függvény

Definíció (FGy2.2.6)

Egy mod m maradékosztály **redukált**, ha minden eleme relatív prím az m modulushoz.

Az előző tétel alapján ehhez elég, hogy a maradékosztálynak legyen olyan eleme, ami relatív prím a modulushoz.

Definíció (FGy2.2.7)

A $0, 1, 2, \dots, m - 1$ számok közül az m -hez relatív prímelek számát jelölje $\varphi(m)$. Ez az úgynevezett **Euler-függvény**.
Tehát $\varphi(m)$ a mod m redukált maradékosztályok száma.

Redukált maradékosztály, Euler-függvény

Definíció (FGy2.2.6)

Egy mod m maradékosztály **redukált**, ha minden eleme relatív prím az m modulushoz.

Az előző tétel alapján ehhez elég, hogy a maradékosztálynak legyen olyan eleme, ami relatív prím a modulushoz.

Definíció (FGy2.2.7)

A $0, 1, 2, \dots, m - 1$ számok közül az m -hez relatív prímelek számát jelölje $\varphi(m)$. Ez az úgynevezett **Euler-függvény**.
Tehát $\varphi(m)$ a mod m redukált maradékosztályok száma.

$\varphi(6) = 2$, mert $0, 1, 2, 3, 4, 5$ közül csak 1 és 5 relatív prím a 6 -hoz.

Redukált maradékosztály, Euler-függvény

Definíció (FGy2.2.6)

Egy mod m maradékosztály **redukált**, ha minden eleme relatív prím az m modulushoz.

Az előző tétel alapján ehhez elég, hogy a maradékosztálynak legyen olyan eleme, ami relatív prím a modulushoz.

Definíció (FGy2.2.7)

A $0, 1, 2, \dots, m - 1$ számok közül az m -hez relatív prímekek számát jelölje $\varphi(m)$. Ez az úgynevezett **Euler-függvény**.

Tehát $\varphi(m)$ a mod m redukált maradékosztályok száma.

$\varphi(6) = 2$, mert $0, 1, 2, 3, 4, 5$ közül csak 1 és 5 relatív prím a 6 -hoz.

$\varphi(10) = 4$, itt $1, 3, 7$ és 9 a megfelelő.

Redukált maradékosztály, Euler-függvény

Definíció (FGy2.2.6)

Egy mod m maradékosztály **redukált**, ha minden eleme relatív prím az m modulushoz.

Az előző tétel alapján ehhez elég, hogy a maradékosztálynak legyen olyan eleme, ami relatív prím a modulushoz.

Definíció (FGy2.2.7)

A $0, 1, 2, \dots, m - 1$ számok közül az m -hez relatív prímekek számát jelölje $\varphi(m)$. Ez az úgynevezett **Euler-függvény**.

Tehát $\varphi(m)$ a mod m redukált maradékosztályok száma.

$\varphi(6) = 2$, mert $0, 1, 2, 3, 4, 5$ közül csak 1 és 5 relatív prím a 6 -hoz.

$\varphi(10) = 4$, itt $1, 3, 7$ és 9 a megfelelő.

$\varphi(25) = 20$, mert csak $0, 5, 10, 15, 20$ **nem** megfelelő.

Redukált maradékosztály, Euler-függvény

Definíció (FGy2.2.6)

Egy mod m maradékosztály **redukált**, ha minden eleme relatív prím az m modulushoz.

Az előző tétel alapján ehhez elég, hogy a maradékosztálynak legyen olyan eleme, ami relatív prím a modulushoz.

Definíció (FGy2.2.7)

A $0, 1, 2, \dots, m - 1$ számok közül az m -hez relatív prímekek számát jelölje $\varphi(m)$. Ez az úgynevezett **Euler-függvény**.

Tehát $\varphi(m)$ a mod m redukált maradékosztályok száma.

$\varphi(6) = 2$, mert $0, 1, 2, 3, 4, 5$ közül csak 1 és 5 relatív prím a 6 -hoz.

$\varphi(10) = 4$, itt $1, 3, 7$ és 9 a megfelelő.

$\varphi(25) = 20$, mert csak $0, 5, 10, 15, 20$ **nem** megfelelő.

HF: Ha p prím, akkor $\varphi(p^n) = p^n - p^{n-1}$.

Az Euler-függvény multiplikatív

Tétel (K, E.4.4)

Ha $(m, n) = 1$, akkor $\varphi(mn) = \varphi(m)\varphi(n)$.

Az Euler-függvény multiplikatív

Tétel (K, E.4.4)

Ha $(m, n) = 1$, akkor $\varphi(mn) = \varphi(m)\varphi(n)$.

Legyenek $a_1, \dots, a_{\varphi(m)}$ a $0, 1, 2, \dots, m-1$ számok közül azok, melyek m -hez relatív prímek,

Az Euler-függvény multiplikatív

Tétel (K, E.4.4)

Ha $(m, n) = 1$, akkor $\varphi(mn) = \varphi(m)\varphi(n)$.

Legyenek $a_1, \dots, a_{\varphi(m)}$ a $0, 1, 2, \dots, m-1$ számok közül azok, melyek m -hez relatív prímek, és $b_1, \dots, b_{\varphi(n)}$ ugyanez n esetén.

Az Euler-függvény multiplikatív

Tétel (K, E.4.4)

Ha $(m, n) = 1$, akkor $\varphi(mn) = \varphi(m)\varphi(n)$.

Legyenek $a_1, \dots, a_{\varphi(m)}$ a $0, 1, 2, \dots, m - 1$ számok közül azok, melyek m -hez relatív prímek, és $b_1, \dots, b_{\varphi(n)}$ ugyanez n esetén. Tekintsük az $\{x \equiv a_i \pmod{m}, x \equiv b_j \pmod{n}\}$ kongruenciarendszert.

Az Euler-függvény multiplikatív

Tétel (K, E.4.4)

Ha $(m, n) = 1$, akkor $\varphi(mn) = \varphi(m)\varphi(n)$.

Legyenek $a_1, \dots, a_{\varphi(m)}$ a $0, 1, 2, \dots, m-1$ számok közül azok, melyek m -hez relatív prímelek, és $b_1, \dots, b_{\varphi(n)}$ ugyanez n esetén. Tekintsük az $\{x \equiv a_i \pmod{m}, x \equiv b_j \pmod{n}\}$ kongruenciarendszert. A kínai maradéktétel miatt ennek egyértelmű megoldása van $0, 1, \dots, mn-1$ között

Az Euler-függvény multiplikatív

Tétel (K, E.4.4)

Ha $(m, n) = 1$, akkor $\varphi(mn) = \varphi(m)\varphi(n)$.

Legyenek $a_1, \dots, a_{\varphi(m)}$ a $0, 1, 2, \dots, m-1$ számok közül azok, melyek m -hez relatív prímek, és $b_1, \dots, b_{\varphi(n)}$ ugyanez n esetén. Tekintsük az $\{x \equiv a_i \pmod{m}, x \equiv b_j \pmod{n}\}$ kongruenciarendszert. A kínai maradéktétel miatt ennek egyértelmű megoldása van $0, 1, \dots, mn-1$ között (hiszen ez teljes maradékrendszer mod mn).

Az Euler-függvény multiplikatív

Tétel (K, E.4.4)

Ha $(m, n) = 1$, akkor $\varphi(mn) = \varphi(m)\varphi(n)$.

Legyenek $a_1, \dots, a_{\varphi(m)}$ a $0, 1, 2, \dots, m-1$ számok közül azok, melyek m -hez relatív prímek, és $b_1, \dots, b_{\varphi(n)}$ ugyanez n esetén. Tekintsük az $\{x \equiv a_i (m), x \equiv b_j (n)\}$ kongruenciarendszert. A kínai maradéktétel miatt ennek egyértelmű megoldása van $0, 1, \dots, mn-1$ között (hiszen ez teljes maradékrendszer mod mn). Ezt a megoldást jelölje $x = f(a_i, b_j)$.

Az Euler-függvény multiplikatív

Tétel (K, E.4.4)

Ha $(m, n) = 1$, akkor $\varphi(mn) = \varphi(m)\varphi(n)$.

Legyenek $a_1, \dots, a_{\varphi(m)}$ a $0, 1, 2, \dots, m-1$ számok közül azok, melyek m -hez relatív prímek, és $b_1, \dots, b_{\varphi(n)}$ ugyanez n esetén. Tekintsük az $\{x \equiv a_i (m), x \equiv b_j (n)\}$ kongruenciarendszert. A kínai maradéktétel miatt ennek egyértelmű megoldása van $0, 1, \dots, mn-1$ között (hiszen ez teljes maradékrendszer mod mn). Ezt a megoldást jelölje $x = f(a_i, b_j)$. Ekkor $(x, mn) = 1$,

Az Euler-függvény multiplikatív

Tétel (K, E.4.4)

Ha $(m, n) = 1$, akkor $\varphi(mn) = \varphi(m)\varphi(n)$.

Legyenek $a_1, \dots, a_{\varphi(m)}$ a $0, 1, 2, \dots, m-1$ számok közül azok, melyek m -hez relatív prímek, és $b_1, \dots, b_{\varphi(n)}$ ugyanez n esetén. Tekintsük az $\{x \equiv a_i (m), x \equiv b_j (n)\}$ kongruenciarendszert. A kínai maradéktétel miatt ennek egyértelmű megoldása van $0, 1, \dots, mn-1$ között (hiszen ez teljes maradékrendszer mod mn). Ezt a megoldást jelölje $x = f(a_i, b_j)$. Ekkor $(x, mn) = 1$, mert ha pl. $p \mid x$ és $p \mid m$ teljesülne egy p prímre,

Az Euler-függvény multiplikatív

Tétel (K, E.4.4)

Ha $(m, n) = 1$, akkor $\varphi(mn) = \varphi(m)\varphi(n)$.

Legyenek $a_1, \dots, a_{\varphi(m)}$ a $0, 1, 2, \dots, m-1$ számok közül azok, melyek m -hez relatív prímek, és $b_1, \dots, b_{\varphi(n)}$ ugyanez n esetén. Tekintsük az $\{x \equiv a_i (m), x \equiv b_j (n)\}$ kongruenciarendszert. A kínai maradéktétel miatt ennek egyértelmű megoldása van $0, 1, \dots, mn-1$ között (hiszen ez teljes maradékrendszer mod mn). Ezt a megoldást jelölje $x = f(a_i, b_j)$. Ekkor $(x, mn) = 1$, mert ha pl. $p \mid x$ és $p \mid m$ teljesülne egy p prímre, akkor $x \equiv a_i (m)$ miatt $p \mid (a_i, m) = 1$ is állna.

Az Euler-függvény multiplikatív

Tétel (K, E.4.4)

Ha $(m, n) = 1$, akkor $\varphi(mn) = \varphi(m)\varphi(n)$.

Legyenek $a_1, \dots, a_{\varphi(m)}$ a $0, 1, 2, \dots, m-1$ számok közül azok, melyek m -hez relatív prímelek, és $b_1, \dots, b_{\varphi(n)}$ ugyanez n esetén. Tekintsük az $\{x \equiv a_i (m), x \equiv b_j (n)\}$ kongruenciarendszert. A kínai maradéktétel miatt ennek egyértelmű megoldása van $0, 1, \dots, mn-1$ között (hiszen ez teljes maradékrendszer mod mn). Ezt a megoldást jelölje $x = f(a_i, b_j)$. Ekkor $(x, mn) = 1$, mert ha pl. $p \mid x$ és $p \mid m$ teljesülne egy p prímmre, akkor $x \equiv a_i (m)$ miatt $p \mid (a_i, m) = 1$ is állna. Az (a_i, b_j) párok száma $\varphi(m)\varphi(n)$,

Az Euler-függvény multiplikatív

Tétel (K, E.4.4)

Ha $(m, n) = 1$, akkor $\varphi(mn) = \varphi(m)\varphi(n)$.

Legyenek $a_1, \dots, a_{\varphi(m)}$ a $0, 1, 2, \dots, m-1$ számok közül azok, melyek m -hez relatív prímelek, és $b_1, \dots, b_{\varphi(n)}$ ugyanez n esetén. Tekintsük az $\{x \equiv a_i (m), x \equiv b_j (n)\}$ kongruenciarendszert. A kínai maradéktétel miatt ennek egyértelmű megoldása van $0, 1, \dots, mn-1$ között (hiszen ez teljes maradékrendszer mod mn). Ezt a megoldást jelölje $x = f(a_i, b_j)$. Ekkor $(x, mn) = 1$, mert ha pl. $p \mid x$ és $p \mid m$ teljesülne egy p prímmre, akkor $x \equiv a_i (m)$ miatt $p \mid (a_i, m) = 1$ is állna. Az (a_i, b_j) párok száma $\varphi(m)\varphi(n)$, így elég belátni, hogy minden mn -hez relatív prím $0 \leq y \leq mn-1$ számot pontosan egyszer kapunk meg $f(a_i, b_j)$ alakban.

Az Euler-függvény multiplikatív

Tétel (K, E.4.4)

Ha $(m, n) = 1$, akkor $\varphi(mn) = \varphi(m)\varphi(n)$.

