第2章 纠错编码的代数基础

第2章 纠错编码的代数基础

◆2.1整数的有关概念 ◆整数与多项式

◆2.2群的基本概念 ◆加法群与乘法群

◆2.3环的基本概念 ◆群、环、域

◆2.4域的基本概念 ◆有限域上的运算

第1讲 整数与多项式

整数中的相关概念	多项式中的相关概念
素数	不可约多项式
公因子	公因子
带余除法	带余除法
辗转相除法	辗转相除法
同余	同余
剩余类	剩余类
剩余类的加法与乘法	模多项式的剩余类的加法与乘法

整数中的一些基本概念

重述几个在编码中常用的概念。

素数：只能被1和它本身整除的整数。

合数：除1和自身外，还存在其他因数的整数。

因子，公因子，最大公因子：

倍数，公倍数，最小公倍数：

带余除法与辗转相除法

带余除法：$a=qb+r \quad 0\le r<b$

辗转相除法：

$a=q_1b+r_1$, $\quad 0\le r_1<b$

$b=q_2r_1+r_2$, $\quad 0\le r_2<r_1$

$r_1=q_3r_2+r_3$, $\quad 0\le r_3<r_2$

… … … …

$r_{n-3}=q_{n-1}r_{n-2}+r_{n-1}$, $\quad 0\le r_{n-1}<r_{n-2}$

$r_{n-2}=q_nr_{n-1}+r_n$, $\quad r_n=0$

带余除法与辗转相除法

例：a=13，b=5

辗转相除法：

$a=q_1b+r_1$， $0\le r_1<b$

$b=q_2r_1+r_2$， $0\le r_2<r_1$

$r_1=q_3r_2+r_3$， $0\le r_3<r_2$

… … … …

$r_{n-3}=q_{n-1}r_{n-2}+r_{n-1}$ ，$0\le r_{n-1}<r_{n-2}$

$r_{n-2}=q_nr_{n-1}+r_n$ ， $r_n=0$

辗转相除法：

$13=2\times5+3$，

$5=1\times3+2$，

$3=1\times2+1$，

$2=2\times1+0$。

7

最大公因子与最小公倍数

辗转相除法：

$a=q_1b+r_1$， $0\le r_1<b$

$b=q_2r_1+r_2$， $0\le r_2<r_1$

$r_1=q_3r_2+r_3$， $0\le r_3<r_2$

… … … …

$r_{n-3}=q_{n-1}r_{n-2}+r_{n-1}$ ，$0\le r_{n-1}<r_{n-2}$

$r_{n-2}=q_nr_{n-1}+r_n$ ， $r_n=0$

最大公因子(a,b)：

$(a,b)=r_{n-1}$

8

用辗转相除法求最大公因子

例：用辗转相除法求13和5的最大公因子。

辗转相除法：

$a=q_1b+r_1$， $0\le r_1<b$

$b=q_2r_1+r_2$， $0\le r_2<r_1$

$r_1=q_3r_2+r_3$， $0\le r_3<r_2$

… … … …

$r_{n-3}=q_{n-1}r_{n-2}+r_{n-1}$ ，$0\le r_{n-1}<r_{n-2}$

$r_{n-2}=q_nr_{n-1}+r_n$ ， $r_n=0$

辗转相除法：

$13=2\times5+3$，

$5=1\times3+2$，

$3=1\times2+1$，

$2=2\times1+0$。

答案：13和5的最大公因子为1。

9

最大公因子与最小公倍数

辗转相除法：

$a=q_1b+r_1$， $0\le r_1<b$

$b=q_2r_1+r_2$， $0\le r_2<r_1$

$r_1=q_3r_2+r_3$， $0\le r_3<r_2$

… … … …

$r_{n-3}=q_{n-1}r_{n-2}+r_{n-1}$ ，$0\le r_{n-1}<r_{n-2}$

$r_{n-2}=q_nr_{n-1}+r_n$ ， $r_n=0$

最大公因子(a,b)：

$(a,b)=r_{n-1}$

最大公因子(a,b)的性质：任意正整数a, b，必存在整数A,B，使(a,b)=Aa+Bb。

最小公倍数$[a,b]$ 的性质：任意正整数a, b，必存在关系式$ab=[a,b](a,b)$。

用辗转相除法求两个整数的最大公因子，并将最大公因子表示成这两个数的线性组合。

10

用辗转相除法求最大公因子

例：用辗转相除法求13和5的最大公因子，并将它表示成13和5的线性组合。

辗转相除法：

$13=2\times5+3$， → $3=13-2\times5$，

$5=1\times3+2$， → $2=5-1\times3$，

$3=1\times2+1$， → $1=3-1\times2$，

$2=2\times1+0$。

$(13,5)=1$

$1=3-2$

$=3-(5-1\times3)$

$=-5+2\times3$

$=-5+2\times(13-2\times5$

$=2\times13+(-5)\times5$

答案：（13，5）= 1 = 2×13 +（-5）×5

11

用辗转相除法求最大公因子

✓课堂练习：用辗转相除法求两个正整数a,b的最大公因子(a,b)，并将它表示为a,b的线性组合。

即：并求出整数A,B, 使得(a,b)=Aa+Bb。

