Lai集与素数

Lai JI YU SU SHU

赖以明 赖君利 赖君良 赖君昉 著

湖南科学技术出版社

Lai集与素数

Lai JI YU SU SHU

赖以明 赖君利 赖君良 赖君昉 著

湖南科学技术出版社

Lai 集与素数

著　　者：赖以明　赖君利　赖君良　赖君昉
责任编辑：沙一飞
出版发行：湖南科学技术出版社
社　　址：长沙市湘雅路 280 号
　　http://www.hnstp.com
印　　刷：湘潭地调彩印厂
　　（印装质量问题请直接与本厂联系）
厂　　址：湘潭市韶山西路何家湾巷七号
邮　　编：411100
出版日期：2004 年 7 月第 1 版第 1 次
开　　本：787mm × 1092mm　1/16
印　　张：21.5
字　　数：556000
书　　号：ISBN 7-5357-4022-7/0.229
定　　价：58.00 元

序　言

刘金旺[①]

数论是研究数的性质的一门学科，是一门有着悠久历史的数学学科，也是我国人民所擅长的学科之一.几千年来，人们运用多种方法，研究数论的相关课题，取得了极其辉煌的成就.但人们在进一步研究探索的道路上，以初等的方法研究数论问题，却遇到了极大的困难.能否以一种新的初等方法，对于数的性质的研究，特别是对于素数的研究乃至其他相关课题的研究，取得新的突破，则备受数学界关注.

赖以明老先生是原湘潭师范学院数学系德高望重的老教师.他肄业于国立师范大学(湖南蓝田)理化系，1958年经湖南省教育厅保送到北京师范大学数学系教师进修班进修，1960年6月毕业后，先任原湘潭师范专科学校物理科主任，后任数学科主任，长期从事高等数学教学工作.1979年退休后，他克服重重困难，坚持不懈，对数论进行研究.他结合初等数论和集合理论，运用他深厚的数学功底，以及几十年从事数学教学的经验，探索出一条新途径，这就是以同余为主要工具，结合数的集合特征，研究得到一种全新的数集：$L(n,i)$.数集 $L(n,i)$ 存在着许多独具的性质和特点.运用这些独具的性质，结合同余理论，展示出整数和素数许多新的探索空间.

全书全面而细致地表述了作者的研究思路及其成果.其重要的研究点在于：

(1) 新的数集的定义.对于任意取定的一个大于1的整数 n，都可以得到从小到大 n 个连续素数，任取其中一个素数，而对于其余 $(n-1)$ 个素数的正整数次幂的积，构成集合 L_i 的元素 l_i.这定义，为我们对于与素数紧密相联的整个数集 $L(n,i)$ 性质的研究，提出了一种全新的研究思路和研究空间.

(2) 同余在数集 $L(n,i)$ 中的巧妙应用，揭示出集合元素 l_i 与素数 a_i 互素这一重要的基本特征.同时对于一个不大于素数 a_n 且又与素数 a_i 互素的正整数 a 又能构成同一集合中这样的新元素：al_i，它表述着数集 $L(n,i)$ 的一个重要特点.

(3) 在数的表述中，作为对整数的表述，作者以一种全新的思路加以展开.基于集合 $L(n,i)$ 和同余的性质，研究得出整数 g 存在且惟一存在 l_i 表示式：

$$g = kc - (l_b + l_d + l_f + \cdots + l_{h1} + l_{h2}).$$

---

① 刘金旺：湖南科技大学数学与计算机科学学院院长、教授.

这是作者的一个新的成果.

(4) 对整数的 l_i 表示式深入研究,相继得到确定一个整数是否为素数的充要条件,这是作者对素数研究理论上的一个重大突破.它将对广泛地研究素数的性质及其特点,产生极其重要的影响.