Legyenek $a_1, \dots, a_{\varphi(m)}$ a $0, 1, 2, \dots, m-1$ számok közül azok, melyek m -hez relatív prímelek, és $b_1, \dots, b_{\varphi(n)}$ ugyanez n esetén. Tekintsük az $\{x \equiv a_i (m), x \equiv b_j (n)\}$ kongruenciarendszert. A kínai maradéktétel miatt ennek egyértelmű megoldása van $0, 1, \dots, mn-1$ között (hiszen ez teljes maradékrendszer mod mn). Ezt a megoldást jelölje $x = f(a_i, b_j)$. Ekkor $(x, mn) = 1$, mert ha pl. $p \mid x$ és $p \mid m$ teljesülne egy p prímmre, akkor $x \equiv a_i (m)$ miatt $p \mid (a_i, m) = 1$ is állna. Az (a_i, b_j) párok száma $\varphi(m)\varphi(n)$, így elég belátni, hogy minden mn -hez relatív prím $0 \leq y \leq mn-1$ számot pontosan egyszer kapunk meg $f(a_i, b_j)$ alakban. Ez nyilvánvaló, a megfelelő a_i az y szám maradéka m -mel osztva

Az Euler-függvény multiplikatív

Tétel (K, E.4.4)

Ha $(m, n) = 1$, akkor $\varphi(mn) = \varphi(m)\varphi(n)$.

Legyenek $a_1, \dots, a_{\varphi(m)}$ a $0, 1, 2, \dots, m-1$ számok közül azok, melyek m -hez relatív prímek, és $b_1, \dots, b_{\varphi(n)}$ ugyanez n esetén. Tekintsük az $\{x \equiv a_i (m), x \equiv b_j (n)\}$ kongruenciarendszert. A kínai maradéktétel miatt ennek egyértelmű megoldása van $0, 1, \dots, mn-1$ között (hiszen ez teljes maradékrendszer mod mn). Ezt a megoldást jelölje $x = f(a_i, b_j)$. Ekkor $(x, mn) = 1$, mert ha pl. $p \mid x$ és $p \mid m$ teljesülne egy p prímmre, akkor $x \equiv a_i (m)$ miatt $p \mid (a_i, m) = 1$ is állna. Az (a_i, b_j) párok száma $\varphi(m)\varphi(n)$, így elég belátni, hogy minden mn -hez relatív prím $0 \leq y \leq mn-1$ számot pontosan egyszer kapunk meg $f(a_i, b_j)$ alakban. Ez nyilvánvaló, a megfelelő a_i az y szám maradéka m -mel osztva (ellenőrizzük, hogy $(a_i, m) = 1$),

Az Euler-függvény multiplikatív

Tétel (K, E.4.4)

Ha $(m, n) = 1$, akkor $\varphi(mn) = \varphi(m)\varphi(n)$.

Legyenek $a_1, \dots, a_{\varphi(m)}$ a $0, 1, 2, \dots, m-1$ számok közül azok, melyek m -hez relatív prímek, és $b_1, \dots, b_{\varphi(n)}$ ugyanez n esetén. Tekintsük az $\{x \equiv a_i (m), x \equiv b_j (n)\}$ kongruenciarendszert. A kínai maradéktétel miatt ennek egyértelmű megoldása van $0, 1, \dots, mn-1$ között (hiszen ez teljes maradékrendszer mod mn). Ezt a megoldást jelölje $x = f(a_i, b_j)$. Ekkor $(x, mn) = 1$, mert ha pl. $p \mid x$ és $p \mid m$ teljesülne egy p prímmre, akkor $x \equiv a_i (m)$ miatt $p \mid (a_i, m) = 1$ is állna. Az (a_i, b_j) párok száma $\varphi(m)\varphi(n)$, így elég belátni, hogy minden mn -hez relatív prím $0 \leq y \leq mn-1$ számot pontosan egyszer kapunk meg $f(a_i, b_j)$ alakban. Ez nyilvánvaló, a megfelelő a_i az y szám maradéka m -mel osztva (ellenőrizzük, hogy $(a_i, m) = 1$), és b_j is hasonlóan kapható. \square

Az Euler-függvény képlete

Illusztráció

Legyen $m = 3$ és $n = 4$,

Az Euler-függvény képlete

Illusztráció

Legyen $m = 3$ és $n = 4$, tehát $a_1 = 1$, $a_2 = 2$,

Az Euler-függvény képlete

Illusztráció

Legyen $m = 3$ és $n = 4$, tehát $a_1 = 1$, $a_2 = 2$, $b_1 = 1$, $b_2 = 3$.

Az Euler-függvény képlete

Illusztráció

Legyen $m = 3$ és $n = 4$, tehát $a_1 = 1$, $a_2 = 2$, $b_1 = 1$, $b_2 = 3$.
Ekkor $f(1, 1) = 1$,

Az Euler-függvény képlete

Illusztráció

Legyen $m = 3$ és $n = 4$, tehát $a_1 = 1$, $a_2 = 2$, $b_1 = 1$, $b_2 = 3$.
Ekkor $f(1, 1) = 1$, $f(1, 3) = 7$,

Az Euler-függvény képlete

Illusztráció

Legyen $m = 3$ és $n = 4$, tehát $a_1 = 1$, $a_2 = 2$, $b_1 = 1$, $b_2 = 3$.
Ekkor $f(1, 1) = 1$, $f(1, 3) = 7$, $f(2, 1) = 5$,

Az Euler-függvény képlete

Illusztráció

Legyen $m = 3$ és $n = 4$, tehát $a_1 = 1$, $a_2 = 2$, $b_1 = 1$, $b_2 = 3$.
Ekkor $f(1, 1) = 1$, $f(1, 3) = 7$, $f(2, 1) = 5$, $f(2, 3) = 11$.

Az Euler-függvény képlete

Illusztráció

Legyen $m = 3$ és $n = 4$, tehát $a_1 = 1$, $a_2 = 2$, $b_1 = 1$, $b_2 = 3$.
Ekkor $f(1, 1) = 1$, $f(1, 3) = 7$, $f(2, 1) = 5$, $f(2, 3) = 11$.

Tétel (FGy2.3.1)

Legyen n kanonikus alakja $p_1^{\alpha_1} \dots p_k^{\alpha_k}$, ahol minden kitevő pozitív.

Az Euler-függvény képlete

Illusztráció

Legyen $m = 3$ és $n = 4$, tehát $a_1 = 1$, $a_2 = 2$, $b_1 = 1$, $b_2 = 3$.
Ekkor $f(1, 1) = 1$, $f(1, 3) = 7$, $f(2, 1) = 5$, $f(2, 3) = 11$.

Tétel (FGy2.3.1)

Legyen n kanonikus alakja $p_1^{\alpha_1} \dots p_k^{\alpha_k}$, ahol minden kitevő pozitív.
Ekkor $\varphi(n) = \prod_{i=1}^k (p_i^{\alpha_i} - p_i^{\alpha_i-1})$

Az Euler-függvény képlete

Illusztráció

Legyen $m = 3$ és $n = 4$, tehát $a_1 = 1$, $a_2 = 2$, $b_1 = 1$, $b_2 = 3$.
Ekkor $f(1, 1) = 1$, $f(1, 3) = 7$, $f(2, 1) = 5$, $f(2, 3) = 11$.

Tétel (FGy2.3.1)

Legyen n kanonikus alakja $p_1^{\alpha_1} \dots p_k^{\alpha_k}$, ahol minden kitevő pozitív.
Ekkor $\varphi(n) = \prod_{i=1}^k (p_i^{\alpha_i} - p_i^{\alpha_i-1}) = n \prod_{i=1}^k (1 - 1/p_i)$.

Az Euler-függvény képlete

Illusztráció

Legyen $m = 3$ és $n = 4$, tehát $a_1 = 1$, $a_2 = 2$, $b_1 = 1$, $b_2 = 3$.
Ekkor $f(1, 1) = 1$, $f(1, 3) = 7$, $f(2, 1) = 5$, $f(2, 3) = 11$.

Tétel (FGy2.3.1)

Legyen n kanonikus alakja $p_1^{\alpha_1} \dots p_k^{\alpha_k}$, ahol minden kitevő pozitív.
Ekkor $\varphi(n) = \prod_{i=1}^k (p_i^{\alpha_i} - p_i^{\alpha_i-1}) = n \prod_{i=1}^k (1 - 1/p_i)$.

Bizonyítás

Mivel $p_i^{\alpha_i}$ páronként relatív prímek, az előző tétel miatt k szerinti indukcióval $\varphi(n) = \prod_{i=1}^k \varphi(p_i^{\alpha_i})$.

Az Euler-függvény képlete

Illusztráció

Legyen $m = 3$ és $n = 4$, tehát $a_1 = 1$, $a_2 = 2$, $b_1 = 1$, $b_2 = 3$.
Ekkor $f(1, 1) = 1$, $f(1, 3) = 7$, $f(2, 1) = 5$, $f(2, 3) = 11$.

Tétel (FGy2.3.1)

Legyen n kanonikus alakja $p_1^{\alpha_1} \dots p_k^{\alpha_k}$, ahol minden kitevő pozitív.
Ekkor $\varphi(n) = \prod_{i=1}^k (p_i^{\alpha_i} - p_i^{\alpha_i-1}) = n \prod_{i=1}^k (1 - 1/p_i)$.

Bizonyítás

Mivel $p_i^{\alpha_i}$ páronként relatív prímek, az előző tétel miatt k szerinti indukcióval $\varphi(n) = \prod_{i=1}^k \varphi(p_i^{\alpha_i})$. Ha p prím, akkor $0, \dots, p^n - 1$ között p -nek p^{n-1} számú többszöröse van,

Az Euler-függvény képlete

Illusztráció

Legyen $m = 3$ és $n = 4$, tehát $a_1 = 1$, $a_2 = 2$, $b_1 = 1$, $b_2 = 3$.
Ekkor $f(1, 1) = 1$, $f(1, 3) = 7$, $f(2, 1) = 5$, $f(2, 3) = 11$.

Tétel (FGy2.3.1)

Legyen n kanonikus alakja $p_1^{\alpha_1} \dots p_k^{\alpha_k}$, ahol minden kitevő pozitív.
Ekkor $\varphi(n) = \prod_{i=1}^k (p_i^{\alpha_i} - p_i^{\alpha_i-1}) = n \prod_{i=1}^k (1 - 1/p_i)$.

Bizonyítás

Mivel $p_i^{\alpha_i}$ páronként relatív prímek, az előző tétel miatt k szerinti indukcióval $\varphi(n) = \prod_{i=1}^k \varphi(p_i^{\alpha_i})$. Ha p prím, akkor $0, \dots, p^n - 1$ között p -nek p^{n-1} számú többszöröse van, a többi szám pedig p^n -hez relatív prím,

Az Euler-függvény képlete

Illusztráció

Legyen $m = 3$ és $n = 4$, tehát $a_1 = 1$, $a_2 = 2$, $b_1 = 1$, $b_2 = 3$.
Ekkor $f(1, 1) = 1$, $f(1, 3) = 7$, $f(2, 1) = 5$, $f(2, 3) = 11$.

Tétel (FGy2.3.1)

Legyen n kanonikus alakja $p_1^{\alpha_1} \dots p_k^{\alpha_k}$, ahol minden kitevő pozitív.
Ekkor $\varphi(n) = \prod_{i=1}^k (p_i^{\alpha_i} - p_i^{\alpha_i-1}) = n \prod_{i=1}^k (1 - 1/p_i)$.

Bizonyítás

Mivel $p_i^{\alpha_i}$ páronként relatív prímek, az előző tétel miatt k szerinti indukcióval $\varphi(n) = \prod_{i=1}^k \varphi(p_i^{\alpha_i})$. Ha p prím, akkor $0, \dots, p^n - 1$ között p -nek p^{n-1} számú többszöröse van, a többi szám pedig p^n -hez relatív prím, így $\varphi(p^n) = p^n - p^{n-1}$. \square

Redukált maradékrendszer

Definíció (FGy2.2.8)

Ha $m > 0$ egész, és mindegyik mod m redukált maradékosztályból kivesszünk pontosan 1 számot, akkor **redukált maradékrendszert** kapunk mod m .

Redukált maradékrendszer

Definíció (FGy2.2.8)

Ha $m > 0$ egész, és mindegyik mod m redukált maradékosztályból kivesszünk pontosan 1 számot, akkor **redukált maradékrendszert** kapunk mod m .

Pl. $1, 5, 7, 11$

redukált maradékrendszer mod 12 .

Redukált maradékrendszer

Definíció (FGy2.2.8)

Ha $m > 0$ egész, és mindegyik mod m redukált maradékosztályból kivesszünk pontosan 1 számot, akkor **redukált maradékrendszert** kapunk mod m .

Pl. $1, 5, 7, 11$ is, $13, 35, 65, 79$ is redukált maradékrendszer mod 12 .

Redukált maradékrendszer

Definíció (FGy2.2.8)

Ha $m > 0$ egész, és mindegyik mod m redukált maradékosztályból kivesszünk pontosan 1 számot, akkor **redukált maradékrendszert** kapunk mod m .

Pl. $1, 5, 7, 11$ is, $13, 35, 65, 79$ is redukált maradékrendszer mod 12 .

