初等数论

II

陈景润 著

科学出版社

初等数论

II

陈景润 著

科学出版社

1980

内 容 简 介

本书是《初等数论》I 的续集，书中介绍了剩余系、数论函数、三角和等方法．每章后有习题，书末附全部习题解答．本书可作为高中学生的课外参考书，也可供中学数学教师及广大数学爱好者阅读．

初 等 数 论

II

陈景润 著

*

科学出版社出版

北京朝阳门内大街137号

中国科学院印刷厂印刷

新华书店北京发行所发行　各地新华书店经售

*

1980年5月第一版　开本：787×1092　1/32

1980年5月第一次印刷　印张：5 3/4

印数：0001—79,130　字数：130,000

统一书号：13031·1249

本社书号：1740·13—1

定价：0.48元

序　言

本书是《初等数论》Ⅰ的续集．书中的内容和中学的数学课程有密切的联系．例如使用连分数的方法可以较快地开平方，并得到较准确的结果；使用数论中的某些初等方法可以较简单地解决高中代数课程中某些较难的问题；使用三角和的方法可以解决高中三角学课程中的不少问题；因而本书也可作为高中数学的课外读物．书中附有一定数量的习题，由于数论的习题较难做，所以在书末附有习题解答．由于本书的读者主要是高中程度的青年同志，所以我力求把此书写得浅显通俗，容易看懂．但由于能力所限，本书很可能存在缺点错误，诚恳希望同志们批评指正．

在本书的写作过程中，中国科学院数学研究所王元、丁夏畦、于坤瑞同志及中国科技大学研究生院丁平和张明尧同志阅读过本书的初稿并提出了宝贵的意见，北京电机厂七·二一大学的领导和老师对本书的写作给予了大力支持，特别是戚鸣皋老师用了大量时间，阅读本书初稿，并做了习题解答，在这里谨向他们表示衷心感谢．

陈景润

1978年12月23日

目　录

第五章　剩余系，欧拉定理、费尔马定理及其应用

§1. 应用方面的例子

设 a, b, c, d 都是正整数. 令 $a^0 = 1$, $a^1 = a$, $a^2 = a \times a$, $a^3 = a \times a \times a$. 当 n 是一个大于 1 的正整数时，我们用 a^n 来表示由 n 个相同的 a 相乘所得的积. 我们还用 a^{b^n} 来表示由 b^n 个相同的 a 相乘所得的积. 由于 $3^4 = 3 \times 3 \times 3 \times 3 = 81$，所以有

$$2^{3^4} = 2^{81} > 10^{24} > 10^4 > (2^3)^4.$$

由于 $4^5 = 1024$，所以有

$$3^{4^5} = 3^{1024} > 10^{488} > (81)^5 = (3^4)^5.$$

因而

$$2^{3^4} > 10^{20} \times (2^3)^4, \quad 3^{4^5} > 10^{478} \times (3^4)^5.$$

由于 $5^6 = 15625$, $6^7 = 279936$，所以有

$$4^{5^6} = 4^{15625} > 10^{9407}, \quad 5^{6^7} = 5^{279936} > 10^{195666}.$$

但是

$$(4^5)^6 = (1024)^6 < 10^{19}, \quad (5^6)^7 = (15625)^7 < 10^{30},$$

因而

$$4^{5^6} > 10^{9388} \times (4^5)^6, \quad 5^{6^7} > 10^{195636} \times (5^6)^7.$$

我们用 $a^{b^{c^n}}$ 来表示由 b^{c^n} 个相同的 a 相乘所得的积，所以有

$$3^{4^{5^6}} = 3^{4^{15625}} \geqslant 10^{10^{9406}}, \quad 4^{5^{6^7}} > 10^{10^{195665}},$$

$$(3^{4^5})^6 = 3^{1024 \times 6} = 3^{6144} \leqslant 10^{2932},$$

$$(4^{5^6})^7 = 4^{15625 \times 7} = 4^{109375} \leqslant 10^{65851}.$$

我们又有

$$(12345^{56}+50)^{40}\leqslant(10^{230})^{40}=10^{9200}\leqslant 10^{9407}\leqslant 4^{56}.$$

设 A 是一个小于 7 的非负整数. 在本章中将证明，如果今天是星期天，从今天起再经过 a^{b^c} 天后是星期 A，那么从今天起再经过 $a^{b^{c^n}}$ 天后，也是星期 A. 其中 n 是任意正整数，而星期 0 定义为星期天. 如果今天是星期天，那么使用本章中所讨论的方法，容易计算出从今天起再经过 a^{b^c} 天后是星期几.

