近世代数

Modern Algebra

裴定一 郭华光 徐祥
王学理 唐西林 胡磊 编

广东科技出版社

近世代数

裴定一　郭华光　徐祥
王学理　唐西林　胡磊　编

广东科技出版社
·广　州·

图书在版编目（CIP）数据

近世代数/裴定一等编. —广州：广东科技出版社，2002

ISBN 7-5359-1984-7

Ⅰ. 近… Ⅱ. 裴… Ⅲ. 抽象代数 Ⅳ. 0153

中国版本图书馆 CIP 数据核字（2002）第 082484 号

Jinshi Daishu

出版发行：广东科技出版社
（广州市环市东路水荫路 11 号 邮码：510075）
E-mail：gdkjzbb@21cn.com
http://www.gdstp.com.cn
出 版 人：黄达全
经 销：广东新华发行集团
排 版：广东科电有限公司
印 刷：广东省肇庆新华印刷有限公司
（广东省肇庆市星湖大道 邮码：526060）
规 格：850mm×1 168mm 1/32 5 印张 字数 150 千
版 次：2003 年 1 月第 1 版
2003 年 1 月第 1 次印刷
印 数：1～2000 册
定 价：10.00 元

前　言

本书是我校教研室多年来进行“近世代数”教学的一个成果。自原广州师范学院1978年复办以来，“近世代数”一直是数学系开设的一门专业必修课，先后采用过多种教材，但结合系里教学的具体情况，都觉得有不尽人意的地方，从而萌发自编一本教材的想法。在我校理学院院长、原广州师范学院教学系主任裴定一教授的直接组织、指导和参与下，教研室的几位老师于1996年开始写作，1998年完成初稿并投入使用。到目前为止，本书已经在原广州师范学院数学系四届毕业生、合并后的广州大学教学系第一届毕业生中使用过，且其间进行了数次修订。可以说，这本书是集体劳动的结晶。

本书包含了“近世代数”这门课程的常规内容：群、环、域，整环上的因子分解等。第一章以讲述整数论的基本知识为主，这主要是考虑到整数是多种代数系统的一个直观模型，而包括我校在内的不少院校的数学系并不把数论作为必修课，因而部分学生可能不熟悉这方面的知识。为了理论联系实际，提高学生的学习兴趣，使学生更好地理解本课程的内容和方法，本书列举了一些应用的例子。其中值得一提的是本书对“近世代数”在编码和信息安全方面的应用有较详细的介绍，这是因为编码和信息安全的理论和实践的发展是最近这二三十年来纯粹数学应用的一个成功而光辉的典范，且作者中不少同志正在从事这方面的研究工作，这也是一次科研与教学相结合的尝试。

我们感谢这几年来在使用本教材的过程中老师和学生所提出的宝贵意见，感谢原广州师范学院教务处和合并重新组建后的广州大学教务处对本教材出版的支持，感谢广东科技出版社在出版过程中所提供的高效和愉快的合作。

目　录

第一章　整数与集合的一些性质

整数及其之间的运算是本课程里要学到的许多代数对象（如群、环等）的典型代表. 因此它为本课程的抽象内容提供了具体的例子，而且有关的一些重要性质、定理都可以从整数中找到启发. 为了便于更好地掌握本课程的知识，首先安排了这一章的内容.

本章从整除这个概念出发，介绍欧氏除法，最大公因数与最小公倍数，算术基本定理，然后引进同余这个重要概念及欧拉定理. 读者将会发现，所有这些内容在以后的章节里都可以找到其影子. 最后介绍集合中的等价关系，它在后面的章节中有重要的作用.

第一节　整除、欧氏除法

我们知道任意两个整数的和、差、积仍为整数，但是两个整数的商（分母不为零）却不一定是整数. 因此我们引入整除这个概念.

定义 1　设 a，$b\in Z$，若存在一整数 q，使得等式

$$a=bq \tag{1}$$

成立，则我们称 b 整除 a 或 a 可以被 b 整除，记成 $b\mid a$. 此时我们也称 b 是 a 的因数，a 是 b 的倍数；若这样的整数 q 不存在，则称 b 不能整除 a 或 a 不能被 b 整除，并记成 $b\nmid a$.