Tétel (FGy2.2.9, 2.2.10)

Adott $\varphi(m)$ szám pontosan akkor alkot redukált maradékrendszert mod m ,

Redukált maradékrendszer

Definíció (FGy2.2.8)

Ha $m > 0$ egész, és mindegyik mod m redukált maradékosztályból kivesszünk pontosan 1 számot, akkor **redukált maradékrendszert** kapunk mod m .

Pl. $1, 5, 7, 11$ is, $13, 35, 65, 79$ is redukált maradékrendszer mod 12 .

Tétel (FGy2.2.9, 2.2.10)

Adott $\varphi(m)$ szám pontosan akkor alkot redukált maradékrendszert mod m , ha páronként inkongruensek mod m ,

Redukált maradékrendszer

Definíció (FGy2.2.8)

Ha $m > 0$ egész, és mindegyik mod m redukált maradékosztályból kivesszünk pontosan 1 számot, akkor **redukált maradékrendszert** kapunk mod m .

Pl. $1, 5, 7, 11$ is, $13, 35, 65, 79$ is redukált maradékrendszer mod 12 .

Tétel (FGy2.2.9, 2.2.10)

Adott $\varphi(m)$ szám pontosan akkor alkot redukált maradékrendszert mod m , ha páronként inkongruensek mod m , és mindegyik relatív prím az m modulushoz.

Redukált maradékrendszer

Definíció (FGy2.2.8)

Ha $m > 0$ egész, és mindegyik mod m redukált maradékosztályból kivesszünk pontosan 1 számot, akkor **redukált maradékrendszert** kapunk mod m .

Pl. $1, 5, 7, 11$ is, $13, 35, 65, 79$ is redukált maradékrendszer mod 12 .

Tétel (FGy2.2.9, 2.2.10)

Adott $\varphi(m)$ szám pontosan akkor alkot redukált maradékrendszert mod m , ha páronként inkongruensek mod m , és mindegyik relatív prím az m modulushoz. Legyen $r_1, \dots, r_{\varphi(m)}$ redukált maradékrendszer mod m .

Redukált maradékrendszer

Definíció (FGy2.2.8)

Ha $m > 0$ egész, és mindegyik mod m redukált maradékosztályból kivesszünk pontosan 1 számot, akkor **redukált maradékrendszert** kapunk mod m .

Pl. $1, 5, 7, 11$ is, $13, 35, 65, 79$ is redukált maradékrendszer mod 12 .

Tétel (FGy2.2.9, 2.2.10)

Adott $\varphi(m)$ szám pontosan akkor alkot redukált maradékrendszert mod m , ha páronként inkongruensek mod m , és mindegyik relatív prím az m modulushoz. Legyen $r_1, \dots, r_{\varphi(m)}$ redukált maradékrendszer mod m . Ha $(a, m) = 1$ akkor ar_1, \dots, ar_m is az.

Redukált maradékrendszer

Definíció (FGy2.2.8)

Ha $m > 0$ egész, és mindegyik mod m redukált maradékosztályból kivesszünk pontosan 1 számot, akkor **redukált maradékrendszert** kapunk mod m .

Pl. $1, 5, 7, 11$ is, $13, 35, 65, 79$ is redukált maradékrendszer mod 12 .

Tétel (FGy2.2.9, 2.2.10)

Adott $\varphi(m)$ szám pontosan akkor alkot redukált maradékrendszert mod m , ha páronként inkongruensek mod m , és mindegyik relatív prím az m modulushoz. Legyen $r_1, \dots, r_{\varphi(m)}$ redukált maradékrendszer mod m . Ha $(a, m) = 1$ akkor ar_1, \dots, ar_m is az.

A bizonyítás hasonló a teljes maradékrendszer esetéhez.

Redukált maradékrendszer

Definíció (FGy2.2.8)

Ha $m > 0$ egész, és mindegyik mod m redukált maradékosztályból kivesszünk pontosan 1 számot, akkor **redukált maradékrendszert** kapunk mod m .

Pl. $1, 5, 7, 11$ is, $13, 35, 65, 79$ is redukált maradékrendszer mod 12 .

Tétel (FGy2.2.9, 2.2.10)

Adott $\varphi(m)$ szám pontosan akkor alkot redukált maradékrendszert mod m , ha páronként inkongruensek mod m , és mindegyik relatív prím az m modulushoz. Legyen $r_1, \dots, r_{\varphi(m)}$ redukált maradékrendszer mod m . Ha $(a, m) = 1$ akkor ar_1, \dots, ar_m is az.

A bizonyítás hasonló a teljes maradékrendszer esetéhez.

Azt kell még ellenőrizni, hogy ar_j relatív prím m -hez. □

Az Euler–Fermat-tétel

Euler–Fermat-tétel (FGy 2.4.1)

Ha $(a, m) = 1$, akkor $a^{\varphi(m)} \equiv 1 \pmod{m}$.

Az Euler–Fermat-tétel

Euler–Fermat-tétel (FGy 2.4.1)

Ha $(a, m) = 1$, akkor $a^{\varphi(m)} \equiv 1 \pmod{m}$.

A bizonyításhoz vegyünk egy $r_1, \dots, r_{\varphi(m)}$ redukált maradékrendszert.

Az Euler–Fermat-tétel

Euler–Fermat-tétel (FGy 2.4.1)

Ha $(a, m) = 1$, akkor $a^{\varphi(m)} \equiv 1 \pmod{m}$.

A bizonyításhoz vegyünk egy $r_1, \dots, r_{\varphi(m)}$ redukált maradékrendszert. Az előző tétel szerint $ar_1, \dots, ar_{\varphi(m)}$ is az,

Az Euler–Fermat-tétel

Euler–Fermat-tétel (FGy 2.4.1)

Ha $(a, m) = 1$, akkor $a^{\varphi(m)} \equiv 1 \pmod{m}$.

A bizonyításhoz vegyünk egy $r_1, \dots, r_{\varphi(m)}$ redukált maradékrendszert. Az előző tétel szerint $ar_1, \dots, ar_{\varphi(m)}$ is az, így minden i -hez egyértelműen van olyan j , hogy $ar_i \equiv r_j \pmod{m}$.

Az Euler–Fermat-tétel

Euler–Fermat-tétel (FGy 2.4.1)

Ha $(a, m) = 1$, akkor $a^{\varphi(m)} \equiv 1 \pmod{m}$.

A bizonyításhoz vegyünk egy $r_1, \dots, r_{\varphi(m)}$ redukált maradékrendszert. Az előző tétel szerint $ar_1, \dots, ar_{\varphi(m)}$ is az, így minden i -hez egyértelműen van olyan j , hogy $ar_i \equiv r_j \pmod{m}$. Ha ezt a $\varphi(m)$ kongruenciát összeszorozzuk, akkor mindegyik r_i -vel szabad egyszerűsíteni,

Az Euler–Fermat-tétel

Euler–Fermat-tétel (FGy 2.4.1)

Ha $(a, m) = 1$, akkor $a^{\varphi(m)} \equiv 1 \pmod{m}$.

A bizonyításhoz vegyünk egy $r_1, \dots, r_{\varphi(m)}$ redukált maradékrendszert. Az előző tétel szerint $ar_1, \dots, ar_{\varphi(m)}$ is az, így minden i -hez egyértelműen van olyan j , hogy $ar_i \equiv r_j \pmod{m}$. Ha ezt a $\varphi(m)$ kongruenciát összeszorozzuk, akkor mindegyik r_i -vel szabad egyszerűsíteni, hiszen $(r_i, m) = 1$.

Az Euler–Fermat-tétel

Euler–Fermat-tétel (FGy 2.4.1)

Ha $(a, m) = 1$, akkor $a^{\varphi(m)} \equiv 1 \pmod{m}$.

A bizonyításhoz vegyünk egy $r_1, \dots, r_{\varphi(m)}$ redukált maradékrendszert. Az előző tétel szerint $ar_1, \dots, ar_{\varphi(m)}$ is az, így minden i -hez egyértelműen van olyan j , hogy $ar_i \equiv r_j \pmod{m}$. Ha ezt a $\varphi(m)$ kongruenciát összeszorozzuk, akkor mindegyik r_i -vel szabad egyszerűsíteni, hiszen $(r_i, m) = 1$. A bal oldalon $a^{\varphi(m)}$ marad,

Az Euler–Fermat-tétel

Euler–Fermat-tétel (FGy 2.4.1)

Ha $(a, m) = 1$, akkor $a^{\varphi(m)} \equiv 1 \pmod{m}$.

A bizonyításhoz vegyünk egy $r_1, \dots, r_{\varphi(m)}$ redukált maradékrendszert. Az előző tétel szerint $ar_1, \dots, ar_{\varphi(m)}$ is az, így minden i -hez egyértelműen van olyan j , hogy $ar_i \equiv r_j \pmod{m}$. Ha ezt a $\varphi(m)$ kongruenciát összeszorozzuk, akkor mindegyik r_i -vel szabad egyszerűsíteni, hiszen $(r_i, m) = 1$. A bal oldalon $a^{\varphi(m)}$ marad, a jobb oldalon 1 . □

Az Euler–Fermat-tétel

Euler–Fermat-tétel (FGy 2.4.1)

Ha $(a, m) = 1$, akkor $a^{\varphi(m)} \equiv 1 (m)$.

A bizonyításhoz vegyünk egy $r_1, \dots, r_{\varphi(m)}$ redukált maradékrendszert. Az előző tétel szerint $ar_1, \dots, ar_{\varphi(m)}$ is az, így minden i -hez egyértelműen van olyan j , hogy $ar_i \equiv r_j (m)$. Ha ezt a $\varphi(m)$ kongruenciát összeszorozzuk, akkor mindegyik r_i -vel szabad egyszerűsíteni, hiszen $(r_i, m) = 1$. A bal oldalon $a^{\varphi(m)}$ marad, a jobb oldalon 1. □

Kis Fermat-Tétel (FGy 2.4.2)

Ha p prím, akkor minden a egészre $a^p \equiv a (p)$.

Az Euler–Fermat-tétel

Euler–Fermat-tétel (FGy 2.4.1)

Ha $(a, m) = 1$, akkor $a^{\varphi(m)} \equiv 1 \pmod{m}$.

A bizonyításhoz vegyünk egy $r_1, \dots, r_{\varphi(m)}$ redukált maradékrendszert. Az előző tétel szerint $ar_1, \dots, ar_{\varphi(m)}$ is az, így minden i -hez egyértelműen van olyan j , hogy $ar_i \equiv r_j \pmod{m}$. Ha ezt a $\varphi(m)$ kongruenciát összeszorozzuk, akkor mindegyik r_i -vel szabad egyszerűsíteni, hiszen $(r_i, m) = 1$. A bal oldalon $a^{\varphi(m)}$ marad, a jobb oldalon 1. □

Kis Fermat-Tétel (FGy 2.4.2)

Ha p prím, akkor minden a egészre $a^p \equiv a \pmod{p}$.

Az Euler–Fermat-tétel miatt $a^{p-1} \equiv 1$, ha $(a, p) = 1$,

Az Euler–Fermat-tétel

Euler–Fermat-tétel (FGy 2.4.1)

Ha $(a, m) = 1$, akkor $a^{\varphi(m)} \equiv 1 \pmod{m}$.

A bizonyításhoz vegyünk egy $r_1, \dots, r_{\varphi(m)}$ redukált maradékrendszert. Az előző tétel szerint $ar_1, \dots, ar_{\varphi(m)}$ is az, így minden i -hez egyértelműen van olyan j , hogy $ar_i \equiv r_j \pmod{m}$. Ha ezt a $\varphi(m)$ kongruenciát összeszorozzuk, akkor mindegyik r_i -vel szabad egyszerűsíteni, hiszen $(r_i, m) = 1$. A bal oldalon $a^{\varphi(m)}$ marad, a jobb oldalon 1. □

Kis Fermat-Tétel (FGy 2.4.2)

Ha p prím, akkor minden a egészre $a^p \equiv a \pmod{p}$.

Az Euler–Fermat-tétel miatt $a^{p-1} \equiv 1$, ha $(a, p) = 1$, hiszen $\varphi(p) = p - 1$.

Az Euler–Fermat-tétel

Euler–Fermat-tétel (FGy 2.4.1)

Ha $(a, m) = 1$, akkor $a^{\varphi(m)} \equiv 1 \pmod{m}$.

A bizonyításhoz vegyünk egy $r_1, \dots, r_{\varphi(m)}$ redukált maradékrendszert. Az előző tétel szerint $ar_1, \dots, ar_{\varphi(m)}$ is az, így minden i -hez egyértelműen van olyan j , hogy $ar_i \equiv r_j \pmod{m}$. Ha ezt a $\varphi(m)$ kongruenciát összeszorozzuk, akkor mindegyik r_i -vel szabad egyszerűsíteni, hiszen $(r_i, m) = 1$. A bal oldalon $a^{\varphi(m)}$ marad, a jobb oldalon 1. □

Kis Fermat-Tétel (FGy 2.4.2)

Ha p prím, akkor minden a egészre $a^p \equiv a \pmod{p}$.