例 1 如果今天是星期一，c 是一个正整数，那么从今天起再过 773^{3169^c} 天后，应该是星期四.

在本章 §5 中将对例 1 加以证明. 令 m 是一个正整数，使用本章中所讨论的方法可以计算出 $(a^b+c)^d$ 被 m 除的余数.

例 2 求证 $(12371^{56}+34)^{28+72^c}$ 被 111 除的余数等于 70，其中 c 是任意非负整数.

在本章 §5 中将给出例 2 的证明. 我们将在第六章说明欧拉定理、费尔马定理在研究循环小数时的作用.

§2. 完全剩余系

设 a，b 是任意二个整数，m 是一个正整数，如果存在一个整数 q，使得 $a-b=mq$ 成立，我们就说 a，b 对模 m 同余，记作 $a\equiv b(\mathrm{mod}\ m)$.

引理 1 如果 a，b，c 是任意三个整数，m 是一个正整数，则当 $a\equiv b(\mathrm{mod}\ m)$，$b\equiv c(\mathrm{mod}\ m)$ 成立时，有

$$a\equiv c(\mathrm{mod}\ m).$$

证 由 $a-b=mq_1$，$b-c=mq_2$，其中 q_1，q_2 是二个整数，得到 $a-b+b-c=mq_1+mq_2$. 故有 $a-c=m(q_1+q_2)$，其中 q_1+q_2 是一个整数.

引理 2 如果 a, b, c 是任意三个整数，m 是一个正整数且 $(m, c) = 1$，则当 $ac \equiv bc \pmod{m}$ 时，有

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

证 由于 $c(a - b) = ac - bc = mq$，其中 q 是一个整数，$(m, c) = 1$，我们有 $a - b = mq_1$，其中 q_1 是一个整数.

引理 3 如果 a, b 是任意二个整数，而 m, n 是二个正整数，则当 $a \equiv b \pmod{m}$ 时，有

$$a^n \equiv b^n \pmod{m}.$$

证 由 $a - b = mq$，其中 q 是一个整数，我们有

$$a^n = (b + mq)^n = b^n + \cdots + (mq)^n = b^n + mq_1,$$

其中 q_1 是一个整数. 故有 $a^n - b^n = mq_1$，即

$$a^n \equiv b^n \pmod{m}.$$

我们把 0，1 叫作模 2 的不为负最小完全剩余系. 我们把所有偶整数(即 $2n$ 形状的所有整数，其中 $n = 0, \pm 1, \pm 2, \cdots$)划成一类，把所有奇整数(即 $2n + 1$ 形状的所有整数，其中 $n = 0, \pm 1, \pm 2, \cdots$)划成一类. 这样我们就把全体整数分成为 2 类，即偶整数类和奇整数类. 从偶整数类中任意取出一个整数 a_1，从奇整数类中任意取出一个整数 a_2. 我们把 a_1，a_2 叫作模 2 的一个完全剩余系. 例如 0，3 是模 2 的一个完全剩余系，而 1，6 也是模 2 的一个完全剩余系. 如果 a_3 是一个奇整数而 a_4 是一个偶整数(或 a_3 是一个偶整数而 a_4 是一个奇整数)，则 a_3，a_4 是模 2 的一个完全剩余系. 所以说模 2 的完全剩余系的个数有无限多个.

设 m 是一个大于 2 的整数，我们把 $0, 1, \cdots, m - 1$ 叫作模 m 的不为负最小的完全剩余系. 我们把能被 m 整除的所有整数(即 mn 形状的所有整数，其中 $n = 0, \pm 1, \pm 2, \cdots$)划成一类；把被 m 除后，余数是 1 的所有整数(即 $mn + 1$ 形状的所有整数，其中 $n = 0, \pm 1, \pm 2, \cdots$) 划成一类；…；把被 m

除后，余数是 $m-1$ 的所有整数(即 $mn+m-1$ 形状的所有整数，其中 $n=0, \pm1, \pm2, \cdots$) 划成一类；这样我们就把全体整数分成为 m 类. 如果从每一类当中各取出一个整数，则这 m 个整数就叫作模 m 的一个完全剩余系.

