信息安全数学基础

第五章 多项式环

聂旭云
信息与软件工程学院
电子科技大学

信息安全数学基础

多项式同余及剩余类环

聂旭云
信息与软件工程学院
电子科技大学

多项式同余

定义5.3.1　设$g(x), h(x) \in F[x]$，如果$f(x)$整除$g(x) - h(x)$，则称$g(x)$与$h(x)$模$f(x)$同余，记为$g(x) \equiv h(x)(mod\, f(x))$。

定理5.3.1（1）$g(x) \equiv h(x)(mod\, f(x))$当且仅当存在$k(x) \in F[x]$，使得$g(x) = k(x)f(x) + h(x)$。

（2）设$g(x) = q_1(x)f(x) + r_1(x)$，$h(x) = q_2(x)f(x) + r_2(x)$，其中$q_1(x), q_2(x), r_1(x), r_2(x) \in F[x]$，$0 \le deg(r_1(x)) < deg(f(x))$，$0 \le deg(r_2(x)) < deg(f(x))$，则$g(x) \equiv h(x)(mod\, f(x))$当且仅当$r_1(x) = r_2(x)$。

多项式同余的性质

- 定理5.3.2（同余的性质）对于所有$g(x), h(x), g_1(x), h_1(x), s(x) \in F[x]$，以下事实成立

（1）（自反性）$g(x) \equiv g(x)(mod\, f\,(x))$；

（2）（对称性）如果$g(x) \equiv h(x)(mod\, f\,(x))$，则$h(x) \equiv g(x)(mod\, f\,(x))$；

（3）（传递性）如果$g(x) \equiv h(x)(mod\, f\,(x))$且$h(x) \equiv s(x)(mod\, f\,(x))$，则$g(x) \equiv s(x)(mod\, f\,(x))$；

（4）如果$g(x) \equiv g_1(x)(mod\, f\,(x))$且$h(x) \equiv h_1(x)(mod\, f\,(x))$，则

$$g(x) + h(x) \equiv g_1(x) + h_1(x)(mod\, f\,(x))$$

且

$$g(x) \cdot h(x) \equiv g_1(x) \cdot h_1(x)(mod\, f\,(x))。$$

多项式剩余类环

模$f(x)$同余是$F[x]$上的一个等价关系。

每一个多项式$g(x)$都与唯一的一个次数比$deg\,f(x)$低的多项式$r(x)$模$f(x)$同余，用$r(x)$作为包含$g(x)$的等价类的代表。记以$r(x)$为代表元的等价类为$[r(x)]$。记$\langle f(x)\rangle$为$f(x)$生成的理想。有$[r(x)] = r(x) + \langle f(x)\rangle$。

商环

$$F[x]/\langle f(x)\rangle = \{[r(x)] | 0 \leq deg(r(x)) < deg(f(x))\}。$$

也可以简单的将$F[x]/\langle f(x)\rangle$记为

$$F[x]/\langle f(x)\rangle = \{r_{n-1}x^{n-1} + r_{n-2}x^{n-2} + \cdots + r_1 x + r_0 | n = deg(f(x)), r_i \in F, 0 \leq i \leq n-1\}$$

其中定义加法和乘法为模$f(x)$的加法与乘法。

$F[x]/\langle f(x)\rangle$是一个有单位元的交换环。

剩余类环的例子

- 例5.3.1设$\boldsymbol{F}=\boldsymbol{Z}_2$，$\boldsymbol{f(x)=x^2+1}$，则

$$F[x]/\langle f(x)\rangle=\{\mathbf{0},\mathbf{1},\boldsymbol{x},\boldsymbol{x}+\mathbf{1}\}$$

+	0	1	x	x+1
0	0	1	x	x+1
1	1	0	x+1	x
x	x	x+1	0	1
x+1	x+1	x	1	0

*	0	1	x	x+1
0	0	0	0	0
1	0	1	x	x+1
x	0	x	1	x+1
x+1	0	x+1	x+1	0

模多项式乘法逆元

定理5.3.3设$f(x),g(x)\in F[x]$为非零多项式，$g(x)$模$f(x)$有乘法逆元当且仅当$\gcd(f(x),g(x))=1$。

证明：必要性。设$\boldsymbol{gcd(f(x),g(x))=1}$，根据定理5.2.2，存在$\boldsymbol{u(x),v(x)}\in \boldsymbol{F[x]}$，使得$\boldsymbol{u(x)f(x)+v(x)g(x)=1}$，即有$\boldsymbol{-u(x)f(x)=v(x)g(x)-1}$，从而$\boldsymbol{f(x)|v(x)g(x)-1}$，根据同余定义有$\boldsymbol{v(x)g(x)\equiv 1(mod\, f(x))}$。所以$\boldsymbol{g(x)}$模$\boldsymbol{f(x)}$有乘法逆元$\boldsymbol{v(x)}$。

充分性。$\boldsymbol{g(x)}$模$\boldsymbol{f(x)}$有乘法逆元，不妨设为$\boldsymbol{v(x)}$，则有$\boldsymbol{g(x)v(x)\equiv 1(mod\, f(x))}$。根据定理5.3.1，存在$\boldsymbol{k(x)\in F[x]}$，使得$\boldsymbol{g(x)v(x)=k(x)f(x)+1}$，即

$$\boldsymbol{g(x)v(x)-k(x)f(x)=1}。$$

同样根据定理5.2.2，有$\boldsymbol{gcd(f(x),g(x))=1}$。

域

- 推论5.3.1如果$f(x)$在F上不可约，则$F[x]/\langle f(x)\rangle$为一个域。
- 证明：只需证明$F[x]/\langle f(x)\rangle$中任意非零元均有乘法逆元。设$r(x) \neq 0 \in F[x]/\langle f(x)\rangle$，则$0 \leq deg(r(x)) < deg(f(x))$，又$f(x)$在$F$上不可约，所以$gcd(f(x), r(x)) = 1$。根据定理5.3.3，$r(x)$在$F[x]/\langle f(x)\rangle$中有乘法逆元。

- 设$f(x)$的次数为n，$F[x]/\langle f(x)\rangle$中的元素可以表示成次数小于n的多项式，即

  $$F[x]/\langle f(x)\rangle = \{r_{n-1}x^{n-1} + r_{n-2}x^{n-2} + \cdots + r_1 x + r_0 | n = deg(f(x)), r_i \in F, 0 \leq i \leq n-1\}$$

- 当$F = Z_p$时，$F[x]/\langle f(x)\rangle$中元素个数为p^n。

域的例子

- 例5.3.2设$\boldsymbol{F}=\boldsymbol{Z}_2$，$\boldsymbol{f}(\boldsymbol{x})=\boldsymbol{x}^2+\boldsymbol{x}+\mathbf{1}$，则

$$\boldsymbol{F}[\boldsymbol{x}]/\langle \boldsymbol{f}(\boldsymbol{x})\rangle=\{\mathbf{0},\mathbf{1},\boldsymbol{x},\boldsymbol{x}+\mathbf{1}\}$$

+	0	1	x	$x+1$
0	0	1	x	$x+1$
1	1	0	$x+1$	x
x	x	$x+1$	0	1
$x+1$	$x+1$	x	1	0

*	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	$x+1$	1
$x+1$	0	$x+1$	1	x

感 谢 聆 听!

xynie@uestc.edu.cn