定理 1　(1) $b\mid a$，$c\mid b$，则 $c\mid a$；

(2) $m\mid a$，$m\mid b$，则 $m\mid(a\pm b)$；

(3) $m\mid a_1$，$m\mid a_2$，$\cdots$，$m\mid a_n$，则

$m\mid(q_1a_1+\cdots+q_na_n)$，这里 q_1，$\cdots$，q_n 为任意整数.

证明　只证明 (3)，(1) 和 (2) 可类似地证明

因为 $m \mid a_i$，所以 $\exists r_i \in Z$，使得 $a_i = r_i m$，$i = 1, 2, \cdots, n$，故

$$q_1 a_1 + q_2 a_2 + \cdots + q_n a_n = (q_1 r_1 + q_2 r_2 + \cdots + q_n r_n)\, m，\text{而}$$

$$q_1 r_1 + q_2 r_2 + \cdots + q_n r_n \in Z，\text{故}$$

$$m \mid (q_1 a_1 + q_2 a_2 + \cdots + q_n a_n)$$

证毕.

定理 2（带余除法） 若 a，$b \in Z$，$b > 0$，则存在唯一的整数 q 与 r，使得

$$a = bq + r，\quad 0 \leqslant r < b \tag{2}$$

成立.

证明 我们看下面的一个整数序列：

$$\cdots，-3b，-2b，-b，0，b，2b，3b，\cdots.$$

则 a 必在上述序列的某二项之间，即存在一个整数 q，使得

$$qb \leqslant a < (q+1)\, b$$

令 $a - qb = r$，则 $a = bq + r$，而 $0 \leqslant r < b$，且 r 为整数.

设 q_1，$r_1 \in Z$ 也满足 (2)，则

$$bq_1 + r_1 = a = bq + r$$

故 $b(q - q_1) = r_1 - r$，从而 $b \mid q - q_1 \mid = \mid r_1 - r \mid < b$

（因为 $0 \leqslant r < b$，$0 \leqslant r_1 < b$）.

因此，$q = q_1$，从而 $r_1 = r_2$.

证毕.

以后，我们称 (2) 中的 q 为 b 除 a 所得的不完全商，r 称为 b 除 a 所得的余数.

利用带余除法，就可以研究整数的最大公因数的存在性和具体的求法.

定义 2 设 a，$b \in Z$，若 $d \mid a$ 且 $d \mid b$，则 d 称为 a 与 b 的一个公因数；a 与 b 的公因数中最大者称为 a 与 b 的最大公因数，并记成 (a, b)；若 $(a, b) = 1$，则称 a 与 b 互素.

定理 3 设 a，b，$c \in Z$，且不全为零，若

$$a = bq + c$$

其中 $q \in Z$，则 $(a, b) = (b, c)$.

证明 设 d 是 a 与 b 的任一公因数，则 $d \mid a$，$d \mid b$，因此 $d \mid (a - bq)$，即 $d \mid c$，从而 d 也是 b 与 c 的公因数. 同理可知 b 与 c 的任一公因数也是 a 与 b 的公因数，这说明 a，b 与 b，c 有完全相同的公因数，特别地有 $(a, b) = (b, c)$.

证毕.

下面我们介绍求任意两个整数 a 与 b 的最大公因数的欧氏除法（通常又称为辗转相除法）.

设 a，$b \in N$，由带余除法，有

$$\begin{aligned}
&a = bq_1 + r_1, && 0 < r_1 < b\\
&b = r_1 q_2 + r_2, && 0 < r_2 < r_1\\
&r_1 = r_1 q_3 + r_3, && 0 < r_3 < r_2\\
&\qquad\cdots\cdots\\
&r_{n-2} = r_{n-1} q_n + r_n, && 0 < r_n < r_{n-1}\\
&r_{n-1} = r_n q_{n+1} + r_{n+1}, && r_{n+1} = 0
\end{aligned} \tag{3}$$

因为 $b > r_1 > r_2 > \cdots > r_n > r_{n+1} > \cdots$，所以一定有某个 n 使得

$$r_{n+1} = 0.$$

于是由定理 3 知

$$\begin{aligned}
r_n &= (0, r_n) = (r_{n+1}, r_n) = (r_n, r_{n-1})\\
&= \cdots = (r_1, b) = (a, b).
\end{aligned}$$

【例 1】 设 $a = 205$，$b = 35$，则

$$\begin{aligned}
&205 = 35 \times 5 + 30, && q_1 = 5, \quad r_1 = 30\\
&35 = 30 \times 1 + 5, && q_2 = 5, \quad r_2 = 30\\
&30 = 5 \times 6 + 0, && q_3 = 5, \quad r_3 = 30
\end{aligned}$$

故 $(205, 35) = 5$.