例 3 求证 $-10, -6, -1, 2, 10, 12, 14$ 是模 7 的一个完全剩余系.

证 由于

$$-10 \equiv 4 \pmod 7, \quad -6 \equiv 1 \pmod 7, \quad -1 \equiv 6 \pmod 7,$$
$$2 \equiv 2 \pmod 7, \quad 10 \equiv 3 \pmod 7, \quad 12 \equiv 5 \pmod 7, \quad 14 \equiv 0 \pmod 7,$$

而 $4, 1, 6, 2, 3, 5, 0$ 和 $0, 1, 2, 3, 4, 5, 6$ 只是在次序上有不同，故 $-10, -6, -1, 2, 10, 12, 14$ 是模 7 的一个完全剩余系.

例 4 求证 $6, 9, 12, 15, 18, 21, 24, 27$ 是模 8 的一个完全剩余系.

证 由于

$$6 \equiv 6 \pmod 8, \quad 9 \equiv 1 \pmod 8, \quad 12 \equiv 4 \pmod 8,$$
$$15 \equiv 7 \pmod 8, \quad 18 \equiv 2 \pmod 8, \quad 21 \equiv 5 \pmod 8,$$
$$24 \equiv 0 \pmod 8, \quad 27 \equiv 3 \pmod 8,$$

而 $6, 1, 4, 7, 2, 5, 0, 3$ 和 $0, 1, 2, 3, 4, 5, 6, 7$ 只是在次序上有不同，故 $6, 9, 12, 15, 18, 21, 24, 27$ 是模 8 的一个完全剩余系.

引理 4 设 m 是一个大于 1 的整数，$a_1, a_2, \cdots, a_m$ 是模 m 的一个完全剩余系. 如在 $a_1, a_2, \cdots, a_m$ 中任取出二个整数，则这二个整数对模 m 是不同余的.

证 以 m 为模，则任何一个整数一定和下列 m 个整数

$$0, 1, \cdots, m-1$$

之一同余. 令 r_i (其中 $i=1, 2, \cdots, m$) 是一个整数，满足条

件

$$a_i \equiv r_i (\mathrm{mod}\, m), \quad 0 \leqslant r_i \leqslant m-1, \tag{1}$$

则我们有

$a_1 \equiv r_1 (\mathrm{mod}\, m)$, $a_2 \equiv r_2 (\mathrm{mod}\, m), \cdots, a_m \equiv r_m (\mathrm{mod}\, m)$. (2)

其中 $0 \leqslant r_1 \leqslant m-1, 0 \leqslant r_2 \leqslant m-1, \cdots, 0 \leqslant r_m \leqslant m-1$. 由于 $a_1, a_2, \cdots, a_m$ 是模 m 的一个完全剩余系，所以 $r_1, r_2, \cdots, r_m$ 和 $0, 1 \cdots, m-1$ 只是在次序上可能有不同. 由于在 $0, 1, \cdots, m-1$ 中，任取出二个整数，这二个整数对模 m 是不同余的，所以在 $r_1, r_2, \cdots, r_m$ 中任取出二个整数，这二个整数对模 m 是不同余的. 故由(2)式知道，在 $a_1, a_2, \cdots, a_m$ 中任取出二个整数，则这二个整数对模 m 是不同余的.

引理 5 设 m 是一个大于 1 的整数，而 $a_1, a_2, \cdots, a_m$ 是 m 个整数，又设在 $a_1, a_2, \cdots, a_m$ 中任取出二个整数时，这二个整数对模 m 是不同余的，则 $a_1, a_2, \cdots, a_m$ 是模 m 的一个完全剩余系.

