

Név: Unger Tamás István

Neptun: FTD1YJ

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

ALGEBRA ÉS SZÁMELMÉLET, ÖTÖDIK HÁZI FELADAT

1. DÖNTSE EL, HOGY TEST-E A MEGADOTT FAKTORGYŰRŰ, HATÁROZZA MEG ELEMEIT, MŰVELETTÁBLÁJÁT ÉS A MEGADOTT ELEMENK INVERZÉT IS!

$$\mathbb{Z}_2[x] / (x^3 + x^2 + \bar{1}), \quad \overline{x^2}^{-1} = ?, \quad \overline{x^2 + x + \bar{1}}^{-1} = ?.$$

Tudjuk, hogy $\mathbb{Z}_2[x] / (x^3 + x^2 + \bar{1})$ test akkor és csak akkor, ha $(x^3 + x^2 + \bar{1})$ irreducibilis $\mathbb{Z}_2$ felett. Világos, hogy

$$\bar{0}^3 + \bar{0}^2 + \bar{1} \neq \bar{0} \quad (= \bar{1}) \quad \text{és} \quad \bar{1}^3 + \bar{1}^2 + \bar{1} \neq \bar{0} \quad (= \bar{1}),$$

így az eredeti polinomunk $\mathbb{Z}_2$ felett nem bontható fel alacsonyabb fokszámú polinomok szorzatára, így $(x^3 + x^2 + \bar{1})$ irreducibilis, $\mathbb{Z}_2[x] / (x^3 + x^2 + \bar{1})$ tehát test. Soroljuk fel az elemeit:

$$\bar{0}, \bar{1}, \bar{x}, \overline{x + \bar{1}}, \overline{x^2}, \overline{x^2 + \bar{1}}, \overline{x^2 + x} \quad \text{és} \quad \overline{x^2 + x + \bar{1}}$$

A véges testünk tehát 8 elemű. A véges test műveletáblái a következőképpen adódnak:

+	$\bar{0}$	$\bar{1}$	$\bar{x}$	$\overline{x + \bar{1}}$	$\overline{x^2}$	$\overline{x^2 + \bar{1}}$	$\overline{x^2 + x}$	$\overline{x^2 + x + \bar{1}}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{x}$	$\overline{x + \bar{1}}$	$\overline{x^2}$	$\overline{x^2 + \bar{1}}$	$\overline{x^2 + x}$	$\overline{x^2 + x + \bar{1}}$
$\bar{1}$	$\bar{1}$	$\bar{0}$	$\overline{x + \bar{1}}$	$\bar{x}$	$\overline{x^2 + \bar{1}}$	$\overline{x^2}$	$\overline{x^2 + x + \bar{1}}$	$\overline{x^2 + x}$
$\bar{x}$	$\bar{x}$	$\overline{x + \bar{1}}$	$\bar{0}$	$\bar{1}$	$\overline{x^2 + x}$	$\overline{x^2 + x + \bar{1}}$	$\overline{x^2}$	$\overline{x^2 + \bar{1}}$
$\overline{x + \bar{1}}$	$\overline{x + \bar{1}}$	$\bar{x}$	$\bar{1}$	$\bar{0}$	$\overline{x^2 + x + \bar{1}}$	$\overline{x^2 + x}$	$\overline{x^2 + \bar{1}}$	$\overline{x^2}$
$\overline{x^2}$	$\overline{x^2}$	$\overline{x^2 + \bar{1}}$	$\overline{x^2 + x}$	$\overline{x^2 + x + \bar{1}}$	$\bar{0}$	$\bar{1}$	$\bar{x}$	$\overline{x + \bar{1}}$
$\overline{x^2 + \bar{1}}$	$\overline{x^2 + \bar{1}}$	$\overline{x^2}$	$\overline{x^2 + x + \bar{1}}$	$\overline{x^2 + x}$	$\bar{1}$	$\bar{0}$	$\overline{x + \bar{1}}$	$\bar{x}$
$\overline{x^2 + x}$	$\overline{x^2 + x}$	$\overline{x^2 + x + \bar{1}}$	$\overline{x^2 + x}$	$\overline{x^2 + \bar{1}}$	$\bar{x}$	$\overline{x + \bar{1}}$	$\bar{0}$	$\bar{1}$
$\overline{x^2 + x + \bar{1}}$	$\overline{x^2 + x + \bar{1}}$	$\overline{x^2 + x}$	$\overline{x^2 + \bar{1}}$	$\overline{x^2}$	$\overline{x + \bar{1}}$	$\bar{x}$	$\bar{1}$	$\bar{0}$