对于多于二个的整数，我们可以类似地定义它们的最大公因数，并且有

定理 4 设 $a_1, a_2, \cdots, a_n \in Z$, d_n 为 $a_1, a_2, \cdots, a_n$ 的最大公因数，那么 d_n 可如下递推求得：

$$d_2=(a_1, a_2), d_3=(d_2, a_3), d_4=(d_3, a_4), \cdots,$$
$$d_n=(d_{n-1}, a_n).$$

证明 习题.

定理 5 设 $a, b \in Z$，则存在 $s, t \in Z$，使得

$$as+bt=(a, b)$$

证明 习题.

习　题

1. 证明定理 4.

2. 证明定理 5.

3. 试证明本节 (3) 式中的 $n \leqslant \dfrac{2\log b}{\log 2}$.

4. 设 ax_0+by_0 是形如 $ax+by(a, b \in Z$ 且不全为 $0, x, y$ 是任意整数) 的数中的最小正数，则有

(1) $(ax_0+by_0) \mid (ax+by), \quad \forall x, y \in Z.$

(2) $ax_0+by_0=(a, b).$

5. 设 $a, b \in Z$，则

$$(a, b)=1 \Longleftrightarrow \exists s, t \in Z \text{ 使得 } as+bt=1.$$

6. 设 $a, b, c \in Z$，若 $a \mid c, b \mid c$，则称 c 是 a 与 b 的一个公倍数. a 与 b 的所有公倍数中最小的正数称为 a 与 b 的最小公倍数，并记作 $[a, b]$.

证明：若 $a, b \in N$，则 $[a, b]=\dfrac{ab}{(a, b)}$.

第二节　素数、算术基本定理

定义3　一个大于1的整数，若它的正因数只有1与它本身，就称为素数，否则就称为合数.

关于素数我们有下述一些结论.

定理6　设 p 是一素数，$q \in Z$，则 $p \mid q$ 或者 $(p, q) = 1$.

证明　因为 $(p, q) > 0$ 且 $(p, q) \mid p$，而 p 为素数，故 $(p, q) = 1$ 或 $(p, q) = p$，后者即 $p \mid q$.

证毕.

推论　设 $a_1, a_2, \cdots, a_n \in Z$，$p$ 是素数，且 $p \mid a_1 a_2 \cdots a_n$，则 p 一定整除某一个 a_i.

证明　对 n 用数学归纳法. $n = 1$，结论显然成立.

假设 $n = k - 1$ 时，结论成立.

设 $n = k$，如果 $p \mid a_1 a_2 \cdots a_{k-1}$，则由归纳法假设 $p \mid a_i$，对某个 i，$1 \leqslant i \leqslant k - 1$；否则 $(p, a_1 a_2 \cdots a_{k-1}) = 1$，由定理5，知存在 $u, v \in Z$，使得

$$up + va_1 a_2 \cdots a_{k-1} = 1$$

在上式两边乘上 a_k 得

$$upa_k + va_1 a_2 \cdots a_{k-1} a_k = a_k$$

现在 p 整除上式左边的每一项，从而 $p \mid a_k$.

证毕.

定理7（算术基本定理）　任一大于1的整数一定能表示成素数的乘积，并且这种表示法除了次序外是唯一的. 即若整数 $a > 1$，则有

$$a = p_1 p_2 \cdots p_n \tag{4}$$

其中 p_i 是素数，并且若又有

$$a = q_1 q_2 \cdots q_m \tag{5}$$

其中 q_i 为素数，则 $m = n$，且适当调整次序后有

$$p_i = q_i (i = 1, 2, \cdots, n).$$

证明 对 a 用数学归纳法.

若 $a = 2$，结论显然成立. 设定理对所有小于 a 的正整数均有 (4) 式的分解，且分解式唯一. 证定理对 a 也成立.

若 a 本身是素数，则结论显然.

若 a 是合数则 $a = bc$，其中 $1 < b, c < a$，于是由归纳假设，有 $b = p_1 p_2 \cdots p_k$，$c = p_{k+1} p_{k+2} \cdots p_n$，故对一切正整数 ($\geqslant 2$) 均可分解成 (4).