(5) 具体求解整数的 l_i 表示式和具体判别素数.本书以较大的篇幅,详细介绍了与其密切相关的特定不定方程及其解法:l_i 系数不定方程及其解法.

l_i 系数不定方程的特殊性在于:无论从理论上还是在实际的解题过程中都显示出:它既有整数解,又有正整数解,其中每个 x_i 的最小正整数的解值存在且惟一存在;而且随着不定方程个数的增多,不定方程组的组解中 x_i 的解值呈现出有规律地重复循环出现($i = 1,2,3,\cdots,n$).

(6) 运用 l_i 系数不定方程解的特性,进一步得到素数的存在定理,得出求解素数及其个数的方法,这就便于研究和解答有关素数的问题.

通观全书,可以说:全书理论充分,方向明确,方法新颖,注重理论与实践的有机结合,开拓出一条全新的研究整数和素数的具体途径,具有很高的理论研究价值.

我们期待着本书早日问世,以激励广大数学爱好者更好地与时俱进,开拓创新,发展科技,为科教兴国,共创辉煌.是为序.

前　言

数论中存在一些问题，迄今还没解决，或者还没有彻底解决. 我从事数学教学几十年，感受颇多，写了些心得笔记. 1979 年秋，我退休后，将其整理，写出几个数学命题. 最初，自己感到很不满意，继而深入细加思考，逐步开拓引申，于是结合集合理论，创建“Lai 集”. 联系素数与合数，写出了“整数的 l_i 表示式”，得出了“素数的充要条件”以及“Y. M. 定理”、“新素数的求法”，等等.

最先的思路是从下列问题开始，逐渐开拓引申的.

《孙子算经》中有这样的问题：

“今有物不知其数，三三数之剩二，五五数之剩三，七七数之剩二，问物几何?”

思考这问题时，首先设有物 x 个. 依照题意有：

用 3 去除 x，得的余数是 2；用 5 去除 x，得的余数是 3；用 7 去除 x，得的余数是 2.

用同余式表示，得

$$x \equiv 2(\mathrm{mod}3), x \equiv 3(\mathrm{mod}5), x \equiv 2(\mathrm{mod}7).$$

因

$$1 \equiv 2 \times 5 \times 7(\mathrm{mod}3),$$

$$1 \equiv 6 \equiv 3 \times 7 \equiv 6 \times 3 \times 7 \equiv 2 \times 3^2 \times 7(\mathrm{mod}5),$$

$$1 \equiv 3 \times 5(\mathrm{mod}7).$$

于是由 $x \equiv 2(\mathrm{mod}3)$ 和 $1 \equiv 2 \times 5 \times 7(\mathrm{mod}3)$，得

$$x \equiv 2^2 \times 5 \times 7(\mathrm{mod}3); \tag{1}$$

由 $x \equiv 3(\mathrm{mod}5)$ 和 $1 \equiv 2 \times 3^2 \times 7(\mathrm{mod}5)$，得

$$x \equiv 2 \times 3^3 \times 7(\mathrm{mod}5); \tag{2}$$

由 $x \equiv 2(\mathrm{mod}7)$ 和 $1 \equiv 3 \times 5(\mathrm{mod}7)$，得

$$x \equiv 2 \times 3 \times 5(\mathrm{mod}7). \tag{3}$$

既然 (1) $x \equiv 2^2 \times 5 \times 7(\mathrm{mod}3)$，而 $2 \times 3^3 \times 7 \equiv 0 \equiv 2 \times 3 \times 5(\mathrm{mod}3)$，故

$$x \equiv 2^2 \times 5 \times 7 + 2 \times 3^3 \times 7 + 2 \times 3 \times 5(\mathrm{mod}3). \tag{4}$$

又 (2) $x \equiv 2 \times 3^3 \times 7(\mathrm{mod}5)$，而 $2^2 \times 5 \times 7 \equiv 0 \equiv 2 \times 3 \times 5(\mathrm{mod}5)$，故

$$x \equiv 2^2 \times 5 \times 7 + 2 \times 3^3 \times 7 + 2 \times 3 \times 5(\mathrm{mod}5). \tag{5}$$

