

Algebra és számelmélet

ELTE Algebra és Számelmélet Tanszék

Konzultáció: Kiss Emil

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

ewkiss@gmail.com

11. előadás

A kongruencia definíciója

Definíció (FGy2.1.1)

Legyen $m \geq 1$ egész. Azt mondjuk, hogy $a, b \in \mathbb{Z}$ **kongruens mod m** , ha $m \mid a - b$.

A kongruencia definíciója

Definíció (FGy2.1.1)

Legyen $m \geq 1$ egész. Azt mondjuk, hogy $a, b \in \mathbb{Z}$ **kongruens mod m** , ha $m \mid a - b$. Jele: $a \equiv b (m)$.

A kongruencia definíciója

Definíció (FGy2.1.1)

Legyen $m \geq 1$ egész. Azt mondjuk, hogy $a, b \in \mathbb{Z}$ **kongruens mod m** , ha $m \mid a - b$. Jele: $a \equiv b (m)$.

Tehát két szám akkor kongruens, ha ugyanazt a maradékot adják m -mel osztva.

A kongruencia definíciója

Definíció (FGy2.1.1)

Legyen $m \geq 1$ egész. Azt mondjuk, hogy $a, b \in \mathbb{Z}$ **kongruens mod m** , ha $m \mid a - b$. Jele: $a \equiv b (m)$.

Tehát két szám akkor kongruens, ha ugyanazt a maradékot adják m -mel osztva. Az m neve **modulus**.

A kongruencia definíciója

Definíció (FGy2.1.1)

Legyen $m \geq 1$ egész. Azt mondjuk, hogy $a, b \in \mathbb{Z}$ **kongruens mod m** , ha $m \mid a - b$. Jele: $a \equiv b (m)$.

Tehát két szám akkor kongruens, ha ugyanazt a maradékot adják m -mel osztva. Az m neve **modulus**. A jelölés az egyenletre hasonlít, mert sok tulajdonság megegyezik.

A kongruencia definíciója

Definíció (FGy2.1.1)

Legyen $m \geq 1$ egész. Azt mondjuk, hogy $a, b \in \mathbb{Z}$ **kongruens mod m** , ha $m \mid a - b$. Jele: $a \equiv b (m)$.

Tehát két szám akkor kongruens, ha ugyanazt a maradékot adják m -mel osztva. Az m neve **modulus**. A jelölés az egyenletre hasonlít, mert sok tulajdonság megegyezik.

Tétel (FGy2.1.2, HF)

Legyenek $m > 1$ és a, b, c egészek.

(1) Minden a -ra $a \equiv a (m)$ (**reflexivitás**).

A kongruencia definíciója

Definíció (FGy2.1.1)

Legyen $m \geq 1$ egész. Azt mondjuk, hogy $a, b \in \mathbb{Z}$ **kongruens mod m** , ha $m \mid a - b$. Jele: $a \equiv b (m)$.

Tehát két szám akkor kongruens, ha ugyanazt a maradékot adják m -mel osztva. Az m neve **modulus**. A jelölés az egyenletre hasonlít, mert sok tulajdonság megegyezik.

Tétel (FGy2.1.2, HF)

Legyenek $m > 1$ és a, b, c egészek.

- (1) Minden a -ra $a \equiv a (m)$ (**reflexivitás**).
- (2) Ha $a \equiv b (m)$, akkor $b \equiv a (m)$ (**szimmetria**).

A kongruencia definíciója

Definíció (FGy2.1.1)

Legyen $m \geq 1$ egész. Azt mondjuk, hogy $a, b \in \mathbb{Z}$ **kongruens mod m** , ha $m \mid a - b$. Jele: $a \equiv b (m)$.

Tehát két szám akkor kongruens, ha ugyanazt a maradékot adják m -mel osztva. Az m neve **modulus**. A jelölés az egyenletre hasonlít, mert sok tulajdonság megegyezik.

Tétel (FGy2.1.2, HF)

Legyenek $m > 1$ és a, b, c egészek.

- (1) Minden a -ra $a \equiv a (m)$ (**reflexivitás**).
- (2) Ha $a \equiv b (m)$, akkor $b \equiv a (m)$ (**szimmetria**).
- (3) Ha $a \equiv b (m)$ és $b \equiv c (m)$, akkor $a \equiv c (m)$ (**tranzitivitás**).

A kongruencia definíciója

Definíció (FGy2.1.1)

Legyen $m \geq 1$ egész. Azt mondjuk, hogy $a, b \in \mathbb{Z}$ **kongruens mod m** , ha $m \mid a - b$. Jele: $a \equiv b (m)$.

Tehát két szám akkor kongruens, ha ugyanazt a maradékot adják m -mel osztva. Az m neve **modulus**. A jelölés az egyenletre hasonlít, mert sok tulajdonság megegyezik.

Tétel (FGy2.1.2, HF)

Legyenek $m > 1$ és a, b, c egészek.

- (1) Minden a -ra $a \equiv a (m)$ (**reflexivitás**).
- (2) Ha $a \equiv b (m)$, akkor $b \equiv a (m)$ (**szimmetria**).
- (3) Ha $a \equiv b (m)$ és $b \equiv c (m)$, akkor $a \equiv c (m)$ (**tranzitivitás**).

E három tulajdonság együttes neve: **ekvivalencia-reláció**.

Kongruenciák és műveletek

Tétel (FGy2.1.2)

Legyenek $m > 1$ és a, b, c, d egészek. Ha $a \equiv b (m)$ és $c \equiv d (m)$,

Kongruenciák és műveletek

Tétel (FGy2.1.2)

Legyenek $m > 1$ és a, b, c, d egészek. Ha $a \equiv b (m)$ és $c \equiv d (m)$, akkor $a + c \equiv b + d (m)$

Kongruenciák és műveletek

Tétel (FGy2.1.2)

Legyenek $m > 1$ és a, b, c, d egészek. Ha $a \equiv b (m)$ és $c \equiv d (m)$, akkor $a + c \equiv b + d (m)$ és $ac \equiv bd (m)$.

Kongruenciák és műveletek

Tétel (FGy2.1.2)

Legyenek $m > 1$ és a, b, c, d egészek. Ha $a \equiv b (m)$ és $c \equiv d (m)$, akkor $a + c \equiv b + d (m)$ és $ac \equiv bd (m)$.

(Azonos modulusú kongruenciák összeadhatók, összeszorozhatók.)

Kongruenciák és műveletek

Tétel (FGy2.1.2)

Legyenek $m > 1$ és a, b, c, d egészek. Ha $a \equiv b (m)$ és $c \equiv d (m)$, akkor $a + c \equiv b + d (m)$ és $ac \equiv bd (m)$.

(Azonos modulusú kongruenciák összeadhatók, összeszorozhatók.)

A feltétel szerint $a - b = mt$ és $c - d = ms$ alkalmas $t, s \in \mathbb{Z}$ -re.

Kongruenciák és műveletek

Tétel (FGy2.1.2)

Legyenek $m > 1$ és a, b, c, d egészek. Ha $a \equiv b \pmod{m}$ és $c \equiv d \pmod{m}$, akkor $a + c \equiv b + d \pmod{m}$ és $ac \equiv bd \pmod{m}$.

(Azonos modulusú kongruenciák összeadhatók, összeszorozhatók.)

A feltétel szerint $a - b = mt$ és $c - d = ms$ alkalmas $t, s \in \mathbb{Z}$ -re. Ezért $(a + c) - (b + d) = m(t + s)$,

Kongruenciák és műveletek

Tétel (FGy2.1.2)

Legyenek $m > 1$ és a, b, c, d egészek. Ha $a \equiv b (m)$ és $c \equiv d (m)$, akkor $a + c \equiv b + d (m)$ és $ac \equiv bd (m)$.

(Azonos modulusú kongruenciák összeadhatók, összeszorozhatók.)

A feltétel szerint $a - b = mt$ és $c - d = ms$ alkalmas $t, s \in \mathbb{Z}$ -re.

Ezért $(a + c) - (b + d) = m(t + s)$, így tényleg $a + c \equiv b + d (m)$.

Kongruenciák és műveletek

Tétel (FGy2.1.2)

Legyenek $m > 1$ és a, b, c, d egészek. Ha $a \equiv b (m)$ és $c \equiv d (m)$, akkor $a + c \equiv b + d (m)$ és $ac \equiv bd (m)$.

(Azonos modulusú kongruenciák összeadhatók, összeszorozhatók.)

A feltétel szerint $a - b = mt$ és $c - d = ms$ alkalmas $t, s \in \mathbb{Z}$ -re.

Ezért $(a + c) - (b + d) = m(t + s)$, így tényleg $a + c \equiv b + d (m)$.

Továbbá $m \mid a - b$ miatt $m \mid (a - b)c$,

Kongruenciák és műveletek

Tétel (FGy2.1.2)

Legyenek $m > 1$ és a, b, c, d egészek. Ha $a \equiv b (m)$ és $c \equiv d (m)$, akkor $a + c \equiv b + d (m)$ és $ac \equiv bd (m)$.

(Azonos modulusú kongruenciák összeadhatók, összeszorozhatók.)

A feltétel szerint $a - b = mt$ és $c - d = ms$ alkalmas $t, s \in \mathbb{Z}$ -re.

Ezért $(a + c) - (b + d) = m(t + s)$, így tényleg $a + c \equiv b + d (m)$.

Továbbá $m \mid a - b$ miatt $m \mid (a - b)c$, tehát $ac \equiv bc (m)$.

Kongruenciák és műveletek

Tétel (FGy2.1.2)

Legyenek $m > 1$ és a, b, c, d egészek. Ha $a \equiv b (m)$ és $c \equiv d (m)$, akkor $a + c \equiv b + d (m)$ és $ac \equiv bd (m)$.

(Azonos modulusú kongruenciák összeadhatók, összeszorozhatók.)

A feltétel szerint $a - b = mt$ és $c - d = ms$ alkalmas $t, s \in \mathbb{Z}$ -re.

Ezért $(a + c) - (b + d) = m(t + s)$, így tényleg $a + c \equiv b + d (m)$.

Továbbá $m \mid a - b$ miatt $m \mid (a - b)c$, tehát $ac \equiv bc (m)$.

Hasonlóan $bc \equiv bd (m)$,

Kongruenciák és műveletek

Tétel (FGy2.1.2)

Legyenek $m > 1$ és a, b, c, d egészek. Ha $a \equiv b \pmod{m}$ és $c \equiv d \pmod{m}$, akkor $a + c \equiv b + d \pmod{m}$ és $ac \equiv bd \pmod{m}$.

(Azonos modulusú kongruenciák összeadhatók, összeszorozhatók.)

A feltétel szerint $a - b = mt$ és $c - d = ms$ alkalmas $t, s \in \mathbb{Z}$ -re.

Ezért $(a + c) - (b + d) = m(t + s)$, így tényleg $a + c \equiv b + d \pmod{m}$.

Továbbá $m \mid a - b$ miatt $m \mid (a - b)c$, tehát $ac \equiv bc \pmod{m}$.

Hasonlóan $bc \equiv bd \pmod{m}$, és a tranzitivitás miatt $ac \equiv bd \pmod{m}$. \square

Kongruenciák és műveletek

Tétel (FGy2.1.2)

Legyenek $m > 1$ és a, b, c, d egészek. Ha $a \equiv b \pmod{m}$ és $c \equiv d \pmod{m}$, akkor $a + c \equiv b + d \pmod{m}$ és $ac \equiv bd \pmod{m}$.

(Azonos modulusú kongruenciák összeadhatók, összeszorozhatók.)

A feltétel szerint $a - b = mt$ és $c - d = ms$ alkalmas $t, s \in \mathbb{Z}$ -re.

Ezért $(a + c) - (b + d) = m(t + s)$, így tényleg $a + c \equiv b + d \pmod{m}$.

Továbbá $m \mid a - b$ miatt $m \mid (a - b)c$, tehát $ac \equiv bc \pmod{m}$.

Hasonlóan $bc \equiv bd \pmod{m}$, és a tranzitivitás miatt $ac \equiv bd \pmod{m}$. \square

Belátjuk: $\overline{x + y} = \bar{x} +_n \bar{y}$

Kongruenciák és műveletek

Tétel (FGy2.1.2)

Legyenek $m > 1$ és a, b, c, d egészek. Ha $a \equiv b \pmod{m}$ és $c \equiv d \pmod{m}$, akkor $a + c \equiv b + d \pmod{m}$ és $ac \equiv bd \pmod{m}$.

(Azonos modulusú kongruenciák összeadhatók, összeszorozhatók.)

A feltétel szerint $a - b = mt$ és $c - d = ms$ alkalmas $t, s \in \mathbb{Z}$ -re.

Ezért $(a + c) - (b + d) = m(t + s)$, így tényleg $a + c \equiv b + d \pmod{m}$.

Továbbá $m \mid a - b$ miatt $m \mid (a - b)c$, tehát $ac \equiv bc \pmod{m}$.

Hasonlóan $bc \equiv bd \pmod{m}$, és a tranzitivitás miatt $ac \equiv bd \pmod{m}$. \square

Belátjuk: $\overline{x + y} = \overline{x} +_n \overline{y}$ (az $\overline{xy} = \overline{x} *_n \overline{y}$ bizonyítása hasonló).

Kongruenciák és műveletek

Tétel (FGy2.1.2)

Legyenek $m > 1$ és a, b, c, d egészek. Ha $a \equiv b \pmod{m}$ és $c \equiv d \pmod{m}$, akkor $a + c \equiv b + d \pmod{m}$ és $ac \equiv bd \pmod{m}$.

(Azonos modulusú kongruenciák összeadhatók, összeszorozhatók.)

A feltétel szerint $a - b = mt$ és $c - d = ms$ alkalmas $t, s \in \mathbb{Z}$ -re.

Ezért $(a + c) - (b + d) = m(t + s)$, így tényleg $a + c \equiv b + d \pmod{m}$.

Továbbá $m \mid a - b$ miatt $m \mid (a - b)c$, tehát $ac \equiv bc \pmod{m}$.

Hasonlóan $bc \equiv bd \pmod{m}$, és a tranzitivitás miatt $ac \equiv bd \pmod{m}$. \square

Belátjuk: $\overline{x + y} = \overline{x} +_n \overline{y}$ (az $\overline{xy} = \overline{x} *_n \overline{y}$ bizonyítása hasonló).

Mivel $\overline{x + y}$ és $\overline{x} +_n \overline{y}$ is n -nel való osztási maradék, elég megmutatni, hogy kongruensek mod n .

Kongruenciák és műveletek

Tétel (FGy2.1.2)

Legyenek $m > 1$ és a, b, c, d egészek. Ha $a \equiv b \pmod{m}$ és $c \equiv d \pmod{m}$, akkor $a + c \equiv b + d \pmod{m}$ és $ac \equiv bd \pmod{m}$.