Az Euler–Fermat-tétel miatt $a^{p-1} \equiv 1$, ha $(a, p) = 1$, hiszen $\varphi(p) = p - 1$. De ha $(a, p) \neq 1$, akkor $p \mid a$,

Az Euler–Fermat-tétel

Euler–Fermat-tétel (FGy 2.4.1)

Ha $(a, m) = 1$, akkor $a^{\varphi(m)} \equiv 1 (m)$.

A bizonyításhoz vegyünk egy $r_1, \dots, r_{\varphi(m)}$ redukált maradékrendszert. Az előző tétel szerint $ar_1, \dots, ar_{\varphi(m)}$ is az, így minden i -hez egyértelműen van olyan j , hogy $ar_i \equiv r_j (m)$. Ha ezt a $\varphi(m)$ kongruenciát összeszorozzuk, akkor mindegyik r_i -vel szabad egyszerűsíteni, hiszen $(r_i, m) = 1$. A bal oldalon $a^{\varphi(m)}$ marad, a jobb oldalon 1. □

Kis Fermat-Tétel (FGy 2.4.2)

Ha p prím, akkor minden a egészre $a^p \equiv a (p)$.

Az Euler–Fermat-tétel miatt $a^{p-1} \equiv 1$, ha $(a, p) = 1$, hiszen $\varphi(p) = p - 1$. De ha $(a, p) \neq 1$, akkor $p \mid a$, ezért $a^p \equiv a (p)$ ekkor is teljesül. □

Wilson tétele

Ha $ab \equiv 1 \pmod{m}$, akkor a és b egymás **inverzei** mod m .

Wilson tétele

Ha $ab \equiv 1 \pmod{m}$, akkor a és b egymás inverzei mod m .
Ilyenkor $(a, m) = 1$.

Wilson tétele

Ha $ab \equiv 1 \pmod{m}$, akkor a és b egymás **inverzei** mod m .

Ilyenkor $(a, m) = 1$. Ha $(a, m) = 1$, akkor $ax \equiv 1 \pmod{m}$ megoldható.

Wilson tétele

Ha $ab \equiv 1 \pmod{m}$, akkor a és b egymás **inverzei** mod m .

Ilyenkor $(a, m) = 1$. Ha $(a, m) = 1$, akkor $ax \equiv 1 \pmod{m}$ megoldható.

Ezért a invertálható.

Wilson tétele

Ha $ab \equiv 1 \pmod{m}$, akkor a és b egymás **inverzei** mod m .

Ilyenkor $(a, m) = 1$. Ha $(a, m) = 1$, akkor $ax \equiv 1 \pmod{m}$ megoldható.

Ezért a invertálható. Az a inverze is mod m egyértelmű.

Wilson tétele

Ha $ab \equiv 1 \pmod{m}$, akkor a és b egymás **inverzei** mod m .

Ilyenkor $(a, m) = 1$. Ha $(a, m) = 1$, akkor $ax \equiv 1 \pmod{m}$ megoldható.

Ezért a invertálható. Az a inverze is mod m egyértelmű.

Az $ax \equiv b \pmod{m}$ kongruencia megoldható a inverzével való beszorzással is.

Wilson tétele

Ha $ab \equiv 1 \pmod{m}$, akkor a és b egymás **inverzei** mod m .

Ilyenkor $(a, m) = 1$. Ha $(a, m) = 1$, akkor $ax \equiv 1 \pmod{m}$ megoldható.

Ezért a invertálható. Az a inverze is mod m egyértelmű.

Az $ax \equiv b \pmod{m}$ kongruencia megoldható a inverzével való

beszorzással is. Az Euler–Fermat-tétel miatt a inverze $a^{\varphi(m)-1}$.

Wilson tétele

Ha $ab \equiv 1 \pmod{m}$, akkor a és b egymás **inverzei** mod m .

Ilyenkor $(a, m) = 1$. Ha $(a, m) = 1$, akkor $ax \equiv 1 \pmod{m}$ megoldható.

Ezért a invertálható. Az a inverze is mod m egyértelmű.

Az $ax \equiv b \pmod{m}$ kongruencia megoldható a inverzével való beszorzással is. Az Euler–Fermat-tétel miatt a inverze $a^{\varphi(m)-1}$.

Wilson-tétel (FGy2.7.1)

Ha p prím, akkor $(p-1)! \equiv -1 \pmod{p}$.

Wilson tétele

Ha $ab \equiv 1 \pmod{m}$, akkor a és b egymás **inverzei** mod m .

Ilyenkor $(a, m) = 1$. Ha $(a, m) = 1$, akkor $ax \equiv 1 \pmod{m}$ megoldható.

Ezért a invertálható. Az a inverze is mod m egyértelmű.

Az $ax \equiv b \pmod{m}$ kongruencia megoldható a inverzével való beszorzással is. Az Euler–Fermat-tétel miatt a inverze $a^{\varphi(m)-1}$.

Wilson-tétel (FGy2.7.1)

Ha p prím, akkor $(p-1)! \equiv -1 \pmod{p}$.

Párosítsuk $1, 2, \dots, p-1$ mindegyikét a mod p inverzével.

Wilson tétele

Ha $ab \equiv 1 \pmod{m}$, akkor a és b egymás **inverzei** mod m .

Ilyenkor $(a, m) = 1$. Ha $(a, m) = 1$, akkor $ax \equiv 1 \pmod{m}$ megoldható.

Ezért a invertálható. Az a inverze is mod m egyértelmű.

Az $ax \equiv b \pmod{m}$ kongruencia megoldható a inverzével való beszorzással is. Az Euler–Fermat-tétel miatt a inverze $a^{\varphi(m)-1}$.

Wilson-tétel (FGy2.7.1)

Ha p prím, akkor $(p-1)! \equiv -1 \pmod{p}$.

Párosítsuk $1, 2, \dots, p-1$ mindegyikét a mod p inverzével.

E szorzatok értéke 1 mod p ,

Wilson tétele

Ha $ab \equiv 1 \pmod{m}$, akkor a és b egymás **inverzei** mod m .
Ilyenkor $(a, m) = 1$. Ha $(a, m) = 1$, akkor $ax \equiv 1 \pmod{m}$ megoldható.
Ezért a invertálható. Az a inverze is mod m egyértelmű.
Az $ax \equiv b \pmod{m}$ kongruencia megoldható a inverzével való
beszorzással is. Az Euler–Fermat-tétel miatt a inverze $a^{\varphi(m)-1}$.

Wilson-tétel (FGy2.7.1)

Ha p prím, akkor $(p-1)! \equiv -1 \pmod{p}$.

Párosítsuk $1, 2, \dots, p-1$ mindegyikét a mod p inverzével.
E szorzatok értéke $1 \pmod{p}$, tehát az $1 \cdot 2 \cdot \dots \cdot (p-1)$ szorzatban
csak azok a számok maradnak meg, amelyek inverze önmaga.

Wilson tétele

Ha $ab \equiv 1 \pmod{m}$, akkor a és b egymás **inverzei** mod m .
Ilyenkor $(a, m) = 1$. Ha $(a, m) = 1$, akkor $ax \equiv 1 \pmod{m}$ megoldható.
Ezért a invertálható. Az a inverze is mod m egyértelmű.
Az $ax \equiv b \pmod{m}$ kongruencia megoldható a inverzével való beszorzással is. Az Euler–Fermat-tétel miatt a inverze $a^{\varphi(m)-1}$.

Wilson-tétel (FGy2.7.1)

Ha p prím, akkor $(p-1)! \equiv -1 \pmod{p}$.

Párosítsuk $1, 2, \dots, p-1$ mindegyikét a mod p inverzével.
E szorzatok értéke $1 \pmod{p}$, tehát az $1 \cdot 2 \cdot \dots \cdot (p-1)$ szorzatban csak azok a számok maradnak meg, amelyek inverze önmaga.
De ha $a^2 \equiv 1 \pmod{p}$, akkor $p \mid a^2 - 1$

Wilson tétele

Ha $ab \equiv 1 \pmod{m}$, akkor a és b egymás **inverzei** mod m .

Ilyenkor $(a, m) = 1$. Ha $(a, m) = 1$, akkor $ax \equiv 1 \pmod{m}$ megoldható.

Ezért a invertálható. Az a inverze is mod m egyértelmű.

Az $ax \equiv b \pmod{m}$ kongruencia megoldható a inverzével való beszorzással is. Az Euler–Fermat-tétel miatt a inverze $a^{\varphi(m)-1}$.

Wilson-tétel (FGy2.7.1)

Ha p prím, akkor $(p-1)! \equiv -1 \pmod{p}$.

Párosítsuk $1, 2, \dots, p-1$ mindegyikét a mod p inverzével.

E szorzatok értéke $1 \pmod{p}$, tehát az $1 \cdot 2 \cdot \dots \cdot (p-1)$ szorzatban csak azok a számok maradnak meg, amelyek inverze önmaga.

De ha $a^2 \equiv 1 \pmod{p}$, akkor $p \mid a^2 - 1 = (a-1)(a+1)$,

Wilson tétele

Ha $ab \equiv 1 \pmod{m}$, akkor a és b egymás **inverzei** mod m .

Ilyenkor $(a, m) = 1$. Ha $(a, m) = 1$, akkor $ax \equiv 1 \pmod{m}$ megoldható.

Ezért a invertálható. Az a inverze is mod m egyértelmű.

Az $ax \equiv b \pmod{m}$ kongruencia megoldható a inverzével való beszorzással is. Az Euler–Fermat-tétel miatt a inverze $a^{\varphi(m)-1}$.

Wilson-tétel (FGy2.7.1)

Ha p prím, akkor $(p-1)! \equiv -1 \pmod{p}$.

Párosítsuk $1, 2, \dots, p-1$ mindegyikét a mod p inverzével.

E szorzatok értéke $1 \pmod{p}$, tehát az $1 \cdot 2 \cdot \dots \cdot (p-1)$ szorzatban csak azok a számok maradnak meg, amelyek inverze önmaga.

De ha $a^2 \equiv 1 \pmod{p}$, akkor $p \mid a^2 - 1 = (a-1)(a+1)$,
vagyis $a \equiv \pm 1 \pmod{p}$.

Wilson tétele

Ha $ab \equiv 1 \pmod{m}$, akkor a és b egymás **inverzei** mod m .
Ilyenkor $(a, m) = 1$. Ha $(a, m) = 1$, akkor $ax \equiv 1 \pmod{m}$ megoldható.
Ezért a invertálható. Az a inverze is mod m egyértelmű.
Az $ax \equiv b \pmod{m}$ kongruencia megoldható a inverzével való
beszorzással is. Az Euler–Fermat-tétel miatt a inverze $a^{\varphi(m)-1}$.

Wilson-tétel (FGy2.7.1)

Ha p prím, akkor $(p-1)! \equiv -1 \pmod{p}$.

Párosítsuk $1, 2, \dots, p-1$ mindegyikét a mod p inverzével.
E szorzatok értéke 1 mod p , tehát az $1 \cdot 2 \cdot \dots \cdot (p-1)$ szorzatban
csak azok a számok maradnak meg, amelyek inverze önmaga.
De ha $a^2 \equiv 1 \pmod{p}$, akkor $p \mid a^2 - 1 = (a-1)(a+1)$,
vagyis $a \equiv \pm 1 \pmod{p}$. Ezért $(p-1)! \equiv 1 \cdot (p-1) \equiv -1 \pmod{p}$. \square

Wilson tétele

Ha $ab \equiv 1 \pmod{m}$, akkor a és b egymás **inverzei** mod m .
Ilyenkor $(a, m) = 1$. Ha $(a, m) = 1$, akkor $ax \equiv 1 \pmod{m}$ megoldható.
Ezért a invertálható. Az a inverze is mod m egyértelmű.
Az $ax \equiv b \pmod{m}$ kongruencia megoldható a inverzével való
beszorzással is. Az Euler–Fermat-tétel miatt a inverze $a^{\varphi(m)-1}$.

Wilson-tétel (FGy2.7.1)

Ha p prím, akkor $(p-1)! \equiv -1 \pmod{p}$.

Párosítsuk $1, 2, \dots, p-1$ mindegyikét a mod p inverzével.
E szorzatok értéke $1 \pmod{p}$, tehát az $1 \cdot 2 \cdot \dots \cdot (p-1)$ szorzatban
csak azok a számok maradnak meg, amelyek inverze önmaga.
De ha $a^2 \equiv 1 \pmod{p}$, akkor $p \mid a^2 - 1 = (a-1)(a+1)$,
vagyis $a \equiv \pm 1 \pmod{p}$. Ezért $(p-1)! \equiv 1 \cdot (p-1) \equiv -1 \pmod{p}$. \square
Megjegyezzük, hogy $p=2$ esetén $1 = p-1$,

Wilson tétele

Ha $ab \equiv 1 \pmod{m}$, akkor a és b egymás **inverzei** mod m .

Ilyenkor $(a, m) = 1$. Ha $(a, m) = 1$, akkor $ax \equiv 1 \pmod{m}$ megoldható.

Ezért a invertálható. Az a inverze is mod m egyértelmű.

Az $ax \equiv b \pmod{m}$ kongruencia megoldható a inverzével való beszorzással is. Az Euler–Fermat-tétel miatt a inverze $a^{\varphi(m)-1}$.