再 (3) $x \equiv 2 \times 5 \times 7(\mathrm{mod}7)$，而 $2^2 \times 5 \times 7 \equiv 0 \equiv 2 \times 3^3 \times 7(\mathrm{mod}7)$，故

$$x \equiv 2^2 \times 5 \times 7 + 2 \times 3^3 \times 7 + 2 \times 3 \times 5(\mathrm{mod}7). \tag{6}$$

于是，依(4)，(5)，(6)，

得 $x \equiv 2^2 \times 5 \times 7 + 2 \times 3^3 \times 7 + 2 \times 3 \times 5(\mathrm{mod}\overline{3 \times 5 \times 7})$.

从而得 $x = 2^2 \times 5 \times 7 + 2 \times 3^3 \times 7 + 2 \times 3 \times 5 - 3 \times 5 \times 7k$，

即 $x = 2^2 \times 5 \times 7 + 2 \times 3^3 \times 7 + 2 \times 3 \times 5 - 105k$，其中 $k = 0, \pm 1, \pm 2, \cdots$.

上面最后一式,不仅可以得出前述问题的答案(即当 $k=5$ 时,得 x 的最小正整数值 23),而且引人入胜,想法万千.

首先,依 $x=2^2\times5\times7+2\times3^3\times7+2\times3\times5-105k$;

若 x 为偶数,则显然 k 也应为偶数;设 k 为 $2k'$,则

$$x=2^2\times5\times7+2\times3^3\times7+2\times3\times5-105\times2k'=$$
$$(2\times5\times7+3^3\times7+3\times5-105k')\times2,\text{ 其中 }k'=0,\pm1,\pm2,\cdots.$$

若 x 应为奇数,则因

$$x\equiv1\equiv105\equiv3\times5\times7\equiv3\times5\times7+2^2\times5\times7+2\times3^3\times7+2\times3\times5\pmod2,$$

显然 $3\times5\times7+2^2\times5\times7+2\times3^3\times7+2\times3\times5\equiv x\pmod{105}\equiv x\pmod{\overline{3\times5\times7}}$.

故 $3\times5\times7+2^2\times5\times7+2\times3^3\times7+2\times3\times5\equiv x\pmod{\overline{2\times3\times5\times7}}$.

从而 $x=3\times5\times7+2^2\times5\times7+2\times3^3\times7+2\times3\times5-2\times3\times5\times7k$,

其中 $k=0,\pm1,\pm2,\cdots$.

这时,x 等于几个特殊积 $3\times5\times7$,$2^2\times5\times7$,$2\times3^3\times7$,$2\times3\times5$ 与 $2\times3\times5\times7k$ 的代数和.

我们注意到这些特殊积 $3\times5\times7$,$2^2\times5\times7$,$2\times3^3\times7$,$2\times3\times5$ 和 $2\times3\times5\times7$ 有着它们内在的特殊规律.因为显然可见:

$$3\times5\times7=2^0\times3\times5\times7,\qquad 2^2\times5\times7=2^2\times3^0\times5\times7,$$
$$2\times3^3\times7=2\times3^3\times5^0\times7,\qquad 3\times5\times7=2\times3\times5\times7^0,$$
$$2\times3\times5\times7=2\times3\times5\times7.$$

其中,除最末一个外,其他每个都含一个素数的零次幂(实际上其值为 1)的因子.

这样的特殊积组,真是巧夺天工,分外耐人寻味.

将上述那种特殊积,逐个拓开分析,更觉异彩纷呈!

