代数基础和有限域

（二）

中国人民解放军治　　语学院翻印

1979年5月

第三章　一元多项式环$F_p[x]$ modf(x) 的同余类环和同余类域

这一节的目的是构造出特征 p 的一切有限域。

第十一节特征 p 的素域 F_p 上的一元多项式环 $F_p[x]$。

$F_p[x]$是由所有下列多项式

$$f(x)=a_0x^n+a_1x^{n-1}+\cdots+a_n$$

组成，其中 n 取任意非负整数，系数 a_0，a_1，$\cdots a_n$ 独立地取 F_p 中任意元素。

$F_p[x]$内多项式相加时，同次项系数相加，按 F_p 内的加法相加。F_p 的元素 a 与多项式相乘时，也是用元素 a 乘多项式各项的系数。

$F_p[x]$内多项式相乘时，按普通多项式的乘法，计算系数时，按 F_p 内的加法与乘法进行运算。

$F_p[x]$对多项式的加法和乘法成为一个交换环，叫做特征 p素域 F_p 上一元多项式环。

以后，F_p 内的运算 $\oplus$ 和 $\odot$ 为书写方便起见，仍然改用“$+$”和“$\cdot$”来表示，只要记住 a,b，…是代表 F_p 中的元素，就不致于与普通整数混淆。

F_p 上一元多项式环 $F_p[x]$ 和有理数域上一元多项式环 $Q[x]$在性质上有类似的地方，也有差异的地方。例如因式倍式，最大公因式与最小公倍式，互素，不可约多项式，以及因式分解唯一性定理，都是类似的，因此，关于有理系数多

项式的可除性的一般结果，对于 $F_p[x]$ 仍然有效。

$F_p[x]$ 与 $Q[x]$不同的地方，标志 $F_p[x]$ 的特点的性质有下列几条：

(i) 对于 $F_p[x]$中任一个多项式 $f(x)$

$$p \cdot f(x) = 0$$

因为，设 $f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n$

$$pf(x) = pa_0x^n + pa_1x^{n-1} + \cdots + pa_n.$$

但是 $pa_i = 0 \quad i = 0, 1, 2, \cdots, n$，所以

$$pf(x) = 0.$$

(ii) 对于 $F_p[x]$ 中任意两个多项式 $f(x)$与 $g(x)$

(1) $[f(x)+g(x)]^p = f^p(x) + g^p(x)$,

一般，对于 $F_p[x]$中任意 r 个多项式 $f_1(x), f_2(x), \cdots, f_r(x)$ 和任意正整数 n。

(2) $[f_1(x) + f_2(x) + \cdots + f_r(x)]^{p^n}$

$$= f_1^{p^n}(x) + f_2^{p^n}(x) + \cdots + f_r^{p^n}(x)$$

特别，当 $f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n$ 时，

$$f^p(x) = a_0x^{np} + a_1x^{(n-1)p} + \cdots + a_n \quad (\because a_i^p = a_i)$$

证明。(1) 直接从第九节定理 2 (i) 得来。(ii) (1) 的证明可完全仿照第九节定理 3 中 (ii) 的证明，在这里不重复了。至于一般公式 (ii) (2) 的证明可分两步

