

$$f = x^2 + 2 \in \mathbb{Z}_3[x]$$

$$g = 2x^2 + 4x + 1 \in \mathbb{Z}_3[x]$$

$$h = x^3 + x + 4 \in \mathbb{Z}_3[x]$$

b

$$g \cdot h \mod x^2 + 2x + 2$$

$$gh = (2x^2 + 4x + 1)(x^3 + x + 4) \mod x^2 + 2x + 2 =$$

$$= (2x^2 + 4 + 1 - 2(x^2 + 2x + 1))(x^3 + x + 4)$$

$$= (0x^2 + 0x - 3)(x^3 + x + 4) \mod x^2 + 2x + 2 = 0$$

c

$$(f - g)(g - h)(f - h) \mod x^2 + 2x + 2$$

lagrange freaky interpolacio

$$c_0, c_1, \dots, c_n \in R \text{ kulonbozo ertek } (R \text{ test})$$

$$d_0, d_1, \dots, d_n \in R \text{ tetszoleges ertek}$$

$$\Rightarrow \exists \text{ legfeljebb } n\text{-ed foku polinom, melyre } f(c_j) = d_j \ (j = 0 \dots n)$$

$$l_j(x) = \frac{\prod_{i \neq j} (x - c_i)}{\prod_{i \neq j} (c_j - c_i)} \quad f(x) = \sum_{j=0}^n d_j \cdot l_j(x)$$