第二章 同余
2015 年04月02 日

信息安全数学基础

陈恭亮 教授 博士生导师

上海交通大学信息安全工程学院

chengl@sjtu.edu.cn

思考题

1. 设m 是正整数.

   1) 对于与m 互素的整数a, 序列$\{a_k = a^k \pmod m, \quad k = 1, 2, \ldots\}$ 是周期序列吗?

   2) 是否存在一个正整数L, 使得: 对于与m 互素的任意整数a, L 都是序列$\{a_k = a^k \pmod m, \quad k = 1, 2, \ldots\}$ 的一个周期? 如何证明欧拉函数$\varphi(m)$ 就是这样的周期?

   3) 序列$\{a_k = a^k \pmod m, \quad k = 1, 2, \ldots\}$ 的最小周期$l(a)$ 是欧拉函数$\varphi(m)$ 的因子吗?

   4) 对于整数e, $(e, l(a)) = 1$, 存在整数d 使得$e \cdot d \equiv 1 \mod m$. 从而, 对于$a^e \equiv c \pmod m$, 有$c^d \equiv a \pmod m$

注 $\{a_k\}_{k\geq 1}$ 称为周期序列, 如果存在一个整数L 使得: 对任意$k \geq 1$, 都有$a_{k+L} = a_k$. 这时, L 称为序列$\{a_k\}_{k\geq 1}$ 的一个周期. 进一步, 称最小的周期L 为序列$\{a_k\}_{k\geq 1}$ 的周期, 记作$l(a)$.

访问主页
标题页
目录页
第 2 页 共 43 页
返回
全屏显示
关闭
退出

2.4.1 欧拉定理

例2.4.1 设 $m=7,\ a=2$. 我们有 $(2,7)=1,\ \varphi(7)=6$.
考虑模 7 的最小非负简化剩余系 1, 2, 3, 4, 5, 6, 有

$$2\cdot1\equiv2,\ 2\cdot2\equiv4,\ 2\cdot3\equiv6,\ 2\cdot4\equiv1,\ 2\cdot5\equiv3,\ 2\cdot6\equiv5,\ (\mathrm{mod}\ 7).$$

上述同余式左右对应相乘, 得到

$$(2\cdot1)(2\cdot2)(2\cdot3)(2\cdot4)(2\cdot5)(2\cdot6)\equiv2\cdot4\cdot6\cdot1\cdot3\cdot5\ (\mathrm{mod}\ 7)$$

或

$$2^6\cdot1\cdot2\cdot3\cdot4\cdot5\cdot6\equiv1\cdot2\cdot3\cdot4\cdot5\cdot6\ (\mathrm{mod}\ 7).$$

注意到

$$1\cdot2\cdot3\cdot4\cdot5\cdot6\equiv(1\cdot6)(2\cdot4)(3\cdot5)\equiv(-1)\cdot1\cdot1\equiv-1\ (\mathrm{mod}\ 7),$$

故 $2^6\equiv1\ (\mathrm{mod}\ 7)$.

例2.4.2 设 $m=30,\ a=7$. 我们有 $(7,30)=1,\ \varphi(30)=8$.
考虑模 30 的最小非负简化剩余系 $1,\ 7,\ 11,\ 13,\ 17,\ 19,\ 23,\ 29$, 有

$$\begin{array}{lll} 7\cdot 1\equiv 7, & 7\cdot 7=49\equiv 19, & 7\cdot 11=77\equiv 17, \\ 7\cdot 13=91\equiv 1, & 7\cdot 17=119\equiv 29, & 7\cdot 19=133\equiv 13, \\ 7\cdot 23=161\equiv 11, & 7\cdot 29=203\equiv 23 & \pmod{30}. \end{array}$$

上述同余式左右对应相乘, 得到

$$\begin{aligned} & (7\cdot 1)(7\cdot 7)(7\cdot 11)(7\cdot 13)(7\cdot 17)(7\cdot 19)(7\cdot 23)(7\cdot 29) \\ \equiv\ & 7\cdot 19\cdot 17\cdot 1\cdot 29\cdot 13\cdot 11\cdot 23 \pmod{30} \end{aligned}$$

或

$$7^8\cdot 1\cdot 7\cdot 11\cdot 13\cdot 17\cdot 19\cdot 23\cdot 29\equiv 1\cdot 7\cdot 11\cdot 13\cdot 17\cdot 19\cdot 23\cdot 29 \pmod{30}.$$

注意到 $(1\cdot 7\cdot 11\cdot 13\cdot 17\cdot 19\cdot 23\cdot 29,\ 30)=1$, 故 $7^8\equiv 1 \pmod{30}$.