（24，30），（39，16），（101，31）

12

用辗转相除法求最大公因子

✓ 答案：

（24，30）= 6 = 30 +（-1）×24

（39，16）= 1 = 7 × 39 +（-17）×16

（101，31）= 1 = 4 × 101 +（-13）×31

13

整数的同余和剩余类

1. 同余：若两整数a，b被同一正整数d除时，有相同的余数，即

$a=q_1d+r$，　　$b=q_2d+r$，　$0 \le r_1 < d$

则称a，b关于d同余，记作

$$a \equiv b[\bmod d]$$

14

剩余类的加法和乘法

2. 剩余类：模d运算余数相同的元素构成的集合为模d的剩余类，记为 $\bar{0},\bar{1},\cdots\overline{d-1}$,

对应代表元：0，1，…，d-1，共有d个值，称为有d个剩余类。

剩余类之间也可定义加法和乘法运算：

$$\bar{a}+\bar{b}=\overline{a+b} \qquad [\bmod d]$$

$$\bar{a}\cdot\bar{b}=\overline{a\cdot b} \qquad [\bmod d]$$

15

同余和剩余类

例子：　d=7，则

$$\bar{1}+\bar{2}=\overline{1+2}=\bar{3} \qquad [\bmod 7]$$

$$\bar{3}\cdot\bar{5}=\overline{3\cdot 5}=\overline{15}=\bar{1} \qquad [\bmod d]$$

模d的全体剩余类对模d加法和模d乘法满足封闭性，

即假设 $D=\{\bar{0},\bar{1},\cdots\overline{d-1}\}$,

如果 $a,b\in D$, 则必有

$$(a+b)[\bmod d]\in D$$

$$(a\cdot b)[\bmod d]\in D$$

16

剩余类的运算

例子：求出模2和模3的加法表和乘法表。

+	0	1
0	0	1
1	1	0

×	0	1
0	0	0
1	0	1

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

×	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

17

剩余类的运算

✓ 课堂练习：求出模5和模6的加法表和乘法表。

18

剩余类的运算

✓ 答案：模5的加法表和乘法表：

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

×	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

19

剩余类的运算

✓ 答案：模6的加法表和乘法表：

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

×	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

20

多项式与不可约多项式

系数取自集合F的多项式的表示形式为

$$f(x)=f_n x^n+f_{n-1}x^{n-1}+\cdots+f_1 x+f_0,\qquad f_i\in F$$

首一多项式：多项式最高次数是系数为1，即 $f_n=1$

多项式的阶：多项式中系数不为0的x的最高次数，记为：$\partial^{\circ} f(x)$

既约（不可约）多项式：阶大于0且在给定集合F上除了常数和常数与本身的乘积外，不能被其他多项式除尽的多项式。

21

不可约多项式

例2：x^2+1是阶为2的首一多项式；

它在实数集合上是不可约多项式；

在复数集合上不是不可约多项式，

因为在复数集合上可以分解为：

$$x^2+1=(x+i)(x-i)$$

22

多项式的带余除法

定理(多项式的带余除法)：给定任意两个多项式 $f(x)$ 和 $p(x)$，$\partial^{\circ} p(x)\le\partial^{\circ} f(x)$ 一定存在唯一的多项式 $q(x)$ 和 $r(x)$, 使得：

$f(x)=q(x)p(x)+r(x)$, $0\le\partial^{\circ} r(x)<\partial^{\circ} p(x)$ 。

其中，$p(x)$称为模多项式，$r(x)$称为余式，记为

$$r(x)=f(x)\ [\mathrm{mod}\, p(x)]$$

23

多项式的带余除法

例：$a(x)=x^5+x^4+x^3+x^2+x+1$

$b(x)=x^4+x^2+x+1$

分别在$Z_2[x]$和$Z_3[x]$中做多项式的带余除法。

解：$Z_2[x]$中：

$$\begin{array}{r|l} & x\quad +1 \\ \hline x^4+x^2+x+1 & x^5+x^4+x^3+x^2+x+1 \\ & x^5+\quad x^3+x^2+x \\ \hline & \quad x^4\qquad\qquad +1 \\ & \quad x^4\quad +x^2+x+1 \\ \hline & \qquad\qquad x^2+x \end{array}$$