第一步

$$[f_1(x) + f_2(x) + \cdots + f_r(x)]^p$$

$$= [f_1(x) + \cdots + f_{r-1}(x)]^p + f_r^p(x)$$

累次应用 (1)，最后得

(3) $[f_1(x) + \cdots + f_r(x)]^p = f_1^p(x) + \cdots + f_r^p(x)$

第二步

$$[f_1(x)+\cdots+f_r(x)]^{p^n}=[f_1^p(x)+\cdots f_r^p(x)]^{p^{n-1}}$$

累次应用（3）即得（2）

(iii) 设 $f(x)$ 是 $F_p[x]$ 内一个次数$\geqslant 1$的多项式，下面三种说法是互相等价的。

1）$f(x)$ 等于某个多项式 $g(x)$ 的 p 次方幂

2）$f(x)$ 可以写成 $g(x^p)$ 的形式，其中 $g(x)$ 是一个适当的多项式。

3）$f(x)$ 的微商 $f'(x)=0$。

证明 1）$\Rightarrow$2），设 $f(x)=g^p(x)$，根据 ii），$g^p(x)=g(x^p)$ 所以 2）成立。

2）$\Rightarrow$3）设 $f(x)=g(x^p)$，将 $g(x)$ 具体写出

$g(x)=b_0x^r+b_1x^{r-1}+\cdots+b_r$，则 $f(x)=g(x^p)=b_0x^{rp}+$

$+b_1x^{(r-1)p}+\cdots+b_{r-1}x^p+b_r$ 因而

$$f'(x)=rpb_0x^{r(p-1)}+(r-1)pb_1x^{(r-1)(p-1)}+\cdots+$$
$$+pb_{r-1}x^{p-1}=0$$

3）$\Rightarrow$1）设 $f'(x)=0$，将 $f(x)$ 具体写出

$$f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_0,$$

于是 $f'(x)=na_nx^{n-1}+(n-1)a_{n-1}x^{n-2}+\cdots+a_1=0$

从而推出 $f'(x)$ 的各项系数为0：

$$ka_k=0,\quad k=0,\ 1,\ 2,\ \cdots n。$$

当 k 不是 p 的倍数时，必须 $a=0$。因此在 $f(x)$ 的表示式中，凡脚标不是 p 的倍数的系数全为0，剩下的各项，它的脚标都是 p 的倍数。因而 $f(x)$ 可写成

$$f(x)=a_{pr}x^{pr}+a_{p(r-1)}x^{p(r-1)}+\cdots+a_px^p+a_0$$
$$=(a_pr x^r+a_{p(r-1)}x^{r-1}+\cdots+a_px+a_0)^p$$

即 1）成立。

从 (iii) 可知 $F_p[x]$中任一个不可约多项式 $p(x)$ 的微商 $p'(x)$ 不等于零，因而与 $p(x)$ 互素。

(iv) 设 $f(x)$是一个次数$\geqslant 1$ 的多项式而且 $f'(x)\neq 0$，又设一个不可约多项式 $p(x)$ 是 $f(x)$ 的 k 重因式，即 $p^k(x)\mid f(x)$ 但 $p^{k+1}(x)\nmid f(x)$，那么，当 $p\nmid k$ 时，$p(x)$ 是 $f'(x)$ 的 $(k-1)$ 重因式，而当 $p\mid k$ 时，$p(x)$ 至少是 $f'(x)$ 的 k 重因式。

证明. 设 $f(x)=p^k(x)\cdot q(x)$，$(p(x),q(x))=1$，于是

$$\begin{aligned} f'(x)&=kp^{k-1}(x)p^1(x)q(x)+p^k(x)q^1(x)\\ &=p^{k-1}(x)[kp^1(x)q(x)+p(x)q^1(x)] \end{aligned}$$

当 $p\nmid k$ 时，方括号内第一项不为 0 且与 $p(x)$ 互素，第二项是 $p(x)$ 的倍式，因而方括号内的因式与 $p(x)$ 互素。所以 $p(x)$ 是 $f'(x)$ 的 $(k-1)$ 重因式。

当 $p\mid k$ 时，此时，

$$f'(x)=p^k(x)q'(x),\quad q'(x)\neq 0\ \text{（因假设 } f'(x)\neq 0\text{）}$$

$p(x)$ 至少是 $f'(x)$ 的 k 重因式。

例 1．设 $f(x)=(x+1)^3(x^3+x^2+1)\in F_2[x]$。此时，$p=2$，$p(x)=x+1$，$k=3$，$2\nmid 3$。计算

$$\begin{aligned} f'(x)&=((x+1)^3)'(x^3+x^2+1)+\\ &\quad+(x+1)^3(x^3+x^2+1)'\\ &=3(x+1)^2(x^3+x^2+1)+(x+1)^3(3x^2+2x)\\ &=(x+1)^2(x^3+x^2+1)+x^2(x+1)^3\\ &=(x+1)^2 \end{aligned}$$