例2.4.1 和例2.4.2 可推广为一般的结论, 即欧拉定理.

定理2.4.1 (Euler) 如果 $(a, m) = 1$, 则 $a^{\varphi(m)} \equiv 1 \pmod m$.

证 取 $r_1, \ldots, r_{\varphi(m)}$ 为模 m 的一个最小正简化剩余系, 则当 a 是满足 $(a, m) = 1$ 的整数时, $ar_1, \ldots, ar_{\varphi(m)}$ 也为模 m 的一个简化剩余系, 这就是说,

$$ar_1, \ldots, ar_{\varphi(m)}$$

模 m 的最小正剩余是 $r_1, \ldots, r_{\varphi(m)}$ 的一个排列. 故乘积 $(ar_1)\cdots(ar_{\varphi(m)})$ 模 m 的最小正剩余和乘积 $r_1\cdots r_{\varphi(m)}$ 模 m 的最小正剩余相等. 即

$$(ar_1)\cdots(ar_{\varphi(m)}) \equiv r_1\cdots r_{\varphi(m)} \pmod m.$$

因此, $r_1\cdots r_{\varphi(m)}\,(a^{\varphi(m)} - 1) \equiv 0 \pmod m$. 又从

$$(r_1, m) = 1, \ldots, (r_{\varphi(m)}, m) = 1$$

及定理1.3.12, 可推出 $(r_1\cdots r_{\varphi(m)},\ m) = 1$.

从而, 根据定理2.1.8, 得到 $a^{\varphi(m)} - 1 \equiv 0 \pmod m$.

例2.4.3 设 $m = 11,\ a = 2$. 则 $(2, 11) = 1,\ \varphi(11) = 10$. 故

$$2^{10} \equiv 1 \pmod{11}.$$

例2.4.4 设 $m = 23,\ 23 \nmid a$. 我们有 $(a, 23) = 1,\ \varphi(23) = 22$. 故

$$a^{22} \equiv 1 \pmod{23}.$$

例2.4.5 设p, q 是两个不同的奇素数, $n = p \cdot q$, a 是与n 互素的整数. 如果整数e 满足

$$1 < e < \varphi(n), \ (e, \varphi(n)) = 1, \tag{1}$$

那么存在整数d, $1 \le d < \varphi(n)$, 使得

$$e \cdot d \equiv 1 \pmod{\varphi(n)}. \tag{2}$$

而且, 对于整数

$$a^e \equiv c \pmod{n}, \quad 1 \le c < n, \tag{3}$$

有

$$c^d \equiv a \pmod{n}. \tag{4}$$

证 因为$(e,\varphi(n))=1$, 根据定理2.3.5, 存在整数$d,\ 1\le d<\varphi(n)$, 使得(2) 成立. 因此, 存在一个正整数k 使得$e\cdot d=1+k\cdot\varphi(n)$. 现在, 根据定理2.4.1 , 得到

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

两端作$k\cdot\dfrac{\varphi(n)}{\varphi(p)}$ 次幂, 并乘以a 得到

$$a^{1+k\cdot\varphi(n)}\equiv a\ (\mathrm{mod}\ p),$$

即 $a^{e\cdot d}\equiv a\ (\mathrm{mod}\ p)$.
同理, $a^{e\cdot d}\equiv a\ (\mathrm{mod}\ q)$.
因为p 和q 是不同的素数, 根据定理2.1.12 ,

$$a^{e\cdot d}\equiv a\ (\mathrm{mod}\ n),$$

因此,

$$c^d\equiv(a^e)^d\equiv a\ (\mathrm{mod}\ n).$$

2.4.2 费马小定理

定理 2.4.2 (Fermat) 设 p 是一个素数. 则对任意整数 a, 有

$$a^p \equiv a \pmod{p}.$$

证 我们分两种情形考虑.