Wilson-tétel (FGy2.7.1)

Ha p prím, akkor $(p-1)! \equiv -1 \pmod{p}$.

Párosítsuk $1, 2, \dots, p-1$ mindegyikét a mod p inverzével.

E szorzatok értéke $1 \pmod{p}$, tehát az $1 \cdot 2 \cdot \dots \cdot (p-1)$ szorzatban csak azok a számok maradnak meg, amelyek inverze önmaga.

De ha $a^2 \equiv 1 \pmod{p}$, akkor $p \mid a^2 - 1 = (a-1)(a+1)$,

vagyis $a \equiv \pm 1 \pmod{p}$. Ezért $(p-1)! \equiv 1 \cdot (p-1) \equiv -1 \pmod{p}$. \square

Megjegyezzük, hogy $p=2$ esetén $1 = p-1$, de akkor $1 \equiv -1 \pmod{p}$.

Wilson tétele

Ha $ab \equiv 1 \pmod{m}$, akkor a és b egymás **inverzei** mod m .

Ilyenkor $(a, m) = 1$. Ha $(a, m) = 1$, akkor $ax \equiv 1 \pmod{m}$ megoldható.

Ezért a invertálható. Az a inverze is mod m egyértelmű.

Az $ax \equiv b \pmod{m}$ kongruencia megoldható a inverzével való beszorzással is. Az Euler–Fermat-tétel miatt a inverze $a^{\varphi(m)-1}$.

Wilson-tétel (FGy2.7.1)

Ha p prím, akkor $(p-1)! \equiv -1 \pmod{p}$.

Párosítsuk $1, 2, \dots, p-1$ mindegyikét a mod p inverzével.

E szorzatok értéke $1 \pmod{p}$, tehát az $1 \cdot 2 \cdot \dots \cdot (p-1)$ szorzatban csak azok a számok maradnak meg, amelyek inverze önmaga.

De ha $a^2 \equiv 1 \pmod{p}$, akkor $p \mid a^2 - 1 = (a-1)(a+1)$,

vagyis $a \equiv \pm 1 \pmod{p}$. Ezért $(p-1)! \equiv 1 \cdot (p-1) \equiv -1 \pmod{p}$. \square

Megjegyezzük, hogy $p=2$ esetén $1 = p-1$, de akkor $1 \equiv -1 \pmod{p}$.

Wilson tételét levezetjük majd a polinomok azonossági tételéből is.

Teljes hatványok

Állítás (FGy, F1.6.1)

Egy pozitív b egész akkor és csak akkor lesz egy pozitív egész c szám k -adik hatványa,

Teljes hatványok

Állítás (FGy, F1.6.1)

Egy pozitív b egész akkor és csak akkor lesz egy pozitív egész c szám k -adik hatványa, azaz **teljes k -adik hatvány**,

Teljes hatványok

Állítás (FGy, F1.6.1)

Egy pozitív b egész akkor és csak akkor lesz egy pozitív egész c szám k -adik hatványa, azaz **teljes k -adik hatvány**, ha a kanonikus alakjában minden kitevő k -val osztható.

Teljes hatványok

Állítás (FGy, F1.6.1)

Egy pozitív b egész akkor és csak akkor lesz egy pozitív egész c szám k -adik hatványa, azaz **teljes k -adik hatvány**, ha a kanonikus alakjában minden kitevő k -val osztható.

c kanonikus alakját k -adikra emelve a kitevők k -val oszthatók. \square

Teljes hatványok

Állítás (FGy, F1.6.1)

Egy pozitív b egész akkor és csak akkor lesz egy pozitív egész c szám k -adik hatványa, azaz **teljes k -adik hatvány**, ha a kanonikus alakjában minden kitevő k -val osztható.

c kanonikus alakját k -adikra emelve a kitevők k -val oszthatók. \square

Állítás (FGy, F1.6.2)

Két relatív prím pozitív egész szorzata akkor és csak akkor lesz teljes k -adik hatvány,

Teljes hatványok

Állítás (FGy, F1.6.1)

Egy pozitív b egész akkor és csak akkor lesz egy pozitív egész c szám k -adik hatványa, azaz **teljes k -adik hatvány**, ha a kanonikus alakjában minden kitevő k -val osztható.

c kanonikus alakját k -adikra emelve a kitevők k -val oszthatók. \square

Állítás (FGy, F1.6.2)

Két relatív prím pozitív egész szorzata akkor és csak akkor lesz teljes k -adik hatvány, ha mindkét tényező az.

Teljes hatványok

Állítás (FGy, F1.6.1)

Egy pozitív b egész akkor és csak akkor lesz egy pozitív egész c szám k -adik hatványa, azaz **teljes k -adik hatvány**, ha a kanonikus alakjában minden kitevő k -val osztható.

c kanonikus alakját k -adikra emelve a kitevők k -val oszthatók. \square

Állítás (FGy, F1.6.2)

Két relatív prím pozitív egész szorzata akkor és csak akkor lesz teljes k -adik hatvány, ha mindkét tényező az.

Mivel a két szám relatív prím, a kanonikus alakjukban nincs közös prímhatvány.

Teljes hatványok

Állítás (FGy, F1.6.1)

Egy pozitív b egész akkor és csak akkor lesz egy pozitív egész c szám k -adik hatványa, azaz **teljes k -adik hatvány**, ha a kanonikus alakjában minden kitevő k -val osztható.

c kanonikus alakját k -adikra emelve a kitevők k -val oszthatók.

Állítás (FGy, F1.6.2)

Két relatív prím pozitív egész szorzata akkor és csak akkor lesz teljes k -adik hatvány, ha mindkét tényező az.

Mivel a két szám relatív prím, a kanonikus alakjukban nincs közös prímhatalvány. Ezért ha minden kitevő k -val osztható, akkor a két számban külön-külön is k -val oszthatók a kitevők.

Teljes hatványok

Állítás (FGy, F1.6.1)

Egy pozitív b egész akkor és csak akkor lesz egy pozitív egész c szám k -adik hatványa, azaz **teljes k -adik hatvány**, ha a kanonikus alakjában minden kitevő k -val osztható.

c kanonikus alakját k -adikra emelve a kitevők k -val oszthatók.

Állítás (FGy, F1.6.2)

Két relatív prím pozitív egész szorzata akkor és csak akkor lesz teljes k -adik hatvány, ha mindkét tényező az.

Mivel a két szám relatív prím, a kanonikus alakjukban nincs közös prímhatalvány. Ezért ha minden kitevő k -val osztható, akkor a két számban külön-külön is k -val oszthatók a kitevők.

HF: Igazoljuk, hogy ha n egész, és $\sqrt[k]{n}$ racionális,

Teljes hatványok

Állítás (FGy, F1.6.1)

Egy pozitív b egész akkor és csak akkor lesz egy pozitív egész c szám k -adik hatványa, azaz **teljes k -adik hatvány**, ha a kanonikus alakjában minden kitevő k -val osztható.

c kanonikus alakját k -adikra emelve a kitevők k -val oszthatók.

Állítás (FGy, F1.6.2)

Két relatív prím pozitív egész szorzata akkor és csak akkor lesz teljes k -adik hatvány, ha mindkét tényező az.

Mivel a két szám relatív prím, a kanonikus alakjukban nincs közös prímhatalvány. Ezért ha minden kitevő k -val osztható, akkor a két számban külön-külön is k -val oszthatók a kitevők.

HF: Igazoljuk, hogy ha n egész, és $\sqrt[k]{n}$ racionális, akkor n teljes k -adik hatvány.

Teljes hatványok

Állítás (FGy, F1.6.1)

Egy pozitív b egész akkor és csak akkor lesz egy pozitív egész c szám k -adik hatványa, azaz **teljes k -adik hatvány**, ha a kanonikus alakjában minden kitevő k -val osztható.

c kanonikus alakját k -adikra emelve a kitevők k -val oszthatók.

Állítás (FGy, F1.6.2)

Két relatív prím pozitív egész szorzata akkor és csak akkor lesz teljes k -adik hatvány, ha mindkét tényező az.

Mivel a két szám relatív prím, a kanonikus alakjukban nincs közös prímhatalvány. Ezért ha minden kitevő k -val osztható, akkor a két számban külön-külön is k -val oszthatók a kitevők.

HF: Igazoljuk, hogy ha n egész, és $\sqrt[k]{n}$ racionális, akkor n teljes k -adik hatvány. Így például $\sqrt{2}$ irracionális.

Pitagoraszi számhármások

Definíció (FGy7.2)

Az $x^2 + y^2 = z^2$ egyenlet pozitív egész megoldásait
Pitagoraszi számhármásoknak nevezzük.

Pitagoraszi számhármások

Definíció (FGy7.2)

Az $x^2 + y^2 = z^2$ egyenlet pozitív egész megoldásait
Pitagoraszi számhármásoknak nevezzük. Pl. $(3, 4, 5)$.

Pitagoraszi számhármások

Definíció (FGy7.2)

Az $x^2 + y^2 = z^2$ egyenlet pozitív egész megoldásait
Pitagoraszi számhármásoknak nevezzük. Pl. $(3, 4, 5)$.

Ókor: derékszög kimérése csomózott kötelekkel.

Pitagoraszi számhármások

Definíció (FGy7.2)

Az $x^2 + y^2 = z^2$ egyenlet pozitív egész megoldásait
Pitagoraszi számhármásoknak nevezzük. Pl. $(3, 4, 5)$.

Ókor: derékszög kimérése csomózott kötelekkel.

Alapmegoldás: x , y , z páronként relatív prímelek.

Pitagoraszi számhármások

Definíció (FGy7.2)

Az $x^2 + y^2 = z^2$ egyenlet pozitív egész megoldásait
Pitagoraszi számhármásoknak nevezzük. Pl. $(3, 4, 5)$.

Ókor: derékszög kimérése csomózott kötelekkel.

Alapmegoldás: x, y, z páronként relatív prímelek.

Az összes megoldás (dx, dy, dz) alakú, ahol (x, y, z) alapmegoldás.

Pitagoraszi számhármások

Definíció (FGy7.2)

Az $x^2 + y^2 = z^2$ egyenlet pozitív egész megoldásait
Pitagoraszi számhármásoknak nevezzük. Pl. $(3, 4, 5)$.

Ókor: derékszög kimérése csomózott kötelekkel.

Alapmegoldás: x, y, z páronként relatív prímelek.

Az összes megoldás (dx, dy, dz) alakú, ahol (x, y, z) alapmegoldás.

Valóban, ha $x^2 + y^2 = z^2$, és pl. $(y, z) \neq 1$,

Pitagoraszi számhármások

Definíció (FGy7.2)

Az $x^2 + y^2 = z^2$ egyenlet pozitív egész megoldásait
Pitagoraszi számhármásoknak nevezzük. Pl. $(3, 4, 5)$.

Ókor: derékszög kimérése csomózott kötelekkel.

Alapmegoldás: x, y, z páronként relatív prímelek.

Az összes megoldás (dx, dy, dz) alakú, ahol (x, y, z) alapmegoldás.

Valóban, ha $x^2 + y^2 = z^2$, és pl. $(y, z) \neq 1$, akkor van olyan
 p prím, hogy $p \mid y$ és $p \mid z$.

Pitagoraszi számhármások

Definíció (FGy7.2)

Az $x^2 + y^2 = z^2$ egyenlet pozitív egész megoldásait **Pitagoraszi számhármásoknak** nevezzük. Pl. $(3, 4, 5)$.

Ókor: derékszög kimérése csomózott kötelekkel.

Alapmegoldás: x, y, z páronként relatív prímelek.

Az összes megoldás (dx, dy, dz) alakú, ahol (x, y, z) alapmegoldás.

Valóban, ha $x^2 + y^2 = z^2$, és pl. $(y, z) \neq 1$, akkor van olyan p prím, hogy $p \mid y$ és $p \mid z$. De akkor $p \mid x^2 = z^2 - y^2$,

Pitagoraszi számhármások

Definíció (FGy7.2)

Az $x^2 + y^2 = z^2$ egyenlet pozitív egész megoldásait **Pitagoraszi számhármásoknak** nevezzük. Pl. $(3, 4, 5)$.

Ókor: derékszög kimérése csomózott kötelekkel.

Alapmegoldás: x, y, z páronként relatív prímelek.

Az összes megoldás (dx, dy, dz) alakú, ahol (x, y, z) alapmegoldás.

Valóban, ha $x^2 + y^2 = z^2$, és pl. $(y, z) \neq 1$, akkor van olyan p prím, hogy $p \mid y$ és $p \mid z$. De akkor $p \mid x^2 = z^2 - y^2$, és mivel p prím, $p \mid x$.

Pitagoraszi számhármások

Definíció (FGy7.2)

Az $x^2 + y^2 = z^2$ egyenlet pozitív egész megoldásait **Pitagoraszi számhármásoknak** nevezzük. Pl. $(3, 4, 5)$.

Ókor: derékszög kimérése csomózott kötelekkel.

Alapmegoldás: x, y, z páronként relatív prímek.

Az összes megoldás (dx, dy, dz) alakú, ahol (x, y, z) alapmegoldás.

