纠错码及其在计算机系统中的应用

西北电讯工程学院

顾慰文 编

国防工业出版社

纠错码及其在计算机系统中的应用

西北电讯工程学院

顾慰文 编

国防工业出版社

内 容 简 介

纠错码是信息论的重要组成部分，近年来在计算机系统中得到了广泛的应用。本书共分七章，前两章介绍纠错码用到的数论及近代代数方面的数学预备知识；第三章介绍通讯、计算机与纠错码；第四章介绍几种常用的检错码；第五、六章分别介绍线性分组码及循环码；第七章介绍循环码在计算机系统中的应用。

纠错码及其在计算机系统中的应用

西北电讯工程学院

顾慰文 编

*

国防工业出版社出版

北京市书刊出版业营业许可证出字第074号

西北电讯工程学院印刷厂印刷

内 部 发 行

*

开本 787×1092 1/16 印张 17

印刷字数 435千字 印数 1—5000册

1980年第一版 1980年6月第一次印刷

统一书号：N15034(教-61) 定价：1.76 元

前　言

纠错编码理论自五十年代开始至今已发展成为信息论这门学科的一个重要组成部分，并在理论上已有相当丰富的内容。近年来，随着数字通信、计算技术及数据处理等科学技术领域广泛采用纠错码而迅速发展，特别在计算机系统及数据通讯系统中已得到很多应用，并展现出新的发展前景。

目前，计算机系统的可靠性已成为突出而重要的问题，容错技术也已成为新的一代计算机的重要标志，我国新的计算机的设计，也日益重视采用冗余编码等容错技术。

本书主要介绍纠错编码的基本理论，并在这基础上阐述它们在计算机系统与计算机网络中的应用，以利于计算技术方面的有关教师、学生及科技工作者学习与应用纠错码。全书共分七章，前两章介绍编码理论用到的一些数学预备知识，包括数论和近代代数方面的有关内容；第三章介绍通讯、计算机与纠错码；第四章介绍几种常用的检错码；第五、六章分别介绍线性分组码及循环码；由于循环码在磁带、磁盘等存贮器及计算机网通讯控制中应用较广，故专设第七章作具体介绍。三、四、五、六、七章构成纠错码的基本概念，以及目前在计算机中得到广泛应用的各种纠错码的基本内容。有的章给出一些习题，每章后均附有参考书目。

本书初稿于1976年写成，曾由西北电讯工程学院计算机专业作为“纠错码及其在计算机系统中的应用”课的参考书，今在此基础上进行补充修改而成，以适应计算机工程与科学专业开设此门选修课的需要，也可供有关科技工作者参考。编写过程中曾得到谢志良同志的鼓励与提出许多宝贵意见，北京大学的孙山泽同志审查了本书，西北电讯工程学院的梁传甲、王新梅同志又审阅了第三、五、六章。排印过程中又得到西北电讯工程学院计算机专业许多同志的协助，在此一并表示感谢。但由于笔者水平有限，定有不妥之处，恳切希望读者批评指正。

编　者

目　录

第一章　数论中有关的基本概念

第二章　近代代数的基本概念

第三章　通讯、计算机与纠错码

第四章　几种常用的检错码

第五章　线性分组码

第六章　循环码

第七章　循环码在计算机系统中的应用

第一章　数论中有关的基本概念

由于编码理论中常常遇到一些数论的概念，本章介绍有关它们的基本概念，作为初学者的数学预备知识，更进一步的知识请参阅[1][2]。

全体整数（包括正、负数和零如…－2，－1，0，1，2，…）集合 I 中任意两个数 a 和 b，对于加法和乘法运算其结果仍然是整数，称集合 I 对这两种运算是自封的。但是 a 被 b 除（$b\neq 0$）所得的商，就不一定是整数，它可以是整数，也可以不是整数而是有理数。

令 α 为一实数，今后常以$[\alpha]$表示不超过 α 的最大整数，例如$[\pi]=3$。有下列不等式：

$$[\alpha]\leqslant\alpha<[\alpha]+1$$

令α 为有理数 $\frac{a}{b}$，$b<0$则有

$$0\leqslant\frac{a}{b}-\left[\frac{a}{b}\right]<1$$

$$0\leqslant a-\left[\frac{a}{b}\right]b<b$$

得到

$$a=\left[\frac{a}{b}\right]b+r,\quad 0\leqslant r<b$$

1.1 整　除　性

设任意两个整数 a 和 b（$b>0$）。假如用 b 去除 a 所得的商是 q，而余数是 r，则可唯一地写成下式

$$a=qb+r,\qquad 0\leqslant r<b \tag{1.1.1}$$

例如　$b=15$，有$170=11\cdot 15+5$，$0<5<15$

若 $r=0$，就称 a 是 b 的倍数，或 b 是 a 的约数（或因数），也可以说 a 被 b 除尽（即整除），或 b 除尽 a，记为 $b|a$。若 b 除不尽 a，可表为 $b\nmid a$。