在$Z_2[x]$中：$a(x)=(x+1)b(x)+x^2+x$

24

多项式的带余除法

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

$b(x) = x^4 + x^2 + x + 1$

分别在$Z_2[x]$和$Z_3[x]$中做多项式的带余除法。

解：$Z_3[x]$中：

$$
\begin{array}{r|l}
 & x + 1 \\
\hline
x^4 + x^2 + x + 1 & x^5 + x^4 + x^3 + x^2 + x + 1 \\
 & x^5 + x^3 + x^2 + x \\
\hline
 & x^4 + 1 \\
 & x^4 + x^2 + x + 1 \\
\hline
 & 2x^2 + 2x
\end{array}
$$

在$Z_3[x]$中： $a(x) = (x + 1)b(x) + 2x^2 + 2x$

25

多项式的相关概念

整除，不整除，

因式，公因式，最大公因式，

倍式，公倍式，最小公倍式；

余式，同余

26

不可约多项式的判断

余元定理：设 $f(x)$ 是$F[x]$中的多项式。而$\alpha \in F$，那么用一次多项式 $x-\alpha$ 去除 $f(x)$ 所得的余式是F中的元素 $f(\alpha)$。

证明：由多项式带余除法：

$$f(x) = q(x)(x-\alpha) + r$$

所以，$f(\alpha)=r$，得证。

27

不可约多项式的判断

余元定理：设 $f(x)$ 是$F[x]$中的多项式。而$\alpha \in F$，那么用一次多项式 $x-\alpha$ 去除 $f(x)$ 所得的余式是F中的元素 $f(\alpha)$。

$$\boxed{f(x) = q(x)(x-\alpha) + f(\alpha)}$$

推论：设 $f(x)$ 是$F[x]$中的多项式。而$\alpha \in F$，那么α是$f(x)$的根当且仅当 $x-\alpha$ 整除 $f(x)$。

28

不可约多项式的判断

例：分别判断 $f(x) = x^2+1$是否为$Z_2[x]$和$Z_3[x]$上的不可约多项式。

解：$Z_2[x]$中：
一次因式：x，$x-1$
$f(0) = 1$；$f(1) = 0$；
1是$f(x)$的根，
所以，$x-1$ 整除 $f(x)$。
∴ $f(x)$在$Z_2[x]$可约。

解：$Z_3[x]$中：
一次因式：x，$x-1$，$x-2$
$f(0) = 1$；$f(1) = 2$；$f(2) = 2$；
0,1,2都不是$f(x)$的根，
所以，$f(x)$在$Z_3[x]$上无一次因式，
∴ $f(x)$在$Z_3[x]$不可约。

推论(余元定理)：设 $f(x)$ 是$F[x]$中的多项式。而$\alpha \in F$，那么α是$f(x)$的根当且仅当 $x-\alpha$ 整除 $f(x)$。

29

不可约多项式的判断

✓ 课堂练习：分别判断 $f(x) = x^3+x+1$是否为$Z_2[x]$和$Z_3[x]$上的不可约多项式。

解：$Z_2[x]$中：
一次因式：x，$x-1$
$f(0) = 1$；$f(1) = 0$；
1是$f(x)$的根，
所以，$x-1$ 整除 $f(x)$。
∴ $f(x)$在$Z_2[x]$可约。

解：$Z_3[x]$中：
一次因式：x，$x-1$，$x-2$
$f(0) = 1$；$f(1) = 2$；$f(2) = 2$；
0,1,2都不是$f(x)$的根，
所以，$f(x)$在$Z_3[x]$上无一次因式，
∴ $f(x)$在$Z_3[x]$不可约。

推论(余元定理)：设 $f(x)$ 是$F[x]$中的多项式。而$\alpha \in F$，那么α是$f(x)$的根当且仅当 $x-\alpha$ 整除 $f(x)$。

