

## 12-1

方法一：利用本原多项式的定义，要满足三个条件：

(1) 第一个条件： $f(x)$  是既约的，即不能再因式分解；

若  $f(x)$  能因式分解，则其因子必然是最高幂指数小于 3 的多项式，一共有以下几种：

$x, x+1, x^2, x^2+1, x^2+x+1$  (【注】不包含  $x^2+x$ ，因为  $x^2+x$  自己都还可以因式分解)。

但这几种都不能整除  $f(x) = x^3 + x^2 + 1$ ，所以  $f(x)$  是既约的；

(2) 第二个条件： $f(x)$  能够整除  $x^7 + 1$ ；

$$\frac{x^7 + 1}{x^3 + x^2 + 1} = x^4 + x^3 + x^2 + 1, \text{ 能整除, 满足条件;}$$

(3) 第三个条件： $f(x)$  不能够整除  $x^3 + 1, x^4 + 1, x^5 + 1, x^6 + 1$ ；

经验证， $f(x)$  确实不能整除  $x^3 + 1, x^4 + 1, x^5 + 1, x^6 + 1$ ；

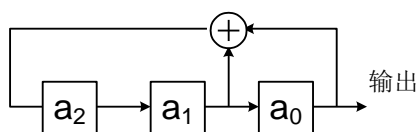
综上， $f(x)$  是本原多项式。

方法二：利用本原多项式与 m 序列的关系，一个线性反馈移存器能产生 m 序列的充要条件是：反馈移存器的特征多项式为本原多项式。

我们只要按照  $f(x) = x^3 + x^2 + 1$  的形式得到一个反馈移存器，若产生的序列周期为

$2^n - 1 = 2^3 - 1 = 7$ ，则  $f(x) = x^3 + x^2 + 1$  即为本原多项式，否则，则不是本原多项式。此

反馈移存器如下：



假设初始状态为：001，则此反馈移存器的数值变换规律如下：

$a_2$	$a_1$	$a_0$
0	0	1
1	0	0
0	1	0
1	0	1
1	1	0
1	1	1
0	1	1
0	0	1
⋮	⋮	⋮

此多项式  $f(x)$  产生的序列周期是 7，即为 m 序列，所以  $f(x)$  是本原多项式。

## 12-3

方法一：按照本原多项式的定义

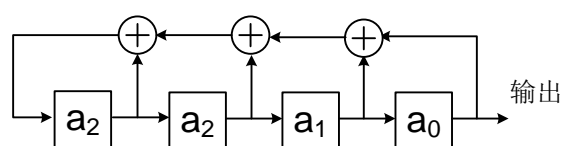
$$(x^{15} + 1) = (x^4 + x + 1)(x^4 + x^3 + 1)(x^4 + x^3 + x^2 + x + 1)(x^2 + x + 1)(x + 1)$$

$$(x^5 + 1) = (x^4 + x^3 + x^2 + x + 1)(x + 1)$$

虽然  $f(x) = x^4 + x^3 + x^2 + x + 1$  是  $x^{15} + 1$  的一个因子，但也是  $x^5 + 1$  的一个因子，不复合本原多项式的定义，所以，不是本原多项式。

方法二：利用本原多项式与 m 序列的关系，一个线性反馈移存器能产生 m 序列的充要条件是：反馈移存器的特征多项式为本原多项式。

我们只要按照  $f(x) = x^4 + x^3 + x^2 + x + 1$  的形式得到一个反馈移存器，若产生的序列周期为  $2^4 - 1 = 2^4 - 1 = 15$ ，则  $f(x) = x^4 + x^3 + x^2 + x + 1$  即为本原多项式，否则，则不是本原多项式。此反馈移存器如下：



假设初始状态为：0001，则此反馈移存器的数值变换规律如下：

$a_3$	$a_2$	$a_1$	$a_0$
0	0	0	1
1	0	0	0
1	1	0	0
0	1	1	0
0	0	1	1
0	0	0	1
1	0	0	0
1	1	0	0
⋮	⋮	⋮	⋮

此多项式  $f(x)$  产生的序列周期是 5，不是 m 序列，所以不  $f(x)$  是本原多项式。