Valóban, ha $x^2 + y^2 = z^2$, és pl. $(y, z) \neq 1$, akkor van olyan

p prím, hogy $p \mid y$ és $p \mid z$. De akkor $p \mid x^2 = z^2 - y^2$,

és mivel p prím, $p \mid x$. Tehát az egyenlet p -vel egyszerűsíthető.

Pitagoraszi számhármások

Definíció (FGy7.2)

Az $x^2 + y^2 = z^2$ egyenlet pozitív egész megoldásait **Pitagoraszi számhármásoknak** nevezzük. Pl. $(3, 4, 5)$.

Ókor: derékszög kimérése csomózott kötelekkel.

Alapmegoldás: x, y, z páronként relatív prímek.

Az összes megoldás (dx, dy, dz) alakú, ahol (x, y, z) alapmegoldás.

Valóban, ha $x^2 + y^2 = z^2$, és pl. $(y, z) \neq 1$, akkor van olyan

p prím, hogy $p \mid y$ és $p \mid z$. De akkor $p \mid x^2 = z^2 - y^2$,

és mivel p prím, $p \mid x$. Tehát az egyenlet p -vel egyszerűsíthető.

Az eljárást folytatjuk addig, amíg alapmegoldást nem kapunk. \square

Pitagoraszi számhármások

Definíció (FGy7.2)

Az $x^2 + y^2 = z^2$ egyenlet pozitív egész megoldásait **Pitagoraszi számhármásoknak** nevezzük. Pl. $(3, 4, 5)$.

Ókor: derékszög kimérése csomózott kötelekkel.

Alapmegoldás: x, y, z páronként relatív prímek.

Az összes megoldás (dx, dy, dz) alakú, ahol (x, y, z) alapmegoldás.

Valóban, ha $x^2 + y^2 = z^2$, és pl. $(y, z) \neq 1$, akkor van olyan

p prím, hogy $p \mid y$ és $p \mid z$. De akkor $p \mid x^2 = z^2 - y^2$,

és mivel p prím, $p \mid x$. Tehát az egyenlet p -vel egyszerűsíthető.

Az eljárást folytatjuk addig, amíg alapmegoldást nem kapunk. \square

Páratlan szám négyzete 4 -gyel osztva 1 -t ad maradékul,

Pitagoraszi számhármások

Definíció (FGy7.2)

Az $x^2 + y^2 = z^2$ egyenlet pozitív egész megoldásait **Pitagoraszi számhármásoknak** nevezzük. Pl. $(3, 4, 5)$.

Ókor: derékszög kimérése csomózott kötelekkel.

Alapmegoldás: x, y, z páronként relatív prímelek.

Az összes megoldás (dx, dy, dz) alakú, ahol (x, y, z) alapmegoldás.

Valóban, ha $x^2 + y^2 = z^2$, és pl. $(y, z) \neq 1$, akkor van olyan

p prím, hogy $p \mid y$ és $p \mid z$. De akkor $p \mid x^2 = z^2 - y^2$,

és mivel p prím, $p \mid x$. Tehát az egyenlet p -vel egyszerűsíthető.

Az eljárást folytatjuk addig, amíg alapmegoldást nem kapunk. \square

Páratlan szám négyzete 4-gyel osztva 1-t ad maradékul, párosé 0-t,

Pitagoraszi számhármások

Definíció (FGy7.2)

Az $x^2 + y^2 = z^2$ egyenlet pozitív egész megoldásait **Pitagoraszi számhármásoknak** nevezzük. Pl. $(3, 4, 5)$.

Ókor: derékszög kimérése csomózott kötelekkel.

Alapmegoldás: x, y, z páronként relatív prímek.

Az összes megoldás (dx, dy, dz) alakú, ahol (x, y, z) alapmegoldás.

Valóban, ha $x^2 + y^2 = z^2$, és pl. $(y, z) \neq 1$, akkor van olyan

p prím, hogy $p \mid y$ és $p \mid z$. De akkor $p \mid x^2 = z^2 - y^2$,

és mivel p prím, $p \mid x$. Tehát az egyenlet p -vel egyszerűsíthető.

Az eljárást folytatjuk addig, amíg alapmegoldást nem kapunk. \square

Páratlan szám négyzete 4 -gyel osztva 1 -t ad maradékul, párosé 0 -t,

mert ha $b \equiv \pm 1 \pmod{4}$,

Pitagoraszi számhármások

Definíció (FGy7.2)

Az $x^2 + y^2 = z^2$ egyenlet pozitív egész megoldásait **Pitagoraszi számhármásoknak** nevezzük. Pl. $(3, 4, 5)$.

Ókor: derékszög kimérése csomózott kötelekkel.

Alapmegoldás: x, y, z páronként relatív prímek.

Az összes megoldás (dx, dy, dz) alakú, ahol (x, y, z) alapmegoldás.

Valóban, ha $x^2 + y^2 = z^2$, és pl. $(y, z) \neq 1$, akkor van olyan

p prím, hogy $p \mid y$ és $p \mid z$. De akkor $p \mid x^2 = z^2 - y^2$,

és mivel p prím, $p \mid x$. Tehát az egyenlet p -vel egyszerűsíthető.

Az eljárást folytatjuk addig, amíg alapmegoldást nem kapunk. \square

Páratlan szám négyzete 4-gyel osztva 1-t ad maradékul, párosé 0-t,

mert ha $b \equiv \pm 1 \pmod{4}$, akkor $b^2 \equiv 1 \pmod{4}$,

Pitagoraszi számhármások

Definíció (FGy7.2)

Az $x^2 + y^2 = z^2$ egyenlet pozitív egész megoldásait **Pitagoraszi számhármásoknak** nevezzük. Pl. $(3, 4, 5)$.

Ókor: derékszög kimérése csomózott kötelekkel.

Alapmegoldás: x, y, z páronként relatív prímek.

Az összes megoldás (dx, dy, dz) alakú, ahol (x, y, z) alapmegoldás.

Valóban, ha $x^2 + y^2 = z^2$, és pl. $(y, z) \neq 1$, akkor van olyan

p prím, hogy $p \mid y$ és $p \mid z$. De akkor $p \mid x^2 = z^2 - y^2$,

és mivel p prím, $p \mid x$. Tehát az egyenlet p -vel egyszerűsíthető.

Az eljárást folytatjuk addig, amíg alapmegoldást nem kapunk. \square

Páratlan szám négyzete 4-gyel osztva 1-t ad maradékul, párosé 0-t,

mert ha $b \equiv \pm 1 \pmod{4}$, akkor $b^2 \equiv 1 \pmod{4}$, ha $2 \mid b$, akkor $4 \mid b^2$.

Pitagoraszi számhármások

Definíció (FGy7.2)

Az $x^2 + y^2 = z^2$ egyenlet pozitív egész megoldásait **Pitagoraszi számhármásoknak** nevezzük. Pl. $(3, 4, 5)$.

Ókor: derékszög kimérése csomózott kötelekkel.

Alapmegoldás: x, y, z páronként relatív prímelek.

Az összes megoldás (dx, dy, dz) alakú, ahol (x, y, z) alapmegoldás.

Valóban, ha $x^2 + y^2 = z^2$, és pl. $(y, z) \neq 1$, akkor van olyan

p prím, hogy $p \mid y$ és $p \mid z$. De akkor $p \mid x^2 = z^2 - y^2$,

és mivel p prím, $p \mid x$. Tehát az egyenlet p -vel egyszerűsíthető.

Az eljárást folytatjuk addig, amíg alapmegoldást nem kapunk. \square

Páratlan szám négyzete 4-gyel osztva 1-t ad maradékul, párosé 0-t,

mert ha $b \equiv \pm 1 \pmod{4}$, akkor $b^2 \equiv 1 \pmod{4}$, ha $2 \mid b$, akkor $4 \mid b^2$.

Ha (x, y, z) alapmegoldás, akkor legfeljebb az egyik szám páros.

Pitagoraszi számhármások

Definíció (FGy7.2)

Az $x^2 + y^2 = z^2$ egyenlet pozitív egész megoldásait **Pitagoraszi számhármásoknak** nevezzük. Pl. $(3, 4, 5)$.

Ókor: derékszög kimérése csomózott kötelekkel.

Alapmegoldás: x, y, z páronként relatív prímek.

Az összes megoldás (dx, dy, dz) alakú, ahol (x, y, z) alapmegoldás.

Valóban, ha $x^2 + y^2 = z^2$, és pl. $(y, z) \neq 1$, akkor van olyan

p prím, hogy $p \mid y$ és $p \mid z$. De akkor $p \mid x^2 = z^2 - y^2$,

és mivel p prím, $p \mid x$. Tehát az egyenlet p -vel egyszerűsíthető.

Az eljárást folytatjuk addig, amíg alapmegoldást nem kapunk. \square

Páratlan szám négyzete 4-gyel osztva 1-t ad maradékul, párosé 0-t, mert ha $b \equiv \pm 1 \pmod{4}$, akkor $b^2 \equiv 1 \pmod{4}$, ha $2 \mid b$, akkor $4 \mid b^2$.

Ha (x, y, z) alapmegoldás, akkor legfeljebb az egyik szám páros.

Ha x, y páratlan, akkor $z^2 = x^2 + y^2 \equiv 1 + 1 = 2 \pmod{4}$, lehetetlen.

Tehát x és y egyike páros, feltehető, hogy ez x , és y , z páratlan.

Tehát x és y egyike páros, feltehető, hogy ez x , és y , z páratlan.
Legyen $a = (z - y)/2$ és $b = (z + y)/2$, ezek tehát egészek,

Tehát x és y egyike páros, feltehető, hogy ez x , és y , z páratlan.
Legyen $a = (z - y)/2$ és $b = (z + y)/2$, ezek tehát egészek, és
 $(x/2)^2 = a \cdot b$.

Tehát x és y egyike páros, feltehető, hogy ez x , és y , z páratlan.
Legyen $a = (z - y)/2$ és $b = (z + y)/2$, ezek tehát egészek, és
 $(x/2)^2 = a \cdot b$. Ha $d \mid a, b$, akkor $d \mid a + b = z$ és $d \mid a - b = y$,

Tehát x és y egyike páros, feltehető, hogy ez x , és y , z páratlan.
Legyen $a = (z - y)/2$ és $b = (z + y)/2$, ezek tehát egészek, és
 $(x/2)^2 = a \cdot b$. Ha $d \mid a, b$, akkor $d \mid a + b = z$ és $d \mid a - b = y$,
azaz $d \mid (y, z) = 1$,

Tehát x és y egyike páros, feltehető, hogy ez x , és y , z páratlan.
Legyen $a = (z - y)/2$ és $b = (z + y)/2$, ezek tehát egészek, és
 $(x/2)^2 = a \cdot b$. Ha $d \mid a, b$, akkor $d \mid a + b = z$ és $d \mid a - b = y$,
azaz $d \mid (y, z) = 1$, ezért beláttuk, hogy $(a, b) = 1$.

Tehát x és y egyike páros, feltehető, hogy ez x , és y , z páratlan.
Legyen $a = (z - y)/2$ és $b = (z + y)/2$, ezek tehát egészek, és
 $(x/2)^2 = a \cdot b$. Ha $d \mid a, b$, akkor $d \mid a + b = z$ és $d \mid a - b = y$,
azaz $d \mid (y, z) = 1$, ezért beláttuk, hogy $(a, b) = 1$. Mivel
 $ab = (x/2)^2$ négyzetszám, és $(a, b) = 1$,

Tehát x és y egyike páros, feltehető, hogy ez x , és y , z páratlan.
Legyen $a = (z - y)/2$ és $b = (z + y)/2$, ezek tehát egészek, és
 $(x/2)^2 = a \cdot b$. Ha $d \mid a, b$, akkor $d \mid a + b = z$ és $d \mid a - b = y$,
azaz $d \mid (y, z) = 1$, ezért beláttuk, hogy $(a, b) = 1$. Mivel
 $ab = (x/2)^2$ négyzetszám, és $(a, b) = 1$, ezért a , b is négyzetszám.

Tehát x és y egyike páros, feltehető, hogy ez x , és y , z páratlan.
Legyen $a = (z - y)/2$ és $b = (z + y)/2$, ezek tehát egészek, és
 $(x/2)^2 = a \cdot b$. Ha $d \mid a, b$, akkor $d \mid a + b = z$ és $d \mid a - b = y$,
azaz $d \mid (y, z) = 1$, ezért beláttuk, hogy $(a, b) = 1$. Mivel
 $ab = (x/2)^2$ négyzetszám, és $(a, b) = 1$, ezért a , b is négyzetszám.
Legyen $a = m^2$ és $b = n^2$.

Tehát x és y egyike páros, feltehető, hogy ez x , és y , z páratlan.
Legyen $a = (z - y)/2$ és $b = (z + y)/2$, ezek tehát egészek, és
 $(x/2)^2 = a \cdot b$. Ha $d \mid a, b$, akkor $d \mid a + b = z$ és $d \mid a - b = y$,
azaz $d \mid (y, z) = 1$, ezért beláttuk, hogy $(a, b) = 1$. Mivel
 $ab = (x/2)^2$ négyzetszám, és $(a, b) = 1$, ezért a, b is négyzetszám.
Legyen $a = m^2$ és $b = n^2$. Ekkor $ab = (x/2)^2$ miatt $x = 2mn$.

