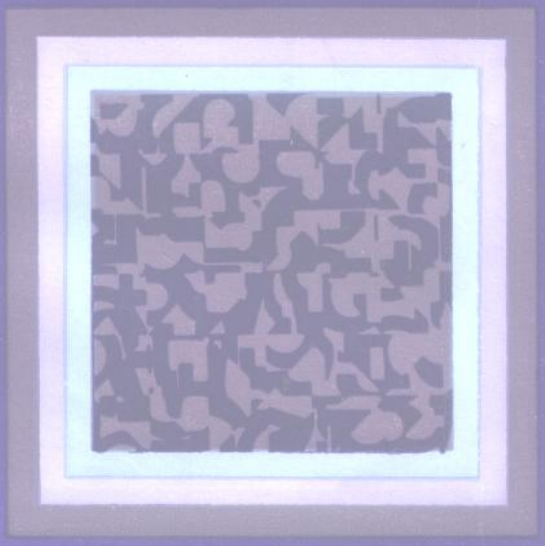
# 密码学与数论基础

于秀源　薛昭雄



山东科学技术出版社

# 密码学与数论基础

于秀源　薛昭雄


山东科学技术出版社

(鲁)新登字 05 号

# 密码学与数论基础

于秀源　薛昭雄

*

山东科学技术出版社出版
（济南市玉函路　邮政编码 250002）
山东省新华书店发行
山东新华印刷厂潍坊厂印刷

*

850×1168 毫米 32 开本　7 印张　150 千字
1993 年 3 月第 1 版　1993 年 3 月第 1 次印刷
印数：1—1000

ISBN　7—5331—1158—3/O・49

定价 4.90 元

# 前　言

密码的研究和使用，有一个很长的历史，可以追溯到古老的战争年代．计算机技术的迅速发展和广泛应用，不但为密码学研究提供了强有力的技术手段，也带来了对信息保密研究的更广泛的需求．这些需求除了来自国防和政府保密部门，还大量地来自经济部门和民间团体，它们形成了促进密码学发展的巨大推动力．

本世纪以来，密码学研究取得了许多令人瞩目的重大进展．特别是 70 年代以来，随着公开钥密码系统的出现，密码学研究发生了质的飞跃，出现了一个崭新的时期．

数论与密码学的密切关系，已经为人们所认识，并且日益受到重视．密码学为数论研究方法和成果提供了广阔的应用场地，同时，也为数论研究的开展增添了新鲜活力．现在，一个重要的课题是，一方面，让从事理论研究的数论工作者了解密码学，特别是了解数论在密码学中的应用状况与前景；另一方面，使信息保密技术研究工作者具备一定的数论知识，提高用理论知识指导应用实践的能力．这两个方面的有机结合（但不是简单拼合），对于数论与密码学的进一步发展，无疑都是有非常重要的意义．

基于上述认识，我们编写了这本关于密码学与数论基础的书，希望对从事数论应用及信息保密技术研究的工作者提供一些有积极意义的帮助．当然，限于我们的水平，书中内容难免有

不妥之处，希望读者不吝赐教.

本书的写作得到了国家自然科学基金与浙江省自然科学基金的资助.李大兴同志对书稿提出了宝贵意见.在此一并致谢.

# 目　录

# 第一章　整除与同余

数论在密码学，尤其是现代密码学的研究中有着重要的作用.本章主要介绍整除理论，同余理论，以及对基本运算的估计，和在密码学研究中所涉及的数论函数.

## 第一节　带余数除法

以下，除特别声明外，字母 $a,b,c,\cdots$ 等均表示整数，以 $\mathbf{Z}$ 表示全体整数的集合，$N$ 表示全体正整数的集合.

**定义 1**　设 $a,b\in\mathbf{Z},b\neq 0$，若有 $c\in\mathbf{Z}$ 使得 $a=bc$，则称 $b$ 整除 $a$，记作 $b|a$，称 $b$ 是 $a$ 的除数(因数，或约数)，$c$ 是 $b$ 除 $a$ 的商，$a$ 是 $b$ 的倍数；若这样的 $c$ 不存在，则称 $a$ 不被 $b$ 整除，记为 $b\nmid a$.

