

Név: Unger Tamás István

Neptun: FTD1YJ

Web: <http://maxwell.sze.hu/~ungert>

## ALGEBRA ÉS SZÁMELMÉLET, NEGYEDIK HÁZI FELADAT

1. OLDJA MEG AZ  $f \cdot u \equiv \bar{1} \pmod{m}$  KONGRUENCIÁT.

$$f = x^2 + \bar{3}x + \bar{1}, \quad m = x^3 + \bar{2}x^2 + \bar{4}x + \bar{2} \in \mathbb{Z}_5[x].$$

A kongruenciareláció definícióját felhasználva világos, hogy

$$f \cdot u \equiv \bar{1} \pmod{m} \Leftrightarrow \exists k \in \mathbb{Z}_5[x] \quad fu = km + \bar{1}, \Leftrightarrow \bar{1} = fu - km, \quad u, k \in \mathbb{Z}_5[x].$$

Az egyenlet megoldásához az euklideszi algoritmust hívjuk segítségül a következőképpen:

$$\begin{array}{r} \frac{m}{f} : (x^3 + \bar{2}x^2 + \bar{4}x + \bar{2}) : (x^2 + \bar{3}x + \bar{1}) = x \\ - (x^3 + \bar{3}x + x) \\ \hline (\bar{4}x^2 + \bar{3}x + \bar{2}) : (x^2 + \bar{3}x + \bar{1}) = x + \bar{4} \\ - (\bar{4}x^2 + \bar{2}x + \bar{4}) \\ \hline x + \bar{3}. \end{array}$$

Az első lépésből tehát az kaptuk, hogy  $m = f(x + \bar{4}) + (x + \bar{3})$ . Az euklideszi algoritmus második lépése:

$$\begin{array}{r} (x^2 + \bar{3}x + \bar{1}) : (x + \bar{3}) = x \\ - (x^2 + \bar{3}x) \\ \hline 1. \end{array}$$

A második lépésből adódik, hogy  $f = (x + \bar{3})x + \bar{1}$ . Egyből látszik, hogy  $\bar{1} = f - (x + \bar{3})x$ . Az algoritmus első lépésének eredményéből azt is látszik, hogy  $(x + \bar{3}) = m - f(x + \bar{4})$ . ViSSzahelyettesítve:

$$\bar{1} = f - (m - f(x + \bar{4}))x = f - (mx - f(x^2 + \bar{4}x)) = f(x^2 + \bar{4}x + \bar{1}) - m(x).$$

Az egyenletből leolvasható a kongruencia egy partikuláris megoldása, így  $u_0 = x^2 + \bar{4}x + \bar{1}$ , és bár nem fontos, de  $k = x$ . Így:

$$u \equiv x^2 + \bar{4}x + \bar{1} \pmod{x^3 + \bar{2}x^2 + \bar{4}x + \bar{2}}.$$

2. OLDJA MEG AZ  $f \cdot u \equiv \bar{1} \pmod{m}$  KONGRUENCIÁT.

$$f = x^2 + \bar{1}, \quad m = x^3 + x^2 + \bar{1} \in \mathbb{Z}_2[x].$$

Definíció alapján:

$$f \cdot u \equiv \bar{1} \pmod{m} \Leftrightarrow \exists k \in \mathbb{Z}_2[x] \quad fu = km + \bar{1}, \Leftrightarrow \bar{1} = fu - km, \quad u, k \in \mathbb{Z}_2[x].$$

Az euklideszi algoritmus első lépése:

$$\begin{array}{r} \frac{m}{f} : (x^3 + x^2 + \bar{1}) : (x^2 + \bar{1}) = x \\ \underline{-(x^3 + x)} \\ (x^2 + x + \bar{1}) : (x^2 + \bar{1}) = x + \bar{1} \\ \underline{-(x^2 + \bar{1})} \\ x. \end{array}$$