Tehát x és y egyike páros, feltehető, hogy ez x , és y , z páratlan.
Legyen $a = (z - y)/2$ és $b = (z + y)/2$, ezek tehát egészek, és
 $(x/2)^2 = a \cdot b$. Ha $d \mid a, b$, akkor $d \mid a + b = z$ és $d \mid a - b = y$,
azaz $d \mid (y, z) = 1$, ezért beláttuk, hogy $(a, b) = 1$. Mivel
 $ab = (x/2)^2$ négyzetszám, és $(a, b) = 1$, ezért a, b is négyzetszám.
Legyen $a = m^2$ és $b = n^2$. Ekkor $ab = (x/2)^2$ miatt $x = 2mn$.

Tétel (FGy7.2.1)

Az $x^2 + y^2 = z^2$ diofantikus egyenlet alapmegoldásai
 $x = 2mn$, $y = m^2 - n^2$, $z = m^2 + n^2$,

Tehát x és y egyike páros, feltehető, hogy ez x , és y , z páratlan.
Legyen $a = (z - y)/2$ és $b = (z + y)/2$, ezek tehát egészek, és $(x/2)^2 = a \cdot b$. Ha $d \mid a, b$, akkor $d \mid a + b = z$ és $d \mid a - b = y$, azaz $d \mid (y, z) = 1$, ezért beláttuk, hogy $(a, b) = 1$. Mivel $ab = (x/2)^2$ négyzetszám, és $(a, b) = 1$, ezért a, b is négyzetszám.
Legyen $a = m^2$ és $b = n^2$. Ekkor $ab = (x/2)^2$ miatt $x = 2mn$.

Tétel (FGy7.2.1)

Az $x^2 + y^2 = z^2$ diofantikus egyenlet alapmegoldásai
 $x = 2mn$, $y = m^2 - n^2$, $z = m^2 + n^2$, ahol $(m, n) = 1$,

Tehát x és y egyike páros, feltehető, hogy ez x , és y , z páratlan.
Legyen $a = (z - y)/2$ és $b = (z + y)/2$, ezek tehát egészek, és $(x/2)^2 = a \cdot b$. Ha $d \mid a, b$, akkor $d \mid a + b = z$ és $d \mid a - b = y$, azaz $d \mid (y, z) = 1$, ezért beláttuk, hogy $(a, b) = 1$. Mivel $ab = (x/2)^2$ négyzetszám, és $(a, b) = 1$, ezért a, b is négyzetszám.
Legyen $a = m^2$ és $b = n^2$. Ekkor $ab = (x/2)^2$ miatt $x = 2mn$.

Tétel (FGy7.2.1)

Az $x^2 + y^2 = z^2$ diofantikus egyenlet alapmegoldásai
 $x = 2mn$, $y = m^2 - n^2$, $z = m^2 + n^2$, ahol $(m, n) = 1$,
 $m > n$,

Tehát x és y egyike páros, feltehető, hogy ez x , és y , z páratlan.
Legyen $a = (z - y)/2$ és $b = (z + y)/2$, ezek tehát egészek, és $(x/2)^2 = a \cdot b$. Ha $d \mid a, b$, akkor $d \mid a + b = z$ és $d \mid a - b = y$, azaz $d \mid (y, z) = 1$, ezért beláttuk, hogy $(a, b) = 1$. Mivel $ab = (x/2)^2$ négyzetszám, és $(a, b) = 1$, ezért a, b is négyzetszám.
Legyen $a = m^2$ és $b = n^2$. Ekkor $ab = (x/2)^2$ miatt $x = 2mn$.

Tétel (FGy7.2.1)

Az $x^2 + y^2 = z^2$ diofantikus egyenlet alapg megoldásai $x = 2mn$, $y = m^2 - n^2$, $z = m^2 + n^2$, ahol $(m, n) = 1$, $m > n$, és m, n közül az egyik páros, a másik páratlan

Tehát x és y egyike páros, feltehető, hogy ez x , és y , z páratlan. Legyen $a = (z - y)/2$ és $b = (z + y)/2$, ezek tehát egészek, és $(x/2)^2 = a \cdot b$. Ha $d \mid a, b$, akkor $d \mid a + b = z$ és $d \mid a - b = y$, azaz $d \mid (y, z) = 1$, ezért beláttuk, hogy $(a, b) = 1$. Mivel $ab = (x/2)^2$ négyzetszám, és $(a, b) = 1$, ezért a, b is négyzetszám. Legyen $a = m^2$ és $b = n^2$. Ekkor $ab = (x/2)^2$ miatt $x = 2mn$.

Tétel (FGy7.2.1)

Az $x^2 + y^2 = z^2$ diofantikus egyenlet alapmegoldásai $x = 2mn$, $y = m^2 - n^2$, $z = m^2 + n^2$, ahol $(m, n) = 1$, $m > n$, és m, n közül az egyik páros, a másik páratlan (továbbá az x és y cseréjével kapott megoldások).

Tehát x és y egyike páros, feltehető, hogy ez x , és y , z páratlan. Legyen $a = (z - y)/2$ és $b = (z + y)/2$, ezek tehát egészek, és $(x/2)^2 = a \cdot b$. Ha $d \mid a, b$, akkor $d \mid a + b = z$ és $d \mid a - b = y$, azaz $d \mid (y, z) = 1$, ezért beláttuk, hogy $(a, b) = 1$. Mivel $ab = (x/2)^2$ négyzetszám, és $(a, b) = 1$, ezért a, b is négyzetszám. Legyen $a = m^2$ és $b = n^2$. Ekkor $ab = (x/2)^2$ miatt $x = 2mn$.

Tétel (FGy7.2.1)

Az $x^2 + y^2 = z^2$ diofantikus egyenlet alapmegoldásai $x = 2mn$, $y = m^2 - n^2$, $z = m^2 + n^2$, ahol $(m, n) = 1$, $m > n$, és m, n közül az egyik páros, a másik páratlan (továbbá az x és y cseréjével kapott megoldások). Az összes megoldás (dx, dy, dz) alakú, ahol (x, y, z) alapmegoldás.

Tehát x és y egyike páros, feltehető, hogy ez x , és y , z páratlan. Legyen $a = (z - y)/2$ és $b = (z + y)/2$, ezek tehát egészek, és $(x/2)^2 = a \cdot b$. Ha $d \mid a, b$, akkor $d \mid a + b = z$ és $d \mid a - b = y$, azaz $d \mid (y, z) = 1$, ezért beláttuk, hogy $(a, b) = 1$. Mivel $ab = (x/2)^2$ négyzetszám, és $(a, b) = 1$, ezért a, b is négyzetszám. Legyen $a = m^2$ és $b = n^2$. Ekkor $ab = (x/2)^2$ miatt $x = 2mn$.

Tétel (FGy7.2.1)

Az $x^2 + y^2 = z^2$ diofantikus egyenlet alapmegoldásai $x = 2mn$, $y = m^2 - n^2$, $z = m^2 + n^2$, ahol $(m, n) = 1$, $m > n$, és m, n közül az egyik páros, a másik páratlan (továbbá az x és y cseréjével kapott megoldások). Az összes megoldás (dx, dy, dz) alakú, ahol (x, y, z) alapmegoldás.

Nyilván $(2mn, m^2 - n^2, m^2 + n^2)$ mindig megoldás, hiszen $(2mn)^2 + (m^2 - n^2)^2 = (m^2 + n^2)^2$ azonosság.

Tehát x és y egyike páros, feltehető, hogy ez x , és y , z páratlan. Legyen $a = (z - y)/2$ és $b = (z + y)/2$, ezek tehát egészek, és $(x/2)^2 = a \cdot b$. Ha $d \mid a, b$, akkor $d \mid a + b = z$ és $d \mid a - b = y$, azaz $d \mid (y, z) = 1$, ezért beláttuk, hogy $(a, b) = 1$. Mivel $ab = (x/2)^2$ négyzetszám, és $(a, b) = 1$, ezért a, b is négyzetszám. Legyen $a = m^2$ és $b = n^2$. Ekkor $ab = (x/2)^2$ miatt $x = 2mn$.

Tétel (FGy7.2.1)

Az $x^2 + y^2 = z^2$ diofantikus egyenlet alapmegoldásai $x = 2mn$, $y = m^2 - n^2$, $z = m^2 + n^2$, ahol $(m, n) = 1$, $m > n$, és m, n közül az egyik páros, a másik páratlan (továbbá az x és y cseréjével kapott megoldások). Az összes megoldás (dx, dy, dz) alakú, ahol (x, y, z) alapmegoldás.

Nyilván $(2mn, m^2 - n^2, m^2 + n^2)$ mindig megoldás, hiszen $(2mn)^2 + (m^2 - n^2)^2 = (m^2 + n^2)^2$ azonosság. Az, hogy m és n eltérő paritású, ahhoz kell, hogy alapmegoldást kapjunk

Tehát x és y egyike páros, feltehető, hogy ez x , és y , z páratlan. Legyen $a = (z - y)/2$ és $b = (z + y)/2$, ezek tehát egészek, és $(x/2)^2 = a \cdot b$. Ha $d \mid a, b$, akkor $d \mid a + b = z$ és $d \mid a - b = y$, azaz $d \mid (y, z) = 1$, ezért beláttuk, hogy $(a, b) = 1$. Mivel $ab = (x/2)^2$ négyzetszám, és $(a, b) = 1$, ezért a, b is négyzetszám. Legyen $a = m^2$ és $b = n^2$. Ekkor $ab = (x/2)^2$ miatt $x = 2mn$.

Tétel (FGy7.2.1)

Az $x^2 + y^2 = z^2$ diofantikus egyenlet alapmegoldásai $x = 2mn$, $y = m^2 - n^2$, $z = m^2 + n^2$, ahol $(m, n) = 1$, $m > n$, és m, n közül az egyik páros, a másik páratlan (továbbá az x és y cseréjével kapott megoldások). Az összes megoldás (dx, dy, dz) alakú, ahol (x, y, z) alapmegoldás.

Nyilván $(2mn, m^2 - n^2, m^2 + n^2)$ mindig megoldás, hiszen $(2mn)^2 + (m^2 - n^2)^2 = (m^2 + n^2)^2$ azonosság. Az, hogy m és n eltérő paritású, ahhoz kell, hogy alapmegoldást kapjunk (különben y és z is páros lenne).

Tehát x és y egyike páros, feltehető, hogy ez x , és y , z páratlan. Legyen $a = (z - y)/2$ és $b = (z + y)/2$, ezek tehát egészek, és $(x/2)^2 = a \cdot b$. Ha $d \mid a, b$, akkor $d \mid a + b = z$ és $d \mid a - b = y$, azaz $d \mid (y, z) = 1$, ezért beláttuk, hogy $(a, b) = 1$. Mivel $ab = (x/2)^2$ négyzetszám, és $(a, b) = 1$, ezért a, b is négyzetszám. Legyen $a = m^2$ és $b = n^2$. Ekkor $ab = (x/2)^2$ miatt $x = 2mn$.

Tétel (FGy7.2.1)

Az $x^2 + y^2 = z^2$ diofantikus egyenlet alapmegoldásai $x = 2mn$, $y = m^2 - n^2$, $z = m^2 + n^2$, ahol $(m, n) = 1$, $m > n$, és m, n közül az egyik páros, a másik páratlan (továbbá az x és y cseréjével kapott megoldások). Az összes megoldás (dx, dy, dz) alakú, ahol (x, y, z) alapmegoldás.

Nyilván $(2mn, m^2 - n^2, m^2 + n^2)$ mindig megoldás, hiszen $(2mn)^2 + (m^2 - n^2)^2 = (m^2 + n^2)^2$ azonosság. Az, hogy m és n eltérő paritású, ahhoz kell, hogy alapmegoldást kapjunk (különben y és z is páros lenne). HF ellenőrizni, hogy x, y, z tényleg relatív prímelek.

A Fermat-sejtés

Fermat-sejtés, Wiles tétele (FGy7.7.1)

Ha $k > 2$, akkor az $x^k + y^k = z^k$ diofantikus egyenlet nem oldható meg pozitív egészekre.

A Fermat-sejtés

Fermat-sejtés, Wiles tétele (FGy7.7.1)

Ha $k > 2$, akkor az $x^k + y^k = z^k$ diofantikus egyenlet nem oldható meg pozitív egészekre.

300 éves probléma volt.

A Fermat-sejtés

Fermat-sejtés, Wiles tétele (FGy7.7.1)

Ha $k > 2$, akkor az $x^k + y^k = z^k$ diofantikus egyenlet nem oldható meg pozitív egészekre.

300 éves probléma volt. Történeti vonatkozások: Fgy 7.7 szakasz.

A Fermat-sejtés

Fermat-sejtés, Wiles tétele (FGy7.7.1)

Ha $k > 2$, akkor az $x^k + y^k = z^k$ diofantikus egyenlet nem oldható meg pozitív egészekre.

300 éves probléma volt. Történeti vonatkozások: FGY 7.7 szakasz.

Ha $k = 4$: létezik elemi bizonyítás pitagoraszai számhármassok felhasználásával (FGy7.7.2).