$x+1$ 是 $f'(x)$ 的 $k-1=2$ 重因式。

例 2．设 $f(x)=(x+1)^2(x^3+x^2+1)\in F_2[x]$。此时

$p=2$，$p(x)=x+1$，$k=2$　$p\mid k$。计算

$$f'(x)=x^2(x+1)^2$$

$(x+1)$ 是 $f'(x)$ 的 $k=2$ 重因式。

例 3．设 $f(x)=(x+1)^2(x^3+x+1)\in F_2[x]$。此时，$p=2$　$p(x)=x+1$，$k=2$，$p\mid k$。计算

$$f'(x)=(x+1)^4。$$

$x+1$ 是 $f'(x)$ 的 $k+2=4$ 重因式。

(v) $F_p[x]$ 内次数 $<n$ 的多项式(包含 0 在内)共有 p^n 个而次数 $=n$ 的多项式共有 $(p-1)p^n$ 个。

证明．任一个次数 $<n$ 的多项式可写成

$$a_0x^{n-1}+a_1x^{n-2}+\cdots+a_{n-1}$$

其中 n 个系数 a_0，a_1，…，a_{n-1} 独立地在域 F_p 内取值。每个 a_i 有 p 种不同的取值，这 n 个系数组合起来共有 p^n 种取法，每个取法确定一个次数 $<n$ 的多项式。所以共有 p^n 个多项式。

次数 $=n$ 的多项式可写成

$$a_0x^n+a_1x^{n-1}+\cdots+a_n,$$

其中 a_0，a_1，a_2，…，a_n 可以独立地任意取值，但 $a_0\neq0$，a_0 只有 $p-1$ 种取法，而其余的每个 a_i 有 p 种取法，组合起来，共有 $(p-1)p^n$ 种取法，所以共有 $(p-1)p^n$ 个多项式。

以下为方便起见，多项式 $f(x)$ 的次数记作 $\partial^0 f(x)$。

第十二节　多项式的同余式和同余方程

1．同余式

在 $F_p[x]$ 内给定一个次数 $\geqslant 1$ 的多项式 $k(x)$，对于任意两个多项式 $g(x)$，$f(x)$，用 $k(x)$ 作带余除法，如果余式相等那么 $f(x)$ 和 $g(x)$ 叫做 $mod\ k(x)$ 同余，并记作

$$f(x)\equiv g(x)\ \ mod\ k(x)$$

$f(x)$ 与 $g(x)$ $mod\ k(x)$ 同余，其充要条件是 $k(x)\mid (f(x)-g(x))$。

多项式的同余式和整数的同余式有相同的性质，列举在下面而不加证明。

(i) 如果 $f_1(x)\equiv g_1(x)\ \ mod\ k(x)$

$f_2(x)\equiv g_2(x)\ \ mod\ k(x)$

则 $f_1(x)+f_2(x)\equiv g_1(x)+g_2(x)\ \ mod\ k(x)$

(ii) 如果 $f(x)\equiv g(x)\ \ mod\ k(x)$

而 $\varphi(x)$ 是任意多项式，则

$$\varphi(x)f(x)\equiv\varphi(x)g(x)\ \ mod\ k(x)$$

(iii) 如果 $f(x)\equiv g(x)\ \ mod\ k(x)$

$g(x)\equiv u(x)\ \ mod\ k(x)$

则 $f(x)\equiv u(x)\ \ mod\ k(x)$

(iv) 如果 $f_1(x)\equiv g_1(x)\ \ mod\ k(x)$

$f_2(x)\equiv g_2(x)\ \ mod\ k(x)$

则 $f_1(x)\cdot f_2(x)\equiv g_1(x)\cdot g_2(x)\ \ mod\ k(x)$。

(v) 如果 $\varphi(x)f(x)\equiv\varphi(x)g(x)\ mod k(x)$

但 $(\varphi(x),\ k(x))=1$，则 $\varphi(x)$ 可以消去。

$f(x)\equiv g(x) \mod k(x)$ 。

(vi) 如果 $f(x)\equiv g(x) \mod h(x)$ ，则 $[f(x), h(x)] = [g(x), h(x)]$ 。特别当 $(f(x), h(x)) = 1$ 时，则也有 $(g(x), h(x)) = 1$ 。