(Azonos modulusú kongruenciák összeadhatók, összeszorozhatók.)

A feltétel szerint $a - b = mt$ és $c - d = ms$ alkalmas $t, s \in \mathbb{Z}$ -re.

Ezért $(a + c) - (b + d) = m(t + s)$, így tényleg $a + c \equiv b + d \pmod{m}$.

Továbbá $m \mid a - b$ miatt $m \mid (a - b)c$, tehát $ac \equiv bc \pmod{m}$.

Hasonlóan $bc \equiv bd \pmod{m}$, és a tranzitivitás miatt $ac \equiv bd \pmod{m}$. \square

Belátjuk: $\overline{x + y} = \overline{x} +_n \overline{y}$ (az $\overline{xy} = \overline{x} *_n \overline{y}$ bizonyítása hasonló).

Mivel $\overline{x + y}$ és $\overline{x} +_n \overline{y}$ is n -nel való osztási maradék, elég megmutatni, hogy kongruensek mod n . Nyilván $x \equiv \overline{x} \pmod{n}$

Kongruenciák és műveletek

Tétel (FGy2.1.2)

Legyenek $m > 1$ és a, b, c, d egészek. Ha $a \equiv b \pmod{m}$ és $c \equiv d \pmod{m}$, akkor $a + c \equiv b + d \pmod{m}$ és $ac \equiv bd \pmod{m}$.

(Azonos modulusú kongruenciák összeadhatók, összeszorozhatók.)

A feltétel szerint $a - b = mt$ és $c - d = ms$ alkalmas $t, s \in \mathbb{Z}$ -re.

Ezért $(a + c) - (b + d) = m(t + s)$, így tényleg $a + c \equiv b + d \pmod{m}$.

Továbbá $m \mid a - b$ miatt $m \mid (a - b)c$, tehát $ac \equiv bc \pmod{m}$.

Hasonlóan $bc \equiv bd \pmod{m}$, és a tranzitivitás miatt $ac \equiv bd \pmod{m}$. \square

Belátjuk: $\overline{x + y} = \overline{x} +_n \overline{y}$ (az $\overline{xy} = \overline{x} *_n \overline{y}$ bizonyítása hasonló).

Mivel $\overline{x + y}$ és $\overline{x} +_n \overline{y}$ is n -nel való osztási maradék, elég megmutatni, hogy kongruensek mod n . Nyilván $x \equiv \overline{x} \pmod{n}$ és $y \equiv \overline{y} \pmod{n}$,

Kongruenciák és műveletek

Tétel (FGy2.1.2)

Legyenek $m > 1$ és a, b, c, d egészek. Ha $a \equiv b \pmod{m}$ és $c \equiv d \pmod{m}$, akkor $a + c \equiv b + d \pmod{m}$ és $ac \equiv bd \pmod{m}$.

(Azonos modulusú kongruenciák összeadhatók, összeszorozhatók.)

A feltétel szerint $a - b = mt$ és $c - d = ms$ alkalmas $t, s \in \mathbb{Z}$ -re.

Ezért $(a + c) - (b + d) = m(t + s)$, így tényleg $a + c \equiv b + d \pmod{m}$.

Továbbá $m \mid a - b$ miatt $m \mid (a - b)c$, tehát $ac \equiv bc \pmod{m}$.

Hasonlóan $bc \equiv bd \pmod{m}$, és a tranzitivitás miatt $ac \equiv bd \pmod{m}$. \square

Belátjuk: $\overline{x + y} = \overline{x} +_n \overline{y}$ (az $\overline{xy} = \overline{x} *_n \overline{y}$ bizonyítása hasonló).

Mivel $\overline{x + y}$ és $\overline{x} +_n \overline{y}$ is n -nel való osztási maradék, elég megmutatni, hogy kongruensek mod n . Nyilván $x \equiv \overline{x} \pmod{n}$ és $y \equiv \overline{y} \pmod{n}$, ezért $x + y \equiv \overline{x} + \overline{y} \pmod{n}$.

Kongruenciák és műveletek

Tétel (FGy2.1.2)

Legyenek $m > 1$ és a, b, c, d egészek. Ha $a \equiv b \pmod{m}$ és $c \equiv d \pmod{m}$, akkor $a + c \equiv b + d \pmod{m}$ és $ac \equiv bd \pmod{m}$.

(Azonos modulusú kongruenciák összeadhatók, összeszorozhatók.)

A feltétel szerint $a - b = mt$ és $c - d = ms$ alkalmas $t, s \in \mathbb{Z}$ -re.

Ezért $(a + c) - (b + d) = m(t + s)$, így tényleg $a + c \equiv b + d \pmod{m}$.

Továbbá $m \mid a - b$ miatt $m \mid (a - b)c$, tehát $ac \equiv bc \pmod{m}$.

Hasonlóan $bc \equiv bd \pmod{m}$, és a tranzitivitás miatt $ac \equiv bd \pmod{m}$. \square

Belátjuk: $\overline{x + y} = \overline{x} +_n \overline{y}$ (az $\overline{xy} = \overline{x} *_n \overline{y}$ bizonyítása hasonló).

Mivel $\overline{x + y}$ és $\overline{x} +_n \overline{y}$ is n -nel való osztási maradék, elég megmutatni, hogy kongruensek mod n . Nyilván $x \equiv \overline{x} \pmod{n}$ és $y \equiv \overline{y} \pmod{n}$, ezért $x + y \equiv \overline{x} + \overline{y} \pmod{n}$. A $+_n$ definíciója szerint $\overline{x} +_n \overline{y} \equiv \overline{x} + \overline{y} \pmod{n}$,

Kongruenciák és műveletek

Tétel (FGy2.1.2)

Legyenek $m > 1$ és a, b, c, d egészek. Ha $a \equiv b \pmod{m}$ és $c \equiv d \pmod{m}$, akkor $a + c \equiv b + d \pmod{m}$ és $ac \equiv bd \pmod{m}$.

(Azonos modulusú kongruenciák összeadhatók, összeszorozhatók.)

A feltétel szerint $a - b = mt$ és $c - d = ms$ alkalmas $t, s \in \mathbb{Z}$ -re.

Ezért $(a + c) - (b + d) = m(t + s)$, így tényleg $a + c \equiv b + d \pmod{m}$.

Továbbá $m \mid a - b$ miatt $m \mid (a - b)c$, tehát $ac \equiv bc \pmod{m}$.

Hasonlóan $bc \equiv bd \pmod{m}$, és a tranzitivitás miatt $ac \equiv bd \pmod{m}$. \square

Belátjuk: $\overline{x + y} = \overline{x} +_n \overline{y}$ (az $\overline{xy} = \overline{x} *_n \overline{y}$ bizonyítása hasonló).

Mivel $\overline{x + y}$ és $\overline{x} +_n \overline{y}$ is n -nel való osztási maradék, elég megmutatni, hogy kongruensek mod n . Nyilván $x \equiv \overline{x} \pmod{n}$ és $y \equiv \overline{y} \pmod{n}$, ezért $x + y \equiv \overline{x} + \overline{y} \pmod{n}$. A $+_n$ definíciója szerint $\overline{x} +_n \overline{y} \equiv \overline{x} + \overline{y} \pmod{n}$, így $\overline{x} +_n \overline{y} \equiv x + y \equiv \overline{x + y} \pmod{n}$. \square

Kongruenciák egyszerűsítése

Tétel (FGy2.1.3)

Ha $ac \equiv bc \pmod{m}$, akkor $a \equiv b \pmod{m/(m, c)}$.

Kongruenciák egyszerűsítése

Tétel (FGy2.1.3)

Ha $ac \equiv bc \pmod{m}$, akkor $a \equiv b \pmod{m/(m, c)}$.

(A modulust le kell osztani m és c kitüntetett közös osztójával.)

Kongruenciák egyszerűsítése

Tétel (FGy2.1.3)

Ha $ac \equiv bc \pmod{m}$, akkor $a \equiv b \pmod{m/(m, c)}$.

(A modulust le kell osztani m és c kitüntetett közös osztójával.)

Bizonyítás

A feltétel szerint $m \mid (a - b)c$,

Kongruenciák egyszerűsítése

Tétel (FGy2.1.3)

Ha $ac \equiv bc \pmod{m}$, akkor $a \equiv b \pmod{m/(m, c)}$.

(A modulust le kell osztani m és c kitüntetett közös osztójával.)

Bizonyítás

A feltétel szerint $m \mid (a - b)c$, így az oszthatóságot $d = (m, c)$ -vel egyszerűsítve $(m/d) \mid (a - b)(c/d)$.

Kongruenciák egyszerűsítése

Tétel (FGy2.1.3)

Ha $ac \equiv bc \pmod{m}$, akkor $a \equiv b \pmod{m/(m, c)}$.

(A modulust le kell osztani m és c kitüntetett közös osztójával.)

Bizonyítás

A feltétel szerint $m \mid (a - b)c$, így az oszthatóságot $d = (m, c)$ -vel egyszerűsítve $(m/d) \mid (a - b)(c/d)$.

A kitüntetett közös osztó kiemelési tulajdonsága miatt $(m/d, c/d)d = (m, c) = d$,

Kongruenciák egyszerűsítése

Tétel (FGy2.1.3)

Ha $ac \equiv bc \pmod{m}$, akkor $a \equiv b \pmod{m/(m, c)}$.

(A modulust le kell osztani m és c kitüntetett közös osztójával.)

Bizonyítás

A feltétel szerint $m \mid (a - b)c$, így az oszthatóságot $d = (m, c)$ -vel egyszerűsítve $(m/d) \mid (a - b)(c/d)$.

A kitüntetett közös osztó kiemelési tulajdonsága miatt $(m/d, c/d)d = (m, c) = d$, azaz $(m/d, c/d) = 1$.

Kongruenciák egyszerűsítése

Tétel (FGy2.1.3)

Ha $ac \equiv bc \pmod{m}$, akkor $a \equiv b \pmod{m/(m, c)}$.

(A modulust le kell osztani m és c kitüntetett közös osztójával.)

Bizonyítás

A feltétel szerint $m \mid (a - b)c$, így az oszthatóságot $d = (m, c)$ -vel egyszerűsítve $(m/d) \mid (a - b)(c/d)$.

A kitüntetett közös osztó kiemelési tulajdonsága miatt $(m/d, c/d)d = (m, c) = d$, azaz $(m/d, c/d) = 1$.

Ezért az $(m/d) \mid (a - b)(c/d)$ oszthatóságból $(m/d) \mid (a - b)$,

Kongruenciák egyszerűsítése

Tétel (FGy2.1.3)

Ha $ac \equiv bc \pmod{m}$, akkor $a \equiv b \pmod{m/(m, c)}$.

(A modulust le kell osztani m és c kitüntetett közös osztójával.)

Bizonyítás

A feltétel szerint $m \mid (a - b)c$, így az oszthatóságot $d = (m, c)$ -vel egyszerűsítve $(m/d) \mid (a - b)(c/d)$.

A kitüntetett közös osztó kiemelési tulajdonsága miatt $(m/d, c/d)d = (m, c) = d$, azaz $(m/d, c/d) = 1$.

Ezért az $(m/d) \mid (a - b)(c/d)$ oszthatóságból $(m/d) \mid (a - b)$, azaz $a \equiv b \pmod{m/(m, c)}$ következik. □

Kongruenciák egyszerűsítése

Tétel (FGy2.1.3)

Ha $ac \equiv bc \pmod{m}$, akkor $a \equiv b \pmod{m/(m, c)}$.

(A modulust le kell osztani m és c kitüntetett közös osztójával.)

Bizonyítás

A feltétel szerint $m \mid (a - b)c$, így az oszthatóságot $d = (m, c)$ -vel egyszerűsítve $(m/d) \mid (a - b)(c/d)$.

A kitüntetett közös osztó kiemelési tulajdonsága miatt $(m/d, c/d)d = (m, c) = d$, azaz $(m/d, c/d) = 1$.

Ezért az $(m/d) \mid (a - b)(c/d)$ oszthatóságból $(m/d) \mid (a - b)$, azaz $a \equiv b \pmod{m/(m, c)}$ következik. □

Általában **nem igaz**, hogy $ac \equiv bc \pmod{m} \implies a \equiv b \pmod{m}$.

Kongruenciák egyszerűsítése

Tétel (FGy2.1.3)

Ha $ac \equiv bc \pmod{m}$, akkor $a \equiv b \pmod{m/(m, c)}$.

(A modulust le kell osztani m és c kitüntetett közös osztójával.)

Bizonyítás

A feltétel szerint $m \mid (a - b)c$, így az oszthatóságot $d = (m, c)$ -vel egyszerűsítve $(m/d) \mid (a - b)(c/d)$.

A kitüntetett közös osztó kiemelési tulajdonsága miatt $(m/d, c/d)d = (m, c) = d$, azaz $(m/d, c/d) = 1$.

Ezért az $(m/d) \mid (a - b)(c/d)$ oszthatóságból $(m/d) \mid (a - b)$, azaz $a \equiv b \pmod{m/(m, c)}$ következik. □

Általában **nem igaz**, hogy $ac \equiv bc \pmod{m} \implies a \equiv b \pmod{m}$.

Például $10 \cdot 2 \equiv 20 \cdot 2 \pmod{20}$,

Kongruenciák egyszerűsítése

Tétel (FGy2.1.3)

Ha $ac \equiv bc \pmod{m}$, akkor $a \equiv b \pmod{m/(m, c)}$.

(A modulust le kell osztani m és c kitüntetett közös osztójával.)

Bizonyítás

A feltétel szerint $m \mid (a - b)c$, így az oszthatóságot $d = (m, c)$ -vel egyszerűsítve $(m/d) \mid (a - b)(c/d)$.

A kitüntetett közös osztó kiemelési tulajdonsága miatt $(m/d, c/d)d = (m, c) = d$, azaz $(m/d, c/d) = 1$.

Ezért az $(m/d) \mid (a - b)(c/d)$ oszthatóságból $(m/d) \mid (a - b)$, azaz $a \equiv b \pmod{m/(m, c)}$ következik. □

Általában **nem igaz**, hogy $ac \equiv bc \pmod{m} \implies a \equiv b \pmod{m}$.

Például $10 \cdot 2 \equiv 20 \cdot 2 \pmod{20}$, de $10 \not\equiv 20 \pmod{20}$.

Kongruenciák egyszerűsítése

Tétel (FGy2.1.3)

Ha $ac \equiv bc \pmod{m}$, akkor $a \equiv b \pmod{m/(m, c)}$.

(A modulust le kell osztani m és c kitüntetett közös osztójával.)

Bizonyítás

A feltétel szerint $m \mid (a - b)c$, így az oszthatóságot $d = (m, c)$ -vel egyszerűsítve $(m/d) \mid (a - b)(c/d)$.

A kitüntetett közös osztó kiemelési tulajdonsága miatt $(m/d, c/d)d = (m, c) = d$, azaz $(m/d, c/d) = 1$.