下面的性质是显然的：

(1) 若 $b|a$，则 $b$ 除 $a$ 的商是唯一的；

(2) $b(\neq 0)$的所有倍数是 $0,\pm b,\pm 2b,\cdots$；

(3) $b|a,c|b\Rightarrow c|a$；

(4) $b|a,a\neq 0\Rightarrow|b|\leqslant|a|$，其中的等号当且仅当 $b=\pm a$ 时成立；

若 $b|a,1<|b|<|a|$，则称 $b$ 是 $a$ 的真除数；

$a$ 与 $-a$ 有相同的除数，$\pm 1$ 与 $\pm a$ 显然是它们的除数；

(5) $b|a_1,b|a_2,m_1,m_2\in\mathbf{Z}\Rightarrow b|a_1m_1+a_2m_2$.

**定义 2** 一个大于 1 的正整数，若除了数 1 和它自身外，它没有另外的除数，则称为素数. 不是素数的正整数称为合数.

**定理 1** 任一整数 $a(a\neq 0, a\neq \pm 1)$的不等于 1 的最小正除数 $d$ 是素数；若 $d\neq a$，则 $d\leqslant\sqrt{|a|}$.

**证明** $a$ 的正除数只有有限个，故必有最小的，设为 $d$. 若 $d$ 不是素数，则有真除数 $d_1, d_1>1, d_1 | d, d>d_1$. 由性质 3，$d_1 | a$，这与 $d$ 的最小性矛盾，因此 $d$ 必是素数. 设 $a=dq$，则 $|a|=|dq|\geqslant d^2$，即 $d\leqslant\sqrt{|a|}$. □

**定理 2** （带余数除法） 设 $a, b\in \boldsymbol{Z}, b>0$，则存在唯一的一对整数 $q, r$，使得

$$a=qb+r,\quad 0\leqslant r<b.$$

**证明** 对于 $q=0, \pm 1, \pm 2, \cdots, a$ 必落在唯一的一个区间 $Iq=[bq, b(q+1)]$中，因而 $r=a-bq$ 是唯一的，并且$0\leqslant r<b$. □

**定理 3** 设 $b>1$ 是整数，则任何正整数 $n$ 都可以唯一地写成

$$n=a_k b^k+a_{k-1}b^{k-1}+\cdots+a_1 b+a_0 \tag{1}$$

的形式，其中 $a_i\in \boldsymbol{N}, 0\leqslant a_i\leqslant b-1, i=0, 1, \cdots, k$，并且 $a_k\neq 0$.

**证明** 由定理 2，依次有

$$\left.\begin{aligned} n&=q_1 b+a_0, & 0\leqslant a_0\leqslant b-1,\\ q_1&=q_2 b+a_1, & 0\leqslant a_1\leqslant b-1,\\ q_2&=q_3 b_1+a_2, & 0\leqslant a_2\leqslant b-1,\\ &\cdots\cdots & \\ q_{k-1}&=q_k b+a_{k-1}, & 0\leqslant a_{k-1}\leqslant b-1,\\ q_k&=0\cdot b+a_k, & 0\leqslant a_k\leqslant b-1. \end{aligned}\right\} \tag{2}$$

综合这些等式，得到

$$n=q_1 b+a_0=q_2 b^2+a_1 b+a_0=q_3 b^3+a_2 b^2+a_1 b+a_0$$

$$=\cdots=q_{k-1}b^{k-1}+a_{k-2}b^{k-2}+\cdots+a_1b+a_0$$
$$=q_kb^k+a_{k-1}b^{k-1}+\cdots+a_1b+a_0$$
$$=a_kb^k+a_{k-1}b^{k-1}+\cdots+a_1b+a_0,$$

这就是表示式(1).