证 以 m 为模，则任何一个整数一定和下列 m 个整数

$$0, 1, \cdots, m-1$$

之一同余. 令 r_i (其中 $i = 1, 2, \cdots, m$) 是一个整数，满足条件

$$a_i \equiv r_i (\mathrm{mod}\, m), \quad 0 \leqslant r_i \leqslant m-1,$$

则我们有

$a_1 \equiv r_1 (\mathrm{mod}\, m)$, $a_2 \equiv r_2 (\mathrm{mod}\, m), \cdots, a_m \equiv r_m (\mathrm{mod}\, m)$. (3)

其中 $0 \leqslant r_1 \leqslant m-1$, $0 \leqslant r_2 \leqslant m-1, \cdots, 0 \leqslant r_m \leqslant m-1$. 由于(3)式和假设在 $a_1, a_2, \cdots, a_m$ 中任取出二个整数时，这二个整数对模 m 不同余，所以当我们在 $r_1, r_2, \cdots, r_m$ 中任取出二个整数时，这二个整数对模 m 不同余. 所以 $r_1, r_2, \cdots, r_m$ 和 $0, 1, \cdots, m-1$ 只是在次序上可能有不同，即 $a_1, a_2, \cdots, a_m$ 是模 m 的一个完全剩余系.

引理 6 设m是一个大于 1 的整数，而$a_1, a_2, \cdots, a_m$是模m的一个完全剩余系，则当b是一个整数时，$a_1+b, a_2+b, \cdots, a_m+b$也是模$m$的一个完全剩余系。

证 设在$a_1+b, a_2+b, \cdots, a_m+b$中存在二个整数$a_k+b, a_\lambda+b$(其中$1 \leqslant k < \lambda \leqslant m$)，使得

$$a_k + b \equiv a_\lambda + b (\mathrm{mod}\, m) \tag{4}$$

成立．我们又有

$$b \equiv b (\mathrm{mod}\, m). \tag{5}$$

由(4)式减去(5)式，得到

$$a_k \equiv a_\lambda (\mathrm{mod}\, m). \tag{6}$$

由引理 4 和$a_1, a_2, \cdots, a_m$是模m的一个完全剩余系，知道(4)式是不可能成立的．所以在$a_1+b, a_2+b, \cdots, a_m+b$中任取出二个整数时，这二个整数对模$m$不同余，而由引理 5 知道$a_1+b, a_2+b, \cdots, a_m+b$是模$m$的一个完全剩余系．

引理 7 设m是一个大于 1 的整数，b是一个整数且满足条件$(b, m)=1$．如果$a_1, a_2, \cdots, a_m$是模m的一个完全剩余系，则$ba_1, ba_2, \cdots, ba_m$也是模m的一个完全剩余系．

证 设在$ba_1, ba_2, \cdots, ba_m$中存在二个整数ba_k, ba_λ(其中$1 \leqslant k < \lambda \leqslant m$)，使得

$$ba_k \equiv ba_\lambda (\mathrm{mod}\, m) \tag{7}$$

成立，则由$(b, m)=1$和引理 2 我们有

$$a_k \equiv a_\lambda (\mathrm{mod}\, m). \tag{8}$$

由引理 4 和$a_1, a_2, \cdots, a_m$是模m的一个完全剩余系，知道(7)式是不可能成立的．所以在$ba_1, ba_2, \cdots, ba_m$中任取出二个整数时，这二个整数对模m不同余，而由引理 5 知道$ba_1, ba_2, \cdots, ba_m$是模m的一个完全剩余系．

引理 8 设m是一个大于 1 的整数，而b, c是二个任意的整数但满足条件$(b, m)=1$．如果$a_1, a_2, \cdots, a_m$是模m

的一个完全剩余系，则 $ba_1+c, ba_2+c, \cdots, ba_m+c$ 也是模 m 的一个完全剩余系.

证 由于 $a_1, a_2, \cdots, a_m$ 是模 m 的一个完全剩余系，从引理 7 和 $(b, m)=1$ 知道 $ba_1, ba_2, \cdots, ba_m$ 也是模 m 的一个完全剩余系. 由于 $ba_1, ba_2, \cdots, ba_m$ 是模 m 的一个完全剩余系，从引理 6 和 c 是一个整数知道 $ba_1+c, ba_2+c, \cdots, ba_m+c$ 也是模 m 的一个完全剩余系.

例 5 使用引理 8 来证明例 4 中的结果.