i) 若 $p \mid a$, 则同时有 $a \equiv 0 \pmod{p}$ 和 $a^p \equiv 0 \pmod{p}$. 因此,

$$a^p \equiv a \pmod{p}.$$

ii) 若 a 不被 p 整数, 则 $(a, p) = 1$ (见例1.3.4). 根据定理 2.4.1,

$$a^{p-1} \equiv 1 \pmod{p}.$$

两端同乘 a, 得到

$$a^p \equiv a \pmod{p}.$$

将费马小定理(定理2.4.2)作进一步的推广,

推论 设p 是一个素数. 则对任意整数a, 以及对任意正整数t, k,,

$$a^{t+k(p-1)} \equiv a^t \pmod p. \tag{5}$$

证 我们分两种情形考虑.

i) 若a 被p 整数, 则同时有

$$a^t \equiv 0 \pmod p \quad \text{和} \quad a^{t+k(p-1)} \equiv 0 \pmod p.$$

因此, (5) 成立.

ii) 若a 不被p 整数, 则$(a, p) = 1$ (见例1.3.4). 根据定理2.4.1,

$$a^{p-1} \equiv 1 \pmod p.$$

两端作k 次方, 有

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

两端左乘a^t, 得到(5) . 证毕

例2.4.6 设$p = 7$. 对任意正整数k, 我们有

$$a^{1+k\cdot 6} \equiv a \pmod p$$

2.4.3 Wilson 定理

定理2.4.3 (Wilson) 设 p 是一个素数. 则

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

证 若 $p=2$, 结论显然成立.

现设 $p \geq 3$. 根据定理2.3.5, 对于每个整数 a, $1 \leq a \leq p-1$, 存在惟一的整数 a', $1 \leq a' \leq p-1$, 使得

$$aa' \equiv 1 \pmod p.$$

又而 $a' = a$ 的充要条件是 a 满足 $a^2 \equiv 1 \pmod p$. 这时, $a=1$ 或 $a = p-1$.

我们将 $2, \cdots, p-2$ 中的 a 与 a' 配对, 得到

$$1 \cdot 2 \cdots (p-2)(p-1) \equiv 1 \cdot (p-1) \prod_a aa' \equiv 1 \cdot (p-1) \equiv -1 \pmod p.$$

因此, 定理2.4.3 成立.

例2.4.7 设 $p = 17$. 我们有

$$\begin{array}{lll} 2\cdot 9 = 18 \equiv 1, & 3\cdot 6 = 18 \equiv 1, & 4\cdot 13 = 52 \equiv 1, \\ 5\cdot 7 = 35 \equiv 1, & 8\cdot 15 = 120 \equiv 1, & 10\cdot 12 = 120 \equiv 1, \\ 11\cdot 14 = 154 \equiv 1, & 1\cdot 16 \equiv -1 & \pmod{17}. \end{array}$$

因此,

$$\begin{aligned} & 1\cdot 2\cdot 3\cdot 4\cdot 5\cdot 6\cdot 7\cdot 8\cdot 9\cdot 10\cdot 11\cdot 12\cdot 13\cdot 14\cdot 15\cdot 16 \\ = \ & (1\cdot 16)(2\cdot 9)(3\cdot 6)(4\cdot 13)(5\cdot 7)(8\cdot 15)(10\cdot 12)(11\cdot 14) \\ \equiv \ & (-1)\cdot 1\cdot 1\cdot 1\cdot 1\cdot 1\cdot 1\cdot 1 \\ \equiv \ & -1 \pmod{17}. \end{aligned}$$

2.5 模重复平方计算法

在模算术计算中, 常对大整数模 m 和大整数 n , 计算

$$b^n \pmod{m}. \tag{6}$$

当然, 可以递归地计算

$$b^n \equiv (b^{n-1} \pmod{m}) \cdot b \pmod{m}.$$

但这种计算较为费时, 须作 $n-1$ 次乘法.
注意到如下的计算特性:

$$b^{16} \equiv \left(\left(\left(b^2\right)^2\right)^2\right)^2 \pmod{m}, \quad b^{128} \equiv \left(\left(\left(\left(\left(\left(b^2\right)^2\right)^2\right)^2\right)^2\right)^2\right)^2 \pmod{m}.$$

则我们可以优化模m 运算.