下面证明表示式(1)是唯一的.若有两个表示式满足(1)式,即有

$$n=a_kb^k+a_{k-1}b^{k-1}+\cdots+a_1b+a_0$$
$$=c_mb^m+c_{m-1}b^{m-1}+\cdots+c_1b+c_0,$$

其中 $0\leqslant a_i,c_j\leqslant b-1,0\leqslant i\leqslant k,0\leqslant j\leqslant m$,则

$$(a_kb^k+\cdots+a_1b)-(c_mb^m+\cdots+c_1b)=c_0-a_0, \tag{3}$$

因此,$b|(c_0-a_0)$,但$|c_0-a_0|<b$,所以 $c_0=a_0$.代入(3)式,并用 $b$ 除等式两端,又可得到 $c_1=a_1$.依次推导,得到

$$k=m,\qquad a_i=c_i\qquad(0\leqslant i\leqslant k).$$ □

**定义 3** 设 $b$ 是正整数,$n$ 是正整数,并且

$$n=a_kb^k+a_{k-1}b^{k-1}+\cdots+a_1b+a_0,$$

其中 $a_k\neq0,0\leqslant a_i\leqslant b-1(0\leqslant i\leqslant k)$,则称$(a_k,a_{k-1},\cdots,a_1,a_0)_b$ 是 $n$ 的 $b$ 进制表示,或数 $n$ 以 $b$ 为基的表示,并且,称 $n$ 是 $k+1$ 位 $b$ 进制数,称 $k+1$ 是 $n$ 的 $b$ 进制位数,$a_i(0\leqslant i\leqslant k)$是 $n$ 的 $b$ 进制表示的第 $i+1$ 个位数码(或第 $i+1$ 位数).

**注 1** 数 $n$ 的 $b$ 进制表示中的位数码的个数是$\lceil\log_bn\rceil+1=\left\lceil\frac{\log n}{\log b}\right\rceil+1$,其中 log 表示以数 $e$ 为底的对数.

**注 2** 由定理 3 的证明见到,数 $n$ 的 $b$ 进制表示的第 $i$ 位数码,就是利用带余数除法所得到的(2)式中的第 $i$ 个等式中的余数 $a_{i-1}$.

**注 3** 对于任意的正实数 $\alpha$,若

$$\alpha=a_kb^k+a_{k-1}b^{k-1}+\cdots+a_1b+a_0+\frac{a-1}{b}+\frac{a-2}{b^2}+\cdots,$$

其中 $0\leqslant a_i\leqslant b-1(i=k,k-1,\cdots,1,0,-1,-2,\cdots)$，则称 $(a_k,a_{k-1},\cdots,a_1,a_0,a_{-1},a_{-2},\cdots)_b$ 是 $\alpha$ 的 $b$ 进制表示，容易证明，若以〔$x$〕表示实数 $x$ 的整数部分，则

$$〔\alpha〕=(a_ka_{k-1}\cdots a_1a_0)_b,$$

$$a_{-i}=〔b^i(\alpha-\sum_{j=-i+1}^{k}a_jb^j)〕,\quad i=1,2,\cdots,$$

由后一等式可以依次求出 $a_{-1},a_{-2},\cdots$.

**例 1** 将 83 写成二进制表示.

**解** 由

$$83=2\cdot 41+1,\qquad 41=2\cdot 20+1,$$
$$20=2\cdot 10+0,\qquad 10=2\cdot 5+0,$$
$$5=2\cdot 2+1,\qquad 2=2\cdot 1+0,$$
$$1=2\cdot 0+1$$

得到 $83=(1010011)_2$.