·	$\bar{0}$	$\bar{1}$	$\bar{x}$	$\overline{x + \bar{1}}$	$\overline{x^2}$	$\overline{x^2 + \bar{1}}$	$\overline{x^2 + x}$	$\overline{x^2 + x + \bar{1}}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{x}$	$\overline{x + \bar{1}}$	$\overline{x^2}$	$\overline{x^2 + \bar{1}}$	$\overline{x^2 + x}$	$\overline{x^2 + x + \bar{1}}$
$\bar{x}$	$\bar{0}$	$\bar{x}$	$\overline{x^2}$	$\overline{x^2 + x}$	$\overline{x^2 + \bar{1}}$	$\overline{x^2 + x + \bar{1}}$	$\bar{1}$	$\overline{x + \bar{1}}$
$\overline{x + \bar{1}}$	$\bar{0}$	$\overline{x + \bar{1}}$	$\overline{x^2 + x}$	$\overline{x^2 + \bar{1}}$	$\bar{1}$	$\bar{x}$	$\overline{x^2 + x + \bar{1}}$	$\overline{x^2}$
$\overline{x^2}$	$\bar{0}$	$\overline{x^2}$	$\overline{x^2 + \bar{1}}$	$\bar{1}$	$\overline{x^2 + x + \bar{1}}$	$\overline{x + \bar{1}}$	$\bar{x}$	$\overline{x^2 + x}$
$\overline{x^2 + \bar{1}}$	$\bar{0}$	$\overline{x^2 + \bar{1}}$	$\overline{x^2 + x + \bar{1}}$	$\bar{x}$	$\overline{x + \bar{1}}$	$\overline{x^2 + x}$	$\overline{x^2}$	$\bar{1}$
$\overline{x^2 + x}$	$\bar{0}$	$\overline{x^2 + x}$	$\bar{1}$	$\overline{x^2 + x + \bar{1}}$	$\bar{x}$	$\overline{x^2}$	$\overline{x + \bar{1}}$	$\overline{x^2 + \bar{1}}$
$\overline{x^2 + x + \bar{1}}$	$\bar{0}$	$\overline{x^2 + x + \bar{1}}$	$\overline{x + \bar{1}}$	$\overline{x^2}$	$\overline{x^2 + x}$	$\bar{1}$	$\overline{x^2 + \bar{1}}$	$\bar{x}$

Most pedig határozzuk meg $\overline{x^2}$ inverzét. Legyen $\bar{u} = \overline{x^2}^{-1}$. Ekkor az kell, hogy

$$\overline{x^2} \cdot \bar{u} = \bar{1} \Leftrightarrow (x^2) u \equiv \bar{1} \pmod{x^3 + x^2 + \bar{1}} \Leftrightarrow \exists k \in \mathbb{Z}_2[x], \quad (x^2) u = k(x^3 + x^2 + \bar{1}) + \bar{1}.$$

Ehhez az euklideszi algoritmust kell segítségül hívni:

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

Azt kaptuk tehát, hogy $(x^3 + x^2 + \bar{1}) = (x^2) x + \bar{1} \Leftrightarrow (x^2) (x + \bar{1}) = (x^3 + x^2 + \bar{1}) + \bar{1}$, tehát $\overline{x^2}$ inverze $\overline{x + \bar{1}}$.

Végül meghatározzuk $\overline{x^2 + x + \bar{1}}$ inverzét, $\overline{x^2 + x + \bar{1}}^{-1} = \bar{u}$. Ebben az esetben

$$\overline{x^2 + x + \bar{1}} \cdot \bar{u} = \bar{1} \Leftrightarrow (x^2 + x + \bar{1}) u \equiv \bar{1} \pmod{x^3 + x^2 + \bar{1}}.$$

A kongruencia definíciója szerint ekkor

$$\exists k \in \mathbb{Z}_2[x], (x^2 + x + \bar{1}) u = k(x^3 + x^2 + \bar{1}) + \bar{1} \Leftrightarrow \bar{1} = (x^2 + x + \bar{1}) u - k(x^3 + x^2 + \bar{1}).$$

Az euklideszi algoritmus szerint:

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

Azt kaptuk, hogy $(x^3 + x^2 + \bar{1}) = (x^2 + x + \bar{1}) x + (x + \bar{1}) \Leftrightarrow (x + \bar{1}) = (x^3 + x^2 + \bar{1}) - (x^2 + x + \bar{1}) x$. A második lépés:

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

Ebből következik, hogy $(x^2 + x + \bar{1}) = (x + \bar{1}) x + \bar{1} \Leftrightarrow \bar{1} = (x^2 + x + \bar{1}) - (x + \bar{1}) x$. Behelyettesítve az első lépésből kapott összefüggést:

$$\begin{aligned} \bar{1} &= (x^2 + x + \bar{1}) - [(x^3 + x^2 + \bar{1}) - (x^2 + x + \bar{1}) x] x, \\ \bar{1} &= (x^2 + x + \bar{1}) - (x^3 + x^2 + \bar{1}) x + (x^2 + x + \bar{1}) x^2, \\ \bar{1} &= (x^2 + \bar{1}) (x^2 + x + \bar{1}) - x (x^3 + x^2 + \bar{1}). \end{aligned}$$

Ebből már $\bar{u}$ értéke leolvasható,

$$\bar{u} = \overline{x^2 + x + \bar{1}}^{-1} = \overline{x^2 + \bar{1}}.$$

Vegyük észre, hogy az alábbi lépések kikerülhetők, amennyiben a véges test szorzótáblája a rendelkezésünkre áll, hiszen a táblázatból az inverzek közvetlenül leolvashatók (azon célról beszélünk, ahol a szorzat értéke $\bar{1}$).