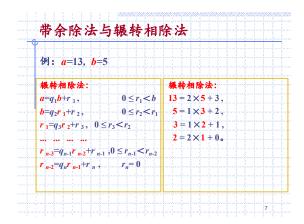
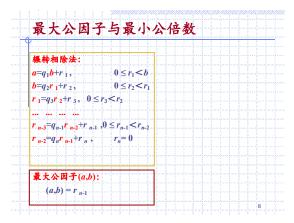


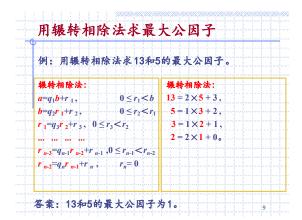
整数中的一些基本概念
重述几个在编码中常用的概念。

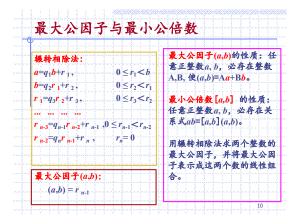
素数: 只能被1和它本身整除的整数。
合数: 除1和自身外, 还存在其他因数的整数。

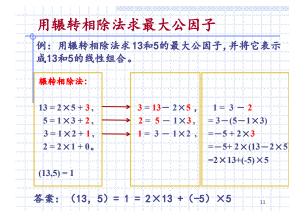
因子, 公因子, 最大公因子:
倍数, 公倍数, 最小公倍数:

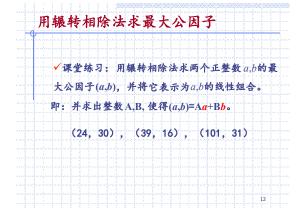












用辗转相除法求最大公因子

✓ 答案:

$$(24, 30) = 6 = 30 + (-1) \times 24$$

 $(39, 16) = 1 = 7 \times 39 + (-17) \times 16$

 $(101, 31) = 1 = 4 \times 101 + (-13) \times 31$

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

 $a \equiv b [\mod d]$

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 $\bar{0}, \bar{1}, \dots \bar{d-1},$

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:

$$\overline{a} + \overline{b} = \overline{a + b} \pmod{d}$$
 $\overline{a} \cdot \overline{b} = \overline{a \cdot b} \pmod{d}$

同余和剩余类

例子: d=7,则

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

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

模心的全体剩余类对模心加法和模心乘法满足封闭性、

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

如果 $a,b \in D$,则必有

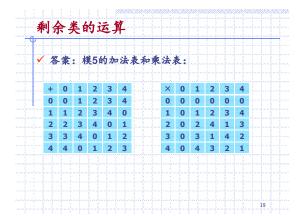
 $(a+b)[\operatorname{mod} d] \in D$

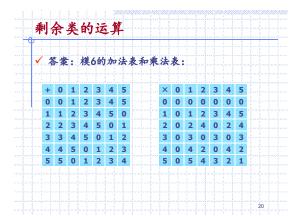
 $(a \cdot b)[\operatorname{mod} d] \in D$

例子:求出模2和模3的加法表和乘法表。													
	+	C)	1			×		D	1			
	0	C)	1			0) (0	0			
	1	1	ų,	0			1		0	1			
nonunununun	+	0	1	2	+		×	0	1	2			
	0	0	1	2	III.		0	0	0	0			
	1	1	2	0	++-		1	0	1	2			
	2	2	0	1	Ш		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。





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

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: $\partial^* f(x)$

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。

不可约多项式 例2: x²+ 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: x²+ 1=(x+i)(x-i)

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), $\partial p(x) \le \partial f(x)$ 一定存在唯一的 多项式 q(x) 和 r(x), 使得:

 $f(x) = q(x)p(x) + r(x), \ 0 \le \partial r(x) < \partial p(x) .$

其中,p(x)称为模多项式,r(x)称为余式,记为

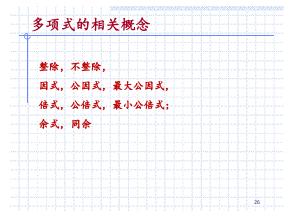
r(x)=f(x) [mod p(x)]

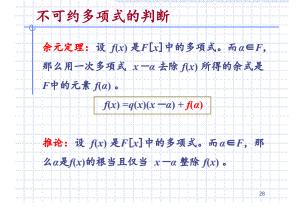
多项式的带余除法

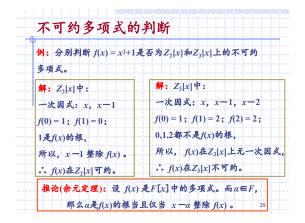
例: $a(x) = x^5 + x^4 + x^3 + x^2 + x + 1$ $b(x) = x^4 + x^2 + x + 1$ 分别在 $Z_2[x]$ 和 $Z_3[x]$ 中做多项式的带余除法。

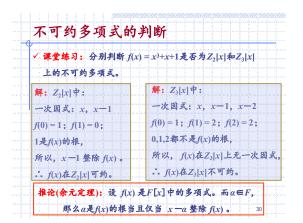
解: $Z_2[x]$ 中: x + 1 $x^4 + x^2 + x + 1$ $x^5 + x^4 + x^3 + x^2 + x + 1$ $x^5 + x^4 + x^3 + x^2 + x + 1$ $x^4 + x^2 + x + 1$ $x^2 + x + x^2 + x + 1$ $x^4 + x^2 + x + 1$ $x^2 + x + x + 1$

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: x + 1 $x^5 + x^4 + x^3 + x^2 + x + 1$ $x^5 + x^3 + x^2 + x$ $x^4 + x^2 + x + 1$ $x^4 + x^4 + x$









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 $Z_2[x] = Z_3[x]$ 上的不可约多项式。

解: Z₂[x]中:

一次因式: x, x-1 f(0) = 1; f(1) = 1; 0, 1都不是f(x)的根, 解: Z₃[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Z₃[x]可约。

... f(x)在Z₂[x]不可约。

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)

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Z₂[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) $x^2 + x = x(x+1)$;

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

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

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

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

多项式的最大公因式

✓课堂练习:用辗转相除法求 Z₃[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。

答案:

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

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

多项式的同余

1. 多项式的同余: 若

 $\begin{aligned} a(x) &= q_1(x) \cdot p(x) + r(x), \\ b(x) &= q_2(x) \cdot p(x) + r(x), \\ 0 &< \partial^o r(x) < \partial^o p(x), \end{aligned}$

 $\mathbb{M} a(x) \equiv b(x) [\bmod p(x)].$

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 $0 \le \partial^0(r(x)) \le 3$,

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:

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

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

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) $\dot{x}(x+1)\oplus(x^2+x)$,
- (3) $\not x (x+1) \otimes (x^2+x)$.

40