**例 2** 将 92 与 17 写成三进制表示.

**解** 由

$$92=3\cdot 30+2,\qquad 17=3\cdot 5+2,$$
$$30=3\cdot 10+0,\qquad 5=3\cdot 1+2,$$
$$10=3\cdot 3+1,\qquad 1=3\cdot 0+1,$$
$$3=3\cdot 1+0,$$
$$1=3\cdot 0+1,$$

得到

$$92=(10102)_3,17=(122)_3.$$

**例 3** 写出 $\pi=3.1415926\cdots$的二进制表示.

**解** $〔\pi〕=3=(11)_2$

$$a_{-1}=[2(\pi-3)]=0,$$

$$a_{-2}=[2^2(\pi-3)]=0,$$

$$a_{-3}=[2^3(\pi-3)]=1,$$

……

继续这样的计算，得到

$$\pi=(11.0010010000111\cdots)_2.$$

下面，考察 $b$ 进制数的四则算术运算.

设

$$A=(\alpha_n\alpha_{n-1}\cdots\alpha_1\alpha_0)_b, B=(\beta_m\beta_{m-1}\cdots\beta_1\beta_0)_b.$$

**Ⅰ 加法**

不妨设 $n\geqslant m$，

$$A+B=\sum_{i=0}^{n}\alpha_i b^i+\sum_{i=0}^{m}\beta_i b^i=(C_kC_{k-1}\cdots C_1C_0)_b.$$

记 $\alpha_0+\beta_0=\gamma_0 b+C_0$，$0\leqslant C_0\leqslant b-1$，则由

$$0\leqslant\alpha_0+\beta_0\leqslant 2b-2$$

可知 $\gamma_0=1$ 或 0，因此

$$C_0=\begin{cases}\alpha_0+\beta_0\\ \alpha_0+\beta_0-b,\end{cases}\quad \gamma_0=\begin{cases}0,\\ 1,\end{cases}\quad \text{当}\quad \begin{array}{l}0\leqslant\alpha_0+\beta_0\leqslant b-1,\\ b\leqslant\alpha_0+\beta_0\leqslant 2b-2.\end{array}$$

一般地，对于 $i\geqslant 1$，记 $\alpha_i+\beta_i+\gamma_{i-1}=\gamma_i b+C_i$（当 $i>m$ 时，令 $\beta_i=0$），则

$$0\leqslant\alpha_i+\beta_i+\gamma_{i-1}\leqslant 2b-1,$$

从而

$$C_i=\begin{cases}\alpha_i+\beta_i+\gamma_{i-1},\\ \alpha_i+\beta_i+\gamma_{i-1}-b,\end{cases}\quad \gamma_i=\begin{cases}0,\\ 1,\end{cases}\quad \text{当}\quad \begin{array}{l}0\leqslant\alpha_i+\beta_i+\gamma_{i-1}\leqslant b-1,\\ b\leqslant\alpha_i+\beta_i+\gamma_{i-1}\leqslant 2b-1,\end{array}$$

此处的 $\gamma_i$ 即是在进行第 $i+1$ 位数码加法后向下一位数码的“进位”.

两个 $n+1$ 位 $b$ 进制数的和是 $n+1$ 位或 $n+2$ 位 $b$ 进制数.

**例 4** 求$(1010011)_2$与$(1000111)_2$之和.

**解**

$$\begin{array}{r} \quad 1\ 1\ 1 \\ 1\ 0\ 1\ 0\ 0\ 1\ 1 \\ +1\ 0\ 0\ 0\ 1\ 1\ 1 \\ \hline 1\ 0\ 0\ 1\ 1\ 0\ 1\ 0, \end{array}$$

即

$$(1010011)_2+(1000111)_2=(10011010)_b.$$

**Ⅱ 减法**

设$A>B$,

$$A-B=\sum_{i=0}^{n}\alpha_i b^i-\sum_{i=0}^{m}\beta_i b^i=(d_k d_{k-1}\cdots d_1 d_0)_b.$$