就 $3\times5\times7=2^0\times3\times5\times7$ 说:

(1) $x\equiv1\equiv3\times5\times7\equiv2^0\times3\times5\times7\equiv$
$2^0\times3\times5\times7+2^0\times3\times5\times7+2^0\times3\times5\times7\equiv2^0\times3^2\times5\times7\equiv$
$2^0\times3\times5\times7+2\times3\times5\times7\equiv2^0\times3^2\times5\times7\equiv$
$2^0\times3^2\times5\times7+2\times3\times5\times7\equiv2^0\times3\times5^2\times7\equiv$
$2^0\times3\times5^2\times7+2\times3\times5\times7\equiv2^0\times3\times5\times7^2\equiv$
$2^0\times3\times5\times7^2+2\times3\times5\times7\equiv2^0\times3^3\times5\times7\equiv$
$2^0\times3^3\times5\times7+2\times3^2\times5\times7\equiv2^0\times3^2\times5^2\times7\equiv$
$\cdots\equiv1\pmod2.$

(2) $2^0\times3\times5\times7+2^0\times3\times5\times7=2\times3\times5\times7.$
$2^0\times3\times5\times7+2^0\times3^2\times5\times7=2^2\times3\times5\times7.$
$2^0\times3\times5^2\times7+2^0\times3\times5\times7^2=2^2\times3^2\times5\times7.$
$2^0\times3^2\times5\times7+2^0\times3\times5^2\times7=2^3\times3\times5\times7.$
……

(3) $2^0\times3\times5\times7+2^0\times3\times5\times7+2^0\times3\times5\times7=2^0\times3^2\times5\times7.$
$2^0\times3\times5\times7+2^0\times3^2\times5\times7+2^0\times3\times5^2\times7=2^0\times3^3\times5\times7.$
$2^0\times3\times5\times7+2^0\times3\times5^2\times7+2^0\times3^2\times5^2\times7=2^0\times3^2\times5\times7^2.$
……

(4) $2\times3\times5\times7-2^0\times3\times5\times7=2^0\times3\times5\times7.$

$2^2\times3\times5\times7-2^0\times3\times5\times7=2^0\times3^2\times5\times7.$

$2^0\times3^2\times5\times7-2\times3\times5\times7=2^0\times3\times5\times7.$

……

(5) $2^0\times3\times5\times7+2^0\times3^3\times5\times7-2^0\times3^2\times5\times7=2^0\times3\times5\times7^2.$

$2^0\times3^3\times5\times7-2^0\times3^2\times5\times7-2^0\times3\times5\times7=2^0\times3\times5^2\times7.$

……

(6) $(2^0\times3\times5\times7)^n=2^0\times3^n\times5^n\times7^n$,($n$ 为正整数).

$(2^0\times3\times5\times7)\times(2^0\times3^2\times5\times7)=2^0\times3^3\times5^2\times7^2.$

……

就其他特殊积(如 $2^2\times3^0\times5\times7$, $2\times3^3\times5^0\times7$, …) 说,也都一样,各有特点.

上述特殊积都是素数 2,3,5 和 7 中每一素数的非负整数次幂与其余各素数的正整数次幂的积.

就其中,如 $2^0\times3\times5\times7$,$2^0\times3^2\times5^2\times7$,… 含因子 2^0 的一些积可以集合为一类;如 $2\times3^0\times5\times7$,$2^2\times3^0\times5\times7$,$2^3\times3^0\times5^2\times7$,… 含因子 3^0 的一些积又可以集合为另一类;…

也就是所有 3,5 和 7 的正整数次幂的积可以集合为一类;所有 2,5 和 7 的正整数次幂的积又可以集合为另一类;…

设 $a_1=2,a_2=3,a_3=5,a_4=7.$

于是,所有 3,5 和 7 的正整数次幂的积可以记为 $\{l_1\mid l_1=a_2^{b_2}a_3^{b_3}a_4^{b_4};b_2,b_3,b_4$ 为正整数$\}=\{l_1\mid l_1=a_1^0a_2^{b_2}a_3^{b_3}a_4^{b_4};b_2,b_3,b_4$ 为正整数$\}$ (因 $a_1^0=1$).