现在, 将n 写成二进制:

$$n = n_0 + n_1 2 + \cdots + n_{k-1} 2^{k-1}, \qquad n_i \in \{0, 1\},\ i = 0, 1, \ldots, k-1. \tag{7}$$

则(6) 的计算可归纳为

$$b^n \equiv \underbrace{\underbrace{\underbrace{\underbrace{\underbrace{b^{n_0}}_{a_0}(\underbrace{b^2}_{b_1})^{n_1}}_{a_1} \cdot \cdots}_{a_{k-3}} \cdot (\underbrace{b^{2^{k-2}}}_{b_{k-2}})^{n_{k-2}}}_{a_{k-2}} \cdot (\underbrace{b^{2^{k-1}}}_{b_{k-1}})^{n_{k-1}}}_{a_{k-1}} \pmod m. \tag{8}$$

或

$$a_0 = b^{n_0},\ \ b_0 = b, \quad b_i = b_{i-1}^2,\ \ a_i = a_{i-1} \cdot b_i, \qquad i = 1, \ldots, k-1. \tag{9}$$

我们最多作$2[\log_2 n]$ 次乘法. 这个计算方法叫做“模重复平方计算法”. 具体算法如下:

$$b^n \equiv \underbrace{\underbrace{\underbrace{b^{n_0}(b^2)^{n_1}}_{a_1}\cdot\cdots\cdot(b^{2^{k-2}})^{n_{k-2}}}_{a_{k-2}}\cdot(b^{2^{k-1}})^{n_{k-1}}}_{a_{k-1}} \pmod{m}.$$

0). 令 $a = 1$, 并将 n 写成二进制: $n = n_0 + n_1 2 + \cdots + n_{k-1}2^{k-1}$, 其中 $n_i \in \{0, 1\}$, $i = 0, 1, \ldots, k-1$.

1). 如果 $n_0 = 1$, 则计算 $a_0 \equiv a \cdot b \pmod{m}$, 否则取 $a_0 = a$. 即计算

$$a_0 \equiv a \cdot b^{n_0} \pmod{m}.$$

再计算 $b_1 \equiv b^2 \pmod{m}$.

2). 如果 $n_1 = 1$, 则计算 $a_1 \equiv a_0 \cdot b_1 \pmod{m}$, 否则取 $a_1 = a_0$. 即计算

$$a_1 \equiv a_0 \cdot b_1^{n_1} \pmod{m}.$$

再计算 $b_2 \equiv b_1^2 \pmod{m}$.

$\cdots\cdots$

$$b^n \equiv \underbrace{\underbrace{\underbrace{b^{n_0}(b^2)^{n_1}}_{a_1} \cdots\cdots (b^{2^{k-2}})^{n_{k-2}}}_{a_{k-2}} \cdot (b^{2^{k-1}})^{n_{k-1}}}_{a_{k-1}} \pmod{m}.$$

模重复平方计算法的具体算法如下:

k-1). 如果 $n_{k-2} = 1$, 则计算 $a_{k-2} \equiv a_{k-3} \cdot b_{k-2} \pmod{m}$,
否则取 $a_{k-2} = a_{k-3}$. 即计算

$$a_{k-2} \equiv a_{k-3} \cdot b_{k-2}^{n_{k-2}} \pmod{m}.$$

再计算 $b_{k-1} \equiv b_{k-2}^2 \pmod{m}$.

k). 如果 $n_{k-1} = 1$, 则计算 $a_{k-1} \equiv a_{k-2} \cdot b_{k-1} \pmod{m}$,
否则取 $a_{k-1} = a_{k-2}$. 即计算

$$a_{k-1} \equiv a_{k-2} \cdot b_{k-1}^{n_{k-1}} \pmod{m}.$$

最后, a_{k-1} 就是 $b^n \pmod{m}$.