记$\alpha_0-\beta_0=-\delta_0 b+d_0$,$0\leqslant d_0\leqslant b-1$,则由

$$-b+1\leqslant\alpha_0-\beta_0\leqslant b-1$$

可知$\delta_0=1$或$0$,即

$$d_0=\begin{cases}\alpha_0-\beta_0, \\ b+\alpha_0-\beta_0,\end{cases}\quad \delta_0=\begin{cases}0, & \text{当}\ \alpha_0-\beta_0\geqslant 0, \\ 1, & \text{当}\ \alpha_0-\beta_0<0.\end{cases}$$

一般地,记$\alpha_i-\beta_i-\delta_{i-1}=-\delta_i b+d_i$,则

$$d_i=\begin{cases}\alpha_i-\beta_i-\delta_{i-1}, \\ b+\alpha_i-\beta_i-\delta_{i-1},\end{cases}\quad \delta_i=\begin{cases}0, & \text{当}\ \alpha_i-\beta_i-\delta_{i-1}\geqslant 0, \\ 1, & \text{当}\ \alpha_i-\beta_i-\delta_{i-1}<0,\end{cases}$$

此处$\delta_i$即是在进行第$i+1$位数码减法时向上一位数码的“借位”.

**例 5** 求$(10110)_2$与$(1110)_2$之差.

**解**

$$\begin{array}{r} -1 \\ 10110 \\ -\ \ 1110 \\ \hline 1000, \end{array}$$

即

$$(10110)_2-(1110)_2=(1000)_2.$$

**Ⅲ 乘法**

由

$$AB=\left(\sum_{i=0}^{n}\alpha_i b^i\right)\left(\sum_{j=0}^{m}\beta_j b^j\right)=\sum_{j=0}^{m}b^j\left(\sum_{i=0}^{n}\alpha_i\beta_j b^i\right)$$

可见,乘法可分以下两步完成:

(i) 对于 $\beta=\beta_j(0\leqslant j\leqslant m)$,计算 $\beta\sum_{i=0}^{n}\alpha_i b^i$.

记 $\beta\alpha_0=q_0b+e_0,0\leqslant e_0\leqslant b-1$,则由 $0\leqslant\beta,\alpha_0\leqslant b-1$ 可知 $0\leqslant q_0\leqslant b-1$.

一般地,记 $\beta\alpha_i+q_{i-1}=q_ib+e_i,0\leqslant e_i\leqslant b-1$,则同样可知 $0\leqslant q_i\leqslant b-1(1\leqslant i\leqslant n)$.

(ii) 将在(i)中得到的 $\beta_j\sum_{i=0}^{n}\alpha_i b^i(0\leqslant j\leqslant m)$ 乘以 $b^j$,并对 $j=0,1,\cdots,m$求和,即可得到乘积 $AB$.

**Ⅳ 除法**

设 $A$ 被 $B$ 除所得的商是 $q=(q_kq_{k-1}\cdots q_1q_0)_b$,余数是 $R$,即

$$A=B\cdot\sum_{i=0}^{k}q_ib^i+R,\quad 0\leqslant R<B,$$

则

$$A-Bq_kb^k=B\sum_{i=0}^{k-1}q_ib^i+R. \tag{3}$$

由于 $q_i \leqslant b-1 (0 \leqslant i \leqslant k-1)$，所以上式右端不大于

$$B(b-1)\frac{b^k-1}{b-1}+B-1=Bb^k-1,$$

因此，

$$0 \leqslant A-Bq_kb^k \leqslant Bb^k-1,$$

$$q_k=\left[\frac{A}{Bb^k}\right], \tag{4}$$

即，若依次做减法 $A-Bb^k, A-2Bb^k, A-3Bb^k, \cdots$，则 $q_k$ 是使 $A-lBb^k \geqslant 0$ 的最大的 $l$ 值.

在确定出 $q_k$ 之后，记 $A_1=A-Bq_kb^k$，并比较 $A_1$ 与 $B$ 的大小(做一次减法). 若 $A_1<B$，则 $R=A_1$；若 $A_1 \geqslant B$，则可用上述方法求出 $q_{k-1}$.