30

不可约多项式的判断

✓ 课堂练习：分别判断 $f(x) = x^3+x+1$ 是否为 $Z_2[x]$ 和 $Z_3[x]$ 上的不可约多项式。

解：$Z_2[x]$ 中：

一次因式：x，$x-1$

$f(0) = 1$；$f(1) = 1$；

0，1都不是 $f(x)$ 的根，

∴ $f(x)$ 在 $Z_2[x]$ 不可约。

解：$Z_3[x]$ 中：

一次因式：x，$x-1$，$x-2$

$f(0) = 1$；$f(1) = 0$；$f(2) = 2$；

1是 $f(x)$ 的根，

所以，$x-1$ 整除 $f(x)$。

∴ $f(x)$ 在 $Z_3[x]$ 可约。

31

多项式的辗转相除法

例：用辗转相除法求 $Z_2[x]$（或 $Z_3[x]$）中多项式 $a(x) = x^5 + x^4 + x^3 + x^2 + x + 1$ 和 $b(x) = x^4 + x^2 + x + 1$ 的最高公因式 $gcd(a(x),b(x))$；并将 $gcd(a(x),b(x))$ 表示成 $a(x)$ 和 $b(x)$ 的线性组合，即

$$gcd(a(x),b(x))=c(x)a(x)+d(x)b(x)$$

32

多项式的辗转相除法

例：用辗转相除法求 $Z_2[x]$（或 $Z_3[x]$）中多项式 $a(x) = x^5 + x^4 + x^3 + x^2 + x + 1$ 和 $b(x) = x^4 + x^2 + x + 1$ 的最高公因式 $gcd(a(x),b(x))$；并将 $gcd(a(x),b(x))$ 表示成 $a(x)$ 和 $b(x)$ 的线性组合，即 $gcd(a(x),b(x))=c(x)a(x)+d(x)b(x)$

例：在 $Z_2[x]$ 中做辗转相除法：

（1）$a(x) = (x + 1)b(x) + x^2 + x$；

（2）$b(x) = (x^2 + x)(x^2 + x) + x + 1$；

（3）$x^2 + x = x(x + 1)$；

∴ $gcd(a(x),b(x)) = x + 1$

求线性组合：

$x + 1 = b(x) + (x^2 + x)(x^2 + x)$

$= b(x) + (x^2 + x)(a(x) + (x + 1)b(x))$

$= (x^2 + x)\, a(x) + (1 + (x^2 + x)(x + 1))b(x)$

$= (x^2 + x)\, a(x) + (x^3 + x + 1)b(x)$

33

多项式的辗转相除法

答案：

在 $Z_2[x]$ 中，

$gcd(a(x), b(x)) = x + 1$

$= (x^2+x)a(x) + (x^3+x+1)\, b(x)$；

在 $Z_3[x]$ 中，

$gcd(a(x), b(x)) = 1$

$= (2x^3 + 2x^2)a(x) + (x^4+2x^3 + x^2 + 2x + 1)\, b(x)$；

34

多项式的最大公因式

✓ 课堂练习：用辗转相除法求 $Z_3[x]$ 中多项式 $a(x) = x^4 + x + 2$ 和 $b(x) = x^3 + 2x + 1$ 的最高公因式 $gcd(a(x), b(x))$；并将 $gcd(a(x), b(x))$ 表示成 $c(x)\, a(x) + d(x)\, b(x)$ 的形式。

35

答案：

$gcd(a(x), b(x)) = 1$

$= 2xa(x) + (x^2 + 1)b(x)$；

36

多项式的同余

1. 多项式的同余：若

$$a(x)= q_1(x)\cdot p(x)+ r(x),$$
$$b(x)= q_2(x)\cdot p(x)+ r(x),$$
$$0 < \partial^o r(x) < \partial^o p(x),$$

则$a(x) \equiv b(x)[\ mod\ p(x)]$。

37

多项式的剩余类

模$p(x)$运算余数相同的多项式集合，记为$\overline{r(x)}$或$r(x)$。

多项式的剩余类具有与整数的剩余类相同的性质。

剩余类的加法:

$a(x) \oplus b(x)=a(x)+ b(x)$

剩余类的乘法:

$a(x)\otimes b(x)=[a(x)\ b(x)][mod\ p(x)]$

38

多项式剩余类的加法和乘法

例：系数取自$\{0,1\}$上的任意多项式以$p(x) = x^3 + x + 1$为模，设所得余式为$r(x)$，则有$0\le\partial^o(r(x))<3$，

全体剩余类为：

$\{0, 1, x, x+1, x^2, x^2+1, x^2+x, x^2+x+1\}$

剩余类的加法：

$(x+1) \oplus (x^2+x) = x^2+1$

剩余类的乘法：

$(x+1) \otimes (x^2+x) =((x+1)\times(x^2+x))[mod\,p(x)]$

$=(x^3+x)[mod\,p(x)]=1$

39

多项式剩余类的加法和乘法

✓ 课堂练习：系数取自{0，1，2}上的任意多项式以$p(x) = x^3 + x + 1$为模，

（1） 求全体剩余类$Z_3[x]_{p(x)}$，

（2） 求$(x+1)\oplus(x^2+x)$，

（3） 求 $(x+1)\otimes(x^2+x)$。

40