将上述过程列成表格为:

i	n_i	a_i	b_i
0	n_0	a_0	b_0
1	n_1	a_1	b_1
$\vdots$	$\vdots$	$\vdots$	$\vdots$
$i-1$	n_{i-1}	a_{i-1}	b_{i-1}
i	n_i	a_i	b_i
$\vdots$	$\vdots$	$\vdots$	$\vdots$
$k-2$	n_{k-2}	a_{k-2}	b_{k-2}
$k-1$	n_{k-1}	a_{k-1}	b_{k-1}

其中
$$\left\{\begin{array}{rclclrcll}
b_0 & = & b & = & b^{2^0}, & a_0 & = & b_0^{n_0} & \\
b_1 & = & b^2 & = & b_0^2, & a_1 & = & a_0 \cdot b_1^{n_1} & \\
 & \vdots & & & & & & & \\
b_i & = & b^{2^i} & = & b_{i-1}^2, & a_i & \equiv & a_{i-1} \cdot b_i^{n_i} \pmod{m} & i \geq 1 \\
 & \vdots & & & & & & & \\
b_{k-1} & = & b^{2^{k-1}} & = & b_{k-2}^2, & a_{k-1} & \equiv & a_{k-2} \cdot b_{k-1}^{n_{k-1}} \pmod{m} &
\end{array}\right.$$

注 在上述表达式中, b_i 的计算可以说是不变的，但a_i 的计算却依赖n.

例2.5.1 计算$12996^{227} \pmod{37909}$.

解 设$m = 37909$, $b = 12996$. 令$a = 1$. 将227 写成二进制,

$$227 = 1 + 2 + 2^5 + 2^6 + 2^7.$$

运用模重复平方法, 我们依次计算如下:

$$12996^{227} = 12996 \cdot (12996^2) \cdot (12996^{2^5}) \cdot (12996^{2^6}) \cdot (12996^{2^7})$$

0). $n_0 = 1$. 计算 $a_0 = a \cdot b \equiv 12996$, $\quad b_1 \equiv b^2 \equiv 11421 \pmod{37909}$.

1). $n_1 = 1$. 计算 $a_1 = a_0 \cdot b_1 \equiv 13581$, $\quad b_2 \equiv b_1^2 \equiv 32281 \pmod{37909}$.

2). $n_2 = 0$. 计算 $a_2 = a_1 \equiv 13581$, $\quad b_3 \equiv b_2^2 \equiv 20369 \pmod{37909}$.

3). $n_3 = 0$. 计算 $a_3 = a_2 \equiv 13581$, $\quad b_4 \equiv b_3^2 \equiv 20065 \pmod{37909}$.

4). $n_4 = 0$. 计算 $a_4 = a_3 \equiv 13581$, $\quad b_5 \equiv b_4^2 \equiv 10645 \pmod{37909}$.

5). $n_5 = 1$. 计算 $a_5 = a_4 \cdot b_5 \equiv 22728$, $\quad b_6 \equiv b_5^2 \equiv 6024 \pmod{37909}$.

6). $n_6 = 1$. 计算 $a_6 = a_5 \cdot b_6 \equiv 24073$, $\quad b_7 \equiv b_6^2 \equiv 9663 \pmod{37909}$.

7). $n_7 = 1$. 计算 $a_7 = a_6 \cdot b_7 \equiv 7775 \pmod{37909}$.

最后, 计算出 $12996^{227} \equiv 7775 \pmod{37909}$.

访问主页
标题页
目录页
第 19 页 共 43 页
返回
全屏显示
关闭
退出

写成表格为

i	n_i	a_i	b_i	i	n_i	a_i	b_i
0	1	12996	12996	4	0	13581	20065
1	1	13581	11421	5	1	22728	10645
2	0	13581	32281	6	1	24073	6024
3	0	13581	20369	7	1	7775	9663

共有11 次乘法运算（包括7 次平方和4 次乘法）.

例2.5.2 计算$312^{13} \pmod{667}$.

