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

目　　录

第一章　整除与同余 …… (1)

第一节　带余数除法 …… (1)

第二节　基本运算的时间估计 …… (10)

第三节　整数的可除性 …… (17)

第四节　数论函数 …… (27)

第五节　同余 …… (35)

第二章　传统密码学 …… (49)

第一节　仿射加密方法 …… (49)

第二节　矩阵加密方法 …… (60)

第三节　数据加密标准 …… (71)

第三章　素性与因数分解 …… (81)

第一节　二次剩余 …… (81)

第二节　原根与指标 …… (94)

第三节　连分数 …… (105)

第四节　判定素性的概率算法 …… (114)

第五节　因数分解 …… (126)

第四章　公开钥密码系统 …… (139)

第一节　公开钥密码系统 …… (139)

第二节　RSA 系统 …… (149)

第三节　Rabin 系统 …… (160)

第四节　背包型公钥密码系统 …… (166)

第五节　其他公钥系统 …… (174)

第六节　L^3 算法 …… (180)
第五章　伪随机数 …… (188)
第一节　Shannon 理论 …… (188)
第二节　线性移位寄存器 …… (196)
第三节　伪随机数生成器 …… (206)

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，± 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 $a, b\in \mathbf{Z}, b>0$，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 $a_i\in N, 0\leqslant a_i\leqslant b-1, i=0,1,\cdots,k$，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

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

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

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

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 $a_k\neq 0,0\leqslant a_i\leqslant b-1(0\leqslant i\leqslant k)$,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$[\log_bn]+1$
$=\left[\dfrac{\log n}{\log b}\right]+1$,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 α,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 α 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

$$83=2\cdot41+1,\qquad 41=2\cdot20+1,$$

$$20=2\cdot10+0,\qquad 10=2\cdot5+0,$$

$$5=2\cdot2+1,\qquad 2=2\cdot1+0,$$

$$1=2\cdot0+1$$

得到　$83=(1010011)_2$.

例 2　将 92 与 17 写成三进制表示.

解　由

$$92=3\cdot30+2,\qquad 17=3\cdot5+2,$$

$$30=3\cdot10+0,\qquad 5=3\cdot1+2,$$

$$10=3\cdot3+1,\qquad 1=3\cdot0+1,$$

$$3=3\cdot1+0,$$

$$1=3\cdot0+1,$$

得到

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

例 3　写出 $\pi=3.1415926\cdots$的二进制表示.

解　〔π〕$=3=(11)_2$

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

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

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

……

继续这样的计算，得到

$$\pi=(11.001001000011\cdots)_2.$$

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

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

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

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

此处的 γ_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

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

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

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

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

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

此处 δ_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

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

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

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

则称α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

$$\lim_{n\to+\infty}\frac{f(n)}{g(n)}=0,$$

则记

$$f(n)=o(g(n)),\quad n\to+\infty.$$

例如,对于任意的 $\epsilon>0$ 及 $k>0$,

$$n^k=o(e^{\epsilon n}),\quad n\to\infty.$$

要注意,符号 O 所表示的是不等式关系,因此,含有符号 O 的等式不具备一般等式的性质. 例如,一般地,由

$$f(x)=O(g(x))\text{与 }h(x)=O(g(x))$$

不能导出 $f(x)=h(x)$,甚至不能导出 $f(x)$与 $g(x)$的量的大小的任何关系,例如,对于 $n\geqslant1$,有

(i) $f(n)=n=O(n^2),h(n)=\sqrt{n}=O(n^2),h(n)=o(f(n)),n\to\infty$;

(ii) $f(n)=n=O(n^2),h(n)=n\sqrt{n}=O(n^2),f(n)=o(h(n)),n\to\infty$;

(iii) $f(n)=n=O(n^2),h(n)=n\sqrt{n}\sin n=O(n^2),f(n)$与 $h(n)$的大小关系是不确定的.

下面给出常用的几个关于大 O 与小 o 的运算法则.

法则 I $f=O(\varphi),\varphi=O(\psi)\Rightarrow f=O(\psi)$.

法则 II $O(f)+O(g)=O(f+g)$.

法则 III $O(f)\cdot O(g)=O(fg)$.

法则 IV $O(f)\cdot o(g)=o(fg)$.

法则 V $o(f)o(g)=o(fg)$.

法则 VI $O(f)+o(f)=O(f)$.

法则 VII $f=O(\varphi),\varphi=o(\psi)\Rightarrow f=o(\psi)$.

法则 VIII 对任意的常数 k,

$$(O(f))^k=O(f^k),$$

一般地，$O(f^k)$中的大 O 常数与 k 和 $O(f)$中的大 O 常数有关.

以上几条法则的证明是容易的.作为例子，给出法则 I 的证明.

法则 I 的证明　设存在常数 M_1 与 M_2，使得当 $x\in\mathscr{X}$ 时，有 $|f(x)|\leqslant M_1\varphi(x)$及 $|\varphi(x)|\leqslant M_2\psi(x)$，则

$$|f(x)|\leqslant M_1M_2\psi(x),\quad x\in\mathscr{X},$$

即 $f(x)=O(\psi(x))$. □

利用上述运算法则，可以推导出许多有用的估计.例如，设 $P(x)$是一个 k 次多项式，$f(x)=O(g(x))$，$x\in\mathscr{X}$，则 $P(f(x))=O(g^k(x))$，$x\in\mathscr{X}$.特别地，有

$$P(\log n)=O(\log^k n)=O(n^\varepsilon)$$

对任意的 $\varepsilon>0$ 及 $n\geqslant 2$ 成立.

以下，研究二进制整数的运算.

定义 3　在数的二进制表示中，称每个位数码为“比特”(bit，是 binary digit 的简写).

定义 4　两个比特的一次加法，减法，乘法，或一个二位的二进制整数被一位的二进制整数除的运算，都称为一次“比特运算”，或“位运算”.

注 1　比特运算次数与完成计算所需要的时间基本上是成正比的.在评价一个算法时，完成它所需要的时间是一个很重要的因素.显然，这与所使用的计算机有关，不同的计算机实行一次比特运算所需时间是不同的.因此，以比特运算次数作为对计算时间的估计，能更切实地反映计算时间量，使之具有可比性.

注 2　除了定义 4 中所提到的比特运算外，还有一种比特运算——“移位”，即将数 n 的位数码向左或右移动几位，并在原

处补上数码“0”. 例如，将$(a_ka_{k-1}\cdots a_1a_0)_2$乘以$2^r$得到的积$(a_ka_{k-1}\cdots a_1a_0\,\overbrace{0\cdots0}^{r个})_2$就是通过移位得到的. 一般地，在运算过程中，完成移位所需要的时间是可以忽略不计的.

定理 1 计算两个k位二进制整数的和或差都需要$O(k)$次比特运算；计算n位数与m位数的积或商都需要$O(mn)$次比特运算.

证明 在第一节中，已经叙述了对于b进制整数的这四种基本运算. 关于加法与减法，利用第一节中叙述的方法，显然只需要$O(k)$次比特运算.

在第一节中所叙述的进行乘法的算法中，由于$b=2$，所以$\beta_i=0$或1，因此，第(i)个步骤中的$\sum_{i=0}^{n}\alpha_i\beta_jb^i$是0或$\sum_{i=0}^{n}\alpha_ib^i$，即$(\alpha_n\alpha_{n-1}\cdots\alpha_1\alpha_0)_2$. 第(ii)个步骤中，乘以$2^i$是进行一次移位，然后是将$m+1$个数求和，即是将移位后的数求和，这些数至多是$m+n$位的二进制数. 因此，完成乘法运算所需要的比特运算次数是$O(m(m+n))$. 由于被乘数与乘数可以互换而不改变乘积，所以可以假定$m\leqslant n$，于是$O(m(m+n))=O(mn)$.

关于完成除法运算所需要的比特运算次数的估计，可以类似地证明. □

为了完成一项计算，不同的算法需要不同的比特运算次数. 下面的定理给出了用更少的计算时间完成乘法运算的算法原理.

定理 2 进行$O(n^{\log_3 2})$次比特运算就可以求出两个n位二进制整数的乘积.

证明 设a和b是两个$2n$位二进制整数.

$$a=(a_{2n-1}a_{2n-2}\cdots a_1a_0)_2,\quad b=(b_{2n-1}b_{2n-2}\cdots b_1b_0)_2.$$

记

$$A_1=(a_{2n-1}\cdots a_{n+1}a_n)_2,\quad A_0=(a_{n-1}\cdots a_1a_0)_2,$$

$$B_1=(b_{2n-1}\cdots b_{n+1}b_n)_2,\quad B_0=(b_{n-1}\cdots b_1b_0)_2,$$

则 $a=2^nA_1+A_0$，$b=2^nB_1+B_0$，以及

$$\begin{aligned}ab=&(2^{2n}+2^n)A_1B_1+2^n(A_1-A_0)(B_0-B_1)\\&+(2^n+1)A_0B_0.\end{aligned}\tag{1}$$

上式右端含有三个 n 位数与 n 位数的乘积，即 A_1B_1，$(A_1-A_0)(B_0-B_1)$，与 A_0B_0，此外，是移位和加法. 因此，若以 $M(k)$ 表示求两个 k 位二进制整数的乘积所需要的比特运算次数，则由(1)式得到

$$M(2k)\leqslant 3M(k)+\lambda k,\tag{2}$$

其中 λ 是与 k 无关的常数，λk 是进行加法运算所需要的比特运算次数的估计.

现在，用归纳法证明：对于任何自然数 k，有

$$M(2^k)\leqslant\mu(3^k-2^k),\tag{3}$$

其中 $\mu=\max(\lambda,M(2))$.

当 $k=1$ 时，(3)式显然成立.

设(3)式对于 k 成立，则由(2)式得到

$$\begin{aligned}M(2^{k+1})=M(2\cdot 2^k)&\leqslant 3M(2^k)+\lambda\cdot 2^k\\&\leqslant 3\mu(3^k-2^k)+\lambda\cdot 2^k\leqslant\mu(3^{k+1}-3\cdot 2^k+2^k)\\&=\mu(3^{k+1}-2^{k+1}),\end{aligned}$$

即(3)式对 $k+1$ 也成立，由归纳法，(3)式对一切自然数 k 成立.

$M(n)$是增函数，所以，由(3)式得到

$$\begin{aligned}M(n)=M(2^{\log_2 n})&\leqslant M(2^{[\log_2 n]+1})\\&=M(2\cdot 2^{[\log_2 n]})\end{aligned}$$

$$\leqslant \mu(3^{[\log_2 n]+1} - 2^{[\log_2 n]+1})$$

$$\leqslant 3\mu \cdot 3^{[\log_2 n]} \leqslant 3\mu \cdot 3^{\log_2 n} = 3\mu \cdot n^{\log_3 2},$$

即 $M(n)=O(n^{\log_3 2})$. □

注 1 由于 $\log_3 2<2$,所以定理 2 提供了一个较好的计算乘积的算法. 目前已经知道:

(i) 存在计算两个 n 位二进制整数乘积的算法,需要 $O(n\log_2 n\log_2\log_2 n)$次比特运算;

(ii) 设 a 和 b 分别是 $2n$ 位和 n 位的二进制整数. 存在计算商 $q=\left[\frac{a}{b}\right]$的算法,需要 $O(M(n))$次比特运算,此处 $M(n)$表示计算两个 n 位二进制整数之积所需要的比特运算次数.

注 2 尽管有更好的乘法(或除法)算法,今后,为方便计,在估计求两个 n 位二进制数 a 与 $b(a\geqslant b)$的积或商所需要的比特运算次数时,仍使用估计 $O(n^2)=O(\log^2 a)$.

例 1 设 n 是 k 位二进制整数,将它写成十进制数时,试对所需要的计算时间进行估计.

解 由定理 1.3 的证明可知,为了将 n 表示为十进制数,要进行$[\log_{10} n]+1$ 次除法,在每次除法中,被除数是一个至多 k 位的二进制整数,除数则是 $10=(1010)_2$ 是一个四位的二进制数. 因此,由定理 1,将 n 写成十进制数时所需要的比特运算次数是 $O(k\cdot 4k)=O(k^2)$.

例 2 对计算 $n!$ (n 是正整数)所需要的比特运算次数做出估计.

解 依次用

$$3!=3\cdot 2!, 4!=4\cdot 3!, \cdots, n!=n\cdot(n-1)!$$

计算 $n!$,共需要 $n-2$ 次乘法,每次乘法是数 $j!$ 与$(j+1)$相乘,它们的位数分别不超过 $n!$ 和 n 的位数.

设 n 是 k 位二进制数，则 $n!$ 是 $O(nk)$位二进制数，因此，计算 $j!$ 与 $j+1$ 的乘积($j\leqslant n-1$)至多需要 $O(nk\cdot k)=O(nk^2)$次比特运算，计算 $n!$ 需要 $n\cdot O(nk^2)=O(n^2k^2)$次比特运算. 由于 $k=O(\log n)$，所以 $O(n^2k^2)=O(n^2\log^2 n)$.

例 3 对计算$\lceil\sqrt{n}\rceil$所需要的比特运算次数做出估计.

解 设 n 的二进制表示有 $k+1$ 位，则

$$2^{\frac{k}{2}}\leqslant\sqrt{n}<2^{\frac{k+1}{2}},$$

因此，$\lceil\sqrt{n}\rceil$的二进制表示中有$\left[\frac{k}{2}\right]+1$个位数码.

设$\lceil\sqrt{n}\rceil=(a_ra_{r-1}\cdots a_1a_0)_2$，　$r=\left[\frac{k}{2}\right]$. 下面说明怎样依次确定 $a_i(o\leqslant i\leqslant r)$.

取 $a_r=1$，记 $m_r=(100\cdots0)_2$，m_r 是 $r+1$ 位二进制数.

若 $m_r^2=n$，则 $m_r=\sqrt{n}$，$\lceil\sqrt{n}\rceil$已求出.

若 $m_r^2\neq n$，则必是 $m_r^2<n$，令

$$a_{r-1}=\begin{cases}1,若((110\cdots0)_2)^2<n\\0,若((110\cdots0)_2)^2>n.\end{cases}$$

一般地，设数码 $a_r,a_{r-1},\cdots,a_i$ 已经确定，若$((a_r,\cdots,a_i,0,\cdots0)_2)^2=n$，则$\lceil\sqrt{n}\rceil$已经求出，否则，令

$$a_{i-1}=\begin{cases}1,若((a_ra_{r-1}\cdots a_i10\cdots0)_2)^2<n,\\0,若((a_ra_{r-1}\cdots a_i10\cdots0)_2)^2>n.\end{cases}$$

如此依次确定 $a_r,\cdots,a_0$，得到$\lceil\sqrt{n}\rceil$.

由上述计算过程，在确定 a_i 时，要计算两个位数不超过$\frac{k}{2}+1$的二进制数的平方，还要做两次两个 k 位数的减法，完成这些计算需要 $O(k^2)$次比特运算. 所以，确定出所有 $a_i(0\leqslant i\leqslant r)$需要 $O(k^3)$比特运算，即 $O(\log^3 n)$次比特运算.

定义 5　设 n_i 是 $k_i(1\leqslant i\leqslant r)$ 位二进制数. 如果存在整数 $d_i>0(1\leqslant i\leqslant r)$，使得完成某个关于 $n_1,\cdots,n_r$ 的算法所需要的比特运算次数为 $O(k_1^{d_1}\cdots k_r^{d_r})$，则称这个算法是多项式时间算法.

除例 2 外，本节中所提到的算法都是多项式时间算法.

习　题

1. 证明关于大 O 与小 o 运算法则 Ⅰ 和法则 Ⅷ.

2. 设 n 是二进制正整数，试对将 n 写成 r 进制数所需要的计算时间做出估计.

3. 设 $n=(33321)_5$，试求 $[\sqrt{n}]$ 的二进制表示.

4. 已知公式

$$(1^2+2^2+\cdots+n^2)=\frac{1}{6}n(n+1)(2n+1),$$

(1) 试对完成左端的计算所需要的时间做出估计(以 n 为变量)；

(2) 试对完成右端的计算所需要的时间做出估计.

5. 将计算 N^n 所需要的时间做出估计(以 N,n 为变量).

第三节　整数的可除性

定理 1(算术基本定理)　对任意正整数 $n>1$，有

$$n=p_1^{\alpha_1}\cdots p_k^{\alpha_k} \tag{1}$$

其中 p_i 是素数，α_i 是正整数$(1\leqslant i\leqslant k)$，若不计较因数的次序，这个表示式是唯一的，称为 n 的标准分解式，或素因数分解式.

证明　若 n 是素数，定理显然成立. 若 n 不是素数，则它的最小真约数 d 是素数，设为 p_1，则 $n=p_1n_1$，若 n_1 是素数，定理得

证. 否则，又有 $n=p_1p_2n_2$，其中 p_2 是素数。如此继续下去，由于 n 是有限数，它的真约数都不小于 2，所以经过有限步骤后，必有 $n=p_1p_2\cdots p_t$，其中 p_i 都是素数。

下证唯一性. 设 $n=p_1p_2\cdots p_s=q_1q_2\cdots q_t$，其中诸 p_i,q_i 都是素数. 由 $p_1|(q_1\cdots q_t)$及算术基本引理(习题 1.7)可知，必有某个 $q_{j1}(1\leqslant j_1\leqslant t)$使得 $p_1|q_{j_1}$，但 q_{j_1}也是素数，所以 $p_1=q_{j_1}$，于是

$$p_2p_3\cdots p_s=q_1\cdots q_{j_1-1}q_{j_1+1}\cdots q_t.$$

同理可以证明，对于每个 i，$2\leqslant i\leqslant s$，都有某个 j_i，使得

$$p_i=q_{j_i}\qquad(2\leqslant i\leqslant s),$$

因此 $s\leqslant t$. 若将上述过程中的 p_i 与 q_i 交换，则有 $t\leqslant s$. 所以 $s=t$，即全体 p_i 的集合与全体 q_i 的集合是相同的. 因此，若写成(1)式的形式，又不计较次序，则(1)式是唯一的. □

推论 若(1)式成立，则 n 的约数具有 $d=\pm p_1^{\lambda_1}\cdots p_k^{\lambda_k}(0\leqslant\lambda_i\leqslant\alpha_i,1\leqslant i\leqslant k)$的形式，$n$ 的倍数具有 $m=lp_1^{\beta_1}\cdots p_k^{\beta_k}(l\in\mathbf{Z},\beta_i\geqslant\alpha_i,1\leqslant i\leqslant k)$的形式.

定义 1 设 $a_i(1\leqslant i\leqslant k)$是不全为零的整数，$d|a_i(1\leqslant i\leqslant k)$，则称 d 是 $a_1,\cdots,a_k$ 的公约数. 数 $a_1,\cdots,a_k$ 的最大的公约数，称为它们的最大公约数，记为 $gcd(a_1,\cdots,a_k)$，或$(a_1,\cdots,a_k)$. 若 $(a_1,\cdots,a_k)=1$，则称 $a_1,\cdots a_k$ 是互素的；若$(a_i,a_j)=1(1\leqslant i<j\leqslant k)$，则称它们是两两互素的.

定义 2 设 b_i 是不为零的整数，$b_i|d,(1\leqslant i\leqslant k)$，则称 d 是 $b_1,\cdots,b_k$ 的公倍数，$b_1,\cdots,b_k$ 的最小的正的公倍数称为它们的最小公倍数，记为 $lcm(b_1,\cdots,b_k)$或$[b_1,\cdots,b_k]$.

推论 下面的结论是成立的：

(1) $(a_1,\cdots,a_k)=(|a_1|,\cdots,|a_k|)$；

(2) $[a_1,\cdots,a_k]=[|a_1|,\cdots,|a_k|]$;

(3) $a|b\Rightarrow(a,b)=|a|,[a,b]=|b|$ $(b\neq0)$.

定理 2 设 $a=p_1^{\alpha_1}\cdots p_r^{\alpha_r},b=p_1^{\beta_1}\cdots p_r^{\beta_r}$,其中诸 p_i 是互不相同的素数,$\alpha_i,\beta_i\geqslant0(1\leqslant i\leqslant r)$,而且,若某个 p_i 不是 a(或 b)的约数,就规定 $\alpha_i=0$(或 $\beta_i=0$). 则

$$(a,b)=\prod_{i=1}^{r}p_i^{\lambda_i},[a,b]=\prod_{i=1}^{r}p_i^{\mu_i}$$

其中

$$\lambda_i=\min(\alpha_i,\beta_i),\mu_i=\max(\alpha_i,\beta_i).$$

证明 由定理 1 的推论可得证. □

推论 1 对任意的正整数 m,有

$$[ma,mb]=m[a,b],$$

$$(ma,mb)=m(a,b).$$

推论 2 若 $d|a,d|b$,则

$$\left[\frac{a}{d},\frac{b}{d}\right]=\frac{1}{d}[a,b],$$

$$\left(\frac{a}{d},\frac{b}{d}\right)=\frac{1}{d}(a,b).$$

推论 3 设 $a>0$, $b>0$,则 $ab=[a,b](a,b)$.

推论 4 a 与 b 的任一公约数是(a,b)的约数;a 与 b 的任一公倍数是$[a,b]$的倍数.

推论 5 若$(a,c)=1$,则$(ab,c)=(b,c)$.

定理 3 若 $a=qb+c$,则$(a,b)=(b,c)$.

证明 由习题 1.4 可知 a 与 b 的全体公约数的集合就是 b 与 c 的全体公约数的集合,因此,它们有共同的最大元素,即$(a,b)=(b,c)$. □

利用定理 3 可以得出一个求出满足 $ax+by=(a,b)$的 x 与

y 的算法，即 Euclid 算法，又称辗转相除法.

Euclid 算法　对于给定的 a,b，依次做下面的除法：

$$\left.\begin{array}{lll} a=q_1b+r_1, & 0<r_1<b, & (b\nmid a), \\ b=q_2r_1+r_2, & 0<r_2<r_1, & (r_1\nmid b), \\ r_1=q_3r_2+r_3, & 0<r_3<r_2, & (r_2\nmid r_1), \\ \cdots\cdots & & \\ r_{n-2}=q_nr_{n-1}+r_n & 0<r_n<r_{n=1}, & (r_{n-1}\nmid r_{n-2}), \\ r_{n-1}=q_{n+1}r_n, & & (r_n\mid r_{n-1}), \end{array}\right\} \tag{2}$$

由于诸 r_i 是正的，并且 $r_{i+1}<r_i$，所以上述除法的次数是有限的.

由定理 3 见到

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

定理 4　设 $a>0,b>0$，并且进行 Euclid 算法，则在(2)式中，有

$$Q_ka-P_kb=(-1)^{k-1}r_k,\ k=1,2,\cdots,n,$$

其中

$$P_0=1,P_1=q_1,P_k=q_kp_{k-1}+p_{k-2},2\leqslant k\leqslant n,$$

$$Q_0=0,Q_1=1,Q_k=q_kQ_{k-1}+Q_{k-2},2\leqslant k\leqslant n.$$

证明　由

$$a-bq_1=Q_1a-P_1b=(-1)^{1-1}r_1$$

可知定理当 $k=1$ 时正确.

再由

$$b=q_2r_1+r_2=q_2(a-q_1b)+r_2,$$

得到

$$(-1)^{2-1}r_2=(q_2a-(q_1q_2+1)b=Q_2a-p_2b,$$

即定理当 $k=2$ 时正确.

设定理对于小于 $k+1$ 的正整数正确，则由 $r_{k-1}=q_{k+1}r_k+r_{k+1}$ 得到

$$r_{k+1}=(-1)^{k-2}(Q_{k-1}a-P_{k-1}b)-q_{k+1}(-1)^{k-1}(Q_ka-P_kb),$$

$$\begin{aligned}(-1)^kr_{k+1}&=Q_{k-1}a-P_{k-1}b+q_{k+1}Q_ka-q_{k+1}P_kb\\&=(q_{k+1}Q_k+Q_{k-1})a-(q_{k+1}P_k+P_{k-1})b\\&=Q_{k+1}a-P_{k+1}b,\end{aligned}$$

即定理对于 $k+1$ 也正确. 由归纳法证得定理. □

注　定理 4 说明，Euclid 算法在求出 (a,b) 的同时，还求出了整数 x_0 与 y_0，使得

$$ax_0+by_0=(a,b). \tag{3}$$

现在，我们来估计用 Euclid 算法计算(3)式中的 x_0,y_0，以及 (a,b) 所需要的运算时间.

定义 3　由

$$f_1=f_2=1,f_n=f_{n-1}+f_{n-2}\quad(n\geqslant 3)$$

定义的数 $f_n(n\geqslant 1)$ 称为 Fibonacci 数.

引理 1　记 $\alpha=\frac{1}{2}(\sqrt{5}+1)$，则 Fibonacci 数满足不等式

$$f_k>\alpha^{k-2},\quad k\geqslant 3. \tag{4}$$

证明　当 $k=3$ 时，(4)式显然成立.

设(4)式当 $k\leqslant n$ 时成立，利用 $\alpha^2=\alpha+1$，得到

$$\alpha^{n-1}=\alpha^2\cdot\alpha^{n-3}=(\alpha+1)\alpha^{n-3}=\alpha^{n-2}+\alpha^{n-3},$$

再由归纳假设，$\alpha^{n-2}<f_n,\alpha^{n-3}<f_{n-1}$，及定义 3，得到 $\alpha^{n-1}<f_n+f_{n-1}=f_{n+1}$. 由归纳法证得引理. □

定理 5　利用 Euclid 算法求两个正整数 a 与 b 的最大公约数所需要的除法运算次数 $n\leqslant 5k$，其中 k 是整数 $\min(a,b)$ 的十进制表示的位数码的个数.

证明 不妨设 $a>b$. 在 Euclid 算法中，由于 $r_n<r_{n-1}$，所以 $q_{n+1}\geqslant 2$，又有 $q_i\geqslant 1(1\leqslant i\leqslant n)$，因此，有

$$r_n\geqslant 1=f_2,$$

$$r_{n-1}\geqslant 2r_n=2=f_3,$$

$$r_{n-2}\geqslant r_{n-1}+r_n\geqslant f_2+f_3=f_4,$$

$$r_{n-3}\geqslant r_{n-2}+r_{n-1}\geqslant f_3+f_4=f_5,$$

$$\cdots\cdots$$

$$r_2\geqslant r_3+r_4\geqslant f_{n-1}+f_{n-2}=f_n,$$

$$b\geqslant r_2+r_1\geqslant f_n+f_{n-1}=f_{n+1},$$

由此及引理 1 推出 $b>\left(\frac{\sqrt{5}+1}{2}\right)^{n-1}$，即

$$\log_{10}b>(n-1)\log_{10}\frac{\sqrt{5}+1}{2}>\frac{n-1}{5}.$$

设 b 的十进制位数是 k，则 $5k>n-1$，因为 n 是整数，所以 $n\leqslant 5k$. □

推论 对于给定的正整数 a,b(设 $a>b$)，用 Euclid 算法计算(a,b)并求出使 $ax+by=(a,b)$ 成立的整数 x,y，需要 $O(\log^2 a\log b)$次比特运算.

证明 利用定理 5，并且注意到，完成 Euclid 算法中的一次除法需要 $O(\log^2 a)$次比特运算. □

定理 6 方程

$$ax+by=c \tag{5}$$

有解的充分必要条件是$(a,b)\mid c$. 若有解(x_0,y_0)，则它的解具有

$$x=x_0+\frac{b}{(a,b)}t,\quad y=y_0-\frac{a}{(a,b)}t,\quad t\in\mathbf{Z} \tag{6}$$

的形式.

证明 由习题 1.6，$(a,b)=\min\{ax+by;x\in\mathbf{Z},y\in\mathbf{Z}\}$.

若$(a,b)|c$,则存在$\bar{x},\bar{y}$,使得$a\bar{x}+b\bar{y}=(a,b)$,此时,容易验证

$$x=\frac{c}{(a,b)}\bar{x},\quad y=\frac{c}{(a,b)}\bar{y}$$

是方程(5)的解.

若方程(5)有解(x_1,y_1),则$ax_1+by_1=c$. 由此及$(a,b)|a$,$(a,b)|b$可推知$(a,b)|c$.

以上证明了定理的前半部分.

现在,设(x_0,y_0)是(5)的解,则

$$a(x-x_0)+b(y-y_0)=0$$

对(5)的任一组解(x,y)成立,即

$$\frac{a}{(a,b)}(x-x_0)=-\frac{b}{(a,b)}(y-y_0).$$

由于$\left(\frac{a}{(a,b)},\frac{b}{(a,b)}\right)=1$,所以

$$\frac{b}{(a,b)}|(x-x_0),\quad \frac{a}{(a,b)}|(y-y_0),$$

因此

$$\frac{\frac{(x-x_0)}{b}}{\frac{}{(a,b)}}=-\frac{\frac{(y-y_0)}{a}}{\frac{}{(a,b)}}=t\in\mathbf{Z},$$

这证明了定理的后半部分结论. □

下面介绍的 Stein 算法可以在更少的时间内求出两个数的最大公约数. 为此,先给出最大公约数的几个性质.

引理 2 设$a>b$

(i) 若$2|a,2|b$,则$(a,b)=2\left(\frac{a}{2},\frac{b}{2}\right)$;

(ii) 若$2|a,2\nmid b$,则$(a,b)=\left(\frac{a}{2},b\right)$;

(iii) 若 $2\nmid a, 2\nmid b$，则 $(a,b)=\left(\frac{a-b}{2},b\right)$.

证明 (i)与(ii)可由定理 2 及其推论导出.

(iii)可由 $(a,b)=(a-b,b)$及(ii)导出. □

Stein 算法 对给定的正整数 $a,b,a>b$，按以下步骤进行：

(i) 求出最大的整数 $\alpha, 2^{\alpha}\mid a, 2^{\alpha}\mid b$，令

$$a_1=a\cdot 2^{-\alpha},\quad b_1=b\cdot 2^{-\alpha}$$

(ii) 若有整数 $\beta(>0)$，使 $2^{\beta}\mid a$，(或 $2^{\beta}\mid b_1$)，令

$$a_2=a_1 2^{-\beta},\quad b_2=b_1(\text{或 } a_2=a_1,\quad b_2=b_1 2^{-\beta});$$

(iii) 若 $a_2>b_2$，令

$$a_3=\frac{1}{2}(a_2-b_2), b_3=b_2;$$

若 $a_2<b_2$，令

$$a_3=a_2,\quad b_3=\frac{1}{2}(b_2-a_2).$$

(iv) 继续重复进行步骤(ii)和(iii)，得到数对 $a_1,b_1;\quad a_2, b_2;\cdots$，当 $a_s=b_s$ 时停止计算. 此时由引理 2 可知

$$(a,b)=2^{\alpha}(a_1,b_1)=2^{\alpha}(a_2,b_2)=\cdots=2^{\alpha}(a_s,b_s)=2^{\alpha}\cdot a_s.$$

定理 7 给定正整数 a 与 b，$a>b$，则用 Stein 算法求 (a,b) 需要 $O(\log^2 a)$次比特运算.

证明 由 Stein 算法中 a_i 与 b_i 的确定方式可知，若记 $a_0=a, b_0=b$，则

$$a_i+b_i\leqslant\frac{1}{2}(a_{i-1}+b_{i-1}),\quad 1\leqslant i\leqslant s,$$

因此，

$$2\leqslant a_s+b_s\leqslant\frac{1}{2^s}(a+b)\leqslant\frac{1}{2^{s-1}}a,$$

即只需要 $s\leqslant\log_2 a+1$ 个步骤即可完成算法.

在算法的每一个步骤中，只有移位(用 2^{α} 或 2^{β} 除一个数)，或减法(比较数的大小)，因此，每个步骤至多是 $O(\log a)$次比特运算，而整个算法需要 $O(\log a)\cdot O(\log a)=O(\log^2 a)$次比特运算.

注 用 Stein 算法求最大公约数所需要的计算时间远少于用 Euclid 算法所需要的计算时间. 但是，Stein 算法不能同时求出 x,y，使得 $ax+by=(a,b)$.

例 1 求 872 与 331 的最大公约数，并求出使 $872x+331y=(872,331)$成立的整数 x 与 y.

解 由 Euclid 算法，有

$$872=2\cdot 331+210$$
$$331=1\cdot 210+121$$
$$210=1\cdot 121+89$$
$$121=1\cdot 89+32$$
$$89=2\cdot 32+25$$
$$32=1\cdot 25+7$$
$$25=3\cdot 7+4$$
$$7=1\cdot 4+3$$
$$4=1\cdot 3+1$$
$$3=3\cdot 1$$

在定理 4 中取 $n=9$，以及

$$q_1=2,\ q_2=1,\ q_3=1,\ q_4=1,\ q_5=2,\ q_6=1,$$
$$q_7=3,\ q_8=1,\ q_9=1,$$

计算

$$P_0=1,\ P_1=2,\ P_2=1\cdot 2+1=3,\ P_3=1\cdot 3+2=5,$$
$$P_4=1\cdot 5+3=8,\ P_5=2\cdot 8+5=21,$$

$P_6=1\cdot 21+8=29$,

$P_7=3\cdot 29+21=108$, $P_8=1\cdot 108+29=137$,

$P_9=1\cdot 137+108=245$,

$Q_0=0$, $Q_1=1$, $Q_2=1\cdot 1+0=1$, $Q_3=1\cdot 1+1=2$,

$Q_4=1\cdot 2+1=3$, $Q_5=2\cdot 3+2=8$, $Q_6=1\cdot 8+3=11$,

$Q_7=3\cdot 11+8=41$, $Q_8=1\cdot 41+11=52$,

$Q_9=1\cdot 52+41=93$,

因此,

$$93\cdot 872-245\cdot 331=(-1)^{9-1}r_9=(872,331),$$

即 $x=93, y=-245$.

例 2 用 Stein 算法求(544,1360).

解 $(544,1360)=16(34,85)=16(85,34)$

$=16(17,34)=16(17,17)=16\cdot 17$

$=272$.

习 题

1. 证明下面的两个等式:

(1) $[[a_1,\cdots,a_i],[a_{i+1},\cdots,a_n]]=[a_1,\cdots,a_n]$;

(2) $\big((a_1,\cdots,a_i),(a_{i+1},\cdots,a_n)\big)=(a_1,\cdots,a_n)$.

2. 用三种方法求 $gcd(360,294)$.

3. 以 $p^\alpha \| a$ 表示 $p^\alpha | a$ 同时 $p^{\alpha+1}\nmid a$,证明

(1) 若 $p^\alpha \| a, p^\beta \| b$,则 $p^{\alpha+\beta} \| ab$;

(2) 若 $p^\alpha \| a, p^\beta \| b, \alpha<\beta$,则 $p^\alpha \| a+b$.

4. 证明:若 $(m,n)=1$, $l|mn$,则必有 l_1 与 l_2,使得 $l=l_1l_2, (l_1,l_2)=1$,并且 $l_1|m$, $l_2|n$.

5. 求解方程：

(1) $3x+5y=142$；

(2) $7x+3y=15$.

6. 设 $d=(m,n)$且 $a>1$，证明$(a^m-1,\ a^n-1)=a^d-1$.

第四节　数论函数

定义 1　在全体(或部分)正整数集合或整数集合上定义的函数，称为数论函数，或算术函数.

一般地，考察的数论函数都是定义在正整数的集合上.

例 1　除数函数 $d(n)$. $d(n)$表示数 n 的正因数的个数，即

$$d(n)=\sum_{d\mid n}1.$$

显然 $d(1)=1$. 若 $n=p_1^{\alpha_1}\cdots p_k^{\alpha_k}$ 是 n 的素因数分解式，则

$$d(n)=(\alpha_1+1)(\alpha_2+1)\cdots(\alpha_k+1) \tag{1}$$

例 2　Eulerφ—函数 $\varphi(n)$. $\varphi(n)$表示不超过 n 的与 n 互素的正整数的个数，即

$$\varphi(n)=\sum_{1\leqslant d\leqslant n,\,(d,n)=1}1.$$

例 3　Möbius 函数 $\mu(n)$. $\mu(n)$如下定义：

$$\mu(n)=\begin{cases}1, & n=1\\ (-1)^S & n=p_1p_2\cdots p_s,\\ 0, & \text{其他}\end{cases}$$

其中 $p_1,\cdots,p_s$ 是互不相同的素数.

例 4　$\pi(x)$. $\pi(x)$等于不超过 x 的素数的个数.

例 5　$[x]$. $[x]$等于不超过 x 的最大整数，即 x 的整数部分.

另外，由 Dirichlet 级数定义的函数

$$\zeta(s)=\sum_{n=1}^{\infty}\frac{1}{n^s}\quad(s=\sigma+it,\ \mathrm{Res}=\sigma>1)$$

在数论研究中也起着非常重要的作用.

定理 1 若$(m,n)=1$，则 $d(mn)=d(m)d(n)$.

证明 由(1)式得证. □

定义 2 若对于任何互素的整数 m 与 n，都有

$$f(mn)=f(m)f(n)\tag{2}$$

成立，则称 $f(n)$是积性函数；若(2)式对任意的 m 与 n 成立，则称 $f(n)$是完全积性函数.

定理 2 $\mu(n)$是积性函数，并且

$$\sum_{d|n}\mu(d)=\begin{cases}1, & n=1\\ 0, & n>1.\end{cases}\tag{3}$$

证明 由 $\mu(n)$的定义可知它是积性函数.

当 $n=1$ 时，(3)式成立.

当 $n>1$ 时，设 $n=p_1^{a_1}\cdots p_k^{a_k}$，则由 $\mu(n)$的定义得到

$$\begin{aligned}\sum_{d|n}\mu(n)&=\mu(1)+\mu(p_1)+\cdots+\mu(p_k)+\mu(p_1p_2)\\&\quad+\mu(p_1p_3)+\cdots+\mu(p_{k-1}p_k)+\cdots+\mu(p_1p_2\cdots p_k)\\&=1+\binom{k}{1}(-1)+\binom{k}{2}(-1)^2+\cdots+\binom{k}{k}(-1)^k\\&=(1-1)^k=0.\end{aligned}$$

□

定理 3 $\varphi(n)$是积性函数，并且

$$\varphi(n)=n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right),\tag{4}$$

其中 $p_1,p_2,\cdots,p_k$ 是 n 的不同的素因数.

证明 当 $n=1$ 时，(4)式显然成立. 若 $n=p^a$，则在不超过 $n=p^a$的正整数中，不与 p^a 互素的数是 $kp(1\leqslant k\leqslant p^{a-1})$，共 p^{a-1}

个，所以 $\varphi(p^a)=p^a-p^{a-1}=p^a\left(1-\frac{1}{p}\right)$. 因此，为了证明定理，只需证明 $\varphi(n)$ 是积性函数.

由 $\varphi(n)$ 的定义及定理 2，有

$$\varphi(n)=\sum_{\substack{1\leqslant d\leqslant n\\(d,n)=1}}1=\sum_{1\leqslant d\leqslant n}\sum_{l\mid(d,n)}\mu(l)$$

$$=\sum_{1\leqslant d\leqslant n}\sum_{\substack{l\mid d\\ l\mid n}}\mu(l)=\sum_{l\mid n}\mu(l)\sum_{\substack{1\leqslant d\leqslant n\\ l\mid d}}1$$

$$=\sum_{l\mid n}\mu(l)\frac{n}{l}=n\sum_{l\mid n}\frac{\mu(l)}{l}. \tag{5}$$

若 $(m,n)=1$，$l\mid mn$，则由习题 3.4 可知，存在 l_1,l_2 使得 $(l_1,l_2)=1$，$l=l_1l_2$，并且 $l_1\mid m_1$，$l_2\mid m_2$，因此，由(5)式得到

$$\varphi(mn)=mn\sum_{l\mid mn}\frac{\mu(l)}{l}=mn\sum_{\substack{l_1l_2\mid mn\\ l_1\mid m,l_2\mid n,(l_1,l_2)=1}}\frac{\mu(l_1l_2)}{l_1l_2}$$

$$=m\sum_{l_1\mid m}\frac{\mu(l_1)}{l_1}\cdot n\sum_{l_2\mid n}\frac{\mu(l_2)}{l_2}=\varphi(m)\varphi(n),$$

上面，我们用到了 $\mu(n)$ 的积性，即当 $(l_1,l_2)=1$ 时，

$$\mu(l_1l_2)=\mu(l_1)\mu(l_2).$$ □

例 6 设 $n=pq$，p 和 q 是不同的素数.

(i) 若已知 p 与 q，则计算 $\varphi(n)$ 需要 $O(\log^2 n)$ 次比特运算；

(ii) 若已知 n 与 $\varphi(n)$，则计算 p 和 q 需要 $O(\log^3 n)$ 次比特运算.

解 (i) 若 $p=2$，则 $q=\frac{n}{2}$，$\varphi(n)=\frac{n}{2}-1$，定理的结论是显然的.

若 p 与 q 都是奇数，则

$$\varphi(n)=\varphi(pq)=(p-1)(q-1)$$

即只需要两次减法和一次乘法，因此，只需要 $O(\log^2 n)$ 次比特运算即可求出 $\varphi(n)$.

(ii) 当 n 与 $\varphi(n)$ 已知时，由

$$p+q=n+1-\varphi(n) \quad 及 \ pq=n$$

可知 p 与 q 分别是方程 $x^2-(n+1-\varphi(n))x+n=0$ 的两个根，即

$$\frac{1}{2}\left((n+1-\varphi(n)\pm\sqrt{(n+1-\varphi(n))^2-4n}\right).$$

由例 2.3 可知，计算这两个根需要 $O(\log^3 n)$ 次比特运算.

注：若 n 与 p，q 均已知，则由

$$\varphi(n)=(p-1)(q-1)=n-p-q+1$$

计算 $\varphi(n)$ 只需 $O(\log n)$ 次比特运算.

例 7 证明 $\sum\limits_{d|n}\varphi(d)=n$.

解 由(5)式，

$$\sum_{d|n}\varphi(d)=\sum_{d|n}d\sum_{l|d}\frac{\mu(l)}{l}=\sum_{l|n}\frac{\mu(l)}{l}\sum_{\substack{l|d\\ d|n}}d$$

$$=\sum_{l|n}\frac{\mu(l)}{l}\sum_{kl|n}kl=\sum_{l|n}\mu(l)\sum_{kl|n}k$$

$$=\sum_{k|n}k\sum_{l|\frac{n}{k}}\mu(l).$$

利用定理 2 可知上式右端等于 n.

定理 4 设 $x\geqslant 1$，则

$$\sum_{n\leqslant x}\varphi(n)=\frac{3}{\pi^2}x^2+O(x\log x).$$

证明 由(5)式得到

$$\sum_{n\leqslant x}\varphi(n)=\sum_{n\leqslant x}n\sum_{l|n}\frac{\mu(l)}{l}=\sum_{l\leqslant x}\frac{\mu(l)}{l}\sum_{\substack{n\leqslant x\\ l|n}}n$$

$$= \sum_{l\leqslant x} \frac{\mu(l)}{l} \sum_{dl\leqslant x} dl = \sum_{l\leqslant x} \mu(l) \sum_{d\leqslant \frac{x}{l}} d$$

$$= \sum_{l\leqslant x} \mu(l) \cdot \frac{1}{2}\left[\frac{x}{l}\right]\left(\left[\frac{x}{l}\right]+1\right)$$

$$= \frac{1}{2}\sum_{l\leqslant x} \mu(l)\left(\frac{x}{l}+O(1)\right)^2$$

$$= \frac{x^2}{2}\sum_{l\leqslant x} \frac{\mu(l)}{l^2} + O\left(\sum_{l\leqslant x} \frac{x}{l}\right) + O(x)$$

$$= \frac{x^2}{2}\sum_{l=1}^{\infty} \frac{\mu(l)}{l^2} - \frac{x^2}{2}\sum_{l>x} \frac{\mu(l)}{l^2} + O(x\log x). \tag{6}$$

另一方面，由定理 2 易知

$$\sum_{n=1}^{\infty} \frac{1}{n^2}\sum_{n=1}^{\infty} \frac{\mu(n)}{n^2} = 1, \tag{7}$$

由此及 $\sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}$，并利用 $|\mu(n)|\leqslant 1$，得到

$$\left|\sum_{l>x} \frac{\mu(l)}{l^2}\right| = O\left(\frac{1}{x}\right).$$

由上式、(7)式、及(6)式，证得定理. □

对于函数$[x]$，下面的性质是易证的：

(i) $x\geqslant y \Rightarrow [x]\geqslant [y]$；

(ii) $x-1<[x]\leqslant x$；

(iii) 若 n 是整数，则$[n+x]=n+[x]$；

(iv) $[x+y]=\begin{cases}[x]+[y], \text{当 } x+y-[x]-[y]<1,\\ [x]+[y]+1, \text{当 } x+y-[x]-[y]\geqslant 1;\end{cases}$

(v) 设 $x>0$，$n\in N$，则不超过 x 且被 n 整除的正整数的个数是$\left[\frac{x}{n}\right]$.

例 8 设 p 与 q 是奇素数，$p\neq q$，则

$$\sum_{0<x<\frac{q}{2}}\left[\frac{p}{q}x\right]+\sum_{0<y<\frac{p}{2}}\left[\frac{q}{p}y\right]=\frac{1}{4}(p-1)(q-1).$$

证明 记 $P=\frac{p-1}{2}, Q=\frac{q-1}{2}$,

在图 1 中,L 是直线 $y=\frac{q}{p}x$. 由于 $p\neq q$,所以在直线 L 上除原点 O 外没有整点(即两个座标都是整数的点). 此外,点 C 的 y 坐标是 $\frac{q}{p}\cdot\frac{p-1}{2}<\frac{q}{2}=Q+\frac{1}{2}$,所以,除 A 点外,在线段 AC 上也没有整点,因此,由

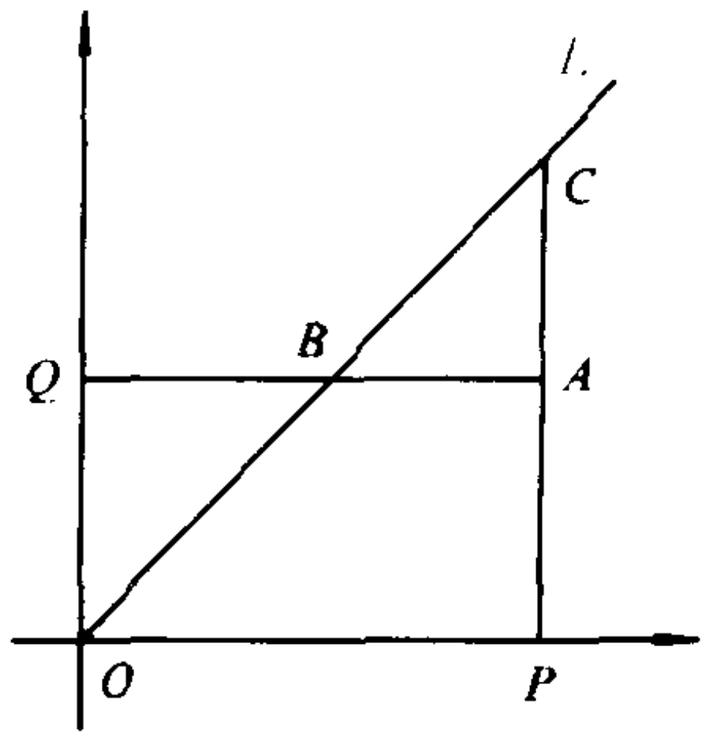


图 1

$\triangle OCP$ 上的整点个数 $+\triangle OBQ$ 上的整点个数 $=$ 矩形 $OPAQ$ 上的整点个数 $-OP$ 与 OQ 上的整点个数,

$$\sum_{j=1}^{P}\left[\frac{p}{q}j\right]=\triangle OCP \text{ 上的整点个数}-OP \text{ 上的整点个数},$$

以及

$$\sum_{j=1}^{Q}\left[\frac{q}{p}j\right]=\triangle OBQ \text{ 上的整点个数}-OQ \text{ 上的整点个数},$$

即可得出结论.

定理 5 在 $n!$ 的素因数分解式中,素因数 p 的指数

$$\alpha=\left[\frac{n}{p}\right]+\left[\frac{n}{p^2}\right]+\cdots+\left[\frac{n}{p^r}\right]+\cdots.$$

证明 由函数 $[x]$ 的性质(Ⅴ),不超过 n 且能被 p^r 整除的正整数有 $\left[\frac{n}{p^r}\right]$ 个,因此,满足

$$m\leqslant n, p^r\mid m, p^{r+1}\nmid m$$

的正整数 m 的个数是 $\left[\frac{n}{p^r}\right]-\left[\frac{n}{p^{r+1}}\right]$. 所以,$n!$ 中所含的 p 的指

数应是

$$\alpha=1\cdot\left(\left[\frac{n}{p}\right]-\left[\frac{n}{p^2}\right]\right)+2\cdot\left(\left[\frac{n}{p^2}\right]-\left[\frac{n}{p^3}\right]\right)+\cdots$$
$$+r\left(\left[\frac{n}{p^r}\right]-\left[\frac{n}{p^{r+1}}\right]\right)+\cdots,$$

这就是定理结论. □

定理 6 有无穷多个素数.

证明 假设只有有限多个素数 $p_1,p_2\cdots,p_n$. 我们要指出至少还有另外一个与它们不同的素数. 事实上,令 $N=p_1p_2\cdots p_n+1$,则由第一章第一节定理 1, N 必定有一个素因数 p. 由于 $p_i\nmid N$ $(1\leqslant i\leqslant n)$,所以 p 是不同于任何 p_i 的另一个素数,这说明素数个数不可能是有限的. □

定理 6 表明,$\pi(x)\to\infty(x\to\infty)$. 关于 $\pi(x)$ 的研究,是数论的重要课题之一.

定理 7 若 $(a,b)=1$,则在数列 $\{an+b\}$ 中,不超过 x 的素数的个数是

$$\pi(x;a,b)=\frac{1}{\varphi(a)}\int_2^x\frac{dt}{\log t}+O(xe^{-c\sqrt{\log x}}),$$

其中 $a\leqslant(\log x)^A$, $A>0$ 是常数, $c>0$ 是与 A 有关的常数.

特别地,

$$\pi(x)=\int_2^x\frac{dt}{\log t}+O(xe^{-c\sqrt{\log x}}).$$

这个定理的证明相当繁,且需要较多的解析数论知识,此处略去.

推论 以 p_n 表示第 n 个素数,则

$$p_n\sim n\log n.$$

证明 由定理 7,

$$n=\pi(p_n)\sim p_n(\log p_n)^{-1},$$

因此，

$$\log n \sim \log p_n,$$

$$p_n \sim n\log p_n \sim n\log n. \qquad \square$$

下面介绍 $\zeta(s)$ 的几个性质：

(1) $\zeta(s)$ 可以解析延拓到全 s 平面 $(s\neq 1)$，$s=1$ 是它的一阶极点；

(2) $\zeta(s)$ 满足函数方程

$$\zeta(s)=2^s\pi^{s-1}\sin\frac{1}{2}s\pi\Gamma(1-s)\zeta(1-s).$$

(3) 除了 $s=-2n(n\in N)$ 是 $\zeta(s)$ 的显然零点外，$\zeta(s)$ 的零点都在由 $0<\mathrm{Re}s<1$ 所确定的带形区域内，这些零点有无限多个，并且关于直线 $\mathrm{Re}s=\frac{1}{2}$ 对称地分布. 对于这些零点的分布状况，有下面的猜测：

Riemann 猜测 $\zeta(s)$ 的非显然零点都在直线 $\mathrm{Re}s=\frac{1}{2}$ 上.

这是一个尚未证实或否定的猜测.

习　题

1. 若 $F(n)=\sum_{d|n}f(d)$，则称 $F(n)$ 是 $f(n)$ 的麦比乌斯(Möbius)变换. 证明

$$f(n)=\sum_{d|n}F(d)\mu(\frac{n}{d}).$$

2. 证明：

(1) $\varphi(n)>\frac{1}{2}\sqrt{n}$；

(2) 若 n 是合数，则 $\varphi(n)\leqslant n-\sqrt{n}$.

3. 定义 Mangolt 函数

$$\Lambda(n)=\begin{cases}\log p \text{ 当 } n=p^k(p \text{ 是素数}),k\geqslant 1;\\ 0,\text{其他}.\end{cases}$$

证明 $\log n$ 是 $\Lambda(n)$的 Möbius 变换.

4. 利用调和级数 $\sum\limits_{n=1}^{\infty}\frac{1}{n}$ 的发散性,证明级数 $\sum\limits_{p}\frac{1}{p}$ 发散,此处 $\sum\limits_{p}$ 是对所有素数求和.

5. 在区间$[n,n^2]$中任取一个奇数,试求这个奇数是素数的概率.

6. 设 n 不是完全平方数,并且 $n-n^{\frac{3}{2}}<\varphi(n)<n-1$,证明 n 是两个素数之积.

第五节　同　　余

定义 1　给定正整数 m,若 $m|(a-b)$,则称 a 与 b 对模 m 同余,记为 $a\equiv b(\mathrm{mod}m)$. 此外,若 $|b|\leqslant\frac{m}{2}$,则称 b 是 a 对于模 m 的绝对最小剩余;若 $0\leqslant b<m-1$,则称 b 是 a 对于模 m 的最小非负剩余.