Ezért az $(m/d) \mid (a - b)(c/d)$ oszthatóságból $(m/d) \mid (a - b)$, azaz $a \equiv b \pmod{m/(m, c)}$ következik. □

Általában **nem igaz**, hogy $ac \equiv bc \pmod{m} \implies a \equiv b \pmod{m}$.

Például $10 \cdot 2 \equiv 20 \cdot 2 \pmod{20}$, de $10 \not\equiv 20 \pmod{20}$.

De a modulushoz relatív prím számmal szabad egyszerűsíteni.

A kongruencia egyszerűsíti a számolásokat

Igazoljuk, hogy $a - b \mid a^n - b^n$.

A kongruencia egyszerűsíti a számolásokat

Igazoljuk, hogy $a - b \mid a^n - b^n$.

$$a - b \mid a - b,$$

A kongruencia egyszerűsíti a számolásokat

Igazoljuk, hogy $a - b \mid a^n - b^n$.

$a - b \mid a - b$, ezért $a \equiv b \pmod{a - b}$.

A kongruencia egyszerűsíti a számolásokat

Igazoljuk, hogy $a - b \mid a^n - b^n$.

$a - b \mid a - b$, ezért $a \equiv b \pmod{a - b}$. Önmagával n -szer összeszorozva $a^n \equiv b^n \pmod{a - b}$,

A kongruencia egyszerűsíti a számolásokat

Igazoljuk, hogy $a - b \mid a^n - b^n$.

$a - b \mid a - b$, ezért $a \equiv b \pmod{a - b}$. Önmagával n -szer összeszorozva $a^n \equiv b^n \pmod{a - b}$, azaz $a - b \mid a^n - b^n$.

A kongruencia egyszerűsíti a számolásokat

Igazoljuk, hogy $a - b \mid a^n - b^n$.

$a - b \mid a - b$, ezért $a \equiv b \pmod{a - b}$. Önmagával n -szer összeszorozva $a^n \equiv b^n \pmod{a - b}$, azaz $a - b \mid a^n - b^n$.

Mi 23^{102} utolsó számjegye?

A kongruencia egyszerűsíti a számolásokat

Igazoljuk, hogy $a - b \mid a^n - b^n$.

$a - b \mid a - b$, ezért $a \equiv b \pmod{a - b}$. Önmagával n -szer összeszorozva $a^n \equiv b^n \pmod{a - b}$, azaz $a - b \mid a^n - b^n$.

Mi 23^{102} utolsó számjegye?

$23 \equiv 3 \pmod{10}$,

A kongruencia egyszerűsíti a számolásokat

Igazoljuk, hogy $a - b \mid a^n - b^n$.

$a - b \mid a - b$, ezért $a \equiv b \pmod{a - b}$. Önmagával n -szer összeszorozva $a^n \equiv b^n \pmod{a - b}$, azaz $a - b \mid a^n - b^n$.

Mi 23^{102} utolsó számjegye?

$23 \equiv 3 \pmod{10}$, ezért $23^{102} \equiv 3^{102} \pmod{10}$.

A kongruencia egyszerűsíti a számolásokat

Igazoljuk, hogy $a - b \mid a^n - b^n$.

$a - b \mid a - b$, ezért $a \equiv b \pmod{a - b}$. Önmagával n -szer összeszorozva $a^n \equiv b^n \pmod{a - b}$, azaz $a - b \mid a^n - b^n$.

Mi 23^{102} utolsó számjegye?

$23 \equiv 3 \pmod{10}$, ezért $23^{102} \equiv 3^{102} \pmod{10}$. De $3^{100} = (3^4)^{25}$

A kongruencia egyszerűsíti a számolásokat

Igazoljuk, hogy $a - b \mid a^n - b^n$.

$a - b \mid a - b$, ezért $a \equiv b \pmod{a - b}$. Önmagával n -szer összeszorozva $a^n \equiv b^n \pmod{a - b}$, azaz $a - b \mid a^n - b^n$.

Mi 23^{102} utolsó számjegye?

$23 \equiv 3 \pmod{10}$, ezért $23^{102} \equiv 3^{102} \pmod{10}$. De $3^{100} = (3^4)^{25} = 81^{25}$.

A kongruencia egyszerűsíti a számolásokat

Igazoljuk, hogy $a - b \mid a^n - b^n$.

$a - b \mid a - b$, ezért $a \equiv b \pmod{a - b}$. Önmagával n -szer összeszorozva $a^n \equiv b^n \pmod{a - b}$, azaz $a - b \mid a^n - b^n$.

Mi 23^{102} utolsó számjegye?

$23 \equiv 3 \pmod{10}$, ezért $23^{102} \equiv 3^{102} \pmod{10}$. De $3^{100} = (3^4)^{25} = 81^{25}$.
Mivel $81 \equiv 1 \pmod{10}$, ezért $3^{102} = 3^2 3^{100}$

A kongruencia egyszerűsíti a számolásokat

Igazoljuk, hogy $a - b \mid a^n - b^n$.

$a - b \mid a - b$, ezért $a \equiv b \pmod{a - b}$. Önmagával n -szer összeszorozva $a^n \equiv b^n \pmod{a - b}$, azaz $a - b \mid a^n - b^n$.

Mi 23^{102} utolsó számjegye?

$23 \equiv 3 \pmod{10}$, ezért $23^{102} \equiv 3^{102} \pmod{10}$. De $3^{100} = (3^4)^{25} = 81^{25}$.
Mivel $81 \equiv 1 \pmod{10}$, ezért $3^{102} = 3^2 3^{100} = 3^2 81^{25} \equiv 3^2 1^{25}$

A kongruencia egyszerűsíti a számolásokat

Igazoljuk, hogy $a - b \mid a^n - b^n$.

$a - b \mid a - b$, ezért $a \equiv b \pmod{a - b}$. Önmagával n -szer összeszorozva $a^n \equiv b^n \pmod{a - b}$, azaz $a - b \mid a^n - b^n$.

Mi 23^{102} utolsó számjegye? Válasz: 9.

$23 \equiv 3 \pmod{10}$, ezért $23^{102} \equiv 3^{102} \pmod{10}$. De $3^{100} = (3^4)^{25} = 81^{25}$.

Mivel $81 \equiv 1 \pmod{10}$, ezért $3^{102} = 3^2 3^{100} = 3^2 81^{25} \equiv 3^2 1^{25} = 9 \pmod{10}$.

A kongruencia egyszerűsíti a számolásokat

Igazoljuk, hogy $a - b \mid a^n - b^n$.

$a - b \mid a - b$, ezért $a \equiv b \pmod{a - b}$. Önmagával n -szer összeszorozva $a^n \equiv b^n \pmod{a - b}$, azaz $a - b \mid a^n - b^n$.

Mi 23^{102} utolsó számjegye? Válasz: 9.

$23 \equiv 3 \pmod{10}$, ezért $23^{102} \equiv 3^{102} \pmod{10}$. De $3^{100} = (3^4)^{25} = 81^{25}$.
Mivel $81 \equiv 1 \pmod{10}$, ezért $3^{102} = 3^2 3^{100} = 3^2 81^{25} \equiv 3^2 1^{25} = 9 \pmod{10}$.

Mutassuk meg, hogy $11 \mid 3^{4n+5} - 5^{3n}$.

A kongruencia egyszerűsíti a számolásokat

Igazoljuk, hogy $a - b \mid a^n - b^n$.

$a - b \mid a - b$, ezért $a \equiv b \pmod{a - b}$. Önmagával n -szer összeszorozva $a^n \equiv b^n \pmod{a - b}$, azaz $a - b \mid a^n - b^n$.

Mi 23^{102} utolsó számjegye? Válasz: 9.

$23 \equiv 3 \pmod{10}$, ezért $23^{102} \equiv 3^{102} \pmod{10}$. De $3^{100} = (3^4)^{25} = 81^{25}$.
Mivel $81 \equiv 1 \pmod{10}$, ezért $3^{102} = 3^2 3^{100} = 3^2 81^{25} \equiv 3^2 1^{25} = 9 \pmod{10}$.

Mutassuk meg, hogy $11 \mid 3^{4n+5} - 5^{3n}$.

Mod 11 számolva $3^{4n+5} - 5^{3n} = 243 \cdot 81^n - 125^n$

A kongruencia egyszerűsíti a számolásokat

Igazoljuk, hogy $a - b \mid a^n - b^n$.

$a - b \mid a - b$, ezért $a \equiv b \pmod{a - b}$. Önmagával n -szer összeszorozva $a^n \equiv b^n \pmod{a - b}$, azaz $a - b \mid a^n - b^n$.

Mi 23^{102} utolsó számjegye? Válasz: 9.

$23 \equiv 3 \pmod{10}$, ezért $23^{102} \equiv 3^{102} \pmod{10}$. De $3^{100} = (3^4)^{25} = 81^{25}$.
Mivel $81 \equiv 1 \pmod{10}$, ezért $3^{102} = 3^2 3^{100} = 3^2 81^{25} \equiv 3^2 1^{25} = 9 \pmod{10}$.

Mutassuk meg, hogy $11 \mid 3^{4n+5} - 5^{3n}$.

Mod 11 számolva $3^{4n+5} - 5^{3n} = 243 \cdot 81^n - 125^n \equiv 1 \cdot 4^n - 4^n = 0$.

A kongruencia egyszerűsíti a számolásokat

Igazoljuk, hogy $a - b \mid a^n - b^n$.

$a - b \mid a - b$, ezért $a \equiv b \pmod{a - b}$. Önmagával n -szer összeszorozva $a^n \equiv b^n \pmod{a - b}$, azaz $a - b \mid a^n - b^n$.

Mi 23^{102} utolsó számjegye? Válasz: 9.

$23 \equiv 3 \pmod{10}$, ezért $23^{102} \equiv 3^{102} \pmod{10}$. De $3^{100} = (3^4)^{25} = 81^{25}$.
Mivel $81 \equiv 1 \pmod{10}$, ezért $3^{102} = 3^2 3^{100} = 3^2 81^{25} \equiv 3^2 1^{25} = 9 \pmod{10}$.

Mutassuk meg, hogy $11 \mid 3^{4n+5} - 5^{3n}$.

Mod 11 számolva $3^{4n+5} - 5^{3n} = 243 \cdot 81^n - 125^n \equiv 1 \cdot 4^n - 4^n = 0$.

Igazoljuk, hogy $641 \mid 2^{32} + 1$.

A kongruencia egyszerűsíti a számolásokat

Igazoljuk, hogy $a - b \mid a^n - b^n$.

$a - b \mid a - b$, ezért $a \equiv b \pmod{a - b}$. Önmagával n -szer összeszorozva $a^n \equiv b^n \pmod{a - b}$, azaz $a - b \mid a^n - b^n$.

Mi 23^{102} utolsó számjegye? Válasz: 9.

$23 \equiv 3 \pmod{10}$, ezért $23^{102} \equiv 3^{102} \pmod{10}$. De $3^{100} = (3^4)^{25} = 81^{25}$.
Mivel $81 \equiv 1 \pmod{10}$, ezért $3^{102} = 3^2 3^{100} = 3^2 81^{25} \equiv 3^2 1^{25} = 9 \pmod{10}$.

Mutassuk meg, hogy $11 \mid 3^{4n+5} - 5^{3n}$.

Mod 11 számolva $3^{4n+5} - 5^{3n} = 243 \cdot 81^n - 125^n \equiv 1 \cdot 4^n - 4^n = 0$.

Igazoljuk, hogy $641 \mid 2^{32} + 1$.

Mod 641 nézve $5 \cdot 2^7 \equiv -1$

A kongruencia egyszerűsíti a számolásokat

Igazoljuk, hogy $a - b \mid a^n - b^n$.

$a - b \mid a - b$, ezért $a \equiv b \pmod{a - b}$. Önmagával n -szer összeszorozva $a^n \equiv b^n \pmod{a - b}$, azaz $a - b \mid a^n - b^n$.

Mi 23^{102} utolsó számjegye? Válasz: 9.

$23 \equiv 3 \pmod{10}$, ezért $23^{102} \equiv 3^{102} \pmod{10}$. De $3^{100} = (3^4)^{25} = 81^{25}$.
Mivel $81 \equiv 1 \pmod{10}$, ezért $3^{102} = 3^2 3^{100} = 3^2 81^{25} \equiv 3^2 1^{25} = 9 \pmod{10}$.

Mutassuk meg, hogy $11 \mid 3^{4n+5} - 5^{3n}$.

Mod 11 számolva $3^{4n+5} - 5^{3n} = 243 \cdot 81^n - 125^n \equiv 1 \cdot 4^n - 4^n = 0$.

Igazoljuk, hogy $641 \mid 2^{32} + 1$.

Mod 641 nézve $5 \cdot 2^7 \equiv -1$ és $5^4 \equiv -2^4$,

A kongruencia egyszerűsíti a számolásokat

Igazoljuk, hogy $a - b \mid a^n - b^n$.

$a - b \mid a - b$, ezért $a \equiv b \pmod{a - b}$. Önmagával n -szer összeszorozva $a^n \equiv b^n \pmod{a - b}$, azaz $a - b \mid a^n - b^n$.

Mi 23^{102} utolsó számjegye? Válasz: 9.

$23 \equiv 3 \pmod{10}$, ezért $23^{102} \equiv 3^{102} \pmod{10}$. De $3^{100} = (3^4)^{25} = 81^{25}$.
Mivel $81 \equiv 1 \pmod{10}$, ezért $3^{102} = 3^2 3^{100} = 3^2 81^{25} \equiv 3^2 1^{25} = 9 \pmod{10}$.

Mutassuk meg, hogy $11 \mid 3^{4n+5} - 5^{3n}$.

Mod 11 számolva $3^{4n+5} - 5^{3n} = 243 \cdot 81^n - 125^n \equiv 1 \cdot 4^n - 4^n = 0$.

Igazoljuk, hogy $641 \mid 2^{32} + 1$.

Mod 641 nézve $5 \cdot 2^7 \equiv -1$ és $5^4 \equiv -2^4$, így
 $2^{32} = 2^4 2^{28}$

A kongruencia egyszerűsíti a számolásokat

Igazoljuk, hogy $a - b \mid a^n - b^n$.

$a - b \mid a - b$, ezért $a \equiv b \pmod{a - b}$. Önmagával n -szer összeszorozva $a^n \equiv b^n \pmod{a - b}$, azaz $a - b \mid a^n - b^n$.

Mi 23^{102} utolsó számjegye? Válasz: 9.

$23 \equiv 3 \pmod{10}$, ezért $23^{102} \equiv 3^{102} \pmod{10}$. De $3^{100} = (3^4)^{25} = 81^{25}$.
Mivel $81 \equiv 1 \pmod{10}$, ezért $3^{102} = 3^2 3^{100} = 3^2 81^{25} \equiv 3^2 1^{25} = 9 \pmod{10}$.