解 设$m = 667$, $b = 312$. 令$a = 1$. 将13 写成二进制,

$$13 = 1 + 2^2 + 2^3.$$

运用模重复平方法, 我们依次计算如下:

0). $n_0 = 1$. 计算 $a_0 = a \cdot b \equiv 312, \quad b_1 \equiv b^2 \equiv 629 \pmod{667}$.

1). $n_1 = 0$. 计算 $a_1 = a_0 \equiv 312, \quad b_2 \equiv b_1^2 \equiv 110 \pmod{667}$.

2). $n_2 = 1$. 计算 $a_2 = a_1 \cdot b_2 \equiv 303, \quad b_3 \equiv b_2^2 \equiv 94 \pmod{667}$.

3). $n_3 = 1$. 计算 $a_3 = a_2 \cdot b_3 \equiv 468 \pmod{667}$.

最后, 计算出$312^{13} \equiv 468 \pmod{667}$.

写成表格为

i	n_i	a_i	b_i	i	n_i	a_i	b_i
0	1	312	312	2	1	303	110
1	0	312	629	3	1	468	94

例2.5.3 计算$501^{13} \pmod{667}$.

解 设$m = 667$, $b = 312$. 令$a = 1$. 将13 写成二进制,

$$13 = 1 + 2^2 + 2^3.$$

运用模重复平方法, 我们依次计算如下:

0). $n_0 = 1$. 计算 $a_0 = a \cdot b \equiv 501, \quad b_1 \equiv b^2 \equiv 209 \pmod{667}$.

1). $n_1 = 0$. 计算 $a_1 = a_0 \equiv 501, \quad b_2 \equiv b_1^2 \equiv 326 \pmod{667}$.

2). $n_2 = 1$. 计算 $a_2 = a_1 \cdot b_2 \equiv 578, \quad b_3 \equiv b_2^2 \equiv 223 \pmod{667}$.

3). $n_3 = 1$. 计算 $a_3 = a_2 \cdot b_3 \equiv 163 \pmod{667}$.

最后, 计算出 $501^{13} \equiv 163 \pmod{667}$.

写成表格为

i	n_i	a_i	b_i	i	n_i	a_i	b_i
0	1	501	501	2	1	578	326
1	0	501	209	3	1	163	223

例2.5.4 计算$468^{237} \pmod{667}$.

解 设$m = 667$, $b = 468$. 令$a = 1$. 将237 写成二进制,

$$237 = 1 + 2^2 + 2^3 + 2^5 + 2^6 + 2^7.$$

运用模重复平方法, 我们依次计算如下:

0). $n_0 = 1$. 计算 $a_0 = a \cdot b \equiv 468$, $b_1 \equiv b^2 \equiv 248 \pmod{667}$.

1). $n_1 = 0$. 计算 $a_1 = a_0 \equiv 468$, $b_2 \equiv b_1^2 \equiv 140 \pmod{667}$.

2). $n_2 = 1$. 计算 $a_2 = a_1 \cdot b_2 \equiv 154$, $b_3 \equiv b_2^2 \equiv 257 \pmod{667}$.

3). $n_3 = 1$. 计算 $a_3 = a_2 \cdot b_3 \equiv 225$, $b_4 \equiv b_3^2 \equiv 16 \pmod{667}$.

4). $n_4 = 0$. 计算 $a_4 = a_3 \equiv 225$, $b_5 \equiv b_4^2 \equiv 256 \pmod{667}$.

5). $n_5 = 1$. 计算 $a_5 = a_4 \cdot b_5 \equiv 238$, $b_6 \equiv b_5^2 \equiv 170 \pmod{667}$.

6). $n_6 = 1$. 计算 $a_6 = a_5 \cdot b_6 \equiv 440$, $b_7 \equiv b_6^2 \equiv 219 \pmod{667}$.

7). $n_7 = 1$. 计算 $a_7 = a_6 \cdot b_7 \equiv 312 \pmod{667}$.

最后, 计算出

$$468^{237} \equiv 312 \pmod{667}.$$

例2.5.5 计算$163^{237} \pmod{667}$.