证 在引理 8 中取 $m=8$, $b=3$, $c=6$, $a_i=i-1$ (其中 $1 \leqslant i \leqslant 8$). 由于 0, 1, 2, 3, 4, 5, 6, 7 是模 8 的一个完全剩余系，并且 $ba_1+c=6$, $ba_2+c=9$, $ba_3+c=12$, $ba_4+c=15$, $ba_5+c=18$, $ba_6+c=21$, $ba_7+c=24$, $ba_8+c=27$, 故由引理 8 知道 6, 9, 12, 15, 18, 21, 24, 27 是模 8 的一个完全剩余系.

引理 9 如果 m 是一个大于 1 的整数而 a, b 是任意的二个整数，使得

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

成立，则有 $(a, m)=(b, m)$.

证 由 $a \equiv b(\mathrm{mod}\ m)$ 得到 $a=b+mt$, 其中 t 是一个整数，故有 $(b, m) \mid a$. 又由 $(b, m) \mid m$ 得到 $(b, m) \mid (a, m)$. 由 $b=a-mt$ 有 $(a, m) \mid b$. 又由 $(a, m) \mid m$ 得到 $(a, m) \mid (b, m)$. 故由 $(b, m) \mid (a, m)$ 和 $(a, m) \mid (b, m)$ 得到 $(a, m)=(b, m)$.

§3. 欧拉函数 $\varphi(m)$

定义 1 我们用 $\varphi(m)$ 来表示不大于 m 而和 m 互素的正整数的个数. 我们把 $\varphi(m)$ 叫做欧拉 (Euler) 函数.

因为无论 n 是什么整数，我们都有 $(n, 1)=1$，所以 1 和任何正整数都是互素的. 我们又有 $\varphi(1)=1$.

引理 10 设 l 是一个正整数，p 是一个素数，则我们有

$$\varphi(p^l) = p^{l-1}(p-1).$$

证 由于 $1, 2, \cdots, p-1$ 中的任何一个整数都是和 p 互素的，故有 $\varphi(p) = p-1$. 当 $l=1$ 时有 $p^{l-1} = p^0 = 1$，因而当 $l=1$ 时本引理成立. 现设 $l>1$，不大于 4 而和 4 互素的正整数是 1，3，共有 2 个，故有 $\varphi(4)=2$. 不大于 8 而和 8 互素的正整数是 1，3，5，7，共有 4 个，故有 $\varphi(8)=4$. 不大于 9 而和 9 互素的正整数是 1，2，4，5，7，8 共有 6 个，故有 $\varphi(9)=6$. 而满足条件 $l>1$ 及 $p^l \leqslant 9$ 的 p^l 只有 4，8，9 这三个数，并且 $\varphi(2^2)=\varphi(4)=2=2^{2-1}(2-1)$，$\varphi(2^3)=\varphi(8)=4=2^{3-1}(2-1)$，$\varphi(3^2)=\varphi(9)=6=3^{2-1}(3-1)$，故当 $l>1$ 而 $p^l \leqslant 9$ 时本引理成立. 现设 $l>1$ 而 $p^l \geqslant 10$. 在不大于 p^l 的正整数中(共有 p^{l-1} 个整数，即)

$$p, 2p, 3p, \cdots, p^{l-1}p$$

是 p 的倍数，而其余的不大于 p^l 的正整数都是和 p 互素的. 又不大于 p^l 的正整数共有 p^l 个，而其中是 p 的倍数的正整数有 p^{l-1} 个，故不大于 p^l 而和 p^l 互素的正整数的个数是 $p^l - p^{l-1}$，即

$$\varphi(p^l) = p^l - p^{l-1} = p^{l-1}(p-1).$$

由引理 10 得到 $\varphi(2)=1$，$\varphi(3)=2$，$\varphi(4)=2$，$\varphi(5)=4$，$\varphi(7)=6$，$\varphi(8)=4$，$\varphi(9)=6$，$\varphi(11)=10$，$\varphi(13)=12$，$\varphi(16)=8$，$\varphi(17)=16$，$\varphi(19)=18$.