为了以后讨论编码理论的需要，我们在讨论整数的同时，将具有类似性质的多项式也一并提出来加以对照。

多项式的整除性

设任意两个多项式 a(x) 和 b(x)，而 $b(x)\neq 0$。

$$a(x)=a_{n-1}x^{n-1}+a_{n-2}x^{n-2}+\cdots+a_1x+a_0$$

$$b(x)=b_kx^k+b_{k-1}x^{k-1}+\cdots+b_1x+b_0$$

$$a(x)=q(x)b(x)+r(x),\ \partial^0 r(x)<\partial^0 b(x) \tag{1.1.2}$$

$\partial^0 r(x)$表示多项式 r(x)的次数。当 $r(x)=0$ 时，说明 a(x)被 b(x)除尽，或 b(x)可整除 a(x)，记为 $b(x)|a(x)$。

多项式除法与整数不同之处，要注意除法进行到其余式 r(x) 的次数小于除式 b(x)的次

数时（即 $\partial^0 r(x) < \partial^0 b(x)$）才停止。其中商式 $q(x) = q_{n-k-1}x^{n-k-1} + \cdots q_1 x + q_0$。

例如，系数只取 0 或 1 的多项式

$$x^5 + x^4 + x^2 + 1 = (x^2 + x + 1)(x^3 + x + 1) + x^2 \tag{1.1.3}$$

可列成如下竖式

$$\begin{array}{r|l} & x^2 + x + 1 \quad \text{——商式} \\ x^3 + x + 1 & x^5 + x^4 \quad + x^2 \quad + 1 \quad \text{——被除式} \\ \text{除式} & x^5 \quad + x^3 + x^2 \\ \hline & x^4 + x^3 \quad + 1 \\ & x^4 \quad + x^2 + x \\ \hline & x^3 + x^2 + x + 1 \\ & x^3 \quad + x + 1 \\ \hline & x^2 \quad \text{——余式} \end{array} \tag{1.1.4}$$

为简单起见，可以只列出各项系数进行运算，如下式

$$\begin{array}{r|l} & 111 \\ 1011 & 110101 \\ & 1011 \\ \hline & 11001 \\ & 1011 \\ \hline & 1111 \\ & 1011 \\ \hline & 100 \end{array} \tag{1.1.5}$$

1.2 最大公约数和最小公倍数

1.2.1 最大公约数

设 a,b,c 都是整数，而 $c \neq 0$，如果 c 既是 a 又是 b 的约数，就称 c 是 a 和 b 的公约数。当 a，b 不全为 0 时，在 a 和 b 的公约数中最大者称为最大公约数，记为(a,b)或 GCD(a, b)。如果 a、b 全等于 0，(0,0)就没有意义。当 a 和 b 的最大公约数为 1 时，即(a，b) = 1，称 a 和 b 互素。例如(25，36) = 1，即数 25 和 36 互素；又如数 8、13、21，由于(8，13) = (8，21) = (13，21) = 1，它们是两两互素的。

类似可定义多项式 a(x)和 b(x)的公约式（或公因式），它是同时能除尽这两个多项式者，其中次数最高的公约式称为 a(x)及 b(x)的最大公约式(或称为最高公因式)，记为(a(x)，b(x))。因最大公约式很多，为唯一决定起见，取最大公约式中(a(x)，b(x)) = d(x)之最高次方的系数为 1 的那个最大公约式为最大公约式。

顺便有如下定义：

定义：首项系数为 1 的多项式称为首一多项式，有下列形式

$$d(x) = x^n + d_{n-1}x^{n-1} + \cdots + d_1 x + d_0 \tag{1.2.1}$$

其中最高项 x^n 之系数为 1。

在系数取 0 和 1 的二进制多项式情况下，公约式则总是首一多项式。

同样，(a(x)，b(x)) = 1，则两多项式称为互素的。

为了研究最大公约数及其重要性质，先讨论欧几里得 (Euclid) 除法律，即转辗相除法。

设 a 和 b 都是正整数，可写成下式：

$$
\begin{aligned}
a &= q_1 b + r_1 \quad , & 0 < r_1 < b \\
b &= q_2 r_1 + r_2 \quad , & 0 < r_2 < r_1 \\
r_1 &= q_3 r_2 + r_3 \quad , & 0 < r_3 < r_2 \\
&\cdots & \cdots \\
r_{n-3} &= q_{n-1} r_{n-2} + r_{n-1}, & 0 < r_{n-1} < r_{n-2} \\
r_{n-2} &= q_n r_{n-1} + r_n \quad , & 0 < r_n < r_{n-1} \\
r_{n-1} &= q_{n+1} r_n
\end{aligned}
\tag{1.2.2}
$$

从 (1.2.2) 式中最后一式看出 $r_n \mid r_{n-1}$，$r_{n+1} = 0$。

现从上到下研究 (1.2.2) 式，a 和 b 的所有公约数合于 b 和 r_1 的所有公约数，也合于 r_1 和 r_2 的所有公约数，…，也合于 r_{n-1} 和 r_n 的所有公约数，最后合于 r_n 的所有公约数，所以有

$$
(a,\ b) = (b,\ r_1) = (r_1 r_2) = \cdots = (r_{n-1},\ r_n) = r_n \tag{1.2.3}
$$