所有 2,5,7 的正整数次幂的积可以记为

$\{l_2\mid l_2=a_1^{b_1}a_3^{b_3}a_4^{b_4},b_1,b_3,b_4$ 为正整数$\}=\{l_2\mid l_2=a_1^{b_1}a_2^0a_3^{b_3}a_4^{b_4};b_1,b_3,b_4$ 为正整数$\}$ (因 $a_2^0=1$).

所有 2,3,7 的正整数次幂的积可以记为

$\{l_3\mid l_3=a_1^{b_1}a_2^{b_2}a_4^{b_4};b_1,b_2,b_4$ 为正整数$\}=\{l_3\mid l_3=a_1^{b_1}a_2^{b_2}a_3^0a_4^{b_4};b_1,b_2,b_4$ 为正整数$\}$ (因 $a_3^0=1$).

……

一般地说,设 n 为正整数;$a_1=2$, $a_2=3,a_3=5,\cdots,a_n$ 为从小到大的 n 个连续素数.在 a_1, a_2, $a_3,\cdots,a_{n-1}$ 和 a_n 这 n 个连续素数中,除素数 a_i 外,所有其余 $n-1$ 个素数的正整数次幂的积可以组成一个集合,这个全新的集合,我们就定义它为 Lai 集,也叫 $L(n,i)$ 集,简称为 Lai 或 L_i,即

$L_i=\{l_i\mid l_i=a_1^{b_1}a_2^{b_2}a_3^{b_3}\cdots a_{i-1}^{b_{i-1}}a_{i+1}^{b_{i+1}}\cdots a_n^{b_n}$, 其中,$b_1,b_2,b_3,\cdots,b_n$ 为正整数$\}$,

$i=1,2,3,\cdots,n$. 其中,l_i 为 L_i 的元素,即 $l_i\in L_i,i=1,2,3,\cdots,n$.

L_i 的元素 l_i 具有许多独具的特点,这些特点,我们就称为 Lai 集的性质,即 l_i 的性质.

对于 Lai 集的定义及其诸多重要的性质,我们将在“Lai 集的意义及其基本性质”这一章里加以明确和研究.

如前所述,若 x 为奇数,则有

$x=3\times5\times7+2^2\times5\times7+2\times3^3\times7+2\times3\times5-2\times3\times5\times7k$, 其中 k 为整数.

上式里,显然第一个乘积中不含素因数 2.

一般地说,设 n 为正整数;$a_1=2,a_2=3,a_3=5,\cdots,a_n$ 为从小到大的 n 个连续素数.若 x 与 $a_1,a_2,a_3,\cdots,a_n$ 都互素,则

$$x=a_2^{b_{12}}a_3^{b_{13}}a_4^{b_{14}}\cdots a_n^{b_{1n}}+a_1^{b_{21}}a_3^{b_{23}}a_4^{b_{24}}\cdots a_n^{b_{2n}}+a_1^{b_{31}}a_2^{b_{32}}a_4^{b_{34}}\cdots a_3^{b_{3n}}+\cdots+$$
$$a_1^{b_{n1}}a_2^{b_{n2}}a_3^{b_{n3}}\cdots a_{n-1}^{b_{n(n-1)}}-a_1a_2a_3\cdots a_nk,$$

其中 k 为整数,$b_{1_2},b_{1_3},b_{1_4},\cdots,b_{n_{(n-1)}}$ 为正整数.