若又有 $a = q_1 q_2 \cdots q_m$，则 $p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_m$. 故

$$p_1 \mid q_1 q_2 \cdots q_m.$$

由定理 6 的推论，p_1 整除某个 q_j，从而 $p_1 = q_j$. 通过调整次序，不妨设 $q_1 = p_1$，因此有 $p_2 p_3 \cdots p_n = q_2 q_3 \cdots q_m$，由归纳假设有

$$n - 1 = m - 1 \text{ 且 } p_i = q_i (2 \leqslant i \leqslant n).$$

于是 $m = n$，且 $p_i = q_i (1 \leqslant i \leqslant n)$.

证毕.

推论

(1) 每一个大于 1 的正整数 a 均能唯一写成

$$a = p_1^{k_1} p_2^{k_2} \cdots p_t^{k_t}, \quad k_i > 0, \quad i = 1, 2, \cdots, t \tag{6}$$

其中 $p_1 < p_2 < \cdots < p_t$ 为素数.

(2) 设 a，b 是任意二个正整数，且

$$a = p_1^{l_1} p_2^{l_2} \cdots p_t^{l_t}, \qquad k_i \geqslant 0, \ \forall i$$

$$b = p_1^{j_1} p_2^{j_2} \cdots p_t^{j_t}, \qquad j_i \geqslant 0, \ \forall i$$

则

$$(a, b) = p_1^{l_1} p_2^{l_2} \cdots p_t^{l_t}$$

$$[a, b] = p_1^{m_1} p_2^{m_2} \cdots p_t^{m_t}$$

其中 $l_i = \min \{k_i, j_i\}$，$m_i = \max \{k_i, j_i\}$

式 (6) 称为 a 的标准分解. 算术基本定理告诉我们任一正整数都能分解成素数的乘积，但并没有给出具体的分解方法. 事实上，将一个正整数分解成素因数的乘积是一个很困难的问题，特别是当整数相当大的时候.

定义 4 设 $a \in N$，记集合 $\{1, 2, 3, \cdots, a\}$ 中与 a 互素的整数的个数为 $\varphi(a)$. φ 是一个定义在全体正整数集合上的一个函数. 我们称之为欧拉函数.

【例 2】 设 p 为素数，则 $\{1, 2, \cdots, p\}$ 中将有 $(p-1)$ 个元素 $1, 2, \cdots, p-1$ 与 p 互素，故 $\varphi(p) = p - 1$. 一般地我们有

$$\varphi(p^k) = p^k - p^{k-1}, \quad k \geqslant 1$$

事实上，集合 $\{1, 2, \cdots, p^k\}$ 共有 p^k 个元素，该集合中的任意元素 a，当且仅当 $a = pt(1 \leqslant t \leqslant p^{k-1})$ 时，$(p^k, a) > 1$，故与 p^k 不互素的数目恰有 p^{k-1} 个，从而与 p^k 互素的数目为 $p^k - p^{k-1}$.

第三节　同余、费尔马小定理、欧拉定理

在这一节，我们引进初等数论中十分重要的概念——同余，剩余类，并证明两个重要的定理——费尔马定理和欧拉定理.

设 m 是一个正整数，由带余除法定理知，任一整数 a 用 m 所除得的余数只能是 $0, 1, 2, \cdots, m-1$ 中的一个. 我们把除得的余数为 i 的所有整数放在一起组成的集合记成 K_i，则显然有

$$Z = \bigcup_{i=0}^{m-1} K_i, \text{ 且 } K_i \cap K_j = \varnothing \quad (i \neq j)$$

我们称 $K_i (0 \leqslant i \leqslant m-1)$ 为模 m 的剩余类. 由此我们有下面的定义 5.

定义 5 在同一个模 m 的剩余类中的任意两个数称为是模 m 同余的. 换言之，两个整数 a 与 b 是模 m 同余的，当且仅当 $m \mid (a-b)$. a 与 b 模 m 同余，记成 $a \equiv b (\mathrm{mod}\ m)$，否则称为模 m 不同

余的，记成 $a \not\equiv b(\mathrm{mod}\ m)$.

定理 8 设 m 为任一正整数，a，b，c，d，a_1，a_2，b_1，b_2 为整数.