即 a 和 b 的所有公约数与它们的最大公约数 r_n 的所有约数相合。(1.2.2)式可改写为

$$
\begin{aligned}
r_1 &= 1 \cdot a - q_1 b \\
r_2 &= 1 \cdot b - q_2 r_1 \\
r_3 &= 1 \cdot r_1 - q_3 r_2 \\
&\cdots \\
r_{n-1} &= 1 \cdot r_{n-3} - q_{n-1} r_{n-2} \\
r_n &= 1 \cdot r_{n-2} - q_n r_{n-1}
\end{aligned}
\tag{1.2.4}
$$

(1.2.4) 式说明 r_n 是 r_{n-2} 和 r_{n-1} 的整数系数的线性组合，将 r_{n-1} 的式子代入 r_n 式得到

$$
r_n = -q_n r_{n-3} + (1 + q_n q_{n-1}) r_{n-2}
$$

此式看出 r_n 又是 r_{n-3} 和 r_{n-2} 的整数系数的线性组合，继续迭代下去就可得到 a 和 b 的最大公约数 r_n 表为 a 和 b 的整数系数的线性组合，即

$$
r_n = ca + db \tag{1.2.5}
$$

其中 c 和 d 都是整数。从上面可推出 a 和 b 的任一公约数都是 r_n 的约数。

例如：利用转辗相除法求(525, 231) = ?

```
525 | 231        525 = 2·231 + 63    63<231
462 |   2        231 = 3·63 + 42     42<63
231 |  63        63 = 1·42 + 21      21<42
189 |   3        42 = 2·21
 63 |  42
 42 |   1        所以  (525,5231) = (231,63) = (63,42) = (42,21) = 21
 42 |  21
 42 |   2
```

最后的正余数 $r_3 = 21$。也可写成

$$
\begin{aligned}
63 &= 525 - 2 \cdot 231 \\
42 &= 231 - 3 \cdot 63 \\
21 &= 63 - 1 \cdot 42
\end{aligned}
$$

将前二式逐步代入第三式，有

$$
21 = 63 - (231 - 3 \cdot 63) = 4 \cdot 63 - 231
$$

$$= 4(525 - 2\cdot 231) - 231 = 4\cdot 525 - 9\cdot 231$$

因此

$$(525,\ 231) = 21$$

同样，多项式也有类似的性质。

设 a(x)和 b(x)都是域 F[x]上（关于“域”第二章中要专门讨论）的多项式中不等于零的多项式。可以用转辗相除法来求(a(x), b(x))，有下面一串式子：

$$\begin{aligned}
&a(x) = q_1(x)b(x) + r_1(x), && 0 \leqslant \partial^0 r_1(x) < \partial^0 b(x),\\
&b(x) = q_2(x)r_1(x) + r_2(x), && 0 \leqslant \partial^0 r_2(x) < \partial^0 r_1(x),\\
&r_1(x) = q_3(x)r_2(x) + r_3(x), && 0 \leqslant \partial^0 r_3(x) < \partial^0 r_2(x).\\
&\quad\cdots && \quad\cdots\\
&r_{n-3}(x) = q_{n-1}(x)r_{n-2}(x) + r_{n-1}(x), && 0 \leqslant \partial^0 r_{n-1}(x) < \partial^0 r_{n-2}(x).\\
&r_{n-2}(x) = q_n(x)r_{n-1}(x) + r_n(x), && 0 \leqslant \partial^0 r_n(x) < \partial^0 r_{n-1}(x)\\
&r_{n-1}(x) = q_{n+1}(x)r_n(x).
\end{aligned}$$

因此

$$(a(x),\ b(x)) = r_n(x) \tag{1.2.7}$$

1.2.2 最小公倍数

设 a 和 b 都是不等于零的整数，如果 c 既是 a 的又是 b 的倍数，就称 c 是 a 和 b 的公倍数，a 和 b 的最小正的公倍数，称为最小公倍数，记为 [a, b]，或 LCM(a, b)。

类似的有多项式 a(x) 和 b(x) 皆能整除之多项式，称为它们的公倍式，其中次数最低的称为最小公倍式（或最低公倍式），记为[a(x), b(x)]。同样也取最高次方系数为 1 的首一多项式为最小公倍式。