推论　下面的性质是容易证明的:

(1) $a\equiv a(\mathrm{mod}m)$

(2) $a\equiv b(\mathrm{mod}m)$,　$b\equiv c(\mathrm{mod}m)\Rightarrow a\equiv c(\mathrm{mod}m)$;

(3) $c\equiv d(\mathrm{mod}m)$,　$(c,m)=1$,　则 $ac\equiv bd(\mathrm{mod}m)$与 $a\equiv b(\mathrm{mod}m)$等价;

(4) 若 $k\neq 0$,则 $a\equiv b(\mathrm{mod}m)$与 $ak=bk(\mathrm{mod}km)$等价;

(5) 若 $A_i\equiv B_i(\mathrm{mod}m)(0\leqslant i\leqslant k),x\equiv y(\mathrm{mod}m)$,

则 $\sum_{i=0}^{k} A_i x^i \equiv \sum_{i=o}^{k} B_i y^i (\mathrm{mod} m)$

(6) 若 $ac \equiv bc(\mathrm{mod}m), d=(m,c)$，则 $a \equiv b(\mathrm{mod}\ \frac{m}{d})$；

(7) $d \mid m, a \equiv b(\mathrm{mod}m) \Rightarrow a \equiv b(\mathrm{mod}d)$

(8) $a \equiv b(\mathrm{mod}m) \Rightarrow (a,m)=(b,m)$

(9) 若$(m_1,m_2)=1$， $a \equiv b(\mathrm{mod}m_1)$， $a \equiv b(\mathrm{mod}m_2)$，则 $a \equiv b(\mathrm{mod}m_1 m_2)$.

定义 2 对于给定的 $m \in Z$，所有对模 m 同余的整数构成的集合，称为模 m 的剩余类.

一个剩余类若含有与 m 互素的整数(由定义 1 推论中的(8)，它所含的整数都与 m 互素)，则称为模 m 的一个互素剩余类.

由同余的基本性质可知，模 m 有 m 个不相交的剩余类，它们的和集就是全体整数集合 Z. 视每个剩余类为元素，它们所成的集合用 Z/mZ 表示，数 0 所在的剩余类称为它的零元素. 以模 m 的互素剩余类为元素的集合用$(Z/mZ)^*$表示.

定义 3 从模 m 的每个剩余类(互素剩余类)中任取一个数，称这些数的集合是模 m 的一个完全剩余系(简化剩余系).

集合$\{0,1,2,\cdots,m-1\}$称为模 m 的最小非负剩余系. 若模 m 的一个完全剩余系中的每个数的绝对值都不超过$\frac{m}{2}$，则称它为模 m 的绝对最小剩余系.

显然，可把 $Z/mZ((Z/mZ)^*)$与 m 的完全剩余系(简化剩余系)等同看待.

定理 1 m 个整数构成模 m 的一个完全剩余系的充分必要条件，是它们两两不对模 m 同余.

定理 2 $\varphi(m)$个整数构成模 m 的一个简化剩余系的充分

必要条件是它们都与模 m 互素，并且对模 m 两两不同余.

以上两个定理证明略去.

定理 3 设 $m\in N$，k 与 l 是任意整数，$(k,m)=1$，则当 x 通过模 m 的完全剩余系时，$kx+l$ 也通过模 m 的完全剩余系.

证明 由定义 1 的推论中性质(3)，若 $x_1\not\equiv x_2(\mathrm{mod}m)$，则 $kx_1+l\not\equiv kx_2+l(\mathrm{mod}m)$，由此及定理 1 得证. □

定理 4 设 $m\in N$，$k\in Z$，$(k,m)=1$，则当 x 通过模 m 的简化剩余系时，kx 也通过模 m 的简化剩余系.

证明 与定理 3 证明类似(略). □

定理 5 设 $m_1,m_2\in N$，$(m_1,m_2)=1$，则当 x 与 y 分别通过模 m_1 与模 m_2 的完全(简化)剩余系时，m_2x+m_1y 通过模 $m_1m_2=m$ 的完全(简化)剩余系.

证明 以简化剩余系为例.

当 x 与 y 分别通过 $\varphi(m_1)$与 $\varphi(m_2)$个值时，m_2x+m_1y 通过 $\varphi(m_1)\varphi(m_2)=\varphi(m)$个值.

若$(x,m_1)=1$，$(y,m_2)=1$，则由定理 3.3 及定理 3.2 的推论，

$$(m_2x+m_1y,m_1)=(m_2x_1,m_1)=(x,m_1)=1,$$

$$(m_2x+m_1y,m_2)=(m_1y,m_2)=(y,m_2)=1,$$

由此，利用$(m_1,m_2)=1$ 及定义 1 推论中性质(9)，得到$(m_2x+m_1y,m_1m_2)=1$.

这样，剩下的只是要证明，若 $x\not\equiv x'(\mathrm{mod}m_1)$或 $y\not\equiv y'(\mathrm{mod}m_2)$，则 $m_2x+m_1y\not\equiv m_2x'+m_1y'(\mathrm{mod}m_1m_2)$.

事实上，若

$$m_2x+m_1y\equiv m_2x'+m_1y'\quad(\mathrm{mod}m_1m_2),$$

则

$$m_2x\equiv m_2x' \pmod{m_1}.$$

但$(m_1,m_2)=1$，故由定义1的推论得到$x\equiv x'(\mathrm{mod}m_1)$；同理得到$y\equiv y'(\mathrm{mod}m_2)$，这是不可能的. □

定理6 设$m>1, m=p_1^{a_1}\cdots p_k^{a_k}, (a,m)=1$，

则

$$a^{\lambda}\equiv 1 \pmod{m},$$

其中

$$\lambda=[\varphi(p_1{}^{a_1},\cdots\varphi(p_k{}^{a_k})].$$

证明 首先，设$m=p^a$，又设$x_1,\cdots x_{\varphi(p^a)}$是模$p^a$的一个简化剩余系，由定理5，$ax_1,\cdots,ax_{\varphi(p^a)}$也是模$p^a$的一个简化剩余系，因此，

$$x_1x_2\cdots x_{\varphi(p^a)}\equiv ax_1\cdot ax_2\cdots ax_{\varphi(p^a)} \pmod{p^a},$$

即

$$x_1x_2\cdots x_{\varphi(p^a)}\equiv a^{\varphi(p^a)}x_1x_2\cdots x_{\varphi(p^a)} \pmod{p^a}.$$

由上式，利用$(x_1x_2\cdots x_{\varphi(p^a)},p^a)=1$及定义1的推论，推出

$$a^{\varphi(p^a)}\equiv 1 \pmod{p^a}.$$

因此，

$$a^{\varphi(p_i^{a_i})}\equiv 1 \pmod{p_i{}^{a_i}},\quad 1\leqslant i\leqslant k,$$

因为$\varphi(p_i^{a_i})\mid\lambda$，所以

$$a^{\lambda}\equiv 1 \pmod{p_i^{a_i}},\quad 1\leqslant i\leqslant k.$$

再利用上式及性质(9)，得到

$$a^{\lambda}\equiv 1 \pmod{m}.$$ □

推论1 (Fermat) 设p是素数，则对于任何正整数a，$a^p\equiv a \pmod{p}$.

证明 若$(a,p)>1$，则$p\mid a$，结论显然成立.

若$(a,p)=1$，则由定理b知$a^{p-1}\equiv 1(\mathrm{mod}p)$，又因为$p\nmid a$，所以$a^p\equiv a(\mathrm{mod}p)$. □

推论 2(Euler)　设$m>1,(a,m)=1$，则

$$a^{\varphi(m)}\equiv 1 \pmod{m}.$$

推论 3　设$(a,m)=1,n\equiv n_1(\mathrm{mod}\lambda)$，$\lambda$同于定理$b$，则$a^n\equiv a^{n_1} \pmod{m}$.

证明　由假设，存在正整数k，使得$n=n_1+k\lambda$或$n+k\lambda=n_1$. 在这两种情形，都可由定理 6 证得结论. □

定理 7　(i) 对于给定的正整数n,b,m，计算$b^n \bmod m$(即b^n对模m的最小非负剩余)需要$O(\log^2 m\cdot\log n)$次比特运算；

(ii) 若$(b,m)=1$且$\varphi(m)$已知，则(i)中大O项中的$\log n$可用$\log\Delta$代替，其中$\Delta=\min(n,\varphi(m))$.

证明　(i) 使用下面的“重复平方法”计算$b^n \bmod m$. 不妨设$b<m$. 在下面的乘法中，每次都将得到的乘积用它对模m的最小非负剩余代替.

设$n=(n_{k-1}n_{k-2}\cdots n_1n_0)_2=n_0+n_1\cdot 2+\cdots+n_{k-1}\cdot 2^{k-1}$，

则

$$b^n=b^{n_0}\cdot(b^2)^{n_1}\cdot\cdots(b^{2^{k-1}})^{n_{k-1}}.$$

依次计算

$$b^2\equiv b_1,\qquad b^{n_0}b_1^{n_1}\equiv c_1 \pmod{m},$$

$$b_1^2\equiv b_2,\qquad c_1b_2^{n_2}\equiv c_2 \pmod{m},$$

……

$$b_{k-2}^2\equiv b_{k-1},\quad c_{k-2}b_{k-1}^{n_{k-1}}\equiv c_{k-1} \pmod{m},$$

则c_{k-1}即所求，其中b_i和c_i都是对模m的最小非负剩余. 如果某个$n_i=0$，则相应的步骤中只有一个同余式需要计算.

由上可见，计算 $b^n \pmod m$ 需要 $k-1$ 个步骤，在每一步骤中，至多做两次乘法和两次除法，而且进行运算的数 $\leqslant m$，所以总的计算量是 $O(\log^2 m)\cdot O(k)=O(\log^2 m\cdot \log n)$ 次比特运算.

(ii) 由(i)的结论及定理 9 的推论 2 即可得到结论(ii). □

例 1 计算 $3^{19971} \pmod{77}$.

解 由于 $(3,77)=1$，并且 $77=7\cdot 11$，$\varphi(7)=6$，$\varphi(11)=10$，$[\varphi(7),\varphi(11)]=30$，$19971\equiv 21 \pmod{30}$，由此及定理 6 的推论 3，

$$3^{19971}\equiv 3^{21} \pmod{77}.$$

利用重复平方法，由 $21=2^4+0\cdot 2^3+2^2+0\cdot 2+1$，得到

$$3^2\equiv 9, \quad 3^1\cdot 9^0\equiv 3 \pmod{77},$$

$$9^2\equiv 4, \quad 3\cdot 4^1\equiv 12 \pmod{77},$$

$$4^2\equiv 16, \quad 12\cdot 16^0\equiv 12 \pmod{77},$$

$$16^2\equiv 25, \quad 12\cdot 25^1\equiv 69 \pmod{77},$$

即 $3^{19971}\equiv 69 \pmod{77}$.

下面我们要研究形如

$$f(x)\equiv 0 \pmod m \tag{1}$$

的方程，其中 $f(x)$ 是整系数多项式. 由定义 1 推论的性质(5)，若 $x=a$ 是(1)的解，则一切

$$x\equiv a \pmod m$$

都是方程(1)的解. 因此，把 a 所在的模 m 的剩余类看做(1)的一个解. 以下，“有唯一解”，“有两个解”等等，都是按这样的意义.

定理 8 设 $m>0$，则方程

$$ax\equiv b \pmod m \tag{2}$$

有解的充分必要条件是 $(a,m)\mid b$. 若有解，则有 (a,m) 个解.

证明 方程(2)等价于不定方程

$$ax+my=b. \tag{3}$$

由定理 3.6,方程(3)有解的充分必要条件是$(a,m)\mid b$,而且,如果有解(x_0,y_0),则(3)的解(即(2)的解)具有

$$x=x_0+\frac{m}{(a,m)}t,\quad y=y_0-\frac{a}{(a,m)}t,\quad t\in\mathbf{Z}$$

的形式. 容易证明,当 $t=1,2,\cdots,(a,m)$时得到(a,m)个对模 m 互不同余的解,另外的 t 值所对应的 x 值必与这(a,m)个解中的一个对于模 m 同余. □

推论 方程(2)若有解,则有一个解满足

$$0\leqslant x<\frac{m}{(a,m)}.$$

定理 9 设$(a,m)=1$,则

$$x\equiv ba^{\varphi(m)-1} \pmod m$$

是方程(2)的解;若存在整数 r,使 $a\mid b+rm$,则

$$x\equiv\frac{b+rm}{a} \pmod m$$

也是(2)的解.

证明 第一个结论由定理 6 推论 2 得到.

第二个结论可直接验证. □

定义 4 若 $ab\equiv1(\mathrm{mod}\ m)$,则称 b 是 a 的对模 m 的乘法逆元素,或对模 m 的逆元素,或者,在不引起误会的情况下,简称为逆元素,记为 $a^{-1}(\mathrm{mod}\ m)$,或 a^{-1}.

注 以后也使用记号 $a^{-n}=a^{-1}\cdot a^{-1}\cdot a^{-1}\cdots a^{-1}$.

定理 10 若$(a,m)=1$,则 $a^{-1}(\mathrm{mod}\ m)$是存在的,当 $a<m$ 时,它的计算需要 $O(\log^3 m)$次比特运算.

证明 由定理 8 及定理 3.5 的推论得到证明. □

推论 1　若 p 是素数，则 $\boldsymbol{Z}/P\boldsymbol{Z}$ 是一个域.

推论 2　若 $a\equiv b(\mathrm{mod}\ m)$，$c\equiv d(\mathrm{mod}\ m)$，$(c,m)=1$，则 $ac^{-1}\equiv bd^{-1}(\mathrm{mod}\ m)$.

定理 11(孙子定理)　设 $m_1,\cdots,m_r$ 是两两互素的正整数，记 $m=m_1m_2\cdots m_r$，$M_i=m/m_i(1\leqslant i\leqslant r)$，则方程组

$$x\equiv c_i \pmod{m_i},\quad 1\leqslant i\leqslant r \tag{4}$$

对模 m 有唯一解

$$x\equiv\sum_{i=1}^{r}M_i^{-1}M_ic_i \pmod{m}, \tag{5}$$

其中 M_i^{-1} 满足

$$M_i\cdot M_i^{-1}\equiv 1 \pmod{m_i}. \tag{6}$$

证明　由(6)式容易得到

$$M_i\cdot M_i^{-1}\cdot c_i\equiv\begin{cases}c_i & (\mathrm{mod}m_i)\\ 0 & (\mathrm{mod}m_j),\ j\neq i,\end{cases}$$

因此，

$$\sum_{i=1}^{r}M_i^{-1}\cdot M_i\cdot c_i\equiv c_i \pmod{m_i},1\leqslant i\leqslant r.$$

由此及定义 1 推论的性质(9)，可知(5)式所确定的 x 是方程组(4)的解.

再证唯一性. 若 x_1 与 x_2 都满足(4)，则对于任何 i，$1\leqslant i\leqslant r$，都有 $x_1\equiv x_2(\mathrm{mod}\ m_i)$，因此，必是 $x_1\equiv x_2(\mathrm{mod}\ m)$. □

注 1　在定理 11 中，一般地，若有 δ_i $(1\leqslant i\leqslant r)$满足条件

$$\delta_i\equiv 1(\mathrm{mod}\ m_i),\delta_i\equiv 0(\mathrm{mod}\ m_j),\ j\neq i,$$

则 $\sum_{i=1}^{r}\delta_ic_i$ 就是方程组(4)的解.

注 2　设 $0\leqslant c_i<m_i<B(1\leqslant i\leqslant r)$，我们来估计定理 11 中计算(5)中的 x 所需要的时间.

由(5)式,需要计算:(1)$M=m_1m_2\cdots m_r$;(2)$M_i=M/m_i$,$1\leqslant i\leqslant r$;(3)$M_i^{-1}(\mathrm{mod}\ m_i)$,$1\leqslant i\leqslant r$;(4)$a_iM_iM_i^{-1}$,$1\leqslant i\leqslant r$;(5)$x\ (\mathrm{mod}\ M)$.

以$O(\log B)$作为c_i,m_i以及M_i^{-1}的二进制表示的位数的估计,则M_i与M_i的二进制位数可以用$O(r\log B)$估计.

(1) 的计算,可用逐次计算$m_1\cdot m_2$,$m_1m_2\cdot m_3$,$\cdots$,$(m_1\cdots m_{r-1})\cdot m_r$来完成,每次需要$O(r\log B\cdot\log B)$次比特运算,共需要$O(r^2\log^2 B)$次比特运算.

(2) 的计算,需要$r\cdot O(r\log B\cdot\log B)=O(r^2\log^2 B)$次比特运算.

(3) 的运算可分两步:第一步,用除法求出M_i对模m_i的最小非负剩余M_i^0,这需要$O(r\log^2 B)$次比特运算;第二步,计算$(M_i^0)^{-1}(\mathrm{mod}\ m_i)$(即$M_i^{-1}(\mathrm{mod}\ m_i)$),这需要$O(\log^3 B)$次比特运算,这样,(3)的计算共需要$r\cdot O(r\log^2 B+\log^3 B)=O(r\log^2 B(r+\log B))$次比特运算.

(4) 的计算,需要$O(r^2\log^2 B)$次比特运算.

(5) 的计算,需要$O(r^2\log^2 B)$次比特运算.

综合以上,总共需要$O(r\log^2 B(r+\log B))$次比特运算.

例 2 求解方程组

$$\begin{aligned} x&\equiv 2 \pmod 3\\ x&\equiv 3 \pmod 5\\ x&\equiv 4 \pmod 7. \end{aligned}$$

解 沿用定理 11 中的记号,容易计算

$m=105$, $M_1=35$, $M_2=21$, $M_3=15$,

$M_1^{-1}=2$, $M_2^{-1}=1$, $M_3^{-1}=1$,

$x\equiv 2\cdot 35\cdot 2+1\cdot 21\cdot 3+1\cdot 15\cdot 4\equiv 53 \pmod{105}$.

下面，是本节定理在分解因数问题中的简单应用.

引理 1　设$(b,m)=1$，a 和 c 是正整数. 若 $b^a\equiv 1(\mathrm{mod}\ m)$且 $b^c\equiv 1(\mathrm{mod}\ m)$，则 $b^d\equiv 1(\mathrm{mod}\ m)$，此处 $d=(a,c)$.

证明　利用 Euclid 算法可求出 x,y，使得 $ax+cy_1=d$. 显然 $xy_1<0$，故不妨设 $x>0$，　$y_1<0$. 记 $y=-y_1$，则 $ax=d+cy$，因此，

$$b^{ax}=b^{d+cy}.$$

由假设条件，得到

$$1\equiv b^{ax}=b^{d+cy}\equiv b^d(\mathrm{mod}\ m).$$　□

定理 12　设 p 是素数，$p\mid(b^n-1)$，则下述结论必有一个成立：

(i) 对于 n 的某个真因数 d，$p\mid(b^d-1)$；

(ii) $p\equiv 1(\mathrm{mod}\ n)$；若 p 和 n 都是奇数，则 $p\equiv 1(\mathrm{mod}\ 2n)$.

证明　由假设，$b^n\equiv 1(\mathrm{mod}\ p)$，又由 Fermat 定理，$b^{p-1}\equiv 1(\mathrm{mod}p)$，因此，由引理 2 得到 $b^d\equiv 1(\mathrm{mod}\ p)$，其中 $d=(n,p-1)$. 若 $d<n$，则结论(i)成立；若 $d=n$，则 $n=d\mid p-1$，结论(ii)成立. 若 p 与 n 都是奇数，则由 $p\equiv 1(\mathrm{mod}\ n)$显然可推出 $p\equiv 1(\mathrm{mod}\ 2n)$.　□

例 3　将 $3^{15}-1=14348906$ 分解为素因数之积.

解　由定理 12，首先从 3^3-1 与 3^5-1 中寻找 $3^{15}-1$ 的素因数：$3^3-1=26=2\cdot 13$，　$3^5-1=242=2\cdot 11^2$，所以，$2\cdot 13\cdot 11^2$ 是 $3^{15}-1$ 的因数，$3^{15}-1=2\cdot 11^2\cdot 13\cdot 4561$.　$3^{15}-1$ 的另外的素因数 p 应满足 $p\equiv 1(\mathrm{mod}2\cdot 15)$，即 $p=30k+1$，$(k=1,2,\cdots)$. 另一方面，若 4561 是合数，则它至少有一个素因素$\leqslant\sqrt{4561}<70$. 检验从 31 到 70 的素数是否整除 4561 之后，可知 4561 是素数，因此，$3^{15}-1=14348906=2\cdot 11^2\cdot 13\cdot 4561$.

引理 2　设 $(b,m)=1$，$m>2$，a 和 c 是正整数，并且 $b^a\equiv -1(\mathrm{mod}\ m)$，$b^c\equiv\pm 1(\mathrm{mod}\ m)$，则 $\frac{a}{d}$ 是奇数，且 $b^d\equiv -1(\mathrm{mod}\ m)$，此处 $d=(a,c)$.

证明　类似于引理 2 的证明可以推出 $b^d=\pm 1(\mathrm{mod}\ m)$. 但是 $b^a=b^{\frac{a}{d}\cdot d}\equiv -1(\mathrm{mod}\ m)$，所以 $b^d\equiv -1(\mathrm{mod}\ m)$，并且 $\frac{a}{d}$ 是奇数. □

定理 13　设 p 是素数，$p|(b^n+1)$，则下述结论之一成立：

(i) 对于 n 的某个真因数 d，$p|b^d+1$ 并且 $\frac{n}{d}$ 是奇数；

(ii) $p\equiv 1 \pmod{2n}$.

证明　由 Fermat 定理，$b^{p-1}\equiv 1(\mathrm{mod}\ p)$，所以 $b^{\frac{p-1}{2}}\equiv\pm 1(\mathrm{mod}\ p)$，因此，由引理 2，$b^d\equiv -1(\mathrm{mod}\ p)$，此处 $d=\left(n,\frac{p-1}{2}\right)$，$\frac{n}{d}$ 是奇数.

若 $d<n$，则结论(i)成立；

若 $d=n$，则 $n\left|\frac{p-1}{2}\right.$，结论(ii)成立. □

例 4　若 $n>1$ 且 a^{n-1} 是素数，则 $a=2$，并且 n 是素数.

解　若 $a>2$，则由 $(a-1)|(a^n-1)$ 可知 a^n-1 非素数.

若 $a=2$，$n=pq$，$p>1$，$q>1$，则由 $(2^p-1)|(2^n-1)$ 可知 2^n-1 非素数.

例 5　若 2^m+1 是素数，则 $m=2^k$.

解　设 $m=ql$，q 是大于 1 且小于 m 的奇数，则由 $2^{ql}+1=(2^l+1)(2^{l(q-1)}-2^{l(q-2)}+\cdots+1)$ 可知 2^m+1 非素数.

注　形如 2^n-1 的素数，称为 Mersenne 素数；形如 $2^{2^n}+1$ 的素数，称为 Fermat 素数.

定义 5 设 $f(x)=\sum_{i=0}^{n}a_ix^i$ 与 $g(x)=\sum_{i=0}^{n}b_ix^i$ 是两个整系数多项式，$a_i\equiv b_i(\mathrm{mod}\ m)$，$0\leqslant i\leqslant n$，则称 $f(x)$与 $g(x)$对模 n 同余，记为 $f(x)=g(x),(\mathrm{mod}\ m)$，

引理 3 在方程式(1)中，设 $m=p$ 是素数，$f(x)=a_nx^n+\cdots+a_0$，$a_n\not\equiv 0(\mathrm{mod}\ p)$，又设 $\alpha_1,\cdots,\alpha_k$ 是方程(1)的 k 个不同的解，则对任何整数 x，

$$f(x)\equiv(x-\alpha_1)\cdots(x-\alpha_k)g(x)\quad(\mathrm{mod}\ p)\tag{7}$$

其中 $g(x)=a_nx^{n-k}+\cdots$是一个多项式.

证明 由多项式带余数除法，

$$f(x)=(x-\alpha_1)g_1(x)+r,$$

其中 $g_1(x)$是首项系数为 a_n 的 $n-1$ 次多项式，r 是常数. 由 $f(\alpha_1)\equiv 0(\mathrm{mod}\ p)$，推出 $r\equiv 0(\mathrm{mod}\ p)$. 因此，对任意的整数 x，有

$$f(x)\equiv(x-\alpha_1)g_1(x)\quad(\mathrm{mod}\ p).$$

令 $x=\alpha_i$ $(2\leqslant i\leqslant k)$，则由 $\alpha_i\not\equiv\alpha_1(\mathrm{mod}\ p)$，以及

$$0\equiv f(\alpha_i)\equiv(\alpha_i-\alpha_1)g_1(\alpha_i)\quad(\mathrm{mod}\ p),$$

利用$(p,\alpha_i-\alpha_1)=1$，得到

$$g_1(\alpha_i)\equiv 0\quad(\mathrm{mod}\ p),\qquad 2\leqslant i\leqslant k.$$

利用归纳法容易证明引理. □

定理 14 设 $f(x)=a_nx^n+\cdots+a_0$，$a_n\not\equiv 0\pmod p$，p 是素数，则方程 $f(x)\equiv 0(\mathrm{mod}\ p)$的解的个数$\leqslant n$.

证明 若所述方程有 $n+1$ 个对模 p 的不同的解 $\alpha_1,\cdots,\alpha_{n+1}$，则由引理 1 得到

$$f(x)\equiv a_n(x-\alpha_1)\cdots(x-\alpha_n)\quad(\mathrm{mod}\ p),$$

$$0\equiv f(\alpha_{n+1})\equiv a_n(\alpha_{n+1}-\alpha_1)\cdots(\alpha_{n+1}-\alpha_n)\quad(\mathrm{mod}\ p).\tag{8}$$

后一同余式是不可能的，因为 $\alpha_{n+1}\not\equiv\alpha_i \pmod{p}$，$1\leqslant i\leqslant n$，同时 $a_n\not\equiv 0 \pmod{p}$. □

定理 15 设 $\alpha>1$，又设 a 是方程

$$f(x)\equiv 0 \pmod{p^{\alpha-1}} \tag{9}$$

的一个解，此处 $f(x)$ 是整系数多项式，则方程

$$f(x)\equiv 0 \pmod{p^{\alpha}} \tag{10}$$

的所有满足条件 $x\equiv a \pmod{p^{\alpha-1}}$，并且对模 p^{α} 两两不同余的解为：

(i) 若 $f'(a)\not\equiv 0 \pmod{p}$，则有一个解

$$x\equiv a+kp^{\alpha-1} \pmod{p^{\alpha}},$$

其中 k 满足 $kf'(a)\equiv -f(a)p^{1-\alpha} \pmod{p}$；

(ii) 若 $f'(a)\equiv 0 \pmod{p}$，且 $f(a)\not\equiv 0 \pmod{p^{\alpha}}$，则无解；

(iii) 若 $f'(a)\equiv 0 \pmod{p}$，且 $f(a)\equiv 0 \pmod{p^{\alpha}}$，则有 p 个解：

$$x\equiv a+kp^{\alpha-1} \pmod{p^{\alpha}},\ 0\leqslant k\leqslant p-1.$$

证明 设 $x=a+kp^{\alpha-1}$ 是(10)的解，则

$$f(x)=f(a+kp^{\alpha-1})=f(a)+f'(a)kp^{\alpha-1}+\frac{f''(a)}{2!}k^2p^{2\alpha-2}+\cdots,$$

由于 $\alpha>1$，$2\alpha-2\geqslant\alpha$，所以

$$f(x)\equiv f(a)+f'(a)kp^{\alpha-1} \pmod{p^{\alpha}}. \tag{11}$$

由此可见，求解 x 等价于求解关于 k 的方程

$$f(a)+f'(a)kp^{\alpha-1}\equiv 0 \pmod{p^{\alpha}}, \tag{12}$$

由此容易得出定理结论. □

推论 若 $f(x)\equiv 0 \pmod{p}$ 与 $f'(x)\equiv 0 \pmod{p}$ 无公共解，则 $f(x)\equiv 0 \pmod{p^{\alpha}}$ 与 $f(x)\equiv 0 \pmod{p}$ 的解的个数相同.

习　题

1. 解方程

(i) $3x\equiv 4 \pmod{121}$;

(ii) $5x^2\equiv 1 \pmod{7^3}$.

2. 证明：十进制数 n 能被 9 整除的充分必要条件是它的各个位数码之和能被 9 整除.

3. 设素数 $p>2$，$m=p^\alpha$ 或 $m=2p^\alpha$，证明：若 $x^2\equiv 1 \pmod{m}$，则 $x\equiv \pm 1 \pmod{m}$ 成立.

4. 设奇数 m 是 k 个不同的素数之积，证明方程 $x^2\equiv 1 \pmod{m}$ 有 2^k 个解.

5. 设 p 是素数，则

$$(p-1)!\equiv -1 \pmod{p}.$$

6. 求方程组

$x\equiv 2 \pmod{3}$，$x\equiv 5 \pmod{7}$ 的最小正整数解.

7. 求　$27^{13} \pmod{37}$.

8. 将　$2^{11}-1=2047$ 分解为素因数之积.

第二章　传统密码学

密码的应用，有悠长的历史，在古代的战争中，人们就已经使用秘密通信方法，例如，古罗马皇帝凯撒所使用的、现在称为“凯撒密码”的，就是其中一例. 随着科学技术的进步，密码学也经历了一个由简单到复杂，由低级到高级的发展过程.

在本章中，主要介绍传统密码学(或称单钥密码学).

第一节　仿射加密方法

在现实生活中，有时由于某种原因(例如，在战争中)，要将一个信息(例如，发动一个战役的时间和部署)传送给一方而不被任何另外的第三者获知，为此常需要将信息以伪装形式传送，然后由合法接收者从中识别出(译出)真实信息. 这样，总的说来，密码学的研究有两个方面：第一，密码编制：研究编制信息的安全的(不易被破译的)伪装形式的方法，既要使合法接收者容易识别密码的真实含义，又要防止非法接收到密码的人从密码中获得这些信息；第二，密码分析：在获得某个密码后，对之进行分析，了解它所传送的真实内容.

定义 1　要传送的信息，称为明文；信息的伪装形式，称为密文；将明文转换为密文的过程，称为加密过程，或加密；合法接收者将密文恢复为它所表示的明文的过程，称为解密过程，或解密.

通常，明文或密文是用某些固定的符号组成，例如，可以是拉丁字母 $a,b,\cdots$，标点符号“，”、“？”、“！”，空格符号“　”，或其他另外的符号. 称这些符号的集合为符号表.

在加密时，又常将明文分成若干个单元(或称段节)，每个单元含有个数相同的符号，然后对每个单元实施加密过程，称这些单元为明文单元；相应地，有密文单元；它们统称为信息单元. 每个信息单元所含符号的个数，称为它的长度. 在将信息分成单元时，可能有一个单元所含符号的个数少于其他单元中的符号个数. 此时，一般地，可以补加几个符号，使这个单元与其他单元有相同的符号个数. 但要注意，补加的符号不应使原文的含义变化，也不应影响加密系统的安全性，即不减弱破译密文的困难程度.

以后，在不致引起误会的情况下，在叙述上将不区别信息与信息单元.

定义 2　以 $\mathscr{P}$ 和 $\mathscr{C}$ 表示所有明文单元和密文单元的集合，分别称为明文单元空间(或明文空间)和密文单元空间(或密文空间). 设 f 是集合 $\mathscr{P}$ 到 $\mathscr{C}$ 上的 1—1 映射，则称 f 是一个加密方法，或加密函数，或加密映射，或密码编制方法.

一般地，一个加密方法包括加密算法与加密钥两部分. 加密算法由公式或计算程序等运算法则组成，是相对稳定的，通常是公开的. 加密钥，是算法中的参数，它是相对不稳定的，经常变的，是保密的，所有供使用的密钥所成的集合，称为密钥空间.

注　通常，将加密方法用 $f_k(p)$ 表示，$p\in\mathscr{P}$，其中 k 表示一个与加密钥有关的参量.

定义 3　利用已知的关于部分密文、部分明文、以及它们之间某种联系的知识，将密文单元还原为明文单元的过程，称为密

码分析，或称破译.

一般地，密码分析是指非法接收者在不掌握解密方法，或不掌握解密钥时，从密文得到相应的明文的过程.

对于加密方法 f_k，它的逆映射 f_k^{-1} 即是解密方法，由于 f_k 是1—1 映射，所以 f_k^{-1} 是存在的，也是 1—1 映射，并且 $f_k^{-1}(f_k(p))=P$. 一般地，f_k^{-1} 也含有一个与密钥有关的信息 k'，称为解密钥. 所有解密钥的集合，称为解密钥空间.

定义 4 密码系统由明文空间，密文空间，加密钥空间，解密钥空间，加密方法，以及解密方法构成.

当前，密码系统主要分传统密码系统与公开钥密码系统两大类. 前者的特点是，由 f_k 容易求出 f_k^{-1}，这包括已知加密钥容易求出解密钥. 因此，加密钥的保护与解密钥的保护是同等重要的，这也是传统密码学有别于公开钥密码学的本质特征. 正因如此，传统密码在使用中须在加解密双方之间建立一个传送密钥的秘密通道.

本章主要研究传统密码系统. 在第四章将介绍公开钥密码系统.

图 1 说明了传统密码系统的编制和密码分析的关系与过程.

对于密码系统的评价，显然应该以它所编制的密文能否易被破译为主要标准. 事实上，一个密码系统应该能够满足以下条件：第一，由明文 P，求出密文 $E=f_R(p)$ 在计算上是容易的；第二，知道密钥后，由密文 E 求出明文 P 在计算上是容易的；第三，不知道解密钥时，由密文 E 求出明文 P 是不可能的，或者，至少在计算上是困难的. 此处的第三个条件，是对密码系统安全性的要求.

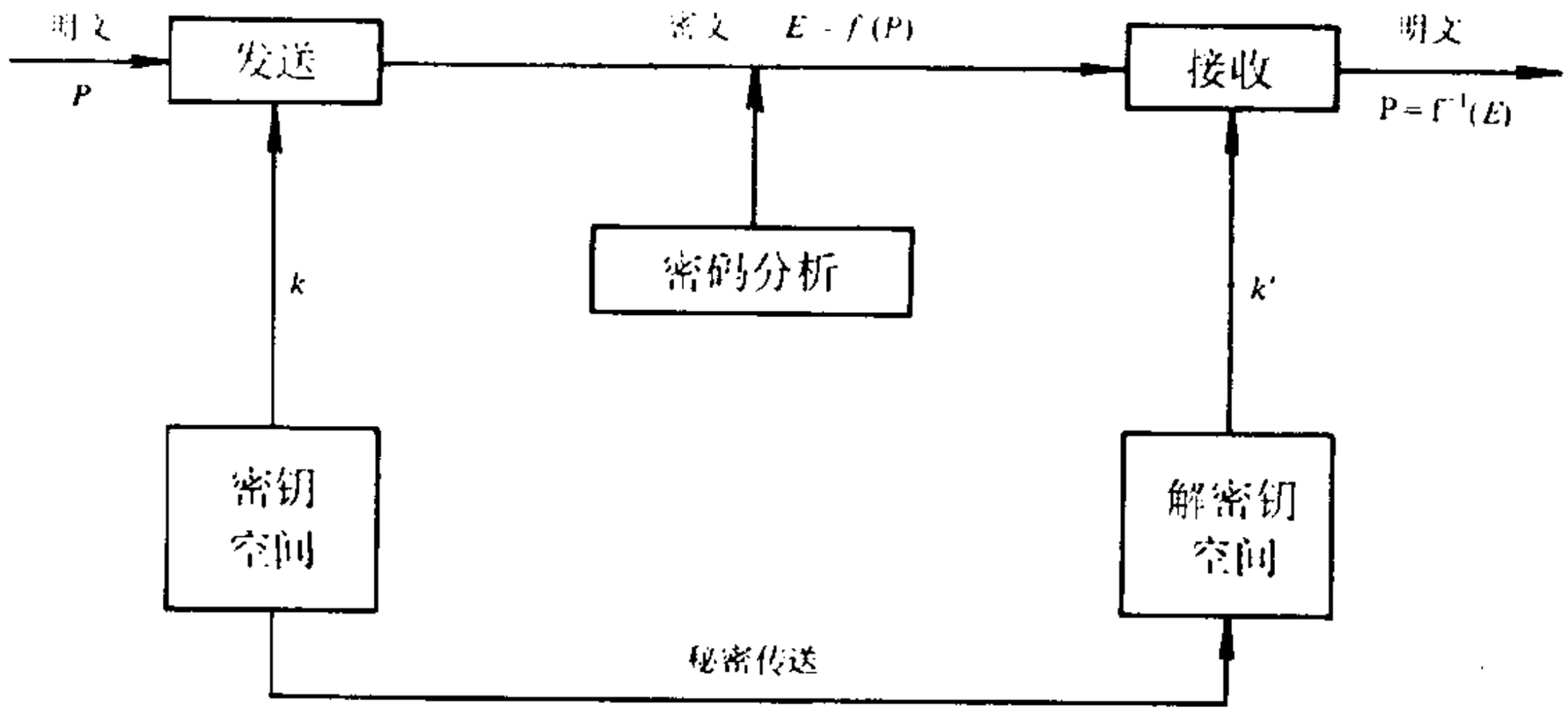


图 1　传统密码的编制、传送与分析

需要指出，所谓密码系统的安全性，主要是指密文“实际上不可破译”，即，在明文需要保密的某个时间范围内，“非法”接收到密文的人不能从密文得到明文.

在理论上，完全保密的密码系统，或不可破译的密码系统是存在的. 使用这样的系统时，对于“非法”接收到密文的人来说，得到密文无助于他去确定相应的明文. 但是在实际应用中，这样的密码系统有许多技术上的困难，因而很少被采用. 关于完全保密的密码系统，将在以后讨论.

为了使用数学手段实现对密码系统的研究，需要将信息单元与数学符号建立联系. 这有不同的方式. 例如，可以用数字表示信息单元，也可以用矩阵，用向量，用曲线上的点，或其他数学符号表示信息单元.

现在，我们说明如何用整数或 Z/mZ（m 是正整数）中的元素表示信息单元.

如前所述，信息单元由构成信息的符号组成，这些符号取自符号表. 设这个符号表含有 N 个符号，那么，可以将它们分别与

整数 0,1,…,N-1 建立一一对应关系,今后,在谈到符号表时,常是同时确定了这样一种对应关系.例如,若符号表由 26 个英文字母 $a,b,c,\cdots,x,y,z$,标点符号“!”、“?”以及“ ”(空格)组成,那么,可取 $N=29$,并做以下对应:

$a\to 0$, $b\to 1$, …, $y\to 24$, $z\to 25$,

!→26, ?→27, “ ” →28 (空格与 28 对应)

若信息单元 p 含有符号 $p_0,\cdots,p_{k-1}$,则记为 $p=(p_0,p_1,\cdots,p_{k-1})$.我们也用 p_i 表示它所对应的整数,即 $0\leqslant p_i\leqslant N-1(1\leqslant i\leqslant k)$,一般地,这不会造成混乱.用

$$p\to p_0N^{k-1}+p_1N^{k-2}+\cdots+p_{k-2}N+p_{k-1} \tag{1}$$

建立信息单元空间与整数集合$\{0,1,\cdots,N^{R-1}\}$之间的对应,显然这是一个一一对应关系.

例 1 设使用符号 $a,b,c,\cdots,x,y,z$ 以及空格“ ”,编写明文 *YOU PAY ME*.分别在

(i) 信息单元含一个符号,

(ii) 信息单元含二个符号

这两种情形,写出与明文对应的整数串.

解 使 $a,b,\cdots,y,z$ 分别与 0,1,…,24,25 对应,使空格与 26 对应.

(i) 信息单元含一个符号时,明文对应的整数串是

YOU PAY ME→24,14,20,26,15,0,24,26,12,4.

(ii) 信息单元含二个符号时,先将明文分成长度为 2 的几个单元,即

$$\underline{YO}\ \underline{U\_}\ \underline{PA}\ \underline{Y\_}\ \underline{ME},$$

利用(1)式求出每个单元所对应的整数:

$$YO\to 24\cdot 27+14=662,$$

$$U \rightarrow 20 \cdot 27+26=566,$$

$$PA \rightarrow 15 \cdot 27+0=405,$$

$$Y \rightarrow 24 \cdot 27+26=674,$$

$$ME \rightarrow 12 \cdot 27+4=328,$$

因此，

$$YOU \quad PAY \quad ME \rightarrow 662,566,405,674,328.$$

例 2 仍使用例 1 中的符号表及符号与整数的对应关系. 已知某信息对应的整数串是 17894,19359,18210,3644，并且每个信息单元含有三个符号，试求出信息原文.

解 由(1)式见到，$p_0,\cdots,p_k$ 就是与信息单元所对应的整数的 N 进制表示中的位数码. 因此，由

$$17894=24 \cdot 27^2+14 \cdot 27+20$$

可知

$$17894 \rightarrow 241420 \rightarrow YOU.$$

同样地，由

$$19359=26 \cdot 27^2+15 \cdot 27+0,$$

$$18210=24 \cdot 27^2+26 \cdot 27+12,$$

$$3644=4 \cdot 27^2+26 \cdot 27+26,$$

得到

$$19359 \rightarrow 26 \quad 15 \quad 0 \rightarrow \quad PA$$

$$18210 \rightarrow 24 \quad 26 \quad 12 \rightarrow Y \quad M,$$

$$3644 \rightarrow 4 \quad 26 \quad 26 \rightarrow E,$$

这样，整个原文是 *YOU PAY ME*.（在字母 E 的后面，有两个空格，这是当初将明文分成长度为 3 的单元时，在最后一个单元中加进去的，用以使这个单元的长度是 3).

今后，在谈到信息单元时，除特别声明外，都是指它所对应

的整数(或 Z/mZ 中的元素),这意味着,已经给定了一个符号表,以及有了信息单元空间与某个整数集合之间的一一对应.此时,一个将明文转换成密文的加密变换(加密算法),就是在这个数字集合上所定义的映射了.

以 P 和 E 分别表示长度为 k 的明文单元和密文单元,也用它们表示相应的在 0 与 N^{k-1} 之间的整数.

定义 5 设 $(a,N)=1$,由

$$E\equiv aP+b \pmod{N^k} \tag{2}$$

确定的加密方法,称为仿射加密方法,其中 b 是整数,$0\leqslant b<N^k$,E 是 $ap+b$ 对于模 N^k 的最小非负剩余.

由此定义,若已知密文 E,则可由

$$P\equiv a^{-1}(E-b) \pmod{N^k} \tag{3}$$

求出明文 P,其中 $a^{-1}\cdot a\equiv 1(\mathrm{mod}N^k)$,$P$ 是 $a^{-1}(E-b)$ 对于模 N^R 的最小非负剩余.

例 3 设符号 $a,b,\cdots,y,z$,分别与整数 $0,1,\cdots,24,25$ 对应.在定义5 中取 $a=1,b=3$,就得到所谓"凯撒密码":

$$E\equiv P+3 \pmod{26}.$$

据此,明文 YES 对应的密文是:

$$YES\rightarrow 24\ \ 4\ \ 18\rightarrow 1\ \ 7\ \ 21\rightarrow BHV.$$

例 4 已知明文单元与密文单元的长度都是 1(即只含一个符号),并且符号表是 26 个英文字母 $a,b,\cdots,y,z$ 组成的,它们分别与 $0,1,\cdots,24,25$ 对应.已知使用公式

$$E\equiv p+b \pmod{26},\quad 0\leqslant E,b<26$$

加密.若已知明文字母 e 与密文字母 u 对应,试求出解密方法.

解 由 $e\rightarrow 4$,$u\rightarrow 20$,以及已知的对应关系,可知

$$20\equiv 4+b \pmod{26},$$

因此 $b=16$. 所以，解密公式为

$$P\equiv E-16 \pmod{26},\quad 0\leqslant p<26.$$

一般地，对于由(2)式定义的仿射加密方法，只要知道两对(不同的)相对应的明文单元和密文单元 P_1,E_1，与 P_2,E_2：$P_1\to E_1, P_2\to E_2$，就可以求出解密方法，事实上，由(2)式及已知的对应关系，

$$E_1\equiv aP_1+b \pmod{N^k},$$

$$E_2\equiv aP_2+b \pmod{N^k}$$

所以

$$E_2-E_1\equiv a(P_2-P_1) \pmod{N^k}.$$

以 $P_i^{-1}(1\leqslant i\leqslant l)$ 表示同余方程

$$x(P_2-P_1)\equiv 1 \pmod{N^k}$$

的全部解，并且，对于 $1\leqslant i\leqslant l$，记

$$a_i\equiv P_i^{-1}(E_2-E_1) \pmod{N^k},\quad 0\leqslant a_i\leqslant N^k,$$

与

$$b_i\equiv E_1-a_iP_1 \pmod{N^k},\quad 0\leqslant b_i<N^k,$$

则 a_i 与 $b_i(1\leqslant i\leqslant l)$ 就可能是(2)式中所使用的 a 和 b. 当 $(P_2-P_1,N^k)=1$ 时，这样的 a_i 与 b_i 只有一组. 当 $(P_2-P_1,N^k)=l>1$ 时，为了确定出正确的 a 与 b，首先，利用定义 5 中的条件 $(a,N)=1$ 删去某些 a_i 与 b_i，其次，可试译部分密文，用以判定出正确的 a 与 b. 将确定了的 a,b 代入(3)式，就得到解密公式.

在现实生活中，无论使用什么语言符号传送信息，各个信息单元的出现频率总是有差别的. 例如，在英语的 26 个字母中，出现频率较高的是 e,t,a,o,n 等，较低的是 z,q,j,x,k 等. 若以两个或多个字母(或其他符号)构成单元，经过大量的统计分析

之后，仍可发现各个单元出现频率的差别．这样，密码分析人员就可以利用统计手段，通过比较明文单元和密文单元的出现频率，猜出两对(或几对)互相对应的信息单元，从而利用上面的方法得到解密公式．因此，仿射加密系统是不安全的．但是，它具有加密与解密速度快的优点．

例 5　已知信息单元含一个符号，并且符号表由 26 个英文字母 $a,b,\cdots,y,z$(分别与 0,1,…,24,25 对应)，空格“　”(与 26 对应)，以及“?”(与 27 对应)组成．此外，已知密文中出现频率最高的三个符号依次是 B,? 与 I，而且，在用这 28 个符号写成的正常英文中，出现频率最高的依次是空格，E 与 T，试求解密公式．

解　设解密公式为

$$P\equiv a'E+b' \pmod{28},\quad 0\leqslant P<28,$$

则由已知的符号与数字的对应关系，比较出现频率的高低，可以假定空格与 E 分别对应着“B”与“?”，于是

$$26\equiv a'\cdot 1+b' \pmod{28},.$$

$$4\equiv a'\cdot 27+b' \pmod{28}.$$

将两式相减，得到

$$26a'\equiv -22\equiv 6 \pmod{28}.$$

这个同余方程有两个解；　$a'_1\equiv 11\pmod{28}$，$a'_2\equiv 25\pmod{28}$，相应地，有 $b'_1\equiv 15\pmod{28}$，$b'_2\equiv 1\pmod{28}$．

这样，得到了两个可能的解密方法：

(i)　$P\equiv 11E+15 \pmod{28}$，

(ii)　$P\equiv 25E+1 \pmod{28}$．

再通过比较出现频率，又可假定 I 与 T 对应(它们对应的数字分别是 8 与 19)，并分别代入(i)与(ii)进行验证，可知解密

方法(i)是正确的.

例 6 已知信息单元含两个符号,它们取自例 1 中的符号表.在统计分析之后发现,密文中出现频率最高的信息单元依次是 *za*,*ia*,与 *iw*.已知在正常英文中出现频率最高的信息单元依次是 *e* (即 *e* 与空格),*s* 与 *t*.试求出所使用的仿射加密方法的解密公式.

解 通过比较出现频率,可以假定密文单元 *za*,*ia* 与 *iw* 分别与明文单元 *e* ,*s* 与 *t* 对应,即

$$675\to 134,\quad 216\to 512,\quad 238\to 721.$$

设解密公式为

$$P\equiv a'E+b' \pmod{27^2},\quad 0\leqslant P<27^2=729,$$

则由三对对应关系得到

$$134\equiv 675a'+b' \pmod{729}, \tag{4}$$

$$512\equiv 216a'+b' \pmod{729}, \tag{5}$$

$$721\equiv 238a'+b' \pmod{729}. \tag{6}$$

将(4)式与(6)式相减,得到

$$437a'\equiv 142 \pmod{729},$$

因此,$a'\equiv 374 \pmod{729}$,$a'=374$.代入(4)式,得到 $b'\equiv 647 \pmod{729}$,$b'=647$.所求的解密公式是

$$P\equiv 374E+647 \pmod{729},\quad 0\leqslant P<729.$$

注 1 一般说来,由(4)、(5)、(6)三个方程中的任何两个都可以确定 a' 与 b' 可能取的值(不一定像利用(4)和(6)那样,只有一组解).如果将(4)式与(5)式相减,就得到

$$459a'\equiv 351 \pmod{729},$$

由于(459,729)=27,所以这个同余方程对于模 729 有 27 个不同的解,于是,得到 27 组可能的 a' 与 b' 的值.为了确定出正确

的一组，需要像在例 5 中那样进行验证，这造成一些技术上的困难. 因此，要尽量减少需要验证的解的个数.

注 2　例 6 中的方法，原则上对于处理信息单元长度为 k 时的仿射加密系统也是有效的，不过，那时需要知道长度为 k 的信息单元的出现频率. 此外，下面的分析也有助于寻求解密公式.

设明文单元与密文单元分别是 $P_0=(p_0,\cdots,p_{k-1})$ 与 $E_0=(e_0,\cdots,e_{k-1})$，其中 $0\leqslant p_i,e_i<N(0\leqslant i\leqslant k-1)$. 为了寻求使

$$P\equiv a'E+b' \pmod{N^k}$$

成立的 a' 与 b'，将 p_0 与 E_0 代入上式，得到

$$\begin{aligned} &p_0N^{k-1}+p_1N^{k-2}+\cdots+p_{k-1}\\ \equiv&a'(e_0N^{k-1}+e_1N^{k-2}+\cdots+e_{k-1}) \pmod{N^k} \end{aligned}$$

于是

$$p_{k-1}\equiv a'e_{k-1} \pmod{N},$$

这给出了确定 a' 的一条途径. 注意，由上式所确定的 a'（即使对于模 N 只有一个）并不是全部可能的 a' 值.

习　题

1. 使用例 1 中的符号表，及仿射加密公式

$$E\equiv 4P+3 \pmod{27},$$

将明文“*I　AM　GOING　OUT*”译成密文.

2. 使用例 1 中的符号表，及仿射加密公式

$$E\equiv 5P+7 \pmod{729},$$

假设信息单元长度为 2，将明文“*IT　IS　A　BOOK*”译成密文.

3. 已知信息单元长度为 2，符号表含 29 个符号：英文字母

$a,b,\cdots,y,z$，空格，?，! 以及 :. 又已知密文单元中出现频率最高的依次是 M ，U ，以及 IH. 利用例 6 中的已知条件，求出密文“$DXM\ \ SCE\ \ DC\ CUVGX$”的含义.

4. 利用上题的加密方法，将明文“$HELP\ \ ME$”译成密文.

第二节 矩阵加密方法

在上一节中，当使用含有 N 个不同符号的符号表时，将长度为 k 的信息单元的集合与整数集合$\{0,1,\cdots,N^k-1\}$建立了一一对应关系. 在本节中，给出这个信息单元集合的另一种对应关系，并且研究矩阵加密方法.

在本节中，主要研究 $k=2$ 的情形. 对于每个符号(例如 a，$b,x,y,\cdots$)，在用它表示符号本身的同时，也表示它所对应的数字.

设 $m\times n$ 矩阵 $\boldsymbol{A}=(a_{ij})_{i,j}(1\leqslant i\leqslant m,1\leqslant j\leqslant n)$的元素 a_{ij}都是整数，则称 $\boldsymbol{A}$ 是整数矩阵，或简称为矩阵。$m\times 1$ 矩阵 $\begin{pmatrix}a_1\\ \vdots\\ a_m\end{pmatrix}$ 也称为 m 维整数向量，或简称为 m 维向量。

定义 1 设 $N>1$ 是正整数，$\boldsymbol{A}=(a_{ij})_{i,j}$与 $\boldsymbol{B}=(b_{ij})_{i,j}$都是 $m\times n$整数矩阵，若

$$a_{ij}\equiv b_{ij}(\mathrm{mod}N),1\leqslant i\leqslant m,1\leqslant j\leqslant n, \tag{1}$$

则称矩阵 $\boldsymbol{A}$ 与 $\boldsymbol{B}$ 对模 N 同余，记为 $\boldsymbol{A}\equiv\boldsymbol{B}(\mathrm{mod}N)$.

在定义 1 的基础上，与同余整数类似地，可以推导出同余矩阵的性质，例如：

(i) 若 $\boldsymbol{A}\equiv\boldsymbol{B},\boldsymbol{B}\equiv\boldsymbol{C}(\mathrm{mod}N)$，则 $\boldsymbol{A}\equiv\boldsymbol{C}(\mathrm{mod}N)$；

(ii) 若 $\boldsymbol{A}\equiv\boldsymbol{B},\boldsymbol{C}\equiv\boldsymbol{D}(\mathrm{mod}N)$，则 $\boldsymbol{A}+\boldsymbol{C}\equiv\boldsymbol{B}+\boldsymbol{D}(\mathrm{mod}N)$；

(iii) 若 $a\in\boldsymbol{Z},\boldsymbol{A}\equiv\boldsymbol{B}(\mathrm{mod}N)$，则 $a\boldsymbol{A}\equiv a\boldsymbol{B}(\mathrm{mod}N)$；

(iv) 若 $\boldsymbol{A}$ 和 $\boldsymbol{B}$ 是 $m\times n$ 整数矩阵，$\boldsymbol{C}$ 和 $\boldsymbol{D}$ 分别是 $n\times p$ 和 $p\times m$ 整数矩阵，并且 $\boldsymbol{A}\equiv\boldsymbol{B}(\mathrm{mod}N)$，则 $\boldsymbol{AC}\equiv\boldsymbol{BC},\boldsymbol{DA}\equiv\boldsymbol{DB}(\mathrm{mod}N)$.