A Fermat-sejtés

Fermat-sejtés, Wiles tétele (FGy7.7.1)

Ha $k > 2$, akkor az $x^k + y^k = z^k$ diofantikus egyenlet nem oldható meg pozitív egészekre.

300 éves probléma volt. Történeti vonatkozások: FGY 7.7 szakasz.

Ha $k = 4$: létezik elemi bizonyítás pitagoraszi számhármassok felhasználásával (FGy7.7.2).

Ha $k = 3$: a bizonyítás az **Euler-egészek** felhasználásával halad.

A Fermat-sejtés

Fermat-sejtés, Wiles tétele (FGy7.7.1)

Ha $k > 2$, akkor az $x^k + y^k = z^k$ diofantikus egyenlet nem oldható meg pozitív egészekre.

300 éves probléma volt. Történeti vonatkozások: FGY 7.7 szakasz.

Ha $k = 4$: létezik elemi bizonyítás pitagoraszi számhármassok felhasználásával (FGy7.7.2).

Ha $k = 3$: a bizonyítás az **Euler-egészek** felhasználásával halad. Ezek az $a + b\omega$ alakú számok, ahol $\omega = \cos 120^\circ + i \sin 120^\circ$

A Fermat-sejtés

Fermat-sejtés, Wiles tétele (FGy7.7.1)

Ha $k > 2$, akkor az $x^k + y^k = z^k$ diofantikus egyenlet nem oldható meg pozitív egészekre.

300 éves probléma volt. Történeti vonatkozások: FGY 7.7 szakasz.

Ha $k = 4$: létezik elemi bizonyítás pitagoraszi számhármassok felhasználásával (FGy7.7.2).

Ha $k = 3$: a bizonyítás az **Euler-egészek** felhasználásával halad. Ezek az $a + b\omega$ alakú számok, ahol $\omega = \cos 120^\circ + i \sin 120^\circ$ (vagyis egy **primitív** harmadik egységgyök).

A Fermat-sejtés

Fermat-sejtés, Wiles tétele (FGy7.7.1)

Ha $k > 2$, akkor az $x^k + y^k = z^k$ diofantikus egyenlet nem oldható meg pozitív egészekre.

300 éves probléma volt. Történeti vonatkozások: FGY 7.7 szakasz.

Ha $k = 4$: létezik elemi bizonyítás pitagoraszi számhármassok felhasználásával (FGy7.7.2).

Ha $k = 3$: a bizonyítás az **Euler-egészek** felhasználásával halad. Ezek az $a + b\omega$ alakú számok, ahol $\omega = \cos 120^\circ + i \sin 120^\circ$ (vagyis egy **primitív** harmadik egységgyök). Ezek között is belátható a számelmélet alaptétele

A Fermat-sejtés

Fermat-sejtés, Wiles tétele (FGy7.7.1)

Ha $k > 2$, akkor az $x^k + y^k = z^k$ diofantikus egyenlet nem oldható meg pozitív egészekre.

300 éves probléma volt. Történeti vonatkozások: FGY 7.7 szakasz.

Ha $k = 4$: létezik elemi bizonyítás pitagoraszi számhármassok felhasználásával (FGy7.7.2).

Ha $k = 3$: a bizonyítás az **Euler-egészek** felhasználásával halad. Ezek az $a + b\omega$ alakú számok, ahol $\omega = \cos 120^\circ + i \sin 120^\circ$ (vagyis egy **primitív** harmadik egységgyök). Ezek között is belátható a számelmélet alaptétele (**euklideszi gyűrűt** alkotnak).

A Fermat-sejtés

Fermat-sejtés, Wiles tétele (FGy7.7.1)

Ha $k > 2$, akkor az $x^k + y^k = z^k$ diofantikus egyenlet nem oldható meg pozitív egészekre.

300 éves probléma volt. Történeti vonatkozások: FGY 7.7 szakasz.

Ha $k = 4$: létezik elemi bizonyítás pitagoraszi számhármassok felhasználásával (FGy7.7.2).

Ha $k = 3$: a bizonyítás az **Euler-egészek** felhasználásával halad. Ezek az $a + b\omega$ alakú számok, ahol $\omega = \cos 120^\circ + i \sin 120^\circ$ (vagyis egy **primitív** harmadik egységgyök). Ezek között is belátható a számelmélet alaptétele (**euklideszi gyűrűt** alkotnak). (lásd a 31. diasorozatot, illetve FGY7.7.10).

A Fermat-sejtés

Fermat-sejtés, Wiles tétele (FGy7.7.1)

Ha $k > 2$, akkor az $x^k + y^k = z^k$ diofantikus egyenlet nem oldható meg pozitív egészekre.

300 éves probléma volt. Történeti vonatkozások: FGY 7.7 szakasz.

Ha $k = 4$: létezik elemi bizonyítás pitagoraszi számhármassok felhasználásával (FGy7.7.2).

Ha $k = 3$: a bizonyítás az **Euler-egészek** felhasználásával halad. Ezek az $a + b\omega$ alakú számok, ahol $\omega = \cos 120^\circ + i \sin 120^\circ$ (vagyis egy **primitív** harmadik egységgyök). Ezek között is belátható a számelmélet alaptétele (**euklideszi gyűrűt** alkotnak). (lásd a 31. diasorozatot, illetve FGY7.7.10).

Ha $k = ab$, akkor az $(x^a)^b + (y^a)^b = (z^a)^b$ átalakítás miatt van megoldás a b kitevőre is.

A Fermat-sejtés

Fermat-sejtés, Wiles tétele (FGy7.7.1)

Ha $k > 2$, akkor az $x^k + y^k = z^k$ diofantikus egyenlet nem oldható meg pozitív egészekre.

300 éves probléma volt. Történeti vonatkozások: FGY 7.7 szakasz.

Ha $k = 4$: létezik elemi bizonyítás pitagoraszi számhármassok felhasználásával (FGy7.7.2).

Ha $k = 3$: a bizonyítás az **Euler-egészek** felhasználásával halad. Ezek az $a + b\omega$ alakú számok, ahol $\omega = \cos 120^\circ + i \sin 120^\circ$ (vagyis egy **primitív** harmadik egységgyök). Ezek között is belátható a számelmélet alaptétele (**euklideszi gyűrűt** alkotnak). (lásd a 31. diasorozatot, illetve FGY7.7.10).

Ha $k = ab$, akkor az $(x^a)^b + (y^a)^b = (z^a)^b$ átalakítás miatt van megoldás a b kitevőre is. Ebből következik, hogy a sejtést elég akkor belátni, ha $k = 4$ vagy k prím (FGy, F7.7.1).

A 12. előadáshoz tartozó vizsgaanyag

Fogalmak

Teljes és redukált maradékrendszer (FGy2.2.2, 2.2.8).

A 12. előadáshoz tartozó vizsgaanyag

Fogalmak

Teljes és redukált maradékrendszer (FGy2.2.2, 2.2.8).

Redukált maradékosztály (FGy2.2.5, 2.2.6).

A 12. előadáshoz tartozó vizsgaanyag

Fogalmak

Teljes és redukált maradékrendszer (FGy2.2.2, 2.2.8).

Redukált maradékosztály (FGy2.2.5, 2.2.6).

Euler-függvény (FGy2.2.7).

A 12. előadáshoz tartozó vizsgaanyag

Fogalmak

Teljes és redukált maradékrendszer (FGy2.2.2, 2.2.8).

Redukált maradékosztály (FGy2.2.5, 2.2.6).

Euler-függvény (FGy2.2.7). Pitagoraszai számhármások,
alpmegoldás (FGy7.2).

A 12. előadáshoz tartozó vizsgaanyag

Fogalmak

Teljes és redukált maradékrendszer (FGy2.2.2, 2.2.8).

Redukált maradékosztály (FGy2.2.5, 2.2.6).

Euler-függvény (FGy2.2.7). Pitagoraszai számhármások,

alapmegoldás (FGy7.2). A Fermat-sejtés (Wiles tétele, Fgy7.7.1).

A 12. előadáshoz tartozó vizsgaanyag

Fogalmak

Teljes és redukált maradékrendszer (FGy2.2.2, 2.2.8).

Redukált maradékosztály (FGy2.2.5, 2.2.6).

Euler-függvény (FGy2.2.7). Pitagoraszai számhármások, alamp megoldás (FGy7.2). A Fermat-sejtés (Wiles tétele, FGY7.7.1).

Tételek

Teljes és redukált maradékrendszer jellemzése (FGy2.2.3, 2.2.9),

A 12. előadáshoz tartozó vizsgaanyag

Fogalmak

Teljes és redukált maradékrendszer (FGy2.2.2, 2.2.8).

Redukált maradékosztály (FGy2.2.5, 2.2.6).

Euler-függvény (FGy2.2.7). Pitagoraszai számhármások,

alapmegoldás (FGy7.2). A Fermat-sejtés (Wiles tétele, FGY7.7.1).

Tételek

Teljes és redukált maradékrendszer jellemzése (FGy2.2.3, 2.2.9), szorzása a modulushoz relatív prímmel (FGy2.2.4, 2.2.10).

A 12. előadáshoz tartozó vizsgaanyag

Fogalmak

Teljes és redukált maradékrendszer (FGy2.2.2, 2.2.8).

Redukált maradékosztály (FGy2.2.5, 2.2.6).

Euler-függvény (FGy2.2.7). Pitagoraszai számhármások,

alapmegoldás (FGy7.2). A Fermat-sejtés (Wiles tétele, FGY7.7.1).

Tételek

Teljes és redukált maradékrendszer jellemzése (FGy2.2.3, 2.2.9),

szorzása a modulushoz relatív prímmel (FGy2.2.4, 2.2.10).

Az Euler-függvény multiplikatív, képlete (K , E4.4, FGY2.3.1).

A 12. előadáshoz tartozó vizsgaanyag

Fogalmak

Teljes és redukált maradékrendszer (FGy2.2.2, 2.2.8).

Redukált maradékosztály (FGy2.2.5, 2.2.6).

Euler-függvény (FGy2.2.7). Pitagoraszai számhármások,

alapmegoldás (FGy7.2). A Fermat-sejtés (Wiles tétele, FGY7.7.1).

Tételek

Teljes és redukált maradékrendszer jellemzése (FGy2.2.3, 2.2.9), szorzása a modulushoz relatív prímmel (FGy2.2.4, 2.2.10).

Az Euler-függvény multiplikatív, képlete (K , E4.4, FGY2.3.1).

Euler–Fermat-tétel, kis Fermat-tétel (FGy2.4.1, 2.4.2).

A 12. előadáshoz tartozó vizsgaanyag

Fogalmak

Teljes és redukált maradékrendszer (FGy2.2.2, 2.2.8).

Redukált maradékosztály (FGy2.2.5, 2.2.6).

Euler-függvény (FGy2.2.7). Pitagoraszai számhármások,

alapmegoldás (FGy7.2). A Fermat-sejtés (Wiles tétele, FGY7.7.1).

Tételek

Teljes és redukált maradékrendszer jellemzése (FGy2.2.3, 2.2.9), szorzása a modulushoz relatív prímmel (FGy2.2.4, 2.2.10).

Az Euler-függvény multiplikatív, képlete (K , E4.4, FGY2.3.1).

Euler–Fermat-tétel, kis Fermat-tétel (FGy2.4.1, 2.4.2).

Wilson tétele (FGy2.7.1).

A 12. előadáshoz tartozó vizsgaanyag

Fogalmak

Teljes és redukált maradékrendszer (FGy2.2.2, 2.2.8).

Redukált maradékosztály (FGy2.2.5, 2.2.6).

Euler-függvény (FGy2.2.7). Pitagoraszai számhármások,

alapmegoldás (FGy7.2). A Fermat-sejtés (Wiles tétele, Fgy7.7.1).

Tételek

Teljes és redukált maradékrendszer jellemzése (FGy2.2.3, 2.2.9), szorzása a modulushoz relatív prímmel (FGy2.2.4, 2.2.10).

Az Euler-függvény multiplikatív, képlete (K , E4.4, Fgy2.3.1).

Euler–Fermat-tétel, kis Fermat-tétel (FGy2.4.1, 2.4.2).

Wilson tétele (FGy2.7.1). Teljes hatványok,

relatív prímekek szorzata mikor teljes hatvány (FGy, F1.6.1–2).

A 12. előadáshoz tartozó vizsgaanyag

Fogalmak

Teljes és redukált maradékrendszer (FGy2.2.2, 2.2.8).

Redukált maradékosztály (FGy2.2.5, 2.2.6).

Euler-függvény (FGy2.2.7). Pitagoraszai számhármások,

alapmegoldás (FGy7.2). A Fermat-sejtés (Wiles tétele, Fgy7.7.1).

Tételek

Teljes és redukált maradékrendszer jellemzése (FGy2.2.3, 2.2.9), szorzása a modulushoz relatív prímmel (FGy2.2.4, 2.2.10).

Az Euler-függvény multiplikatív, képlete (K , E4.4, Fgy2.3.1).

Euler–Fermat-tétel, kis Fermat-tétel (FGy2.4.1, 2.4.2).

Wilson tétele (FGy2.7.1). Teljes hatványok,

relatív prímekek szorzata mikor teljes hatvány (FGy, F1.6.1–2).

Képlet a pitagoraszai számhármásokra (FGy7.2.1).