1.3 素数和素因数分解

自然数即正整数 1,2,3,…可分成三类：

(1) 正整数 1，只有一个正的约数，就是 1 本身。

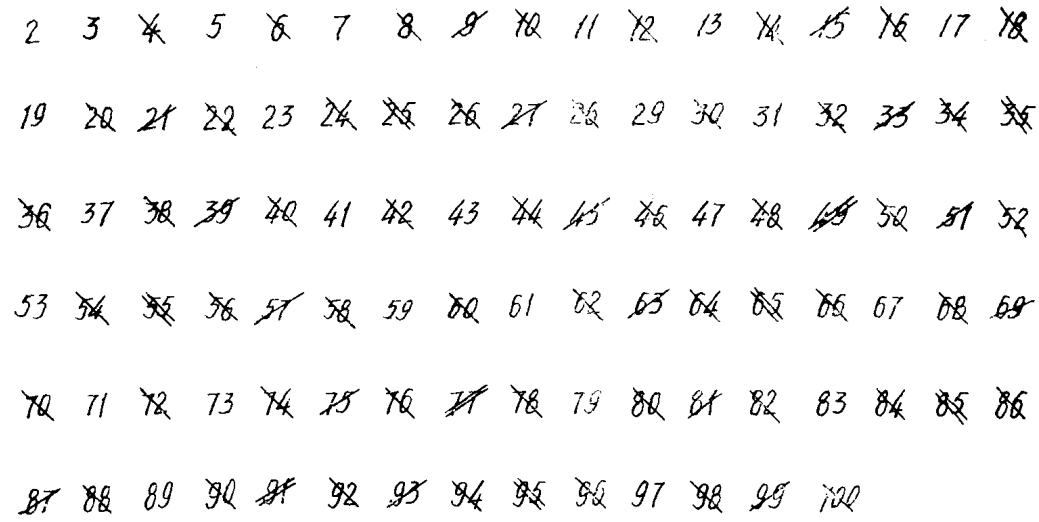
所以 1在自然数的序列中占有特殊的地位。

(2) 设 p 是大于 1 的正整数，若 p 只有两个正的约数，就是 1 和 p 本身，而不能被别的整数整除的，则称 p 为素数。如 2，3，5，7，11，13，17 等等。

(3) 设 n 不是素数而是大于 1 的整数，除 1 和它本身外，还能被别的整数整除的，即有真约数之自然数，它有两个以上的约数，称为合数。如4，6，8，9，10，12，14，等等。

能被 2 整除的数称为偶数，非偶数之整数称为奇数。显然大于 2 之偶数皆非素数。

素数的数目有无限多个，要选出不超过知某一正整数的所有素数可用 Eratosthenes 氏筛选法求得。若 $n \leqslant N$，而 n 非素数，则 n 必为一不大于 $\sqrt{N}$ 之素数所整除。例如要求≤100 的素数，先列出所有不超过 100 之正整数如下：



然后从2到100的整数序列中筛出：2是其中最小的一个数，它只能被1和它本身除尽，是一素数，把2挑出去，然后把2的倍数4，6，8，…即由2^2起的一切偶数划去。接着第一个没有划掉的数是3，它也是素数，把它挑出来，然后划去3以外的所有3的倍数，即由3^2起9，15，21，27，…。接着是5，划去5以外的5^2起的所有5的倍数25，35，55，65，…。如此继续下去，直到剩下的没有划去的尚未挑选出来的数里最小的一个数是11为止，因为≤100的合数一定有一个素因数≤$\sqrt{100}=10$，所以这时剩下的数就都是素数。从上可见，要划掉素数p的倍数，可以从p^2开始划起。要组成素数≤N的表，只要划掉不超过$\sqrt{N}$的素数的所有合数的倍数就行了。如此可得到≤100的素数表如下：

2，3，5，7，11，13，17，19，23，29，31，37，41，43，47，53，59，61，67，71，73，79，83，89，97。

一个整数，如果能被一个素数所整除，这个素数就叫做该整数的素因子。素因子分解有下列唯一分解定理，即

定理1.3.1 算术基本定理

每一个大于1的整数n，都可分解成一些素数的乘积，若不计这些素数因子的次序时，n只能由唯一的方法表示为下列形式：

$$n=p_1p_2\cdots p_k,\qquad p_1,\ p_2,\ \cdots p_k \text{ 均为素数} \tag{1.3.1}$$

例如：$315=3\cdot3\cdot5\cdot7$，$10725=3\cdot5\cdot5\cdot11\cdot13$。

相同的素因数可用幂次方表示，如$315=3^2\cdot5\cdot7$，$10725=3\cdot5^2\cdot11\cdot13$。一般有重复的因子可表为“标准”分解式如下：

$$n=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_K^{\alpha_k} \tag{1.3.2}$$

其中$p_1<p_2<\cdots<p_k$，$\alpha_i>0$，$i=1,\ 2,\ \cdots,\ k$。

顺便指出，1不为素数的原因，也可以从n的标准分解式中看出，若1为素数，1之任何次幂可均为因子，分解的唯一性将被破坏。

由整数素因子分解求最大公约数和最小公倍数很方便，例如求：(150,42)，[150,42]