Mutassuk meg, hogy $11 \mid 3^{4n+5} - 5^{3n}$.

Mod 11 számolva $3^{4n+5} - 5^{3n} = 243 \cdot 81^n - 125^n \equiv 1 \cdot 4^n - 4^n = 0$.

Igazoljuk, hogy $641 \mid 2^{32} + 1$.

Mod 641 nézve $5 \cdot 2^7 \equiv -1$ és $5^4 \equiv -2^4$, így
 $2^{32} = 2^4 2^{28} \equiv -5^4 (2^7)^4$

A kongruencia egyszerűsíti a számolásokat

Igazoljuk, hogy $a - b \mid a^n - b^n$.

$a - b \mid a - b$, ezért $a \equiv b \pmod{a - b}$. Önmagával n -szer összeszorozva $a^n \equiv b^n \pmod{a - b}$, azaz $a - b \mid a^n - b^n$.

Mi 23^{102} utolsó számjegye? Válasz: 9.

$23 \equiv 3 \pmod{10}$, ezért $23^{102} \equiv 3^{102} \pmod{10}$. De $3^{100} = (3^4)^{25} = 81^{25}$.
Mivel $81 \equiv 1 \pmod{10}$, ezért $3^{102} = 3^2 3^{100} = 3^2 81^{25} \equiv 3^2 1^{25} = 9 \pmod{10}$.

Mutassuk meg, hogy $11 \mid 3^{4n+5} - 5^{3n}$.

Mod 11 számolva $3^{4n+5} - 5^{3n} = 243 \cdot 81^n - 125^n \equiv 1 \cdot 4^n - 4^n = 0$.

Igazoljuk, hogy $641 \mid 2^{32} + 1$.

Mod 641 nézve $5 \cdot 2^7 \equiv -1$ és $5^4 \equiv -2^4$, így
 $2^{32} = 2^4 2^{28} \equiv -5^4 (2^7)^4 = -(5 \cdot 2^7)^4$

A kongruencia egyszerűsíti a számolásokat

Igazoljuk, hogy $a - b \mid a^n - b^n$.

$a - b \mid a - b$, ezért $a \equiv b \pmod{a - b}$. Önmagával n -szer összeszorozva $a^n \equiv b^n \pmod{a - b}$, azaz $a - b \mid a^n - b^n$.

Mi 23^{102} utolsó számjegye? Válasz: 9.

$23 \equiv 3 \pmod{10}$, ezért $23^{102} \equiv 3^{102} \pmod{10}$. De $3^{100} = (3^4)^{25} = 81^{25}$.
Mivel $81 \equiv 1 \pmod{10}$, ezért $3^{102} = 3^2 3^{100} = 3^2 81^{25} \equiv 3^2 1^{25} = 9 \pmod{10}$.

Mutassuk meg, hogy $11 \mid 3^{4n+5} - 5^{3n}$.

Mod 11 számolva $3^{4n+5} - 5^{3n} = 243 \cdot 81^n - 125^n \equiv 1 \cdot 4^n - 4^n = 0$.

Igazoljuk, hogy $641 \mid 2^{32} + 1$.

Mod 641 nézve $5 \cdot 2^7 \equiv -1$ és $5^4 \equiv -2^4$, így
 $2^{32} = 2^4 2^{28} \equiv -5^4 (2^7)^4 = -(5 \cdot 2^7)^4 \equiv -1$.

Lineáris kongruencia

Definíció (FGy2.5.1)

Ha $a, b, m \in \mathbb{Z}$ és $m > 0$, akkor $ax \equiv b \pmod{m}$ **lineáris kongruencia**.

Lineáris kongruencia

Definíció (FGy2.5.1)

Ha $a, b, m \in \mathbb{Z}$ és $m > 0$, akkor $ax \equiv b \pmod{m}$ **lineáris kongruencia**.

Példa: Mik $8x \equiv 4 \pmod{6}$ megoldásai?

Lineáris kongruencia

Definíció (FGy2.5.1)

Ha $a, b, m \in \mathbb{Z}$ és $m > 0$, akkor $ax \equiv b \pmod{m}$ **lineáris kongruencia**.

Példa: Mik $8x \equiv 4 \pmod{6}$ megoldásai?

Egyszerűsítsünk 4-gyel.

Lineáris kongruencia

Definíció (FGy2.5.1)

Ha $a, b, m \in \mathbb{Z}$ és $m > 0$, akkor $ax \equiv b \pmod{m}$ **lineáris kongruencia**.

Példa: Mik $8x \equiv 4 \pmod{6}$ megoldásai?

Egyszerűsítsünk 4-gyel. Mivel $(4, 6) = 2$, ezért $2x \equiv 1 \pmod{3}$ adódik.

Lineáris kongruencia

Definíció (FGy2.5.1)

Ha $a, b, m \in \mathbb{Z}$ és $m > 0$, akkor $ax \equiv b \pmod{m}$ **lineáris kongruencia**.

Példa: Mik $8x \equiv 4 \pmod{6}$ megoldásai?

Egyszerűsítsünk 4-gyel. Mivel $(4, 6) = 2$, ezért $2x \equiv 1 \pmod{3}$ adódik.
2-vel szorozva $4x \equiv 2 \pmod{3}$.

Lineáris kongruencia

Definíció (FGy2.5.1)

Ha $a, b, m \in \mathbb{Z}$ és $m > 0$, akkor $ax \equiv b \pmod{m}$ **lineáris kongruencia**.

Példa: Mik $8x \equiv 4 \pmod{6}$ megoldásai?

Egyszerűsítsünk 4-gyel. Mivel $(4, 6) = 2$, ezért $2x \equiv 1 \pmod{3}$ adódik.

2-vel szorozva $4x \equiv 2 \pmod{3}$. De $4x \equiv x \pmod{3}$,

Lineáris kongruencia

Definíció (FGy2.5.1)

Ha $a, b, m \in \mathbb{Z}$ és $m > 0$, akkor $ax \equiv b \pmod{m}$ **lineáris kongruencia**.

Példa: Mik $8x \equiv 4 \pmod{6}$ megoldásai?

Egyszerűsítsünk 4-gyel. Mivel $(4, 6) = 2$, ezért $2x \equiv 1 \pmod{3}$ adódik.

2-vel szorozva $4x \equiv 2 \pmod{3}$. De $4x \equiv x \pmod{3}$, azaz $x \equiv 2 \pmod{3}$.

Lineáris kongruencia

Definíció (FGy2.5.1)

Ha $a, b, m \in \mathbb{Z}$ és $m > 0$, akkor $ax \equiv b \pmod{m}$ **lineáris kongruencia**.

Példa: Mik $8x \equiv 4 \pmod{6}$ megoldásai?

Egyszerűsítsünk 4-gyel. Mivel $(4, 6) = 2$, ezért $2x \equiv 1 \pmod{3}$ adódik.

2-vel szorozva $4x \equiv 2 \pmod{3}$. De $4x \equiv x \pmod{3}$, azaz $x \equiv 2 \pmod{3}$.

Tehát azok az x számok adnak megoldást, melyek 3-mal osztva 2 maradékot adnak.

Lineáris kongruencia

Definíció (FGy2.5.1)

Ha $a, b, m \in \mathbb{Z}$ és $m > 0$, akkor $ax \equiv b \pmod{m}$ **lineáris kongruencia**.

Példa: Mik $8x \equiv 4 \pmod{6}$ megoldásai?

Egyszerűsítsünk 4-gyel. Mivel $(4, 6) = 2$, ezért $2x \equiv 1 \pmod{3}$ adódik.

2-vel szorozva $4x \equiv 2 \pmod{3}$. De $4x \equiv x \pmod{3}$, azaz $x \equiv 2 \pmod{3}$.

Tehát azok az x számok adnak megoldást, melyek 3-mal osztva

2 maradékot adnak. Ezek a $3k + 2$ alakú számok, ahol $k \in \mathbb{Z}$.

Lineáris kongruencia

Definíció (FGy2.5.1)

Ha $a, b, m \in \mathbb{Z}$ és $m > 0$, akkor $ax \equiv b \pmod{m}$ **lineáris kongruencia**.

Példa: Mik $8x \equiv 4 \pmod{6}$ megoldásai?

Egyszerűsítsünk 4-gyel. Mivel $(4, 6) = 2$, ezért $2x \equiv 1 \pmod{3}$ adódik.

2-vel szorozva $4x \equiv 2 \pmod{3}$. De $4x \equiv x \pmod{3}$, azaz $x \equiv 2 \pmod{3}$.

Tehát azok az x számok adnak megoldást, melyek 3-mal osztva 2 maradékot adnak. Ezek a $3k + 2$ alakú számok, ahol $k \in \mathbb{Z}$.

Ha egy egyenletet négyzetre emelünk, **hamis megoldások** keletkezhetnek.

Lineáris kongruencia

Definíció (FGy2.5.1)

Ha $a, b, m \in \mathbb{Z}$ és $m > 0$, akkor $ax \equiv b \pmod{m}$ **lineáris kongruencia**.

Példa: Mik $8x \equiv 4 \pmod{6}$ megoldásai?

Egyszerűsítsünk 4-gyel. Mivel $(4, 6) = 2$, ezért $2x \equiv 1 \pmod{3}$ adódik.

2-vel szorozva $4x \equiv 2 \pmod{3}$. De $4x \equiv x \pmod{3}$, azaz $x \equiv 2 \pmod{3}$.

Tehát azok az x számok adnak megoldást, melyek 3-mal osztva

2 maradékot adnak. Ezek a $3k + 2$ alakú számok, ahol $k \in \mathbb{Z}$.

Ha egy egyenletet négyzetre emelünk, **hamis megoldások** keletkezhetnek. Ha egy kongruenciát számmal szorzunk, akkor is.

Lineáris kongruencia

Definíció (FGy2.5.1)

Ha $a, b, m \in \mathbb{Z}$ és $m > 0$, akkor $ax \equiv b \pmod{m}$ **lineáris kongruencia**.

Példa: Mik $8x \equiv 4 \pmod{6}$ megoldásai?

Egyszerűsítsünk 4-gyel. Mivel $(4, 6) = 2$, ezért $2x \equiv 1 \pmod{3}$ adódik.

2-vel szorozva $4x \equiv 2 \pmod{3}$. De $4x \equiv x \pmod{3}$, azaz $x \equiv 2 \pmod{3}$.

Tehát azok az x számok adnak megoldást, melyek 3-mal osztva 2 maradékot adnak. Ezek a $3k + 2$ alakú számok, ahol $k \in \mathbb{Z}$.

Ha egy egyenletet négyzetre emelünk, **hamis megoldások** keletkezhetnek. Ha egy kongruenciát számmal szorzunk, akkor is.

Példa: $2x \equiv 1 \pmod{3}$ -at 3-mal szorozva $6x \equiv 3 \pmod{3}$,

Lineáris kongruencia

Definíció (FGy2.5.1)

Ha $a, b, m \in \mathbb{Z}$ és $m > 0$, akkor $ax \equiv b \pmod{m}$ **lineáris kongruencia**.

Példa: Mik $8x \equiv 4 \pmod{6}$ megoldásai?

Egyszerűsítsünk 4-gyel. Mivel $(4, 6) = 2$, ezért $2x \equiv 1 \pmod{3}$ adódik.

2-vel szorozva $4x \equiv 2 \pmod{3}$. De $4x \equiv x \pmod{3}$, azaz $x \equiv 2 \pmod{3}$.

Tehát azok az x számok adnak megoldást, melyek 3-mal osztva

2 maradékot adnak. Ezek a $3k + 2$ alakú számok, ahol $k \in \mathbb{Z}$.

Ha egy egyenletet négyzetre emelünk, **hamis megoldások** keletkezhetnek. Ha egy kongruenciát számmal szorzunk, akkor is.

Példa: $2x \equiv 1 \pmod{3}$ -at 3-mal szorozva $6x \equiv 3 \pmod{3}$,

itt minden x szám megoldás.

Lineáris kongruencia

Definíció (FGy2.5.1)

Ha $a, b, m \in \mathbb{Z}$ és $m > 0$, akkor $ax \equiv b \pmod{m}$ **lineáris kongruencia**.

Példa: Mik $8x \equiv 4 \pmod{6}$ megoldásai?

Egyszerűsítsünk 4-gyel. Mivel $(4, 6) = 2$, ezért $2x \equiv 1 \pmod{3}$ adódik.

2-vel szorozva $4x \equiv 2 \pmod{3}$. De $4x \equiv x \pmod{3}$, azaz $x \equiv 2 \pmod{3}$.

Tehát azok az x számok adnak megoldást, melyek 3-mal osztva 2 maradékot adnak. Ezek a $3k + 2$ alakú számok, ahol $k \in \mathbb{Z}$.

Ha egy egyenletet négyzetre emelünk, **hamis megoldások** keletkezhetnek. Ha egy kongruenciát számmal szorzunk, akkor is.

Példa: $2x \equiv 1 \pmod{3}$ -at 3-mal szorozva $6x \equiv 3 \pmod{3}$,

itt minden x szám megoldás.

HF: A modulushoz relatív prímmel való szorzás ekvivalens átalakítás, ilyenkor nem keletkezik hamis megoldás.

Visszavezetés lineáris diofantikus egyenletre

Ismétlés: $8x \equiv 4 \pmod{6}$ megoldásai a $3k + 2$ alakú számok ($k \in \mathbb{Z}$).

Visszavezetés lineáris diofantikus egyenletre

Ismétlés: $8x \equiv 4 \pmod{6}$ megoldásai a $3k + 2$ alakú számok ($k \in \mathbb{Z}$).

Definíció (FGy2.2.1)

Rögzített m modulus esetén az m -mel osztva r maradékot adó számok halmazát az r **maradékosztályának** nevezzük mod m .

Visszavezetés lineáris diofantikus egyenletre

Ismétlés: $8x \equiv 4 \pmod{6}$ megoldásai a $3k + 2$ alakú számok ($k \in \mathbb{Z}$).

Definíció (FGy2.2.1)

Rögzített m modulus esetén az m -mel osztva r maradékot adó számok halmazát az r **maradékosztályának** nevezzük mod m .
Ez tehát az $mk + r$ alakú számok halmaza, ahol $k \in \mathbb{Z}$.

Visszavezetés lineáris diofantikus egyenletre

Ismétlés: $8x \equiv 4 \pmod{6}$ megoldásai a $3k + 2$ alakú számok ($k \in \mathbb{Z}$).

Definíció (FGy2.2.1)

Rögzített m modulus esetén az m -mel osztva r maradékot adó számok halmazát az r **maradékosztályának** nevezzük mod m .
Ez tehát az $mk + r$ alakú számok halmaza, ahol $k \in \mathbb{Z}$.

Tétel (FGy2.5.3–4)

Az $ax \equiv b \pmod{m}$ pontosan akkor oldható meg, ha $(a, m) \mid b$.