依 Lai 集的定义,显然

$$a_2^{b_{12}}a_3^{b_{13}}a_4^{b_{14}}\cdots a_n^{b_{1n}}=l_1\in L_1,$$
$$a_1^{b_{21}}a_3^{b_{23}}a_4^{b_{24}}\cdots a_n^{b_{2n}}=l_2\in L_2,$$
$$a_1^{b_{31}}a_2^{b_{32}}a_4^{b_{34}}\cdots a_n^{b_{3n}}=l_3\in L_3,$$
$$\cdots\cdots\cdots\cdots$$
$$a_1^{b_{n1}}a_2^{b_{n2}}a_3^{b_{n3}}\cdots a_{n-1}^{b_{n(n-1)}}=l_n\in L_n;$$
$$a_1a_2a_3\cdots a_n=c.$$

于是 $x=l_1+l_2+l_3+\cdots+l_i+\cdots+l_n-kc$,它是 $l_1,l_2,l_3,\cdots,l_n$ 和 kc 的代数和.

若 x 只含素因数 a_1,而与其他素数都互素,则上式里缺首项;

若 x 只含素因数 a_2,而与其他素数都互素,则前式里缺第二项;

$\cdots\cdots\cdots\cdots$

如上面用含有 L_1, L_2, $L_3,\cdots,L_n$ 的元素 $l_1,l_2,l_3,\cdots,l_n$ 与 c 所表示的代数式,我们称它们为 l_i 表示式.

显然,l_i 表示式是一个与素数紧密联系着的代数式.它展示出 Lai 集的独具特性,由此产生、得到突出而重要的规律.如上面所展示的 l_i 表示式里,若整数 x 的表示式为

$$l_1+l_2+l_3+\cdots+l_n-kc, \tag{1}$$

且整数 x 大于素数 a_n 而小于 a_{n+1}^2(a_{n+1} 是大于素数 a_n 的最小素数)时,整数 x 便大于 a_n 而小于 a_{n+1}^2 且与素数 $a_1,a_2,a_3,\cdots,a_n$ 都互素,x 便是一个素数,(1) 式便是素数 x 的 l_i 表示式.否则,(1) 式所表示的整数 x 虽与 n 个素数 $a_1,a_2,a_3,\cdots,a_n$ 都互素,我们还不能判定 整数 x 一定是素数.

若
$$x=l_2+l_3+l_4+\cdots+l_n-kc, \tag{2}$$

其中,整数 $x=2$ 时,(2) 式便是最小素数 a_1(即 2) 的 l_i 表示式.它表示整数 x 只含素因数 a_1 而与其他素数 $a_2,a_3,a_4,\cdots,a_n$ 都互素.a_1 是最小的素数.若(2) 式表示的整数 x 大于 2,则整数 x 是含素因数 a_1(即 2) 而与其他素数 $a_2,a_3,a_4,\cdots,a_n$ 都互素,并且是大于素数 a_1(即 2) 的偶数里的合数.这样,(2) 式便是合数 x 的 l_i 表示式.

一般地说,若
$$x=l_1+l_2+l_3+\cdots+l_{j-1}+l_{j+1}+\cdots+kc, \tag{3}$$

由于上式里缺 L_j 的元素 l_j,这表明整数 x 只含素因数 a_j,而与其他素数 $a_1,a_2,a_3,\cdots,a_{j-1},a_{j+1},\cdots,a_n$ 都互素.因而当整数 $x=a_j$(素数) 时,整数 x 就是素数 a_j.这样,(3) 式便是素数 x 的 l_i 表示式.

当整数 x 大于素数 a_j 时,则整数 x 是大于素数 a_j 的 a_j 的倍数,整数 x 是一个合数.于是,(3) 式便是合数 x 的 l_i 表示式.

这正表明,我们研究 l_i 表示式,挖掘它的内部特性,探索出将整数里的 1、素数和合数都用

这种全新的 l_i 表示式作为对整数的重新表述，它为我们对整数的深入研究展示出一个全新而广阔的空间.

我们依据 Lai 集所独具的特性，结合 l_i 表示式，运用同余理论，探索、研究、论证整数的 l_i 表示式存在定理，证明在整数里每个整数都存在着它的 l_i 表示式，并且当 $l_j \in L_j$ 且 $l_j < c$ 时，表示式是惟一的.