因 $150=2^1\cdot3^1\cdot5^2\cdot7^0$，$42=2^1\cdot3^1\cdot5^0\cdot7^1$。

故 $(150,42)=2^1\cdot3^1\cdot5^0\cdot7^0=6$。

$[150,42]=2^1\cdot3^1\cdot5^2\cdot7^1=1050$。

与整数中素数相类似的，在多项式中，不可再分解的多项式称为不可约多项式或既约多项式。不可约多项式 $p(x)=p_mx^m+\cdots+p_1x+p_0$ 除常数 c 和 p(x) 本身外，别无其它因式，且 $\partial^0p(x)>0$。特别要注意的是，给定多项式 p(x)的可约性和不可约性依赖于所讨论的系数范围（以后会知道，所谓什么范围也就是与在什么域上有关），如一次多项式 ax+b，$a\neq0$($b=0$，ax；$b\neq0$，ax+b)在任何域上(即任何讨论的系数范围内）都是不可约多项式。而二次多项式 x^2+1 在实数域(范围)R 上是不可约的，但在复数域C下，因 $x^2+1=(x+i)\cdot(x-i)$，是可约的。x^2-2 在有理数域 Q 和整数模 3 域 I_3 上是不可约的；但在 I_7 上 $x^2-2=(x+3)(x+4)$，并且在实数域 R 上 $x^2-2=(x+\sqrt{2})(x-\sqrt{2})$，因此在这两种情况中是可约的。类似的，$x^2+x+1$ 在模 2 域 I_2 上是不可约的，而在模 3 域 I_3 上 $x^2+x+1=(x+2)^2$ 是可约的。关于域上的多项式在第二章中还要讨论。

与整数算术基本定理相类似的有下列定理。

定理 1.3.2 每一首一多项式必可分解为首一不可约多项式之积，若不计这些因式的次序，这种分解是唯一的，可表成

$$f(x)=p_1^{\alpha_1}(x)p_2^{\alpha_2}(x)\cdots p_r^{\alpha_r}(x) \tag{1.3.3}$$

1.4 Euler 函数

对于所有正整数 n，欧拉(Euler)函数 φ(n)表示在序列 0，1，2，…，n-1 中与 n 互素的个数。

例如

$\varphi(1)=1$　　$\varphi(4)=2$

$\varphi(2)=1$　　$\varphi(5)=4$

$\varphi(3)=2$　　$\varphi(6)=2$

φ(n) 的主要性质如下：

(1) 设 n(n>1) 的标准分解式为

$$n=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$$

则 $$\varphi(n)=\prod_{i=1}^{k}(p_i^{\alpha_i}-p_i^{\alpha_i-1})=(p_1^{\alpha_1}-p_1^{\alpha_1-1})(p_2^{\alpha_2}-p_2^{\alpha_2-1})$$

$$\cdots(p_k^{\alpha_k}-p_k^{\alpha_k-1})$$

$$=n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_1}\right)\cdots\left(1-\frac{1}{p_k}\right) \tag{1.4.1}$$

例如，$60=2^2\cdot3\cdot5$

$$\varphi(60)=(2^2-2^1)(3^1-3^0)(5^1-5^0)=2\cdot2\cdot4=16.$$

特别 $$\varphi(p^\alpha)=p^\alpha-p^{\alpha-1} \tag{1.4.2}$$

$$\varphi(p)=p-1 \tag{1.4.3}$$

其中 p 是素数。

如上面列出的 $\varphi(2)=2-1=1$，$\varphi(3)=3-1=2$，$\varphi(5)=5-1=4$。

(2) 函数$\varphi(n)$是积性函数

设 n_1，n_2 之素因子分解式为

$$n_1=\prod_{i=1}^{k}p_i^{\alpha_i},\quad n_2=\prod_{i=1}^{k'}q_i^{\beta_i}$$

且 $(n_1,n_2)=1$（互素），$n=n_1n_2$。

因此

$$n=\prod_{i=1}^{k}p_i^{\alpha_i}\prod_{i=1}^{k'}q_i^{\beta_i}$$

$$\varphi(n)=\varphi(n_1)\varphi(n_2)=n_1n_2\prod_{i=1}^{k}\left(1-\frac{1}{p_i}\right)\prod_{i=1}^{k'}\left(1-\frac{1}{q_i}\right) \tag{1.4.4}$$

例如 $\varphi(405)=\varphi(81)\varphi(5)=54\cdot 4=216$。

(3) $\varphi(n)$满足

$$\sum_{d\mid n}\varphi(d)=n$$

$$\sum_{d\mid n}\varphi(d)=[1+\varphi(p_1)+\varphi(p_1^{2})+\cdots+\varphi(p_1^{\alpha_1})]+\cdots+[1+\varphi(p_k)$$

$$+\varphi(p_k^{2})+\cdots+\varphi(p_k^{\alpha_k})]=\prod_{i=1}^{k}p_i^{\alpha_i}=n \tag{1.4.5}$$

例如 $n=12$，12 的所有约数为 1，2，3，4，6，12，求得

$$\varphi(1)+\varphi(2)+\varphi(3)+\varphi(4)+\varphi(6)+\varphi(12)=1+1+2+2+2+4=12.$$