(vii) 如果 $f(x)\equiv g(x) \mod h(x)$，$d(x)$ 是 $f(x), g(x)$ 和 $h(x)$ 的公因式。令 $f(x)=f_1(x)d(x)$，$g(x)=g_1(x)d(x)$ $h(x)=h_1(x)d(x)$。

则 $f_1(x)\equiv g_1(x) \mod h_1(x)$ 。

(viii) 如果 $f(x)\equiv g(x) \mod h(x)$，$h_1(x)\mid h(x)$，则 $f(x)\equiv g(x) \mod h_1(x)$

2．同余方程

在多项式的同余式中含有一个未知的量（是指未知的多项式不是指 x）则这个同余式叫做多项式的同余方程。什么叫做同余方程的解？如何区别两个解相同或不相同？它们的意义完全和整数的同余方程所规定的意义一样。在这里就不一一重复了。我们只着重讨论一元一次同余方程和一元一次同余方程组的问题。它们的结论和用到的证明方法也都和整数的情况完全一样。因此，我们只把结论罗列在下面，证明就不重复了。

（1）一次同余方程

$f(x)y\equiv g(x) \mod h(x)$

有解的充要条件是 $[f(x), h(x)] \mid g(x)$。在有解的情况下设 $(f(x), h(x)) = d(x)$，$h(x)=h_1(x)d(x)$。任意两个解 $\mod h_1(x)$ 都同余。设 $y=\varphi(x)$ 为其一解。则全部的解可写成 $\varphi(x)+q(x)\cdot h_1(x)$

其中 $q(x)$ 取次数$<\partial^0 d(x)$ 的一切多项式。（包括0）共有 p 个解，$m=\partial^0 d(x)$。特别，当 $(f(x), h(x))=1$ 时，方程恒有解而且只有一个解。

（2）设 $h_1(x)$，$h_2(x)$，…，$h_r(x)$ 是 r 个两两互素的多项式。则下列同余方程组

$$\begin{cases} y \equiv 0 \mod h_1(x) \\ \cdots \quad \cdots \\ y \equiv 0 \mod h_{i-1}(x) \\ y \equiv 1 \mod h_i(x) \\ y \equiv 0 \mod h_{i+1}(x) \\ \cdots \quad \cdots \\ y \equiv 0 \mod h_r(x) \end{cases} \qquad 1 \leqslant i \leqslant r,$$

恒有解。记 $f_i(x)=\prod_{\substack{j=1 \\ j\neq i}}^{r} k_i(x)$，并设 $\varphi_i(x)$ 是同余方程

$$f_i(x)y \equiv 1 \mod h_i(x)$$

的一解。则 $y=f_i(x)$。$\varphi_i(x)$ 就是上方程组的一解。

（3）孙子定理的推广。设 $h_1(x)$，$h_2(x)$，…，$h_r(x)$ 是两两互素的多项式。$g_1(x)$，$g_2(x)$，…，$g_r(x)$ 为任意给定的多项式。则下列一次同余方程组

$$\begin{cases} y \equiv g_1(x) \mod h_1(x) \\ y \equiv g_2(x) \mod h_2(x) \\ \cdots \\ y \equiv g_r(x) \mod h_r(x) \end{cases}$$

恒有解。记 $h(x)=\prod_{i=1}^{r} h_i(x)$。则任意两解 $\mod h(x)$ 同余。就是说，把解限制在次数 $<\partial^0 h(x)$ 的范围内，则解就是唯

一的。记（2）中方程的解为 $e_i(x)=f_i(x)\cdot\varphi_i(x)$，$i=1$，2，…，r，则上述方程组的解为

$$c(x)=g_1(x)c_1(x)+g_2(x)c_2(x)+\cdots+$$
$$+g_r(x),c_r(x)\ 。$$

第十三节　欧拉函数　欧拉—费尔马定理的推广和多项式的周期

整数环中的欧拉函数和欧拉—弗尔马定理可以推广到有限域 F_p 上一元多项式环。不仅这两个结果重要而且所用的证明方法也是重要的。因此，我们不仅叙述结论而且给予平行的证明。