由定义 1 及同类整数矩阵的性质，可以将所有整数矩阵对模 N 分类，每一类中的矩阵对于模 N 是互相同余的. 称这些矩阵类为模 N 的同余矩阵类，并且把属于同一类的矩阵看成是相同的.

以下，用 $M_n(\boldsymbol{Z}/N\boldsymbol{Z})$表示所有的模 N 的同余 n 阶整数矩阵类的集合，用$(\boldsymbol{Z}/N\boldsymbol{Z})^k$ 表示所有的模 N 的同余 k 维整数向量类的集合.

定义 2 设 $\boldsymbol{A},\boldsymbol{B}\in M_2(\boldsymbol{Z}/N\boldsymbol{Z})$，若

$$\boldsymbol{AB}\equiv\boldsymbol{BA}\equiv\begin{pmatrix}1&0\\0&1\end{pmatrix}\quad(\mathrm{mod}N),$$

则称 $\boldsymbol{B}$ 是 $\boldsymbol{A}$ 对于模 N 的逆矩阵，记为 $\boldsymbol{A}^{-1}(\mathrm{mod}N)$，在不致引起误会的情形，也记作 $\boldsymbol{B}\equiv\boldsymbol{A}^{-1}$或 $\boldsymbol{B}=\boldsymbol{A}^{-1}$.

定理 设 $\boldsymbol{A}=\begin{pmatrix}a&b\\c&d\end{pmatrix}\in M_2(\boldsymbol{Z}/N\boldsymbol{Z}),D=ad-bc$，则下面的四个结论等价：

(i) $(D,N)=1$；

(ii) $\boldsymbol{A}$ 在 $M_2(\boldsymbol{Z}/N\boldsymbol{Z})$中有对于模 N 的逆矩阵；

(iii) 由

$$\begin{pmatrix}x'\\y'\end{pmatrix}\equiv\boldsymbol{A}\begin{pmatrix}x\\y\end{pmatrix}=\begin{pmatrix}ax+by\\cx+dy\end{pmatrix}\quad(\mathrm{mod}N)$$

所确定的$(Z/NZ)^2$到自身的映射是一一对应的；

(iv) 若$\begin{pmatrix}x\\y\end{pmatrix}\not\equiv\begin{pmatrix}0\\0\end{pmatrix}\pmod N$，则

$$A\begin{pmatrix}x\\y\end{pmatrix}\not\equiv\begin{pmatrix}0\\0\end{pmatrix}\pmod N.$$

证明

(i)⇒(ii)　因为$(D,N)=1$，所在存在D^{-1}，使得$DD^{-1}\equiv1\pmod N$，记

$$A^{-1}=\begin{pmatrix}D^{-1}d & -D^{-1}b\\ -D^{-1}c & D^{-1}a\end{pmatrix},$$

则

$$AA^{-1}=\begin{pmatrix}a & b\\ c & d\end{pmatrix}\begin{pmatrix}D^{-1}d & -D^{-1}b\\ -D^{-1}c & D^{-1}a\end{pmatrix}=\begin{pmatrix}D^{-1}D & 0\\ 0 & D^{-1}D\end{pmatrix}$$

$$\equiv\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}\pmod N,$$

同理可证　$A^{-1}A\equiv\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}\pmod N$，即$A^{-1}$是$A$对模$N$的逆矩阵.

(ii)⇒(iii)　若$A^{-1}(\mathrm{mod}N)$存在，则由

$$\begin{pmatrix}x'\\y'\end{pmatrix}\equiv A\begin{pmatrix}x\\y\end{pmatrix}\pmod N$$

得到$\begin{pmatrix}x'\\y'\end{pmatrix}$的唯一原象

$$\begin{pmatrix}x\\y\end{pmatrix}\equiv A^{-1}\begin{pmatrix}x'\\y'\end{pmatrix}\pmod N.$$

(iii)⇒(iv)　若$\begin{pmatrix}x\\y\end{pmatrix}\not\equiv\begin{pmatrix}0\\0\end{pmatrix}\pmod N$，则必是$A\begin{pmatrix}x\\y\end{pmatrix}\not\equiv$

$\begin{pmatrix}0\\0\end{pmatrix}$ $(\mathrm{mod}N)$，否则，由于 $\boldsymbol{A}\begin{pmatrix}0\\0\end{pmatrix}\equiv\begin{pmatrix}0\\0\end{pmatrix}(\mathrm{mod}N)$，可得到$\begin{pmatrix}0\\0\end{pmatrix}$的两个原象，这与(iii)矛盾.

(iv)⇒(i)　若$(D,N)=\delta>1$，令 $N=\delta N_1$，则有三种可能情形：

Ⅰ. a,b,c,d 都被 δ 整除，此时，取$\begin{pmatrix}x\\y\end{pmatrix}=\begin{pmatrix}N_1\\N_1\end{pmatrix}$，得到

$$\boldsymbol{A}\begin{pmatrix}N_1\\N_1\end{pmatrix}\equiv\begin{pmatrix}0\\0\end{pmatrix}\quad(\mathrm{mod}N),$$

但$\begin{pmatrix}N_1\\N_1\end{pmatrix}\not\equiv\begin{pmatrix}0\\0\end{pmatrix}$ $(\mathrm{mod}N)$，这与(iii)矛盾；

Ⅱ. a 与 b 中有一个不被 δ 整除，此时，取$\begin{pmatrix}x\\y\end{pmatrix}=\begin{pmatrix}-bN_1\\aN_1\end{pmatrix}\not\equiv\begin{pmatrix}0\\0\end{pmatrix}(\mathrm{mod}N)$，得到

$$\boldsymbol{A}\begin{pmatrix}x\\y\end{pmatrix}=\begin{pmatrix}a&b\\c&d\end{pmatrix}\begin{pmatrix}-bN_1\\aN_1\end{pmatrix}=\begin{pmatrix}-abN_1+abN_1\\-bcN_1+adN_1\end{pmatrix}$$

$$=\begin{pmatrix}0\\DN_1\end{pmatrix}\equiv\begin{pmatrix}0\\0\end{pmatrix}\quad(\mathrm{mod}N),$$

这与结论(iii)矛盾；

Ⅲ. c 与 d 中有一个不被 δ 整除，可类似于情形 Ⅱ 进行证明. □

定义 3　设 $\boldsymbol{A}=\begin{pmatrix}a&b\\c&d\end{pmatrix}\in M_2(\boldsymbol{Z}/N\boldsymbol{Z})$，$D=ad-bc$，$(D,N)=1$. 对于含两个符号 p_1,p_2（$0\leqslant p_1,p_2<N$，即它们取自含 N 个不同符号的符号表）的信息单元 $\boldsymbol{P}$，使它与二维向量$\begin{pmatrix}p_1\\p_2\end{pmatrix}$对应，

记 $\boldsymbol{P}=\begin{pmatrix}p_1\\p_2\end{pmatrix}$，并且用

$$\boldsymbol{E}\equiv\boldsymbol{AP}\quad(\mathrm{mod}N),\tag{2}$$

即

$$\boldsymbol{E}=\begin{pmatrix}e_1\\e_2\end{pmatrix}\equiv\begin{pmatrix}a&b\\c&d\end{pmatrix}\begin{pmatrix}p_1\\p_2\end{pmatrix}\quad(\mathrm{mod}N),\ 0\leqslant e_1,e_2<N$$

作为明文单元 $\boldsymbol{P}$ 所对应的密文单元. 这样的加密方法，称为线性矩阵加密方法，矩阵 $\boldsymbol{A}$ 称为加密矩阵(加密钥).

由定理，若已知密文单元 $\boldsymbol{E}=\begin{pmatrix}e_1\\e_2\end{pmatrix}$，则可用

$$\boldsymbol{P}=\begin{pmatrix}p_1\\p_2\end{pmatrix}\equiv\boldsymbol{A}^{-1}\boldsymbol{E}\quad(\mathrm{mod}N),\quad 0\leqslant p_1,p_2<N\tag{3}$$

求出明文单元 $\boldsymbol{P}$. 称 $\boldsymbol{A}^{-1}$ 为解密矩阵(解密钥).

例 1　已知明文单元含二个符号，取自含 26 个英文字母 $a,b,\cdots,y,z$ 的符号表，这些符号分别与 0,1,…,24,25 对应。已知使用线性矩阵加密方法对“*GOAWAY*”加密，加密矩阵为 $\begin{pmatrix}22&3\\7&8\end{pmatrix}$，试求出密文.

解　*GOAWAY* 所对应的数串是 6　14　0　22　0　24，将它们分成三个单元，即 $\begin{pmatrix}6\\14\end{pmatrix}$，$\begin{pmatrix}0\\22\end{pmatrix}$ 与 $\begin{pmatrix}0\\24\end{pmatrix}$. 由(2)式计算与 $\begin{pmatrix}6\\14\end{pmatrix}$ 对应的密文：

$$\begin{pmatrix}6\\14\end{pmatrix}\rightarrow\begin{pmatrix}2&3\\7&8\end{pmatrix}\begin{pmatrix}6\\14\end{pmatrix}\equiv\begin{pmatrix}2\\24\end{pmatrix}\quad(\mathrm{mod}26),$$

即 $GO\rightarrow CY$. 同样地得到 $AW\rightarrow OU$，$AY\rightarrow UK$. 因此，所求的密文是 *CYOUUK*.

例 2　使用例 1 的加密系统及同一个符号表，求出与密文 *CHIQEFKM* 对应的明文.

解　$\boldsymbol{A}=\begin{pmatrix}2 & 3\\ 7 & 8\end{pmatrix}$，$D=2\cdot 8-3\cdot 7=-5$，$D^{-1}\equiv 5(\mathrm{mod}26)$，

因此，由定理 1，

$$\boldsymbol{A}^{-1}\equiv\begin{pmatrix}5\cdot 8 & -5\cdot 3\\ -5\cdot 7 & 5\cdot 2\end{pmatrix}\equiv\begin{pmatrix}14 & 11\\ 17 & 10\end{pmatrix}(\mathrm{mod}26).$$

CHIQEFKM 对应的数串是 2　7　8　16　4　5　10　12，因此，利用(3)式，得到明文所对应的数串

$$\begin{pmatrix}p_1 & p_3 & p_5 & p_7\\ p_2 & p_4 & p_6 & p_8\end{pmatrix}\equiv\boldsymbol{A}^{-1}\begin{pmatrix}2 & 8 & 4 & 10\\ 7 & 16 & 5 & 12\end{pmatrix}$$

$$\equiv\begin{pmatrix}14 & 11\\ 17 & 10\end{pmatrix}\begin{pmatrix}2 & 8 & 4 & 10\\ 7 & 16 & 5 & 12\end{pmatrix}\equiv\begin{pmatrix}1 & 2 & 7 & 12\\ 0 & 10 & 14 & 4\end{pmatrix}$$

$(\mathrm{mod}26)$，

因此，所求的明文是 *BACKHOME*.

例 3　设明文信息单元含二个符号，这些符号可能是 $a,b,\cdots,y,z$，空格，?，!，并且它们分别与数 $0,1,\cdots,24,25,26,27,28$ 对应. 已经知道密文 *GFPYJPLADPLW*，并且知道最后五个字符是发送者的签名 *MARLA*，求这段密文的含义.

解　已经知道了五对对应的符号，就可以得到密文与明文的几种对应关系，例如

$$DPLW\rightarrow ARLA,$$

$$APLW\rightarrow MRLA,$$

等等.

假定采用对应关系 $DPLW\rightarrow ARLA$ 来破译密文，则

$$DPLW\rightarrow\begin{pmatrix}3 & 11\\ 15 & 22\end{pmatrix}\rightarrow ARLA\rightarrow\begin{pmatrix}0 & 11\\ 17 & 0\end{pmatrix},$$

因此，若解密矩阵为 A^{-1}，则

$$\begin{pmatrix} 0 & 11 \\ 17 & 0 \end{pmatrix} \equiv A^{-1} \begin{pmatrix} 3 & 11 \\ 15 & 22 \end{pmatrix} \pmod{29},$$

因此，

$$A^{-1} \equiv \begin{pmatrix} 0 & 11 \\ 17 & 0 \end{pmatrix} \begin{pmatrix} 3 & 11 \\ 15 & 22 \end{pmatrix}^{-1} \pmod{29}.$$

记 $D=3 \cdot 22-11 \cdot 15 \equiv 17 \pmod{29}$，则由 $(D,29)=1$，$D^{-1} \equiv 12 \pmod{29}$，及定理 1 得到

$$\begin{pmatrix} 3 & 11 \\ 15 & 22 \end{pmatrix}^{-1} \equiv \begin{pmatrix} 12 \cdot 22 & -12 \cdot 11 \\ -12 \cdot 15 & 12 \cdot 3 \end{pmatrix} \equiv \begin{pmatrix} 3 & 13 \\ 23 & 7 \end{pmatrix} \pmod{29},$$

于是

$$A^{-1} \equiv \begin{pmatrix} 0 & 11 \\ 17 & 0 \end{pmatrix} \begin{pmatrix} 3 & 13 \\ 23 & 7 \end{pmatrix} \equiv \begin{pmatrix} 21 & 19 \\ 22 & 18 \end{pmatrix} \pmod{29}.$$

利用(3)式求出明文

$$\begin{pmatrix} p_1 & p_3 & p_5 & p_7 & p_9 & p_{11} \\ p_2 & p_4 & p_6 & p_8 & p_{10} & p_{12} \end{pmatrix}$$

$$\equiv \begin{pmatrix} 21 & 19 \\ 22 & 18 \end{pmatrix} \begin{pmatrix} 6 & 15 & 9 & 11 & 3 & 11 \\ 5 & 24 & 15 & 0 & 15 & 22 \end{pmatrix}$$

$$\equiv \begin{pmatrix} 18 & 17 & 10 & 28 & 0 & 11 \\ 19 & 8 & 4 & 10 & 7 & 0 \end{pmatrix} \pmod{29},$$

即明文为 *STRIKE! MARLA.*

一般地，如果存在几种可能的明文与密文的对应关系，就必须对每一种可能，使用上例中的方法，求出解密矩阵，然后决定出正确的解密钥. 在上例中，当然可以先采用其他对应关系来求解密矩阵. 但是，容易判断，由它们推导出的解密矩阵，不能用以得到有意义的明文，从而知道这样的解密矩阵是不正确的.

例 4　已知信息单元含两个符号，它们是 26 个英文字母 $a,\cdots,z$，分别与 $0,\cdots,25$ 对应. 已知密文 $WKNCCHSSJH$ 的前四个字对应的明文是 $GIVE$，并且知道是使用线性矩阵加密方法，试译出明文.

解　已知

$$WKNC\rightarrow\begin{pmatrix}22 & 13\\ 10 & 2\end{pmatrix}\rightarrow\begin{pmatrix}6 & 21\\ 8 & 4\end{pmatrix}\rightarrow GIVE.$$

设解密矩阵为 $\boldsymbol{A}^{-1}$，则

$$\begin{pmatrix}6 & 21\\ 8 & 4\end{pmatrix}\equiv\boldsymbol{A}^{-1}\begin{pmatrix}22 & 13\\ 10 & 2\end{pmatrix}\pmod{26}. \tag{4}$$

令 $\boldsymbol{C}=\begin{pmatrix}22 & 13\\ 10 & 2\end{pmatrix}$，则它的行列式 $D=22\cdot 2-13\cdot 10=-96$. 由于 $(-96,26)=2$，所以 $\boldsymbol{C}$ 在 $M_2(\boldsymbol{Z}/26\boldsymbol{Z})$ 中没有逆矩阵，因此，不能用例 3 中的方法求出 $\boldsymbol{A}^{-1}\pmod{26}$. 因此，我们将先求出 $\boldsymbol{A}^{-1}\pmod{13}$，然后确定 $\boldsymbol{A}^{-1}\pmod{26}$.

由(4)式，

$$\begin{pmatrix}6 & 8\\ 8 & 4\end{pmatrix}\equiv\boldsymbol{A}_0^{-1}\begin{pmatrix}9 & 0\\ 10 & 2\end{pmatrix}\pmod{13},$$

其中 $\boldsymbol{A}_0^{-1}\equiv\boldsymbol{A}^{-1}\pmod{13}$. 上式右端的矩阵的行列式是 $2\cdot 9-10\cdot 0=18$，$(18,13)=1$，所以矩阵 $\begin{pmatrix}9 & 0\\ 10 & 2\end{pmatrix}$ 对模 13 的逆矩阵存在，即

$$\begin{pmatrix}9 & 0\\ 10 & 2\end{pmatrix}^{-1}\equiv\begin{pmatrix}8\cdot 2 & -8\cdot 0\\ -8\cdot 10 & 8\cdot 9\end{pmatrix}\equiv\begin{pmatrix}3 & 0\\ 11 & 7\end{pmatrix}\pmod{13},$$

于是

$$\boldsymbol{A}_0^{-1}\equiv\begin{pmatrix}6 & 8\\ 8 & 4\end{pmatrix}\begin{pmatrix}3 & 0\\ 11 & 7\end{pmatrix}\equiv\begin{pmatrix}2 & 4\\ 3 & 2\end{pmatrix}\pmod{13}. \tag{5}$$

设 $\boldsymbol{A}^{-1}=\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ (mod26)，显然有 $\boldsymbol{A}^{-1}\equiv\boldsymbol{A}_0^{-1}$(mod13)，

因此，

$$\boldsymbol{A}^{-1}\equiv\boldsymbol{A}_0^{-1}+13\boldsymbol{A}_1,\quad (\mathrm{mod}26),$$

其中 $\boldsymbol{A}_1$ 是以 0 或 1 为元素的矩阵. 因此，$13\boldsymbol{A}_1$ 共有 16 种可能的取值，即是

$$\boldsymbol{A}_1=\begin{pmatrix} \alpha & \beta \\ \lambda & \mu \end{pmatrix},\quad \alpha,\beta,\gamma,\mu\in\{0,1\}.$$

由于 $\boldsymbol{A}^{-1}$对于模 26 的矩阵 $\boldsymbol{A}$ 是存在的，所以，由定理 1，$\boldsymbol{A}^{-1}$的行列式与 26 互素；此外，$\boldsymbol{A}$ 又应该满足(4)式. 用这两个条件去考察所有可能的 A_1，就可以删去 14 种可能性，只余下两种可能，即

$$\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}\text{与}\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix},$$

相应的 $\boldsymbol{A}^{-1}$是

$$\boldsymbol{A}_1=\begin{pmatrix} 15 & 17 \\ 16 & 15 \end{pmatrix}\text{与 }\boldsymbol{A}_2=\begin{pmatrix} 15 & 4 \\ 16 & 15 \end{pmatrix}.$$

用这两个 $\boldsymbol{A}^{-1}$ 分别试译明文. 用 $\boldsymbol{A}_1$ 时，得到明文 *GIVETHEMUP*；用 $\boldsymbol{A}_2$ 时，得到明文 *GIVEHEMHP*. 于是可以断定，应该取 $\boldsymbol{A}_1$ 为 $\boldsymbol{A}^{-1}$，第一个明文是正确的.

定义 4　设 $\boldsymbol{A}=(a_{ij})_{i,j}\in M_k(\boldsymbol{Z}/N\boldsymbol{Z})$，$\boldsymbol{A}^{-1}(\mathrm{mod}N)$存在，

$\boldsymbol{B}=\begin{pmatrix} b_1 \\ \vdots \\ b_k \end{pmatrix}$ 是 k 维整数向量. 对于明文单元 $\boldsymbol{P}=\begin{pmatrix} p_1 \\ \vdots \\ p_k \end{pmatrix}$，用公式

$$\boldsymbol{E}=\begin{pmatrix} e_1 \\ \vdots \\ e_k \end{pmatrix}\equiv\boldsymbol{AP}+\boldsymbol{B}\quad (\mathrm{mod}N),0\leqslant e_1,\cdots,e_k<N,$$

确定与 P 对应的密文. 称这样的加密方法为仿射矩阵加密方法.

特别地,若

$$A=(a_{ij})_{i,j},\quad a_{ij}=0\quad (i\neq j),a_{ii}=1,1\leqslant i\leqslant k,$$

则称这样的加密方法为 Vigenère 加密方法,即,若明文为 $p_1\cdots p_n$,则对应的密文是 $e_1\cdots e_n$,

$$e_i\equiv p_i+b_{i(\mathrm{mod}k)}\quad (\mathrm{mod}N),\quad 1\leqslant i\leqslant n,\qquad (6)$$

其中 $i(\mathrm{mod}k)$表示 i 对模 k 的最小非负剩余.

显然,如果 $b_1,\cdots,b_k$ 对模 N 是互不同余的,则密文 $e_1\cdots e_n$ 就是由 k 组互不相交的明文经过使用不同加密钥的凯撒加密方法得到的. 因此,若 N 与 k 已知,则可用第一节的方法破译 Vigenère 方法加密后的密文. 下面,叙述一个求 k 的期望值的方法.

为了简化讨论,设符号表含有 N 个互不相同的符号:1,2,…,N,它们被随机选取构成符号串的概率都是 $\frac{1}{N}$. 又设符号 i 在正常的信息(例如正常语言叙述)中出现的概率为 $p(i),i=1,2,\cdots,N$.

假设整个密文含有 n 个符号,即在 n 个位置上各标着某个符号 $i(1\leqslant i\leqslant N)$,我们来考察,任意两个位置上有相同符号的可能性. 假设密文由(6)式确定,其中 $b_1,\cdots,b_k$ 是互不相同的.

在 n 个位置中任取两个位置的方法有 $C_n^2=\frac{1}{2}n(n-1)$种.

根据(6)式,可以将 n 个位置分成 k 组,每一组由 $\frac{n}{k}$ 个符号组成,它们对应着相同的 b_i.

如果两个位置属于同一组,由于是使用同一个加密变换(有

相同的加密钥 b_i)，所以，在这两个位置上有相同符号的概率是 $\sum_{i=1}^{N} p^2(i)$. 对于每个选定的位置，它所在的那一组里尚有 $\frac{n}{k}-1$ 个位置，因此，在任意两个不同位置(但属于同一组)上有相同符号的频率是

$$A_1 = \left(\frac{1}{2}n(n-1)\right)^{-1} \cdot \frac{1}{2}n\left(\frac{n}{k}-1\right)\sum_{i=1}^{N} p^2(i). \qquad (7)$$

如果这两个位置不属于同一组，由于密文中各符号的出现是等概率的，所以，在指定的两个位置上有相同符号的概率是 $\sum_{i=1}^{N} \frac{1}{N}\cdot\frac{1}{N} = \frac{1}{N}$. 在选定一个位置后，在另外的组里选一个位置的方法是 $n-\frac{n}{k}$ 个，因此，不属于同一组的两个位置上有相同符号的频率是

$$A_2 = \left(\frac{1}{2}n(n-1)\right)^{-1} \cdot \frac{1}{2}n\left(n-\frac{n}{k}\right)\cdot\frac{1}{N}.$$

由上式及(7)式，得到，任意两个位置上有相同符号的频率

$$A \doteq A_1 + A_2 = \frac{1}{n-1}\left(\frac{n}{k}-1\right)\sum_{i=1}^{N} p^2(i)$$

$$+ \frac{1}{n-1}\left(n-\frac{n}{k}\right)\cdot\frac{1}{N}. \qquad (8)$$

另一方面，假设在整个密文中符号 $i(1\leqslant i\leqslant N)$ 的个数是 n_i，那么，在任意两个位置上同时有符号 i 的频率是

$$\left(\frac{1}{2}n(n-1)\right)^{-1} \cdot \frac{1}{2}n_i(n_i-1),$$

因此，在任意两个位置上有相同符号的频率是

$$A = (n(n-1))^{-1}\sum_{i=1}^{N} n_i(n_i-1).$$

比较上式与(8)式，就可以得出数 k 的期望值.

还有另外的估计 k 值的方法. 例如，在密文中若有高频率重复出现的符号(或符号串)，则它们之间的距离就可能是 k 的倍数. 因此，通过寻求这个距离的数值，进行因数分解和试译，就可以得到 k 值.

习　题

1. 已知明文单元含二个符号，它们取自 $a,b,\cdots,y,z$ 构成的符号表. 使用线性矩阵加密方法，将 *TAKEITBACK* 加密，设加密矩阵是 $\begin{pmatrix}7 & 9\\ 8 & 3\end{pmatrix}$.

2. 使用例 3 中的符号表. 已知信息单元含二个符号，在密文“! *IWGVIEX*! *ZRADRYD*”中，已知最后五个字符对应的明文是发送者的签名 *MARIA*，求明文.

3. 计算下列矩阵的逆矩阵：

(1) $\begin{pmatrix}1 & 7\\ 6 & 5\end{pmatrix}$ (mod11)；

(2) $\begin{pmatrix}2 & 3\\ 7 & 4\end{pmatrix}$ (mod17).

4. 求解同余方程组：

$$17x+11y\equiv 7 \pmod{29}$$
$$13x+10y\equiv 1 \pmod{29}.$$

第三节　数据加密标准

在考察密码系统的安全性时，一般地，总是假定密码分析人员知道加密时所使用的算法. 但是，在大多数情况下，密码系统的设计者总是尽量将算法的一些细节保密. 1977 年，美国国家

标准局颁布了由 IBM 公司提出的数据加密标准(Data Encryption Standard),简称 DES,供民用或非国防性政府部门使用. 由于 DES 将加密算法全部公开,因此,被看做是密码学研究中的一个重大成果.

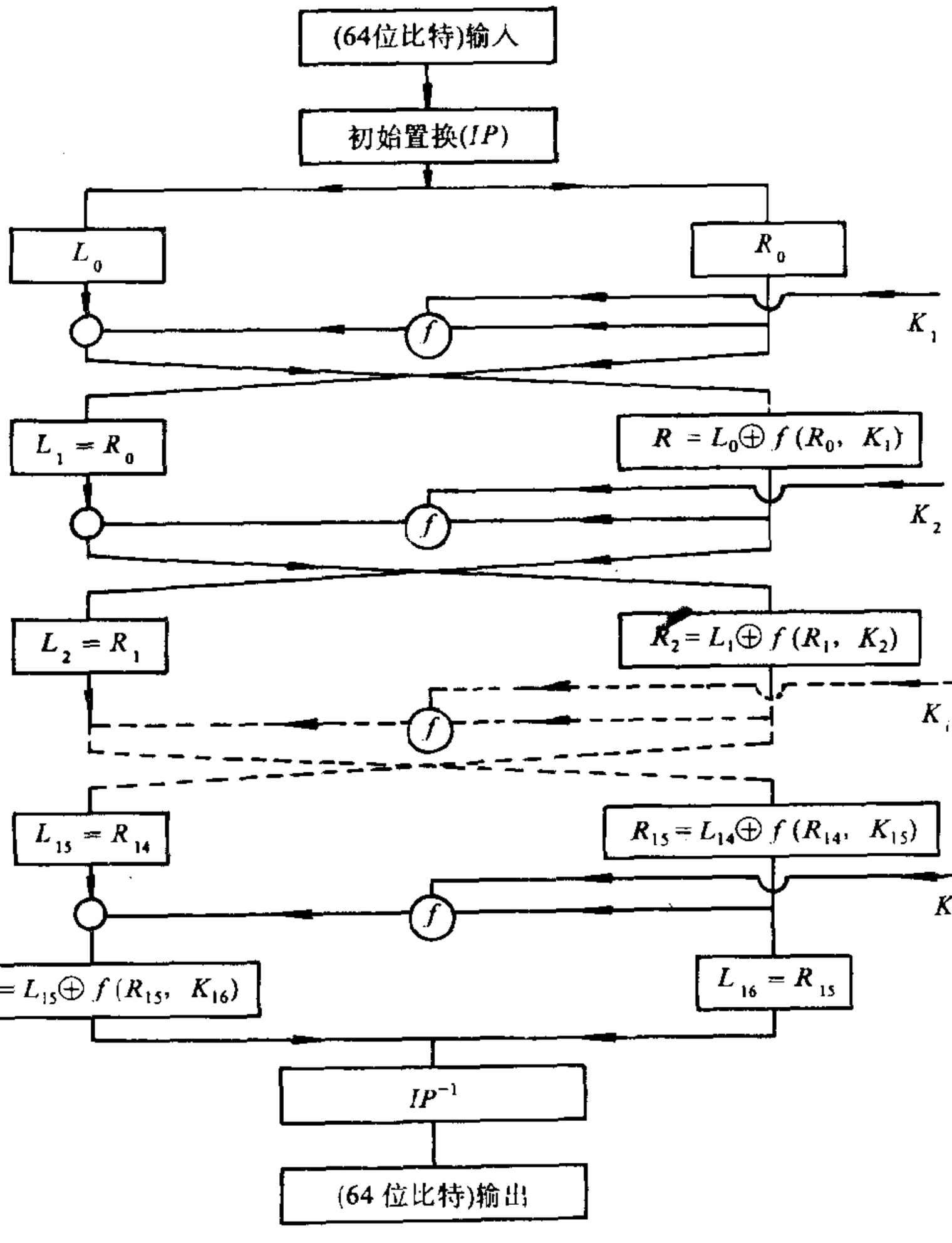


图 1　DES 加密算法

DES 对长度为 64 的二进制数加密,使用的密钥及输出的密文也都是长度为 64 的二进制数. 加密的全部过程如图 1 所

示，它包括三大部分：初始置换，逆置换，以及 16 次迭代过程. 因此，DES 是多个加密算法的复合. 下面，对这三个部分加以说明.

Ⅰ. 初始置换 IP 是将明文的位数码进行一次置换，IP^{-1}则是初始置换的逆置换，它们由表 1 决定.

表 1　　*IP* 与 IP^{-1}

IP

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

IP^{-1}

40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

置换(或逆置换)是这样进行的：从左往右，从上往下地数起，第 i 个位置上的数，就是明文中第 i 个位数码的置换(或逆置换)结果. 以 M' 表示输入 M 置换后的结果，那么，M' 的第 3 个位数码是 M 的第 42 个位数码，等等.

容易看出，IP^{-1}确是 IP 的逆.

Ⅱ. 迭代过程　共有16 次. 每次迭代过程产生长度为 64 比特的数据. 将第 i 次迭代后的数据分成 L_i(由左面的 32 个比特组成)与 R_i(由右面的 32 个比特组成)两部分，第 $i+1$ 次迭代结果就是

$$L_{i+1}=R_i, R_{i+1}=L_i \oplus f(R_i, k_{i+1}), \tag{1}$$

其中 $f(R_i, k_{i+1})$是一个含 32 个比特的数，k_{i+1}由密钥 e 决定，符

号⊕表示对模 2 的加法.

Ⅲ. $k_i(1\leqslant i\leqslant 16)$的确定. 设密钥 $e=(e_1e_2\cdots e_{64})_2$,将每个 e_i 按次序分成 8 组,每组含 8 个比特. 每一组中的第八个比特是奇偶性校验位,用以校验加密过程中可能出现的错误(例如,在计算 k_i 或存贮时的误差,等等),在计算 k_i 时并不使用它们.

$k_i(1\leqslant i\leqslant 16)$的确定方式见图 2.

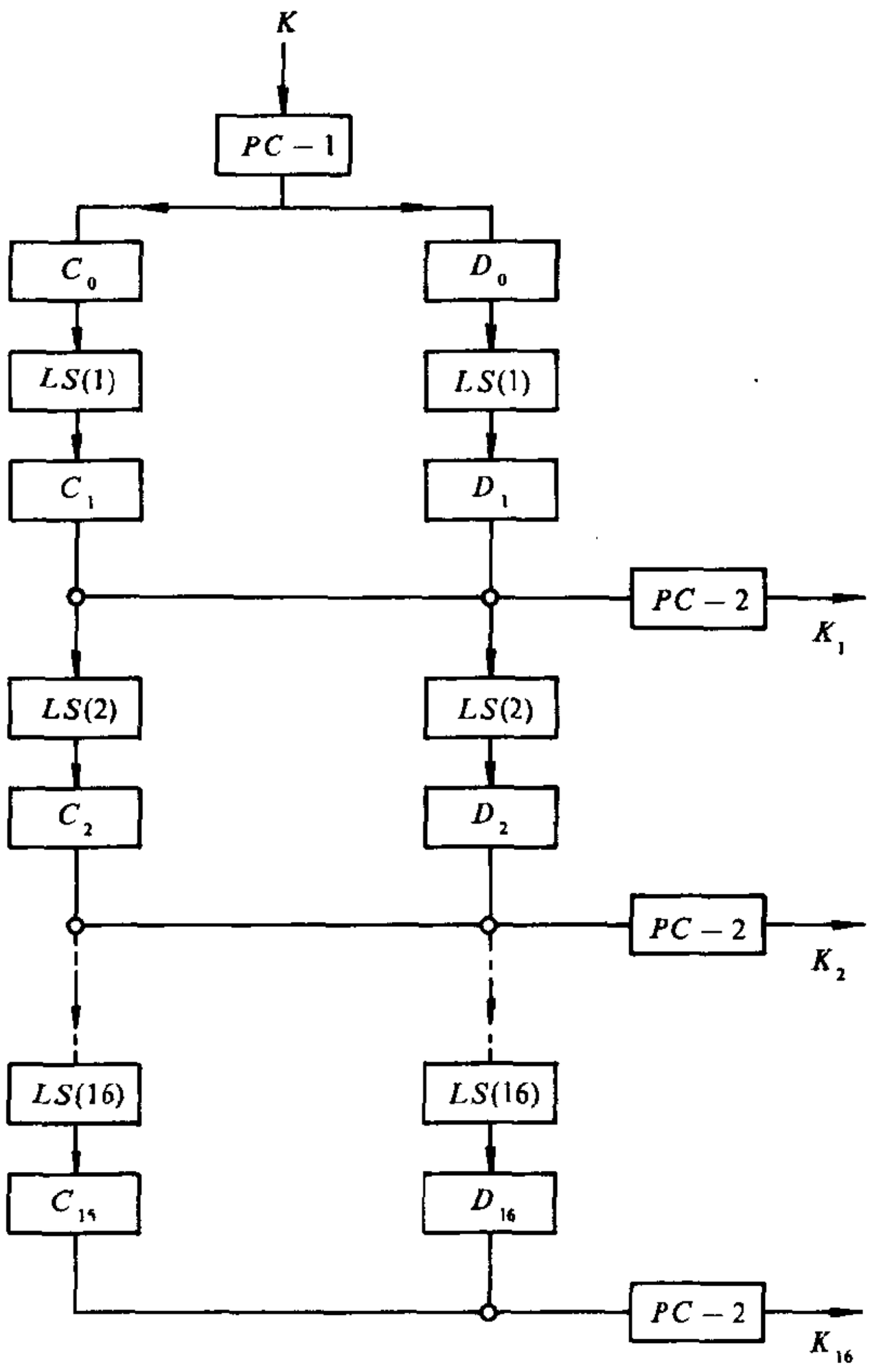


图 2　密钥 k 的生成

(i) 密钥 e 经置换 $PC-1$ 后，生成 C_0 与 D_0，它们分别是 e 经过置换 $PC-1$ 后的前一半(28 个)比特，与后一半(28 个)比特. $PC-1$ 由表 2 决定。例如，置换后的第一个位数码是 e 的第 57 个位数码，置换后的第二个位数码是 e 的第 49 个位数码，等等. 这样，有

$$C_0=e_{57}e_{49}e_{41}\cdots e_{52}e_{44}e_{36},$$

$$D_0=e_{63}e_{55}e_{47}\cdots e_{20}e_{12}e_4.$$

表 2　　$PC-1$ 与 $PC-2$

$PC-1$

57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

$PC-2$

14	17	11	24	1	5
3	28	15	6	21	10
23	19	12	4	26	8
16	7	27	20	13	2
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32

(ii) C_{i+1}与 $D_{i+1}(0\leqslant i\leqslant 15)$分别由 C_i 与 D_i 左移 LS_{i+1}位而得到. LS_i 的数值见表 3.

表 3　　LS_i 数值

迭代次数	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
LS_i	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

例如，若

$$C_2=c_1\cdots c_{28},\quad D_2=d_1\cdots d_{28},$$

则

$$C_3=c_3c_4\cdots c_1c_2,\quad D_3=d_3d_4\cdots d_1d_2.$$

(iii) k_i 是 C_iD_i 经置换 $PC-2$ 后得到的.

例如,若 $C_iD_i=\alpha_1\cdots\alpha_{56}$,则

$$k_i=\alpha_{14}\alpha_{17}\cdots\alpha_{29}\alpha_{32}.$$

Ⅳ. 迭代函数 $f(R,k)$的作用.

(i) 利用选位器 E 将 R_{i-1}的 32 位比特(即 R_{i-1})转换为 48 位比特,其选位方式由表 4 确定.

表 4　　选位器 E

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

例如,若

$$R_{i-1}=r_1r_2\cdots r_{32},$$

则经过选位后,得到

$$E(R_{i-1})=r_{32}r_1r_2r_3\cdots r_{31}r_{32}r_1.$$

显然,在 $E(R_{i-1})$中,不同位置上的比特可能是 R_{i-1}中的同一个比特.

(ii) 将 $E(R_{i-1})$与 k_i 做模 2 加法.将所得到的 48 位比特,按照它们的顺序分成八组,每组六个比特.用 $E_i(1\leqslant i\leqslant 8)$表示这八个比特数组.

(iii) 选择函数 S_i. $E_i(1\leqslant i\leqslant 8)$经过由 S_i 决定的变换,成为有四个比特的数. $S_i(1\leqslant i\leqslant 8)$见于表 5. 每个 S_i 是一个四行十

六列的表.

表 5　　选择函数 S_i

行＼列	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
S_1 0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13
S_2 0	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
1	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
2	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
3	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9
S_3 0	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
1	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
2	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
3	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12
S_4 0	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
1	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
2	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
3	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14
S_5 0	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
1	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
2	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
3	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3
S_6 0	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
1	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
2	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
3	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13
S_7 0	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
1	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
2	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
3	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12
S_8 0	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
1	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
2	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
3	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

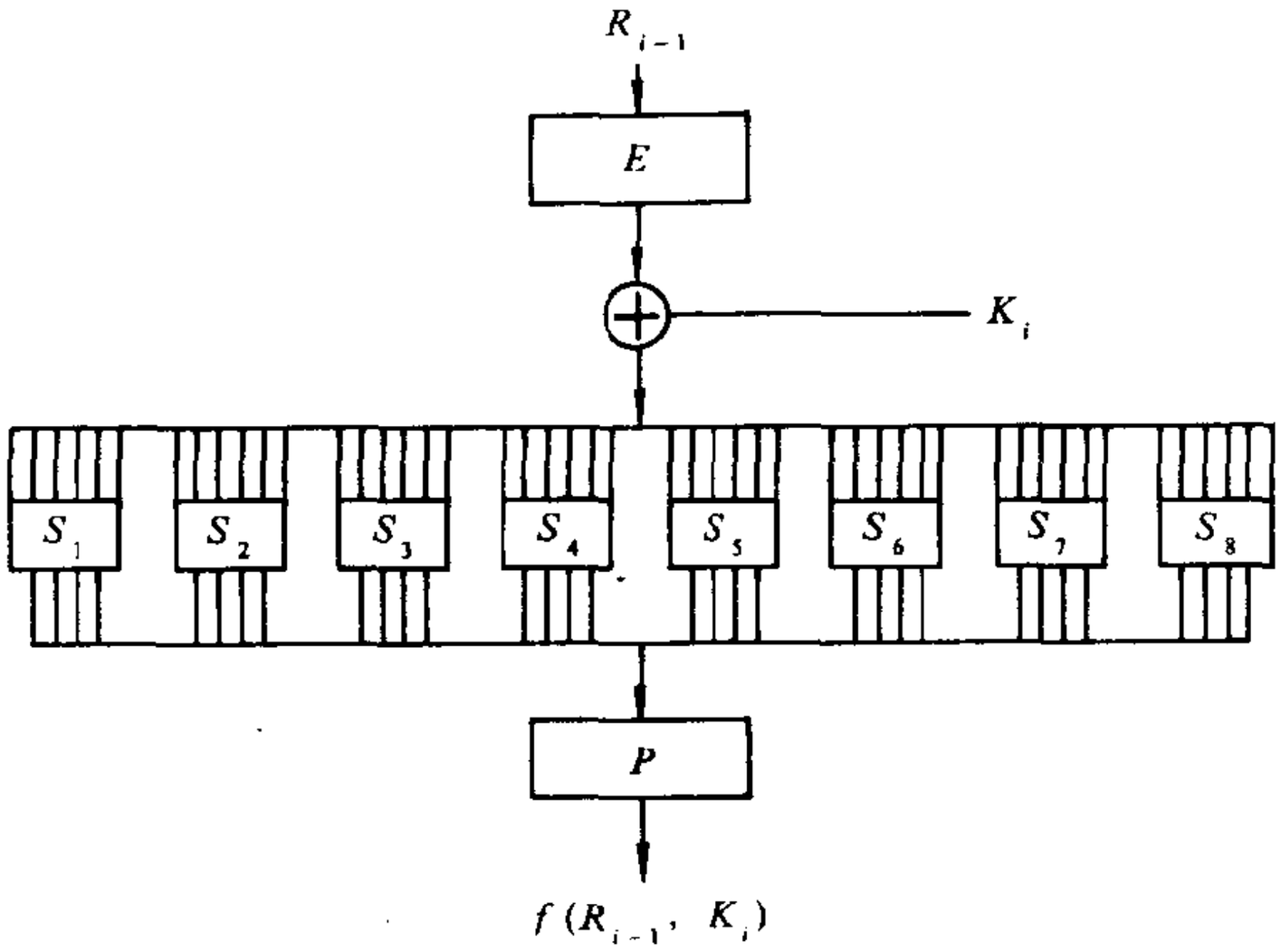


图 3　函数 $f(R_{i-1},k_i)$

以 $S_i(m,n)$表示表 S_i 中位于第 m 行、第 n 列的数的二进制表示，设 $E_i=\beta_1\beta_2\beta_3\beta_4\beta_5\beta_6$，又设二进制数$(\beta_2\beta_3\beta_4\beta_5)_2=B$，$(\beta_1\beta_6)_2=B'$，此处 B 与 B'是十进制数，则 $S_i(B',B)$就是 E_i 经函数 S_i 作用后的结果。例如，设 E_1 由六个比特 000111 构成，则

$$B=(0011)_2=3,\quad B'=(0,1)_2=1,$$

在 S_1 中，第一行、第三列的元素是 $4=(0100)_2$，则经过 S_1 的作用后，E_1 成为 0100.

(iv) 置换 P 是将经过 $S_i(1\leqslant i\leqslant 8)$作用后得到的 32 个比特进行一次由表 6 所确定的置换. 例如，若它们是 $f_1\cdots f_{32}$，则经置换 P 后，得到 $f_{16}f_7\cdots f_4f_{25}$.

在图 3 中，说明了 $f(R_{i-1},k_i)$的作用.

由(1)式得到

$$R_i=L_{i+1},L_i=R_{i+1}\oplus f(R_i,k_{i+1})=R_{i+1}\oplus f(L_{i+1},k_{i+1}),$$

因此，解密算法与加密算法是相同的，但密钥却是颠倒次序使用

的，即依次使用 $k_{16}, k_{15}, \cdots, k_1$.

表 6　　置换 P

16	7	20	21
29	12	28	17
1	15	23	26
5	18	31	10
2	8	24	14
32	27	3	9
19	13	30	6
22	11	4	25

对于 *DES* 的评价，主要有两个方面的批评：第一，密钥的有效长度(56 比特)可能太小. 例如，Diffie 和 Hellman 就提出设计一种专用机，对所有可能的密钥实行穷举搜索的办法，破译 DES 密码. 第二，函数 $S_i(1 \leqslant i \leqslant 8)$的设计仍然是保密的，而其中可能含有不安全因素.

下面，简单介绍关于加密方法的复合.

定义　设 f_1 与 f_2 是两个加密函数，即对于明文 P，由 f_1 与 f_2 加密后的密文分别为 $f_1(P)$与 $f_2(P)$. 以 $\mathscr{P}$ 表示所有可能的明文的集合，记

$$\mathscr{C}_1 = \{f_1(P);\quad P \in \mathscr{P}\}.$$

又设 $f_2(P)$在 $\mathscr{C}_1$ 上有定义，则称加密函数

$$f(P) = f_2(f_1(P))$$

是 f_1 与 f_2 的复合，记为 $f = f_2 \circ f_1$. 显然，利用 $f(P)$可以建立一个新的密码系统.

DES 是一个多次复合加密方法. 下面是复合加密方法的另一个例子.

例 设 N_1,N_2,a_1,a_2,b_1,b_2 都是正整数，

$$N_2>N_1,(a_1,N_1)=(a_2,N_2)=1.$$

设明文为 $P,0\leqslant P<N_1$，则

$$f(P)\equiv a_2f_1(P)+b_2 \pmod{N_2},0\leqslant f(P)<N_2,$$

就是由仿射加密函数

$$E=f_1(P)\equiv a_1P+b_1 \pmod{N_1},\quad 0\leqslant E<N_1,$$

与

$$E=f_2(P)\equiv a_2P+b_2 \pmod{N_2},\quad 0\leqslant E<N_2$$

复合而成.

注 一般地，例中的复合加密函数不再是仿射加密函数.

习 题

1. 设明文为

$$P=0100\ \ 0000\ \ 1101\ \ 1001\ \ 1010\ \ 1111$$
$$1000\ \ 0101\ \ 0000\ \ 0111\ \ 1011\ \ 0101$$
$$1110\ \ 1110\ \ 0101\ \ 1001\ \ 1110,$$

密钥为

$$e=0000\ \ 1001\ \ 0101\ \ 0011\ \ 0001\ \ 1110$$
$$1010\ \ 1011\ \ 1110\ \ 1001\ \ 0111\ \ 0001$$
$$1011\ \ 0000\ \ 0101\ \ 1010,$$

试求 L_1 与 R_1.

2. 证明例的注中的结论.

第三章　素性与因数分解

在现代密码学的研究中，整数的素性的判定，以及整数的因数分解，都起着很重要的作用. 在本章中，主要介绍常用的几种判定素性的方法，研究将大整数分解因数的手段. 与此相关的，还要介绍关于二次剩余，原根，指标，以及连分数的基本理论，和它们在密码学中的应用.

第一节　二 次 剩 余

在本节中，除特别说明，p 均表示奇素数.

定义　若 $(a,m)=1$ 并且 $x^2\equiv a(\mathrm{mod}m)$ 有解，则称 a 是“模 m 的二次剩余”，或“二次剩余 $\mathrm{mod}m$”，记作 $a\in QR(m)$，否则，称 a 是“模 m 的二次非剩余”，或“二次非剩余 $\mathrm{mod}m$”，记作 $a\in QNR(m)$.

下面的定理说明，对于素数 p，模 p 的二次剩余是存在的.

定理 1　在模 p 的简化系中，二次剩余与二次非剩余各有一半.

证明　考察模 p 的简化系 $1,2,\cdots,p-1$，由

$$i^2\equiv(p-i)^2 \pmod{p},\ 1\leqslant i\leqslant\frac{1}{2}(p-1)$$

可知，在 $1^2,2^2,\cdots,(p-1)^2$ 中只有 $\frac{1}{2}(p-1)$ 个模 p 的二次剩余. 因为 $(i^2,p)=(i,p)=1\left(1\leqslant i\leqslant\frac{p-1}{2}\right)$，所以它们都与 p 互

素. 又因为当 $1\leqslant j\leqslant i\leqslant p-1$ 时，

$$p\nmid(i^2-j^2) \quad 即 \quad i^2\not\equiv j^2 \pmod{p},$$

所以它们对模 p 互不同余. 这证明了定理. □

定义 2 Legendre 符号$\left(\frac{a}{p}\right)$的取值为

$$\left(\frac{a}{p}\right)=\begin{cases}0, 若(a,p)\neq 1;\\ 1, 若\ a\in QR(m),\\ -1, 若\ a\in QNR(m).\end{cases}$$

注 由定义 2，若 $a\equiv b\pmod{p}$，则$\left(\frac{a}{p}\right)=\left(\frac{b}{p}\right)$.

引理 方程 $x^2\equiv a\pmod{p}$至多有两个解，此处把所有对模 p 同余的解作为一个解(见定理 1.5.8 前的说明).

证明 若$(a,p)>1$，即 $p\mid a$，则方程 $x^2\equiv a\pmod{p}$只有一个解 $x\equiv 0\pmod{p}$.

若方程有一个非零解 $x_0\not\equiv 0\pmod{p}$，$1\leqslant x_0\leqslant p-1$，又设 x 是它的另一个解，$1\leqslant x\leqslant p-1$，则由

$$x_0^2\equiv a\pmod{p},\ x^2\equiv a\pmod{p}$$

得到

$x_0^2-x^2\equiv 0\pmod{p}$，即 $p\mid(x_0+x)(x_0-x)$，因此 $p\mid x_0+x$ 或 $p\mid x_0-x$，即 $x\equiv -x_0\pmod{p}$或 $x\equiv x_0\pmod{p}$. 由此可见，若方程有一个非零解 x_0，则它还有一个解$-x_0\equiv p-x_0\pmod{p}$，它与 x_0 对模 p 不同余，因为，若 $x_0\equiv -x_0\pmod{p}$，则 $p\mid 2x_0$，这与 $p\nmid 2$; $p\nmid x_0$ 矛盾. □

定理 2 设$(a,p)=1$，则

$$-\left(\frac{a}{p}\right)(p-1)!\equiv a^{\frac{1}{2}(p-1)} \pmod{p}. \tag{1}$$

证明 设 $S=\{1,2,\cdots,p-1\}$是模 p 的简化系. 由定理

1.5.8,对于每个 $x\in S$,都有 $y\in S$,使得

$$yx\equiv a \pmod{p}. \tag{2}$$

若 $\left(\frac{a}{p}\right)=-1$,即 a 是模 p 的二次非剩余,则 $x\not\equiv y(\mathrm{mod}\,p)$,

于是 S 中的元素可以分成 $\frac{p-1}{2}$ 对,每一对都满足(2)式,从而

$$1\cdot 2\cdots(p-1)\equiv a^{\frac{1}{2}(p-1)} \pmod{p},$$

即(1)式成立.

若 $\left(\frac{a}{p}\right)=1$,设 $x_0^2\equiv a(\mathrm{mod}\,p)$,则也有 $(p-x_0)^2\equiv a(\mathrm{mod}\,p)$.

由于 $1\leqslant x_0, p-x_0\leqslant p-1$, $p\nmid 2x_0$,所以 $x_0\not\equiv p-x_0(\mathrm{mod}\,p)$,即 x_0 与 $p-x_0$ 是 $x^2\equiv a(\mathrm{mod}\,p)$的两个不同的解. 由引理 1,这个方程不再有另外的解,因此,除 x_0 与 $p-x_0$ 外,剩下的 S 中的 $p-3$ 个数可以两两配对使满足(2)式,由此推出

$$\begin{aligned}1\cdot 2\cdots(p-1)&\equiv x_0(p-x_0)a^{\frac{1}{2}(p-3)}\equiv -x_0^2\cdot a^{\frac{1}{2}(p-3)}\\&\equiv -a^{\frac{p-1}{2}} \pmod{p},\end{aligned}$$

即(1)式成立. □

推论 1 (Wilson) $(p-1)!\equiv -1 \pmod{p}$.

证明 在定理 2 中取 $a=1$. □

推论 2 (Euler 判别法) 设 $(a,p)=1$,则

$$\left(\frac{a}{p}\right)\equiv a^{\frac{p-1}{2}}(\mathrm{mod}\,p).$$

证明 由定理 2 及推论 1 推出. □

推论 3 $\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}$.

推论 4 $\left(\frac{ab}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

证明 若 $(a,p)\neq 1$ 或 $(b,p)\neq 1$,推论显然成立. 若 $(a,p)=(b,p)=1$,则由推论 2 得到

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)\equiv a^{\frac{p-1}{2}}b^{\frac{p-1}{2}}\equiv\left(\frac{ab}{p}\right)\pmod{p},$$

由于上式两端都只有 1 和 -1 两个值，且 $1\not\equiv -1\pmod{p}$，所以推论成立. □

推论 5 若 $(a,p)=1$，$a=\pm q_1q_2\cdots q_sb^2$，其中诸 q_i 是互不相同的素数，b 是整数，则

$$\left(\frac{a}{p}\right)=\left(\frac{\pm 1}{p}\right)\left(\frac{q_1}{p}\right)\cdots\left(\frac{q_s}{p}\right).$$

定理 3 (Gauss 引理) 设 $(a,p)=1$，$ak\left(k=1,2,\cdots,\frac{p-1}{2}\right)$ 对模 p 的最小非负剩余是 r_k. 若在 $r_1,\cdots,r_{\frac{p-1}{2}}$ 中恰有 m 个 $r_k>\frac{p}{2}$，则 $\left(\frac{a}{p}\right)=(-1)^m$.