1.5 同余式和剩余类

同余的概念在日常生活中时常会遇到，例如“每逢星期二上课一次”，即是以七为模计之。1.6. 节中要讨论的孙子定理，就是同余式研究之例。

定义 1.5.1 如果两个整数 a和b，被m 除后有相同的余数 r，即

$$a=g_1m+r$$
$$b=g_2m+r$$

就称 a、b 对模 m 同余，可写成

$$a\equiv b\pmod{m}$$

$a\equiv b\pmod{m}$等价于 $m\mid(a-b)$，或 $a=b+mt$，$a-b=mt$。反之，a 与 b 对模 m 不同余，可表为

$$a\not\equiv b\pmod{m}$$

同余式与等式有类似的基本性质如下：

(1) $a \equiv a \pmod{m}$ (反身性)

(2) $a \equiv b \Rightarrow b \equiv a \pmod{m}$ (对称性)

(3) $a \equiv b \pmod{m}$, $b \equiv c \pmod{m} \Rightarrow a \equiv c \pmod{m}$ (传递性)

定理 1.5.1 如果

$$a_1 \equiv b_1 \pmod{m}, \quad a_2 \equiv b_2 \pmod{m}$$

下列同余式运算成立：

$$a_1 + a_2 \equiv b_1 + b_2 \pmod{m}$$

$$a_1 - a_2 \equiv b_1 - b_2 \pmod{m}$$

$$a_1 \times a_2 \equiv b_1 \times b_2 \pmod{m}$$

还可以将同余式两边同乘上一个整数：

$$ak = bk \pmod{m}$$

定理 1.5.2 同余式两边可以被它们的公约数除，如果这公约数与模 m 互素的话，从

$$a \equiv b \pmod{m}, \quad a = a_1 d, \quad b = b_1 d$$

推出

$$a - b = (a_1 - b_1)d$$

能被 m 除尽，因此处 $(a, m) = 1$，故 $a_1 - b_1$ 能被 m 除尽，

即 $$a_1 \equiv b_1 \pmod{m}$$

从同余式 $a \equiv b \pmod{m}$ 看出，对于模 m 同余的那些数，可以组成由模 m 决定的数集合，两整数 a、b 对模 m 同余的充分必要条件是这两个整数处于同一剩余类中，任一整数被一正整数 m 除，所得余数必小于 m，如为 0,1,2,…, m-1 共 m 个可能的不同余数。如果将所有整数用 m 除，那末就可把有相同余数的数划在一个类里，共有 m 个这样的不同的剩余类。这种运算所得的类称为模 m 的剩余类。取模的运算，是一种将数进行按模化简而取其非负最小剩余。这种运算在计算机和编码理论中都是非常重要的。

例 1．按模 2 运算，可将整数划分成奇数和偶数两大剩余类{0}和{1}。

{0}	{1}
0	1
2	3
4	5
6	7
8	9
⋮	⋮

例 2．按模 5 运算，可将整数划分成五类{0}，{1},{2},{3},{4}。

{0}	{1}	{2}	{3}	{4}
5	6	7	8	9
10	11	12	13	14
15	16	17	18	19
20	21	22	23	24
……				

例 3．与模 15 互素的剩余类为{1},{2},{4},{7},{8},{11},{13},{14}共 8 类。

定义 1.5.2 同一模的两个剩余类{a}、{b}进行加法和乘法运算定义如下：

$$\{a\}+\{b\}=\{a+b\}$$
$$\{a\}\cdot\{b\}=\{a\cdot b\}$$

例如模 2 剩余类中对加法和乘法如下表：

加法 +	{0}	{1}
{0}	{0}	{1}
{1}	{1}	{0}

乘法 ·	{0}	{1}
{0}	{0}	{0}
{1}	{0}	{1}

由此可见，剩余类对加法、乘法运算都是封闭的，它具有很好的代数性质。

又如模 5 剩余类中

$$\{4\}+\{12\}=\{16\}=\{1\} \pmod 5 \quad \text{为非负最小剩余}$$
$$\{4\}\cdot\{12\}=\{48\}=\{3\} \pmod 5 \quad \text{为非负最小剩余}$$

类似于整数按模 m 运算，对于任意多项式 f(x)，若用某一次数为 m 的多项式 g(x)去除，可得到商式 q(x)及次数低于 m 的余式 r(x)，即

$$f(x)=q(x)g(x)+r(x)$$

或写成

$$f(x)\equiv r(x) \pmod{g(x)} \tag{1.5.2}$$

称按模 g(x)运算。

以后要介绍的循环码，是以 x^n-1 为模运算，若用 x^n-1 除任意多项式 f(x)，可得到一余式，共有 2^n 个不同的余式，构成以次数小于 n 的多项式为余式的 2^n 个剩余类。例如，以 x^3+1 为模共有 $2^3=8$ 个剩余类，即 $\{x^2+x+1\}$，$\{x^2+x\}$，$\{x^2+1\}$，$\{x^2\}$，$\{x+1\}$，$\{x\}$，$\{1\}$，$\{0\}$。

