

Table 4.7 Polynomial Arithmetic Modulo $(x^3 + x + 1)$

(a) Addition

		000	001	010	011	100	101	110	111
	+	0	1	x	$x + 1$	x^2	$x^2 + 1$	$x^2 + x$	$x^2 + x + 1$
000	0	0	1	x	$x + 1$	x^2	$x^2 + 1$	$x^2 + x$	$x^2 + x + 1$
001	1	1	0	$x + 1$	x	$x^2 + 1$	x^2	$x^2 + x + 1$	$x^2 + x$
010	x	x	$x + 1$	0	1	$x^2 + x$	$x^2 + x + 1$	x^2	$x^2 + 1$
011	$x + 1$	$x + 1$	x	1	0	$x^2 + x + 1$	$x^2 + x$	$x^2 + 1$	x^2
100	x^2	x^2	$x^2 + 1$	$x^2 + x$	$x^2 + x + 1$	0	1	x	$x + 1$
101	$x^2 + 1$	$x^2 + 1$	x^2	$x^2 + x + 1$	$x^2 + x$	1	0	$x + 1$	x
110	$x^2 + x$	$x^2 + x$	$x^2 + x + 1$	x^2	$x^2 + 1$	x	$x + 1$	0	1
111	$x^2 + x + 1$	$x^2 + x + 1$	$x^2 + x$	$x^2 + 1$	x^2	$x + 1$	x	1	0

(b) Multiplication

		000	001	010	011	100	101	110	111
	\times	0	1	x	$x + 1$	x^2	$x^2 + 1$	$x^2 + x$	$x^2 + x + 1$
000	0	0	0	0	0	0	0	0	0
001	1	0	1	x	$x + 1$	x^2	$x^2 + 1$	$x^2 + x$	$x^2 + x + 1$
010	x	0	x	x^2	$x^2 + x$	$x + 1$	1	$x^2 + x + 1$	$x^2 + 1$
011	$x + 1$	0	$x + 1$	$x^2 + x$	$x^2 + 1$	$x^2 + x + 1$	x^2	1	x
100	x^2	0	x^2	$x + 1$	$x^2 + x + 1$	$x^2 + x$	x	$x^2 + 1$	1
101	$x^2 + 1$	0	$x^2 + 1$	1	x^2	x	$x^2 + x + 1$	$x + 1$	$x^2 + x$
110	$x^2 + x$	0	$x^2 + x$	$x^2 + x + 1$	1	$x^2 + 1$	$x + 1$	x	x^2
111	$x^2 + x + 1$	0	$x^2 + x + 1$	$x^2 + 1$	x	1	$x^2 + x$	x^2	$x + 1$

Table 4.10 GF(2³) Arithmetic Using Generator for the Polynomial (x³ + x + 1)

(a) Addition

		000 0	001 1	010 G	100 g ²	011 g ³	110 g ⁴	111 g ⁵	101 g ⁶
000	0	0	1	G	g ²	g + 1	g ² + g	g ² + g + 1	g ² + 1
001	1	1	0	g + 1	g ² + 1	g	g ² + g + 1	g ² + g	g ²
010	g	g	g + 1	0	g ² + g	1	g ²	g ² + 1	g ² + g + 1
100	g ²	g ²	g ² + 1	g ² + g	0	g ² + g + 1	g	g + 1	1
011	g ³	g + 1	g	1	g ² + g + 1	0	g ² + 1	g ²	g ² + g
110	g ⁴	g ² + g	g ² + g + 1	g ²	g	g ² + 1	0	1	g + 1
111	g ⁵	g ² + g + 1	g ² + g	g ² + 1	g + 1	g ²	1	0	g
101	g ⁶	g ² + 1	g ²	g ² + g + 1	1	g ² + g	g + 1	g	0

(b) Multiplication

		000 0	001 1	010 G	100 g ²	011 g ³	110 g ⁴	111 g ⁵	101 g ⁶
000	0	0	0	0	0	0	0	0	0
001	1	0	1	G	g ²	g + 1	g ² + g	g ² + g + 1	g ² + 1
010	g	0	g	g ²	g + 1	g ² + g	g ² + g + 1	g ² + 1	1
100	g ²	0	g ²	g + 1	g ² + g	g ² + g + 1	g ² + 1	1	g
011	g ³	0	g + 1	g ² + g	g ² + g + 1	g ² + 1	1	g	g ²
110	g ⁴	0	g ² + g	g ² + g + 1	g ² + 1	1	g	g ²	g + 1
111	g ⁵	0	g ² + g + 1	g ² + 1	1	g	g ²	g + 1	g ² + g
101	g ⁶	0	g ² + 1	1	g	g ²	g + 1	g ² + g	g ² + g + 1