1．欧拉函数的推广

设 $f(x)$ 是 $F_p[x]$ 中一个 n 次多项式。而且 $f(x)$ 已分解成不同的不可约因式 $p_1(x)$，…，$p_r(x)$ 的方幂的乘积

$$f(x)=p_1^{e_1}(x)p_2^{e_2}(x)\cdots p_r^{e_r}(x)，\ e_i\geqslant 1\ 。$$

$p_i(x)$ 的次数记作 n_i。

在 $F_p[x]$ 内次数$<$而且与 $f(x)$ 互素的多项式的个数记作 $\varphi(f)$。$\varphi(f)$ 是推广了的欧拉函数。我们有类似的

定理 1　设 $f(x)$ 为 $F_p[x]$ 中一个 n 次多项式，$p_1(x)$，$p_2(x)$，…，$p_r(x)$ 为 $f(x)$ 的全部不同的不可约因式。$p_i(x)$ 的次数记作 n_i。则 $f(x)$ 的欧拉函数

$$\varphi(f)=p^n\prod_{i=1}^{r}\left(1-\frac{1}{p^{n_i}}\right)\ 。$$

证明，先证明两条引理

引理 1。设 $g(x)$，$h(x)\in F_p[x]$ 是两个互素的多项式。则

$$\varphi\ (g(x)\cdot h(x)) = \varphi\ (g(x))\cdot\varphi\ (h(x))\ 。$$

证明。用 $r(x)$，$s(x)$ 和 $t(x)$ 分别表示与 $g(x)\cdot h(x)$，$g(x)$ 和 $h(x)$ 互素的多项式而且次数

$$\partial^0 r(x)<\partial^0(g\cdot h),\ \partial^0 s(x)<\partial^0 g(x),$$
$$\partial^0 t(x)<\partial^0 h(x)$$

它们分别有 $\varphi(f(x),\ h(x))$，$\varphi(g(x))$，$\varphi(h(x))$ 个。

对于每个 $v(x)$，存在一个 $s(x)$ 和一个 $t(x)$ 使得

$$v(x)\equiv s(x)\ \ mod\ g(x),$$
$$v(x)\equiv t(x)\ \ mod\ h(x)\ ,$$

而且 $s(x)$ 和 $t(x)$ 被 $v(x)$ 唯一决定。因为 $v(x)$ 与 $g(x)$，$h(x)$ 互素，因而与 $g(x)$ 和 $h(x)$ 都互素，因而 $s(x)$ 与 $g(x)$ 互素，$t(x)$ 与 $h(x)$ 互素。

反之，对于任一对 $s(x)$，$t(x)$，同余方程组

$$\begin{cases} y\equiv s(x)\ \ mod\ g(x) \\ y\equiv t(x)\ \ mod\ h(x) \end{cases}$$

按照孙子定理，有唯一解。这个解一定是某个 $v(x)$。这是因为，$s(x)$ 与 $g(x)$ 互素，因而 $v(x)$ 与 $g(x)$ 互素。$t(x)$ 与 $h(x)$ 互素，因而 $v(x)$ 与 $h(x)$ 互素。所以 $v(x)$ 与 $g(x)$，$h(x)$ 互素。

由此可知，$v(x)$ 的个数 $\varphi(g(x),\ h(x))$ 等于由 $s(x)$，$t(x)$ 组成的 $(s(x),\ t(x))$ 的个数。而 $(s(x),\ t(x))$ 的个数为 $\varphi(g(x))$，$\varphi(k(x))$。所以

$$\varphi[g(x)\cdot h(x)]=\varphi[g(x)]\cdot\varphi[h(x)]$$

应用引理 1 于 $f(x)$ 的分解式得到

$$\varphi(f(x))=\varphi(p_1^{e_1}(x))\cdot\varphi(p_2^{e_2}(x))\cdots\varphi(p_r^{e_r}(x))。$$

这就把问题归结到

引理2。设$p(x)$为$F_p[x]$中一个m次不可约多项式，e为任意正整数。则

$$\varphi(p^e(x))=p^{me}(1-\frac{1}{p^m})。$$

证明。次数$<em$的多项式（包含0）的个数为p^{me}。计算次数$<me$且与$p^e(x)$不互素的多项式的个数。设$g(x)$与$p^e(x)$不互素且$\partial^0 g(x)<me$。那么，$g(x)$与$p^e(x)$至少有一个公因式$p(x)$。于是

$$g(x)=q(x)\ p(x)$$

而且$\partial^0 q(x)<me-m$。反之，如果$g(x)=q(x)p(x)$而且$\partial^0 q(x)<me-m$，则$g(x)$与$p^e(x)$不互素而且$\partial^0 g(x)<me$。因此，$g(x)$的个数等于$q(x)$的个数p^{me-m}。所以，次数$<me$且与$p^e(x)$互素的多项式的个数等于$p^{me}-p^{me-m}=p^{me}(1-\frac{1}{p^m})$。