1.6 孙子定理

孙子算经是我国古代(3～5 世记)数学的重要成就之一，其中有“物不知其数”一问题，称：“今有物不知其数，三三数之剩二，五五数之剩三，七七数之剩二，问物几何？”解这个问题的算法答：“术曰：三三数之剩二，置一百四十；五五数之剩三，置六十三；七七数之剩二，置三十；并之得二百三十三；以二百一十减之即得。凡三三数之剩一，则置七十；五五数之剩一，则置二十一；七七数之剩一，则置十五；一百六以上，以一百五减之即得。”

此例是求适合下列三个同余式的公解

$$x\equiv 2 \pmod 3$$
$$x\equiv 3 \pmod 5$$
$$x\equiv 2 \pmod 7$$

其解是

$$x\equiv 2\cdot c_1\cdot 5\cdot 7+3\cdot c_2\cdot 3\cdot 7+2\cdot c_3\cdot 3\cdot 5 \pmod{3\cdot 5\cdot 7}$$

而常数 c_1，c_2，c_3 满足下列同余式

$$c_1\cdot 5\cdot 7+c_2\cdot 3\cdot 7+c_3\cdot 3\cdot 5\equiv 1 \pmod{3\cdot 5\cdot 7}$$

或满足下列一组同余式

$c_1 \cdot 5 \cdot 7 \equiv 1 \pmod 3$　$c_1 \cdot 5 \cdot 7 \equiv 0 \pmod 5$　$c_1 \cdot 5 \cdot 7 \equiv 0 \pmod 7$

$c_2 \cdot 3 \cdot 7 \equiv 0 \pmod 3$　$c_2 \cdot 3 \cdot 7 \equiv 1 \pmod 5$　$c_2 \cdot 3 \cdot 7 \equiv 0 \pmod 7$

$c_3 \cdot 3 \cdot 5 \equiv 0 \pmod 3$　$c_3 \cdot 3 \cdot 5 \equiv 0 \pmod 5$　$c_3 \cdot 3 \cdot 5 \equiv 1 \pmod 7$

故

$$c_1 = 2$$
$$c_2 = 1$$
$$c_3 = 1$$

即

$$70 + 21 + 15 = 106 \equiv 1 \pmod{105}$$

而解为

$$x = 140 + 63 + 30 = 233 \equiv 23 \pmod{105}$$

根据此例，孙子定理一般叙述如下：

给定 l 个两两互素的大于 1 的整数 $m_1, m_2, \cdots, m_l$ 和整数 $a_1, a_2 \cdots, a_l$，若有 l 个同余式组。

$$\begin{aligned} &x \equiv a_1 \pmod{m_1} \\ &x \equiv a_2 \pmod{m_2} \\ &\cdots \\ &x \equiv a_l \pmod{m_l} \end{aligned}$$

或　$x \equiv a_i \pmod{m_i}$，$i = 1, 2, \cdots, l$

则其有唯一的一个满足下列同余式的解

$$x \equiv a_1 \cdot c_1 \cdot m_2 \cdot m_3 \cdots m_l + a_2 \cdot c_2 \cdot m_1 \cdot m_3 \cdots m_l + \cdots + a_l \cdot c_l \cdot m_1 \cdot m_2 \cdots m_{l-1} \pmod n \tag{1.6.1}$$

或

$$x = \sum_{i=1}^{l} a_i \cdot c_i \cdot \prod_{\substack{j=1 \\ j \neq i}}^{l} m_j \pmod n$$

其中　$n = m_1 \cdot m_2 \cdots m_l = \prod_{j=1}^{l} m_j$

且其中 l 个常数 $c_i (i = 1, 2, \cdots, l)$ 满足下列同余式

$$c_1 m_2 m_3 \cdots m_l + c_2 m_1 m_3 \cdots m_l + \cdots + c_l m_1 m_2 \cdots m_{l-1} \equiv 1 \pmod n$$

或

$$\sum_{i=1}^{l} c_i \cdot \prod_{\substack{j=1 \\ j \neq i}}^{l} m_j \equiv 1 \pmod n.$$

显然有

$$\begin{cases} c_i \cdot m_1 m_2 \cdots m_{i-1} m_{i+1} \cdots m_l \equiv 1 \pmod{m_i} \\ c_i \cdot m_1 m_2 \cdots m_{i-1} m_{i+1} \cdots m_l \equiv 0 \pmod{m_j} \end{cases}$$

或

$$c_i\prod_{\substack{j=1\\ j\neq i}}^{l} m_j \equiv 1 \pmod{m_i},\quad i=1,2,\cdots,l$$

$$c_i\prod_{\substack{j=1\\ j\neq i}}^{l} m_j \equiv 0 \pmod{m_j},\quad j\neq i。$$