解 设$m=667,\ b=468$. 令$a=1$. 将237 写成二进制,

$$237 = 1 + 2^2 + 2^3 + 2^5 + 2^6 + 2^7.$$

运用模重复平方法, 我们依次计算如下:

0). $n_0=1$. 计算 $a_0 = a\cdot b \equiv 163,\quad b_1 \equiv b^2 \equiv 556 \pmod{667}$.

1). $n_1=0$. 计算 $a_1 = a_0 \equiv 163,\quad b_2 \equiv b_1^2 \equiv 315 \pmod{667}$.

2). $n_2=1$. 计算 $a_2 = a_1\cdot b_2 \equiv 653,\quad b_3 \equiv b_2^2 \equiv 509 \pmod{667}$.

3). $n_3=1$. 计算 $a_3 = a_2\cdot b_3 \equiv 211,\quad b_4 \equiv b_3^2 \equiv 285 \pmod{667}$.

4). $n_4=0$. 计算 $a_4 = a_3 \equiv 211,\quad b_5 \equiv b_4^2 \equiv 518 \pmod{667}$.

5). $n_5=1$. 计算 $a_5 = a_4\cdot b_5 \equiv 577,\quad b_6 \equiv b_5^2 \equiv 190 \pmod{667}$.

6). $n_6=1$. 计算 $a_6 = a_5\cdot b_6 \equiv 242,\quad b_7 \equiv b_6^2 \equiv 82 \pmod{667}$.

7). $n_7=1$. 计算 $a_7 = a_6\cdot b_7 \equiv 501 \pmod{667}$.

最后, 计算出

$$163^{237} \equiv 501 \pmod{667}.$$

因为n 的二进制可写成

$$\begin{aligned} n &= n_0 + n_1 \cdot 2 + \cdots + n_{k-3} \cdot 2^{k-3} + n_{k-2} \cdot 2^{k-2} + n_{k-1} \cdot 2^{k-1} \\ &= n_0 + (n_1 + \cdots \underbrace{(n_{k-3} + \underbrace{(n_{k-2} + \underbrace{(n_{k-1} \cdot 2)} \cdot 2)} \cdot 2)} \cdots) \cdot 2 \end{aligned}$$

所以我们有 $b^n = b^{n_0} \cdot (b^{n_1} \cdots \cdot \underbrace{(b^{n_{k-3}} \cdot \underbrace{(b^{n_{k-2}} \cdot (\underbrace{(b^{n_{k-1}})^2})^2})^2)} \cdots)^2$

将227 写成

$$\begin{aligned} 227 &= 1 + 113 \cdot 2 = 1 + (1 + 7 \cdot 2^4) \cdot 2 = 1 + (1 + (1 + 3 \cdot 2) \cdot 2^4) \cdot 2 \\ &= 1 + (1 + (1 + (1 + 2) \cdot 2) \cdot 2^4) \cdot 2 \end{aligned}$$

我们有 $b^{227} = b \cdot (\underbrace{b \cdot (\underbrace{b \cdot (\underbrace{b \cdot b^2})^2})^{2^4}})^2$

共有11次乘法运算（包括7 次平方和4 次乘法）. 此运算方法的计算量（平方运算个数和乘法运算个数）与模重复平方法的计算量相同. 且进行乘法运算的一个乘法因子b 是固定的. 这样当b 很小时, 乘法运算的时间可忽略不计，由此得到的总运算时间就等同于$[\log_2 n]$ 个平方运算的时间.

写成加法时我们有

$$
\begin{aligned}
n &= n_{k-1}\cdot 2^{k-1} + n_{k-2}\cdot 2^{k-2} + n_{k-3}\cdot 2^{k-3} + \cdots + n_1\cdot 2 + n_0 \\
&= 2\cdot(\cdots 2\cdot(\underbrace{2\cdot(\underbrace{2\cdot(\underbrace{2\cdot n_{k-1}})+n_{k-2}})+n_{k-3}}) + \cdots + n_1) + n_0
\end{aligned}
$$

和

$$
nP = 2\cdot(\cdots 2\cdot(\underbrace{2\cdot(\underbrace{2\cdot(\underbrace{2\cdot n_{k-1}P})+n_{k-2}P})+n_{k-3}P}) + \cdots + n_1P) + n_0P
$$

$$
227 = 2^7 + 2^6 + 2^5 + 2 + 1 = 2\cdot(2^4\cdot(2\cdot(2+1)+1)+1)+1
$$

$$
227P = 2(2^4(2(2P+P)+P)+P)+P
$$

例2.5.6 计算$12996^{227} \pmod{37909}$.