证明 以 $a_1,\cdots,a_s$ 表示小于 $\frac{p}{2}$ 的 r_k，$b_1,\cdots,b_m$ 表示大于 $\frac{p}{2}$ 的 $r_k\left(1\leqslant k\leqslant\frac{p-1}{2}\right)$，则

$$a^{\frac{p-1}{2}}\left(\frac{p-1}{2}\right)!=\prod_{k=1}^{\frac{1}{2}(p-1)}(ak)\equiv\prod_{i=1}^{s}a_i\prod_{j=1}^{m}bj\pmod{p}.\quad(3)$$

首先指出，对于任何 a_i 及 b_j，$a_i\neq p-b_j$. 否则，有 $a_i+b_j=p$，即有 k_1 与 k_2，$1\leqslant k,k_2\leqslant\frac{p-1}{2}$ 使得 $a(k_1+k_2)\equiv 0\pmod{p}$，这与 $(a,p)=1$ 及 $k_1+k_2\leqslant p-1$ 矛盾. 类似地可以证明，当 $i\neq j$ 时，$a_i\neq a_j$，$b_i\neq b_j$. 这样，由(3)式得到

$$\begin{aligned}a^{\frac{p-1}{2}}\left(\frac{p-1}{2}\right)!&\equiv\prod_{i=1}^{s}a_i\cdot(-1)^m\prod_{j=1}^{m}(p-b_j)\\&=(-1)^m\left(\frac{p-1}{2}\right)!\pmod{p},\end{aligned}$$

即

$$a^{\frac{p-1}{2}}\equiv(-1)^m \pmod{p}.$$

由此及定理 2 的推论 2 得到定理结论. □

定理 4 若$(a,p)=1,2\nmid a$,则

$$\left(\frac{a}{p}\right)=(-1)^m,\quad m=\sum_{k=1}^{\frac{1}{2}(p-1)}\left[\frac{ak}{p}\right],$$

$$\left(\frac{2}{p}\right)=(-1)^{\frac{1}{8}(p^2-1)}.$$

证明 使用定理 3 中的符号 r_k,a_i,b_j,s 以及 m.

由 $ak=p\left[\frac{ak}{p}\right]+r_k$ 及定理 3 的证明,有

$$a\cdot\frac{p^2-1}{8}=p\sum_{k=1}^{\frac{p-1}{2}}\left[\frac{ak}{p}\right]+\sum_{i=1}^{s}a_i+\sum_{j=1}^{m}b_j$$

$$=p\sum_{k=1}^{\frac{1}{2}(p-1)}\left[\frac{ak}{p}\right]+\sum_{i=1}^{s}a_i+\sum_{j=1}^{m}(p-b_j)$$

$$-pm+2\sum_{j=1}^{m}bj$$

$$\equiv p\sum_{k=1}^{\frac{p-1}{2}}\left[\frac{ak}{p}\right]+\sum_{k=1}^{\frac{p-1}{2}}k-pm$$

$$\equiv p\sum_{k=1}^{\frac{1}{2}(p-1)}\left[\frac{ak}{p}\right]+\frac{p^2-1}{8}+m \pmod 2. \quad (4)$$

若 $2\nmid a$,则由上式及 $8\mid p^2-1$ 得到

$$m\equiv\sum_{k=1}^{\frac{1}{2}(p-1)}\left[\frac{ak}{p}\right] \pmod 2;$$

若 $a=2$,则由 $0\leqslant\left[\frac{ak}{p}\right]\leqslant\left[\frac{p-1}{p}\right]=0$ 及(4)式得到 $m\equiv\frac{p^2-1}{8} \pmod 2$.

利用定理 3 得证. □

定理 5(二次互反律) 设 p 与 q 都是奇素数,$(p,q)=1$,则

$$\left(\frac{q}{p}\right)=(-1)^{\frac{(p-1)(q-1)}{4}}\left(\frac{p}{q}\right).$$

证明 利用定理 4 及例 1.4.8 得证. □

例 1 设素数 $p\equiv 3(\mathrm{mod}4)$,$\left(\frac{a}{p}\right)=1$,则方程

$$x^2\equiv a \pmod{p} \tag{5}$$

的解是 $x\equiv\pm a^{k+1}(\mathrm{mod}p)$,其中 $k=\frac{1}{4}(p-3)$.

解 由于 $a\in QR(p)$,所以 $a^{\frac{p-1}{2}}\equiv 1(\mathrm{mod}p)$,即

$$a^{2k+1}\equiv 1 \pmod{p}.$$

所以

$$a^{2k+2}=(a^{k+1})^2\equiv a \pmod{p}.$$

因为 $(2,p)=(a,p)=1$,所以 $2a^{k+1}\not\equiv 0(\mathrm{mod}p)$,即 $a^{k+1}\not\equiv -a^{k+1}$ $(\mathrm{mod}p)$,结论得证.

例 2 设素数 $p\equiv 5(\mathrm{mod}8)$,$\left(\frac{a}{p}\right)=1$,记 $k=\frac{p-5}{8}$,则(5)的解是 $x\equiv\pm 2^{(2k+1)t}a^{k+1}(\mathrm{mod}p)$,其中 t 为 0 或 1.

解 类似于例 1,可得到

$$a^{4k+2}\equiv 1 \pmod{p},$$

$$(a^{2k+1}+1)(a^{2k+1}-1)\equiv 0 \pmod{p}.$$

由于 $p\nmid 2$,所以上式左端两因子中有且仅有一个被 p 整除.

(i) 若 $a^{2k+1}\equiv 1 \pmod{p}$,则

$$a^{2k+2}=(a^{k+1})^2\equiv a \pmod{p},$$

即 $x\equiv\pm a^{k+1}(\mathrm{mod}p)$是(3)的解.

(ii) 若 $a^{2k+1}\equiv -1(\mathrm{mod}p)$,由定理 4 知,2 是模 p 的二次非剩余,所以 $2^{\frac{p'-1}{2}}=2^{4k+2}\equiv -1(\mathrm{mod}p)$,于是 $a^{2k+2}\cdot 2^{4k+2}\equiv a$

$(\mathrm{mod}\,p)$，即

$$(a^{k+1}\cdot 2^{2k+1})^2\equiv a \pmod{p},$$

因此，$x\equiv\pm 2^{2k+1}a^{k+1}(\mathrm{mod}\,p)$是(5)的解.

例3 计算$\left(\frac{42}{61}\right)$.

解 由定理4及定理5，

$$\left(\frac{42}{61}\right)=\left(\frac{2\cdot 3\cdot 7}{61}\right)=\left(\frac{2}{61}\right)\left(\frac{3}{61}\right)\left(\frac{7}{61}\right)$$

$$=(-1)^{\frac{1}{8}(61^2-1)}\left(\frac{61}{3}\right)(-1)^{\frac{1}{4}(3-1)(61-1)}$$

$$\cdot\left(\frac{61}{7}\right)(-1)^{\frac{1}{4}(7-1)(61-1)}$$

$$=-\left(\frac{1}{3}\right)\left(\frac{-2}{7}\right)=-\left(\frac{-1}{7}\right)\left(\frac{2}{7}\right)=-(-1)^{\frac{7-1}{2}+\frac{7^2-1}{8}}$$

$$=1$$

例4 设p是奇素数，$(a,p)=1$，估计计算$\left(\frac{a}{p}\right)$所需要的时间.

解 设$a=k\cdot p+a_1$，$k\geqslant 0$，$1\leqslant a_1\leqslant p-1$，则由定义1的注，$\left(\frac{a}{p}\right)=\left(\frac{a_1}{p}\right)$，即

$$\left(\frac{a}{p}\right)=\left(\frac{a_1}{p}\right)\equiv a_1^{\frac{p-1}{2}} \pmod{p}.$$

由定理1.5.7，由上式计算$\left(\frac{a}{p}\right)$需要$O(\log^3 p)$次比特运算. 利用一次除法得到a_1，需要$O(\log a\log p)$次比特运算. 所以，共需要$O(\log p)\cdot O(\log a+\log^2 p)$次比特运算.

定义3 设$p_1,\cdots,p_r$是奇素数，$P=p_1p_2\cdots p_r$，规定Jacobi符号

$$\left(\frac{a}{P}\right)=\prod_{i=1}^{r}\left(\frac{a}{p_i}\right)$$

注 Jacobi 符号是 Legendre 符号的推广，但是，它与模 P 的二次剩余没有任何确定的关系.

定理 6 Jacobi 符号具有以下性质：

(1) $\left(\frac{a}{P}\right)$是 a 的周期（为 P 的）积性函数；

(2) $\left(\frac{1}{P}\right)=1$, $\left(\frac{a^2}{P}\right)=1$;

(3) $\left(\frac{-1}{P}\right)=(-1)^{\frac{1}{2}(P-1)}$;

(4) $\left(\frac{2}{P}\right)=(-1)^{\frac{1}{8}(P^2-1)}$;

(5) $\left(\frac{Q}{P}\right)=(-1)^{\frac{(P-1)(Q-1)}{4}}\left(\frac{P}{Q}\right)$, $2\nmid PQ$.

证明 这些性质都可以由定义 3 及 Legendre 符号的相应性质推导出. 以性质(5)为例：

设 $P=p_1\cdots p_s, Q=q_1\cdots q_r$，其中诸 p 与 q 都是奇素数. 不妨设$(p_i,q_j)=1(1\leqslant i\leqslant s,1\leqslant j\leqslant r)$，否则，(5)显然成立.

由定理 5，$\left(\frac{Q}{P}\right)\left(\frac{P}{Q}\right)=(-1)^k$，其中

$$k=\sum_{i=1}^{s}\sum_{j=1}^{r}\frac{1}{4}(p_{i-1})(q_j-1)$$

$$=\sum_{i=1}^{s}\frac{p_i-1}{2}\sum_{j=1}^{s}\frac{q_j-1}{2}$$

$$\equiv\frac{1}{2}\left(\prod_{i=1}^{s}\left(1+2\frac{p_i-1}{2}\right)-1\right)\cdot\frac{1}{2}\left(\prod_{j=1}^{r}\left(1+2\cdot\frac{q_j-1}{2}\right)-1\right)$$

$$\equiv\frac{1}{2}(p_1\cdots p_s-1)\cdot\frac{1}{2}(q_1\cdots q_r-1)$$

$$\equiv\frac{1}{4}(P-1)(Q-1)\quad(\mathrm{mod}2),$$

结论得证. □

例 5　判断二次同余式

$$x^2\equiv 888 \pmod{1999}$$

是否有解.

解　由

$$\left(\frac{888}{1999}\right)=\left(\frac{2}{1999}\right)^3\cdot\left(\frac{111}{1999}\right)$$

及

$$\left(\frac{2}{1999}\right)=(-1)^{\frac{1999^2-1}{8}}=1$$

得到

$$\left(\frac{888}{1999}\right)=\left(\frac{111}{1999}\right)=(-1)^{\frac{111-1}{2}\cdot\frac{1999-1}{2}}\left(\frac{1999}{111}\right)$$

$$=-\left(\frac{1}{111}\right)=-1,$$

所以,原同余方程无解.

定理 7　设 p 是奇素数,$\left(\frac{a}{p}\right)=1$,若已知 $b\in QNR(p)$,则存在计算 a 的平方根 $\bmod p$ 的算法,需要 $O(\log^4 p)$ 次比特运算.此处称 r 是 a 的平方根 $\bmod p$(或 a 对于模 p 的平方根),若 $r^2\equiv a(\bmod p)$ 成立.有时也将 r 记作 $\sqrt{a}\bmod p$.

证明　首先,叙述求 a 的平方根 $\bmod p$ 的方法,然后估计所需要的计算时间.

(i) 设 $p-1=2^cP$,$2\nmid P$

(ii) 依次地按下述方法确定整数 k_i 与 a_i:

$$a_1=a$$

$$k_{i-1}=\min\{k;k\geqslant 0,a_{i-1}^{2^kP}\equiv 1 \pmod p\},$$

$$a_i\equiv a_{i-1}b^{2^{c-k_{i-1}}}(\bmod p),\quad i\geqslant 2,$$

此处及以下,a_i 都是取对于模 p 的最小非负剩余.

由 k_i 与 a_i 的定义方式可知

$$a_i^{2^{k_i-1}P} \equiv (a_{i-1}b^{2^{c-k_i-1}})^{2^{k_i-1}P}$$

$$\equiv a_{i-1}^{2^{k_i-1}P}b^{2^{c-1}P} \pmod{p}. \tag{6}$$

因为 $b \in QNR(p)$，所以，由 Euler 判别法，

$$-1 = \left(\frac{b}{p}\right) \equiv b^{\frac{p-1}{2}} = b^{2^{c-1}P} \pmod{p},$$

由此及(6)式，并由 k_{i-1} 的定义，得到

$$a_i^{2^{k_i-1}P} \equiv (-1)(-1) = 1 \pmod{p}.$$

由上式可见，若 $k_{i-1} \geqslant 1$，则必有 $k_i < k_{i-1}$. 这说明，按上述 k_i 的确定方法，总可找到某个 $k_n = 0$，此时，由 k_n 的定义可知

$$(a_n^{\frac{1}{2}(P+1)})^2 \equiv a_n \pmod{p}. \tag{7}$$

(iii) 记

$$r_n \equiv a_n^{\frac{1}{2}(P+1)} \pmod{p},$$

此处 r_n 及以下的 r_i 是对于模 p 的最小非负剩余. 依次地定义

$$r_i \equiv r_{i+1}(b^{2^{c-k_i-1}})^{-1}, \pmod{p}, \quad 1 \leqslant i \leqslant n-1,$$

其中 A^{-1} 表示 A 对于模 p 的乘法逆元素.

由 r_n 的定义及(7)式，显然

$$r_n^2 \equiv a_n \pmod{p}. \tag{8}$$

记 $A^{-2} = A^{-1} \cdot A^{-1}$，若 $r_{i+1}^2 \equiv a_{i+1} \pmod{p}$，则

$$r_i^2 \equiv r_{i+1}^2(b^{2^{c-k_i-1}})^{-2} \equiv a_{i+1}(b^{2^{c-k_i-1}})^{-2}$$

$$\equiv a_i b^{2^{c-k_i}}(b^{2^{c-k_i-1}})^{-2} \equiv a_i \pmod{p},$$

因此，利用归纳法，容易证明

$$r_i^2 \equiv a_i \pmod{p}, \quad 1 \leqslant i \leqslant n-1,$$

因而 $r_1^2 \equiv a_1 = a \pmod{p}$，即 r_1 是 a 对于模 p 的平方根.

下面分析求出 r_1 所需要的计算时间.

在步骤(i)中，作一次减法及移位，需要 $O(\log p)$ 次比特运算.

在步骤(ii)中，最多确定 c 个 a_i，$c=O(\log p)$. 当 $a_{i-1}(<p)$ 确定后，利用重复平方法确定 k_{i-1} 需要 $O(\log^4 p)$ 次比特运算，由 a_{i-1} 与 b 计算 a_i 也需要 $O(\log^3 p)$ 次比特运算. 因此，计算出 a_n 需要 $O(\log^4 p)$ 次比特运算.

在步骤(iii)中，利用重复平方法，由 r_{i+1} 及 b 确定 r_i(包括求 $b^{-1}\bmod p$)需要 $O(\log^3 p)$ 次比特运算. 因此，求出 r_1 共需要 $O(\log^4 p)$ 次比特运算.

综合以上，求出 a 对于模 p 的平方根共需要 $O(\log^4 p)$ 次比特运算. □

注 一般地，并不知道求 $b\in QNR(p)$ 的多项式时间算法是存在的. 但是，由定理 1 可知，这样的概率算法是存在的.

定理 8 设 $m=p_1^{a_1}\cdots p_k^{a_k}$，所有的 p_i 都是奇素数. 若已知 $a\in QR(m)$，$(a,m)=1$，以及 $b_i(1\leqslant i\leqslant k)$ 使得 $\left(\frac{b_i}{p_i}\right)=-1$，则计算 a 对于模 m 的平方根需要 $O(\log^A m)$ 次比特运算，$A>0$ 是常数.

证明 由定理 7，对每个 $p=p_i(1\leqslant i\leqslant k)$，存在 x_0，使得 $x_0^2\equiv a(\bmod p)$.

对于 $j\geqslant 2$，假设已知

$$x'=x_0+x_1p+\cdots+x_{j-2}p^{j-2}$$

满足 $x'^2\equiv a(\bmod p^{j-1})$，则存在某个整数 b，使得

$$x'^2=a+bp^{j-1}. \tag{9}$$

令

$$x=x'+x_{j-1}p^{j-1}=x_0+x_1p+\cdots+x_{j-1}p^{j-1}, \tag{10}$$

则由(9)式容易得到

$$x^2=(x'+x_{j-1}p^{j-1})^2\equiv a+bp^{j-1}+2x_0x_{j-1}p^{j-1}$$
$$=a+p^{j-1}(b+2x_0x_{j-1})\pmod{p^j}.$$

由于 p 是奇素数，$x_0\in QR(p)$，所以$(2x_0,p)=1$，所以存在某个 x_{j-1}使得

$$b+2x_0x_{j-1}\equiv 0\pmod{p}. \tag{11}$$

对于这样确定的 x_{j-1}，由(10)式确定的 x 显然满足 $x^2\equiv a\pmod{p^j}$. 照此方法，由 x_0 开始，可以逐步地确定 $x_1,\cdots x_{\alpha-1}$，并利用(10)式确定 x，使得

$$x^2\equiv a\pmod{p^\alpha}. \tag{12}$$

设 $\lambda_i(1\leqslant i\leqslant k)$是对应于 $p_i^{\alpha_i}$ 的方程(12)的解，利用孙子定理可以求得 x，使得

$$x\equiv\lambda_i\pmod{p_i^{\alpha_i}},\quad 1\leqslant i\leqslant k, \tag{13}$$

容易证明，x 就是 a 对于模 m 的平方根.

下面分析计算时间.

由定理 7，对于每个 p_i，求出相应的 x_0 需要 $O(\log^4 p)$次比特运算. 因此，求出这 k 个分别与 $p_1,\cdots,p_k$ 相应的 x_0，需要 $O(\log^4 p_1)+\cdots+O(\log^4 p_k)=O(\log^{A_1}m)$次比特运算，此处及以下的 A_1,A_2,A_3,A_4 都是正常数.

由 x_0 求出满足(12)式的 x，需要求出 $\alpha-1$ 个系数. 计算每个系数时，先要计算 x'^2，并且确定(9)式中的 a 与 b，再要解关于 x_{j-1}的方程(11)，因此，求出与 p^α 对应的满足(12)的 x 需要 $O(\log^{A_2}p^\alpha)$次比特运算. 求出与 $p_1^{\alpha_1},\cdots,p_k^{\alpha_k}$ 对应的 $\lambda_1,\cdots,\lambda_k$ 共需要

$$\sum_{i=1}^{k}O(\log^{A_2}p_i^{\alpha_i})=O(\log^{A_3}m)$$

次比特运算.

由定理 1.5.11 的注 2,利用孙子定理由 $\lambda_1,\cdots,\lambda_k$ 确定满足(13)式的 x,需要 $O(\log^{A_4}m)$次比特运算.

综合以上,证得定理. □

推论 设 p 与 q 是不同的奇素数,a 是对模 $n=pq$ 的二次剩余.若已知 a 对模 p 和对模 q 的平方根分别是 x 和 y,则存在多项式时间算法可以计算出 a 对模 n 的平方根.

证明 (留作习题).

例 6 设 n 是奇数,则存在数 $b,(b,n)=1$,使得

$$b^{\frac{n-1}{2}}\not\equiv\left(\frac{b}{n}\right)\pmod{n}. \tag{14}$$

解 分两种情况考虑:

(i) 存在奇素数 $p,p^2\mid n$. 取 $b=1+\frac{n}{p}$. 设 $n=kp^2$,则$(b,n)=(1+kp,kp^2)=(1+kp,-p)=(1,-p)=1$,同时

$$\left(\frac{b}{n}\right)=\left(\frac{1+kp}{kp^2}\right)=\left(\frac{1+kp}{k}\right)\left(\frac{1+kp}{p^2}\right)=\left(\frac{1}{k}\right)=1.$$

另一方面,由

$$b^{\frac{n-1}{2}}=(1+kp)^{\frac{n-1}{2}}\equiv 1+\frac{n-1}{2}kp\pmod{n}$$

及 $p\nmid\frac{n-1}{2}$可知 $b^{\frac{n-1}{2}}\not\equiv 1\pmod{n}$.

(ii) $n=p_1\cdots p_s$,其中诸 p_i 是不相同的奇素数. 任取 $a\in QNR(p_1)$,并利用孙子定理求出 b,使得

$$b\equiv a\pmod{p_1},\quad b\equiv 1\pmod{p_2\cdots p_s},$$

则

$$\left(\frac{b}{n}\right)=\left(\frac{b}{p_1}\right)\left(\frac{b}{p_2\cdots p_s}\right)=-1.$$

但是,由于 $b^{\frac{n-1}{2}}\equiv 1(\mathrm{mod}\,p_2\cdots p_s)$,所以,不可能有 $b^{\frac{n-1}{2}}\equiv -1$

(mod$n$)，即(14)式成立.

习　题

1. 计算$\left(\frac{91}{167}\right),\left(\frac{71}{73}\right),\left(\frac{-35}{97}\right),\left(\frac{3083}{3911}\right)$.

2. 设p是奇素数，证明：

(1) $\left(\frac{-1}{p}\right)=1$的充分必要条件是$p\equiv1(\mathrm{mod}4)$

(2) $\left(\frac{2}{p}\right)=1$的充分必要条件是$p\equiv\pm1(\mathrm{mod}8)$

(3) $\left(\frac{-2}{p}\right)=1$的充分必要条件是$p\equiv1$或$3(\mathrm{mod}8)$

3. 设$p>3$是素数，证明：

(i) $\left(\frac{3}{p}\right)=1$的充分必要条件是$p\equiv\pm1(\mathrm{mod}12)$；

(ii) $\left(\frac{-3}{p}\right)=1$的充分必要条件是$p\equiv1(\mathrm{mod}6)$

4. 设n是正整数，$4n+3$与$8n+7$都是素数，则

$$2^{4n+3}\equiv1\quad(\mathrm{mod}8n+7),$$

并由此证明$23\mid2^{11}-1,47\mid2^{23}-1$.

5. 对于$p=7,13$与17，求出所有$QR(p)$.

6. 设p是奇素数，a,b,c是整数，并且$p\nmid a$. 证明方程$ax^2+bx+c\equiv0(\mathrm{mod}p)$在$\{0,1,2,\cdots,p-1\}$中的解的个数是$1+\left(\frac{D}{p}\right)$，其中$D=b^2-4ac$.

7. 确定定理8中常数A的上界.

8. 证明定理8的推论.

第二节　原根与指标

以下，设m是大于1的整数.

定义 1　设$(a,m)=1$,若d是使

$$a^d\equiv 1 \pmod{m}$$

成立的最小正整数,则称它是a对模m的指数,记为$\mathrm{Ord}_m a$.

定义 2　若$\mathrm{Ord}_m a=\varphi(m)$,则称$a$是模$m$的原根,或简称为$m$的原根.

推论　若$a\equiv b(\mathrm{mod}m)$,则$\mathrm{Ord}_m a=\mathrm{Ord}_m b$.

定理 1　$a^k\equiv 1(\mathrm{mod}m)$的充分必要条件是$\mathrm{Ord}_m a\mid k$.

证明　令$t=\mathrm{Ord}_m a, k=st+r, 0\leqslant r<t$,则

$$1\equiv a^k=a^{st+r}\equiv a^r \pmod{m}.$$

若$r\neq 0$,则上式与$t=\mathrm{Ord}_m a$的定义矛盾,所以$r=0$,即$\mathrm{Ord}_m a\mid k$. 充分条件是显然的. □

推论 1　若$(a,m)=1$,则$\mathrm{Ord}_m a\mid\varphi(m)$.

证明　由 Euler 定理,$a^{\varphi(m)}\equiv 1 \pmod{m}$,再由定理 1 得证. □

推论 2　设$(a,m)=1$,则

$$a^{k_1}\equiv a^{k_2} \pmod{m}\Leftrightarrow \mathrm{Ord}_m a\mid k_1-k_2.$$

推论 3　设$(a,m)=1, t=\mathrm{Ord}_m a$,则$1,a^1,\cdots,a^t$对模$m$两两不同余;特别地,若$a$是模$m$的原根,则

$$1,a^1,a^2,\cdots,a^{\varphi(m)}$$

构成模m的简化剩余系.

定理 2　设$\mathrm{Ord}_m a=t$,则对于任意的正整数b,$\mathrm{Ord}_m a^b=t/(b,t)$.

证明　设$s=\mathrm{Ord}_m a^b, d=(b,t), b=b_1 d, t=t_1 d$,则$(b_1,t_1)=1$. 利用定理 1,由

$$(a^b)^{t_1}=(a^t)^{b_1}\equiv 1 \pmod{m}$$

可知$s\mid t_1$. 同样地,由

$$(a^b)^s=a^{bs}\equiv 1 \pmod{m}$$

可知 $t\mid bs$，即 $t_1\mid b_1 s$，但是$(t_1,b_1)=1$，所以 $t_1\mid s$. 因此，$s=t_1=t/(b,t)$. □

推论 1 设 g 是模 m 的原根，则 g^b 是模 m 的原根的充分必要条件是$(b,\varphi(m))=1$.

推论 2 设模 m 有一个原根，则它就有 $\varphi(\varphi(m))$个互不同余的原根.

证明 由推论 1，若 g 是模 m 的原根，则有 $\varphi(\varphi(m))$个 b，$0\leqslant b<\varphi(m)$，使得 g^b 是模 m 的原根. 若有 $b_1\neq b_2$，$0\leqslant b_1,b_2<\varphi(m)$使得

$$g^{b_1}\equiv g^{b_2} \pmod{m},$$

则由定理 1 的推论 2 得到 $\varphi(m)\mid b_1-b_2$，这是不可能的. □

例 求模 7 与模 15 的原根.

解 模 7 的简化系是{1,2,3,4,5,6}，将它们的指数列表如下：

a	1	2	3	4	5	6
$\mathrm{Ord}_7 a$	1	3	6	3	6	2

可见，3 与 5 都是模 7 的原根.

对于模 15 的简化系，列表

a	1	2	4	7	8	11	13	14
$\mathrm{Ord}_{15} a$	1	4	2	4	4	2	4	2

可见，模 15 没有原根.

定理 3 模 m 的原根存在的必要条件是 $m=2,4,p^\alpha$，或 $2p^\alpha$，此处 p 是奇素数.

证明 (i) 对任意的奇数 a，设 $a=2k+1$，则

$$a^{2^{3-2}}=4k(k+1)\equiv 1 \pmod{2^3}.$$

假设对于 $n\geqslant 3$,有

$$a^{2^{n-2}}\equiv 1 \pmod{2^n}, \tag{1}$$

则存在整数 t,使得 $a^{2^{n-2}}=1+t\cdot 2^n$,因此,

$$a^{2^{(n+1)-2}}\equiv(1+t\cdot 2^n)^2\equiv 1 \pmod{2^{n+1}}.$$

这样,利用归纳法可知(1)式对于 $n\geqslant 3$ 成立.但是,$\varphi(2^n)=2^{n-1}$,因此,(1)式说明,当 $n\geqslant 3$ 时,任何奇数都不是模 2^n 的原根,即只有模 2 与模 4 才可能有原根.

(ii) 设 $m=2^\alpha p_1^{\alpha_1}\cdots p_k^{\alpha_k}$ 是 m 的标准分解式。若$(a,m)=1$,则必$(a,2^\alpha)=1$,$(a,p_i)=1(1\leqslant i\leqslant k)$.由(i)及 Euler 定理,

$$a^{\varphi(p_i^{\alpha_i})}\equiv 1 \pmod{p_i^{\alpha_i}} \quad (1\leqslant i\leqslant k), \tag{2}$$

$$a^{\frac{1}{2}\varphi(2^\alpha)}\equiv 1 \pmod{2^\alpha}, \quad \alpha\geqslant 3, \tag{3}$$

又容易验证

$$a^{\varphi(2^\alpha)}\equiv 1 \pmod{2^\alpha}, \quad \alpha=1,2, \tag{4}$$

记

$$\lambda(m)=[\delta,\varphi(p_1^{\alpha_1}),\cdots,\varphi(p_k^{\alpha_k})],$$

此处右端是最小公倍数,并且

$$\delta=\begin{cases}\varphi(2^\alpha), & \alpha=1,2\\ \dfrac{1}{2}\varphi(2^\alpha), & \alpha\geqslant 3,\end{cases}$$

则由(2),(3),(4)式得出

$$a^{\lambda(m)}\equiv 1 \pmod{m}.$$

若 $\alpha\geqslant 3$,则 $\delta<\varphi(2^\alpha)$;若 $k\geqslant 2$,则因为对每个 i,$1\leqslant i\leqslant k$,都有 $2\mid\varphi(p_i^{\alpha_i})$,所以 $\lambda(m)<\varphi(m)$.因此,在这些情形,模 m 都没有原根.

综上，得出定理结论. □

注 $\lambda(m)$称为 Carmichael 函数.

容易验证，1 是模 2 的原根，3 是模 4 的原根.

定理 4 若 p 是奇素数，则模 p 的原根存在.

证明 记 $\tau=[\mathrm{Ord}_p1,\mathrm{Ord}_p2,\cdots,\mathrm{Ord}_p(p-1)]$，并设 τ 的标准分解式是 $\tau=q_1^{a_1}\cdots q_k^{a_k}$.

对每个 $i,1\leqslant i\leqslant k$，必有某个 $j_i,1\leqslant j_i\leqslant p-1$，使得 $\mathrm{Ord}_p j_i=\lambda q_i^{a_i},\lambda\in\mathbf{Z}$，即

$$j_i^{\lambda q_i^{a_i}}\equiv 1 \pmod p. \tag{5}$$

因此，若令 $C_i=\mathrm{Ord}_p j_i^{\lambda}$，则由(5)式得到 $C_i\mid q_i^{a_i}$. 另一方面，$j_i^{\lambda C_i}\equiv 1 \pmod p$，所以，又有 $\mathrm{Ord}_p j_i\mid \lambda C_i$，即 $q_i^{a_i}\mid C_i$，因此 $C_i=q_i^{a_i}$. 这样，必有 k 个数 $x_1,\cdots,x_k$，使得

$$\mathrm{Ord}_p x_i=q_i^{a_i}\qquad(1\leqslant i\leqslant k).$$

令 $g=x_1x_2\cdots\cdots x_k$. 设 $C=\mathrm{Ord}_p g$，又记 $q_i^{a_i}=d_i,D_i=\dfrac{\tau}{d_i}$，则 $(d_i,D_i)=1$. 对任意的 $i,1\leqslant i\leqslant k$，由同余式

$$g^{\tau}=(x_1\cdots x_k)^{\tau}\equiv 1 \pmod p$$

可知 $C\mid\tau$. 另一方面，

$$1\equiv g^{CD_i}\equiv x_i^{CD_i} \pmod p,$$

所以 $d_i=\mathrm{Ord}_p x_i\mid CD_i$. 但是 $(d_i,D_i)=1$，所以 $d_i\mid C(1\leqslant i\leqslant k)$，于是 $\tau=[d_1,\cdots,d_k]\mid C$. 这就证明了 $C=\tau$，即 $\mathrm{Ord}_p g=\tau$.

根据 τ 的定义，每个 $x_i(1\leqslant i\leqslant p-1)$都是方程

$$x^{\tau}-1\equiv 0 \pmod p$$

的解. 由定理 1.5.14，$\tau\geqslant p-1$. 但是，由定理 1 又有 $\tau\mid p-1$，因此，必是 $\tau=p-1$，即 g 是模 p 的原根. □

定理 5 设 p 是奇素数，则模 $p^{\alpha}(\alpha>1)$的原根存在.

证明 设 g 是模 p 的一个原根，则 $g^{p-1}\equiv 1(\mathrm{mod}p)$，即 $g^{p-1}=1+pt_0$，t_0 是某个整数.

对于任意的 $t\in\mathbf{Z}$，

$$(g+pt)^{p-1}=1+p(t_0-g^{p-2}t+pT)=1+pm, \tag{6}$$

其中 $T\in\mathbf{Z}$，并且

$$m=t_0-g^{p-2}t+pT\equiv t_0-g^{p-2}t \pmod{p}. \tag{7}$$

因为 $(g,p)=1$，所以，关于 t 的方程 $g^{p-2}t\equiv t_0(\mathrm{mod}p)$ 只有一个解，因此，存在 t_1 使得 $p\nmid m_0$，此处 m_0 是当 $t=t_1$ 时由(7)式所确定的 m 的值.

由(6)式，

$$(g+pt_1)^{p(p-1)}=(1+pm_0)^p=1+p^2m_1,$$

其中 $m_1\equiv m_0(\mathrm{mod}p)$，所以，$p\nmid m_1$.

同样地可以证明，对于 $k\geqslant 2$，有

$$(g+pt_1)^{p^k(p-1)}=1+p^{k+1}m_k,\ p\nmid m_k. \tag{8}$$

设 $\delta=\mathrm{Ord}_{p^\alpha}(g+pt_1)$，则 $(g+pt_1)^\delta\equiv 1(\mathrm{mod}p^\alpha)$，$(g+pt_1)^\delta\equiv g^\delta\equiv 1(\mathrm{mod}p)$，所以 $(p-1)\mid\delta$. 另一方面，又有 $\delta\mid\varphi(p^\alpha)=p^{\alpha-1}(p-1)$，所以 δ 必是 $\delta=p^{r-1}(p-1)$ 的形式，$1\leqslant r\leqslant\alpha$. 由(8)式，

$$(g+pt_1)^\delta=1+p^rm_\delta\equiv 1 \pmod{p^\alpha},$$

其中 $(m_\delta,p)=1$，所以 $p^\alpha\mid p^r$，$\alpha\leqslant r$. 与已知的 $r\leqslant\alpha$ 结合，推出 $r=\alpha$，即 $\delta=\varphi(p^\alpha)$，$g+pt_1$ 是模 p^α 的原根. □

定理 6 设 p 是奇素数，则模 $2p^\alpha$ 的原根存在.

证明 设 g 是模 p^α 的原根.

若 $2\nmid g$，则

$$g^{\varphi(p^\alpha)}\equiv 1 \pmod{p^\alpha}, \tag{9}$$

$$g\equiv 1,\quad g^{\varphi(p^\alpha)}\equiv 1\pmod 2,$$

所以

$$g^{\varphi(p^\alpha)}\equiv 1\pmod{2p^\alpha}. \tag{10}$$

因为由(10)式可以导出(9)式，g 是模 p^α 的原根，所以，在(10)式中，不能用小的指数代替 $\varphi(p^\alpha)$，即 $\mathrm{Ord}_{2p^\alpha}g=\varphi(p^\alpha)=\varphi(2p^\alpha)$，$g$ 是模 $2p^\alpha$ 的原根.

若 $2\mid g$，则 $2\nmid g+p^\alpha$. 易证 $g+p^\alpha$ 也是模 p^α 的原根. 由上面的推理可知 $g+p^\alpha$ 是模 $2p^\alpha$ 的原根. □

以下，假定 $m=2,4,p^\alpha$ 或 $2p^\alpha$，其中 p 是奇素数，又设 g 是模 m 的一个原根.

由定理 1 的推论 2，当 γ 通过模 $\varphi(m)$ 的最小非负剩余系时，g^γ 通过模 m 的简化系.

定义 3 对于整数 $a,(a,m)=1$，若

$$a\equiv g^\gamma\pmod m,\quad 0\leqslant\gamma<\varphi(m),$$

则称 γ 是以 g 为底的 a 对模 m 的指标，记为 $\gamma=\mathrm{ind}_g a$.

在不致引起误会的情况下，我们将略去记号 g，即记 $\gamma=\mathrm{ind}a$，并称为 a 对模 m 的指标.

定理 7 设 $(a,m)=1,\gamma_0=\mathrm{ind}_g a$，则对任意的 $\gamma_1,g^{\gamma_0}\equiv g^{\gamma_1}\pmod m$ 与 $\gamma_0\equiv\gamma_1\pmod{\varphi(m)}$ 是等价的.

证明 由原根的定义及定理 1 的推论 2 得出.

定理 8 下面的结论成立：

(i) $\mathrm{ind}(ab)\equiv\mathrm{ind}a+\mathrm{ind}b\pmod{\varphi(m)}$；

(ii) $\mathrm{ind}_{g_1}g_2\cdot\mathrm{ind}_{g_2}g_1\equiv 1\pmod{\varphi(m)}$，其中 g_1 与 g_2 都是模 m 的原根；

(iii) $\mathrm{Ord}_m a=\dfrac{\varphi(m)}{(\mathrm{ind}_g a,\varphi(m))}$，

其中 g 是模 m 的原根.

证明 (i) 由定理 7 得出.

(ii) 设 $\gamma_1=\mathrm{ind}g_1g_2$, $\gamma_2=\mathrm{ind}g_2g_1$,则

$$g_1^{\gamma_1}\equiv g_2 \pmod{m},\quad g_2^{\gamma_2}\equiv g_1 \pmod{m},$$

因此,

$$g_1^{\gamma_1\gamma_2}\equiv g_1 \pmod{m}.$$

由此及定理 7 推出 $\gamma_1\gamma_2\equiv 1(\mathrm{mod}\varphi(m))$.

(iii) 由 $a=g^{\mathrm{ind}ga}$ 及定理 2 得出. □

推论 下面的结论成立:

(i) 对于模 m 的任意的原根 g,

$$\mathrm{ind}g1\equiv 0 \pmod{\varphi(m)};$$

(ii) 对于任意的正整数 k 及 $a,(a,m)=1$,

$$\mathrm{ind}a^k\equiv k\cdot\mathrm{ind}a \pmod{\varphi(m)}.$$

定理 9 设 g 是模 m 的原根,$(a,m)=1$,k 是正整数,则方程 $x^k\equiv a(\mathrm{mod}m)$有解的充分必要条件是$(k,\varphi(m))\mid\mathrm{ind}a$. 若有解,则解的个数是$(k,\varphi(m))$.

证明 设 $x\equiv g^y(\mathrm{mod}m)$,则 $x^k\equiv a(\mathrm{mod}m)$等价于 $ky\equiv\mathrm{ind}a$ $(\mathrm{mod}\varphi(m))$. 由定理 1.5.8 得证. □

定义 4 设 k 与 n 是正整数,$(a,n)=1$,若方程 $x^k\equiv a$ $(\mathrm{mod}n)$有解,则称 a 是模 n 的 k 次剩余.

定理 10 设 k 是正整数,整数 $n>1$,$(a,n)=1$,并且模 n 有原根,则 a 是模 n 的 k 次剩余的充分必要条件是

$$a^{\frac{\varphi(n)}{(\varphi(n),k)}}\equiv 1 \pmod{n}, \tag{11}$$

并且模 n 的 k 次剩余的个数是$\dfrac{\varphi(n)}{(\varphi(n),k)}$.

证明 设 g 是模 n 的原根,由

$$a^{\frac{\varphi(n)}{(\varphi(n),k)}}\equiv g^{\frac{\varphi(n)}{(\varphi(n),k)}\mathrm{ind}a} \pmod{n}$$

可知(11)式等价于

$$\varphi(n)\mid\frac{\varphi(n)}{(\varphi(n),k)}\cdot \mathrm{ind}a,$$

又等价于$(\varphi(n),k)\mid \mathrm{ind}a$,再由定理 9 证得定理的前一部分.

在模 n 的简化系 $g^0,g^1,\cdots,g^{\varphi(n)-1}$ 中,指标能被$(\varphi(n),k)$整除的恰有$\frac{\varphi(n)}{(\varphi(n),k)}$个,这证明了定理的后一部分. □

下面,给出一个计算指标的方法.

设 q 是奇素数,g 是模 q 的原根,并且

$$q-1=p_1^{a_1}\cdots p_k^{a_k}$$

是 $q-1$ 的标准分解式.

设$(a,q)=1$,为了求出 $x=\mathrm{ind}_g a$ 使得

$$g^x\equiv a \pmod{q}, \tag{12}$$

按以下步骤进行.

步骤 I 对于 $1\leqslant i\leqslant k$,记

$$x_i\equiv x \pmod{p_i^{a_i}},\quad 0\leqslant x_i<p_i^{a_i} \tag{13}$$

为了书写方便,记 p_i 为 p,a_i 为 α.

设

$$x_i=x_{i,0}+x_{i,1}p+\cdots+x_{i,\alpha-1}p^{\alpha-1},\quad 0\leqslant x_i<p. \tag{14}$$

令

$$\beta_i\equiv g^{\frac{q-1}{p}} \pmod{q},$$

则由(12)式,(14)式以及原根的性质,得到

$$a^{\frac{q-1}{p}}\equiv g^{x\frac{q-1}{p}}\equiv g^{x_i\frac{q-1}{p}}\equiv\beta_i^{x_{i,0}} \pmod{q}.$$

因此,将 $a^{\frac{q-1}{p}} \pmod{q}$ 与

$$1,\beta_i,\beta_i^2,\cdots,\beta_i^{p-1} \pmod{q} \tag{15}$$

比较，可以唯一地确定 $x_{i,0}$.

一般地，若 $x_{i,0}, x_{i,1}, \cdots, x_{i,l-1}$ 已经求出，如果 $\alpha=l$，则 x_i 已经求出；如果 $\alpha>l$，则由(12)式、(14)式以及原根的性质，得到

$$\begin{aligned}&(ag^{-x_{i,0}-x_{i,1}p-\cdots-x_{i,l-1}p^{l-1}})^{(q-1)/pl+1}\\ \equiv& g^{(x_i-x_{i,0}-x_{i,1}p-\cdots-x_{i,l-1}p^{l-1})(q-1)/p^{l+1}}\\ \equiv& g^{x_{i,l}(g-1)/p}\equiv\beta_i^{x_{i,l}} \pmod q.\end{aligned}$$

因此，将上式左端与(11)中的数比较，可以唯一地确定 $x_{i,l}$. 此处及以后，$b^{-k}(\mathrm{mod}q)$表示$(b^{-1})^k(\mathrm{mod}q)$，其中 b^{-1}是 b 对模 q 的乘法逆元素.

在逐次地求出 $x_{i,0}, \cdots, x_{i,a-1}$后，由(14)式就求出了 x_i. 显然，

$$a^{(q-1)/p^a}\equiv g^{x_i(q-1)/p^a} \pmod q. \tag{16}$$

步骤Ⅰ 求同余方程组

$$x\equiv x_i(\mathrm{mod}\,p_i^{a_i}),\quad 1\leqslant i\leqslant k \tag{17}$$

的解 x_0，$0\leqslant x_0<q-1$.

现在来证明 x_0使得(12)式成立.

由孙子定理(定理1.5.11)，同余方程组

$$x\equiv C_i(\mathrm{mod}\,p_i^{a_i}),\quad 1\leqslant i\leqslant k \tag{18}$$

的解是

$$x\equiv\sum_{i=1}^{k}\lambda_i C_i\frac{(q-1)}{p_i^{a_i}} \pmod{(q-1)}, \tag{19}$$

其中 $\lambda_i(1\leqslant i\leqslant k)$是与 $C_1, \cdots, C_k$ 无关的整数. 在(18)中若令 $C_i=1(1\leqslant i\leqslant k)$，则相应的(18)的解是

$$\sum_{i=1}^{k}\lambda_i(q-1)p_i^{-a_i}.$$

由于 $x\equiv1(\mathrm{mod}(q-1))$也是当 $C_1=\cdots=C_k=1$时，方程(18)的

解，所以，利用解的唯一性得出

$$\sum_{i=1}^{k}\lambda_i(q-1)p_i^{-a_i}\equiv 1 \pmod{(q-1)}. \tag{20}$$

在(19)式中令 $C_i=x_i(1\leqslant i\leqslant k)$，则得到方程组(17)的解

$$x_0\equiv\sum_{i=1}^{k}\lambda_i x_i(q-1)p_i^{-a_i} \pmod{(q-1)}. \tag{21}$$

由(16)，(20)及(21)式，得到

$$\begin{aligned} g^{x_0}&\equiv g^{\lambda_1 x_1(q-1)p_1^{-a_1}}\cdot g^{\lambda_2 x_2(q-1)p_2^{-a_2}}\cdot\cdots\cdot g^{\lambda_k x_k(q-1)p_k^{-a_k}}\\ &\equiv a^{\lambda_1(q-1)p_1^{-a_1}}\cdot a^{\lambda_2(q-1)p_2^{-a_2}}\cdots\cdot a^{\lambda_k(q-1)p_k^{-a_k}}\\ &\equiv a^{\lambda_1(q-1)p_1^{-a_1}+\lambda_2(q-1)p_2^{-a_2}+\cdots+\lambda_k(q-1)p_k^{-a_k}}\\ &\equiv a^1=a \pmod{q}, \end{aligned}$$

这就证明了 $x_0=\mathrm{ind}_g a$.

定理11 设 q 是奇素数，g 是模 q 的原根，并且 $q-1$的所有素因数不大于 $|P(\log q)|$，此处 $P(x)$是一个次数为 k 的多项式，则存在多项式时间算法，对于任何 $a,(a,q)=1$，可以求出 $\mathrm{ind}_g a$.

证明 前述求 $\mathrm{ind}_g a$ 的方法即是定理中的算法. 对于运算时间的估计，留作习题. □

习 题

1. 求模11的原根.

2. 求 $\mathrm{Ord}_{43}7$与 $\mathrm{Ord}_{13}10$.

3. 设 p 是奇素数，g 是模 p 的原根，证明

$$\mathrm{ind}_g(-1)=\frac{1}{2}(p-1).$$

4. 利用指标，解方程

(1) $x^{12}\equiv 16 \pmod{17}$

(2) $3^x \equiv 2 \pmod{23}$.

5. 设 $m>2$并且有原根存在，证明：

(1) a 是模 m 的二次剩余的充分必要条件是 $a^{\frac{1}{2}\varphi(m)} \equiv 1 \pmod{m}$；

(2) 若 a 是模 m 的二次剩余，则 $x^2 \equiv a \pmod{m}$ 恰有两个解；

(3) 模 m 恰有 $\frac{1}{2}\varphi(m)$ 个二次剩余.

6. 设 $n \geqslant 3$，证明 $\mathrm{Ord}_{2^n} 5 = 2^{n-2}$.

7. 对定理11中的算法所需要的计算时间做出估计.

第三节 连 分 数

定义 设 $a_i (i \geqslant 1)$是实数，若分数

$$a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \ddots + \cfrac{1}{a_n}}} \tag{1}$$

有意义，则称它为有限连分数，记为 $a_1 + \cfrac{1}{a_2 + a_3 + \cdots \cfrac{1}{a_n}}$，或$[a_1, \cdots, a_n]$，并称

$$\frac{p_k}{q_k} = [a_1, \cdots, a_k]$$

为它的第 $k(1 \leqslant k \leqslant n)$个渐近分数. 若极限

$$A = \lim_{n \to \infty} \frac{p_n}{q_n} = \lim_{n \to \infty} [a_1, \cdots, a_n]$$

存在有限，则称$[a_1, a_2, \cdots, a_n, \cdots]$是无限连分数，$A$ 是它的值，它是 A 的连分数.

如果 $a_1\in\boldsymbol{Z}, a_i\in\boldsymbol{N}(i\geqslant 2)$，则称$[a_1,\cdots,a_n,\cdots]$是无限简单连分数，若诸 a_i 中只有有限个不为0，则称$[a_1,\cdots,a_n]$是有限简单连分数.

注意，在本节中，$[a_1,\cdots,a_n]$表示(1)式中的连分数，而不是最小公倍数.

定理1 设$\frac{p_k}{q_k}(k\geqslant 1)$是$[a_1,a_2,\cdots,a_n,\cdots]$的第 k 个渐近分数，则

(i) $p_1=a_1, p_2=a_2a_1+1, p_k=a_kp_{k-1}+p_{k-2}, \quad (k\geqslant 3)$,

$q_1=1, q_2=a_2, \quad q_k=a_kq_{k-1}+q_{k-2}, \quad (k\geqslant 3)$;

(ii) $p_kq_{k-1}-p_{k-1}q_k=(-1)^k \quad (k\geqslant 2)$;

(iii) $p_kq_{k-2}-p_{k-2}q_k=(-1)^{k-1}a_k \quad (k\geqslant 3)$.

证明 (i) 对于 $k=1,2,3$，可以直接验证结论成立. 若对于小于 k 的正整数，结论成立，则

$$p_{k-1}=a_{k-1}p_{k-2}+p_{k-3}, q_{k-1}=a_{k-1}q_{k-2}+q_{k-3}, \tag{2}$$

并且

$$\frac{p_k}{q_k}=[a_1,a_2,\cdots,a_{k-1},a_k]=\left[a_1,a_2,\cdots,a_{k-2},a_{k-1}+\frac{1}{a_k}\right]$$

$$=\frac{\left(a_{k-1}+\frac{1}{a_k}\right)p_{k-2}+p_{k-3}}{\left(a_{k-1}+\frac{1}{a_k}\right)q_{k-2}+q_{k-3}}=\frac{a_k(a_{k-1}p_{k-2}+p_{k-3})+p_{k-2}}{a_k(a_{k-1}q_{k-2}+q_{k-3})+q_{k-2}},$$

由此及(2)式可知结论对于 k 成立. 由归纳法证得结论(i).

(ii) 当 $k=2$时，直接验证结论成立. 设结论对于 $k-1$成立，即 $p_{k-1}q_{k-2}-p_{k-2}q_{k-1}=(-1)^{k-1}$，则由结论(i)，

$$p_kq_{k-1}-p_{k-1}q_k=(a_kp_{k-1}+p_{k-2})q_{k-1}-p_{k-1}(a_kq_{k-1}-q_{k-2})$$

$$=p_{k-2}q_{k-1}-p_{k-1}q_{k-2}=(-1)^k.$$

由归纳法证得结论(ii).

(iii) 由(i)及(ii)，

$$p_kq_{k-2}-q_kp_{k-2}=(a_kp_{k-1}+p_{k-2})q_{k-2}-(a_kq_{k-1}+q_{k-2})p_{k-2}$$
$$=a_k(p_{k-1}q_{k-2}-p_{k-2}q_{k-1})=(-1)^{k-1}a_k. \quad \square$$

推论1 设$[a_1,\cdots,a_n,\cdots]$是简单连分数，$\frac{p_k}{q_k}$是它的第k个渐近分数，则

(i) 当$k\geqslant 3$时，$q_k\geqslant q_{k-1}+1$；$q_k\geqslant k-1$；

(ii) $\frac{p_{2(k-1)}}{q_{2(k-1)}}>\frac{p_{2k}}{q_{2k}}>\frac{p_{2k-1}}{q_{2k-1}}>\frac{p_{2k-3}}{q_{2k-3}}$；

(iii) 对于$k\geqslant 1$，$(p_k,q_k)=1$.

证明 结论(i)由定理1的结论(i)推出. 结论(iii)由定理1的结论(ii)推出. 另外，由定理1的结论(iii)，

$$\frac{p_{2k}}{q_{2k}}-\frac{p_{2(k-1)}}{q_{2(k-1)}}=\frac{(-1)^{2k-1}a_k}{q_{2k}q_{2(k-1)}}<0,$$

$$\frac{p_{2k-1}}{q_{2k-1}}-\frac{p_{2k-3}}{q_{2k-3}}=\frac{(-1)^{2k-2}a_{2k-1}}{q_{2k-1}q_{2k-3}}>0,$$

再由定理1的结论(ii)，

$$\frac{p_{2k}}{q_{2k}}-\frac{p_{2k-1}}{q_{2k-1}}=\frac{(-1)^{2k}}{q_{2k}q_{2k-1}}>0.$$

综合以上三个不等式，得出结论(ii). $\square$

推论2 任何简单连分数都表示一个实数.

证明 设简单连分数$[a_1,\cdots,a_n,\cdots]$的渐近分数列是$\left\{\frac{p_k}{q_k}\right\}$，则由推论2可知，$\left\{\frac{p_{2k-1}}{q_{2k-1}}\right\}$是一个有界递增数列，$\left\{\frac{p_{2k}}{q_{2k}}\right\}$是有界递减数列，并且

$$0<\frac{p_{2k}}{q_{2k}}-\frac{p_{2k-1}}{q_{2k-1}}=\frac{1}{q_{2k}q_{2k-1}}\leqslant\frac{1}{(2k-1)(2k-2)}\to 0 \quad (k\to\infty),$$

因此极限$\lim\limits_{k\to\infty}\frac{p_k}{q_k}$存在有限，即$[a_1,\cdots,a_n,\cdots]$表示一个实数. $\square$

定理2 α 是有理数的充分必要条件，是它可以表示为有限简单连分数.

证明 充分性是显然的. 下面证明必要性.

设有理数 $\alpha=\frac{c}{b}$，$b>0$，则由带余数除法得到

$$\frac{c}{b}=a_1+\frac{r_1}{b},\quad 0<r_1<b,$$

$$\frac{b}{r_1}=a_2+\frac{r_2}{r_1},\quad 0<r_2<r_1,\quad a_2\geqslant 1,$$

……

$$\frac{r_{n-3}}{r_{n-2}}=a_{n-1}+\frac{r_{n-1}}{r_{n-2}},\quad 0<r_{n-1}<r_{n-2},a_{n-1}\geqslant 1$$

$$\frac{r_{n-2}}{r_{n-1}}=a_n,\quad a_n>1.$$

由于 $b>r_1>\cdots>r_{n-1}$，所以 n 是有限数，因此必有

$$\alpha=\frac{c}{b}=[a_1,\cdots,a_n].\qquad \square$$

注 由于 $[a_1,\cdots,a_n]=[a_1,\cdots,a_n-1,1]$，所以每个有理数有两种表示为简单连分数的方式. 但是，若简单连分数

$$[a_1,\cdots,a_n]=[b_1,\cdots,b_m],\quad a_n>1,b_m>1,$$

则 $m=n,a_i=b_i,(1\leqslant i\leqslant n)$.

定理3 设 α 是实无理数，则可以唯一地用简单连分数表示.

证明 首先注意，由定理2，表示 α 的简单连分数必是无限连分数.

