

**Exercise 2.37** from *An Introduction to Mathematical Cryptography*

The multiplication table for the field  $\mathbb{F}_2[x]/(x^3+x+1)$  is given in Table 2.5, but we have omitted fourteen entries. Fill in the missing entries. (This is the field described in Example 2.57. *Hint.* Once you compute  $\mathbf{a} \cdot \mathbf{b}$ , you've also computed  $\mathbf{b} \cdot \mathbf{a}$ .)

	0	1	$x$	$x^2$	$1+x$	$1+x^2$	$x+x^2$	$1+x+x^2$
0	0	0	0	0	0	0	0	0
1	0	1	$x$			$1+x^2$	$x+x^2$	$1+x+x^2$
$x$	0	$x$	$x^2$		$x+x^2$	1		$1+x^2$
$x^2$	0			$x+x^2$	$1+x+x^2$	$x$	$1+x^2$	1
$1+x$	0		$x+x^2$	$1+x+x^2$	$1+x^2$		1	$x$
$1+x^2$	0	$1+x^2$	1	$x$		$1+x+x^2$	$1+x$	
$x+x^2$	0	$x+x^2$		$1+x^2$	1	$1+x$	$x$	
$1+x+x^2$	0	$1+x+x^2$	$1+x^2$	1	$x$			$1+x$

Table 2.5: Multiplication table for the field  $\mathbb{F}_2[x]/(x^3+x+1)$ .