解 设$m = 37909$, $b = 12996$. 令$a = 1$. 将227 写成二进制,

$$227 = 1 + 2 + 2^5 + 2^6 + 2^7.$$

我们可以依次计算如下:

1). $n_7 = 1$. 计算 $a_7 = b^{n_7} \equiv 12996$, $b_7 \equiv a_7^2 \equiv 11421 \pmod{37909}$.

2). $n_6 = 1$. 计算 $a_6 = b^{n_6} \cdot b_7 \equiv 13581$, $b_6 \equiv a_6^2 \equiv 16276 \pmod{37909}$.

3). $n_5 = 1$. 计算 $a_5 = b^{n_5} \cdot b_6 \equiv 28585$, $b_5 \equiv a_5^2 \equiv 11639 \pmod{37909}$.

4). $n_4 = 0$. 计算 $a_4 = b^{n_4} \cdot b_5 \equiv 11639$, $b_4 \equiv a_4^2 \equiv 17464 \pmod{37909}$.

5). $n_3 = 0$. 计算 $a_3 = b^{n_3} \cdot b_4 \equiv 17464$, $b_3 \equiv a_3^2 \equiv 13391 \pmod{37909}$.

6). $n_2 = 0$. 计算 $a_2 = b^{n_2} \cdot b_3 \equiv 13391$, $b_2 \equiv a_2^2 \equiv 9311 \pmod{37909}$.

7). $n_1 = 1$. 计算 $a_1 = b^{n_1} \cdot b_2 \equiv 228$, $b_1 \equiv a_1^2 \equiv 14075 \pmod{37909}$.

8). $n_0 = 1$. 计算 $a_0 = b^{n_0} \cdot b_1 \equiv 7775 \pmod{37909}$.

最后, 计算出

$$12996^{227} \equiv 7775 \pmod{37909}.$$

如果不习惯a_i, b_i 的下标是从大到小，我们可以将下标换成从小到大:

例2.5.6 计算$12996^{227} \pmod{37909}$.

解 设$m = 37909$, $b = 12996$. 令$a = 1$. 将227 写成二进制,

$$227 = 1 + 2 + 2^5 + 2^6 + 2^7.$$

我们可以依次计算如下:

1). $n_7 = 1$. 计算 $a_0 = b^{n_7} \equiv 12996$, $b_0 \equiv a_0^2 \equiv 11421 \pmod{37909}$.

2). $n_6 = 1$. 计算 $a_1 = b^{n_6} \cdot b_0 \equiv 13581$, $b_1 \equiv a_1^2 \equiv 16276 \pmod{37909}$.

3). $n_5 = 1$. 计算 $a_2 = b^{n_5} \cdot b_1 \equiv 28585$, $b_2 \equiv a_2^2 \equiv 11639 \pmod{37909}$.

4). $n_4 = 0$. 计算 $a_3 = b^{n_4} \cdot b_2 \equiv 11639$, $b_3 \equiv a_3^2 \equiv 17464 \pmod{37909}$.

5). $n_3 = 0$. 计算 $a_4 = b^{n_3} \cdot b_3 \equiv 17464$, $b_4 \equiv a_4^2 \equiv 13391 \pmod{37909}$.

6). $n_2 = 0$. 计算 $a_5 = b^{n_2} \cdot b_4 \equiv 13391$, $b_5 \equiv a_5^2 \equiv 9311 \pmod{37909}$.

7). $n_1 = 1$. 计算 $a_6 = b^{n_1} \cdot b_5 \equiv 228$, $b_6 \equiv a_6^2 \equiv 14075 \pmod{37909}$.

8). $n_0 = 1$. 计算 $a_7 = b^{n_0} \cdot b_6 \equiv 7775 \pmod{37909}$.

最后, 计算出

$$12996^{227} \equiv 7775 \pmod{37909}.$$