(1) 对于所有的 a，$a \equiv a(\mathrm{mod}\ m)$；

(2) 若 $a \equiv b(\mathrm{mod}\ m)$，则 $b \equiv a(\mathrm{mod}\ m)$；

(3) 若 $a \equiv b$，$b \equiv c(\mathrm{mod}\ m)$，则 $a \equiv c(\mathrm{mod}\ m)$；

(4) 若 $a_1 \equiv b_1$，$a_2 \equiv b_2(\mathrm{mod}\ m)$，则

$$a_1 + a_2 \equiv b_1 + b_2(\mathrm{mod}\ m);$$

(5) 若 $a + b \equiv c(\mathrm{mod}\ m)$，则 $a \equiv c - b(\mathrm{mod}\ m)$；

(6) 若 $a_1 \equiv b_1$，$a_2 \equiv b_2(\mathrm{mod}\ m)$，则

$$a_1 a_2 \equiv b_1 b_2(\mathrm{mod}\ m);$$

(7) 若 $a_1 d \equiv b_1 d(\mathrm{mod}\ m)$ 且 $(d, m) = 1$，则

$$a_1 \equiv b_1(\mathrm{mod}\ m);$$

(8) 若 $a \equiv b(\mathrm{mod}\ m)$，$d$ 是 a，b，m 的任一公因数，则

$$\frac{a}{d} \equiv \frac{b}{d}\left(\mathrm{mod}\ \frac{m}{d}\right);$$

(9) 若 $a \equiv b(\mathrm{mod}\ m_i)$ $i = 1, 2, \cdots, t$，则

$$a \equiv b(\mathrm{mod}\ [m_1, m_2, \cdots, m_t]);$$

(10) 若 $a \equiv b(\mathrm{mod}\ m)$，$d \mid m$，$d > 0$，则

$$a \equiv b(\mathrm{mod}\ d);$$

(11) 若 $a \equiv b(\mathrm{mod}\ m)$，则

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

证明 习题.

定义 6 设 a_0，a_1，$\cdots$，$a_{m-1} \in Z$，若其中任意两个数均不在同一剩余类中，则称 $\{a_0, a_1, \cdots, a_{m-1}\}$ 为模 m 的一个完全剩余类代表系.

定理 9 若 m，$n \in N$，且 $(m, n) = 1$，则当 x 与 y 分别跑遍模 m、n 的一个完全剩余类代表系时，$nx + my$ 恰好跑遍模 mn 的

一个完全剩余类代表系.

证明 显然 $nx + my$ 这样的数恰好有 mn 个，我们只要证明它们是模 mn 两两不同余的. 设有

$$nx_1 + my_1 \equiv nx_2 + my_2 \pmod{mn}.$$

由定理 8(10)有

$$nx_1 \equiv nx_2 \pmod{m};$$

$$my_1 \equiv my_2 \pmod{n}.$$

又因为 $(m, n) = 1$，由定理 8(7)，$x_1 \equiv x_2 \pmod{m}$，$y_1 \equiv y_2 \pmod{n}$. 因为 x_1 与 x_2 为完全剩余类代表系中元素，故 $x_1 = x_2$；同理 $y_1 = y_2$.

证毕.

现在我们利用同余概念来描述上节中引进的欧拉函数. 由定理 8(11) 知 K_i 中任意两个数与 m 有相同的最大公因数. 特别地，如果 K_i 中有某个数与 m 互素，则 K_i 中所有的数与 m 均互素. 此时我们称 K_i 是与模 m 互素的一个剩余类. 因此 $\varphi(m)$ 等于与模 m 互素的剩余类的个数. 在与模 m 互素的剩余类中任意取定一个数，可得 $\varphi(m)$ 个数，这 $\varphi(m)$ 个数模 m 是两两不同余的. 这 $\varphi(m)$ 个数组成的集合称为模 m 的一个简化剩余类代表系. 于是有：

定理 10 若 $a_1, a_2, \cdots, a_{\varphi(m)} \in Z$，则 $\{a_1, a_2, \cdots, a_{\varphi(m)}\}$ 是模 m 的一个简化剩余类代表系的充分必要条件是

$$(a_i, m) = 1, \text{且 } a_i \not\equiv a_j \pmod{m} \quad \forall i, j = 1, 2, \cdots, \varphi(m).$$

定理 11 若 $m, n \in N$ 且 $(m, n) = 1$，则当 x, y 分别跑遍模 m, n 的一个简化剩余类代表系时，$nx + my$ 恰好跑遍模 mn 的一个简化剩余类代表系. 特别地有 $\varphi(mn) = \varphi(m)\varphi(n)$.