Visszavezetés lineáris diofantikus egyenletre

Ismétlés: $8x \equiv 4 \pmod{6}$ megoldásai a $3k + 2$ alakú számok ($k \in \mathbb{Z}$).

Definíció (FGy2.2.1)

Rögzített m modulus esetén az m -mel osztva r maradékot adó számok halmazát az r **maradékosztályának** nevezzük mod m .
Ez tehát az $mk + r$ alakú számok halmaza, ahol $k \in \mathbb{Z}$.

Tétel (FGy2.5.3–4)

Az $ax \equiv b \pmod{m}$ pontosan akkor oldható meg, ha $(a, m) \mid b$.
Ilyenkor a megoldások egyetlen maradékosztályt alkotnak mod $m/(a, m)$.

Visszavezetés lineáris diofantikus egyenletre

Ismétlés: $8x \equiv 4 \pmod{6}$ megoldásai a $3k + 2$ alakú számok ($k \in \mathbb{Z}$).

Definíció (FGy2.2.1)

Rögzített m modulus esetén az m -mel osztva r maradékot adó számok halmazát az r **maradékosztályának** nevezzük mod m .
Ez tehát az $mk + r$ alakú számok halmaza, ahol $k \in \mathbb{Z}$.

Tétel (FGy2.5.3–4)

Az $ax \equiv b \pmod{m}$ pontosan akkor oldható meg, ha $(a, m) \mid b$.
Ilyenkor a megoldások egyetlen maradékosztályt alkotnak mod $m/(a, m)$. Ez (a, m) darab mod m maradékosztály egyesítése.

Visszavezetés lineáris diofantikus egyenletre

Ismétlés: $8x \equiv 4 \pmod{6}$ megoldásai a $3k + 2$ alakú számok ($k \in \mathbb{Z}$).

Definíció (FGy2.2.1)

Rögzített m modulus esetén az m -mel osztva r maradékot adó számok halmazát az r **maradékosztályának** nevezzük mod m . Ez tehát az $mk + r$ alakú számok halmaza, ahol $k \in \mathbb{Z}$.

Tétel (FGy2.5.3–4)

Az $ax \equiv b \pmod{m}$ pontosan akkor oldható meg, ha $(a, m) \mid b$. Ilyenkor a megoldások egyetlen maradékosztályt alkotnak mod $m/(a, m)$. Ez (a, m) darab mod m maradékosztály egyesítése.

Megoldhatóság: Nyilván $ax \equiv b \pmod{m}$ pontosan akkor, ha $m \mid ax - b$,

Visszavezetés lineáris diofantikus egyenletre

Ismétlés: $8x \equiv 4 \pmod{6}$ megoldásai a $3k + 2$ alakú számok ($k \in \mathbb{Z}$).

Definíció (FGy2.2.1)

Rögzített m modulus esetén az m -mel osztva r maradékot adó számok halmazát az r **maradékosztálynak** nevezzük mod m .
Ez tehát az $mk + r$ alakú számok halmaza, ahol $k \in \mathbb{Z}$.

Tétel (FGy2.5.3–4)

Az $ax \equiv b \pmod{m}$ pontosan akkor oldható meg, ha $(a, m) \mid b$.
Ilyenkor a megoldások egyetlen maradékosztályt alkotnak mod $m/(a, m)$. Ez (a, m) darab mod m maradékosztály egyesítése.

Megoldhatóság: Nyilván $ax \equiv b \pmod{m}$ pontosan akkor, ha $m \mid ax - b$, vagyis ha van olyan y egész, hogy $my = ax - b$.

Visszavezetés lineáris diofantikus egyenletre

Ismétlés: $8x \equiv 4 \pmod{6}$ megoldásai a $3k + 2$ alakú számok ($k \in \mathbb{Z}$).

Definíció (FGy2.2.1)

Rögzített m modulus esetén az m -mel osztva r maradékot adó számok halmazát az r **maradékosztálynak** nevezzük mod m . Ez tehát az $mk + r$ alakú számok halmaza, ahol $k \in \mathbb{Z}$.

Tétel (FGy2.5.3–4)

Az $ax \equiv b \pmod{m}$ pontosan akkor oldható meg, ha $(a, m) \mid b$. Ilyenkor a megoldások egyetlen maradékosztályt alkotnak mod $m/(a, m)$. Ez (a, m) darab mod m maradékosztály egyesítése.

Megoldhatóság: Nyilván $ax \equiv b \pmod{m}$ pontosan akkor, ha $m \mid ax - b$, vagyis ha van olyan y egész, hogy $my = ax - b$. Tanultuk, hogy az $ax - my = b$ lineáris diofantikus egyenlet pontosan akkor oldható meg, ha $(a, -m) = (a, m) \mid b$.

A megoldások halmaza

Tétel (FGy2.5.3–4)

Az $ax \equiv b \pmod{m}$ pontosan akkor oldható meg, ha $(a, m) \mid b$.

A megoldások halmaza

Tétel (FGy2.5.3–4)

Az $ax \equiv b \pmod{m}$ pontosan akkor oldható meg, ha $(a, m) \mid b$.
Ilyenkor a megoldások egyetlen maradékosztályt alkotnak
mod $m/(a, m)$.

A megoldások halmaza

Tétel (FGy2.5.3–4)

Az $ax \equiv b \pmod{m}$ pontosan akkor oldható meg, ha $(a, m) \mid b$.
Ilyenkor a megoldások egyetlen maradékosztályt alkotnak mod $m/(a, m)$.

Bizonyítás

Ha $ax \equiv b \pmod{m}$ megoldható, akkor $(a, m) \mid b$,

A megoldások halmaza

Tétel (FGy2.5.3–4)

Az $ax \equiv b \pmod{m}$ pontosan akkor oldható meg, ha $(a, m) \mid b$.
Ilyenkor a megoldások egyetlen maradékosztályt alkotnak mod $m/(a, m)$.

Bizonyítás

Ha $ax \equiv b \pmod{m}$ megoldható, akkor $(a, m) \mid b$, tehát egyszerűsíthetünk (a, m) -mel.

A megoldások halmaza

Tétel (FGy2.5.3–4)

Az $ax \equiv b \pmod{m}$ pontosan akkor oldható meg, ha $(a, m) \mid b$.
Ilyenkor a megoldások egyetlen maradékosztályt alkotnak mod $m/(a, m)$.

Bizonyítás

Ha $ax \equiv b \pmod{m}$ megoldható, akkor $(a, m) \mid b$, tehát egyszerűsíthetünk (a, m) -mel. Az eredmény $a'x \equiv b' \pmod{m'}$, ahol $m' = m/(a, m)$, $a' = a/(a, m)$ és $b' = b/(a, m)$.

A megoldások halmaza

Tétel (FGy2.5.3–4)

Az $ax \equiv b \pmod{m}$ pontosan akkor oldható meg, ha $(a, m) \mid b$.
Ilyenkor a megoldások egyetlen maradékosztályt alkotnak mod $m/(a, m)$.

Bizonyítás

Ha $ax \equiv b \pmod{m}$ megoldható, akkor $(a, m) \mid b$, tehát egyszerűsíthetünk (a, m) -mel. Az eredmény $a'x \equiv b' \pmod{m'}$, ahol $m' = m/(a, m)$, $a' = a/(a, m)$ és $b' = b/(a, m)$.
De $a' = a/(a, m)$ és $m' = m/(a, m)$ már relatív prímek.

A megoldások halmaza

Tétel (FGy2.5.3–4)

Az $ax \equiv b \pmod{m}$ pontosan akkor oldható meg, ha $(a, m) \mid b$.
Ilyenkor a megoldások egyetlen maradékosztályt alkotnak mod $m/(a, m)$.

Bizonyítás

Ha $ax \equiv b \pmod{m}$ megoldható, akkor $(a, m) \mid b$, tehát egyszerűsíthetünk (a, m) -mel. Az eredmény $a'x \equiv b' \pmod{m'}$, ahol $m' = m/(a, m)$, $a' = a/(a, m)$ és $b' = b/(a, m)$.
De $a' = a/(a, m)$ és $m' = m/(a, m)$ már relatív prímek.
Ha x_0 megoldás, akkor x akkor és csak akkor megoldás, ha $a'x \equiv b' \pmod{m'}$

A megoldások halmaza

Tétel (FGy2.5.3–4)

Az $ax \equiv b \pmod{m}$ pontosan akkor oldható meg, ha $(a, m) \mid b$.
Ilyenkor a megoldások egyetlen maradékosztályt alkotnak mod $m/(a, m)$.

Bizonyítás

Ha $ax \equiv b \pmod{m}$ megoldható, akkor $(a, m) \mid b$, tehát egyszerűsíthetünk (a, m) -mel. Az eredmény $a'x \equiv b' \pmod{m'}$, ahol $m' = m/(a, m)$, $a' = a/(a, m)$ és $b' = b/(a, m)$.
De $a' = a/(a, m)$ és $m' = m/(a, m)$ már relatív prímek.
Ha x_0 megoldás, akkor x akkor és csak akkor megoldás, ha $a'x \equiv b' \equiv a'x_0 \pmod{m'}$,

A megoldások halmaza

Tétel (FGy2.5.3–4)

Az $ax \equiv b \pmod{m}$ pontosan akkor oldható meg, ha $(a, m) \mid b$.
Ilyenkor a megoldások egyetlen maradékosztályt alkotnak mod $m/(a, m)$.

Bizonyítás

Ha $ax \equiv b \pmod{m}$ megoldható, akkor $(a, m) \mid b$, tehát egyszerűsíthetünk (a, m) -mel. Az eredmény $a'x \equiv b' \pmod{m'}$, ahol $m' = m/(a, m)$, $a' = a/(a, m)$ és $b' = b/(a, m)$.
De $a' = a/(a, m)$ és $m' = m/(a, m)$ már relatív prímek.
Ha x_0 megoldás, akkor x akkor és csak akkor megoldás, ha $a'x \equiv b' \equiv a'x_0 \pmod{m'}$, azaz ha $m' \mid a'(x - x_0)$.

A megoldások halmaza

Tétel (FGy2.5.3–4)

Az $ax \equiv b \pmod{m}$ pontosan akkor oldható meg, ha $(a, m) \mid b$.
Ilyenkor a megoldások egyetlen maradékosztályt alkotnak mod $m/(a, m)$.

Bizonyítás

Ha $ax \equiv b \pmod{m}$ megoldható, akkor $(a, m) \mid b$, tehát egyszerűsíthetünk (a, m) -mel. Az eredmény $a'x \equiv b' \pmod{m'}$, ahol $m' = m/(a, m)$, $a' = a/(a, m)$ és $b' = b/(a, m)$.
De $a' = a/(a, m)$ és $m' = m/(a, m)$ már relatív prímek.
Ha x_0 megoldás, akkor x akkor és csak akkor megoldás, ha $a'x \equiv b' \equiv a'x_0 \pmod{m'}$, azaz ha $m' \mid a'(x - x_0)$.
Mivel $(a', m') = 1$, ez azzal ekvivalens, hogy $m' \mid x - x_0$.

A megoldások halmaza

Tétel (FGy2.5.3–4)

Az $ax \equiv b \pmod{m}$ pontosan akkor oldható meg, ha $(a, m) \mid b$.
Ilyenkor a megoldások egyetlen maradékosztályt alkotnak mod $m/(a, m)$.

Bizonyítás

Ha $ax \equiv b \pmod{m}$ megoldható, akkor $(a, m) \mid b$, tehát egyszerűsíthetünk (a, m) -mel. Az eredmény $a'x \equiv b' \pmod{m'}$, ahol $m' = m/(a, m)$, $a' = a/(a, m)$ és $b' = b/(a, m)$.

De $a' = a/(a, m)$ és $m' = m/(a, m)$ már relatív prímek.

Ha x_0 megoldás, akkor x akkor és csak akkor megoldás,

ha $a'x \equiv b' \equiv a'x_0 \pmod{m'}$, azaz ha $m' \mid a'(x - x_0)$.

Mivel $(a', m') = 1$, ez azzal ekvivalens, hogy $m' \mid x - x_0$.

Így a megoldások az x_0 szám mod m' maradékosztályának elemei.

A megoldás maradékosztályok egyesítése

Minden mod $m/(a, m)$ maradékosztály (a, m) darab mod m maradékosztály egyesítése.

A megoldás maradékosztályok egyesítése

Minden mod $m/(a, m)$ maradékosztály (a, m) darab mod m maradékosztály egyesítése.

Például a $3k + 2$ alakú számok két maradékosztályt alkotnak mod 6:

A megoldás maradékosztályok egyesítése

Minden mod $m/(a, m)$ maradékosztály (a, m) darab mod m maradékosztály egyesítése.

Például a $3k + 2$ alakú számok két maradékosztályt alkotnak mod 6: a 2 és az 5 maradékosztályát.

A megoldás maradékosztályok egyesítése

Minden mod $m/(a, m)$ maradékosztály (a, m) darab mod m maradékosztály egyesítése.

Például a $3k + 2$ alakú számok két maradékosztályt alkotnak mod 6: a 2 és az 5 maradékosztályát.

Bizonyítás

Legyen $d = (a, m)$, és $m' = m/(a, m)$.

A megoldás maradékosztályok egyesítése

Minden mod $m/(a, m)$ maradékosztály (a, m) darab mod m maradékosztály egyesítése.

Például a $3k + 2$ alakú számok két maradékosztályt alkotnak mod 6: a 2 és az 5 maradékosztályát.

Bizonyítás

Legyen $d = (a, m)$, és $m' = m/(a, m)$. Megmutatjuk, hogy az x_0 mod (m') maradékosztálya az x_0, x_1, \dots, x_{d-1} számok mod m maradékosztályainak egyesítése,

A megoldás maradékosztályok egyesítése

Minden mod $m/(a, m)$ maradékosztály (a, m) darab mod m maradékosztály egyesítése.

Például a $3k + 2$ alakú számok két maradékosztályt alkotnak mod 6: a 2 és az 5 maradékosztályát.

Bizonyítás

Legyen $d = (a, m)$, és $m' = m/(a, m)$. Megmutatjuk, hogy az x_0 mod (m') maradékosztálya az x_0, x_1, \dots, x_{d-1} számok mod m maradékosztályainak egyesítése, ahol $x_1 = x_0 + m'$, $x_2 = x_0 + 2m'$, \dots , $x_{d-1} = x_0 + (d-1)m'$.

A megoldás maradékosztályok egyesítése

Minden mod $m/(a, m)$ maradékosztály (a, m) darab mod m maradékosztály egyesítése.

Például a $3k + 2$ alakú számok két maradékosztályt alkotnak mod 6: a 2 és az 5 maradékosztályát.