根据引理1和引理2

$$\begin{aligned}\varphi(f)&=\varphi(p_1^{e_1}(x))\cdot\varphi(p_2^{e_2}(x))\cdots\varphi(p_r^{e_r}(x))\\&=p^{n_1e_1}(1-\frac{1}{p^{n_1}})\cdot p^{n_2e_2}(1-\frac{1}{p^{n_2}})\\&\quad\cdots p^{n_re_r}(1-\frac{1}{p^{n_r}})\\&=p^n(1-\frac{1}{p^{n_1}})(1-\frac{1}{p^{n_2}})\cdots(1-\frac{1}{p^{n_r}})。\end{aligned}$$

这就证明了定理1。

这个公式和欧拉函数比较，p^n相当于素数p_i的地位。

例。设$p=2$，x^2+x+1和x^3+x+1是$F_2[x]$中不可约多项式。

设 $f(x)=(x^2+x+1)(x^3+x+1)=x^5+x^4+1$。则

$$\varphi(f)=2^5\left(1-\frac{1}{2^2}\right)\left(1-\frac{1}{2^3}\right)=21。$$

次数<5且与$f(x)$互素的多项式共21个。这21个多项式可以表成下列形式

$$u(x)(x^2+x+1)+v(x)(x^3+x+1)$$

其中$u(x)\neq 0$，$\partial^0 u(x)<3$，$v(x)\neq 0$，$\partial^0 v(x)<2$

2．欧拉—费尔马定理的推广

定理2（欧拉—费尔马定理的推广）设$f(x)$是$F_p[x]$内任一个次数$\geqslant 1$的多项式而且$f(0)\neq 0$即$f(x)$与x互素，于是

$$x^{\varphi(f)}\equiv 1 \bmod f(x)$$

其中$\varphi(f)$是推广的欧拉函数，特别，当$f(x)=p(x)$是一个r次不可约多项式时，

$$x^{p^r-1}\equiv 1 \bmod p(x)$$

证明，$\varphi(f)$简记作N，$F_p[x]$内次数$<\partial^0 f(x)$且与$f(x)$互素的多项式。共有N个，分别记作

（1）$r_1(x)$，$r_2(x)$，…，$r_N(x)$

这N个多项式$\bmod f(x)$互不同余，任何一个与$f(x)$互素的多项式，必与（1）中之一同余，而且只与其中之一同余，用x乘（1）中各项得

（2）$x r_1(x)$，$x r_2(x)$，…，$x r_N(x)$

（2）中每个多项式与$f(x)$互素，因而（2）中每个$x\,r_i(x)$必与而且只与（1）之一同余，设$x\,r_i(x)$与$\gamma_{\alpha_i}(x)$同余。

（3） $x\,r_i(x)\equiv\gamma_{\alpha_i}(x)\ mod\ f(x)$，$i=1,\ 2,\ \cdots,\ N$，

由于x与$f(x)$互素，按照第十二节1，（v），当$i\neq j$时，

$$x\,r_i(x)\not\equiv x\,r_j(x)\ mod\ f(x)$$

因而 $$\gamma_{\alpha_i}(x)\not\equiv r_j(x)\ mod\ f(x)$$

可见$\gamma_{\alpha_1}(x)$，$\gamma_{\alpha_2}(x)$，$\cdots$，$\gamma_{\alpha_N}(x)$不过是$r_1(x)$，$r_2(x)$，$\cdots$，$r_N(x)$的某一个排列。将（3）中N个同余式相乘，得