§4. 简化剩余系

如果 m 是一个大于 1 的整数，由定义 1 知道不大于 m 而和 m 互素的正整数有 $\varphi(m)$ 个. 现设 $1 < a_2 < \cdots < a_{\varphi(m)}$ 是不大于 m 而和 m 互素的全体正整数. 我们把被 m 除后，余数是 1 的所有整数(即 $mn+1$ 形状的所有整数，其中 $n=0$，

$\pm1, \pm2, \cdots$)划成一类. 把被m除后,余数是a_2的所有整数(即$mn + a_2$形状的所有整数,其中$n = 0, \pm1, \pm2, \cdots$)划成一类,…,把被$m$除后,余数是$a_{\varphi(m)}$的所有整数(即$mn + a_{\varphi(m)}$形状的所有整数,其中$n = 0, \pm1, \pm2, \cdots$)划成一类. 以$m$为模,则任何一个整数一定和下列$m$个整数

$$0, 1, \cdots, m-1$$

之一同余. 由引理9知道,如果a和b对于模m同余,则由$(a, m) = 1$可得到$(b, m) = 1$. 因而以m为模,任何一个和m互素的整数一定和下列$\varphi(m)$个整数

$$1, a_2, \cdots, a_{\varphi(m)}$$

之一同余. 故按照前面分类的方法,我们就把全体和m互素的整数分成为$\varphi(m)$类. 从每一类当中各取出一个整数,则这$\varphi(m)$个整数就叫做以m为模的一个简化剩余系.

例6 求证4, 8, 16, 28, 32, 44, 52, 56是模15的一个简化剩余系.

证 由于小于15而和15互素的正整数共有8个,即

$$1, 2, 4, 7, 8, 11, 13, 14,$$

我们有

$$4 \equiv 4 \pmod{15}, \quad 8 \equiv 8 \pmod{15}, \quad 16 \equiv 1 \pmod{15},$$
$$28 \equiv 13 \pmod{15}, \quad 32 \equiv 2 \pmod{15}, \quad 44 \equiv 14 \pmod{15},$$
$$52 \equiv 7 \pmod{15}, \quad 56 \equiv 11 \pmod{15}.$$

由于4,8,1,13,2,14,7,11和1,2,4,7,8,11,13,14只是在次序上不同,所以4, 8, 16, 28, 32, 44, 52, 56是模15的一个简化剩余系.

引理11 设m是一个大于1的整数$b_1, b_2, \cdots, b_{\varphi(m)}$是模$m$的一个简化剩余系. 如在$b_1, b_2, \cdots, b_{\varphi(m)}$中任取出二个整数,则这二个整数对模$m$是不同余的. 如在$b_1, b_2, \cdots, b_{\varphi(m)}$中任取出一个整数,则这个整数是和$m$互素的.

证 设 $1<a_2<\cdots<a_{\varphi(m)}$ 是不大于 m 而和 m 互素的全体正整数. 令 r_i (其中 $i=1,2,\cdots,m$) 是一个整数,满足条件

$$b_i \equiv r_i \pmod m, \quad 0 \leqslant r_i \leqslant m-1,$$

则我们有

$$b_1 \equiv r_1 \pmod m,\ b_2 \equiv r_2 \pmod m,\ \cdots,\ b_{\varphi(m)} \equiv r_{\varphi(m)} \pmod m. \tag{9}$$

其中 $0 \leqslant r_1 \leqslant m-1$, $0 \leqslant r_2 \leqslant m-1$, $\cdots$, $0 \leqslant r_{\varphi(m)} \leqslant m-1$. 由于 $b_1, b_2, \cdots, b_{\varphi(m)}$ 是模 m 的一个简化剩余系, 所以 $r_1, r_2, \cdots, r_{\varphi(m)}$ 和 $1, a_2, \cdots, a_{\varphi(m)}$ 只是在次序上可能有不同. 由于在 $1, a_2, \cdots, a_{\varphi(m)}$ 中,任取出二个整数时,这二个整数对模 m 是不同余的,所以在 $r_1, r_2, \cdots, r_{\varphi(m)}$ 中任取出二个整数时,这二个整数对模 m 是不同余的. 故由 (9) 式知道, 在 $b_1, b_2, \cdots, b_{\varphi(m)}$ 中任取出二个整数,则这二个整数对模 m 是不同余的. 由于在 $1, a_2, \cdots, a_{\varphi(m)}$ 中,任取出一个整数时,这个整数和 m 是互素的,所以在 $r_1, r_2, \cdots, r_{\varphi(m)}$ 中,任取出一个整数时,这个整数和 m 是互素的. 故由 (9) 式和引理 9 知道,在 $b_1, b_2, \cdots, b_{\varphi(m)}$ 中任取出一个整数时, 则这个整数是和 m 互素的.