Bizonyítás

Legyen $d = (a, m)$, és $m' = m/(a, m)$. Megmutatjuk, hogy az x_0 mod (m') maradékosztálya az x_0, x_1, \dots, x_{d-1} számok mod m maradékosztályainak egyesítése, ahol $x_1 = x_0 + m'$, $x_2 = x_0 + 2m'$, \dots , $x_{d-1} = x_0 + (d-1)m'$.
Ha $x \equiv x_0 \pmod{m'}$, akkor $x = x_0 + m'k$ alkalmas k -ra.

A megoldás maradékosztályok egyesítése

Minden mod $m/(a, m)$ maradékosztály (a, m) darab mod m maradékosztály egyesítése.

Például a $3k + 2$ alakú számok két maradékosztályt alkotnak mod 6: a 2 és az 5 maradékosztályát.

Bizonyítás

Legyen $d = (a, m)$, és $m' = m/(a, m)$. Megmutatjuk, hogy az x_0 mod (m') maradékosztálya az x_0, x_1, \dots, x_{d-1} számok mod m maradékosztályainak egyesítése, ahol $x_1 = x_0 + m'$, $x_2 = x_0 + 2m'$, \dots , $x_{d-1} = x_0 + (d-1)m'$.
Ha $x \equiv x_0 \pmod{m'}$, akkor $x = x_0 + m'k$ alkalmas k -ra. Legyen $k = dq + r$, ahol $0 \leq r \leq d-1$.

A megoldás maradékosztályok egyesítése

Minden mod $m/(a, m)$ maradékosztály (a, m) darab mod m maradékosztály egyesítése.

Például a $3k + 2$ alakú számok két maradékosztályt alkotnak mod 6: a 2 és az 5 maradékosztályát.

Bizonyítás

Legyen $d = (a, m)$, és $m' = m/(a, m)$. Megmutatjuk, hogy az x_0 mod (m') maradékosztálya az x_0, x_1, \dots, x_{d-1} számok mod m maradékosztályainak egyesítése, ahol $x_1 = x_0 + m'$, $x_2 = x_0 + 2m'$, \dots , $x_{d-1} = x_0 + (d-1)m'$.
Ha $x \equiv x_0 \pmod{m'}$, akkor $x = x_0 + m'k$ alkalmas k -ra. Legyen $k = dq + r$, ahol $0 \leq r \leq d-1$. Belátjuk, hogy $x \equiv x_r \pmod{m}$.

A megoldás maradékosztályok egyesítése

Minden mod $m/(a, m)$ maradékosztály (a, m) darab mod m maradékosztály egyesítése.

Például a $3k + 2$ alakú számok két maradékosztályt alkotnak mod 6: a 2 és az 5 maradékosztályát.

Bizonyítás

Legyen $d = (a, m)$, és $m' = m/(a, m)$. Megmutatjuk, hogy az x_0 mod (m') maradékosztálya az x_0, x_1, \dots, x_{d-1} számok mod m maradékosztályainak egyesítése, ahol

$$x_1 = x_0 + m', x_2 = x_0 + 2m', \dots, x_{d-1} = x_0 + (d-1)m'.$$

Ha $x \equiv x_0 \pmod{m'}$, akkor $x = x_0 + m'k$ alkalmas k -ra. Legyen

$k = dq + r$, ahol $0 \leq r \leq d-1$. Belátjuk, hogy $x \equiv x_r \pmod{m}$.

Valóban, $x = m'k + x_0 = m'dq + m'r + x_0$

A megoldás maradékosztályok egyesítése

Minden mod $m/(a, m)$ maradékosztály (a, m) darab mod m maradékosztály egyesítése.

Például a $3k + 2$ alakú számok két maradékosztályt alkotnak mod 6: a 2 és az 5 maradékosztályát.

Bizonyítás

Legyen $d = (a, m)$, és $m' = m/(a, m)$. Megmutatjuk, hogy az x_0 mod (m') maradékosztálya az x_0, x_1, \dots, x_{d-1} számok mod m maradékosztályainak egyesítése, ahol

$$x_1 = x_0 + m', x_2 = x_0 + 2m', \dots, x_{d-1} = x_0 + (d-1)m'.$$

Ha $x \equiv x_0 \pmod{m'}$, akkor $x = x_0 + m'k$ alkalmas k -ra. Legyen

$k = dq + r$, ahol $0 \leq r \leq d-1$. Belátjuk, hogy $x \equiv x_r \pmod{m}$.

Valóban, $x = m'k + x_0 = m'dq + m'r + x_0 = mq + x_r$

A megoldás maradékosztályok egyesítése

Minden mod $m/(a, m)$ maradékosztály (a, m) darab mod m maradékosztály egyesítése.

Például a $3k + 2$ alakú számok két maradékosztályt alkotnak mod 6: a 2 és az 5 maradékosztályát.

Bizonyítás

Legyen $d = (a, m)$, és $m' = m/(a, m)$. Megmutatjuk, hogy az x_0 mod (m') maradékosztálya az x_0, x_1, \dots, x_{d-1} számok mod m maradékosztályainak egyesítése, ahol

$$x_1 = x_0 + m', x_2 = x_0 + 2m', \dots, x_{d-1} = x_0 + (d-1)m'.$$

Ha $x \equiv x_0 \pmod{m'}$, akkor $x = x_0 + m'k$ alkalmas k -ra. Legyen

$k = dq + r$, ahol $0 \leq r \leq d-1$. Belátjuk, hogy $x \equiv x_r \pmod{m}$.

Valóban, $x = m'k + x_0 = m'dq + m'r + x_0 = mq + x_r \equiv x_r \pmod{m}$.

A megoldás maradékosztályok egyesítése

Minden mod $m/(a, m)$ maradékosztály (a, m) darab mod m maradékosztály egyesítése.

Például a $3k + 2$ alakú számok két maradékosztályt alkotnak mod 6: a 2 és az 5 maradékosztályát.

Bizonyítás

Legyen $d = (a, m)$, és $m' = m/(a, m)$. Megmutatjuk, hogy az x_0 mod (m') maradékosztálya az x_0, x_1, \dots, x_{d-1} számok mod m maradékosztályainak egyesítése, ahol

$$x_1 = x_0 + m', x_2 = x_0 + 2m', \dots, x_{d-1} = x_0 + (d-1)m'.$$

Ha $x \equiv x_0 \pmod{m'}$, akkor $x = x_0 + m'k$ alkalmas k -ra. Legyen

$k = dq + r$, ahol $0 \leq r \leq d-1$. Belátjuk, hogy $x \equiv x_r \pmod{m}$.

Valóban, $x = m'k + x_0 = m'dq + m'r + x_0 = mq + x_r \equiv x_r \pmod{m}$.

Megfordítva, ha $x \equiv x_r \pmod{m}$, akkor $x \equiv x_r \equiv x_0 \pmod{m'}$,

A megoldás maradékosztályok egyesítése

Minden mod $m/(a, m)$ maradékosztály (a, m) darab mod m maradékosztály egyesítése.

Például a $3k + 2$ alakú számok két maradékosztályt alkotnak mod 6: a 2 és az 5 maradékosztályát.

Bizonyítás

Legyen $d = (a, m)$, és $m' = m/(a, m)$. Megmutatjuk, hogy az x_0 mod (m') maradékosztálya az x_0, x_1, \dots, x_{d-1} számok mod m maradékosztályainak egyesítése, ahol

$$x_1 = x_0 + m', x_2 = x_0 + 2m', \dots, x_{d-1} = x_0 + (d-1)m'.$$

Ha $x \equiv x_0 \pmod{m'}$, akkor $x = x_0 + m'k$ alkalmas k -ra. Legyen

$k = dq + r$, ahol $0 \leq r \leq d-1$. Belátjuk, hogy $x \equiv x_r \pmod{m}$.

Valóban, $x = m'k + x_0 = m'dq + m'r + x_0 = mq + x_r \equiv x_r \pmod{m}$.

Megfordítva, ha $x \equiv x_r \pmod{m}$, akkor $x \equiv x_r \equiv x_0 \pmod{m'}$, hiszen $m' \mid m$.

Megoldás euklideszi algoritmussal

Lásd FGy7.1.1, ill. 2.5. szakasz

Oldjuk meg a $14x \equiv 2 \pmod{34}$ kongruenciát.

Megoldás euklideszi algoritmussal

Lásd FGy7.1.1, ill. 2.5. szakasz

Oldjuk meg a $14x \equiv 2 \pmod{34}$ kongruenciát.

Első lépésként átírjuk diofantikus egyenletre: $14x - 2 = 34y$.

Megoldás euklideszi algoritmussal

Lásd FGy7.1.1, ill. 2.5. szakasz

Oldjuk meg a $14x \equiv 2 \pmod{34}$ kongruenciát.

Első lépésként átírjuk diofantikus egyenletre: $14x - 2 = 34y$.

Kifejezzük a kisebbik együtthatójú ismeretlent: $x = (34y + 2)/14$.

Megoldás euklideszi algoritmussal

Lásd FGy7.1.1, ill. 2.5. szakasz

Oldjuk meg a $14x \equiv 2 \pmod{34}$ kongruenciát.

Első lépésként átírjuk diofantikus egyenletre: $14x - 2 = 34y$.

Kifejezzük a kisebbik együtthatójú ismeretlent: $x = (34y + 2)/14$.

Elvégezzük az osztást: $34 = 2 \cdot 14 + 6$,

Megoldás euklideszi algoritmussal

Lásd FGy7.1.1, ill. 2.5. szakasz

Oldjuk meg a $14x \equiv 2 \pmod{34}$ kongruenciát.

Első lépésként átírjuk diofantikus egyenletre: $14x - 2 = 34y$.

Kifejezzük a kisebbik együtthatójú ismeretlent: $x = (34y + 2)/14$.

Elvégezzük az osztást: $34 = 2 \cdot 14 + 6$, így $x = 2y + (6y + 2)/14$.

Megoldás euklideszi algoritmussal

Lásd FGy7.1.1, ill. 2.5. szakasz

Oldjuk meg a $14x \equiv 2 \pmod{34}$ kongruenciát.

Első lépésként átírjuk diofantikus egyenletre: $14x - 2 = 34y$.

Kifejezzük a kisebbik együtthatójú ismeretlent: $x = (34y + 2)/14$.

Elvégezzük az osztást: $34 = 2 \cdot 14 + 6$, így $x = 2y + (6y + 2)/14$.

Bevezetjük a $z = (6y + 2)/14 = (3y + 1)/7$ új (egész) ismeretlent.

Megoldás euklideszi algoritmussal

Lásd FGy7.1.1, ill. 2.5. szakasz

Oldjuk meg a $14x \equiv 2 \pmod{34}$ kongruenciát.

Első lépésként átírjuk diofantikus egyenletre: $14x - 2 = 34y$.

Kifejezzük a kisebbik együtthatójú ismeretlent: $x = (34y + 2)/14$.

Elvégezzük az osztást: $34 = 2 \cdot 14 + 6$, így $x = 2y + (6y + 2)/14$.

Bevezetjük a $z = (6y + 2)/14 = (3y + 1)/7$ új (egész) ismeretlent.

Ekkor $7z = 3y + 1$, ahol z is egész.

Megoldás euklideszi algoritmussal

Lásd FGy7.1.1, ill. 2.5. szakasz

Oldjuk meg a $14x \equiv 2 \pmod{34}$ kongruenciát.

Első lépésként átírjuk diofantikus egyenletre: $14x - 2 = 34y$.

Kifejezzük a kisebbik együtthatójú ismeretlent: $x = (34y + 2)/14$.

Elvégezzük az osztást: $34 = 2 \cdot 14 + 6$, így $x = 2y + (6y + 2)/14$.

Bevezetjük a $z = (6y + 2)/14 = (3y + 1)/7$ új (egész) ismeretlent.

Ekkor $7z = 3y + 1$, ahol z is egész. Ismételjük az eljárást.

Megoldás euklideszi algoritmussal

Lásd FGy7.1.1, ill. 2.5. szakasz

Oldjuk meg a $14x \equiv 2 \pmod{34}$ kongruenciát.

Első lépésként átírjuk diofantikus egyenletre: $14x - 2 = 34y$.

Kifejezzük a kisebbik együtthatójú ismeretlent: $x = (34y + 2)/14$.

Elvégezzük az osztást: $34 = 2 \cdot 14 + 6$, így $x = 2y + (6y + 2)/14$.

Bevezetjük a $z = (6y + 2)/14 = (3y + 1)/7$ új (egész) ismeretlent.

Ekkor $7z = 3y + 1$, ahol z is egész. Ismételjük az eljárást.

$y = (7z - 1)/3 = 2z + u$, ahol $u = (z - 1)/3$.

Megoldás euklideszi algoritmussal

Lásd FGy7.1.1, ill. 2.5. szakasz

Oldjuk meg a $14x \equiv 2 \pmod{34}$ kongruenciát.

Első lépésként átírjuk diofantikus egyenletre: $14x - 2 = 34y$.

Kifejezzük a kisebbik együtthatójú ismeretlent: $x = (34y + 2)/14$.

Elvégezzük az osztást: $34 = 2 \cdot 14 + 6$, így $x = 2y + (6y + 2)/14$.

Bevezetjük a $z = (6y + 2)/14 = (3y + 1)/7$ új (egész) ismeretlent.

Ekkor $7z = 3y + 1$, ahol z is egész. Ismételjük az eljárást.

$y = (7z - 1)/3 = 2z + u$, ahol $u = (z - 1)/3$.

Tehát $3u = z - 1$,

Megoldás euklideszi algoritmussal

Lásd FGy7.1.1, ill. 2.5. szakasz

Oldjuk meg a $14x \equiv 2 \pmod{34}$ kongruenciát.

Első lépésként átírjuk diofantikus egyenletre: $14x - 2 = 34y$.

Kifejezzük a kisebbik együtthatójú ismeretlent: $x = (34y + 2)/14$.

Elvégezzük az osztást: $34 = 2 \cdot 14 + 6$, így $x = 2y + (6y + 2)/14$.

Bevezetjük a $z = (6y + 2)/14 = (3y + 1)/7$ új (egész) ismeretlent.

Ekkor $7z = 3y + 1$, ahol z is egész. Ismételjük az eljárást.

$y = (7z - 1)/3 = 2z + u$, ahol $u = (z - 1)/3$.

Tehát $3u = z - 1$, azaz $z = 3u + 1$.

Megoldás euklideszi algoritmussal

Lásd FGy7.1.1, ill. 2.5. szakasz

Oldjuk meg a $14x \equiv 2 \pmod{34}$ kongruenciát.

Első lépésként átírjuk diofantikus egyenletre: $14x - 2 = 34y$.

Kifejezzük a kisebbik együtthatójú ismeretlent: $x = (34y + 2)/14$.

Elvégezzük az osztást: $34 = 2 \cdot 14 + 6$, így $x = 2y + (6y + 2)/14$.

Bevezetjük a $z = (6y + 2)/14 = (3y + 1)/7$ új (egész) ismeretlent.