记

$$\alpha=a_1+\frac{1}{\alpha_1},\quad a_1=[\alpha],\quad \alpha_1=\frac{1}{\alpha-[\alpha]}(>1),$$

$$\alpha_1=a_2+\frac{1}{\alpha_2},\quad a_2=[\alpha_1],\quad \alpha_2=\frac{1}{\alpha_1-[\alpha_1]}(>1),$$

…

$$\alpha_{k-1}=a_k+\frac{1}{\alpha_k},a_k=[\alpha_{k-1}],\alpha_k=\frac{1}{\alpha_{k-1}-[\alpha_{k-1}]}(>1),$$

则 $\alpha=[a_1,\ a_2,\ \cdots,\ a_k,\ \alpha_k]$，并且，由定理1，

$$\alpha=\frac{\alpha_1 a_1+1}{\alpha_1}=\frac{\alpha_k p_k+p_{k-1}}{\alpha_k q_k+q_{k-1}},\quad k\geqslant 2,$$

以及

$$\alpha-\frac{p_k}{q_k}=\frac{\alpha_k p_k+p_{k-1}}{\alpha_k q_k+q_{k-1}}-\frac{p_k}{q_k}=\frac{(-1)^{k-1}}{q_k(\alpha_k q_k+q_{k-1})}. \tag{3}$$

再由定理1的推论1，得到

$$\left|\alpha-\frac{p_k}{q_k}\right|<\frac{1}{k(k-1)}=o\ (1)\qquad (k\to\infty),$$

即 $\lim\limits_{k\to\infty}\frac{p_k}{q_k}=\alpha.$

下面证明表示方法是唯一的．设 α 有两种表示方法，即

$$\alpha=[a_1,\ a_2,\ \cdots,\ a_k,\ \cdots]=[b_1,\ b_2,\ \cdots,\ b_k,\ \cdots],$$

记 $\alpha_k=[a_{k+1},\ a_{k+2},\ \cdots,\ \cdots]$，$\beta_k=[b_{k+1},\ b_{k+2},\ \cdots]$，由于 α 的两种表示都必定是无限简单连分数，所以 $\alpha_k>1$，$\beta_k>1$ $(k\geqslant 1)$.

显然 $a_1=[\alpha]=b_1$，$\alpha_1=\beta_1$.

设 $a_i=b_i$ 及 $\alpha_i=\beta_i$ 对于 $1\leqslant i\leqslant k$ 成立，则由 $\alpha_k=\beta_k$ 又得到 $a_{k+1}=b_{k+1}$. 唯一性由归纳法得证. □

推论 存在 δ_k 与 η_k，$0<\delta_k,\ \eta_k<1$，使得

$$\alpha-\frac{p_k}{q_k}=\frac{(-1)^{k-1}\delta_k}{q_k q_{k+1}},\quad \alpha-\frac{p_k}{q_k}=\frac{(-1)^{k-1}\eta_k}{q_k^2}.$$

证明 因为 $\alpha_k>a_{k+1}$，所以 $0<\frac{1}{\alpha_k q_k+q_{k-1}}<\frac{1}{q_{k+1}}<\frac{1}{q_k}$，由此

及（3）式得证. □

注 由推论可知，α 总是位于它的两个相邻的渐近分数之间.

以下均简称简单连分数为连分数.

定理4 设 α 是实数，$\frac{p_k}{q_k}$ 是它的连分数的第 k 个渐近分数，则对于任何整数 p，q，$0<q\leqslant q_k$，有

$$\left|\alpha-\frac{p_k}{q_k}\right|\leqslant\left|\alpha-\frac{p}{q}\right|.$$

证明 不妨设 $\alpha\neq\frac{p_k}{q_k}$，于是 α 有第 $k+1$ 个渐近分数 $\frac{p_{k+1}}{q_{k+1}}$，并且不妨设

$$\frac{p_k}{q_k}<\frac{p_{k+1}}{q_{k+1}}, \tag{4}$$

（否则，可用同样方法证明）.

首先证明，若 $0<q\leqslant q_k$，则

$$\frac{p}{q}\notin\left(\frac{p_k}{q_k},\ \frac{p_{k+1}}{q_{k+1}}\right]. \tag{5}$$

事实上，由定理1的推论1，$q\leqslant q_k<q_{k+1}$，并且 $\frac{p_{k+1}}{q_{k+1}}$ 是既约分数，

因此，若（5）式不成立，则必是 $\frac{p_k}{q_k}<\frac{p}{q}<\frac{p_{k+1}}{q_{k+1}}$，于是

$$\frac{p}{q}-\frac{p_k}{q_k}=\frac{pq_k-qp_k}{qq_k}\geqslant\frac{1}{qq_k},\quad \frac{p_{k+1}}{q_{k+1}}-\frac{p}{q}\geqslant\frac{1}{qq_{k+1}},$$

因此，

$$\frac{p_{k+1}}{q_{k+1}}-\frac{p_k}{q_k}\geqslant\frac{1}{qq_k}+\frac{1}{qq_{k+1}}>\frac{1}{q_kq_{k+1}},$$

这与定理3的推论矛盾. 因此，（5）式成立，即

$$\frac{p}{q}\leqslant\frac{p_k}{q_k}\text{或}\frac{p_{k+1}}{q_{k+1}}<\frac{p}{q} \tag{6}$$

成立.

另一方面，由（4）式及定理3的推论，推出

$$\frac{p_k}{q_k}<\alpha\leqslant\frac{p_{k+1}}{q_{k+1}},$$

因此，若（6）式中的第一个不等式成立，则定理结论得证. 若（6）式中的第二个不等式成立，则由

$$\left|\alpha-\frac{p}{q}\right|\geqslant\left|\frac{p_{k+1}}{q_{k+1}}-\frac{p}{q}\right|\geqslant\frac{1}{qq_{k+1}}\geqslant\frac{1}{q_kq_{k+1}}$$

及定理3的推论，推出定理结论. □

定理5 设实数 $\alpha(>1)$ 的渐近分数列是 $\frac{p_k}{q_k}(k\geqslant1)$，则

$$|p_k^2-\alpha^2q_k^2|<2\alpha,k=1,2\cdots.$$

证明 由定理3的推论，α 总是位于 $\frac{p_k}{q_k}$ 与 $\frac{p_{k+1}}{q_{k+1}}$ 之间，并且

$$\begin{aligned}|p_k^2-\alpha^2q_k^2|&=q_k^2\cdot\left|\frac{p_k}{q_k}-\alpha\right|\cdot\left|\frac{p_k}{q_k}+\alpha\right|\\&<q_k^2\cdot\frac{1}{q_kq_{k+1}}\cdot\left(2\alpha+\left|\frac{p_k}{q_k}-\alpha\right|\right)\\&\leqslant\frac{q_k}{q_{k+1}}\left(2\alpha+\frac{1}{q_kq_{k+1}}\right)\\&=2\alpha-\frac{q_{k+1}-q_k}{q_{k+1}}\cdot2\alpha+\frac{1}{q_{k+1}^2}\\&=2\alpha-2\alpha\left(\frac{q_{k+1}-q_k}{q_{k+1}}-\frac{1}{2\alpha q_{k+1}^2}\right)<2\alpha.\end{aligned}$$ □

推论 设 n 是正整数，并且 n 不是完全平方数. 又设 $\sqrt{n}$ 的渐近分数列是 $\frac{p_k}{q_k}(k=1,2,\cdots)$，则 p_k^2 对于模 n 的绝对最小剩余小于 $2\sqrt{n}$.

证明 在定理5中取 $\alpha=\sqrt{n}$. □

定理6 设实无理数 α 的渐近分数列是 $\left\{\frac{p_k}{q_k}\right\}(k=1,2,\cdots)$，则

(i) 在任何两个连续的渐近分数中，至少有一个 $\frac{p}{q}$ 使得

$$\left|\alpha-\frac{p}{q}\right|<\frac{1}{2q^2}; \tag{7}$$

(ii) 在任何三个连续的渐近分数中，至少有一个 $\frac{p}{q}$ 使得

$$\left|\alpha-\frac{p}{q}\right|<\frac{1}{\sqrt{5}\,q^2}. \tag{8}$$

证明 (i) 若定理结论不成立，则由定理3的推论及定理1，得到

$$\frac{1}{q_kq_{k+1}}=\left|\frac{p_{k+1}}{q_{k+1}}-\frac{p_k}{q_k}\right|=\left|\frac{p_{k+1}}{q_{k+1}}-\alpha\right|+\left|\alpha-\frac{p_k}{q_k}\right|$$

$$\geqslant\frac{1}{2q_k^2}+\frac{1}{2q_{k+1}^2}>\frac{1}{q_kq_{k+1}},$$

这是不可能的.

(ii) 设 α 的三个渐近分数 $\frac{p_i}{q_i}(i=k-1,k,k+1)$ 都不使(8)式成立，那么，由定理3的推论及定理1，得到

$$\frac{1}{q_kq_{k+1}}=\left|\frac{p_{k+1}}{q_{k+1}}-\frac{p_k}{q_k}\right|=\left|\frac{p_{k+1}}{q_{k+1}}-\alpha\right|+\left|\alpha-\frac{p_k}{q_k}\right|$$

$$\geqslant\frac{1}{\sqrt{5}}\left(\frac{1}{q_k^2}+\frac{1}{q_{k+1}^2}\right),$$

即

$$\frac{q_{k+1}}{q_k}+\frac{q_k}{q_{k+1}}<\sqrt{5}, \tag{9}$$

其中删去了等号，因为 $\sqrt{5}$ 是无理数，等号不可能成立. 同样地，又有

$$\frac{q_k}{q_{k-1}}+\frac{q_{k-1}}{q_k}<\sqrt{5}. \tag{10}$$

利用一元二次函数的性质可知，若 $y=x+\frac{1}{x}<\sqrt{5}$，且 $x>1$，则必是 $x<\frac{1}{2}(1+\sqrt{5})$，因此，由(9)式与(10)式得到

$$\frac{q_{k+1}}{q_k}<\frac{1}{2}(1+\sqrt{5}),\frac{q_{k-1}}{q_k}>\left(\frac{1}{2}(1+\sqrt{5})\right)^{-1}=\frac{1}{2}(\sqrt{5}-1)$$

$$\frac{q_{k+1}-q_{k-1}}{q_k}<\frac{1}{2}(\sqrt{5}+1)-\frac{1}{2}(\sqrt{5}-1)=1,$$

$$q_{k+1}<q_k+q_{k-1},$$

这与定理1的结论(i)矛盾. □

例1 求出 $\frac{173}{55}$ 的连分数.

解 利用定理2的证明方法，有

$$\frac{173}{55}=3+\frac{8}{55};\frac{55}{8}=6+\frac{7}{8};\frac{8}{7}=1+\frac{1}{7},$$

因此，

$$\frac{173}{55}=[3,6,1,7].$$

例2 证明：若 $\lambda>\sqrt{5}$，则存在实数 α，使得只有有限多个既约分数 $\frac{p}{q}$ 满足不等式

$$\left|\alpha-\frac{p}{q}\right|<\frac{1}{\lambda q^2}.$$

解 取 $\alpha=\frac{1}{2}(\sqrt{5}-1)$，若有无穷多个 $\frac{p}{q}$，使得

$$\frac{1}{2}(\sqrt{5}-1)=\frac{p}{q}+\frac{\delta}{q^2},|\delta|<\frac{1}{\lambda}<\frac{1}{\sqrt{5}},$$

则

$$\frac{\delta}{q}-\frac{1}{2}\sqrt{5}\,q=-\frac{1}{2}q-p.$$

将上式两边平方，得到

$$\frac{\delta^2}{q^2}-\sqrt{5}\,\delta=\left(\frac{1}{2}q+p\right)^2-\frac{5}{4}q^2=pq-q^2+p^2.$$

当 q 充分大时，上式左端的绝对值小于1，因此，对于充分大的 q，有 $pq-q^2+p^2=0$，即 $(2p+q)^2=5q^2$，这是不可能的.

注 例2说明，(8)式中的系数 $\sqrt{5}$ 不可能再小了.

习　题

1. 求出 $\frac{1173}{48}$ 的连分数.
2. 求出 $\sqrt{2}$ 的连分数的前面四个渐近分数.
3. 求 $\alpha=[2,1,2,1,2,1,\cdots]$ 所满足的整系数方程。

第四节　判定素性的概率算法

对于给定的奇数，确切地判断它是否素数，一般地，是很困难的. 本节介绍几个判定素性(即，整数是否素数这一性质)的概率算法，使用它们判定给出的奇数的素性时，结论错误的概率是很小的.

定义1　设 n 是奇合数，$(b,n)=1$. 若

$$b^{n-1}\equiv 1 \pmod{n}, \tag{1}$$

则称 n 是对基 b 的伪素数.

定理1　设 n 是奇合数.

(i) 若 $(b,n)=1$，则 n 是对基 b 的伪素数的充要条件是 b 对模 n 的指数整除 $n-1$；

(ii) 设 n 分别是对基 b_1 和对基 b_2 的伪素数，则 n 也是对基 b_1b_2，$b_1b_2^{-1}$ 的伪素数，此处 b_2^{-1} 是 b_2 对模 n 的乘法逆元素；

(iii) 若存在 $b\in(\boldsymbol{Z}/n\boldsymbol{Z})^*$ 使得(1)式不成立，则在 $(\boldsymbol{Z}/n\boldsymbol{Z})^*$

中至少有一半的数 b 使得(1)式不成立.

证明 (i) 由定理2.1推出.

(ii) 由同余式的基本性质推出.

(iii) 设 $b_1,\cdots,b_k$ 是$(Z/nZ)^*$中所有的使(1)式成立的不同的数. 由(ii)可知,数 $bb_i(1\leqslant i\leqslant k)$不使(1)式成立,而且,由于 $b_i\not\equiv b_j(\mathrm{mod}n)(i\neq j)$,所以 $bb_i\not\equiv bb_j(\mathrm{mod}n)$,即 $bb_1,\cdots,bb_k$ 是互不相同的. 因此,使(1)式不成立的数的个数至少是 k 个. 由此得出结论(iii). □

定义2 设 n 是合数,若对任何 $b\in(Z/nZ)^*$,(1)式都成立,则称 n 是 Carmichael 数.

定理2 设 n 是奇合数,

(i) 若 n 被某个平方数整除,则 n 不是 Carmichael 数;

(ii) 若 n 没有平方因数,则 n 是 Carmichael 数的充要条件是由 $p|n$ 可以导出 $p-1|n-1$.

证明 (i) 设有素数 $p\neq 2,p^\alpha|n,p^{\alpha+1}\nmid n,\ \alpha\geqslant 2,g$ 是模 p^α 的原根,则

$$g^{p^{\alpha-1}(p-1)}\equiv 1\pmod{p^\alpha}.$$

记 $n=p^\alpha n'$,并且以

$$b\equiv g\pmod{p^\alpha},\quad b\equiv 1\pmod{n'}$$

确定 b,则 b 也是 p^α 的原根,$(b,n)=1$. 若 n 是对基 b 的伪素数,则(1)式成立,从而有 $b^{n-1}\equiv 1(\mathrm{mod}p^\alpha)$,因此,由定理2.1得到

$$p^{\alpha-1}(p-1)|n-1,$$

于是 $p^{\alpha-1}|n-1$,这与 $p^\alpha|n$ 矛盾,所以,b 不使(1)式成立,从而,n 不是 Carmichael 数.

(ii) 若 $n=p_1\cdots p_k$,而且 $p_i-1|n-1(1\leqslant i\leqslant k)$,其中诸 p_i 是互不相同的素数. 设 b 是任意整数,$(b,n)=1$,则对于$1\leqslant i\leqslant$

k,由 Fermat 定理得到,对于$1\leqslant i\leqslant k$,

$$b^{p_i-1}\equiv 1 \pmod{p_i},\quad b^{n-1}\equiv 1 \pmod{p_i},$$

因此

$$b^{n-1}\equiv 1 \pmod{n},$$

即 n 是对基 b 的伪素数. 由于 b 是任意取的,所以 n 是 Carmichael 数.

若 n 是 Carmichael 数,则用证明(i)的方法可得到 $p_i-1\mid n-1$对任意的 $p_i\mid n$ 成立. □

推论1 任何 Carmichael 数至少有三个不同的素因数.

证明 由定理2,只需证明,若 p 与 q 是不同的素数,则 $n=pq$ 不是 Carmichael 数.

设 n 是 Carmichael 数. 不妨设 $p<q$. 利用对定理2结论(i)的证明方法,可推出 $q-1\mid n-1$,由此及

$$n-1=pq-1\equiv p-1 \pmod{q-1}$$

得到 $q-1\mid p-1$,这与 $p<q$ 矛盾. □

推论2 设 r,p,q 是互不相同的素数,则当 r 固定时,形如 rpq 的 Carmichael 数的个数有限.

证明 不妨只考虑 $p>q$ 的情形.

若 pqr 是 Carmichael 数,用证明定理2的方法,可以得到$(p-1)\mid(rpq-1)$,$(q-1)\mid(rpq-1)$,因此,

$$0\equiv rpq-1\equiv rq-1 \pmod{p-1},$$

$$0\equiv rpq-1\equiv rp-1 \pmod{q-1}.$$

所以,存在某个整数 a,$1<a<r$,使得

$$rp-1=a(q-1),aq=rp+a-1, \tag{2}$$

并且

$$0\equiv a(rq-1)=raq-a=r(rp+a-1)-a$$

$$\equiv r^2 + ra - r - a = (r-1)(a+r) \pmod{p-1}. \quad (3)$$

当 r 固定时，a 的取值至多是 $r-1$个；由(3)式，p 的取值至多是$2r^2$个；由(2)式，q 的取值也是有限多个. □

定义3 设 n 是奇合数，$(b,n)=1$，若

$$b^{\frac{n-1}{2}} \equiv \left(\frac{b}{n}\right) \pmod{n}, \quad (4)$$

其中$\left(\frac{b}{n}\right)$是 Jaccobi 符号，则称 n 是对基 b 的 Euler 型伪素数.

由 Jacobi 符号的性质可知，Euler 型伪素数必是伪素数.

对于任何奇数 n，当 $b=\pm 1$时，(4)式都成立. 以后，不考虑这两种平凡情形.

定理3 设 n 是奇合数，则在$(Z/nZ)^*$中至少有一半的整数 b 使(4)式不成立.

证明 设 $b' \in (Z/nZ)^*$ 不使(4)式成立，并且 $b_1, \cdots, b_k \in (Z/nZ)^*$ 是使(4)式成立的所有整数. 由 Jacobi 符号的性质可知，对于$1 \leqslant i \leqslant k$，

$$\left(\frac{b'b_i}{n}\right) = \left(\frac{b'}{n}\right)\left(\frac{b_i}{n}\right) \not\equiv (b_i b)^{\frac{n-1}{2}} \pmod{n},$$

即 $b'b_i$ 不使(4)式成立. 容易证明，当 $i \neq j$ 时，$b'b_i$ 与 $b'b_j$ 是$(Z/nZ)^*$中的不同元素，所以定理结论成立.

关于 b' 的存在性，已在例1.6中证明. □

定义4 设 n 是奇合数，$n-1=2^s t$，$2 \nmid t$，又设 $b \in (Z/nZ)^*$. 若

$$b^t \equiv 1 \pmod{n}, \text{或 } b^{2^r t} \equiv -1 \pmod{n} \quad (5)$$

对于某个 r，$0 \leqslant r < s$ 成立，则称 n 是对基 b 的强伪素数.

定理4 若 n≡3(mod4)，则 n 是对基 b 的强伪素数的充要条件是，n 是对基 b 的 Euler 型伪素数.

证明 因为 $n\equiv 3(\mathrm{mod}4)$，所以$2\nmid\frac{n-1}{2}$，因此，n 是对基 b 的强伪素数的充要条件是

$$b^{\frac{n-1}{2}}\equiv\pm 1 \quad (\mathrm{mod}n). \tag{6}$$

若 n 是对基 b 的 Euler 型伪素数，上式显然成立.

若(6)式成立，则由 $n\equiv 3(\mathrm{mod}4)$及 Jacobi 符号的性质，得到$\left(\frac{\pm 1}{n}\right)=\pm 1$，于是

$$\left(\frac{b}{n}\right)=\left(\frac{b\cdot(b^2)^{\frac{n-3}{4}}}{n}\right)=\left(\frac{b^{\frac{n-1}{2}}}{n}\right)\equiv b^{\frac{n-1}{2}} \quad (\mathrm{mod}n),$$

即 n 是对基 b 的 Euler 型伪素数. □

定理5 设 n 是对基 b 的强伪素数，则它必是对基 b 的 Euler 型伪素数.

证明 记 $n-1=2^st$，$2\nmid t$. 则(5)式成立.

考虑以下三种情况.

(i) $b^t\equiv 1(\mathrm{mod}n)$.

此时 $b^{\frac{n-1}{2}}\equiv 1(\mathrm{mod}n)$，并且

$$1=\left(\frac{1}{n}\right)=\left(\frac{b^t}{n}\right)=\left(\frac{b}{n}\right)^t.$$

因为 t 是奇数，所以$\left(\frac{b}{n}\right)=1$，因此 n 是对基 b 的 Euler 型伪素数.

(ii) $b^{\frac{n-1}{2}}\equiv -1(\mathrm{mod}n)$.

对于 n 的任一素因数 p，记

$$p-1=2^\alpha\beta,\ 2\nmid\beta. \tag{7}$$

首先，证明 $\alpha\geqslant s$，并且

$$\left(\frac{b}{p}\right)=\begin{cases}-1,\text{若 }\alpha=s,\\ 1,\text{若 }\alpha>s.\end{cases} \tag{8}$$

事实上，由假设，即

$$b^{\frac{n-1}{2}}=b^{2^{s-1}t}\equiv -1(\mathrm{mod}n)$$

及 $p|n$ 得到

$$(b^{2^{s-1}\beta})^t\equiv -1 \pmod{p}. \tag{9}$$

因此，若 $\alpha<s$，则

$$b^{p-1}=b^{2^{\alpha-1}\beta}\not\equiv 1 \pmod{p},$$

这与 Fermat 定理矛盾，故必是 $\alpha\geqslant s$.

当 $\alpha=s$，由(9)式得到

$$-1\equiv b^{\frac{p-1}{2}}\equiv\left(\frac{b}{p}\right) \pmod{p}.$$

当 $\alpha>s$ 时，由(9)式得到

$$\left(\frac{b}{p}\right)\equiv b^{\frac{p-1}{2}}=(b^{2^{s-1}\beta})^{2^{\alpha-s}}\equiv 1 \pmod{p}.$$

这就证明了(8)式.

其次，设 $n=\prod p$，其中 p 是素数，并且有 k 个 p 所对应的(7)式中的 $\alpha=s$. 由(8)式可知，

$$\left(\frac{b}{n}\right)=\prod\left(\frac{b}{p}\right)=(-1)^k. \tag{10}$$

由于

$$p\equiv\begin{cases}1 & (\mathrm{mod}2^{s+1})，当\ \alpha>s，\\ 1+2^s & (\mathrm{mod}2^{s+1})，当\ \alpha=s，\end{cases}$$

所以，由 $2\nmid t$ 推出

$$\begin{aligned}1+2^s\equiv 1+2^st &\equiv \prod p\equiv(1+2^s)^k\\ &\equiv 1+k\cdot 2^s \pmod{2^{s+1}},\end{aligned} \tag{11}$$

因此，$2\nmid k$，再利用(10)式，得出 $\left(\frac{b}{n}\right)=-1$，即(4)式成立.

(iii) $b^{2^{r-1}t}\equiv -1 \pmod{n}$，$0<r<s$.

此时 $b^{\frac{n-1}{2}}\equiv 1 \pmod{n}$.

对任意的 n 的素因数 p，记 $p-1=2^{\alpha}\beta, 2\nmid\beta$，类似于在(ii)中的推理，可以证明 $\alpha\geqslant r$，并且

$$\left(\frac{b}{p}\right)=\begin{cases}-1, & \text{当 } \alpha=r\\ 1, & \text{当 } \alpha>r.\end{cases}$$

用 $\mathrm{mod}2^{r+1}$ 代替(ii)的推理中的 $\mathrm{mod}2^{s+1}$，类似地，可以证出

$$\left(\frac{b}{n}\right)=1\equiv b^{\frac{n-1}{2}} \pmod{n}. \qquad \square$$

定理6 设 n 是奇合数，$0<b<n$，$(b,n)=1$，则 n 是对基 b 的强伪素数的概率不大于 $\frac{1}{4}$.

证明 分以下几种情形.

(i) n 有平方因数 p^2，p 是素数.

记 $n=p^2n'$，则有

$$b=mp^2+b',\ 0<b'<p^2,\ 0\leqslant m<n'-1.$$

因此，只需证明，对于每个固定的 m，b' 能使 n 对于基 b 是强伪素数的概率 $\Delta\leqslant\frac{1}{4}$.

不妨设 $m=0$，此时 $0<b<p^2$，$(b,n)=1$.

若 n 是对基 b 的强伪素数，则也是对基 b 的伪素数，因此，

$$b^{n-1}\equiv 1 \pmod{p^2}. \tag{12}$$

由定理2.9，这个同余方程的解的个数是 $d=(n-1,p(p-1))$.

因为 $p\nmid n-1$，所以 $d\leqslant p-1$，于是

$$\Delta\leqslant\frac{p-1}{p^2-1}=\frac{1}{p+1}\leqslant\frac{1}{4}.$$

(ii) 设 $n=p_1\cdots p_k$ 是 k 个不同的素数之积.

记

$$p_i-1=2^{\alpha_i}\beta_i,\quad 2\nmid\beta_i,\quad 1\leqslant i\leqslant k.$$

若 n 是对基 b 的强伪素数，则同余方程组

$$b^t\equiv 1 \pmod{p_i},\quad 1\leqslant i\leqslant k \tag{13}$$

与

$$b^{2^r t}\equiv -1 \pmod{p_i},\quad 1\leqslant i\leqslant k \tag{14}$$

中至少有一组成立，其中$0\leqslant r<s$，s 见于定义4.

若方程组(13)成立，由定理2.9，对于模 p_i，同余方程组(13)中的每个方程的解至多是 $d_i=(t,p_i-1)=(t,\beta_i)$个. 利用孙子定理易知，对于模 n，同余方程组(13)的解的个数不超过 $d_1\cdot d_2\cdots d_k\leqslant\beta_1\beta_2\cdots\beta_k$.

若方程组(14)成立，由定理2.9，容易推出，仅当 $r<\alpha_i$ 时，(14)中的同余方程有$2^r(t,\beta_i)$个解，因此，对于模 n，同余方程组(14)的解的个数不超过(设 $\alpha_0=\min(\alpha_1,\cdots,\alpha_k)$)

$$\sum_{r=0}^{\alpha_0-1}2^{kr}d_1\cdots d_k\leqslant\prod_{i=1}^{k}\beta_i\sum_{r=0}^{\alpha_0-1}2^{kr}.$$

综合以上结果得到，对于$0<b<n$，n 是对基 b 的强伪素数的概率

$$\Delta\leqslant\frac{1}{n-1}\prod_{i=1}^{k}\beta_i\left(1+\sum_{r=0}^{\alpha_0-1}2^{kr}\right).$$

由此及

$$n-1\geqslant\varphi(n)=\prod_{i=1}^{k}(p_i-1)=2^{\alpha_1+\cdots+\alpha_k}\prod_{i=1}^{k}\beta_i,$$

得到

$$\Delta\leqslant 2^{-\alpha_1-\cdots-\alpha_k}\left(1+\sum_{r=0}^{\alpha_0-1}2^{kr}\right). \tag{15}$$

不妨设 $\alpha_1=\min(\alpha_1,\cdots,\alpha_n)$.

当 $k\geqslant 3$时，由(15)式推出

$$\Delta \leqslant 2^{-ka_1}\left(1+\frac{2^{ka_1}-1}{2^k-1}\right)=2^{-ka_1}\frac{2^k-2}{2^k-1}+\frac{1}{2^k-1}$$

$$\leqslant 2^{-k}\left(1+\frac{2^k-1}{2^k-1}\right)=2^{1-k}\leqslant\frac{1}{4}.$$

当 $k=2$时，分两种情形考虑.

(a) $\alpha_1<\alpha_2$. 由(15)式得到

$$\Delta\leqslant 2^{-2a_1-1}\left(1+\frac{4^{a_1}-1}{4-1}\right)\leqslant\frac{1}{3}\cdot 2^{-2a_1}+\frac{1}{6}\leqslant\frac{1}{4}.$$

(b) $\alpha_1=\alpha_2$. 此时，不可能同时有 $d_1=\beta_1$与 $d_2=\beta_2$成立，否则，由

$$d_1=(t,\beta_1)=\beta_1, d_2=(t,\beta_2)=\beta_2,$$

$\beta_1\mid t$，以及

$$n-1=2^st=p_1p_2-1\equiv p_2-1 \pmod{p_1-1}$$

得到

$$2^st\equiv p_2-1 \pmod{\beta_1},\quad \beta_1\mid p_2-1, \beta_1\mid\beta_2.$$

同理可以得到 $\beta_2\mid\beta_1$，于是 $\beta_1=\beta_2$，这与 $p_1\neq p_2$相互矛盾.

这样，$d_1\neq\beta_1$或 $d_2\neq\beta_2$ 至少有一个成立. 因此，由于 β_1与 β_2都是奇数，又得到 $d_1d_2=(t,p_1)(t,p_2)\leqslant\frac{1}{3}\beta_1\beta_2$，所以同余方程组(13)和(14)的解的个数都不超过

$$\frac{1}{3}\beta_1\beta_2+\frac{1}{3}\beta_1\beta_2(1+2^2+\cdots+2^{2(\alpha_1-1)}).$$

由此及前面已有的推导，得到

$$\Delta\leqslant 2^{-\alpha_1-\alpha_2}\cdot\frac{1}{3}(1+1+2^2+\cdots+2^{2(\alpha_1-1)})$$

$$=4^{-\alpha_1}\cdot\frac{1}{3}\left(1+\frac{4^{\alpha_1}-1}{4-1}\right)<\frac{1}{4}.$$ □

利用定理3与定理6，容易证明，存在着判定整数的素性的算

法，它得到正确结论的概率是很大的.

定理7 对于给定的奇数 n，

(i) 随机地选取 b，$0<b<n$，$(b,n)=1$；

(ii) 计算 $\left(\frac{b}{n}\right)$ 与 $b^{\frac{n-1}{2}}(\mathrm{mod}n)$；

(iii) 若(4)式不成立，则 n 是合数；若(4)式成立，则重复步骤(i)与(ii).

在对 k 个不同的 b 值实行上述算法后，可以断定，n 是合数的概率不超过 2^{-k}.

定理8 对于给定的奇数 n，

(i) 随机地选取 b，$0<b<n$，$(b,n)=1$；

(ii) 计算 $b^t, b^{2t}, b^{2^2t}, \cdots, b^{2^{s-1}t}(\mathrm{mod}n)$，$s$ 与 t 见于定义4；

(iii) 若(5)式不成立，则 n 是合数；若(5)式成立，则重复步骤(i)与(ii).

在对 k 个不同的 b 值实行上述算法后，可以断定，n 是合数的概率不超过 4^{-k}.

以上两个定理的证明，留给读者.

注 使用定理8中的算法检验 n 是否素数时，一般地，并不需要使用太多的数 b. 例如，计算结果表明，在不超过 2.5×10^{10} 的正奇数中，只有 $n=3215031751$ 是对四个基(2,3,5,7)的强伪素数.

例1 设 p 与 $2p-1$ 都是素数，$n=p(2p-1)$，则使 n 是伪素数的基 b 的概率是 $\frac{1}{2}$.

证明 由

$$n-1=p(2p-1)-1\equiv0 \quad (\mathrm{mod}p-1)$$

及

$$n-1=p(2p-1)-1\equiv p-1 \pmod{2p-2}$$

可知

$$b^{n-1}\equiv 1 \pmod{p},$$

$$b^{n-1}\equiv b^{p-1}=b^{\frac{2p-1-1}{2}}\equiv\left(\frac{b}{2p-1}\right) \pmod{2p-1},$$

因此，$b^{n-1}\equiv 1(\bmod p(2p-1))$ 与 $\left(\frac{b}{2p-1}\right)=1$ 等价. 使 $\left(\frac{b}{2p-1}\right)=1$的数 b 出现的概率是$\frac{1}{2}$.

例2 若 n 是对基 b 的伪素数，$(b-1,n)=1$，则 $N=\frac{b^n-1}{b-1}$ 也是对基 b 的伪素数. 特别地，若 n 是对基2的伪素数，则2^n-1 也是对基2的伪素数.

证明 n 是对基 b 的伪素数，所以，n 是奇合数，并且$(b,n)=1$. 因为$2\nmid n$，所以

$$2\nmid N=\frac{b^n-1}{b-1}=b^{n-1}+b^{n-2}+\cdots+1.$$

此外，设 $n=kl$，$(k>1,l>1)$，则$2\nmid k$，$2\nmid l$，于是

$$N=\frac{b^{kl}-1}{b-1}=(b^{l-1}+\cdots+1)(b^{l(k-1)}+\cdots+1),$$

即 N 也是合数，所以 N 是奇合数.

在等式

$$N-1=\frac{b^n-1}{b-1}-1=b\cdot\frac{b^{n-1}-1}{b-1}$$

的右端，由伪素数的定义可知 $n\mid b^{n-1}-1$，由此及$(b,n)=(b-1,n)=1$，得到 $n\mid N-1$，再与

$$b^n-1=N(b-1)\equiv 0 \pmod{N}$$

联合，推出

$$b^n\equiv 1 \pmod{N},\quad b^{N-1}\equiv 1 \pmod{N},$$

即 N 是对基 b 的伪素数.

例3 设 $n=pq$ 是两个不同的奇素数之积，$d=(p-1,q-1)$. 证明：n 是对基 b 的伪素数的充要条件是：

$$b^d\equiv 1 \pmod{n}. \tag{16}$$

证明 设 n 是对基 b 的伪素数，即 $b^{n-1}\equiv 1(\mathrm{mod}n)$，则由

$$b^{n-1}\equiv 1 \pmod{p},$$

$$n-1=pq-1\equiv q-1 \pmod{p-1},$$

以及 Fermat 定理，得到

$$b^{q-1}\equiv 1 \pmod{p}, b^{p-1}\equiv 1 \pmod{p}. \tag{17}$$

利用引理1.5.1，得到

$$b^d\equiv 1 \pmod{p}.$$

同理可以证明

$$b^d\equiv 1 \pmod{q}.$$

将以上两式联合，得到(16)式. 必要性得证.

若(16)式成立，则由 $d\mid n-1=pq-1=(p-1)q+q-1$，可知 n 是对基 b 的伪素数. 充分性得证.

推论 若 $n=pq$ 是不同的奇素数之积，$d=(p-1,q-1)$，则有 d^2 个 $b\in(\mathbf{Z}/n\mathbf{Z})^*$，使得 n 对基 b 是伪素数.

证明 (16)式等价于同余方程组

$$\begin{cases} b^d\equiv 1 \pmod{p}. & (18)\\ b^d\equiv 1 \pmod{q}. & (19)\end{cases}$$

设 g 是模 p 的原根，$k=\mathrm{ind}gb$，则(18)式等价于

$$kd\equiv 0 \pmod{p-1},$$

它有 d 个对模 $p-1$ 不同余的解，即

$$k_i=i\cdot\frac{p-1}{d},\quad i=0,1,\cdots,d-1.$$

同理可以证明，(19)有 d 个对模 $q-1$ 不同余的解. 因此，由(18)与(19)所成的方程组的解的个数是 d^2. □

习　题

1. 证明定理7与定理8.

2. 证明3·11·17是最小的 Carmichael 数.

3. 证明：当 $b=2$，3或5时，有无穷多个对基 b 的伪素数.

4. 设整数 $b>1$，奇素数 p 不是数 b，$b-1$，或 $b+1$ 的因数. 记 $n=\dfrac{b^{2p}-1}{b^2-1}$. 证明：$n$ 是对基 b 的伪素数. 并且由此推出，对于任何基 b，有无穷多个对基 b 的伪素数.

5. 设 $n=p\ (2p-1)$，p 是奇素数. 证明：对于任意的 $b\in(\mathbf{Z}/n\mathbf{Z})^*$，$n$ 是对基 b 的 Euler 型伪素数的概率是 $\dfrac{1}{4}$.

6. 证明：若 n 是对基 b 的强伪素数，则它也是对基 b^k 的强伪素数，此处 k 是任意的正整数.

7. 证明：若 n 是对基2的伪素数，则 2^n-1 也是对基2的强伪素数.

8. 设 $n=p^\alpha$ 是奇素数 p 的幂，$\alpha>1$. 证明：n 是对基 b 的强伪素数的充分必要条件是，n 是对基 b 的伪素数.

第五节　因 数 分 解

在实际应用中，不但需要判断一个给定数是否素数，而且，当它是合数时，还需要知道它的因数. 在本节中，要研究因数分解问题.

由整数的素因数分解式容易证明下面的结论：若有整数 a，

b,使得

$$a^2\equiv b^2 \pmod{n},\quad a\not\equiv \pm b \pmod{n}, \tag{1}$$

则$(a+b,n)>1$,$(a-b,n)>1$,即可以求出 n 的至少一个真因数.

例如,由

$$118^2\equiv 5^2 \pmod{4633},\quad 118\not\equiv \pm 5 \pmod{4633},$$

可以求出4633的因数

$$(118+5,4633)=41 \text{与} (118-5,4633)=113.$$

一般地,当 n 较大时,找到满足(1)式的 a 与 b 并不容易.因此,需要将上述方法加以改进.为此,首先引进因数基的概念.

定义1 设数集 $B=\{p_1,\cdots,p_k\}$ 是 k 个互不相同的素数的集合,(p_1可能取值-1),则称 B 是一个因数基.此外,对于给定的正整数 n,若 b^2 对模 n 的绝对最小剩余可以表示成 B 中的数的乘积,则称 b 是 $B(n)$—数,在不致引起误会的情形,也简称为 B—数.

例1 对于 $n=73$,$B=\{2,3\}$,由

$$9^2\equiv 8=2^3 \pmod{73},$$

$$11^2\equiv 48=2^4\cdot 3 \pmod{73},$$

可知9与11都是 $B(73)$—数.

对于 $n=4633$,$B=\{-1,2,3\}$,由

$$67^2\equiv -144=-2^4\cdot 3^2 \pmod{4633},$$

$$68^2\equiv -9=-3^2 \pmod{4633},$$

$$69^2\equiv 128=2^7 \pmod{4633},$$

可知67,68,69都是 $B(4633)$—数.

定义2 以 $(Z/2Z)^h$ 表示所有向量$(\varepsilon_1,\cdots,\varepsilon_h)$的集合,其中 $\varepsilon_i=0$或$1(1\leqslant i\leqslant h)$.对于任何向量$(x_1,\cdots,x_h)\in Z^h$,若 $x_i\equiv$

$\varepsilon_i(\mathrm{mod}2)$ $(1\leqslant i\leqslant h)$，则称向量$(x_1,\cdots,x_h)$对模2与向量$(\varepsilon_1,\cdots,\varepsilon_h)$同余，记为

$$(x_1,\cdots,x_h)\equiv(\varepsilon_1,\cdots,\varepsilon_h)\quad(\mathrm{mod}2).$$

Fermat 分解因数法　对于给定的整数 n，按以下步骤求 n 的因数：

Ⅰ　选定因数基 $B=\{p_1,\cdots,p_h\}$，其中除 p_1 可以是 -1 外，$p_i(2\leqslant i\leqslant h)$是互不相同的素数；

Ⅱ　随机地选取 k 个 B—数 $b_i(1\leqslant i\leqslant k)$，设最小绝对剩余

$$a_i\equiv b_i^2(\mathrm{mod}n)=p_1^{\alpha_{i1}}p_2^{\alpha_{i2}}\cdots p_h^{\alpha_{ih}},\tag{2}$$

记

$$\bar{\alpha}_i=(\alpha_{i1},\cdots,\alpha_{ih}),\quad 1\leqslant i\leqslant k.$$

Ⅲ　选取适当的$\{\bar{\alpha}_{j1},\cdots,\bar{\alpha}_{jm}\}\subset\{\bar{\alpha}_1,\cdots,\bar{\alpha}_k\}(m\leqslant k)$，使得

$$\bar{\alpha}_{j1}+\cdots+\bar{\alpha}_{jm}\equiv(0,\cdots,0)\quad(\mathrm{mod}2).\tag{3}$$

为叙述方便，设 $m=k$，$\bar{\alpha}_{ji}=\bar{\alpha}_i(1\leqslant i\leqslant k)$，则由(2)式与(3)式可知，存在整数 $\beta_1,\cdots,\beta_k$，使得

$$\prod_{i=1}^{k}a_i\equiv\prod_{i=1}^{k}p_i^{\beta_i},2\mid\beta_i,1\leqslant i\leqslant k,$$

即

$$b^2=\Big(\prod_{i=1}^{k}b_i\Big)^2\equiv\prod_{i=1}^{k}p_i^{\beta_i}=c^2\quad(\mathrm{mod}n).\tag{4}$$

Ⅳ　若 $b\not\equiv\pm c(\mathrm{mod}n)$，则可得到 n 的真因数.

若 $b\equiv\pm c(\mathrm{mod}n)$，则重复上述步骤，直到可以求出 n 的真因数.

注1　由线性代数理论可知，当 $k\geqslant h+1$时，满足(3)式的$\bar{\varepsilon}_{j1},\cdots,\bar{\varepsilon}_{jm}$总是可以选出的.

注2　一般地，可以取因数基 B 为不超过 y 的全体素数的

集合，其中 y 是适当的数值. 此外，可以证明，使用 Fermat 分解因数法求 n 的真因数时，需要 $O(e^{c\sqrt{\log n\log\log n}})$ 次比特运算，此处 c 是常数.

引理1 设 $n=p_1^{a_1}\cdots p_r^{a_r}$，其中诸 p 是不同的素数，记同余方程

$$f(x)\equiv 0 \pmod{n}$$

的解的个数为 $\rho(f,n)$，其中 $f(x)$ 是整系数多项式，则

$$\rho(f,n)=\prod_{i=1}^{r}\rho(f,p_i^{a_i}).$$

证明 不妨设 $n=n_1n_2,(n_1,n_2)=1$.

设 $f(x)\equiv 0 \pmod{n_i}$ $(1\leqslant i\leqslant n)$对模 n_i 的不同余的解是

$$x\equiv a_{ij} \pmod{n_i},\quad 1\leqslant j\leqslant T_i=\rho(f,n_i).$$

由

$$f(x)\equiv 0 \pmod{n}\Leftrightarrow\begin{cases}f(x)\equiv 0 \pmod{n_1}\\ f(x)\equiv 0 \pmod{n_2},\end{cases}$$

及对于 $i=1,2$，有

$$f(x)\equiv 0 \pmod{n_i}\Leftrightarrow x\equiv a_{ij} \pmod{n_i},$$

其中$1\leqslant j\leqslant T_i$，因此，

$$f(x)\equiv 0 \pmod{n}\Leftrightarrow\begin{cases}x\equiv a_{1j} \pmod{n_1}\\ x\equiv a_{2k} \pmod{n_2},\end{cases}\tag{5}$$

其中$1\leqslant j\leqslant T_1,1\leqslant k\leqslant T_2$，即方程 $f(x)\equiv 0 \pmod{n}$ 等价于 T_1T_2 个形如(5)式中的一次同余方程组. 由孙子定理可知，方程组(5)有唯一解

$$x_{jk}\equiv n_2^{-1}n_2a_{1j}+n_1^{-1}n_1a_{2k} \pmod{n},\tag{6}$$

其中 n_1^{-1} 与 n_2^{-1} 分别是 n_1 对模 n_2 与 n_2 对模 n_1 的乘法逆元素. 由第一章第五节定理4，对于$1\leqslant j\leqslant n_1,1\leqslant k\leqslant n_2$，诸 x_{jk} 对模 n 是互不

同余的，因此，$\rho(f,n_1n_2)=\rho(f,n_1)\rho(f,n_2)$. □

定理1 设奇数 n 有 r 个不同的素因数，$(b,n)=1$，则同余方程

$$x^2\equiv b^2 \pmod{n}$$

有 2^r 个对模 n 不同余的解.

证明 由引理1，只需证明方程

$$x^2\equiv b^2 \pmod{p^a} \tag{7}$$

有两个解，其中 $p^a\|n$.

首先，方程

$$x^2\equiv b^2 \pmod{p}$$

有两个解，即 $x\equiv\pm b \pmod{p}$，由于 $(b,p)=1$，这两个解是不同的.

其次，方程

$$(x^2-b^2)'=2x\equiv 0 \pmod{p}$$

与方程(7)显然没有公共解. 因此，由定理1.5.15的推论，方程(7)有两个解. □

注 由定理1，对于由(4)式确定的数 b 与 c，同余式

$$b\equiv\pm c \pmod{n}$$

成立的概率是 $2\cdot\frac{1}{2^r}\leqslant\frac{1}{2}$，因此，在使用 Fermat 因数分解法时，若重复步骤 Ⅰ — Ⅲ k 次，那么，仍旧不能得到 n 的真因数的概率不超过 $\frac{1}{2^k}$.

例2 设 $n=4633$，试求出一个因数基 B，使得68，69及96都是 B—数，并将 n 分解因数.

解 在例1中已经见到，绝对最小剩余 $68^2 \pmod{4633}$ 与 $69^2 \pmod{4633}$ 都可以表示成 -1，2与3的乘积. 由于 $96^2\equiv$

$-50=-2\cdot5^2(\mathrm{mod}4633)$，所以，可以取 $B=\{-1,2,3,5\}$. 此时，

$$68^2\equiv-9=(-1)^1\cdot2^0\cdot3^2\cdot5^0 \quad (\mathrm{mod}4633),$$

$$69^2\equiv128=(-1)^0\cdot2^7\cdot3^0\cdot5^0 \quad (\mathrm{mod}4633),$$

$$96^2\equiv-50=(-1)^1\cdot2^1\cdot3^0\cdot5^2 \quad (\mathrm{mod}4633),$$

并且，相应地，有

$$\bar{\alpha}_1=(1,0,2,0)\equiv(1,0,0,0)=\bar{\varepsilon}_1 \quad (\mathrm{mod}2),$$

$$\bar{\alpha}_2=(0,7,0,0)\equiv(0,1,0,0)=\bar{\varepsilon}_2 \quad (\mathrm{mod}2),$$

$$\bar{\alpha}_3=(1,1,0,2)\equiv(1,1,0,0)=\bar{\varepsilon}_3 \quad (\mathrm{mod}2).$$

显然，$\bar{\varepsilon}_1+\bar{\varepsilon}_2+\bar{\varepsilon}_3\equiv(0,0,0,0) \quad (\mathrm{mod}2)$，因此，由(4)式，记

$$b=68\cdot69\cdot96\equiv1031 \quad (\mathrm{mod}4633),$$

$$c=(2^8\cdot3^2\cdot5^2)^{\frac{1}{2}}\equiv240 \quad (\mathrm{mod}4633),$$

那么，由于 $b\not\equiv\pm c(\mathrm{mod}4633)$，由

$$(1031+240,4633)=41,$$

$$(1031-240,4633)=113,$$

得到4633的两个真因数，以及 $4633=41\cdot113$.

注 由上例可见，在使用 Fermat 因数分解法时，将绝对最小剩余 $b^2(\mathrm{mod}n)$ 表示成小素数的乘积是重要的一步. 但是，一般地，仅当绝对最小剩余是较小的数时，这才容易做到. 为了得到较小的绝对最小剩余 $b^2(\mathrm{mod}n)$，可以在“靠近”$\sqrt{kn}$（k 取较小的数值）的数里去选取 B—数，然后使用 Fermat 因数分解法，这样的方法，称为广义 Fermat 分解因数法.

例3 将 $n=1829$ 分解因数.

解 首先，设法选取形如 $[\sqrt{1829k}]$ 或 $[\sqrt{1829k}]+1$ 的数 b，使绝对最小剩余 $b^2(\mathrm{mod}1829)$ 的素因数不太大. 在本例中，取

因数基 $B=\{-1,2,3,5,7,11,13\}$，对于 $k=1,2,3,4$，计算

$b_1=[\sqrt{1829\cdot 1}]=42$，　$42^2\equiv(-1)^1\cdot 2^0\cdot 3^0\cdot 5^1\cdot 7^0\cdot 11^0\cdot 13^1 \pmod{1829}$，

$b_2=42+1=43$，　$43^2\equiv(-1)^0\cdot 2^2\cdot 3^0\cdot 5^1\cdot 7^0\cdot 11^0\cdot 13^0 \pmod{1829}$，

$b_3=[\sqrt{1829\cdot 2}]=60$，　$60^2\equiv(-1)^1\cdot 2^1\cdot 29 \pmod{1829}$，

$b_4=61$，　$61^2\equiv(-1)^0\cdot 2^0\cdot 3^2\cdot 5^0\cdot 7^1\cdot 11^0\cdot 13^0 \pmod{1829}$，

$b_5=[\sqrt{1829\cdot 3}]=74$，　$74^2\equiv(-1)^1\cdot 2^0\cdot 3^0\cdot 5^0\cdot 7^0\cdot 11^1\cdot 13^0 \pmod{1829}$，

$b_6=75$，　$75^2\equiv 2\cdot 3\cdot 23 \pmod{1829}$，

$b_7=[\sqrt{1829\cdot 4}]=85$，　$85^2\equiv(-1)^1\cdot 2^0\cdot 3^0\cdot 5^0\cdot 7^1\cdot 11^0\cdot 13^1 \pmod{1829}$，

$b_8=86$，　$86^2\equiv(-1)^0\cdot 2^4\cdot 3^0\cdot 5^1\cdot 7^0\cdot 11^0\cdot 13^0 \pmod{1829}$.

由上可见，b_1,b_2,b_4,b_5,b_7,b_8都是 B—数，与它们相应的向量 $\bar{\alpha}$ 是

$\bar{\alpha}_1=(1,0,0,1,0,0,1)$，　$\bar{\alpha}_2=(0,2,0,1,0,0,0)$，

$\bar{\alpha}_4=(0,0,2,0,1,0,0)$，　$\bar{\alpha}_5=(1,0,0,0,0,1,0)$，

$\bar{\alpha}_7=(1,0,0,0,1,0,1)$，　$\bar{\alpha}_8=(0,4,0,1,0,0,0)$.

有两组 B—数可以用于 Fermat 因数分解法，即$\{b_2,b_8\}$与$\{b_1,b_2,b_4,b_7\}$.

由$\{b_2,b_8\}$，得到同余式

$$(43\cdot 86)^2\equiv(2^{\frac{6}{2}}\cdot 5^{\frac{2}{2}})^2 \pmod{1829},$$

即

$$(43\cdot 86)^2\equiv 40^2 \pmod{1829}.$$

由于 $43\cdot 86\equiv 40 \pmod{1829}$，所以从上式不能得到1829的真因数.

由$\{b_1,b_2,b_4,b_7\}$得到同余式

$$(42\cdot 43\cdot 61\cdot 85)^2\equiv(2\cdot 3\cdot 5\cdot 7\cdot 13)^2 \pmod{1829},$$

即

$$1459^2\equiv 901^2 \pmod{1829},$$

由于$1459\not\equiv\pm 901 \pmod{1829}$，所以，上式给出1829的真因数

$$(1459+901,1829)=59,$$

$$(1459-901,1829)=31.$$

除了利用$[\sqrt{kn}],[\sqrt{kn}]+1,\cdots,[\sqrt{kn}]+l$寻求 B—数外，还可以利用第三节定理5的推论寻求 B—数，即依照下面的步骤：

记

$$b_{-1}=1,\quad b_0=a_0=[\sqrt{n}],\quad x_0=\sqrt{n}-a_0,$$

先取一个较小的正整数 k，对于 $i=1,2,\cdots,k$，依次计算

Ⅰ $a_i=\left[\frac{1}{x_{i-1}}\right],\quad x_i=\frac{1}{x_{i-1}}-a_i;$

Ⅱ $b_i\equiv a_ib_{i-1}+b_{i-2} \pmod{n},\quad 0\leqslant b_i<n;$

Ⅲ $B_i\equiv b_i^2 \pmod{n},\quad |B_i|\leqslant\frac{n}{2},\quad 0\leqslant i\leqslant k;$

Ⅳ 用数-1和满足以下条件的素数 p 组成因数基：p 能整除两个以上的 $B_i(1\leqslant i\leqslant k)$，或者，某个 B_i 的标准分解式中含有 p 的偶数次幂；

Ⅴ 从 $B_0,\cdots,B_k$ 中选出所有的 B—数，并使用 Fermat 因数分解法. 若不能求出 n 的真因数，则选一个 $k_1>k$，用它代替

k,并重复进行以上步骤.

上述用连分数寻求 B—数,并且将 n 分解因数的方法,称为**连分数分解因数法**.

例4 将17873分解因数.

解 记

$$b_{-1}=1,\quad b_0=a_0=[\sqrt{17873}]=133,$$

利用连分数分解因数法,对于 $i=0,1,2,3,4,5$,计算 a_i,b_i 以及绝对最小剩余 $b_i^2(\mathrm{mod}17873)$,得到

$i=$	0	1	2	3	4	5
$a_i=$	133	1	2	4	2	3
$b_i=$	133	134	401	1738	3877	13369
$b_i^2(\mathrm{mod}17873)=$	−184	83	−56	107	−64	161.