证明从略。

应当指出，孙子定理要求各模数 $m_i(i=1,2,\cdots,l,)$两两互素。若非两两互素时，可作如下简化修正。这时可构造出另一组两两互素的整数 $m_i'(i=1,2,\cdots,l)$，使得

$$n=\mathrm{LCM}(m_1,\ m_2,\ \cdots,\ m_l)=m_1'\cdot m_2'\cdots m_l'=\prod_{j=1}^{l} m_j'.$$

并使

$$a_i\equiv a'_i \pmod{m'_i},\quad i=1,\ 2,\cdots,l.$$

则就在满足 l 个同余式组

$$x\equiv a'_i \pmod{m'_i},\quad i=1,2,\cdots,l.$$

的解 x 也就是满足原来 l 个同余式组

$$x\equiv a_i \pmod{mi},\quad i=1,2,\cdots l.$$

之解。

如孙子算经上原来的例子，若最后不用七七数之剩二，而是六六数之剩五，则

$$x\equiv 2 \pmod 3$$
$$x\equiv 3 \pmod 5$$
$$x\equiv 5 \pmod 6$$

由于 6 与 3 不互素，改取 2 为模，最后一式改写为

$$x\equiv 1 \pmod 2$$

则

$$c_1\cdot 5\cdot 2\equiv 1 \pmod 3$$
$$c_2\cdot 3\cdot 2\equiv 1 \pmod 5$$
$$c_3\cdot 3\cdot 5\equiv 1 \pmod 2$$

故

$$c_1=1,\ c_2=1,\ c_3=1$$

得解为

$$x=2\cdot 1\cdot 5\cdot 2+3\cdot 1\cdot 3\cdot 2+1\cdot 1\cdot 3\cdot 5=53\equiv 23(\mathrm{mod}\ 30)$$

若最后用十十数之剩三，

$$x\equiv 3 \pmod{10}$$

则 10 与 5 不互素，亦可改取 2 为模

$$x\equiv 1 \pmod 2$$

最后得到同样结果。

若最后取十二、十二数之剩十一，

$$x \equiv 11 \pmod{12}$$

则改取 4 为模

$$x \equiv 3 \pmod{4}$$

则
$$c_1 \cdot 5 \cdot 4 \equiv 1 \pmod{3}$$
$$c_2 \cdot 3 \cdot 4 \equiv 1 \pmod{5}$$
$$c_3 \cdot 3 \cdot 5 \equiv 1 \pmod{4}$$

故 $c_1 = 2,\ c_2 = 3,\ c_3 = 3.$

得解为

$$x = 2 \cdot 2 \cdot 5 \cdot 4 + 3 \cdot 3 \cdot 3 \cdot 4 + 3 \cdot \cdot 3 \cdot 3 \cdot 5 = 323 \equiv 23 \pmod{60}$$

1.7 Euler 定理和 Fermat 定理

Euler (欧拉) 定理：设 $m>1$，且 $(a,m)=1$，有

$$a^{\varphi(m)} \equiv 1 \pmod{m} \tag{1·7.1}$$

例如：$2^{\varphi(5)} = 2^4 \equiv 1 \pmod{5}$，$3^{\varphi(5)} = 3^4 \equiv 1 \pmod{5}$，$4^{\varphi(5)} = 4^4 \equiv 1 \pmod{5}$

此定理在大指数计算时可作化简，例如

$$2^{151} = (2^4)^{37} \cdot 2^3 \equiv 2^3 \equiv 3 \pmod{5}$$

当 p 为素数，且 a 不被 p 除尽，即 $(a,p)=1$，因与 p 互素的剩余类中，比 p 小的有 $\{1\}$，$\{2\}$，…，$\{p-1\}$，乃 $\varphi(p) = p-1$，因此

$$a^{\varphi(p)} = a^{p-1} \equiv 1 \pmod{p}. \tag{1.7.2}$$

或

$$a^p \equiv a \pmod{p} \tag{1.7.3}$$

这就是Fermat (费马) 定理。

1.8 指数和原根

定义　若 $(a,m)=1$，满足 $a^r \equiv 1 \pmod{m}$ 的最小自然数 r，称为 a 对于 m 的指数，记为 $r = \text{ind } a \pmod{m}$。

指数与通常的对数有相仿的性质：

(1) $\text{ind } ab \equiv \text{ind } a + \text{ind } b \pmod{p-1}$

(2) $\text{ind } a^l = l \cdot \text{ind } a \pmod{p-1}$

注意，仅当 $p \nmid a$ 时，ind a 才有意义，这与 log 0 无相同意义。

定义，若 $(a,m)=1$，且 a 对于 m 的指数 $r = \varphi(m)$，则称 a 为 m 的原根。

或者，指数为 p − 1 的数，称为 p 之原根。

例如，$(2,3)=1$，$2^2 \equiv 1 \pmod{3}$，$r = \varphi(3) = 2$.

$(3,4)=1$，$3^2 \equiv 1 \pmod{4}$，$r = \varphi(4) = 2$.

1.9 二次剩余和 Legendre 符号

定义　若 $(a,p)=1$，p 为单素数，