$$x^N\prod_{i=1}^{N}r_i(x)\equiv\prod_{i=1}^{N}\gamma_{\alpha_i}(x)\ mod\ f(x)$$

但是$\prod_{i=1}^{N}r_i(x)=\prod_{i=1}^{N}\gamma_{\alpha_i}(x)$而且与$f(x)$互素，按照第十二节1，（v）消去$\prod_{i=1}^{N}r_i(x)$即得

$$x^N\equiv 1\ mod\ f(x)$$

定理于是证毕。

在定理的证明中，只用到x与$f(x)$互素这一点，因而对于与$f(x)$互素的任一个多项式$g(x)$都有

$$g^N(x)\equiv 1\ mod\ f(x)\ 。$$

仅就$p=2$的情况举例

例1．$p=2$，x^2+x+1是$F_2[x]$内不可约多项式，

$\varphi(f)=2^2(1-\frac{1}{2^2})=3$，所以

$$x^3\equiv 1\ mod(x^2+x+1),$$

实际上，$x^3-1=(x+1)(x^2+x+1)$，$(x^2+x+1)|x^3-1$

例2．$p=2$，x^3+x+1是$F_2[x]$内不可约多项式。

$\varphi(f)=2^3(1-\frac{1}{2^3})=7$　于是

$$x^7\equiv 1\ mod(x^3+x+1)$$

实际上，$x^7-1=(x^3+x+1)(x^3+x^2+1)(x+1)$，

$(x^3+x+1)|x^7-1$。

例3．$p=2$　x^4+x+1是$F_2[x]$内不可约多项式，

$\varphi(f)=2^4(1-\frac{1}{2^4})=15$。于是

$$x^{15}\equiv 1\ mod(x^4+x+1)$$

实际上，$x^{15}-1=(x^4+x+1)(x+1)(x^2+x+1)$

$(x^4+x^3+1)(x^4+x^3+x^2+x+1)$，

$(x^4+x+1)|x^{15}-1$。

例4．$p=2$，$f(x)=(x^2+x+1)(x^3+x+1)$

$=x^5+x^4+1$，$\varphi(f)=2^5(1-\frac{1}{2^2})(1-\frac{1}{2^3})=21$，于是

$$x^{21}\equiv 1\ mod\ f(x)$$

可用带余除法验算

3．多项式的周期

设$f(x)$为$F_p[x]$内任一次数$\geqslant 1$的多项式而且$f(0)\neq 0$，根据本节定理2，$f(x)|x^{\varphi(f)}-1$，必须存在一个最小正整数e使得

$$f(x)|x^e-1$$

e 就叫做 $f(x)$ 的周期。

特别二项多项式 x^r-1 的周期就是 r。

为了下面要用到，先讲一个事实，

$x^r-1 \mid x^s-1$ 的充要条件是 $r \mid s$。

证明. 先证充分性。设 $r \mid s$。则 $s=kr$，

$$x^s-1=x^{kr}-1=(x^r-1)(x^{r(k-1)}+x^{r(k-2)}+\cdots+x^r+1)。$$

所以 $x^r-1 \mid x^s-1$。反之，设 $x^r-1 \mid x^s-1$。作带余除法 $s=qr+k$，$0 \leqslant k < r$。于是

$$x^s-1=x^{qr+k}-1=x^{qr+k}-x^k+x^k-1$$
$$=x^k(x^{qr}-1)+x^k-1,$$
$$x^s-1=x^k(x^{qr}-1)+x^k-1。$$

x^r-1 整除等式左边，又整除等式右边第一项，则 x^r-1 整除等式右边第二项。但 $0 \leqslant k < r$，这只有在 $k=0$ 的情况下才是可能的。所以 $k=0$，$r \mid s$。

(i) 设 $f(x)$ 的周期为 e，则

$f(x) \mid x^r-1$

的充要条件是

$e \mid r$

特别 $e \mid \varphi(f)$.

证明. 先证充分性。假设 $e \mid r$，于是 $x^e-1 \mid x^r-1$ 由 $f(x) \mid x^e-1$ 即得 $f(x) \mid x^r-1$。

反之，假设 $f(x) \mid x^r-1$，用 e 除 r 作带余除法

$r=ke+s$，$0 \leqslant s < e$

于是

$$x^r-1=x^{ke+s}-1=x^s(x^{ke}-1)+x^s-1$$