在 $b_i^2(\mathrm{mod}17873)$中,83与107是素数. 取因数基 $B=\{-1,2,7,23\}$,则 b_0,b_2,b_4与 b_5都是 B—数,按照(2)式,与 $b_i(i=0,2,4,5)$ 相应的向量 $\bar{\alpha}$ 是

$$\bar{\alpha}_0=(1,3,0,1),\quad \bar{\alpha}_2=(1,3,1,0),$$

$$\bar{\alpha}_4=(1,6,0,0),\quad \bar{\alpha}_5=(0,0,1,1),$$

其中

$$\bar{\alpha}_0+\bar{\alpha}_2+\bar{\alpha}_5\equiv(0,0,0)\pmod 2.$$

因此,利用 Fermat 分解因数法,令

$$b=133\cdot401\cdot13369,\quad c=2^3\cdot7\cdot23=1288,$$

则 $b^2\equiv c^2\pmod{17873}$. 但是,因为

$$b\equiv c\pmod{17873},$$

所以无法得到17873的真因数. 因此,需要多计算几个 b_i. 对 $i=6,7,8$,有

$$\begin{array}{rrrr} i= & 6 & 7 & 8 \\ a_i= & 1 & 2 & 1 \\ b_i= & 17246 & 12115 & 11488 \\ b_i^2(\mathrm{mod}17873)= & -77 & 149 & -88, \end{array}$$

其中149是素数，并且

$$-77=(-1)\cdot 7\cdot 11, \quad -88=(-1)\cdot 2^3\cdot 11,$$

因此，取新的因数基 $B'=\{-1,2,7,11,23\}$，则 b_0,b_2,b_4,b_5,b_6 与 b_8 都是 B—数，相应的向量 $\bar{\alpha}$ 是

$$\bar{\alpha}_0=(1,3,0,0,1), \quad \bar{\alpha}_2=(1,3,1,0,0),$$

$$\bar{\alpha}_4=(1,6,0,0,0), \quad \bar{\alpha}_5=(0,0,1,0,1),$$

$$\bar{\alpha}_6=(1,0,1,1,0), \quad \bar{\alpha}_8=(1,3,0,1,0),$$

其中

$$\bar{\alpha}_2+\bar{\alpha}_4+\bar{\alpha}_6+\bar{\alpha}_8\equiv(0,0,0,0) \pmod 2.$$

令

$$b=401\cdot 3877\cdot 17246\cdot 11488\equiv 7272 \pmod{17873},$$

$$c=(-1)^2\cdot 2^6\cdot 7^1\cdot 11^1\cdot 23^0=4928,$$

则由 $b^2\equiv c^2, b\not\equiv\pm c \pmod{17873}$，得到17873的因数

$$(7272+4928,17873)=61,$$

$$(7272-4928,17873)=293.$$

下面，介绍另一个求真因数的方法，即

Monte Carlo 方法，它包含以下步骤：

Ⅰ　随机地选取一个将 Z/nZ 映到自身的映射（例如，一个整系数多项式），及一个整数 x_0；

Ⅱ　取 $j=j_0$ 是某个正整数，计算

$$x_{i+1}\equiv f(x_i) \pmod n, \quad 0\leqslant i<j; \tag{8}$$

Ⅲ　计算

$$d_{jk}=(x_j-x_k,n),\quad 0\leqslant k<j; \tag{9}$$

Ⅳ　若有某个 $d_{jk}>1$，则它是 n 的真因数；若在步骤Ⅲ中，所有的 $d_{jk}=1$，则将 j 换成 $j+1$，并重复以上步骤.

注1　由(8)式容易见到，如果对于某个 r，$r|n$，有

$$x_{j_0}-x_{k_0}\equiv 0 \pmod{r}, \tag{10}$$

则对于任何满足　$j-k=j_0-k_0$ 的 j,k，都有

$$x_j-x_k\equiv 0 \pmod{r}.$$

因此，在实际应用中，可将上述方法的第Ⅲ个步骤做如下改进：在依次计算出 $x_1,\cdots,x_j$ 后，对于满足 $2^h\leqslant j<2^{h+1}$ 的 j，取 $k=2^h-1$，只计算这样的 d_{jk}. 这一改进的优点，是对于每个 x_j，只需计算一次最大公约数；它的缺点是，若有 $(x_j-x_k,n)>1$，则可能有另外的 $j_0<j,k_0<k$，使得 $(x_{j_0}-x_{k_0},n)>1$.

注2　若 j_0 与 k_0 是第一对使(10)式成立的整数，j_0 是 $h+1$ 位的二进制数. 令 $k=2^{h+1}-1$，则当 $j=k+(j_0-k_0)$ 时，就可由改进的 Monte Carlo 方法求出 n 的真因数. 此时，有 $j<2^{h+2}<4j_0$.

例5　用 $f(x)=x^2+1$ 及 $x_0=1$，将8051分解因数.

解　使用 Monte Carlo 方法以及在注1中所作的改进，有

$x_0=1$，

$x_1=f(x_0)=1^2+1=2,(x_1-x_0,8051)=1$；

$x_2=f(x_1)=5,(x_2-x_1,8051)=(3,8051)=1$；

$x_3=f(x_2)=26,(x_3-x_1,8051)=(24,8051)=1$；

$x_4=f(x_3)=677,(x_4-x_3,8051)=(651,8051)=1$；

$x_5\equiv f(x_4)=677^2+1\equiv 7474 \pmod{8051}$，

$(x_5-x_3,8051)=(7448,8051)=1$；

$$x_6\equiv f(x_5)=7474^2+1\equiv 2839 \pmod{8051},$$

$$(x_6-x_3,8051)=(2813,8051)=97,$$

$$8051=97\cdot 83.$$

引理2 设集合 S 含有 r 个元素，$\mathscr{F}$ 是将 S 映射到自身的所有映射 f 构成的集合. 对于每个 $x_0\in S$ 及 $f\in\mathscr{F}$，记

$$x_{j+1}=f(x_j),\ j=0,1,2,\cdots.$$

对于任意给定的 $\lambda>0$，记 $l=1+[\sqrt{2\lambda r}]$，那么，在所有可能的二元素组(f,x_0)($f\in\mathscr{F}$，$x_0\in S$)中，能使 $x_0,x_1,\cdots,x_l$ 互不相同的二元素组(f,x_0)所占的比例 $\Delta<e^{\lambda}$.

证明 所有可能的(f,x_0)共有 $r\cdot r^r=r^{r+1}$个.

在映射 f 的取值中，若 $x_0,\cdots,x_l$ 是互不相同的，则这样的(f,x_0)的个数至多是 $r(r-1)\cdots(r-l)r^{r-l}$，因此

$$\Delta\leqslant r^{-(r+1)}r(r-1)\cdots(r-l)r^{r-l}=\prod_{j=1}^{l}\left(1-\frac{j}{r}\right).$$

由此，利用不等式$1-x<e^{-x}(0<x<1)$，以及

$$\sum_{j=1}^{l}\frac{j}{r}=\frac{l(l+1)}{2r}>\frac{l^2}{2r}>\frac{2r\lambda}{2r}=\lambda,$$

得出 $\Delta<e^{-\lambda}$. □

定理2 设 n 是奇合数，$r\mid n$，$r<\sqrt{n}$. 在利用改进的 Monte Carlo 方法求 n 的真因数时，存在正常数 C，使得对于任意给定的 $\lambda>0$，在 $C\sqrt{\lambda}\sqrt[4]{n}\log^3 n$ 次比特运算后仍不能成功的概率小于 $e^{-\lambda}$. 假定 f 只取次数不高的多项式.

证明 在第一章第二节和第三节中已经知道，存在常数 C_1 和 C_2，使得当 $x,y\leqslant n$ 时，求$(x-y,n)$与 $f(x)\pmod n$可以分别在 $C_1\log^3 n$ 与 $C_2\log^2 n$ 次比特运算后完成. 设 j_0与 k_0是使(10)式成立的第一对下标，即 $x_{j_0}\equiv x_{k_0}\pmod r$，$k_0<j_0$. 由对 Monte

Carlo 方法的注2，利用改进的方法时，在计算到 x_{4j_0} 时，必定可以求出 r.（严格地说，这时求出的真因数不一定再是 r，而可能是 r 的倍数。此处，我们不予详细讨论.）

由上可知，求出 r 所需要的比特运算次数

$$M\leqslant 4j_0(C_1\log^3 n+C_2\log^2 n).$$

如果 $j_0\leqslant 1+\sqrt{2\lambda r}$，则由 $r<\sqrt{n}$，得到

$$\begin{aligned} M&\leqslant 4(1+\sqrt{2\lambda r}(C_1\log^3 n+C_2\log^2 n)\\ &\leqslant C\sqrt{\lambda}\,n^{\frac{1}{4}}\log^3 n, \end{aligned}$$

其中 C 是绝对常数. 另一方面，由引理1可知，$j_0>1+\sqrt{2\lambda r}$ 的概率小于 $e^{-\lambda}$，定理得证. □

习　题

1. 用 Fermat 分解因数法求下列数的真因数：

（1）8633；　（2）809009.

2. 用广义的 Fermat 分解因数法求下列数的真因数：

（1）68987；　（2）19578709.

3. 用连分数分解因数法求13561的真因数.

4. 取 $f(x)=x^2+x+1$，$x_0=2$，利用 Monte Carlo 方法求4087的真因数.

5. 取 $f(x)=x^2-1$，$x_0=5$，用上题方法，求7031的真因数.

第四章　公开钥密码系统

70年代以来，公开钥密码系统的出现，使密码学的研究和应用都发生了巨大的变化，有了显著的进展.

本章介绍公开钥密码系统(或称双钥密码系统)的基本思想，几种典型的公钥系统，以及公开钥密码系统的应用.

第一节　公开钥密码系统

第二章中所介绍的几种传统加密方法的共同特点，是由加密方法及加密钥可以导出解密方法及解密钥，而且，当解密钥已知时，对密文的解密可以用多项式时间算法完成. 为了保证密码系统的安全性，需要有一个传送解密钥的安全通道，这既造成了使用这种系统的困难，又增加了泄露解密钥的危险.

从实用的观点来看，由于“保密”本身是有时间性的，所以，密码系统的安全性要求也是有时间性的，即，只要在某个时间期限内，密文不被破译，就可以认为这个密码系统是安全的. 例如，若用一个密码系统传送一个三天后发动进攻的战斗命令，如果所使用的密文被非法接收者破译所需要的时间在十年以上，那么，就可以认为这个密码系统是安全的. 基于这个认识，即基于安全性的时间性，1976年，W. Diffie 与 M. Hellman 提出了建立公开钥密码系统的思想，开辟了密码学研究的新时期.

与传统的密码系统相比，公开钥密码系统有以下特点：

(i) 加密算法和加密钥是公开的；

(ii) 加密和解密都是计算上容易的，即可以用多项式时间算法完成它们，此处所说的解密是由“合法”接收者由密文信息获得明文信息；

(iii) 密码分析人员从密文破译出明文是计算上困难的，即破译工作无法在多项式时间内完成.

为了使(i)和(iii)满足，必须满足条件：不存在由公开钥求出解密钥的多项式时间算法，即由公开钥求出解密钥是计算上困难的. 同时，为了使(ii)满足，即合法接收者由密文求出明文是计算上容易的，则需要使他掌握某种信息，使得解密是计算上容易的.

定义 1 设 $E=f(P)$ 是定义在集合 $\mathscr{P}$ 上的一一对应的函数，它的函数值集合是 $\mathscr{C}$. 若对给定的 $P\in\mathscr{P}$，求 $E=f(P)$ 是计算上容易的，但对给定的 $E\in\mathscr{C}$，求 $P=f^{-1}(E)$ 却是计算上困难的，则称 $f(p)$ 是单向函数.

定义 2 设 $E=f_k(P)$ 是含参变量 k 的单向函数. 若有 $d(k)$ 存在，使得当 $d(k)$ 已知时，由给定的 E，$E=f_k(P)$，求 $P=f_k^{-1}(E)$ 是计算上容易的，则称 $f_k(P)$ 是单向陷门函数，$d(k)$ 是陷门信息.

利用单向陷门函数，可以构造公开钥密码系统的加密算法. 一般地，$d(k)$ 与 $f_k(P)$ 是无关的，因此，在整个加密过程中可以将它保密. 密文的合法接收者掌握了信息 $d(k)$，就可以容易地得到明文.

一般的公开钥密码系统的信息流程图见图 1.

由图 1 可见，使用公开钥密码系统时，不需要传送解密钥的秘密通道，这使它比传统密码系统更便于实际应用.

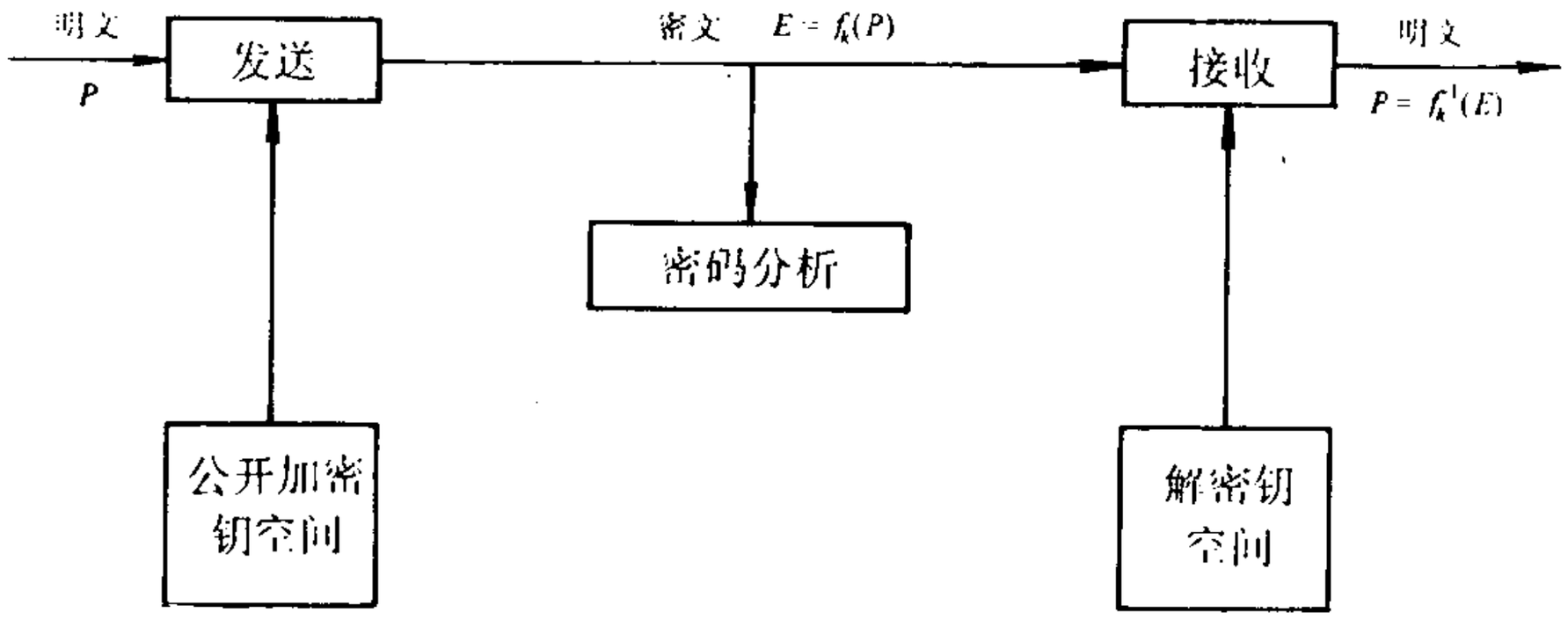


图 1　公开钥密码系统流程图

公开钥密码系统的加密钥是公开的，这对于以密文形式传送信息提供了极大的便利. 例如，可以将加密算法及公开钥列成表 1 的形式，供传送信息使用.

表 1　　公钥系统使用表

接收者	加密算法	公开钥
A	RSA	(n_A,e_A)
B	RSA	(n_B,e_B)
C	MH	$(a_1,\cdots,a_n)$
…		

这样，如果某 D 要向 A 用 RSA 系统传送信息 P，只需按 RSA 系统的加密算法及从表 1 中查到的对 A 所使用的加密钥 (n_A,e_A)进行加密，然后将密文 E 发送给 A 即可. 对 A 来说，他掌握有相应的陷门信息，所以能在有效时间内从密文求出明文. 对于非法接收者(密码分析人员)来说，由于不掌握必要的陷门信息，就不能在有效时间内得到明文.

由于公开钥密码系统的这些特点，使它在许多方面(除传送信息外)取得了应用. 下面举几个例子.

交换密钥 为了弥补传统密码系统需要传送解密钥通道的缺陷，人们采用公开钥密码系统实现传送解密钥的过程，即，在使用传统密码系统时，每更换一次加密钥，都用公开钥密码系统将新的解密钥传送给合法接收者.

数字签名 在社会生活中，在处理具体事务时，常需要当事人进行签证(签名)，以保证他做出的许诺，或送出的信息的可靠性与合法性. 例如，在签署文件时，由当事人签名，盖章，签署日期，以及重要的特殊记号，常是必不可少的环节. 这样的签证，显然应该满足下面的要求.

假设 A 签证一个文件给 B，那么：

Ⅰ B 应该能够确定这是否 A 的签证；

Ⅱ 任何其他人，无法伪造 A 的签证，即 A 有其独特的签证方式，例如，私章，公章，或者亲笔签名，等等；

Ⅲ 有一个仲裁签证是否由 A 发出的方法. 例如，当 A 否认这个签证时，就需要有这样的方法鉴定真伪.

许多公开钥密码系统可以用来进行签证，这不需当事人到场，只需传送必要的信息.

设单向陷门函数 $E=f_k(P)$ 满足条件

$$f_k(f_k^{-1}(E))=E,\quad f_k^{-1}(f_k(E))=E, \tag{1}$$

又假设 A 所使用的加密函数及公开钥是 $f_A(P)$ 与 e_A，B 所使用的加密函数及公开钥是 $f_B(P)$ 与 e_B.

假定需要签证的信息是 M(例如，它是签证人的姓名，签证日期，特定的标志，等等)，并且，已经按一个符号表将 M 与一个数字对应. 为方便计，用 M 同时表示签证文字以及它所对应的数字.

A 要将签证信息 M 传送给 B 时，可计算

$$M'=f_B(f_A^{-1}(M)), \tag{2}$$

然后将 M' 传送给 B. 由于求 $f_A^{-1}(M)$ 所需要的陷门信息只有 A 掌握，而且，f_B 与 e_B 是公开的，所以，计算 M' 只对 A 是容易的，即任何人都无法伪造.

B 收到 M' 后，计算

$$M''=f_B^{-1}(M')=f_B^{-1}(f_B(f_A^{-1}(M)))=f_A^{-1}(M), \tag{3}$$

以及

$$f_A(M'')=f_A(f_A^{-1}(M))=M, \tag{4}$$

可以验证这是否 A 的签证 M. 对 B 来说，他掌握求出 $f_B^{-1}(M')$ 所需要的陷门信息，又有计算 $f_A(M'')$ 所需要的加密钥 e_A（这是公开的），所以(3)与(4)的计算都是容易的.

显然，任何第三者都可以按照(3)和(4)式鉴定 B 所收到的信息是否 A 的签证. 当然，此处假定任何一个不是 A 的人，无法由 M 按照(2)式计算 M'，即已知 M 时，求 $f_A^{-1}(M)$ 是计算上困难的.

信息集合加密 假设 $\mathscr{M}$ 是由 n 个信息 $F_1,\cdots,F_n$ 组成的集合，又设按某种对应关系使这 n 个信息与 n 个整数对应. 为简便计，将用 $F_i(1\leqslant i\leqslant n)$ 同时表示它所对应的整数.

下面叙述一种对 $\mathscr{M}$ 的加密方法，满足这样的条件：可以从密文得到某个信息 F_i，对它进行修改，同时，不影响其他信息 F_j $(j\neq i)$ 的保密.

取正整数 $m_1,\cdots,m_n$，使得

$$m_i>F_i(1\leqslant i\leqslant n),\quad (m_i,m_j)=1(i\neq j).$$

记

$$M=m_1m_2\cdots m_n,\quad M_i=\frac{M}{m_i}(1\leqslant i\leqslant n),$$

又设 $M_i^{-1}(1\leqslant i\leqslant n)$由下面的同余式确定：

$$M_iM_i^{-1}\equiv 1 \pmod{m_i},\quad 1\leqslant M_i^{-1}<m_i.$$

将 $\mathscr{M}$ 按下述方式加密：

$$E=E(\mathscr{M})=\sum_{i=1}^{n}M_iM_i^{-1}F_i \pmod{M}. \tag{5}$$

若要从密文 E 中求出 F_i，可利用公式

$$F_i\equiv\sum_{i=1}^{n}M_iM_i^{-1}F_i\equiv E \pmod{m_i},$$

$$0\leqslant F_i<m_i.$$

在这一加密方法中，$m_i, M_i, M_i^{-1}(1\leqslant i\leqslant n)$都是保密的. 显然，

(i) 只有掌握 m_i，才能由 E 得到 F_i；

(ii) 在掌握 m_i 的条件下，可以求出 F_i，并且可以在修改 F_i 成 F'_i 之后，重新对由 $F_1,\cdots,F_{i-1},F'_i,F_{i+1},\cdots,F_n$ 组成的新集合 $\mathscr{M}'$ 加密；

(iii) 无论求出 F_i 或对 F_i 进行修改，对其他信息 $F_j(j\neq i)$ 均无影响.

例 1 设某数据库含四段文字：$F_1=(0111)_2=7, F_2=(1001)_2=9, F_3=(1100)_2=12, F_4=(1111)_2=15$. 取

$$m_1=11, m_2=13, m_3=17, m_4=19,$$

则

$$M=11\cdot 13\cdot 17\cdot 19=46189,$$

$$M_1=13\cdot 17\cdot 19=4199,\quad M_2=11\cdot 17\cdot 19=3553,$$

$$M_3=11\cdot 13\cdot 19=2717,\quad M_4=11\cdot 13\cdot 17=2431,$$

$$M_1^{-1}=7,\quad M_2^{-1}=10,\quad M_3^{-1}=11,\quad M_4^{-1}=18.$$

对集合{7,9,12,15}加密，得到

$$E \equiv \sum_{i=1}^{4} M_i M_i^{-1} F_i = 4199 \cdot 7 \cdot 7 + 3553 \cdot 10 \cdot 9 +$$
$$+2717 \cdot 11 \cdot 12 + 2431 \cdot 18 \cdot 15 \equiv 16298 \pmod{46189},$$

即 $E=16298$.

若要求出 F_2,则由

$$F_2 \equiv 16298 \equiv 9 \pmod{13},$$

得到 $F_2=9$. 若要将 F_2 改变成 10,并且将新的数据库加密,则{7,10,12,15}对应的密文是

$$E' \equiv 4199 \cdot 7 \cdot 7 + 3553 \cdot 10 \cdot 10 + 2717 \cdot 11 \cdot 12 +$$
$$2431 \cdot 18 \cdot 19 \equiv 5639 \pmod{46189},$$

即 $E'=5639$.

秘密共管 为了保存一个信息 M,使它不被盗取或丢失,可以采用共管的办法,即建立由 M 决定的 r 个子信息,使得从其中的 $s(s \leqslant r)$个子信息求出 M 是计算上容易的,同时,当子信息的个数少于 s 时,求出 M 却是计算上困难的。

为此,取素数 $p>M$. 又取两两互素的自然数 $m_1,\cdots,m_r, m_1<m_2<\cdots<m_r, p\nmid m_1m_2\cdots m_r$,并且

$$m_1m_2\cdots m_s > pm_rm_{r-1}\cdots m_{r-s+2}. \tag{6}$$

随机地选取正整数 t,

$$t \leqslant \frac{1}{p} m_1\cdots m_s - 1. \tag{7}$$

对于 $i=1,2,\cdots,n$,令

$$E_i \equiv M + tP \pmod{m_i}. \tag{8}$$

下面说明 $E_1,\cdots,E_n$ 是满足前述要求的子信息.

(i) 由 s 个 E_i 可以容易地求出 M.

设这 s 个子信息是 $E_{i1},\cdots,E_{is}$,则由孙子定理可知,存在唯

一的 x_0，$0\leqslant x_0<m_{i1}\cdots m_{is}$，满足方程组

$$X\equiv E_{ik}\pmod{m_{ik}},\quad 1\leqslant k\leqslant s. \tag{9}$$

显然 $M+tp$ 满足方程组(9)，而且，由于 $P>M$ 及 t 的选取方式，可知

$$\begin{aligned} M+tp&<(t+1)p\leqslant\frac{1}{p}m_1\cdots m_s\cdot p=m_1\cdots m_s\\ &\leqslant m_{i1}\cdots m_{is}, \end{aligned} \tag{10}$$

因此，必是 $x_0=M+tp$，即 $M=x_0-tp$ 是唯一地确定的.

(ii) 设仅知 $E_{j1},\cdots,E_{je}$，$l\leqslant s-1$，则无法确定 M.

事实上，由孙子定理，方程组

$$X\equiv E_{jk}\pmod{m_{jk}},\quad 1\leqslant k\leqslant l \tag{11}$$

对模 $m_{j1}\cdots m_{jl}$ 有唯一解 x_0，$0\leqslant x_0<m_{j1}\cdots m_{jl}$。因为 $m_1,\cdots m_n$ 是两两互素的，由(9)式与(11)式得到

$$x_0\equiv M+tP\pmod{m_{j1}\cdots m_{jl}}, \tag{12}$$

即

$$M+tp-x_0=\lambda m_{j1}\cdots m_{jl},$$

其中 λ 是整数. 要确定 M，必须确定 λ 的值. 由(12)式，得到

$$0\leqslant\lambda\leqslant\frac{M+tp-x_0}{m_{j1}\cdots m_{jl}}.$$

另一方面，由(6)式，(7)式，以及 $l\leqslant s-1$，得到

$$\frac{M+tp-x_0}{m_{j1}\cdots m_{jl}}>\frac{M+tp}{m_rm_{r-1}\cdots m_{r-s+2}}-1.$$

由(10)式，$M+tp$ 可能的取值在 1 与 $m_1\cdots m_s$ 之间，因此，利用(6)式可知，λ 的取值可能是 $0,1,2,\cdots,p-1$，即在没有附加条件时，单由(12)式无法确定 λ 的值，从而不能确定 M.

例 2 设要三方共管的信息是 $M=5$. 取 $p=7$，$m_1=11$，$m_2=12$，$m_3=17$，则

$$11 \cdot 12 > 7 \cdot 17.$$

取 $t \doteq 14 \leqslant \frac{1}{p} m_1 m_2 - 1 = \frac{1}{7} \cdot 11 \cdot 12 - 1.$

三个子信息为

$$E_1 \equiv 5 + 14 \cdot 7 \equiv 4 \pmod{11},$$

$$E_2 \equiv 5 + 14 \cdot 7 \equiv 7 \pmod{12},$$

$$E_3 \equiv 5 + 14 \cdot 7 \equiv 1 \pmod{17}.$$

由 E_1, E_2 与 E_3 中的任意两个都可以确定出 M。例如，假设已知 $E_1 = 4$ 与 $E_2 = 7$，利用孙子定理，得到方程组

$$x \equiv 4 \pmod{11}$$

$$x \equiv 7 \pmod{12}$$

的解 $x_0 \equiv 103 \pmod{11 \cdot 12}$，于是

$$M = x_0 - tp = 103 - 14 \cdot 7 = 5.$$

智力扑克 设加密函数 $f_1(p)$与 $f_2(p)$满足条件

$$f_1(f_2(p)) = f_2(f_1(p)), \quad P \in \mathscr{P},$$

则可以用它们进行智力扑克游戏，即利用通信网络打牌.

假设 A 与 B 打牌，共有 s 张牌. 下面以每人各送 k 张牌为例，说明打牌的步骤.

以 $m_1, \cdots, m_s$ 表示这 s 张牌.

(i) A 将 $m_1, \cdots, m_s$ 用 $f_1(p)$加密，得到

$$E_i = f_1(m_i), 1 \leqslant i \leqslant s, \tag{13}$$

将它们随机地排列，发送给 B. 此处假定只有 A 掌握计算 $f_1^{-1}(E_i)$所需要的陷门信息；

(ii) B 随机地从 $E_1, \cdots, E_s$ 中取出 k 个，假设是 $e'_1, \cdots, e'_k$，将它们发送给 A；

(iii) A 计算

$$f_1^{-1}(e'_i)=f_1^{-1}(f_1(m'_i))=m'_i,\quad 1\leqslant i\leqslant k,$$

得到他的 k 张牌 $m'_1,\cdots,m'_k$，此处 m'_i 满足 $e'_i=f_1(m'_i)$，$1\leqslant i\leqslant k$.

(iv) B 又随机地从剩下的 $s-k$ 张牌里取出 k 张，设是 $e''_1,\cdots,e''_k$，计算

$$g_i=f_2(e''_i)=f_2(f_1(m''_i))=f_1(f_2(m''_i)),$$

$1\leqslant i\leqslant k$，其中 m''_i 满足 $e''_i=f_1(m''_i)$，$1\leqslant i\leqslant k$. 将 $g_1,\cdots,g_k$ 发送给 A；

(v) A 计算

$$g'_i=f_1^{-1}(g_i)=f_1^{-1}(f_1(f_2(m''_i)))=f_2(m''_i),1\leqslant i\leqslant k,$$

并且将 $g'_1,\cdots,g'_k$ 发送给 B；

(vi) B 计算

$$f_2^{-1}(g'_i)=f_2^{-1}(f_2(m''_i))=m''_i,\quad 1\leqslant i\leqslant k,$$

得到他的 k 张牌.

至此，A 与 B 各得到 k 张牌. 以后的打牌也照此进行. 由于 A 与 B 不掌握对方的解密方法，所以都不能从上面的任何一个步骤中知道对方的牌. 此外，需要仲裁游戏过程中有无欺骗行为时，可将双方解密函数公开，进行验证和鉴定.

但是，上述方案是有缺陷的，即存在着进行欺骗的可能性. 若采用概率加密系统来实现智力扑克，不但可以去掉可交换函数这一条件，而且可以克服上述方案中的缺陷，此处不再细述.

习　题

1. 设某数据库由四个文件组成：$F_1=4,F_2=6,F_3=10$，以及 $F_4=13$. 试设计一个对该数据库加密的方法，但要能求出个别的 $F_i(1\leqslant i\leqslant 4)$，同时不影响其他文件的保密.

2. 利用本节中的秘密共管方案，设计一个由三方共管信息 $M=3$ 的方法，要求，在有两个子信息时就可以求出 M，但是，由一个子信息无法确定 M.

（提示：取 $p=5, m_1=8, m_2=9, m_3=11, t=15$）.

3. 利用定理 1.5.14，证明：设 $f(x)$ 是 $n-1$ 次整系数多项式，p 是素数，$x_1,\cdots,x_n$ 是对模 p 互不同余的整数，则对于任何整数 x，有

$$f(x)\equiv\sum_{j=1}^{n}f(x_j)\prod_{\substack{i=1\\ i\neq j}}^{n}(x-x_i)(x_i-x_j)^{-1}\pmod{p},$$

其中 $(x_i-x_j)^{-1}$ 是 x_i-x_j 对模 p 的乘法逆元素.

4. 设 $f(x)$ 是 $s-1$ 次整系数多项式，p 是素数，M 与 r 是正整数，$p>M, p>r$，M 是 $f(x)$ 的常数项. 又设 $x_1,\cdots,x_r$ 是两两对模 p 不同余的整数，记

$$E_i\equiv f(x_i)\pmod{p},\quad 0\leqslant E_i<p\quad(1\leqslant i\leqslant r).$$

证明：

（1）由 $E_1,\cdots,E_r$ 中的任意 s 个可以求出 M；

（2）由 $E_1,\cdots E_r$ 中的 $t(\leqslant s-1)$ 个无法确定 M.

说明实现秘密共管的一个方法.

第二节　RSA 系统

基于大整数因数分解问题的困难程度，R. L. Rivest，A. Shamir与 L. Adleman 在 1978 年提出了一个公开钥密码系统，即 RSA 系统.

RSA 系统的设计

I　参数的选取

随机地选取大素数 p 与 q，计算

$$n=pq,\quad \varphi(n)=(p-1)(q-1);$$

再随机地选取 $e\in N,(e,\varphi(n))=1$，并计算 d，使得

$$ed\equiv 1 \pmod{\varphi(n)}. \tag{1}$$

公开 n,e，做为加密钥，保密 $p,q,\varphi(n)$，以及 d.

Ⅱ 加密 设明文是 $P,0\leqslant P<n$，计算密文

$$E\equiv P^e \pmod{n},\quad 0\leqslant E<n.$$

Ⅲ 解密 已知密文 E 时，明文 P 由下式确定：

$$P\equiv E^d \pmod{n},\quad 0\leqslant P<n. \tag{2}$$

对于以上设计的 RSA 系统，简记为 RSA(n,e).

下面的定理给出了 RSA(n,e)的解密算法的依据.

定理 1 设 $n=p_1\cdots p_k$ 是 k 个不同的素数之积，$(e,\varphi(n))=1$，并且(1)式成立，则对于任意的 $a\in N$，有

$$a^{ed}\equiv a \pmod{n}.$$

证明 对于任意的 $p_i(1\leqslant i\leqslant k)$，若$(a,p_i)=1$，则由 Fermat 定理(定理 1.5.6 的推论 1)，

$$a^{p_i-1}\equiv 1 \pmod{p_i}.$$

由(1)式，$ed=r\varphi(n)+1=r(p_1-1)\cdots(p_k-1)+1$，其中 r 是非负整数，所以，上式给出

$$a^{ed}\equiv a \pmod{p_i}.$$

当$(a,p_i)>1$ 时，这个同余式当然也成立. 由于 $p_1,\cdots,p_k$ 是互不相同的素数，由同余式的性质即可证得定理. □

在设计 RSA(n,e)时，我们假定明文 P(所对应的整数)满足条件 $0\leqslant P<n$. 如果 $P>n$，例如，$0\leqslant P<n^{k+1}$，则可以利用

$$P=\sum_{i=0}^{k}P_in^i,\quad 0\leqslant P_i<n, \tag{3}$$

使 P 与$(P_0,\cdots,P_k)$建立一一对应的关系，此后，使用 RSA(n,e)分别对 $P_i(0\leqslant i\leqslant k)$加密，得到相应的密文 E_i，于是，明文 P 所对应的密文就是

$$E=\sum_{i=0}^{k}E_i n^i. \tag{4}$$

若要由密文 E 求出明文 P，则由(4)式先求出 $E_0,\cdots,E_k$，再由 RSA(n,e)的解密算法求出 $P_0,\cdots,P_k$，利用(3)式得到明文 P.

在第二章第一节中已经谈到，若使用含 N 个符号的符号表，那么，若信息单元 P 的长度是 k，则它们与整数列 $P_{k-1},\cdots,P_0$ 以下述形式建立一一对应关系：

$$P=P_{k-1}N^{k-1}+\cdots+P_0.$$

现在，使用 RSA(n,e)，假设 $N^k<n\leqslant N^l$，又设明文 P 所对应的密文是 E，那么，利用等式

$$E=E_{l-1}N^{l-1}+\cdots+E_0$$

就可以使 E 与整数列 $E_{l-1},\cdots,E_0$ 建立一一对应关系.

例 设明文与密文的信息单元都由 26 个英文字母 $A,B,\cdots,Y,Z$(分别与 0,1,…,24,25 对应)组成. 又设明文单元含三个字母，密文单元含四个字母。求使用 RSA(n,e)对明文 YES 加密后的密文，此处 $n=281\cdot 167=46927$，$e=39423$，$d=26767$.

解 由

$$Y\rightarrow 24,\quad E\rightarrow 4,\quad S\rightarrow 18$$

得到

$$YES\rightarrow 24\cdot 26^2+4\cdot 26+18=16346,$$

利用加密公式，由

$$E\equiv 16346^{39423}\equiv 21166 \pmod{46927}$$

及

$$21166=1\cdot 26^3+5\cdot 26^2+8\cdot 26+2,$$

$$1\to B,\quad 5\to F,\quad I\to 8,\quad 2\to C,$$

得到密文 BFIC.

对 RSA 系统安全性的分析

Ⅰ　如果密码分析人员能将 n 分解因数，即能求出素因数 p 与 q，使得 $n=pq$，则可求出 $\varphi(n)=(p-1)(q-1)$，又可以利用 Euclid 算法得到(1)式中的 d，就能由(2)式从密文求出明文. 因此，破译 RSA 密文不会比将 n 分解因数困难. 但是，将大整数分解因数的问题是困难的，所以，利用这一途径破译 RSA 密文是困难的.

Ⅱ　如果密码分析人员能用某种方法(不是先将 n 分解因数)求出 $\varphi(n)$，则也可以破译 RSA 密文. 此时，由例 1.4.1，我们知道，在多项式时间内就可以将 n 分解因数. 这说明，求出 $\varphi(n)$ 与将 n 分解因数在计算上是同样困难的.

Ⅲ　若能求出整数 d'，使得

$$ed'\equiv 1 \pmod{\varphi(n)}, \tag{5}$$

则可以利用定理 1 破译 RSA 密文. 下面的定理说明，这时，就有将 n 分解因数的概率多项式算法存在.

定理 2　若已知 n 是两个不同的素数之积，并且已知使(5)式成立的 d'，则存在概率多项式时间算法，可以求出 n 的真因数.

证明　记 $\lambda=ed'-1$，则对于任何整数 a，$(a,n)=1$，有

$$a^{\lambda}\equiv 1 \pmod{n}.$$

令 $\lambda=2^{\alpha}\beta$，$2\nmid\beta$，以 B_n 表示与 n 互素的满足以下条件的整数 a $(1\leqslant a<n)$：

(i) $a^{\beta}\equiv 1 \pmod{n}$,

或者

(ii) 存在 $j<\alpha$,使得 $a^{2^j\beta}\equiv -1 \pmod{n}$.

以 A_n 表示与 n 互素的、但不属于 B_n 的整数 $a(1\leqslant a<n)$的集合.

对于 $a\in A_n$,记

$$k'=\min\{k;\quad a^{2^k\beta}\equiv 1 \pmod{n}\}.$$

由 A_n 的定义,$k'\geqslant 1$. 记

$$b\equiv a^{2^{k'-1}\beta} \pmod{n},$$

则显然是 $b^2\equiv 1 \pmod{n}$,并且

$$b\not\equiv \pm 1 \pmod{n},$$

因此,可以将 n 分解因数,即从$(b+1,n)$及$(b-1,n)$得到 n 的真因数.

另一方面,记

$$p-1=2^{\alpha_1}\beta_1,\quad q-1=2^{\alpha_2}\beta_2,\quad 2\nmid\beta_1,\quad 2\nmid\beta_2,$$

此处 p 与 q 表示 n 的两个素因数,令

$$s=\min\{\alpha_1,\alpha_2\},\quad t=\gcd(\beta,\beta_1)\cdot\gcd(\beta,\beta_2),$$

那么,类似于对定理 3.4.6 的证明,可以得到,集合 B_n 所含的元素个数不超过

$$\left(1+\frac{4^s-1}{3}\right)t\leqslant\frac{1}{2}\varphi(n)=2^{\alpha_1+\alpha_2-1}\beta_1\beta_2,$$

因此,A_n 所含的元素个数$\geqslant\frac{1}{2}\varphi(n)$. 这说明,随机地选取 a,$(a,n)=1$,则能将 n 分解因数的概率不小于$\frac{1}{2}$. 因此,将 n 分解因数的概率多项式时间算法是存在的.(详细证明留作习题). □

Ⅳ 关于 RSA(n,e)的不动点.

定义 1　若 $0 \leqslant P < n$，如果

$$P^{e^k} \equiv P \pmod{n} \tag{6}$$

对某个正整数 k 成立，则称 P 是 RSA(n,e)的 k 阶不动点.

从安全性考虑出发，我们希望 RSA(n,e)的不动点少一些，而且，希望不动点的阶要相当大，否则，密码分析人员可以在多项式时间内用穷举法得到明文.

设 $n=pq$，p 与 q 是不同的素数. 不妨设$(P,n)=1$，否则，从$(P,n)>1$ 就可以求出 n 的真因数了.

利用定理 3.2.9，容易得出关于 P 的方程(6)的解的个数是

$$g(n)=(1+(e^k-1,p-1))(1+(e^k-1,q-1)).$$

由于 $2 \nmid e$，所以 $g(n) \geqslant 9$。为了使 $g(n)$不太大，就需要 e^k-1 与 $p-1$ 和 $q-1$ 的最大公约数都不能太大. 例如，可取 $p=2p'+1$，$q=2q'+1$，此处 p' 与 q' 都是素数.

RSA 系统参数的选取

基于对密码系统安全性的考虑，在设计 RSA 系统的参数时，下面的一些要求是应该满足的.

I　差值 $p-q$ 不宜太小. 事实上，如果 p 与 q 的数值相当接近，则 $\frac{1}{2}(p+q) \sim \sqrt{n}$，并且 $\frac{1}{2}(p-q)$是一个相当小的数，因此，等式

$$\left(\frac{p+q}{2}\right)^2 - n = \left(\frac{p-q}{2}\right)^2$$

的右端是一个相当小的平方数. 这样，就可以利用 Fermat 分解因数法(见第三章第五节)将 n 分解因数，即，如果对于大于 $\sqrt{n}$(或 $\sqrt{kn}$，k 是某个小整数)的整数 t 逐个计算 t^2-n，将能很快地找到整数 s，使得

$$t^2 \equiv s^2 \pmod{n},$$

$$t \not\equiv \pm s \pmod{n},$$

从而由$(t \pm s, n)$求出 n 的真因数，也就可以破译 RSA 密文.

Ⅰ　$p-1$ 与 $q-1$ 的最大公约数 $d=(p-1, q-1)$不能太大. 否则，由例 3.4.3 可知，有 d^2 个整数 b，使得 n 对基 b 是伪素数，这就增加了将 n 分解因数的可能性. 例如，当 d 较大时，就有较大的可能从这 d^2 个 b 中选出某个 b'，使得 n 对基 b' 不是强伪素数. 利用强伪素数的定义，可以求出某个数 $c \not\equiv \pm 1 \pmod{n}$，但是 $c^2 \equiv 1 \pmod{n}$，从而由$(c \pm 1, n)$得到 n 的真因数.

Ⅱ　$p-1$ 与 $q-1$ 都应该至少有一个大的素因数. 否则，例如，就可以利用 J. M. Pollard 所提出的方法求出 n 的真因数. 关于这个方法的细节，读者可参阅他的文章：Theorems on factorization and primality testing (Proc. Cambr. Philos. Soc. 76 (1974)521～528).

此外，从分解因数的困难程度考虑，p 与 q 的数量级至少要是 10^{100}. 当然，这里所提到的数量级，与实际具有的计算能力是有关的.

Ⅳ　现在，说明怎样选取大素数 p. 基本思想是，任选一个奇数，再检验它的素性. 即采取下面的步骤：

(i) 随机地取一个 r 位的奇数 a；

(ii) 检验 a 是否素数(利用已有的素性检验方法)；

(iii) 若 a 不是素数，则重复步骤(i)，(ii)，直到找出素数 a 为止.

由于 r 位的奇数有 $\frac{1}{2}(10^r - 10^{r-1})$个，所以，由素数定理，当随机地选取一个 r 位的奇数时，它的素数的概率是

$$\frac{\pi(10^r)-\pi(10^{r-1})}{\frac{1}{2}(10^r-10^{r-1})}\sim\frac{\frac{10^r}{\log 10^r}-\frac{10^{r-1}}{\log 10^{r-1}}}{\frac{1}{2}(10^r-10^{r-1})}$$

$$=\frac{2}{9\log 10}\cdot\frac{9r-10}{r(r-1)}.$$

若 $r=100$，上式右端近似地等于 $\frac{1}{115}$. 这说明，大概在检验 115 个奇数之后，就可以找到一个 100 位的素数了.

前面已经看到，几种破译 RSA 密文的可能途径的困难程度都几乎相当于将大整数分解因数的困难程度. 那么，从 RSA 密文获得部分明文内容(例如，这是明文的二进制表示中的某个位数码)，是否会容易一些呢？下面的定理否定了这一猜测.

定义 2 设整数 x 的二进制表示是 $(x_k\cdots x_0)_2$，称 x_i 是 x 的第 $i+1$ 个位数码，记为

$$B_{i+1}(x)=x_i,\quad 0\leqslant i\leqslant k.$$

以下，假设 RSA(n,e)是给定的.

引理 设整数 D 满足条件

$$D\cdot 2^e\equiv 1\pmod{n},\quad 1\leqslant D<n, \tag{7}$$

则对于任意的 $P\in(\boldsymbol{Z}/n\boldsymbol{Z})^*$，有

(i) $n-p^e\equiv(n-p)^e\pmod{n}$;

(ii) 若 $2\mid P$，则

$$D\cdot P^e\equiv\left(\frac{P}{2}\right)^e\pmod{n};$$

(iii) 若 $2\nmid P$，则

$$D\cdot(n-P^e)\equiv\left(\frac{n-P}{2}\right)^e\pmod{n}.$$

证明 由(7)式，

$$P^e \equiv 2^e \cdot D \cdot P^e \pmod{n}.$$

因此，如果 $2 \mid P$，则由 $(2,n)=1$ 及上式，可以推出

$$\left(\frac{P}{2}\right)^e \equiv D \cdot P^e \pmod{n},$$

即结论(ii).

同理可以证明结论(iii).

结论(i)可以由二项式定理推出. □

定理 3 对于 RSA(n,e)，下面的两个结论是等价的：

(i) 存在多项式时间算法，对于任意的 P，$(P,n)=1$，由 $P^e \pmod{n}$ 可以求出 $B_0(P)=P_0$，此处假定 P 的二进制表示是 $(p_k \cdots p_0)_2$；

(ii) 存在多项式时间算法，对于任意的 P，$(P,n)=1$，由 $P^e \pmod{n}$ 可以求出 P.

证明 只需证明：若有多项式算法 A 满足(i)中的条件，即，对于任意的 P，$(P,n)=1$，

$$A(P^e(\bmod n))=P_0,$$

则存在一个确定 P(当 $P^e(\bmod n)$ 已知)的多项式算法.

记 $E \equiv P^e \pmod{n}$，$0 \leqslant E < n$.

下面的算法 B 可以由 E 确定出 P.

算法 B 含以下步骤.

步骤 Ⅰ 计算 D，使得

$$D \cdot 2^e \equiv 1 \pmod{n}, \quad 1 \leqslant D < n;$$

步骤 Ⅱ 计算 $A(E)=p_0$；

步骤 Ⅲ 计算 E_1，使得

$$E_1 \equiv D \cdot E \pmod{n}, \text{若 } p_0=0,$$

$$E_1 \equiv D \cdot (n-E) \pmod{n}, \text{若 } p_0=1.$$

步骤Ⅳ　将 E 用 E_1 代替，并且重复步骤Ⅰ和步骤Ⅲ.

显然，在完成步骤Ⅱ后，就确定了 p_0.

由引理可知

$$E_1\equiv\begin{cases}\left(\dfrac{P}{2}\right)^e \pmod{n}, & \text{当 } p_0=0,\\ \left(\dfrac{n-P}{2}\right)^e \pmod{n}, & \text{当 } p_0=1.\end{cases}$$

因此，在对 E 完成步骤Ⅰ—Ⅳ后，求 P 的各个位数码的问题化成求

$$P_1=\begin{cases}\dfrac{P}{2}, & \text{当 } p_0=0,\\ \dfrac{1}{2}(n-P), & \text{当 } p_0=1\end{cases}\tag{8}$$

的各个位数码的问题. 记

$$P_1=(p'_{r_1}p'_{r_1-1}\cdots p'_0)_2$$

则由 $p'_i(0\leqslant i\leqslant r_1)$ 可以确定出 $p_i(1\leqslant i\leqslant k)$. 特别地，对 E_1 实行步骤Ⅰ，则由

$$A(E_1)=p'_0$$

及(8)式，可以确定出 p_1. 再对 E_1 实行步骤Ⅲ和Ⅳ，就将求 P_1 的各个位数码 $p'_i(1\leqslant i\leqslant r_1)$ 归化为求 P_2 的各个位数码，此处

$$P_2=\begin{cases}\dfrac{1}{2}P_1, & \text{当 } p'_0=0,\\ \dfrac{1}{2}(n-P_1), & \text{当 } p'_0=1.\end{cases}$$

记 $P_2=(p''_{r_2}p''_{r_2-1}\cdots p''_0)_2$，以及

$$E_2\equiv\begin{cases}\left(\dfrac{P_1}{2}\right)^e \pmod{n}, & \text{当 } p'_0=0,\\ \left(\dfrac{n-P_1}{2}\right)^e \pmod{n}, & \text{当 } p'_0=1,\end{cases}\tag{9}$$

那么，可以求出

$$A(E_2)=p''_0.$$

由 p''_0 及(9)式可以确定出 p'_1，再由(8)式可以确定 p_2.

如此逐步进行下去，就可以将 $p_0,p_1,\cdots,p_k$ 全部确定. 由于 $k\leqslant\log_2 n+1$，而且算法 A 是多项式时间算法，所以，求出 P_0，$\cdots,P_k$ 的算法 B 也是多项式时间算法. □

作为本节的结尾，介绍 RSA 系统的一个推广.

RSA_k 系统

Ⅰ 参数的选取

取 $k\in N$. 随机地选取大素数 p 与 q，计算 $n=pq,\varphi(n)=(p-1)(q-1)$. 再随机地选取 k 个正整数 $e_j(1\leqslant j\leqslant k)$，$e_j<\varphi(n)$，并且

$$(e_1\cdots e_k,\varphi(n))=1.$$

计算 $d_i(1\leqslant i\leqslant k)$，使得

$$e_1d_1+\cdots+e_kd_k\equiv 1 \pmod{\varphi(n)}.$$

Ⅱ 加密 设明文为 P，$0\leqslant P<n$，计算

$$E_i\equiv P^{e_i} \pmod n,\quad 0\leqslant E_i<n,$$

将 k 维向量 $(E_1,\cdots,E_k)$ 做为与 P 对应的密文.

Ⅲ 解密 按下面的公式由 $(E_1,\cdots,E_k)$ 求出明文 P：

$$P\equiv E_1^{d_1}E_2^{d_2}\cdots E_k^{d_k} \pmod n,\quad 0\leqslant P<n.$$

关于这一系统的具体分析，留给读者.

习 题

1. 使用含有 26 个英文字母的符号表，假设信息单元含两个符号，使用 RSA(899,9) 将 COMEBACK 加密.

2. 证明 RSA_k 系统的解密公式.

3. 说明如何用 RSA 系统实现数字签名.

第三节　Rabin 系统

本节介绍 RSA 系统的一个改进，即 Rabin 公钥密码系统，这是由 M. O. Rabin 提出的. 它有两个值得注意的特点：第一，它不是以一一对应的单向陷门函数为基础，因此，对应于同一个密文，有两个以上的可能的明文. 这种不确定性，增加了密码分析的困难. 第二，破译 Rabin 密文与分解因数有相同程度的计算困难.

Rabin 系统的设计

Ⅰ　参数的选取

随机地选取大素数 p 与 q，计算 $n=pq$，以及由同余方程组

$$\begin{cases} a\equiv 1 \pmod{p} \\ a\equiv 0 \pmod{q} \end{cases} \quad \text{与} \quad \begin{cases} b\equiv 0 \pmod{p} \\ b\equiv 1 \pmod{q} \end{cases}$$

所确定的 a 与 b.

将 n 公开；将 p,q,a,b 保密.

Ⅱ　加密　设明文为 p，$0\leqslant P<n$，计算密文

$$E\equiv P^2 \pmod{n}, \quad 0\leqslant E<n. \tag{1}$$

Ⅲ　解密

(i) 求方程

$$x^2\equiv E \pmod{p} \tag{2}$$

的解 x_1,x_2，以及方程

$$y^2\equiv E \pmod{q} \tag{3}$$

的解 y_1,y_2.

(ii) 计算

$$P_{ij}\equiv ax_i+by_j \pmod{n},\quad i,j=1,2; \tag{4}$$

(iii) 从 $P_{ij}(i,j=1,2)$中确定明文 P.

注 1 关于 p 与 q 的选取,见第二节中对 *RSA* 系统设计的说明.此外,p 与 q 的选取应使得方程(2)与(3)的求解是计算上容易的.例如,可以选取 p,q,使得

$$p\equiv q\equiv 3 \pmod{4},$$

(见例 3.1.1).

注 2 由 a、b 的确定方法,以及(2)式和(3)式,

$$(ax_i+by_j)^2\equiv E \pmod{p},$$

$$(ax_i+by_j)^2\equiv E \pmod{q},$$

因此,

$$P_{ij}^2\equiv E \pmod{n},\quad i,j=1,2,$$

即 $P_{11},P_{12},P_{21},P_{22}$都是关于 P 的方程(1)的解.这样,为了确定明文 P,尚需要某些附加条件.例如,可以用某种方式在明文后面补加几位数字做为校正码(或称识别码),用它们从四个可能的明文中确定出正确的明文.

注 3 一般地,Rabin 系统的加密公式是

$$E\equiv P(P+b) \pmod{n}, \tag{5}$$

其中 b 是任选的某个整数.由于 n 是奇数,所以存在整数 k,使得

$$2k\equiv 1 \pmod{n},$$

因此,(5)式成为

$$E+k^2b^2\equiv P^2+2kPb+k^2b^2=(P+kb)^2 \pmod{n},$$

这就是前面所讨论的加密形式.

下面考察 Rabin 系统的安全性.

引理 1　设 $n=pq$ 是两个不同的奇素数之积，$a\in QR(n)$，则方程

$$x^2\equiv a \pmod{n} \tag{6}$$

有四个不同的解.

证明　由引理 3.1.1，方程

$$x^2\equiv a \pmod{p} \quad 与 \quad x^2\equiv a \pmod{q}$$

各有两个解

$$x\equiv \pm c \pmod{p} \quad 与 \quad x\equiv \pm d \pmod{q}.$$

利用孙子定理可以得到方程(6)的四个不同的解，即是由四个同余方程

$$\begin{cases} x\equiv (-1)^i c \pmod{p} \\ x\equiv (-1)^j d \pmod{q} \end{cases}$$

所确定的 $x_{i,j}(i,j=0,1)$. 容易看出，

$$x_{0,0}\equiv -x_{1,1} \pmod{n},$$

$$x_{1,0}\equiv -x_{0,1} \pmod{n}. \qquad \square$$

引理 2　设 p 与 q 是不同的奇素数，$n=pq$，则 $x\in QR(n)$ 的充分必要条件是 $x\in QR(p)$，同时 $x\in QR(q)$.