引理 12 设 m 是一个大于 1 的整数, $b_1, b_2, \cdots, b_{\varphi(m)}$ 是 $\varphi(m)$ 个和 m 互素的整数. 又设在 $b_1, b_2, \cdots, b_{\varphi(m)}$ 中任取出二个整数时, 这二个整数对模 m 是不同余的, 则 $b_1, b_2, \cdots, b_{\varphi(m)}$ 是模 m 的一个简化剩余系.

证 设 $1<a_2<\cdots<a_{\varphi(m)}$ 是不大于 m 而和 m 互素的全体正整数. 令 r_i (其中 $i=1,2,\cdots,m$) 是一个整数,满足条件

$$b_i \equiv r_i \pmod m, \quad 0 \leqslant r_i \leqslant m-1,$$

则我们有

$$b_1 \equiv r_1 \pmod m,\ b_2 \equiv r_2 \pmod m,\ \cdots,\ b_{\varphi(m)} \equiv r_{\varphi(m)} \pmod m. \tag{10}$$

其中 $0 \leqslant r_1 \leqslant m-1$, $0 \leqslant r_2 \leqslant m-1, \cdots, 0 \leqslant r_{\varphi(m)} \leqslant m-1$. 由于在 $b_1, b_2, \cdots, b_{\varphi(m)}$ 中，任取出一个整数时，这个整数和 m 是互素的，故由 (10) 式和引理 9 知道，在 $r_1, r_2, \cdots, r_{\varphi(m)}$ 中任取出一个整数时，则这个整数是和 m 互素的. 由于在 $b_1, b_2, \cdots, b_{\varphi(m)}$ 中任取出二个整数时，这二个整数对模 m 是不同余的，故由 (10) 式知道，在 $r_1, r_2, \cdots, r_{\varphi(m)}$ 中任取出二个整数时，则这二个整数对模 m 是不同余的. 因而 $r_1, r_2, \cdots, r_{\varphi(m)}$ 和 $1, a_2, \cdots, a_{\varphi(m)}$ 只是在次序上可能有不同，即 $b_1, b_2, \cdots, b_{\varphi(m)}$ 是模 m 的一个简化剩余系.

引理 13 设 m 是一个大于 1 的整数，a 是一个整数且满足条件 $(a, m) = 1$. 如果 $b_1, b_2, \cdots, b_{\varphi(m)}$ 是模 m 的一个简化剩余系，则

$$ab_1, ab_2, \cdots, ab_{\varphi(m)}$$

也是模 m 的一个简化剩余系.

证 由于引理 11 和 $b_1, b_2, \cdots, b_{\varphi(m)}$ 是模 m 的一个简化剩余系，我们知道在 $b_1, b_2, \cdots, b_{\varphi(m)}$ 中任取出一个整数时，则这个整数和 m 是互素的. 由于 $(a, m) = 1$，我们知道在 $ab_1, ab_2, \cdots, ab_{\varphi(m)}$ 中任取出一个整数时，则这个整数和 m 是互素的. 设在 $ab_1, ab_2, \cdots, ab_{\varphi(m)}$ 中存在二个整数 ab_k, ab_λ (其中 $1 \leqslant k < \lambda \leqslant \varphi(m)$)，使得

$$ab_k \equiv ab_\lambda \pmod{m} \tag{11}$$

成立. 由 $(a, m) = 1$，(11) 式和引理 2，我们有

$$b_k \equiv b_\lambda \pmod{m}. \tag{12}$$

由于引理 11 和 $b_1, b_2, \cdots, b_{\varphi(m)}$ 是模 m 的一个简化剩余系，故在 $b_1, b_2, \cdots, b_{\varphi(m)}$ 中任取出二个整数时，这二个整数对模 m 是不同余的，故 (12) 式不成立，从而 (11) 式不成立. 因而在 $ab_1, ab_2, \cdots, ab_{\varphi(m)}$ 中任取出二个整数时，则这二个整数对模 m 是不同余的. 由引理 12 及在 $ab_1, ab_2, \cdots, ab_{\varphi(m)}$ 中任取