证明 由定理 9 知，当 x, y 分别跑遍模 mn 的完全剩余类代表系时，$nx + my$ 跑遍模 mn 的完全剩余系.

若 $(x, m) = (y, n) = 1$，

由 $(m, n) = 1$ 知 $(nx, m) = (my, n) = 1$，故

$(nx + my, m) = (nx + my, n) = 1$，从而

$(nx + my, mn) = 1$；反之，若

$(nx + my, mn) = 1$. 则显然

$(nx + my, m) = (nx + my, n) = 1$，即

$(nx, m) = (my, n) = 1$，故

$(x, m) = (y, n) = 1$.

这说明当 x，y 分别跑遍模 m，n 的简化剩余类代表系时，$nx + my$ 恰好跑遍模 mn 简化剩余类代表系.

证毕.

推论 设 $a = p_1^{k_1} p_2^{k_2} \cdots p_t^{k_t}$，则

$$\varphi(m) = a(1 - \frac{1}{p_1})(1 - \frac{1}{p_2})\cdots(1 - \frac{1}{p_t}).$$

定理 12(欧拉定理) 设 m 是大于 1 的整数，$(a, m) = 1$，则

$$a^{\varphi(m)} = 1(\mathrm{mod}\ m)$$

证明 设 $a_1, a_2, \cdots, a_{\varphi(m)}$ 是模 m 的一个简化剩余类代表系，则易证明 $aa_1, aa_2, \cdots, aa_{\varphi(m)}$ 也是个简化剩余类代表系. 注意到两个简化剩余类代表系可以是不同的，但它们取模 m 后的余数却是对应相等的，由定理 8(6)，有

$$(aa_1)(aa_2)\cdots(aa_{\varphi(m)}) \equiv a_1 a_2 \cdots a_{\varphi(m)}(\mathrm{mod}\ m) \quad \text{即}$$

$$a^{\varphi(m)}(a_1 a_2 \cdots a_{\varphi(m)}) \equiv a_1 a_2 \cdots a_{\varphi(m)}(\mathrm{mod}\ m)$$

又 $(a_i, m) = 1$，故 $(a_1 a_2 \cdots a_{\varphi(m)}, m) = 1$，由定理 8(7)知

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

证毕.

推论(费尔马小定理) 若 p 为素数，则

$$a^p = a(\mathrm{mod}\ p)$$

习　题

1. 证明定理 11 的推论.

2. 设 $(a, m) = 1$，则当 x 跑遍模 m 的一个简化剩余类代表系时，ax 也跑遍模 m 的一个简化剩余类代表系.

3. (1) 证明 $\varphi(1) + \varphi(p) + \cdots + \varphi(p^t) = p^t$，其中 p 为素数.

(2) 证明 $\sum\limits_{d \mid a} \varphi(d) = a$.

4. 求 $(12371^{56} + 34)^{28}$ 被 111 除的余数.

5. 如果今天是星期一，问再过 $10^{11^{12}}$ 天是星期几.

6. (1) 不用费尔马小定理，直接证明

$(h_1 + h_2 + \cdots + h_t)^p \equiv h_1^p + p_2^p + \cdots + h_t^p, (\mathrm{mod}\ p)$，

p 为素数.

(2) 应用(1) 证明费尔马小定理；

(3) 应用费尔马小定理证明欧拉定理.

7. 设 p 为素数，证明威尔逊(Wilson) 定理：

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

第四节 同余式、中国剩余定理

定义 7 设 $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$ 是一个整系数多项式，则

$$f(x) \equiv 0 (\mathrm{mod}\ m)$$

称为模 m 的同余式.

若 $a_n \not\equiv 0 (\mathrm{mod}\ m)$，则称它是 n 次同余式.

若 $a \in Z$，使得 $f(a) \equiv 0 (\mathrm{mod}\ m)$ 成立，

则称 $x \equiv a (\mathrm{mod}\ m)$ 为该同余式的一个解.

定理 13 一次同余式 $ax \equiv b (\mathrm{mod}\ m)$，$a \not\equiv 0 (\mathrm{mod}\ m)$ 有解的充分必要条件是 $(a, m) \mid b$. 此时它恰有 (a, m) 个解(对模 m 而言).