证明　必要性是显然的.

设 $x\in QR(p)$，并且 $x\in QR(q)$，则存在 u,v，使得

$$x\equiv u^2 \pmod{p}, \quad x\equiv v^2 \pmod{q}.$$

设 s,t 使得 $sp+tq=1$，则

$$sp\equiv 1 \pmod{q}, \quad tq\equiv 1 \pmod{p},$$

因此，

$$(tqu+spv)^2\equiv (tqu)^2\equiv x \pmod{p},$$

$$(tqu+spv)^2\equiv (spv)^2\equiv x \pmod{q},$$

$$(tqu+spv)^2\equiv x \pmod{n},$$

即 $x\in QR(n)$，充分性得证. □

定理 1 设 $n=pq$ 是两个不同的奇素数之积，并且 $p\equiv q\equiv 3(\mathrm{mod}4)$.

(i) 若 $x,y,-x,-y$ 是方程 $x^2\equiv y^2 \pmod{n}$的不同的解，则

$$\left(\frac{x}{n}\right)=-\left(\frac{y}{n}\right),$$

此处$\left(\frac{a}{b}\right)$是雅可比符号；

(ii) 映射 $f(x)$：$x\to x^2 \pmod{n}$，其中 $x\in QR(n)$，是一一对应的满射，即，模 n 的每个二次剩余有且仅有一个也是模 n 的二次剩余的平方根.

证明 (i) 因为 $x,y,-x,-y$ 对模 n 是不同的，并且 $pq=n\mid(x^2-y^2)=(x+y)(x-y)$，所以 p 与 q 只能分别整除 $x+y$ 与 $x-y$ 中的一个，不妨设

$$p\mid x+y,\quad q\mid x-y,$$

则由 $p\equiv 3(\mathrm{mod}4)$，推出

$$x\equiv -y \pmod{p},\quad x\equiv y \pmod{q},$$

$$\left(\frac{x}{p}\right)=-\left(\frac{y}{p}\right),\left(\frac{x}{q}\right)=\left(\frac{y}{q}\right).$$

因此，

$$\left(\frac{x}{n}\right)=\left(\frac{x}{p}\right)\left(\frac{x}{q}\right)=-\left(\frac{y}{p}\right)\left(\frac{y}{q}\right)=-\left(\frac{y}{n}\right).$$

(ii) 设 $c\in QR(n)$，由引理 1，方程

$$x^2\equiv c \pmod{n} \tag{7}$$

有四个不同的解 $x,-x,y,-y$. 由结论 1，$\left(\frac{x}{n}\right)=-\left(\frac{y}{n}\right)$，因此，不妨设$\left(\frac{x}{n}\right)=\left(\frac{x}{p}\right)\left(\frac{x}{q}\right)=1$，所以，必是

$$\left(\frac{x}{p}\right)=\left(\frac{x}{q}\right)=1 \quad \text{或} \quad \left(\frac{x}{p}\right)=\left(\frac{x}{q}\right)=-1.$$

若上述第一个等式成立，则由引理 2，$x\in QR(n)$；若第二个等式，则由于 $p\equiv q\equiv 3(\mathrm{mod}4)$，有

$$\left(\frac{-1}{p}\right)=\left(\frac{-1}{q}\right)=-1,$$

因此，

$$\left(\frac{-x}{p}\right)=\left(\frac{-x}{q}\right)=1,$$

即 $$-x\in QR(n).$$ □

定理 2 若有多项式时间算法 A，对于任何 $n=pq$，p 与 q 是不同的素数，$p\equiv q\equiv 3(\mathrm{mod}4)$，$A(n)=p$，则存在多项式时间算法 B，对于任何 $c\in QR(n)$，可以求出方程(7)的一个解 x，$x\in QR(n)$，此处 n 满足前述条件.

证明 算法 B 由以下步骤组成：

Ⅰ 计算 $p=A(n)$，$q=\frac{n}{p}$；

Ⅱ 计算 $u\in QR(p)$与 $v\in QR(q)$，使得

$$u^2\equiv c \pmod{p}, \quad v^2\equiv c \pmod{q};$$

Ⅲ 计算 s,t，使得 $sp+tq=1$；

Ⅳ 计算 $x\equiv tqu+spv \pmod{n}$.

显然，这是一个多项式时间算法.

由引理 2 的证明过程可见，x 是方程(7)的解. 此外，由

$$\left(\frac{x}{p}\right)=\left(\frac{tqu+spv}{p}\right)=\left(\frac{tqu}{p}\right)=\left(\frac{u}{p}\right)=1,$$

$$\left(\frac{x}{q}\right)=\left(\frac{tqu+spv}{q}\right)=\left(\frac{spv}{q}\right)=\left(\frac{v}{q}\right)=1,$$

得到 $x\in QR(p)$，$x\in QR(q)$. 由引理 2，$x\in QR(n)$. □

定理 3　设 $n=pq$，p 与 q 是两个不同的奇素数. 若有多项式时间算法 A，使得对于任何 $c\in QR(n)$，都可以给出方程(7)的一个解，则存在概率算法 B，可以在多项式时间内求出 n 的真因数.

证明　算法 B 由以下步骤组成：

Ⅰ　随机地选取 $a,(a,n)=1$，计算

$$c\equiv a^2 \pmod{n};$$

Ⅱ　利用算法 A，求出方程(7)的一个解 x；

Ⅲ　计算　$(x+a,n)$与$(x-a,n)$.

Ⅳ　若在步骤Ⅲ中可以求出 n 的真因数，算法终止，否则，重复步骤Ⅰ—Ⅲ.

对于在步骤Ⅰ中求出的 x，有以下四种可能的情形：

(i) $x\equiv a \pmod{p}$，　$x\equiv a \pmod{q}$，

(ii) $x\equiv a \pmod{p}$，　$x\equiv -a \pmod{q}$，

(iii) $x\equiv -a \pmod{p}$，　$x\equiv a \pmod{q}$，

(iv) $x\equiv -a \pmod{p}$，　$x\equiv -a \pmod{q}$.

当情形(ii)和(iii)出现时，在步骤Ⅲ都可以得到 n 的真因数. 这说明，对于随机选取的 $a,(a,n)=1$，利用算法 B 可以得到 n 的真因数的概率$\geqslant\frac{1}{2}$. 因此，对于 k 个随机选取的 $a,(a,n)=1$，实行步骤Ⅰ，Ⅱ，Ⅲ k 次后仍不能得到 n 的真因数的概率$\leqslant\frac{1}{2^k}$.　□

由以上定理可以看出，破译 Rabin 密文的困难程度与分解因数的困难程度是相当的.

习　题

1. 证明：若 p 是素数，$p\equiv 3 \pmod 4$，则有唯一的 $b\in QR(p)$，使得 $b^2\equiv a \pmod p$，此处 a 是模 p 的二次剩余.

2. 当 $p\equiv 1 \pmod 4$，p 是素数时，上题结论是否仍成立？

第四节　背包型公钥密码系统

假设 $a_1,\cdots,a_n$ 是正整数，对于给定的整数 b，方程

$$a_1x_1+\cdots+a_nx_n=b \tag{1}$$

是否有 0—1 解，即解 $(x_1,\cdots,x_n)$，$x_i=0$ 或 $1(1\leqslant i\leqslant n)$？

这就是背包问题. 一般地，求解背包问题是计算上困难的.

但是，对于某些特殊的整数 $a_1,\cdots,a_n$，背包问题是容易解决的.

例如，若 $a_1,\cdots a_n$ 满足条件

$$a_i>a_1+\cdots+a_{i-1},\quad 2\leqslant i\leqslant n, \tag{2}$$

则方程(1)可按以下步骤进行：

Ⅰ　比较 b 与 a_n、若 $a_n>b$，则 $x_n=0$；否则，$x_n=1$；

Ⅱ　若 $x_n,x_{n-1}\cdots,x_{k+1}$ 已经确定，则由方程

$$a_1x_1+\cdots+a_kx_k=b-(a_nx_n+\cdots+a_{k+1}x_{k+1})$$

及步骤Ⅰ确定 x_k；

Ⅲ　重复步骤Ⅰ与Ⅱ，直到求出所有的 $x_i(1\leqslant i\leqslant n)$；或者，断定方程(1)没有 0—1 解.

定义 1　若 $a_1,\cdots,a_n$ 都是正整数，则称向量 $(a_1,\cdots,a_n)$ 是背包向量. 称满足条件(2)的背包向量为超增向量，或超增背包向量.

背包问题是著名的 NP 完全性问题. 一般地，求解背包问题是计算上困难的.

一般背包问题与特殊背包问题的求解在计算困难程度上的差别，是设计背包型公钥密码系统的基础. 1978 年，R. C. Merkle 与 M. E. Hellman 提出了一个背包型公钥系统，即 MH 系统.

MH 系统的设计

I　参数的选取

随机地选取正整数 $M,k,(M,k)=1$，以及超增背包向量 $(a_1,\cdots,a_n)$，使得

$$a_1+\cdots+a_n<M. \tag{3}$$

计算

$$b_i\equiv ka_i \pmod{M},\quad 1\leqslant b_i<M,\quad 1\leqslant i\leqslant n \tag{4}$$

以及 k^{-1}，使得

$$kk^{-1}\equiv 1 \pmod{M}. \tag{5}$$

将背包向量 $(b_1,\cdots,b_n)$ 公开，作为加密钥；将 M,k,k^{-1}，以及 $(a_1,\cdots,a_n)$ 保密.

I　加密　设明文 P 的二进制表示是 $P=(p_1\cdots p_n)_2$，计算 P 对应的密文

$$E=b_1p_1+\cdots+b_np_n. \tag{6}$$

II　解密

(i) 计算

$$E_0\equiv k^{-1}E \pmod{M},\quad 0\leqslant E_0<M. \tag{7}$$

(ii) 由

$$E_0=a_1p_1+\cdots+a_np_n \tag{8}$$

求出 $p_1,\cdots,p_n$.

注 1　解密公式的合理性的证明：

由(6)式及(5)式，

$$k^{-1}E \equiv k^{-1}(b_1p_1 + \cdots + b_np_n)$$

$$\equiv kk^{-1}(a_1p_1 + \cdots + a_np_n)$$

$$\equiv a_1p_1 + \cdots + a_np_n \pmod{M}. \tag{9}$$

由(3)式，

$$0 \leqslant a_1p_1 + \cdots + a_np_n \leqslant a_1 + \cdots + a_n < M,$$

所以，由(9)式，上式，以及(7)式，推出(8)式.

注 2　若 N 是正整数，

$$(2^i - 1) \cdot 2^N < a_i < 2^i \cdot 2^N, \quad 1 \leqslant i \leqslant n, \tag{10}$$

则应有

$$M > 2^N \sum_{i=1}^{n} 2^i = 2^N(2^{n+1} - 1). \tag{11}$$

从求解一般背包问题的困难程度考虑，n 和 N 的数值都不应小于 100，即 $a_i(1 \leqslant i \leqslant 100)$ 的数量级约为 2^{100+i}，M 的数量级约为 2^{202}. 由此可见，使用 MH 系统时，虽然加密与解密的速度都相当快，但是，所需要的计算机容量却是很大的，这是它的一个缺点.

注 3　在 MH 系统中，实际公开的加密钥常是由(4)式确定的向量 $(b_1, \cdots, b_n)$ 的一个置换.

对于 MH 系统的推广，是下面的迭代 MH 系统.

迭代 MH 系统的设计

Ⅰ　参数的选取

随机地选取超增背包向量 $(a_1, \cdots, a_n)$.

随机地选取正整数 $M_1, k_1, (M_1, k_1) = 1$，使得　$a_1 + \cdots + a_n < M_1$，计算

$$c_i \equiv k_1 a_i \pmod{M_1}, \quad 1 \leqslant c_i < M_1, \quad 1 \leqslant i \leqslant n;$$

随机地选取正整数 $M_2, k_2, (M_2, k_2)=1$，使得 $c_1+\cdots+c_n < M_2$，计算

$$b_i \equiv k_2 c \pmod{M_2}, \quad 1 \leqslant b_i < M_2, \quad 1 \leqslant i \leqslant n.$$

将 $(b_1, \cdots, b_n)$ 公开，做为加密钥.

将 $(a_1, \cdots, a_n), k_1, k_2, M_1, M_2$，以及由下式确定的 k_1^{-1} 与 k_2^{-1} 保密：

$$k_i k_i^{-1} \equiv 1 \pmod{M_i}, \quad i=1,2.$$

Ⅱ 加密 仍使用(6)式.

Ⅲ 解密 由密文 E，首先计算

$$E'_0 \equiv k_2^{-1} E \pmod{M_2}, \quad 0 \leqslant E'_0 < M_2,$$

再计算

$$E_0 \equiv k_1^{-1} E'_0 \pmod{M_1}, \quad 0 \leqslant E_0 < M_1,$$

再由(8)式求出明文 P.

一般地，可以类似地设计 k 次 MH 迭代系统，即 MH_k 系统.

例 1 利用超增向量(119, 241, 480, 959, 1917)设计一个 MH 系统，并且将 YES 加密，此处假设符号表由 26 个英文字母构成，信息单元只含一个符号.

解 由

$$119+241+480+959+1917=3716,$$

取 $M=3837$.

取 $k=1001$，则$(1001, 3837)=1$，计算

$$b_1 \equiv 1001 \cdot 119 \equiv 172 \pmod{3837},$$

取 $b_1=172$. 同样地，取

$$b_2=3347, b_3=855, b_4=709, b_5=417.$$

由(5)式，k^{-1}应满足

$$k^{-1}\cdot 1001\equiv 1 \pmod{3837},$$

由 Euclid 算法，得到 $k^{-1}=23$.

使 $a,b,\cdots,y,z$ 分别与 $0,1,\cdots,24,25$ 对应，则

$$Y\to 24=(11000)_2,\quad E\to 4=(00100)_2,$$

$$S\to 18=(10010)_2.$$

利用(6)式计算与 Y 对应的密文：

$$Y\to(11000)_2\to 172\cdot 1+3347\cdot 1+855\cdot 0$$
$$+709\cdot 0+417\cdot 0=3519.$$

同样地，得到

$$E\to 855,\qquad S\to 881.$$

整个密文由三个数组成：3519,855,881.

若要从密文得到明文，例如，求 881 所对应的明文，则利用(7)式，计算

$$k^{-1}\cdot 881=23\cdot 881=20263\equiv 1078 \pmod{3837},$$

再由方程

$$119x_1+241x_2+480x_3+959x_4+1917x_5=1078$$

解出 $x_1=1,x_2=x_3=0,x_4=1,x_5=0$，因此，明文是

$$(10010)_2=18\to S.$$

例 2 给定超增向量(5,10,20)，以及 $k_1=17,M_1=47,k_2=3,M_2=89$，试求出迭代 MH 系统的加密钥.

解 记 $(a_1,a_2,a_3)=(5,10,20)$，则由

$$c_i\equiv 17a_i \pmod{47},\quad 1\leqslant i\leqslant 3$$

得到 $(c_1,c_2,c_3)=(38,29,11)$，再由

$$b_i\equiv 3c_i \pmod{89},\quad 1\leqslant i\leqslant 3$$

得到加密钥 $(b_1,b_2,b_3)=(25,87,33)$.

注 1 由例 2 可见，一般地，迭代 MH 向量不是 MH 向量. 在本例中，不可能有 M 与 k，$(k,M)=1$，使得

$$M>a_1+a_2+a_3=35,$$

$$b_i\equiv ka_i \pmod{M}, \quad 1\leqslant i\leqslant 3. \tag{12}$$

事实上，若这样的 k 与 M 存在，则(12)式即是

$$25\equiv 5k \pmod{M},$$

$$87\equiv 10k \pmod{M},$$

$$33\equiv 20k \pmod{M}.$$

由前两个同余式，得到 $37\equiv 0 \pmod{M}$，所以 $M=37$. 代入第一个同余式，得到 $k=5$. 但是，当 $M=37$，$k=5$ 时，第三个同余式是不成立的.

注 2 例 2 中所得到的迭代 MH 向量(b_1,b_2,b_3)是一个超增向量的置换. 这说明，MH 迭代系统不一定就比 MH 系统有更好的安全性. 此外，这个例子还说明，有可能找到正整数 M_0 与 k_0，$(M_0,K_0)=1$，使得由

$$d_i\equiv k_0 b_i \pmod{M_0}, \quad 1\leqslant i\leqslant n \tag{13}$$

所确定的$(d_1,\cdots,d_n)$是某个超增向量的置换，因此，求出明文成为计算上容易的. 基于这一思想，1982 年，A. Shamir 提出了破译 MH 系统的多项式时间算法，读者可参阅他的文章“A polynomial time algorithm for breaking the basic Merkle-Hellman cryptosystem”(Proc. of the 23rd Ann. Symp. on the Found. of Comp. Sci. (1982)，145—152).

1983 年，J. C. Lagarias 与 A. M. Odlyzko 在他们的文章中提出了求解“低密度”背包问题的算法(见第六节)，这使得相当广的一类背包型公钥系统的安全性受到影响.

下面，介绍由 B. Chor 和 R. Rivest 提出的一个背包型公钥

密码系统，它可以避免上面提到的两个算法的攻击. 下面的定理，是这个系统的基础.

定理(Bose-Chowla)　设 p 是素数，$h\geqslant 2$ 是整数，则存在整数 $a_i(0\leqslant i\leqslant p-1)$满足以下条件：

(i) $1\leqslant a_i\leqslant p^h-1$，　$0\leqslant i\leqslant p-1$；

(ii) 若 $x_i(0\leqslant i\leqslant p-1)$与 $y_j(0\leqslant j\leqslant p-1)$都是非负整数，并且

$$\sum_{i=0}^{p-1}x_i\leqslant h,\quad \sum_{i=0}^{p-1}y_i\leqslant h, \tag{14}$$

$$(x_0,\cdots,x_{p-1})\neq(y_0,\cdots,y_{p'-1}), \tag{15}$$

则

$$\sum_{i=0}^{p-1}a_ix_i\neq\sum_{i=0}^{p-1}a_iy_i. \tag{16}$$

Chor-Rivest 系统的设计

I　参数的选取

(i) 选取素数幂 q，正整数 $h<q$，使得在下面步骤(iv)中对于 $a_i(0\leqslant i\leqslant q-1)$的计算可以用多项式算法完成；

(ii) 随机地取一个 $GF(q)$上的次数为 h 的代数元素 $t\in GF(q^h)$，设它的最小多项式是 $f(t)$；

(iii) 随机地选取 $GF(q^h)$的一个乘法生成元 g；

(iv) 计算由下面的等式所确定的 a_i：

$$g^{a_i}=t+i,\ i=0,1,2,\cdots,q-1;$$

(v) 随机地选取一个对$\{0,1,\cdots,q-1\}$的置换 π：$\{0,1,\cdots q-1\}\to\{0,1,\cdots,q-1\}$，令

$$b_i=a_{\pi(i)},\qquad i=0,1,\cdots,q-1;$$

(vi) 随机地选取 d，$0\leqslant d<q^h-2$，令

$$c_i=b_i+d,\qquad i=0,1,\cdots,q-1.$$

将背包向量$(c_0,\cdots,c_{q-1})$及q,h公开，作为加密钥；将t,g,d，以及置换π保密.

Ⅰ　加密

设明文P的二进制表示是$P=(p_k\cdots p_0)_2$，其中$p_{i_1}=p_{i_2}=\cdots=p_{i_h}=1$，其余的位数码都是0.

与P相应的密文是

$$E\equiv C_{i_1}+C_{i_2}+\cdots+C_{i_h}\pmod{q^h-1}.$$

Ⅱ　解密

(i) 计算

$$r(t)\equiv t^h\pmod{f(t)},$$

即，$r(t)$是t^h被$f(t)$除所得的余式，此处$f(t)$是密钥t的最小多项式。显然，$r(t)$的次数$\leqslant h-1$；

(ii) 计算

$E'\equiv E-hd\pmod{q^h-1}$，$0\leqslant E'<q^h-1$，此处$E$是密文；

(iii) 计算

$$u(t)\equiv g^{E'}\pmod{f(t)}$$

及

$$v(t)=t^h+u(t)-r(t);$$

(iv) 在$GF(q)$上将$v(t)$分解因式：

$$v(t)=(t+i_1)\cdots(t+i_h),$$

由此得到　$i_1,\cdots,i_h$，

(v) 利用(iv)中的$i_1,\cdots,i_h$及π的逆置换，得出明文P中不为0的h个位数码，从而确定明文P.

注　一般地，选取$GF(q^h)$的乘法生成元并不总是计算上容易的.此外，在g已知的情况下，计算对基g的离散对数(即确

定加密钥时所用到的 $a_0,\cdots,a_{p-1}$)也不总是容易的. 因此,在设计本系统时需要认真选取合适的参数. B. chor 与 R. Rivest 曾提出了几组可用的(q,h)值,即(197,24),(211,24),(243,24),以及(256,25). 关于这个公钥系统的安全性等有关问题,可参阅他们的文章"A knapsack-type public key cryptosystem based on arithmetic in finite fields"(IEEE Trans. Inform. Theory IT—34(1988),901—909).

习　题

1. 设$\{a_n\}$满足条件:$a_i\in N(i\geqslant 1)$,并且

$$a_n>\sum_{i=1}^{n-1}a_i,\quad n\geqslant 2,$$

试对 a_n 的增长做出估计.

2. 利用超增向量(2,3,7,20,35)以及 $M=71,k=41$ 设计一个 MH 系统,并求出与 BEGIN 对应的密文,此处假定信息单元仅含一个符号,共有 26 个英文字母作为符号.

3. 已知一个迭代 MH 系统的公开钥是向量(23161,6726,4326,16848,21805,11073,120,15708,2608,341),又已知 $k_1=533,M_1=2617,k_2=10175,M_2=27103$,试求解密钥向量.

第五节　其他公钥系统

70 年代以来,公钥密码系统的研究发展很快. 继 RSA 系统与 MH 系统之后,许多新的公钥密码系统相继出现,要想一一列举是困难的. 本节主要介绍与离散对数有关的几个公开钥密码系统,以及概率加密公开钥密码系统.

定义 设 G 是有限群，$a,b\in G$，a 是 b 的幂，若整数 x 使得 $b^x=a$，则称 x 是 a 对底 b 的离散对数.

通常，定义中的 G 是有限域，b 是 G 的一个生成元，这样，G 中的每个非零元素都有唯一的对底 b 的离散对数.

利用证明第三章第二节定理 11 中的方法，可以得到下面的定理(此处略去证明).

定理 设 b 是 $GF(q)$ 的生成元，q 是某个素数的幂，$q-1=p_1^{a_1}\cdots p_k^{a_k}$，其中 $p_1<p_2<\cdots<p_k$ 都是素数，$\alpha_i>0$，$1\leqslant i\leqslant k$. 对于任意给定的 $t_1,\cdots,t_k$，$0\leqslant t_i\leqslant 1(1\leqslant i\leqslant k)$，存在求 $GF(q)$ 中的元素 a 对底 b 的离散对数的算法，所需要的算术运算次数为

$$O\Big(\sum_{i=1}^{k}(\alpha_i\log_2 q+(1+t_i\log_2 p_i)(p_i^{t_i}+\alpha_i p_i^{1-t_i}))\Big).$$

由定理可见，一般地，求离散对数的问题不能用多项式时间算法完成. 事实上，人们认为，求离散对数的困难程度几乎与分解因数问题的困难程度相当. 基于这一认识，出现了以离散对数问题为依据的公钥密码系统. 下面是几个例子.

Massey-Omura 公钥密码系统

Ⅰ 参数的选取

选取大素数 q.

随机地选取正整数 e，$(e,q-1)=1$.

计算 d，使得 $de\equiv 1(\mathrm{mod}q-1)$.

将 q 公开，做为加密钥，将 e,d 保密.

Ⅱ 加密与解密

假设 A 方要将信息 $P(0\leqslant p<q)$ 传送到 B 方，又设 q 是双方共用的加密钥，e_A 与 d_A 是 A 方的保密钥，e_B 与 d_B 是 B 方的保密钥.

按以下步骤传送信息 P.

(i) A 发送下面的 E_1 给 B:

$$E_1 \equiv P^{e_A} \pmod{q}, \quad 0 \leqslant E_1 < q;$$

(ii) B 发送下面的 E_2 给 A:

$$E_2 \equiv E_1^{e_B} \equiv P^{e_A e_B} \pmod{q}, \quad 0 \leqslant E_2 < q;$$

(iii) A 发送下面的 E_3 给 B:

$$E_3 \equiv E_2^{d_A} \pmod{q}, \quad 0 \leqslant E_3 < q;$$

(iv) B 由下式得到明文 P:

$$P \equiv E_3^{d_B} \pmod{q}, \quad 0 \leqslant P < q.$$

注 1 在步骤(iii)中,

$$E_3 \equiv E_2^{d_A} \equiv P^{e_A d_A e_B} \pmod{q}.$$

由定理 3.2.1,

$$E_3 \equiv P^{e_B} \pmod{q},$$

因此,再利用第四章第二节定理 1,得到步骤(iv)的合理性.

注 2 在步骤(i)和步骤(iv)中,B 方掌握了信息 P^{e_A} 与 P. 如果离散对数是易求的,B 方就可以求出 e_A,从而可以破译 A 方用同一系统发出的其他信息.

注 3 单纯地依照上述步骤,则明文有被第三方截获的可能性. 例如,若有 C 方也得到 E_1,并且用他自己的保密钥 e_c 和 d_c 进行步骤 Ⅱ 和 Ⅳ,那么,C 就可以得到明文 P. 因此,使用本公钥密码系统时,必须伴有对发送信息的"签证",以使接收的一方能确认是合法发送者发出.

EIGamal 公钥密码系统

Ⅰ 参数的选择

选取大的正整数 $q = p^a$,p 是素数. 随机地选取域 $GF(q)$ 的生成元 g,以及正整数 e,$0 < e < q-1$.

计算

$$g_0 \equiv g^e \pmod{q}, \quad 1 \leqslant g_0 < q.$$

将 g, g_0 与 q 公开，作为加密钥，将 e 保密.

Ⅱ 加密

设明文为 P，$0 \leqslant P < q$，相应的密文由

$$E_1 \equiv g^k \pmod{q} \text{与 } E_2 \equiv P g_0^{\,k} \pmod{q},$$

$$0 \leqslant E_1, E_2 < q,$$

组成，此处 k 是密文发送者随机地选用的整数.

Ⅲ 解密

(i) 计算

$$P_1 \equiv E_1^e \pmod{q}, \quad 0 \leqslant P_1 < q,$$

以及 P_1'，使得

$$P_1' P_1 \equiv 1 \pmod{q};$$

(iii) 与 (E_1, E_2) 相应的明文是

$$P \equiv P_1' E_2 \pmod{q}, \quad 0 \leqslant P < q.$$

注 解密过程的合理性是显然的. 在这个系统的使用过程中，密码分析人员可以掌握公开传送的信息 g^k 以及公开钥 g^e. 如果由此可以求出 g^{ek}，则不必求离散对数，也可以求出明文. 因此，这个公钥密码系统以下面的假设为前提：由 g^k 与 g^e 求 g^{ek} 是计算上困难的.

Diffie—Hellman 交换系统

这是一个利用离散对数问题所构造的传送共用信息(例如，是传统密码系统中使用的加密钥)的系统.

随机地选定一个大素数 p，以及正整数 a，$(a, p) = 1$，将 a 与 p 公开. 随机地选取正整数 e，将 e 保密.

假设 A 方与 B 方要确定一个共用的加密钥. 他们在使用本

系统时的保密钥，分别是 e_1 和 e_2，则可依下述步骤进行.

(i) A 与 B 分别计算

$$E_1 \equiv a^{e_1} (\mathrm{mod}\, p) \text{与} E_2 \equiv a^{e_2} (\mathrm{mod}\, p),$$

并且发给对方；

(ii) A 方与 B 方分别计算

$$E_2{}^{e_1} (\mathrm{mod}\, p) \text{与} E_1{}^{e_2} (\mathrm{mod}\, p),$$

得到共用的加密钥 $a^{e_1 e_2} (\mathrm{mod}\, p)$.

注 1 为了传送一个共用信息，用任何公钥密码系统都可以做到，因此，Diffie-Hellman 型系统并非唯一的方法.

注 2 用类似的方法，可以建立一个传送 k 个人共用信息的交换系统，即，假设这 k 个人的保密钥分别为 $e_1, \cdots, e_k$，那么，他们共用的信息将是 $a^{e_1 \cdots e_k} (\mathrm{mod}\, p)$.

下面，介绍概率加密公开钥密码系统.

GM 公开钥密码系统

它是 S. Goldwasser 与 S. Micali 提出的，以下述假设为基础：若合数 n 的素因数未知，$\left(\frac{a}{n}\right)=1$，判定 $a \in QR(n)$ 是计算上困难的.

它的设计如下.

I 参数的选取

随机地选取大素数 p 与 q，$p \neq q$，记 $n=pq$；

随机地选取 $b \in (\boldsymbol{Z}/n\boldsymbol{Z})^*$，$b \in QNR(n)$，$\left(\frac{b}{n}\right)=1$；

将 n 与 b 公开，做为加密钥，将 p 与 q 保密.

II 加密

设明文 P 的二进制表示是 $P=(p_k \cdots p_1)_2$，则与 P 相应的密文是 $E=(e_k, \cdots, e_1)$，其中

$$e_i \equiv b^{1-p_i} x_i^2 \pmod{n}, \quad 0 \leqslant e_i < n, 1 \leqslant i \leqslant k,$$

并且 $x_1, \cdots, x_k$ 都是从 $(Z/nZ)^*$ 中互相独立地随机选取的.

Ⅲ 解密

由密文 $E=(e_k, \cdots, e_1)$ 恢复明文 $P=(p_k \cdots p_1)_2$，使用下面的公式：

$$p_i = \begin{cases} 1, & \text{若 } e_i \in QR(n), \\ 0, & \text{若 } e_i \in QNR(n), \end{cases} \quad 1 \leqslant i \leqslant k.$$

这一公式的合理性是显然的.

注 1 加密时所使用的 $x_1, \cdots, x_k$ 是随机地选取的，因此，对于同一个明文 P，不同的 $x_1, \cdots, x_k$ 将产生出不同的密文，即明文不是由加密系统唯一地确定.

注 2 设明文 P 是长度为 k 的二进制数，n 是长度为 l 的二进制数，则密文 E 是长度为 kl 的二进制数，这成为使用 GM 系统的一个困难，因为，为了避免通过将 n 分解因数对系统的攻击，n 的长度 l 不能太小.

BBS 公开钥密码系统

这是由 L. Blum，M. Blum，与 M. Shub 提出的. 它的设计如下.

以下，以 $b^0(a)$ 表示数 a 的二进制表示中的最后一个位数码.

Ⅰ 参数的选取

随机地选取素数 p 与 q，$p \neq q$，$p \equiv q \equiv 3 \pmod 4$，记 $n=pq$.

将 n 公开，做为加密钥；将 p 与 q 保密.

Ⅱ 加密

设明文 P 的二进制表示是 $P=(p_k \cdots p_1)_2$

随机地选取 $a \in (Z/nZ)^*$，计算

$$a_0 \equiv a^2 \pmod{n}, \quad 0 \leqslant a_0 < n,$$

$$a_i \equiv a_{i-1}^2 \pmod{n}, \quad 0 \leqslant a_i < n, \quad 1 \leqslant i \leqslant k+1. \ (*)$$

与 P 相应的密文是 $E=(e_k,\cdots,e_1,a_{k+1})$，其中

$$e_i \equiv p_i + b^0(a_i) \pmod{2}, \quad 1 \leqslant i \leqslant k.$$

Ⅲ 解密

(i) 由 a_{k+1}及(*)式，依次求出 $a_k,\cdots,a_1$. 由定理 3.1，它们是唯一地确定的.

(ii) 明文 $P=(p_k\cdots p_1)_2$ 由下式确定：

$$p_i \equiv e_i + b^0(a_i) \pmod{2}, 1 \leqslant i \leqslant k.$$

这一公式的合理性是显然的.

注 若明文 P 与 n 分别是长度为 k 与 l 的二进制数，则密文是长度为 $k+l$ 的二进制数，这是 BBS 系统比 GM 系统的一个优点.

习 题

1. 若要在 k 个人之间交换一个共用的密钥，试设计一个可以达此目的的传送方法.

2. 使用只含 26 个英文字母的符号表，假设使用 GM 系统传送明文 YES，并且设 $n=35$，试列出加密与解密过程.

第六节 L^3 算 法

本节介绍格的约化基，求约化基的 L^3 算法，以及 L^3 算法的应用. 限于篇幅，以介绍结论为主.

以下，使用欧几里德空间中的长度与内积的概念，即，若向量 $\bar{a}=(a_1,\cdots,a_n)\in \boldsymbol{R}^n, \bar{b}=(b_1,\cdots,b_n)\in \boldsymbol{R}^n$，则 $\bar{a}$ 的长度是

$$\| \bar{a} \| = (a_1^2 + \cdots + a_n^2)^{\frac{1}{2}},$$

$\bar{a}$ 与 $\bar{b}$ 的内积是

$$(\bar{a}, \bar{b}) = a_1 b_1 + \cdots + a_n b_n,$$

若 $(\bar{a}, \bar{b}) = 0$，则称 $\bar{a}$ 与 $\bar{b}$ 是正交的.

定义 1 设 $\bar{a}_i = (a_{i1}, \cdots, a_{in})(1 \leqslant i \leqslant n)$ 是 $\boldsymbol{R}^n$ 中的 n 个线性无关向量，则称集合

$L = L(\bar{a}_1, \cdots, \bar{a}_n) = \left\{ \sum_{i=1}^{n} \lambda_i \bar{a}_i ; \lambda_i \in \boldsymbol{Z}, 1 \leqslant i \leqslant n \right\}$ 是由向量 $\bar{a}_1$，$\cdots, \bar{a}_n$ 所生成的格，n 是 L 的秩，称 $\bar{a}_1, \cdots, \bar{a}_n$ 是 L 的一个基.

定理 1 设 $\bar{a}_1, \cdots, \bar{a}_n \in \boldsymbol{R}^n$ 是线性无关的向量，令

$$\bar{a}_1^* = \bar{a}_1,$$

$$\mu_{i,j} = (\bar{a}_i^*, \bar{a}_j^*)/(\bar{a}_j^*, \bar{a}_j^*), \quad 1 \leqslant j < i \leqslant n, \tag{1}$$

$$\bar{a}_i^* = \bar{a}_i - \sum_{j=1}^{i-1} \mu_{i,j} \bar{a}_j^*, \quad 2 \leqslant i \leqslant n, \tag{2}$$

则 $\bar{a}_1^*, \cdots, \bar{a}_n^*$ 两两正交，即

$$(\bar{a}_i^*, \bar{a}_j^*) = 0, \quad i \neq j. \tag{3}$$

证明 这是代数学中的定理，也可直接验证. □

定义 2 沿用定理 1 中的记号，若 $\bar{a}_1, \cdots, \bar{a}_n$ 是格 L 的一个基，并且

$$|\mu_{i,j}| \leqslant \frac{1}{2}, \quad 1 \leqslant j < i \leqslant n, \tag{4}$$

$$\| \bar{a}_i^* + \mu_{i,i-1} \bar{a}_{i-1}^* \|^2 \geqslant y \| \bar{a}_{i-1}^* \|^2, \quad 1 \leqslant i \leqslant n, \tag{5}$$

其中常数 y 满足 $\frac{1}{4} < y < 1$，则称 $\bar{a}_1, \cdots, \bar{a}_n$ 是一个 y—约化基.

以下，在谈到约化基时，均指 $y = \frac{3}{4}$.

定理 2 设 $\bar{a}_1, \cdots, \bar{a}_n$ 是格 $L \subset \boldsymbol{R}^n$ 的一个约化基，$\bar{a}_1^*, \cdots, \bar{a}_n^*$ 见于定理 1，则

(i) $\| \bar{a}_j \|^2 \leqslant 2^{i-1} \| \bar{a}_i^* \|^2, \quad 1 \leqslant j < i \leqslant n;$

(ii) $\| \bar{a}_1 \|^2 \leqslant 2^{\frac{n-1}{4}} d(L)^{\frac{1}{n}};$

(iii) $d(L) \leqslant \prod_{i=1}^{n} \| \bar{a}_i \| \leqslant 2^{\frac{n(n-1)}{4}} d(L),$

其中 $d(L) = |\det(\bar{a}_1, \cdots, \bar{a}_n)|$, $\det(\bar{a}_1, \cdots, \bar{a}_n)$是由 $\bar{a}_1, \cdots, \bar{a}_n$ 构成的矩阵的行列式，即，若记 $\bar{a}_i = (a_{i1}, \cdots, a_{in})$, $1 \leqslant i \leqslant n$, 则 $\det(\bar{a}_1, \cdots, \bar{a}_n) = |a_{i,j}|_{i,j=1}^{n}$.

证明 由(4)式及(5)式，对于 $1 < i \leqslant n$, 有

$$\| \bar{a}_i^* \|^2 \geqslant \frac{3}{4} \| \bar{a}_{i-1}^* \|^2 - \mu_{i,i-1}^2 \| \bar{a}_{i-1}^* \|^2 \geqslant \frac{1}{2} \| \bar{a}_{i-1}^* \|^2,$$

由此得到

$$\| \bar{a}_j^* \|^2 \leqslant 2^{i-j} \| \bar{a}_i^* \|^2, \quad 1 \leqslant j < i \leqslant n. \tag{6}$$

利用上式，(2)式与(4)式，推出

$$\| \bar{a}_i \|^2 = \| \bar{a}_i^* + \sum_{j=1}^{i-1} \mu_{i,j} \bar{a}_j^* \|^2 = \| \bar{a}_i^* \|^2 + \sum_{j=1}^{i-1} \mu_{i,j}^2 \| \bar{a}_j^* \|^2$$

$$\leqslant \| \bar{a}_i^* \|^2 + \frac{1}{4} \sum_{j=1}^{i-1} 2^{i-j} \| \bar{a}_i^* \|^2 \leqslant 2^{i-1} \| \bar{a}_i^* \|^2, \tag{7}$$

因此，由(6)式，

$$\| \bar{a}_j \|^2 \leqslant 2^{j-1} \| \bar{a}_j^* \|^2 \leqslant 2^{i-1} \| \bar{a}_i^* \|^2, \quad 1 \leqslant j < i \leqslant n,$$

即结论(i).

由 $d(L)$的定义，(2)式，以及(3)式，易知

$$d(L) = |\det(\bar{a}_1, \cdots, \bar{a}_n)| = |\det(\bar{a}_1^*, \cdots, \bar{a}_n^*)|$$

$$= \prod_{i=1}^{n} \| \bar{a}_i^* \|,$$

由 Hadamard 不等式，得到结论(iii)的前半部分；再利用上式及(7)式，得到(iii)的后半部分.

在结论(i)中取 $j=1$, 则

$$\| \bar{a}_1 \|^2 \leqslant 2^{i-1} \| \bar{a}_i^* \|^2, \quad 1 \leqslant i \leqslant n.$$

将上式两端对 $1 \leqslant i \leqslant n$ 求积，得到

$$\| \bar{a}_1 \|^{2n} \leqslant 2^{\frac{n(n-1)}{2}} \prod_{i=1}^{n} \| \bar{a}_i^* \|^2 = 2^{\frac{n(n-1)}{2}} (d(L))^2,$$

由此推出结论(ii). □

注 定理 2 中的约化基，其实是 $\frac{3}{4}$—约化基. 一般地，对于 y—约化基，结论(i)，(ii)，(iii)中，2 的幂应改为 $\frac{4}{4y-1}$ 的幂.

定理 3 设 $\bar{a}_1, \cdots, \bar{a}_n$ 是格 $L \subset \boldsymbol{R}^n$ 的约化基，则对于任意的 $\bar{x} \in L, \bar{x} \neq 0$，有

$$\| \bar{a}_1 \|^2 \leqslant 2^{n-1} \| \bar{x} \|^2.$$

证明 设

$$\bar{x} = \sum_{i=1}^{n} \lambda_i \bar{a}_i = \sum_{i=1}^{n} \mu_i \bar{a}_i^*,$$

其中 $\lambda_i \in \boldsymbol{Z}, \mu_i \in \boldsymbol{R}, 1 \leqslant i \leqslant n$.

若 $\lambda_n = \lambda_{n-1} = \cdots = \lambda_{k+1} = 0, \lambda_k \neq 0$，则由(2)式，以及 $\bar{a}_1, \cdots, \bar{a}_n$ 的线性无关性可知 $\mu_k = \lambda_k$，于是，由 $\bar{a}_1^*, \cdots, \bar{a}_n^*$ 的正交性，得到

$$\| x \|^2 \geqslant \mu_k^2 \| \bar{a}_k^* \|^2 \geqslant \| \bar{a}_k^* \|^2.$$

由上式及定理 2 的结论(i)，推出

$$\| \bar{a}_1 \|^2 \leqslant 2^{k-1} \| \bar{a}_k^* \|^2 \leqslant 2^{n-1} \| \bar{x} \|^2. \quad \square$$

定理 4 设 $\bar{a}_1, \cdots, \bar{a}_n$ 是格 $L \subset \boldsymbol{R}^n$ 的约化基，$\bar{x}_1, \cdots, \bar{x}_m$ 是 L 中的线性无关向量，则

$$\max_{1 \leqslant j \leqslant m} \| \bar{a}_j \|^2 \leqslant 2^{n-1} \max\{ \| \bar{x}_1 \|^2, \cdots, \| x_m \|^2 \}.$$

证明 记

$$\bar{x}_j = \sum_{i=1}^{n} r_{ij} \bar{a}_i, r_{ij} \in \boldsymbol{Z}, 1 \leqslant i \leqslant n, 1 \leqslant j \leqslant m.$$

对于每个固定的 j，以 $i(j)$表示使 $r_{ij} \neq 0$ 的最大的 i 值，则由定

理 3 的证明可知

$$\| \bar{x}_j \|^2 \geqslant \| \bar{a}^*_{i(j)} \|^2, \quad 1 \leqslant j \leqslant m. \tag{8}$$

若将 $\bar{x}_1, \cdots, \bar{x}_m$ 重新排列，使得 $i(1) \leqslant i(2) \leqslant \cdots \leqslant i(m)$，则必有 $j \leqslant i(j)(1 \leqslant j \leqslant m)$. 事实上，若有某个 $j_0, 1 \leqslant j_0 \leqslant m$，使得 $j_0 > i(j_0)$，则由 $i(j)$的定义，向量 $\bar{x}_1, \cdots, \bar{x}_{j_0}$ 都可以由 $\bar{a}_1, \cdots, \bar{a}_{j_0-1}$ 线性表示，这与 $\bar{x}_1, \cdots \bar{x}_m$ 的线性无关性矛盾.

由(8)式及定理 2 的结论(i)得到，对于任意的 $j, 1 \leqslant j \leqslant m$，有

$$\| \bar{a}_j \|^2 \leqslant 2^{i(j)-1} \| \bar{a}^*_{i(j)} \|^2 \leqslant 2^{n-1} \| \bar{a}^*_{i(j)} \|^2 \leqslant$$
$$\leqslant 2^{n-1} \| \bar{x}_j \|^2,$$

由此易得定理结论. □

注 由定理 3 和定理 4 看到，约化基中的向量是比较“短”的.

对于格 L，若已知它的一个基，则可以用 L^3 算法求出它的一个约化基，这是由 A. K. Lenstra, Jr. H. W. Lenstra 与 I. Lovász 提出的.

L^3 算法

设已知格 L 的一个基$(\bar{a}_1, \cdots, \bar{a}_n)$，求约化基的算法如下.

$\bar{a}_i^* := \bar{a}_i$;

$\left.\begin{array}{l} \mu_{i,j} := (\bar{a}_i, \bar{a}_j^*)/B_j, \\ \bar{a}_i^* := \bar{a}_i^* - \mu_{i,j}\bar{a}_j^*, \end{array}\right\} j = 1, \cdots, i-1$

$B_i := (\bar{a}_i^*, \bar{a}_i^*)$,

$k := 2$;

$\left.\begin{array}{l} \text{(i) 对 } l = k-1, \text{完成(*)(见下面)}; \\ \text{若 } B_k < \left(\frac{3}{4} - \mu_{k,k-1}^2\right) B_{k-1}, \text{则转(ii)}; \end{array}\right\} i = 1, 2, \cdots, n;$

对 $l=k-2,k-3,\cdots,2,1$ 完成(*)；

若 $k=n$，终止；

$k:=k+1$；转(i).

(ii) $\mu:=\mu_{k,k-1}$； $B:=B_k+\mu^2B_{k-1}$； $\mu_{k,k-1}:=\mu B_{k-1}/B$；

$B_k:=B_{k-1}B_k/B$； $B_{k-1}:=B$；

$$\begin{pmatrix}\bar{a}_{k-1}\\ \bar{a}_k\end{pmatrix}:=\begin{pmatrix}\bar{a}_k\\ \bar{a}_{k-1}\end{pmatrix};$$

$$\begin{pmatrix}\mu_{k-1,j})\\ \mu_{k,j}\end{pmatrix}:=\begin{pmatrix}\mu_{k,j}\\ \mu_{k-1,j}\end{pmatrix},j=1,2,\cdots,k-2;$$

$$\begin{pmatrix}\mu_{i,k-1}\\ \mu_{i,k}\end{pmatrix}:=\begin{pmatrix}1 & \mu_{k,k-1}\\ 0 & 1\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & -\mu\end{pmatrix}\begin{pmatrix}\mu_{i,k-1}\\ \mu_{i,k}\end{pmatrix},$$

$$i=k+1,k+2,\cdots,n;$$

若 $k>2$，则 $k:=k-1$；

转(i)

(*)若 $|\mu_{k,l}|>\frac{1}{2}$，则

$$\begin{cases}r:=\text{与 }\mu_{k,l}\text{距离最小的整数};\bar{a}_k:=\bar{a}_k-r\bar{a}_l;\\ \mu_{k,j}:=\mu_{k,j}-r\mu_{l,j},j=1,2,\cdots,l-1,\\ \mu_{k,l}:=\mu_{k,l}-r.\end{cases}$$

定理 5 设格 $L\subset Z^n$ 有一个基是 $\bar{a}_1,\cdots,\bar{a}_n$，又设 $B\in R,B\geqslant 2$，使得 $\|\bar{a}_i\|^2\leqslant B,1\leqslant i\leqslant n$. 则求约化基的 L^3 算法需要 $O(n^4\log B)$次算术运算.

J. C. Lagarias 与 A. M. Odlyzko 将 L^3 算法用于破译相当广的一类背包型公钥密码系统. 他们指出，求解背包问题

$$\sum_{i=1}^{n}a_ix_i=M,x_i=0\text{ 或 }1,\quad 1\leqslant i\leqslant n,\tag{9}$$

可以转化为求格 $L=L(a_1,\cdots,a_n,M)$ 中的短向量，此处 L 是由向量

$$\left.\begin{aligned}
&\bar{b}_1=(1,0,\cdots,0,-a_1),\\
&\bar{b}_2=(0,1,\cdots,0,-a_2),\\
&\cdots\cdots\\
&\bar{b}_n=(0,0,\cdots,1,-a_n),\\
&\bar{b}_{n+1}=(0,0,\cdots,0,M)
\end{aligned}\right\} \tag{10}$$

所生成的格. 利用 L^3 算法，他们提出了求解方程(q)的“最短向量算法”，简称 SV 算法.

SV 算法

(i) 列出由(10)式确定的向量 $\bar{b}_i(1\leqslant i\leqslant n+1)$；

(ii) 利用 L^3 算法求出由 $\bar{b}_1,\cdots,\bar{b}_{n+1}$ 所生成的格 L 的约化基 $b_1^*,\cdots,\bar{b}_{n+1}^*$；

(iii) 若有某个 $\bar{b}_i^*=(b_{i,1},\cdots,b_{i,n+1})$，使得

$$b_{i,j}=0 \text{ 或 } \alpha,\quad 1\leqslant j\leqslant n, \tag{11}$$

其中 α 是常数. 令

$$x_j=\frac{1}{\alpha}b_{i,j},\quad 1\leqslant j\leqslant n,$$

验证$(x_1,\cdots,x_n)$是否方程(9)的解；若是解，算法终止；

否则，算法继续；

(iv) 用 $M'=\sum_{i=1}^{n}a_i-M$ 代替方程(9)中的 M，并且重复(i)，(ii)，(iii). 若新方程的解是$(x'_1,\cdots,x'_n)$，则$(1-x'_1,\cdots,1-x'_n)$是原方程的解.

算法终止.

注 完成 SV 算法所用的计算时间，大致等于完成两次 L^3

算法所用的计算时间，因此，SV 算法是多项式时间算法.

定理 6 设 $B\geqslant 2^{(1+\beta)n^2}$，$\beta>0$，在满足

$$1\leqslant a_i\leqslant B,\quad 1\leqslant i\leqslant n$$

的所有向量 $\bar{a}=(a_1,\cdots,a_n)$ 中，利用 *SV* 算法可以求解方程(9)的向量 $\bar{a}$ 的个数是 $B^n(1-\epsilon)$个，其中

$$\epsilon\leqslant D(1+\beta)\cdot B^{3\frac{\log n}{n}-r},$$

D 是常数，$\gamma=\dfrac{\beta}{1+\beta}$.

这个定理的证明较繁，略去. 读者可查阅 J. C. Lagarias 与 A. M. Odlyzko 的文章“Solving low density subset sum problems”(J. Assoc. Comp. Mah. ,32(1985),229—246).

定义 3 对于给定的向量 $\bar{a}=(a_1,\cdots,a_n)$，称

$$d(\bar{a})=n(\log_2(\max_{1\leqslant i\leqslant n}|a_i|))^{-1}$$

是 $\bar{a}$ 的密度。

由定理 6，对于给定的 $B>0$，当 $n\geqslant n_0(\beta)$时，对于“几乎”所有的满足

$$d(\bar{a})<\frac{1}{n(1+\beta)}$$

的向量 $\bar{a}$，用 SV 算法可以求解方程(9). 用这样的向量做为加密钥的背包型公钥密码系统，是不安全的.

第五章　伪随机数

对伪随机数的研究，在实用上和理论上，都是很有价值的. 本章主要介绍线性伪随机数生成器. 此外，介绍了 Shannon 理论的基本知识.

第一节　Shannon 理论

本节介绍 Shannon 理论的基本知识.

我们知道，密码系统的保密性能是基于这样一个假定：密码分析人员从密文不能得到明文，或者说，不能得到可以确定明文的足够信息，即密文提供的关于明文的信息是不确定的. 事实上，由于明文是正常文字，符合一定的熟知的规律（例如字符出现的频率），这些规律就是有助于确定明文的信息，此外，部分明文与密文的对应信息也可能被获知. 当各种确定明文的信息达到一定数量时，明文就能被确定. 因此，对这样的信息进行分析研究，无论对于密码系统设计者，还是对于密码分析人员，都是非常重要的.

定义 1　设 X 是定义在 $\{x_1,\cdots,x_n\}$ 上的，并且 X 取值 x_i 的概率是

$$P_X\{X=x_i\}=p_X(x_i)=p_i,\quad 1\leqslant i\leqslant n,$$

此处 $p_1+\cdots+p_n=1$. 记 $\overline{p}=(p_1,\cdots,p_n)$，称

$$H(\bar{p}) = H(X) = -\sum_{i=1}^{n} p_i \log_2 p_i \tag{1}$$

是 X 的熵.

注 $H(X)$所反映的,是变量 X 取不同值时所提供的信息量的平均值.

定理 1 $H(X)$具有以下性质:

(i) $H(p_1,\cdots,p_n)=H(p_1,\cdots,p_n,0)$;

(ii) $H(p_1,p_2,\cdots,p_n)=H(p_{\sigma(1)},p_{\sigma(2)},\cdots,p_{\sigma(n)})$,

其中 σ 是对$\{1,2,\cdots,n\}$的任一置换;

(iii) $0\leqslant H(p_1,p_2,\cdots,p_n)\leqslant H\left(\frac{1}{n},\frac{1}{n},\cdots,\frac{1}{n}\right)$;

(iv) $H\left(\frac{1}{2},\frac{1}{2}\right)<H\left(\frac{1}{3},\frac{1}{3},\frac{1}{3}\right)<\cdots<H\left(\frac{1}{n},\cdots\frac{1}{n}\right)<\cdots$;

(v) $H(p_1,p_2,\cdots,p_n)=H(p_1,p_2,\cdots p_{n-2},p_{n-1}+p_n)$

$$+(p_{n-1}+p_n)H\left(\frac{p_{n-1}}{p_{n-1}+p_n},\frac{p_n}{p_{n-1}+p_n}\right).$$

证明 (i) 由定义 1 及已知的极限

$$\lim_{p\to 0+} p\log_2 p=0$$

即可得证.

(ii) 结论显然成立.

(iii) $H(p_1,\cdots,p_n)\geqslant 0$ 是显然的. 下面,用 Lagrange 乘数法求函数 $H(p_1,\cdots,p_n)$在条件 $p_1+\cdots+p_n=1$ 下的极值点与极值. 令

$$F(\bar{p},\lambda)=H(p_1,\cdots,p_n)+\lambda(p_1+\cdots+p_{n-1}),$$

则由

$$\frac{\partial F}{\partial p_i}=-\log_2 p_i-\log_2 e+\lambda=0,\quad 1\leqslant i\leqslant n,$$

$$\frac{\partial F}{\partial \lambda}=p_1+\cdots+p_{n-1}=0,$$

解出

$$p_1=\cdots=p_n=\frac{1}{n},$$

即 $H(p_1,\cdots,p_n)$在点$\left(\frac{1}{n},\cdots\frac{1}{n}\right)$达到极值 $H\left(\frac{1}{n},\cdots\frac{1}{n}\right)$,容易证明这是最大值.