Azt kaptuk, hogy  $m = f(x + \bar{1}) + x$ . A második lépés:

$$\begin{array}{r} (x^2 + \bar{1}) : x = x \\ \underline{-(x^2)} \\ 1, \end{array}$$

amelyből  $f = x \cdot x + \bar{1}$  adódik. Az ismert módon tovább haladva:

$$\bar{1} = f - x \cdot x, \text{ és } x = m - f(x + \bar{1}), \bar{1} = f - (m - f(x + \bar{1}))x = f(x^2 + x + \bar{1}) - mx.$$

Egyből látszik, hogy  $u_0 = x^2 + x + \bar{1}$  és  $k = x$ , így a kongruencia megoldása:

$$u \equiv x^2 + x + \bar{1} \pmod{x^3 + x^2 + \bar{1}}.$$

**3. OLDJA MEG AZ  $f \cdot u \equiv \bar{1} \pmod{m}$  KONGRUENCIÁT.**

$$f = \bar{2}x^2 + \bar{4}, \quad m = x^3 + x^2 + x + \bar{1} \in \mathbb{Z}_5[x].$$

Definíció alapján:

$$f \cdot u \equiv \bar{1} \pmod{m} \Leftrightarrow \exists k \in \mathbb{Z}_5[x] \quad fu = km + \bar{1}, \Leftrightarrow \bar{1} = fu - km, \quad u, k \in \mathbb{Z}_5[x].$$

Az euklideszi algoritmus első lépése:

$$\begin{array}{r} \frac{m}{f} : (x^3 + x^2 + x + \bar{1}) : (\bar{2}x^2 + \bar{4}) = \bar{3}x \\ \underline{-(x^3 + \bar{2}x)} \\ (x^2 + \bar{4}x + \bar{1}) : (\bar{2}x^2 + \bar{4}) = \bar{3}x + \bar{3} \\ \underline{-(x^2 + \bar{2})} \\ \bar{4}x + \bar{4}. \end{array}$$

Az első lépésből adódik, hogy  $m = f(\bar{3}x + \bar{3}) + (\bar{4}x + \bar{4})$ . Az euklideszi algoritmus második lépése:

$$\begin{array}{r} (\bar{2}x^2 + \bar{4}) : (\bar{4}x + \bar{4}) = \bar{3}x \\ \underline{-(\bar{2}x^2 + \bar{2})} \\ (\bar{3}x + \bar{4}) : (\bar{4}x + \bar{4}) = \bar{3}x + \bar{2} \\ \underline{-(\bar{3}x + \bar{3})} \\ \bar{1}. \end{array}$$

A második lépésből adódik, hogy  $f = (\bar{4}x + \bar{4})(\bar{3}x + \bar{2}) + \bar{1}$ . Egyből látszik, hogy  $\bar{1} = f - (\bar{4}x + \bar{4})(\bar{3}x + \bar{2})$ . Az euklideszi algoritmus első lépéséből adódó összefüggést átrendezve

azt kapjuk, hogy  $(\overline{4x} + \overline{4}) = m - f(\overline{3x} + \overline{3})$ . Ezt behelyettesítve a második lépésből adódó összefüggésbe adódik:

$$\overline{1} = f - (m - f(\overline{3x} + \overline{3}))(\overline{3x} + \overline{2}) = f - ((\overline{3x} + \overline{2})m - f(\overline{3x} + \overline{3})(\overline{3x} + \overline{2})).$$

Elvégezve a zárójel felbontását, abeszorzást és legvégül az összevonásokat:

$$\overline{1} = f - (\overline{3x} + \overline{2})m + f(\overline{4x^2} + x + \overline{4x} + \overline{1}) = f(\overline{4x^2} + \overline{2}) - (\overline{3x} + \overline{2})m.$$

Készen vagyunk, hiszen egyből látszik, hogy  $u_0 = \overline{4x^2} + \overline{2}$  és  $k = \overline{3x} + \overline{2}$ , így a kongruencia megoldása:

$$u \equiv \overline{4x^2} + \overline{2} \pmod{x^3 + x^2 + x + \overline{1}}.$$