重复以上过程，可逐次求出 $q_i (0 \leqslant i \leqslant k)$ 以及 $R$.

**注** 乘法与除法都亦可像十进制数那样地用竖式进行，如下面的两个例子所示.

**例 6** 求 $(221)_3$ 与 $(12)_3$ 之积.

**解**

$$\begin{array}{r} 1 \\ 2\,2\,1 \\ \times\quad 1\,2 \\ \hline 1\,2\,1\,2 \\ 2\,2\,1 \\ \hline 1\,1\,1\,2\,2 \end{array}$$

即 $(221)_3 \cdot (12)_3=(11122)_3$.

**例 7** 求 $(40122)_7$ 被 $(126)_7$ 除所得的商和余数.

**解**

$$
\begin{array}{r}
260 \\
126\overline{)40122} \\
\underline{255} \\
1132 \\
\underline{1131} \\
12
\end{array}
$$

即商为$(260)_7$，余数为$(12)_7$.

## 习　题

1. 求$(316)_7$与$(246)_7$之积.

2. 求$(203)_5$除$(4213)_5$所得的商和余数.

3. 设$a=bq+r$，证明$d|a$同时$d|b$的充要条件是$d|b$同时$d|r$.

4. 设$p$是素数，$p\nmid a$，证明：对于自然数$k=1,2,\cdots$，能使$p|ak$的最小$k$值是$p$.

5. 证明：能够同时整除$a$和$b$的最大整数是

$$\min\{ax+by;\quad ax+by>0, x\in\mathbf{Z}, y\in\mathbf{Z}\}.$$

6. 利用第5题证明：若$p$是素数，并且$p|ab$，则$p|a$或$p|b$至少有一个成立.（**算术基本引理**）.

7. 设$0<\alpha<1$，它的$b$进制表示是$(0,r_1r_2\cdots r_tr_{t+1}r_{t+2}\cdots)_b$. 如果对于任何自然数$k$，都有

$$r_{k+i}=r_i\quad(1\leqslant i\leqslant t),$$

则称$\alpha$是周期为$t$的对基$b$的纯循环小数. 证明：既约分数$\frac{A}{B}$($A<B$)的$b$进制表示是周期为$t$的纯循环小数的充要条件是，$d|(b^t-1)$.

## 第二节　基本运算的时间估计

使用计算机完成一项计算时，所需要的计算时间是一个重要的考虑因素，当然，这与所使用的算法密切相关. 在本节中，主要考察算术四则运算的时间估计，为此，先对以后常用的符号大“$O$”与小“$o$”的基本性质做些介绍.

设 $f(x)$与 $g(x)$在集合 $\mathscr{X}$ 上定义.

**定义 1**　若存在常数 $M>0$，使得对于一切 $x\in\mathscr{X}$ 都有 $|f(x)|\leqslant M\cdot|g(x)|$，则记 $f(x)=O(|g(x)|)$，称 $M$ 为大 $O$ 常数.

例如，任何常数都是 $O(1)$，并且对于任何 $\varepsilon>0$ 及 $k>0$，

$$x^k=O(e^{\varepsilon x}),\qquad x>1,$$

$$(\log x)^k=O(x^\varepsilon),\quad x>3.$$

**定义 2**　设 $f(x)$与 $g(x)$是定义在 $[x_0-\delta,x_0+\delta](\delta>0)$上的函数，若

$$\lim_{x\to x_0}\frac{f(x)}{g(x)}=0,$$

则记

$$f(x)=0(g(x)),\qquad x\to x_0.$$

例如，

$$x^2=o(x),\qquad x\to 0,$$

$$\log(1-x)=o\left(\frac{1}{1-x}\right),\quad x\to 1-0,$$

$$\log x=o(x^\varepsilon),\varepsilon>0,\qquad x\to+\infty.$$

作为定义 2 的特例，设 $f(n)$与 $g(n)$对所有正整数 $n\geqslant N_0$（$N_0$ 是固定的数）有定义，若