(iv) 由

$$H\left(\frac{1}{n},\cdots,\frac{1}{n}\right)=\log_2 n,\quad n\geqslant 2$$

即可得出结论.

(v) 由(1)式得到

$$\begin{aligned}&-(p_{n-1}+p_n)\log(p_{n-1}+p_n)+\\&(p_{n-1}+p_n)H\left(\frac{p_{n-1}}{p_{n-1}+p_n},\frac{p_n}{p_{n-1}+p_n}\right)\\=&-(p_{n-1}+p_n)\log(p_{n-1}+p_n)\\&-p_{n-1}\log\left(\frac{p_{n-1}}{p_{n-1}+p_n}\right)-p_n\log\frac{p_n}{p_{n-1}+p_n}\\=&-p_{n-1}\log p_{n-1}-p_n\log p_n,\end{aligned}$$

再利用(1)式,可得到结论. □

注 记 $J(p_i)=-\log_2 p_i=-\log_2 P_X\{X=x_i\}$,它反映了事件$\{X=x_i\}$发生时所提供的信息量. 由(1)式所定义的 $H(p_1,\cdots,p_n)$就是 $J(p_i)$的期望值,即

$$H(p_1,\cdots,p_n)=\sum_{i=1}^{n}p_iJ(p_i).$$

定义 2 设随机变量 X 与 Y 分别定义在$\{x_1,\cdots,x_n\}$与$\{y_1,\cdots,y_m\}$上,X 取值 x_i 的概率是 $p_X(x_i)$;Y 取值 y_j 的概率是 $p_Y(y_j)$;X 取值 x_i 同时 Y 取值 y_j 的概率是 $p_{X,Y}(x_i,y_j)$;当 $Y=y_j$ 时,X 取值 x_i 的概率是 $p_{X|Y}(x_i|y_j)$. 记

$$H(X|Y=y_j)=-\sum_{i=1}^{n}p_{X|Y}(x_i|y_j)\log_2 p_{X|y}(x_i|y_j),\quad(2)$$

则称 $H(X|Y=y_j)$的期望值

$$H(X|Y)=\sum_{j=1}^{m}p_Y(y_j)H(X|Y=y_j)\qquad(3)$$

是给定 Y 时 X 的暧昧度,或条件熵.

注 由(2)式及(3)式,利用已知的条件概率的乘法定理,

$$p_{X,Y}(x,y)=p_Y(y)p_{X|Y}(x|y)\qquad(4)$$

得到

$$H(X|Y)=-\sum_{j=1}^{m}p_Y(y_j)\sum_{j=1}^{n}p_{X|Y}(x_i|y_j)\log_2 p_{X|Y}(x_i|y_j)$$

$$=-\sum_{j=1}^{m}\sum_{i=1}^{n}p_{X,Y}(x_i,y_j)\log_2 p_{X|Y}(x_i|y_j)\qquad(5)$$

定理 2 $H(X,Y)=H(Y)+H(X|Y)=H(X)+H(Y|X)$

证明 由于对称性,只需证明前一个等式.

由(1)式,(4)式及(5)式,

$$H(X,Y)=-\sum_{i=1}^{n}\sum_{j=1}^{m}p_{X,Y}(x_i,y_j)\log_2 p_{X,Y}(x_i,y_j)$$

$$=-\sum_{i=1}^{n}\sum_{j=1}^{m}p_{X,Y}(x_i,y_j)\log_2 p_Y(y_j)$$

$$-\sum_{i=1}^{n}\sum_{j=1}^{m}p_{X,Y}(x_i,y_j)\log_2 p_{X|Y}(x_i|y_j)$$

$$=H(Y)+H(X|Y).\qquad\square$$

推论 若随机变量 X 与 Y 是相互独立的,则

(i) $H(X,Y)=H(X)+H(Y)$;

(ii) $H(X|Y)=H(X)$;

(iii) $H(Y|X)=H(Y)$.

证明 (i)若随机变量 X 与 Y 是相互独立的,则 $p_{X,Y}(x,y)$

$= p_X(x)p_Y(y)$，因此，

$$H(X,Y) = -\sum_{i=1}^{n}\sum_{j=1}^{m} p_{X,Y}(x_i,y_j)\log_2 p_{X,Y}(x_i,y_j)$$

$$= -\sum_{i=1}^{n}\sum_{j=1}^{m} p_X(x_i)p_Y(y_j)(\log_2 p_X(x_i) + \log_2 p_Y(y_j))$$

$$- \sum_{j=1}^{m} p_Y(y_j)\sum_{i=1}^{n} p_X(x_i)\log_2 p_X(x_i)$$

$$- \sum_{i=1}^{n} p_X(x_i)\sum_{j=1}^{m} p_Y(y_j)\log_2 p_Y(y_j)$$

$$= -\sum_{i=1}^{n} p_X(x_i)\log_2 p_X(x_i) - \sum_{j=1}^{m} p_Y(y_j)\log_2 p_Y(y_j)$$

$$= H(X) + H(Y).$$

结论(ii)和(iii)由结论(i)及定理 2 推出. □

现在考虑密码系统的安全性问题. 设明文空间是 $\mathscr{M} = \{m_1,\cdots,m_s\}$，$m_i$ 被发送的概率是 $p_m(m_i)$，$1\leqslant i\leqslant s$，设密钥空间是 $\mathscr{K} = \{k_1,\cdots,k_t\}$，$k_i$ 被使用的概率是 $p_K(k_i)$，$1\leqslant i\leqslant t$. 又设每个明文都是由 n 个符号组成，这些符号取自含 A 个符号的符号表 $\mathscr{A}$.

假设下面的条件是满足的：

(i) 每个密码被选用的概率是相同的；

(ii) 在所有的含 n 个符号(取自 $\mathscr{A}$)的符号串中，无意义的符号串出现的概率总和是很小的；

(iii) 有意义的符号串(即可能的明文)出现的概率是相同的.

由 $\mathscr{A}$ 中的 n 个符号组成的符号串共有 A^n 个. 假设其中有意义的符号串是 $A^n{}_1$ 个，则有意义符号串(明文)出现的概率是：

$$A^{n_1} \cdot A^{-n} = A^{n_1-n} = 2^{(n_1-n)\log_2 A}.$$

定义 3 称

$$D_n = (1-\frac{n_1}{n})\log_2 A$$

为语言的多余度.

注 由于有意义的明文是 A^{n_1} 个，并且它们被发送的概率相同，即是 $p=A^{-n_1}$. 因此，将明文 M 视为随机变量，则

$$H(M) = -A^{n_1} \cdot A^{-n_1}\log_2 A^{-n_1} = n_1\log_2 A,$$

于是

$$D_n = \log_2 A - \frac{1}{n}H(M). \tag{6}$$

Shannon 提出，多余度是密码分析的基础，并且提出了唯一解码量的概念. 对于含有 t 个不同密钥的密钥空间 $\mathcal{K}$，由于假定每个密钥被使用的概率是相同的，即 $p=\frac{1}{t}$，所以，将密钥 K 视为随机变量，则

$$H(k) = -t \cdot \frac{1}{t}\log_2 \frac{1}{t} = \log_2 t,$$

$$t = 2^{H(K)}. \tag{7}$$

由前面的讨论可知，用 t 个密钥将密文恢复为明文时，得到有意义译文的期望值是

$$2^{H(K)} \cdot 2^{(n_1-n)\log_2 A} = 2^{H(K)} \cdot 2^{-nD_n} = 2^{H(K)-nD_n}. \tag{8}$$

定义 4 使 $H(K)-nD_n=0$ 成立的数值 n，称为唯一解码量.

注 由(8)式，当 $H(K)=nD_n$ 时，利用所有密钥解密得到有意义的译文的期望值是 1. 若只有一个有意义的译文，它就应该是正确的明文.

如何对密码系统的安全性做出定量分析，一直是密码学研究中的重要课题，并且已经提出了一些分析模式. 下面，介绍完全保密的概念.

除前面使用的记号 $\mathscr{M}$，$p_M(m_i)$，$\mathscr{K}$，$p_k(k_i)$外，又设密文空间是 $\mathscr{E}=\{e_1,\cdots,e_r\}$，并且以 $p_E(e_i)$表示密文是 e_i 的概率($1\leqslant i\leqslant r$). 此外，将明文 M，密钥 K，及密文 E 分别看做定义在 $\mathscr{M}$，$\mathscr{K}$，及 $\mathscr{E}$ 上的随机变量.

定义 5 对于任意的密文 $e\in\mathscr{E}$ 及任意的明文 $m\in\mathscr{M}$，如果总有

$$p_{MIE}(m|e)=p_M(m), \tag{9}$$

则称密码系统是完全保密的.

定理 3 密码系统是完全保密的必要条件是，对于任意的明文 $m\in\mathscr{M}$ 与密文 $e\in\mathscr{E}$，若 $p_M(m)p_E(e)\neq 0$，则

$$p_{EIM}(e|m)=p_E(e).$$

证明 利用(4)式，得到

$$p_E(e)p_{M|E}(m|e)=p_M(m)p_{E|M}(e|m).$$

由上式及(9)式即可得证. □

定理 4 设密码系统的明文空间，密文空间，及密钥空间所含的元素个数都相同，则它是完全保密的充要条件是：

(i) 对于任意的明文 $m\in\mathscr{M}$，及密文 $e\in\mathscr{E}$，将 m 加密为 e 的密钥只有一个；

(ii) 对于任何密钥，被使用的概率相同.

证明 充分性 由条件(i)与(ii)，对于任意的明文 $m\in\mathscr{M}$ 与密文 $e\in\mathscr{E}$，将 m 加密成 e 所使用的密钥 $k(k\in\mathscr{K})$是唯一的，并且是等概率的，因此，

$$P_{E|M}(e|m)=\frac{1}{s}, \tag{10}$$

此处 s 是 $\mathscr{K}$ 中的元素个数.

另一方面,对于任意固定的密文 $e\in\mathscr{E}$,假设将明文 $m_i\in\mathscr{M}$ $(1\leqslant i\leqslant s)$加密成 e 所使用的密钥是 $k_i\in\mathscr{K}(1\leqslant i\leqslant s)$,则由定理的条件,得到

$$P_E(e)=\sum_{i=1}^{s}P_M(m_i)\cdot\frac{1}{s}=\frac{1}{s}.$$

由此及(10)式可知密码系统是完全保密的.

必要性 由定理 3,在完全保密的密码系统中,固定某个明文 $m\in\mathscr{M}$,则对于任意的密文 $e\in\mathscr{E}$,都有相应的密钥 $k\in\mathscr{K}$,将 m 加密成 e. 这样,若密文总数与密钥总数相同,则条件(i)必成立. 另外,对于固定的某个密文 $e\in\mathscr{E}$,以及任意的 $m_i\in\mathscr{M}$,将 m_i 变成 e 的唯一密钥的概率是 $P_{E|M}(e|m_i)$,由定理 3,这是常数,即条件(ii)成立. □

习 题

1. 设明文空间共含有 7 个信息 $m_i(1\leqslant i\leqslant 7)$,并且

$$p_M(m_1)=p_M(m_2)=p_M(m_3)=\frac{1}{6},$$

$$p_M(m_4)=p_M(m_5)=\frac{1}{16},$$

$$p_M(m_6)=p_M(m_7)=\frac{3}{16},$$

求 $H(M)$.

2. 证明:在完全保密的密码系统中,密钥总数不少于可能的明文总数.

第二节　线性移位寄存器

在第一节中谈到，能够完全保密(或“不可破译”)的加密系统是存在的. 例如，对于要传送的每一个明文 P，假设与它对应的整数(也用 P 表示)的二进制表示是 $(p_1\cdots p_k)_2$，使 p 所对应的密文为 $E=(e_1\cdots e_k)_2$，其中

$$e_i\equiv p_i+\delta_i \pmod 2,\quad 1\leqslant i\leqslant k,$$

每个 δ_i 是随机地取值 0 或 1(例如，利用抛掷钱币所得到的正面或反面而确定 $\delta_i=0$ 或 1)，那么，这样的加密系统就是完全保密的. 此处所使用的加密钥 $\delta_1,\cdots,\delta_k$ 中的每一个数都是随机地选取的. 这样的数列，称为随机数列. 在实际应用中，使用随机数列作为加密钥有许多难以克服的困难，例如，需要一个容量非常大的密钥空间，需要随时传送解密钥等等. 因此，这样的加密系统是极少采用的.

尽管使用随机数列作为加密钥是十分困难的，它却提示了一种建立加密系统的方式，即使用所谓“伪随机数列”作为加密钥，它们是用一定的算法所生成的(因而不是随机选取的)，却又很难预测它的生成(所以可以认为具有“随机”的性质). 用来产生伪随机数的算法，称为伪随机数生成器.

为了给随机数列以量的描述，先引进几个概念.

定义 1　用 $\{s_n\}_n\geqslant 0$ 表示 0—1 数列 $s_0,s_1,\cdots,s_n,\cdots$，以 p 表示使

$$s_{n+k}=s_n,\quad n\geqslant 0$$

成立的最小的 k 值，并称 p 是 $\{s_n\}_n\geqslant 0$ 的周期. 若使上式成立的 k 不存在，则称 $\{s_n\}_n\geqslant 0$ 是没有周期的，记为 $p=\infty$.

在本章中，总假定 $p<\infty$. 在不引起误会的情形，用$\{s_n\}$代替$\{s_n\}_n\geqslant 0$. 此外，对于任意的 i，也称数列 $s_{i+1},\cdots,s_{i+p}$是$\{s_i\}$的一个周期.

定义 2 在 0—1 数列$\{s_n\}$中，两个数码 1 之间的连续 k 个数码 0 称为 0 的 k 游程；两个数码 0 之间的连续 k 个数码 1，称为 1 的 k 游程，在两种情形中，都称 k 是游程的长度.

例如，在数列 10010001010100001110…中，依次是1 的 1 游程，0 的 2 游程，1 的 1 游程，0 的 3 游程，….

定义 3 以$|A|$表示集合 A 所含元素的个数. 设 0—1 数列$\{s_n\}$的周期为 p，对于任意的非负整数 k，记

$$A(k)=|\{i;\quad 0\leqslant i<p,\quad s_i=s_{i+k}\}|,$$

$$B(k)=|\{i,\quad 0\leqslant i<p,\quad s_i\neq s_{i+k}\}|,$$

称

$$AC(k)=\frac{1}{p}(A(k)-B(k))$$

是$\{s_n\}$的自相关数，若 $p|k$，则称为异相自相关数.

显然，若 $p|k$，则 $AC(k)=1$.

对于 0—1 序列$\{s_n\}$，S. W. Golombs 提出了以下三条随机性公设：

公设 1 若$\{s_n\}$的周期 p 是偶数，则在任意的连续 p 个数码中，0 和 1 的个数相同；若 p 是奇数，则数码 1 的个数与 0 的个数之差为 1.

公设 2 若$\{s_n\}$的周期为 p，则在任意的连续 p 个数码中，1 游程的个数为游程总数的$\frac{1}{2}$，2 游程的个数是游程总数的$\frac{1}{4}$，…，k 游程的个数是游程总数的 2^{-k}. 此外，对于任何非负整数 k，0 的 k 游程个数与 1 的 k 游程个数相等.

公设 3 对任意的 k，异相自相关数是常数.

由公设 1，数列$\{s_n\}$中 0 与 1 出现的概率“基本”上相同. 由公设 Ⅰ，数码 0 与 1 在第几个位置上出现的概率是相同的. 公设 Ⅱ 则表明，若将$\{s_n\}_{n\geqslant 0}$与$\{s_{n+k}\}_{n\geqslant 0}$比较，无法得到关于$\{s_n\}$的实质性信息(例如它的周期).

从密码系统的角度看，一个伪随机数列还应该满足下面的条件.

(i) $\{s_n\}_{n\geqslant 0}$的周期相当大，(例如，是可与 10^{50}相比较的)；

(ii) $\{s_n\}_{n\geqslant 0}$的确定是计算上容易的；

(iii) 由密文及相应的明文的部分信息，不能确定整个$\{s_n\}$.

定义 4 设 $y=f(x_0,\cdots,x_{n-1})$是一个取整数值的 n 元函数. 对于给定的数值 $s_0,s_1,\cdots,s_{n-1}$，$s_i=0$ 或 1，$0\leqslant i\leqslant n-1$，利用

$$s_{n+i}=f(s_i,s_{i+1},\cdots,s_{i+n-1}),\quad i\geqslant 0,$$

依次地确定 $s_n,s_{n+1},\cdots$，从而得到 0—1 数列$\{s_n\}_{n\geqslant 0}$. 这种算法称为反馈移位寄存器，或移位寄存器. 称 $f(x_0,\cdots,x_{n-1})$为反馈函数，n 是移位寄存器的长度.

特别地，当

$$f(x_0,\cdots,x_{n-1})=c_0x_0\oplus c_1x_1\oplus\cdots\oplus c_{n-1}x_{n-1} \tag{1}$$

时，称相应的反馈移位寄存器为线性移位寄存器，此处的“$\oplus$”表示对模 2 的加法.

对于由(1)中的函数所给出的线性移位寄存器，给定$(s_0,\cdots,s_{n-1})\in\{0,1\}^n$后，$s_i(i\geqslant n)$由下式确定：

$$s_{n+k}=c_0s_k\oplus c_1s_{k+1}\oplus\cdots\oplus c_{n-1}s_{n+k-1},\quad k\geqslant 0, \tag{2}$$

即是

$$c_0s_k\oplus c_1s_{k+1}\oplus\cdots\oplus c_{n-1}s_{n+k-1}\oplus s_{n+k}=0,\quad k\geqslant 0. \tag{3}$$

记　$s(i)=(s_i,s_{i+1},\cdots,s_{i+n-1})$，并称 $s(i)$是数列$\{s_k\}_{k\geqslant 0}$的第 i 个状态. 由(2)式，

$$s(k+n)=c_0s(k)\oplus c_1s(k+1)\oplus\cdots\oplus c_{n-1}s_{(k+n-1)},\quad k\geqslant 0$$

此处将 $s(i)$看成矢量.

图 1 说明了线性移位寄存器的工作情况.

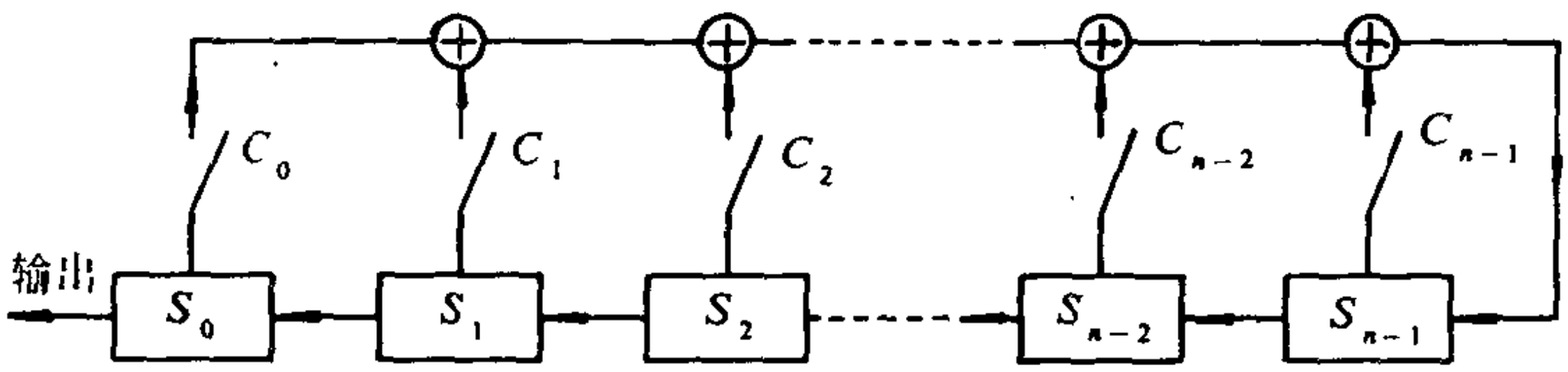


图 1　线性移位寄存器

在图 1 中，若 $c_i=0$，则相应的开关处于“开”的状态；否则，处于“合”的状态. 其中⊕表示对模 2 相加.

例 1　在由(1)确定的线性移位寄存器中，若 $n=4,c_0=c_1=1,c_2=c_3=0$，起始状态为 $s_0=1,s_1=s_2=s_3=0$，求所产生出的数列$\{s_n\}$.

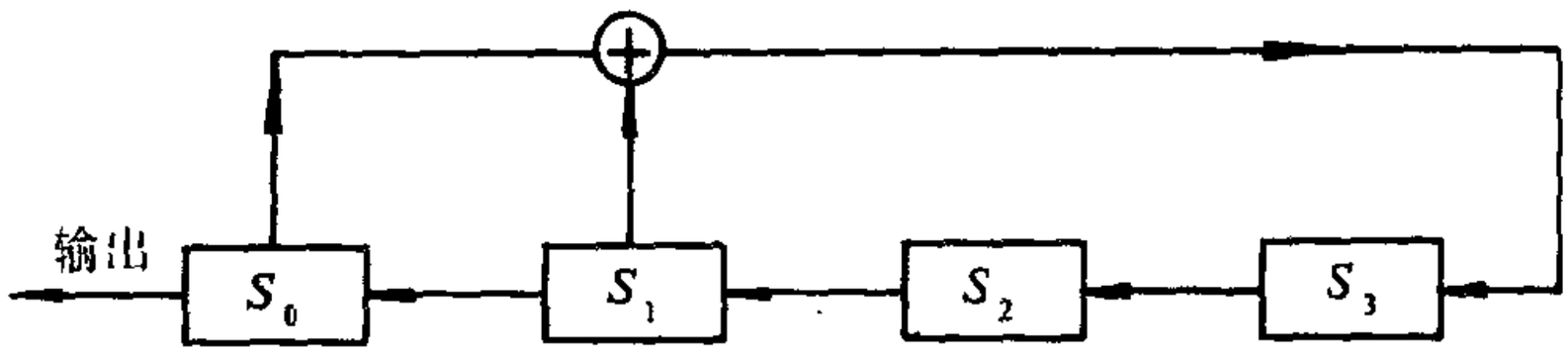
解　由于$\{s_n\}$的每一个状态由前一状态唯一的确定，所以，逐次求出各个状态如图 2 所示：

由图 2 看到，$s(15)=s(0)$，因此，$s(16)=S(1),s(17)=s(2),\cdots$，即$\{s_n\}$的周期是 15.

定义 5　设一个线性移位寄存器的长度为 n，若由它产生的数列$\{s_n\}$的周期是 2^n-1，则称$\{s_n\}$为 $PN-$数列，或 $m-$数列.

注　由定义 4，对于给定的长度为 n 的线性移位寄存器，输出数列$\{s_n\}_{n\geqslant 0}$由初始数值 $s_0,\cdots,s_{n-1}$完全确定，此处 $s_i=0$ 或 $1,0\leqslant i\leqslant n-1$. 这样的初始值共有 2^n 组，但由 $s_i=0,0\leqslant i\leqslant n$ 这一组

所确定的$\{s_n\}$是一个零数列. 因此,每个输出数列的周期至多是2^n-1.



$s(0)$	1	0	0	0
$s(1)$	0	0	0	1
$s(2)$	0	0	1	0
$s(3)$	0	1	0	0
$s(4)$	1	0	0	1
$s(5)$	0	0	1	1
$s(6)$	0	1	1	0
$s(7)$	1	1	0	1
$s(8)$	1	0	1	0
$s(9)$	0	1	0	1
$s(10)$	1	0	1	1
$s(11)$	0	1	1	1
$s(12)$	1	1	1	1
$s(13)$	1	1	1	0
$s(14)$	1	1	0	0
$s(15)$	1	0	0	0
……				

图 2　例 1 中的线性移位寄存器

定理 1　设$\{s_i\}$是由长度为n的线性移位寄存器生成的PN—数列,则它的所有状态必是2^n-1个不相同的非零状态的循

环排列. 寄存器的任何非零输出数列，是$\{s_i\}$的一个移位.

证明 由定义 5 及注得出. □

定义 6 对于由(3)式确定的线性移位寄存器，称

$$f(x)=c_0+c_1x+\cdots+c_{n-1}x^{n-1}+x^n \tag{4}$$

是它的特征多项式，并且，记

$$\Omega(f)=\{\{s_i\}_{i\geqslant 0};\quad \{s_i\}_{i\geqslant 0}\text{满足(2)式}\}.$$

以后总假定 $c_0=1$.

定义 7 对于数列$\{s_i\}_{i\geqslant o}$，称

$$S(x)=\sum_{i=0}^{\infty}s_ix^i \tag{5}$$

为$\{s_i\}_{i\geqslant o}$的生成函数(或母函数). 若$\{s_i\}_{i\geqslant 0}\in\Omega(f)$，则也记$S(x)\in\Omega(f)$

本节中以下所提到的多项式，都是在有限域$GF(2)$上的多项式. 此外，将用到有限域理论中的下述定理(定理 A—C)，关于它们的证明，此处略去.

定理 A 设 $f(x)$是多项式，$f(0)=1$，则存在整数 m，使得 $f(x)\mid x^m+1$.

在定理 A 中的最小的 m 值称为 $f(x)$的周期.

定理 B 设 $f(x)$是 n 次不可约多项式，则 $f(x)$的周期整除 2^n-1.

若 n 次不可约多项式 $f(x)$的周期为 2^n-1，则称 $f(x)$是本原多项式，x 是$GF(2)[x]/(f(x))$上的本原元素.

定理 C n 次本原多项式的个数是$\frac{1}{n}\varphi(2^n-1)$，其中 $\varphi(n)$是 Euler 函数.

定理 2 设$\{s_i\}_i\geqslant 0\in\Omega(f)$，$f(x)$见于(4). 则$\{s_i\}_{i\geqslant 0}$的生成函数

$$S(x)=g(x)(f^*(x))^{-1},$$

其中

$$g(x)=\sum_{j=0}^{n-1}\Big(\sum_{i=0}^{j}c_{n-i}s_{j-i}\Big)x^j,$$

$$f^*(x)=x^nf(\frac{1}{x})=c_0x^n+c_1x^{n-1}+\cdots+c_n. \qquad (6)$$

证明 由(6)式及(5)式，

$$S(x)f^*(x)=\Big(\sum_{k=0}^{\infty}s_kx^k\Big)\Big(\sum_{i=0}^{n}c_{n-i}x^i\Big)$$

$$=\sum_{j=0}^{n-1}x^j\sum_{i=0}^{j}s_{j-i}C_{n-i}+\sum_{j\geqslant n}x^i\sum_{i=0}^{n}s_{j-i}c_{n-i}$$

$$=g(x)+\sum_{j\geqslant n}x^j\sum_{k=0}^{n}C_ks_{j-n+k}.$$

由此及(3)式，即可得证. □

引理 1 设 $f(x)$是 n 次多项式，周期为 m，$\{s_i\}_{i\geqslant 0}\in\Omega(f)$，由$\{s_i\}$的周期 $p\mid m$.

证明 设 $x^m+1=f(x)h(x)$，$h(x)$是 $m-n$ 次多项式. 使用定理 2 中的记号，并记 $h^*(x)=x^{m-n}h(\frac{1}{x})$，则

$$x^m+1=f^*(x)h^*(x).$$

由此及定理 2 可知，存在次数$\leqslant n-1$ 的多项式 $g(x)$，使得

$$S(x)=g(x)(f^*(x))^{-1}=g(x)h^*(x)(1+x^m)^{-1},$$

即

$$(1+x^m)\sum_{i=0}^{\infty}s_ix^i=g(x)h^*(x),$$

其中 $g(x)h^*(x)$的次数$\leqslant n-1+m-n=m-1$. 因此，必是

$$s_{i+m}=s_i,\quad i\geqslant 0.$$

设 $m=pk+l$，$0\leqslant l<k$，则上式给出

$$s_{i+m}=s_{pk+l+i}=s_{l+i}=s_i, i\geqslant 0.$$

由数列周期的定义，可知 $l=0$，即 $p|m$. □

定理 3 设 $f(x)$是 n 次多项式，周期为 m，并且是不可约的. 若$\{s_i\}_{i\geqslant 0}\in\Omega(f)$，则$\{s_i\}_{i\geqslant 0}$的周期是 m.

证明 设$\{s_i\}_{i\geqslant 0}$的周期为 p，则由引理 1，$p|m$，并且

$$S(x)=\sum_{i=0}^{\infty}s_ix^i=\sum_{i=0}^{p-1}\sum_{j=0}^{\infty}s^{pj+i}x^{pj+i}$$

$$=\sum_{i=0}^{p-1}\sum_{j=0}^{\infty}s_ix^{pj+i}=\sum_{i=0}^{p-1}s_ix^i\sum_{j=0}^{\infty}x^{pj}$$

$$=(1+x^p)^{-1}u(x),$$

其中 $u(x)=\sum_{i=0}^{p-1}s_ix^i$. 为叙述简便，对任何 k 次多项式 $p(x)$，记 $p^*(x)=x^kp(\frac{1}{x})$，则由上式及定理 2，存在次数$\leqslant n-1$ 的多项式 $g(x)$，使得

$$(1+x^p)g(x)=f^*(x)u(x),$$

因此

$$(1+x^p)g^*(x)=f(x)u^*(x).$$

在上式中，$f(x)$是周期为 m 的 n 次不可约多项式，$g^*(x)$的次数$\leqslant n-1$，所以 $f(x)$整除 $1+x^p$，因此 $m|p$. 所以 $m=p$.

□

定理 4 设$\{s_i\}_{i\geqslant 0}$是以 $f(x)$为特征多项式的线性移位寄存器的输出数列，则$\{s_i\}$是 PN－数列的充要条件是，$f(x)$是本原多项式.

证明 设$\{s_i\}$是 PN－数列，则以 2^n-1 为它的周期. 由引理 1，$2^n-1|m$，此处 m 是 $f(x)$的周期. 但是，由定理 B，$f(x)$的周期不超过 2^n-1，所以，必是 $m=2^n-1$. 若 $f(x)$是可约的，则

有

$$f(x)=f_1(x)f_2(x), \tag{7}$$

其中 $f_1(x)$与 $f_2(x)$是次数$<n$ 的多项式. 不妨设 $f_1(x)$是次数 $n_1<n$ 的不可约多项式,那么,容易证明,$\Omega(f_1)\subset\Omega(f)$. 这样,对于任何$\{a_i\}_{i\geqslant 0}\in\Omega(f_1)\subset\Omega(f)$,一方面,由$\{a_i\}\in\Omega(f_1)$及引理1,可知$\{a_i\}$的周期 $p\leqslant 2^{n_1}-1$;另一方面,由$\{a_i\}\in\Omega(f)$及定理1,$p=2^n-1$. 这个矛盾说明(7)式不可能成立,即 $f(x)$是不可约多项式. 因此,$f(x)$是本原多项式,必要性得证.

下证充分性. 若 $f(x)$是本原多项式,则是周期为 2^n-1 的不可约多项式. 由定理 3,若$\{s_i\}\in\Omega(f)$,则$\{s_i\}$的周期为 2^n-1,即$\{s_i\}$是 PN—数列. □

至此,我们见到,PN—数列确实存在,它们可用反馈函数是本原多项式的线性移位寄存器生成.

下面说明,PN—数列能满足 Golomb 的随机性公设.

(i) 由定义 5 及其注,线性移位寄存器在生成 PN—数列时,必定是先经过这个数列的 2^n-1 个不同的非零状态,然后重复这样的过程. 每个状态的左边的一个数码,就是要输出的下一个数码,因此,在每一个周期中,有 2^{n-1}个数码 1,有 $2^{n-1}-1$ 个数码 0. 这满足了公设 1.

(ii) 对于任何 $k\leqslant n-2$,1 的 k 游程或 0 的 k 游程必是

$$\cdots 01\underbrace{\cdots 1}_{k\text{个}}0\cdots \quad \text{或} \quad \cdots 10\underbrace{\cdots 0}_{k\text{个}}1\cdots$$

的形式,因此,它们的个数都是 2^{n-k-2}个.

当 $k=n$ 时,0 的 n 游程不会产生,否则,就出现全 0 状态;1 的 n 游程具有

$$01\underbrace{\cdots 1}_{n\text{个}}0 \tag{3}$$

的形式.

当 $k=n-1$ 时,0 的 $n-1$ 游程具有

$$10\cdots01$$

的形式. 1 的 $n-1$ 游程是不存在的,这是因为,当(3)式中的状态向下面的状态变化时,依次出现了状态

$$01\cdots1,\ 1\cdots1,\ 1\cdots10,$$

但是,其中的第一个状态和第三个状态都只能出现一次,所以不可能有 1 的 $n-1$ 游程.

当 $k\geqslant n+1$ 时,1 的 k 游程与 0 的 k 游程都不可能出现. 事实上,0 的 k 游程造成全 0 状态,1 的 k 游程至少造成两个相邻的全是 1 的状态.

总之,1 游程的总数和 0 游程的总数都是

$$1+\sum_{k=1}^{n-2}2^{n-k-2}=2^{n-2}$$

个. 由此易知公设 2 满足.

(iii) 设 $\{s_i\}_{i\geqslant 0}$ 是线性移位寄存器生成的 PN—数列. 由定义 5 及(i)可知 $\{s_{i+k}\}_{i\geqslant 0}$ 是由同一移位寄存器生成的 PN—数列,由于寄存器的反馈函数是线性的,所以 $\{s_i+s_{i+k}\}_{i\geqslant 0}$ 也是 PN—数列. 显然,在一个周期中,$\{s_i\}_{i\geqslant 0}$ 与 $\{s_{i+k}\}_{i\geqslant 0}$ 中有相同对应数码的数码个数等于 $\{s_i+s_{i+k}\}$ 中的数码 0 的个数,由(i),即是 2^n-1 个,因此,

$$AC(k)=\frac{(2^{n-1}-1)-2^{n-1}}{2^n-1}=-\frac{1}{2^n-1},\quad 1\leqslant k<2^n-1.$$

这说明公设 3 满足.

关于 PN—数列是否满足条件(i)～(iii)(见 P. 198)的问题,作为习题留给读者.

习　题

1. 在定义 6 中，假定 $c_0=1$. 试解释这一假定的理由.

2. 证明定理 2 的推论.

3. 考察 PN—数列是否满足条件(i)～(iii).

4. 证明：若已知 PN—数列的连续 $2n$ 个数码，则可以求出产生这一数列的线性移位寄存器的反馈函数.

第三节　伪随机数生成器

在上节中，讨论了一种产生伪随机数的方法. 在这一节，继续给出两种产生伪随机数的方法.

首先，考察一种一般的线性伪随机数生成器.

设 a,b,m 是给定的正整数.

对于任意的非负整数 $x<m$，定义

$$\begin{aligned} x_0&=x \pmod m,\\ x_i&\equiv ax_{i-1}+b \pmod m,\quad i\geqslant 1, \end{aligned} \tag{1}$$

此处及以后均取 x_i 为对模 m 的最小非负剩余.

定义 1　对于给定的正整数 a,b,m，以及非负整数 $x<m$，称由(1)式确定的、计算 $\{x_i\}i\geqslant 0$ 的算法为线性伪随机数生成器，记为 $L(x;a,b,m)$，也记 $L(x;a,b,m)=\{x_i\}_{i\geqslant 0}=\{x_0,x_1,\cdots\}$.

例 1　若取 $x=1,a=2,b=3,m=17$，则

$$x_0=1,x_1\equiv 2\cdot 1+3\equiv 5,x_2\equiv 2\cdot 5+3\equiv 13,$$

$$x_3\equiv 2\cdot 13+3\equiv 12,\cdots \pmod{17},$$

因此，

$$L(1;2,3,17)=\{1,5,13,12,\cdots\}.$$

以下，为叙述方便，记

$$x'_{i+1}=x_{i+1}-x_i,\quad i\geqslant 0. \tag{2}$$

定理 1 下面的结论成立：

(i) $x_n\equiv a^n x_0+(a^{n-1}+\cdots+a+1)b \pmod m$, $n\geqslant 0$;

(ii) $x'_n\equiv a^{n-1}x'_1 \pmod m$, $n\geqslant 1$;

若$(a,m)=1$，则又有

(iii) $x_n\equiv(x_{n+1}-b)a^{\varphi(m)-1} \pmod m$;

(iv) 若$(a-1)\mid b$，则 $x_n=x_{\varphi(m)+n}$;

(v) $x'_n=x'_{\varphi(m)+n}$.

证明 (i) 当 $n=0$ 时，结论显然成立. 若结论对于 $n-1$ 成立，则由(1)式，

$$\begin{aligned}x_n&\equiv ax_{n-1}+b\equiv a(a^{n-1}x_0+(a^{n-2}+\cdots+a+1)b)+b\\&=a^n x_0+(a^{n-1}+\cdots+a+1)b \pmod m.\end{aligned}$$

由归纳法得证.

(ii) 由(2)及(1)式，显然

$$x'_{i+1}\equiv ax'_i \pmod m, i\geqslant 1,$$

由上式及归纳法得证.

(iii) 若$(a,m)=1$，则由 Euler 定理得到

$$a^{\varphi(m)}\equiv 1 \pmod m. \tag{3}$$

由(1)式，有

$$ax_n\equiv x_{n+1}-b \pmod m,$$

因此，

$$x_n\equiv a^{\varphi(m)}x_n\equiv a^{\varphi(m)-1}(x_{n+1}-b) \pmod m.$$

(iv) 若$(a-1)\mid b$，则由结论(i)及(3)式，

$$x_n\equiv a^n x_0+(a^n-1)\frac{b}{a-1}\pmod m,$$

$$x_{\varphi(m)+n}\equiv a^{\varphi(m)+n}x_0+(a^{\varphi(m)+n}-1)\frac{b}{a-1}$$

$$\equiv a^n x_0+(a^n-1)\frac{b}{a-1}\equiv x_n\pmod m,$$

由于上式两端都是最小非负剩余，所以结论成立.

(v) 由结论(ii)及(3)式推出. □

引理 对于 $i\geqslant 1$，令 $g_i=(x'_1,\cdots x'_i)$，设 i_0 是使 $g_i\mid x'_{i+1}$ 成立的最小的 i 值，则 $i_0\leqslant 2+[\log_2 m]$.

证明 不失一般性，可以设 $i_0\geqslant 3$. 显然

$$g_1=x'_1,g_{i+1}=(g_i,x'_{i+1}),\quad i\geqslant 1.$$

因此，若 $g_i\nmid x'_{i+1}$，则由引理 1.3.2 可知，

$$|g_{i+1}|\leqslant\frac{1}{2}|g_i|,$$

于是
$$|g_{i_0-1}|\leqslant\frac{1}{2}|g_{i_0-2}|\leqslant\cdots\leqslant\frac{1}{2^{i0-2}}|x'_1|,$$

$$2^{i_0-2}\leqslant|x'_1|\cdot|g_{i_0-1}|^{-1}<m,$$

$$i_0\leqslant[\log_2 m]+2.$$ □

定理 2 存在多项式时间(关于 $\log m$)算法 A，如果已知 $L(x;a,b,m)=\{x_i\}_{i\geqslant 0}$ 的前 i_0+2 个数 $x_i(0\leqslant i\leqslant i_0+1)$，$i_0$ 见于引理，则可以求出 a' 与 b'，使得

$$x_i\equiv a'x_{i-1}+b'\pmod m,\quad i\geqslant 1. \tag{4}$$

证明 首先指出，算法 A 可以由以下步骤组成：

(i) 计算 $x'_i=x_i-x_{i-1},1\leqslant i\leqslant i_0+1$；

(ii) 计算 $d=(x'_1,\cdots,x'_{i_0})$ 及 $y_1,\cdots,y_{i_0}$，使得

$$d=y_1x'_1+\cdots+y_{i_0}x'_{i_0}. \tag{5}$$

(iii) 计算

$$a'=\sum_{i=1}^{i_0} y_i \frac{x'_{i+1}}{d},\quad b'=x_1-a'x_0. \tag{6}$$

下面证明，在步骤(iii)中确定的 a' 与 b' 满足(4)式.

记 $g=(m,d)$，则由(5)式，(2)式，(1)式，及(6)式，推出

$$\begin{aligned} ad &= a\sum_{i=1}^{i_0} y_i x'_i \equiv \sum_{i=1}^{i_0} y_i x'_{i+1} = d\sum_{i=1}^{i_0} y_i \frac{x'_{i+1}}{d} \\ &= a'd \pmod{m}, \end{aligned}$$

因此，由定义 1.5.1 的推论，

$$a\equiv a' \pmod{\frac{m}{g}}.$$

对于 $i\geqslant 1$，有 $g\mid(x'_i,m)$，所以，由上式得到

$$a\equiv a' \pmod{\frac{m}{(x'_i,m)}},\quad i\geqslant 1. \tag{7}$$

另一方面，关于未知数 t 的方程

$$x'_i\cdot t\equiv x'_{i+1} \pmod{m} \tag{8}$$

有解 $t\equiv a(\mathrm{mod}m)$，因此，由定理 1.5.8，方程(8)的通解是

$$t\equiv a+\frac{m}{(x'_i,m)}j, j=0,1,\cdots,(x'_i,m)-1.$$

由(7)式，a' 是方程(8)的解. 于是，对于 $i\geqslant 1$，

$$\begin{aligned} a'x_i+b'-x_{i+1} &= a'x_i+(x_1-a'x_0)-x_{i+1} \\ &= a'(x_i-x_0)-(x_{i+1}-x_1) \\ &= a'\sum_{k=1}^{i} x'_k-\sum_{k=1}^{i} x'_{k+1}=\sum_{k=1}^{i}(a'x'_k-x'_{k+1}) \\ &\equiv 0 \pmod{m}. \end{aligned}$$

□

由定理 1 及定理 2，当 $(a-1)\mid b$ 时，用 $L(x;a,b,m)$ 所生成的数列 $\{x_i\}_{i\geqslant 0}$ 的周期不大于 $\varphi(m)$. 一般地，它的周期 $\leqslant m$. 此外，由引理及定理 2，若已知 $x_0,x_1,\cdots,x_t,t\geqslant 2+[\log_2 m]$，则可

以用多项式时间算法求出使(4)式成立的 a' 与 b'，即可以确定整个 $\{x_i\}_{i\geqslant 0}$. 此外，有下面的定理.

定理 3 设 $\{x_i\}_{i\geqslant 0}$ 由 $L(x;a,b,m)$ 生成. 若已知 $x_0,x_1,\cdots,x_s$，其中 s 不小于使 $g_i|x'_{i+1}$ 成立的最小 i 值与 1 之和，g_i 与 x'_i 见于定理 2. 则存在多项式时间算法，可以求出 a',b',m'，使得

$$x_i\equiv a'x_{i-1}+b' \pmod{m'}$$

对于 $1\leqslant i\leqslant s$ 成立.

这个定理的证明，此处略去. 对于线性伪随机数生成器的其他研究，可参考 D. E. Knuth 的书：The art of computer programming：semi-numerical algorithms.

下面，介绍另一种伪随机数发生器，即 $\frac{1}{p}$—发生器.

以下，在本节中，p 是奇素数，b 是模 p 的一个原根，记 $l(p)=[\log_b p]$，并称它为 p 的长度. 此外，对于满足 $0\leqslant a<b$ 的整数 a，也称它是一个 b—数码.

设 a 是整数，$0<a<b$，记

$$a_m\equiv ab^m \pmod{p},\ 0\leqslant a_m<p,\ m\geqslant 0. \tag{9}$$

由 Fermat 定理(定理 1.5.6 的推论 1)，数列 $\{a_m\}$ 的周期是 $p-1$.

利用 Euclid 算法及(9)式可知，存在非负整数 $q_m(m\geqslant 1)$，使得对于 $m\geqslant 0$，有

$$\frac{a_0}{p}=\frac{q_1}{b}+\frac{q_2}{b^2}+\cdots+\frac{q_m}{b_m}+\frac{1}{b^m}\cdot\frac{a_m}{p}, \tag{10}$$

即

$$a_0b^m=(q_1b^{m-1}+\cdots+q_m)p+a_m. \tag{11}$$

以后，将用

$$(x_1x_2\cdots x_m)_b \text{ 与 } (.x_1x_2\cdots x_m)_b$$

分别表示

$$x_1b^{m-1}+\cdots+x_m \quad 与 \quad \frac{x_1}{b}+\frac{x_2}{b^2}+\cdots+\frac{x_m}{b^m},$$

这样,(10)式与(11)式分别为

$$\frac{a_0}{p}=(.\,q_1\cdots q_m)_b+\frac{1}{b^m}\cdot\frac{a_m}{p}$$

与

$$a_0b^m=(q_1\cdots q_m)_bp+a_m.$$

一般地,容易验证,对于 $i\geqslant 0$,有

$$a_ip^{-1}=(.\,q_{i+1}\cdots q_{i+m})_b+\frac{1}{b^m}\cdot\frac{a_{i+m}}{p}, \tag{12}$$

$$a_ib^m=(q_{i+1}\cdots q_{i+m})_bp+a_{i+m}. \tag{13}$$

定义 2 由 b—数码组成的数列$\{x_i\}_{i\geqslant 1}$若满足以下条件,则称它为以 $p-1$ 为周期的对基 b 的 de Bruijn 数列:

(i) $\{x_i\}_{i\geqslant 1}$是周期等于 $p-1$ 的数列;

(ii) 任何一个由 $l(p)-1$ 个 b—数码组成的有限数列至少与$\{x_i\}$的一个周期内的某一段重合;

(iii) 任何一个由 $l(p)$个 b 一数码组成的有限数列至多与$\{x_i\}$的一个周期内的某一段重合.

例 2 数列 0,1,0,1,0,…是周期为 2 的对基 2 的 de Bruijn 数列($p=3$);

数列 0,1,1,0,0,1,1,0,…是周期为 4 的对基 2 的 de Bruijn 数列($p=5$).

定义 3 对给定的素数 p,模 p 的原根 b,以及正整数 $a<b$,计算(12)式中的 $q_1,q_2,\cdots$的算法,称为$\frac{1}{p}$—发生器,简记为 $P(p;a,b)$,也用 $P(p;a;b)$表示计算出的数列$\{q_i\}_i\geqslant 1$.

注 用$\frac{1}{p}$—发生器计算出的数列$\{q_i\}_{i\geqslant 1}$显然满足

$$\frac{a_k}{p}=(.\,q_{k+1}q_{k+2}\cdots)_b=\sum_{i=1}^{\infty}\frac{q_{k+i}}{b^i},k\geqslant 0. \tag{14}$$

定理 4 对于模 p 的任何原根 b，以及正整数 $a<b$，数列 $P(p;a,b)$是周期为 $p-1$ 的对基 b 的 de Bruijn 数列.

证明 设 $P(p;a,b)=\{q_i\}_{i\geqslant 1}$，则(14)式成立，其中 $a_k(k\geqslant 0)$由(9)式确定. 由于$\{a_k\}_{k\geqslant 0}$是周期为 $p-1$ 的数列，所以，对任何 $i\geqslant 0$，有 $a_i=a_{i+p-1}$，因此，由(14)式得到

$$(.\,q_{i+1}q_{i+2}\cdots)_b=(.\,q_{i+p}q_{i+p+1}\cdots)_b, \tag{15}$$

于是，数列$\{q_k\}_{k\geqslant 1}$的周期必定$\leqslant p-1$.

假设$\{q_k\}$的周期是 t，$0<t<p-1$，则对于任意的 $k\geqslant 1$，

$$(.\,q_{t+k}q_{t+k+1}\cdots)_b=(.\,q_kq_{k+1}\cdots)_b,$$

即是$\frac{a_{k-1+t}}{p}=\frac{a_{k-1}}{p}$，这是不可能的，因为$\{a_i\}$的周期是 $p-1$. 因此，$\{q_k\}$的周期是 $p-1$，定义 2 中的条件(i)满足.

设 $\bar{e}=\{e_1,\cdots,e_\lambda\}$是由 b—数码组成的有限数列，$\lambda\geqslant l(p)-1$. 容易证明，下面的四个结论是等价的：

(i) $\bar{e}$ 是数列$\{q_k\}_{k\geqslant 1}$的一段；

(ii) 存在非负整数 i，使得 $\bar{e}$ 是数列 $q_{i+1},q_{i+2},\cdots$的开始的一段；

(iii) 存在非负整数 i，使得 $\bar{e}$ 是$\frac{a_i}{p}$的 b 进制表示的开始的一段位数码数列；

(iv) 存在非负整数 k，使得 $\bar{e}$ 是$\frac{k}{p}$的 b 进制表示的开始的一段位数码数列.

对于每个由 b 一数码组成的有限数列 $\bar{e}=\{e_1,\cdots,e_\lambda\}$，可以使它与 b 进制数$(.\,e_1\cdots e_\lambda)_b$ 所在的区间

$$\left(\frac{i}{b^\lambda},\frac{i+1}{b^\lambda}\right) \tag{16}$$

相对应，此处 i 是小于 b^λ 的某个非负整数. 显然，这样的区间是唯一的.

因为 $b^{l(p)-1}<p\leqslant b^{l(p)}$，所以

$$\frac{1}{b^{l(p)}}\leqslant\frac{1}{p}<\frac{1}{b^{l(p)-1}},$$

因此，对于任何非负整数 $i<b^{l(p)-1}-1$，下面的两个结论成立：

结论 Ⅰ　至少有一个非负整数 $k<p$，使得

$$\frac{k}{p}\in\left[\frac{i}{b^{l(p)-1}},\frac{i+1}{b^{l(p)-1}}\right);$$

结论 Ⅱ　至多有一个非负整数 $k<p$，使得

$$\frac{k}{p}\in\left[\frac{i}{b^{l(p)}},\frac{i+1}{b^{l(p)}}\right).$$

利用结论(i)—(iv)，结论 Ⅰ，结论 Ⅱ，即可推知 $\{q_i\}_{i\geqslant1}$ 满足定义 2 中的条件(ii)与(iii)(详细证明留作习题).

定理 5　$p,b,\{q_i\}_{i\geqslant1}$，以及 $\{a_m\}_{m\geqslant0}$ 的意义同上. 设 k 是不小于 $\log_b(2p^2)$ 的最小整数，则存在算法 A，由 b 及 $q_{m+1},q_{m+2},\cdots q_{m+k}$（$m$ 是任意的非负整数）可以求出 p 与 a_m，并且，完成这一算法只需要 $O(\log^\lambda p)$ 次比特运算，λ 是正常数.

证明　以 $\frac{P_1}{Q_1},\frac{P_2}{Q_2},\cdots$ 表示 $\frac{\alpha}{b^k}$ 的渐近分数，此处 $\alpha=(q_{m+1}\cdots q_{m+k})_b$. 由 k 的定义可知 $b^k\geqslant2p^2$，因此，由(12)式及

$$\frac{1}{b^k}\cdot\frac{a_{k+m}}{p}<\frac{1}{b^k}$$

得到

$$\left|\frac{\alpha}{b^k}-\frac{a_m}{p}\right|<\frac{1}{b^k}\leqslant\frac{1}{2p^2}.$$

利用定理 3.3.4 及定理 3.3.6 知道，$\frac{a_m}{p}$必是$\frac{\alpha}{b^k}$的一个渐近分数，即存在某个非负整数 i，使得

$$\frac{a_m}{p}=\frac{P_i}{Q_i}. \tag{17}$$

由于$(p,a_m)=(P_i,Q_i)=1$，所以 $a_m=P_i, p=Q_i$.

由以上讨论，算法 A 可以这样设计：依次计算$\frac{\alpha}{b^k}$的渐近分数$\frac{P_1}{Q_1},\frac{P_2}{Q_2},\cdots$，直到某个$\frac{P_j}{Q_j}$的 b 进制表示以 $q_{m+1},\cdots,q_{m+k}$为它的前 k 个位数码时终止. 由(17)式，$j\leqslant i$. 若 $j<i$，则$\frac{P_j}{Q_j}\neq\frac{P_i}{Q_i}$，从而

$$\frac{1}{Q_iQ_j}\leqslant\left|\frac{P_iQ_j-P_jQ_i}{Q_iQ_j}\right|=\left|\frac{P_i}{Q_i}-\frac{P_j}{Q_j}\right|<\frac{1}{b^k}.$$

因为 $j\leqslant i$，所以 $Q_j\leqslant Q_i$，于是由上式，k 的定义，以及 $p=Q_i$，推出

$$2Q_i^2=2p^2\leqslant b^k<Q_iQ_j\leqslant Q_i^2,$$

这个矛盾说明 $j<i$ 是不可能的. 因此，$i=j$，即可以用算法 A 确定出 p 与 a_m.

关于运算时间的估计，留作习题. □

最后，需要指出，在上一节和这一节中所介绍的几种伪随机数生成器，在安全性方面都有不足之处. 比它们有更好安全性的伪随机数生成器是存在的，例如，二次剩余生成器，指标生成器，平方中段生成器，等等. 限于本书篇幅，不再做介绍.

习　题

1. 写出 $L(4;7,11,23)$的前 7 个数.

2. 写出 $P(71;5,7)$的前五个数.

3. (1)用 $e_1,\cdots,e_\lambda$ 表示出(16)式中的 i.

(2)完成定理 4 的证明,即证明 $\{q_i\}_{i\geqslant 1}$ 满足定义 2 中的条件(ii)和(iii).

4. 利用习题 3.3.4,完成定理 5 的证明.