Ekkor $7z = 3y + 1$, ahol z is egész. Ismételjük az eljárást.

$y = (7z - 1)/3 = 2z + u$, ahol $u = (z - 1)/3$.

Tehát $3u = z - 1$, azaz $z = 3u - 1$. Itt már nem szerepelnek törtek, ezért megállunk, majd sorban visszahelyettesítjük az ismeretleneket.

Megoldás euklideszi algoritmussal

Lásd FGy7.1.1, ill. 2.5. szakasz

Oldjuk meg a $14x \equiv 2 \pmod{34}$ kongruenciát.

Első lépésként átírjuk diofantikus egyenletre: $14x - 2 = 34y$.

Kifejezzük a kisebbik együtthatójú ismeretlent: $x = (34y + 2)/14$.

Elvégezzük az osztást: $34 = 2 \cdot 14 + 6$, így $x = 2y + (6y + 2)/14$.

Bevezetjük a $z = (6y + 2)/14 = (3y + 1)/7$ új (egész) ismeretlent.

Ekkor $7z = 3y + 1$, ahol z is egész. Ismételjük az eljárást.

$y = (7z - 1)/3 = 2z + u$, ahol $u = (z - 1)/3$.

Tehát $3u = z - 1$, azaz $z = 3u + 1$. Itt már nem szerepelnek törtek, ezért megállunk, majd sorban visszahelyettesítjük az ismeretleneket.

$y = 2z + u = 6u + 2 + u = 7u + 2$.

Megoldás euklideszi algoritmussal

Lásd FGy7.1.1, ill. 2.5. szakasz

Oldjuk meg a $14x \equiv 2 \pmod{34}$ kongruenciát.

Első lépésként átírjuk diofantikus egyenletre: $14x - 2 = 34y$.

Kifejezzük a kisebbik együtthatójú ismeretlent: $x = (34y + 2)/14$.

Elvégezzük az osztást: $34 = 2 \cdot 14 + 6$, így $x = 2y + (6y + 2)/14$.

Bevezetjük a $z = (6y + 2)/14 = (3y + 1)/7$ új (egész) ismeretlent.

Ekkor $7z = 3y + 1$, ahol z is egész. Ismételjük az eljárást.

$y = (7z - 1)/3 = 2z + u$, ahol $u = (z - 1)/3$.

Tehát $3u = z - 1$, azaz $z = 3u + 1$. Itt már nem szerepelnek törtek, ezért megállunk, majd sorban visszahelyettesítjük az ismeretleneket.

$y = 2z + u = 6u + 2 + u = 7u + 2$.

$x = 2y + z = (14u + 4) + (3u + 1) = 17u + 5$.

Megoldás euklideszi algoritmussal

Lásd FGy7.1.1, ill. 2.5. szakasz

Oldjuk meg a $14x \equiv 2 \pmod{34}$ kongruenciát.

Első lépésként átírjuk diofantikus egyenletre: $14x - 2 = 34y$.

Kifejezzük a kisebbik együtthatójú ismeretlent: $x = (34y + 2)/14$.

Elvégezzük az osztást: $34 = 2 \cdot 14 + 6$, így $x = 2y + (6y + 2)/14$.

Bevezetjük a $z = (6y + 2)/14 = (3y + 1)/7$ új (egész) ismeretlent.

Ekkor $7z = 3y + 1$, ahol z is egész. Ismételjük az eljárást.

$y = (7z - 1)/3 = 2z + u$, ahol $u = (z - 1)/3$.

Tehát $3u = z - 1$, azaz $z = 3u + 1$. Itt már nem szerepelnek törtek, ezért megállunk, majd sorban visszahelyettesítjük az ismeretleneket.

$y = 2z + u = 6u + 2 + u = 7u + 2$.

$x = 2y + z = (14u + 4) + (3u + 1) = 17u + 5$.

Ellenőrzés: $14(17u + 5) - 2 = 34(7u + 2)$ tényleg azonosság.

Megoldás euklideszi algoritmussal

Lásd FGy7.1.1, ill. 2.5. szakasz

Oldjuk meg a $14x \equiv 2 \pmod{34}$ kongruenciát.

Első lépésként átírjuk diofantikus egyenletre: $14x - 2 = 34y$.

Kifejezzük a kisebbik együtthatójú ismeretlent: $x = (34y + 2)/14$.

Elvégezzük az osztást: $34 = 2 \cdot 14 + 6$, így $x = 2y + (6y + 2)/14$.

Bevezetjük a $z = (6y + 2)/14 = (3y + 1)/7$ új (egész) ismeretlent.

Ekkor $7z = 3y + 1$, ahol z is egész. Ismételjük az eljárást.

$y = (7z - 1)/3 = 2z + u$, ahol $u = (z - 1)/3$.

Tehát $3u = z - 1$, azaz $z = 3u + 1$. Itt már nem szerepelnek törtek, ezért megállunk, majd sorban visszahelyettesítjük az ismeretleneket.

$y = 2z + u = 6u + 2 + u = 7u + 2$.

$x = 2y + z = (14u + 4) + (3u + 1) = 17u + 5$.

Ellenőrzés: $14(17u + 5) - 2 = 34(7u + 2)$ tényleg azonosság.

Így $14x \equiv 2 \pmod{34}$ megoldásai a $17u + 5$ alakú számok,

Megoldás euklideszi algoritmussal

Lásd FGy7.1.1, ill. 2.5. szakasz

Oldjuk meg a $14x \equiv 2 \pmod{34}$ kongruenciát.

Első lépésként átírjuk diofantikus egyenletre: $14x - 2 = 34y$.

Kifejezzük a kisebbik együtthatójú ismeretlent: $x = (34y + 2)/14$.

Elvégezzük az osztást: $34 = 2 \cdot 14 + 6$, így $x = 2y + (6y + 2)/14$.

Bevezetjük a $z = (6y + 2)/14 = (3y + 1)/7$ új (egész) ismeretlent.

Ekkor $7z = 3y + 1$, ahol z is egész. Ismételjük az eljárást.

$y = (7z - 1)/3 = 2z + u$, ahol $u = (z - 1)/3$.

Tehát $3u = z - 1$, azaz $z = 3u + 1$. Itt már nem szerepelnek törtek, ezért megállunk, majd sorban visszahelyettesítjük az ismeretleneket.

$y = 2z + u = 6u + 2 + u = 7u + 2$.

$x = 2y + z = (14u + 4) + (3u + 1) = 17u + 5$.

Ellenőrzés: $14(17u + 5) - 2 = 34(7u + 2)$ tényleg azonosság.

Így $14x \equiv 2 \pmod{34}$ megoldásai a $17u + 5$ alakú számok, vagyis 5 maradékosztálya mod 17.

Szimultán kongruenciarendszer

Tétel (FGy2.6.1)

Az $x \equiv c_1 \pmod{m_1}$ és $x \equiv c_2 \pmod{m_2}$ kongruenciákból álló rendszer pontosan akkor oldható meg, ha $(m_1, m_2) \mid c_1 - c_2$.

Szimultán kongruenciarendszer

Tétel (FGy2.6.1)

Az $x \equiv c_1 \pmod{m_1}$ és $x \equiv c_2 \pmod{m_2}$ kongruenciákból álló rendszer pontosan akkor oldható meg, ha $(m_1, m_2) \mid c_1 - c_2$.
Ilyenkor a megoldás egyetlen maradékosztály mod $[m_1, m_2]$.

Szimultán kongruenciarendszer

Tétel (FGy2.6.1)

Az $x \equiv c_1 \pmod{m_1}$ és $x \equiv c_2 \pmod{m_2}$ kongruenciákból álló rendszer pontosan akkor oldható meg, ha $(m_1, m_2) \mid c_1 - c_2$.
Ilyenkor a megoldás egyetlen maradékosztály mod $[m_1, m_2]$.

Bizonyítás

A két kongruencia átírható $x = c_1 + ym_1$ és $x = c_2 + zm_2$ alakba alkalmas $y, z \in \mathbb{Z}$ -re,

Szimultán kongruenciarendszer

Tétel (FGy2.6.1)

Az $x \equiv c_1 \pmod{m_1}$ és $x \equiv c_2 \pmod{m_2}$ kongruenciákból álló rendszer pontosan akkor oldható meg, ha $(m_1, m_2) \mid c_1 - c_2$.
Ilyenkor a megoldás egyetlen maradékosztály mod $[m_1, m_2]$.

Bizonyítás

A két kongruencia átírható $x = c_1 + ym_1$ és $x = c_2 + zm_2$ alakba alkalmas $y, z \in \mathbb{Z}$ -re, ahonnan $ym_1 - zm_2 = c_2 - c_1$.

Szimultán kongruenciarendszer

Tétel (FGy2.6.1)

Az $x \equiv c_1 \pmod{m_1}$ és $x \equiv c_2 \pmod{m_2}$ kongruenciákból álló rendszer pontosan akkor oldható meg, ha $(m_1, m_2) \mid c_1 - c_2$.
Ilyenkor a megoldás egyetlen maradékosztály mod $[m_1, m_2]$.

Bizonyítás

A két kongruencia átírható $x = c_1 + ym_1$ és $x = c_2 + zm_2$ alakba alkalmas $y, z \in \mathbb{Z}$ -re, ahonnan $ym_1 - zm_2 = c_2 - c_1$.
Ezért ha van megoldás, akkor $(m_1, m_2) \mid c_1 - c_2$.

Szimultán kongruenciarendszer

Tétel (FGy2.6.1)

Az $x \equiv c_1 \pmod{m_1}$ és $x \equiv c_2 \pmod{m_2}$ kongruenciákból álló rendszer pontosan akkor oldható meg, ha $(m_1, m_2) \mid c_1 - c_2$.
Ilyenkor a megoldás egyetlen maradékosztály mod $[m_1, m_2]$.

Bizonyítás

A két kongruencia átírható $x = c_1 + ym_1$ és $x = c_2 + zm_2$ alakba alkalmas $y, z \in \mathbb{Z}$ -re, ahonnan $ym_1 - zm_2 = c_2 - c_1$.

Ezért ha van megoldás, akkor $(m_1, m_2) \mid c_1 - c_2$.

Megfordítva, ha a diofantikus egyenletnek van megoldása, akkor $x = c_1 + ym_1 = c_2 + zm_2$ megoldása a kongruenciarendszernek.

Szimultán kongruenciarendszer

Tétel (FGy2.6.1)

Az $x \equiv c_1 \pmod{m_1}$ és $x \equiv c_2 \pmod{m_2}$ kongruenciákból álló rendszer pontosan akkor oldható meg, ha $(m_1, m_2) \mid c_1 - c_2$.
Ilyenkor a megoldás egyetlen maradékosztály mod $[m_1, m_2]$.

Bizonyítás

A két kongruencia átírható $x = c_1 + ym_1$ és $x = c_2 + zm_2$ alakba alkalmas $y, z \in \mathbb{Z}$ -re, ahonnan $ym_1 - zm_2 = c_2 - c_1$.

Ezért ha van megoldás, akkor $(m_1, m_2) \mid c_1 - c_2$.

Megfordítva, ha a diofantikus egyenletnek van megoldása, akkor $x = c_1 + ym_1 = c_2 + zm_2$ megoldása a kongruenciarendszernek.

Ha x_0 megoldás, akkor x pontosan akkor lesz megoldás, ha $x \equiv c_1 \equiv x_0 \pmod{m_1}$

Szimultán kongruenciarendszer

Tétel (FGy2.6.1)

Az $x \equiv c_1 \pmod{m_1}$ és $x \equiv c_2 \pmod{m_2}$ kongruenciákból álló rendszer pontosan akkor oldható meg, ha $(m_1, m_2) \mid c_1 - c_2$.
Ilyenkor a megoldás egyetlen maradékosztály mod $[m_1, m_2]$.

Bizonyítás

A két kongruencia átírható $x = c_1 + ym_1$ és $x = c_2 + zm_2$ alakba alkalmas $y, z \in \mathbb{Z}$ -re, ahonnan $ym_1 - zm_2 = c_2 - c_1$.

Ezért ha van megoldás, akkor $(m_1, m_2) \mid c_1 - c_2$.

Megfordítva, ha a diofantikus egyenletnek van megoldása, akkor $x = c_1 + ym_1 = c_2 + zm_2$ megoldása a kongruenciarendszernek.

Ha x_0 megoldás, akkor x pontosan akkor lesz megoldás, ha $x \equiv c_1 \equiv x_0 \pmod{m_1}$ és $x \equiv c_2 \equiv x_0 \pmod{m_2}$,

Szimultán kongruenciarendszer

Tétel (FGy2.6.1)

Az $x \equiv c_1 \pmod{m_1}$ és $x \equiv c_2 \pmod{m_2}$ kongruenciákból álló rendszer pontosan akkor oldható meg, ha $(m_1, m_2) \mid c_1 - c_2$.
Ilyenkor a megoldás egyetlen maradékosztály mod $[m_1, m_2]$.

Bizonyítás

A két kongruencia átírható $x = c_1 + ym_1$ és $x = c_2 + zm_2$ alakba alkalmas $y, z \in \mathbb{Z}$ -re, ahonnan $ym_1 - zm_2 = c_2 - c_1$.

Ezért ha van megoldás, akkor $(m_1, m_2) \mid c_1 - c_2$.

Megfordítva, ha a diofantikus egyenletnek van megoldása, akkor $x = c_1 + ym_1 = c_2 + zm_2$ megoldása a kongruenciarendszernek.

Ha x_0 megoldás, akkor x pontosan akkor lesz megoldás, ha $x \equiv c_1 \equiv x_0 \pmod{m_1}$ és $x \equiv c_2 \equiv x_0 \pmod{m_2}$, azaz ha $m_1 \mid x - x_0$

Szimultán kongruenciarendszer

Tétel (FGy2.6.1)

Az $x \equiv c_1 \pmod{m_1}$ és $x \equiv c_2 \pmod{m_2}$ kongruenciákból álló rendszer pontosan akkor oldható meg, ha $(m_1, m_2) \mid c_1 - c_2$.
Ilyenkor a megoldás egyetlen maradékosztály mod $[m_1, m_2]$.

Bizonyítás

A két kongruencia átírható $x = c_1 + ym_1$ és $x = c_2 + zm_2$ alakba alkalmas $y, z \in \mathbb{Z}$ -re, ahonnan $ym_1 - zm_2 = c_2 - c_1$.

Ezért ha van megoldás, akkor $(m_1, m_2) \mid c_1 - c_2$.

Megfordítva, ha a diofantikus egyenletnek van megoldása, akkor $x = c_1 + ym_1 = c_2 + zm_2$ megoldása a kongruenciarendszernek.

Ha x_0 megoldás, akkor x pontosan akkor lesz megoldás, ha $x \equiv c_1 \equiv x_0 \pmod{m_1}$ és $x \equiv c_2 \equiv x_0 \pmod{m_2}$, azaz ha $m_1 \mid x - x_0$ és $m_2 \mid x - x_0$.

