# Kongruenciák

Ha $a$ és $b$ ugyanazt a maradékot adja $m$-mel osztva, akkor azt mondjuk, hogy $a$ és $b$ kongruensek modulo $m$, és ezt a tényt így jelöljük:

$$a \equiv b \bmod m$$

Megnézem a kapcsolódó epizódot

---

Reflexív:

$$a \equiv a \bmod m$$

Szimmetrikus:

$$a \equiv b \bmod m \Rightarrow b \equiv a \bmod m$$

Tranzitív:

$$a \equiv b \bmod m \text{ és } b \equiv c \bmod m \Rightarrow a \equiv c \bmod m$$

Összefüggés összeadásra:

$$a \equiv b \bmod m \text{ és } c \equiv d \bmod m \Rightarrow a + c \equiv b + d \bmod m$$

Összefüggés szorzásra:

$$a \equiv b \bmod m \text{ és } c \equiv d \bmod m \Rightarrow a \cdot c \equiv b \cdot d \bmod m$$

Megnézem a kapcsolódó epizódot

---

Legyenek $a$ és $b$ egész számok és $m$ pozitív egész szám.

Ekkor

$$a \equiv b \bmod m, \text{ ha } m \mid a - b$$

Megnézem a kapcsolódó epizódot

---

$$a \equiv b \bmod m \Rightarrow a \cdot c \equiv b \cdot c \bmod m$$

$$a \cdot c \equiv b \cdot c \bmod m \Rightarrow a \equiv b \bmod m \quad (m, c) = 1$$

Megnézem a kapcsolódó epizódot

---

Egy adott $m$ modulus esetén az $a$-val kongruens elemek halmazát az $a$ által reprezentált maradékosztálynak nevezzük.

Megnézem a kapcsolódó epizódot

---

Egy mod $m$ modulus esetén az $m$-hez relatív prím elemekből álló maradékosztályokat redukált maradékosztálynak nevezzük.

A redukált maradékosztályok számát a $\varphi(m)$ számelméleti függvény írja le.

Megnézem a kapcsolódó epizódot

---

Az euler féle $\varphi$ függvény azt adja meg, hogy hány $m$-nél nem nagyobb, $m$-hez relatív prím pozitív szám létezik.

Ha $p$ prím, akkor

$$\varphi(p) = p - 1$$

$$\varphi(p^\alpha = p^\alpha - p^{\alpha-1}$$

És ha

$$m = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_n^{\alpha_n}$$

akkor

$$\varphi(m) = \left(p_1^{\alpha_1} - p_1^{\alpha_1 - 1}\right) \cdot \dots \cdot \left(p_n^{\alpha_n} - p_n^{\alpha_n - 1}\right)$$

Továbbá

$$\varphi(ab) = \varphi(a) \cdot \varphi(b)$$

Megnézem a kapcsolódó epizódot

---

$a^{\varphi(m)} \equiv 1 \bmod m$ ha $(a, m) = 1$

Megnézem a kapcsolódó epizódot

---

$a^p \equiv a \bmod p$ ha $p$ prím

Megnézem a kapcsolódó epizódot

---

A lineáris kongruenciák így néznek ki:

$$ax \equiv b \bmod m$$

És érdemes megjegyezni, hogy csak akkor oldhatók meg, ha $(a, m) \mid b$.

Megnézem a kapcsolódó epizódot

---

A lineáris kongruenciák így néznek ki:

$$ax \equiv b \bmod m$$

Megoldás csak akkor létezik, ha $(a,m) \mid b$.

A megoldás menete a következő:

1. lépés: Redukálunk

$$a_1 x \equiv b_1 \bmod m$$

2. lépés: Leosztunk $a_1$-gyel, de $b_1$-et lélekben fel kell erre készíteni

A megoldások száma: $(a,m)$

Megnézem a kapcsolódó epizódot

---

Az RSA lényege, hogy a titkosítás kulcsa nyilvános, vagyis azt bárki ismerheti. Csak a dekódolás kulcsa az, ami titkos.

Az alapötlete a következő:

Veszünk két jó nagy prímet, $p$-t és $q$-t amit csak mi ismerünk, ezek titkosak.

Elkészítjük az $N = p \cdot q$ számot és $\varphi(N)$-et, amit csak mi ismerünk.

Ha $p$ és $q$ többszázjegyű prímek, akkor $N$ prímfelbontása a jelenlegi számítógépekkel több ezer évig tartana, és így $\varphi(N)$ kiszámolása is lehetetlen.

Végül már csak egy dolog kell, egy $e$ kitevő, amire teljesül, hogy $(e, \varphi(N)) = 1$

Ezt követően jön a titkosítás.

A visszafejtéshez pedig az Euler-Fermat tétel kell, aminek segítségével megalkotjuk a $d$ megfejtő kulcsot.

Megnézem a kapcsolódó epizódot

---