

*primitive*. Thus, if  $f(x)$  is primitive, then  $F^*$  can be completely generated by constructing powers of  $x$  modulo  $f(x)$ . This is useful because it allows products of elements in  $F^*$  to be formed by converting the elements into their representations as powers of  $x$ , multiplying the powers of  $x$ , and then converting the result back into an element in  $F^*$ . We illustrate this in the following example.

**Example 1.10** Consider the field  $D/B$  in Example 1.9. We can use the identity  $x^2 = 2x + 1$  to construct the elements in this field that correspond to powers of  $x$ . For example, we can construct the field element that corresponds to  $x^3$  as follows.

$$x^3 = x^2x = (2x + 1)x = 2x^2 + x = 2(2x + 1) + x = 5x + 2 = 2x + 2$$

Thus,  $x^3 = 2x + 2$  in  $D/B$ . Also, we can construct the field element that corresponds to  $x^4$  as follows.

$$x^4 = x^3x = (2x + 2)x = 2x^2 + 2x = 2(2x + 1) + 2x = 6x + 2 = 2$$

Thus,  $x^4 = 2$  in  $D/B$ . The field elements that correspond to subsequent powers of  $x$  can be constructed similarly. We list the field elements that correspond to the first 8 powers of  $x$  in the following table.

Power	Field Element
$x^1$	$x$
$x^2$	$2x + 1$
$x^3$	$2x + 2$
$x^4$	$2$
$x^5$	$2x$
$x^6$	$x + 2$
$x^7$	$x + 1$
$x^8$	$1$

Note that the only element in  $D/B$  not listed in this table is 0. Since all nonzero elements in  $D/B$  are generated by computing powers of  $x$ , then  $f(x) = x^2 + x + 2$  is primitive in  $\mathbb{Z}_3[x]$ . This table is useful for computing products in  $D/B$ . For example, we can compute the product of  $2x + 1$  and  $2x + 2$  in  $D/B$  as follows.

$$(2x + 1)(2x + 2) = x^2x^3 = x^5 = 2x$$

Note that this result is identical to the product we obtained for the same elements by two other methods in Example 1.9. We can also compute the