Szimultán kongruenciarendszer

Tétel (FGy2.6.1)

Az $x \equiv c_1 \pmod{m_1}$ és $x \equiv c_2 \pmod{m_2}$ kongruenciákból álló rendszer pontosan akkor oldható meg, ha $(m_1, m_2) \mid c_1 - c_2$.
Ilyenkor a megoldás egyetlen maradékosztály mod $[m_1, m_2]$.

Bizonyítás

A két kongruencia átírható $x = c_1 + ym_1$ és $x = c_2 + zm_2$ alakba alkalmas $y, z \in \mathbb{Z}$ -re, ahonnan $ym_1 - zm_2 = c_2 - c_1$.

Ezért ha van megoldás, akkor $(m_1, m_2) \mid c_1 - c_2$.

Megfordítva, ha a diofantikus egyenletnek van megoldása, akkor $x = c_1 + ym_1 = c_2 + zm_2$ megoldása a kongruenciarendszernek.

Ha x_0 megoldás, akkor x pontosan akkor lesz megoldás, ha $x \equiv c_1 \equiv x_0 \pmod{m_1}$ és $x \equiv c_2 \equiv x_0 \pmod{m_2}$, azaz ha $m_1 \mid x - x_0$ és $m_2 \mid x - x_0$. Ez azzal ekvivalens, hogy $[m_1, m_2] \mid x - x_0$. □

A kínai maradéktétel

Ha m_1 és m_2 relatív prímelek, akkor az $x \equiv c_1 \pmod{m_1}$, $x \equiv c_2 \pmod{m_2}$ rendszernek mindig van megoldása,

A kínai maradéktétel

Ha m_1 és m_2 relatív prímelek, akkor az $x \equiv c_1 \pmod{m_1}$, $x \equiv c_2 \pmod{m_2}$ rendszernek mindig van megoldása, és a megoldás mod $[m_1, m_2] = m_1 m_2$ lesz egyértelmű (előző tétel).

A kínai maradéktétel

Ha m_1 és m_2 relatív prímelek, akkor az $x \equiv c_1 (m_1)$, $x \equiv c_2 (m_2)$ rendszernek mindig van megoldása, és a megoldás mod $[m_1, m_2] = m_1 m_2$ lesz egyértelmű (előző tétel).

Kínai maradéktétel (FGy2.6.2)

Tegyük fel, hogy m_1, m_2, \dots, m_n páronként relatív prímelek. Ekkor az $x \equiv c_1 (m_1), \dots, x \equiv c_n (m_n)$ rendszernek van megoldása,

A kínai maradéktétel

Ha m_1 és m_2 relatív prímek, akkor az $x \equiv c_1 (m_1)$, $x \equiv c_2 (m_2)$ rendszernek mindig van megoldása, és a megoldás mod $[m_1, m_2] = m_1 m_2$ lesz egyértelmű (előző tétel).

Kínai maradéktétel (FGy2.6.2)

Tegyük fel, hogy m_1, m_2, \dots, m_n páronként relatív prímek. Ekkor az $x \equiv c_1 (m_1), \dots, x \equiv c_n (m_n)$ rendszernek van megoldása, és a megoldások egy mod $m_1 \dots m_n$ maradékosztályt alkotnak.

A kínai maradéktétel

Ha m_1 és m_2 relatív prímek, akkor az $x \equiv c_1 (m_1)$, $x \equiv c_2 (m_2)$ rendszernek mindig van megoldása, és a megoldás mod $[m_1, m_2] = m_1 m_2$ lesz egyértelmű (előző tétel).

Kínai maradéktétel (FGy2.6.2)

Tegyük fel, hogy m_1, m_2, \dots, m_n páronként relatív prímek. Ekkor az $x \equiv c_1 (m_1), \dots, x \equiv c_n (m_n)$ rendszernek van megoldása, és a megoldások egy mod $m_1 \dots m_n$ maradékosztályt alkotnak.

Ez n szerinti indukcióval következik az előző tételből.

A kínai maradéktétel

Ha m_1 és m_2 relatív prímelek, akkor az $x \equiv c_1 (m_1)$, $x \equiv c_2 (m_2)$ rendszernek mindig van megoldása, és a megoldás mod $[m_1, m_2] = m_1 m_2$ lesz egyértelmű (előző tétel).

Kínai maradéktétel (FGy2.6.2)

Tegyük fel, hogy m_1, m_2, \dots, m_n páronként relatív prímelek. Ekkor az $x \equiv c_1 (m_1), \dots, x \equiv c_n (m_n)$ rendszernek van megoldása, és a megoldások egy mod $m_1 \dots m_n$ maradékosztályt alkotnak.

Ez n szerinti indukcióval következik az előző tételből.
Az $n = 1$ eset nyilvánvaló.

A kínai maradéktétel

Ha m_1 és m_2 relatív prímelek, akkor az $x \equiv c_1 (m_1)$, $x \equiv c_2 (m_2)$ rendszernek mindig van megoldása, és a megoldás mod $[m_1, m_2] = m_1 m_2$ lesz egyértelmű (előző tétel).

Kínai maradéktétel (FGy2.6.2)

Tegyük fel, hogy m_1, m_2, \dots, m_n páronként relatív prímelek. Ekkor az $x \equiv c_1 (m_1), \dots, x \equiv c_n (m_n)$ rendszernek van megoldása, és a megoldások egy mod $m_1 \dots m_n$ maradékosztályt alkotnak.

Ez n szerinti indukcióval következik az előző tételből.

Az $n = 1$ eset nyilvánvaló. Tegyük fel, hogy $n - 1$ -re igaz az állítás.

A kínai maradéktétel

Ha m_1 és m_2 relatív prímelek, akkor az $x \equiv c_1 (m_1)$, $x \equiv c_2 (m_2)$ rendszernek mindig van megoldása, és a megoldás mod $[m_1, m_2] = m_1 m_2$ lesz egyértelmű (előző tétel).

Kínai maradéktétel (FGy2.6.2)

Tegyük fel, hogy m_1, m_2, \dots, m_n páronként relatív prímelek. Ekkor az $x \equiv c_1 (m_1), \dots, x \equiv c_n (m_n)$ rendszernek van megoldása, és a megoldások egy mod $m_1 \dots m_n$ maradékosztályt alkotnak.

Ez n szerinti indukcióval következik az előző tételből.

Az $n = 1$ eset nyilvánvaló. Tegyük fel, hogy $n - 1$ -re igaz az állítás.

Legyen $M = m_1 m_2 \dots m_{n-1}$.

A kínai maradéktétel

Ha m_1 és m_2 relatív prímelek, akkor az $x \equiv c_1 (m_1)$, $x \equiv c_2 (m_2)$ rendszernek mindig van megoldása, és a megoldás mod $[m_1, m_2] = m_1 m_2$ lesz egyértelmű (előző tétel).

Kínai maradéktétel (FGy2.6.2)

Tegyük fel, hogy m_1, m_2, \dots, m_n páronként relatív prímelek. Ekkor az $x \equiv c_1 (m_1), \dots, x \equiv c_n (m_n)$ rendszernek van megoldása, és a megoldások egy mod $m_1 \dots m_n$ maradékosztályt alkotnak.

Ez n szerinti indukcióval következik az előző tételből.

Az $n = 1$ eset nyilvánvaló. Tegyük fel, hogy $n - 1$ -re igaz az állítás. Legyen $M = m_1 m_2 \dots m_{n-1}$. Az első $n - 1$ kongruenciából álló rendszer az indukciós feltevés miatt helyettesíthető egy $x \equiv c (M)$ kongruenciával.

A kínai maradéktétel

Ha m_1 és m_2 relatív prímelek, akkor az $x \equiv c_1 (m_1)$, $x \equiv c_2 (m_2)$ rendszernek mindig van megoldása, és a megoldás mod $[m_1, m_2] = m_1 m_2$ lesz egyértelmű (előző tétel).

Kínai maradéktétel (FGy2.6.2)

Tegyük fel, hogy m_1, m_2, \dots, m_n páronként relatív prímelek. Ekkor az $x \equiv c_1 (m_1), \dots, x \equiv c_n (m_n)$ rendszernek van megoldása, és a megoldások egy mod $m_1 \dots m_n$ maradékosztályt alkotnak.

Ez n szerinti indukcióval következik az előző tételből.

Az $n = 1$ eset nyilvánvaló. Tegyük fel, hogy $n - 1$ -re igaz az állítás. Legyen $M = m_1 m_2 \dots m_{n-1}$. Az első $n - 1$ kongruenciából álló rendszer az indukciós feltevés miatt helyettesíthető egy $x \equiv c (M)$ kongruenciával. Ennek és az $x \equiv c_n (m_n)$ kongruenciának a közös megoldásait keressük.

A kínai maradéktétel

Ha m_1 és m_2 relatív prímek, akkor az $x \equiv c_1 (m_1)$, $x \equiv c_2 (m_2)$ rendszernek mindig van megoldása, és a megoldás mod $[m_1, m_2] = m_1 m_2$ lesz egyértelmű (előző tétel).

Kínai maradéktétel (FGy2.6.2)

Tegyük fel, hogy m_1, m_2, \dots, m_n páronként relatív prímek. Ekkor az $x \equiv c_1 (m_1), \dots, x \equiv c_n (m_n)$ rendszernek van megoldása, és a megoldások egy mod $m_1 \dots m_n$ maradékosztályt alkotnak.

Ez n szerinti indukcióval következik az előző tételből.

Az $n = 1$ eset nyilvánvaló. Tegyük fel, hogy $n - 1$ -re igaz az állítás.

Legyen $M = m_1 m_2 \dots m_{n-1}$. Az első $n - 1$ kongruenciából álló rendszer az indukciós feltevés miatt helyettesíthető egy $x \equiv c (M)$ kongruenciával. Ennek és az $x \equiv c_n (m_n)$ kongruenciának a közös megoldásait keressük. Erre alkalmazható a fenti tétel:

A kínai maradéktétel

Ha m_1 és m_2 relatív prímelek, akkor az $x \equiv c_1 (m_1)$, $x \equiv c_2 (m_2)$ rendszernek mindig van megoldása, és a megoldás mod $[m_1, m_2] = m_1 m_2$ lesz egyértelmű (előző tétel).

Kínai maradéktétel (FGy2.6.2)

Tegyük fel, hogy m_1, m_2, \dots, m_n páronként relatív prímelek. Ekkor az $x \equiv c_1 (m_1), \dots, x \equiv c_n (m_n)$ rendszernek van megoldása, és a megoldások egy mod $m_1 \dots m_n$ maradékosztályt alkotnak.

Ez n szerinti indukcióval következik az előző tételből.

Az $n = 1$ eset nyilvánvaló. Tegyük fel, hogy $n - 1$ -re igaz az állítás.

Legyen $M = m_1 m_2 \dots m_{n-1}$. Az első $n - 1$ kongruenciából álló rendszer az indukciós feltevés miatt helyettesíthető egy $x \equiv c (M)$ kongruenciával. Ennek és az $x \equiv c_n (m_n)$ kongruenciának a közös megoldásait keressük. Erre alkalmazható a fenti tétel:

m_1, m_2, \dots, m_n páronként relatív prímelek, így $(M, m_n) = 1$

A kínai maradéktétel

Ha m_1 és m_2 relatív prímelek, akkor az $x \equiv c_1 (m_1)$, $x \equiv c_2 (m_2)$ rendszernek mindig van megoldása, és a megoldás mod $[m_1, m_2] = m_1 m_2$ lesz egyértelmű (előző tétel).

Kínai maradéktétel (FGy2.6.2)

Tegyük fel, hogy m_1, m_2, \dots, m_n páronként relatív prímelek. Ekkor az $x \equiv c_1 (m_1), \dots, x \equiv c_n (m_n)$ rendszernek van megoldása, és a megoldások egy mod $m_1 \dots m_n$ maradékosztályt alkotnak.

Ez n szerinti indukcióval következik az előző tételből.

Az $n = 1$ eset nyilvánvaló. Tegyük fel, hogy $n - 1$ -re igaz az állítás.

Legyen $M = m_1 m_2 \dots m_{n-1}$. Az első $n - 1$ kongruenciából álló rendszer az indukciós feltevés miatt helyettesíthető egy $x \equiv c (M)$ kongruenciával. Ennek és az $x \equiv c_n (m_n)$ kongruenciának a közös megoldásait keressük. Erre alkalmazható a fenti tétel:

m_1, m_2, \dots, m_n páronként relatív prímelek, így $(M, m_n) = 1$ (hiszen nincs közös prímosztójuk).

A 11. előadáshoz tartozó vizsgaanyag

Fogalmak

Kongruencia (FGy2.1.1).

A 11. előadáshoz tartozó vizsgaanyag

Fogalmak

Kongruencia (FGy2.1.1).

Lineáris kongruencia (FGy2.5.1).

A 11. előadáshoz tartozó vizsgaanyag

Fogalmak

Kongruencia (FGy2.1.1).

Lineáris kongruencia (FGy2.5.1).

Maradékosztály (FGy2.2.1).

A 11. előadáshoz tartozó vizsgaanyag

Fogalmak

Kongruencia (FGy2.1.1).

Lineáris kongruencia (FGy2.5.1).

Maradékosztály (FGy2.2.1).

Tételek

A kongruenciák alaptulajdonságai, egyszerűsítése (FGy2.1.2–3).

A 11. előadáshoz tartozó vizsgaanyag

Fogalmak

Kongruencia (FGy2.1.1).

Lineáris kongruencia (FGy2.5.1).

Maradékosztály (FGy2.2.1).

Tételek

A kongruenciák alaptulajdonságai, egyszerűsítése (FGy2.1.2–3).

A lineáris kongruencia megoldásai, eljárás (FGy2.5.3–4, 7.1.1).

A 11. előadáshoz tartozó vizsgaanyag

Fogalmak

Kongruencia (FGy2.1.1).

Lineáris kongruencia (FGy2.5.1).

Maradékosztály (FGy2.2.1).

Tételek

A kongruenciák alaptulajdonságai, egyszerűsítése (FGy2.1.2–3).

A lineáris kongruencia megoldásai, eljárás (FGy2.5.3–4, 7.1.1).

Szimultán kongruenciarendszer (FGy2.6.1).

A 11. előadáshoz tartozó vizsgaanyag

Fogalmak

Kongruencia (FGy2.1.1).

Lineáris kongruencia (FGy2.5.1).

Maradékosztály (FGy2.2.1).

Tételek

A kongruenciák alaptulajdonságai, egyszerűsítése (FGy2.1.2–3).

A lineáris kongruencia megoldásai, eljárás (FGy2.5.3–4, 7.1.1).

Szimultán kongruenciarendszer (FGy2.6.1).

A kínai maradéktétel (FGy2.6.2).