不仅如此，我们根据其存在的条件与各自表述的特点和相互间的表述差异，研究其基本而重要的性质，…… 继续深入探讨，挖掘他们内在的规律和特点，得到极其重要的判别素数或合数的充要条件，即：素数的充要条件. 这全新的素数判定定理，无论在理论上还是在实际运用中，使得我们对素数和合数更深入的认识成为可能，同时在研究和解答有关的问题时，它表现独具的极其重要的作用. 运用它，我们有着许多新的发现，同时也证明得到重要的“在素数 a_n 与 $2a_n$ 之间存在奇素数定理”. 所有这些，我们将在“整数的 l_i 表示式和素数的充要条件”一章中着重研究并给出较为详细的论证.

以 Lai 集中的元素为基点，应用一次不定方程，结合 l_i 表示式，我们得出一类独特的不定方程：“l_i 系数不定方程”，即

$$l_1x_1 + l_2x_2 + l_3x_3 + \cdots + l_nx_n - cy = d_1 \quad (d_1 \text{ 为整数})$$

或

$$cy - l_1x_1 - l_2x_2 - l_3x_3 - \cdots - l_nx_n = d_2 \quad (d_2 \text{ 为整数}).$$

它有着独具的特点，它不仅有整数解、正整数解、最小正整数解，而且还有负整数解、最大负整数解、非负整数解，…… 以及惟一存在的独特解：l_i 系数不定方程的最小正整数解.

进一步研究 l_i 系数不定方程，我们得到

$$\pm l_1x_1 \pm l_2x_2 \pm l_3x_3 \pm \cdots \pm l_nx_n \mp cy = d, \tag{A}$$

$$\pm l_3x_3 \pm l_4x_4 \pm l_5x_5 \pm \cdots \pm l_nx_n \mp cy = 6d \tag{B}$$

和

$$\pm l_4x_4 \pm l_5x_5 \pm l_6x_6 \pm \cdots \pm l_nx_n \mp cy = 30d, \tag{C}$$

其中，d 为整数，$c = a_1a_2a_3\cdots a_n$. 它们都还有大 L_y 解和 L_y 解.

l_i 系数不定方程(B) 与 l_i 系数不定方程(C) 还有其独特的小 L_y 解.

l_i 系数不定方程(A)，即 l_i 系数不定方程

$$l_1x_1 + l_2x_2 + l_3x_3 + \cdots + l_nx_n - cy = d_1 \quad (d_1 \text{ 为整数}) \tag{A_1}$$

和

$$cy - l_1x_1 - l_2x_2 - l_3x_3 - \cdots - l_nx_n = d_2 \quad (d_2 \text{ 为整数}) \tag{A_2}$$

有大 L_y 解的充要条件是 d_1 或 d_2 为素数 a_j 的倍数(或 0)，$j \in \{1,2,3,\cdots,n\}$

l_i 系数不定方程(A_1)[或(A_2)] 有 L_y 解的充要条件是 d_1(或 d_2) 与素数 a_i 互素，$i = 1,2,\cdots,n$.

当 $n, l_1, l_2, l_3, \cdots, l_n$ 和 d_1(或 d_2) 的值取定后，l_i 系数不定方程(A_1)[或(A_2)] 有其惟一的、x_i 的值为不大于素数 a_i 的最小正整数($i = 1,2,3,\cdots,n$) 和 y 值为整数的整数解.

如果依次分别以连续数的每一个数作为 d_1(或 d_2) 的值，依次得到一些如(A_1)[或(A_2)] 型的 l_i 系数不定方程，将这些不定方程每 a_j 个分为一组，依次得到第一组，第二组，第三组，$\cdots, j \in \{1,2,3,\cdots,n\}$. 则各组里的不定方程，每个有其惟一的、$x_i$ 值为不大于 a_i 的正整数($i = 1,2,3,\cdots,n$)，y 值为整数的整数解.

所有各个不定方程的整数解中，x_j 的值依次排列一线，便成为一个项数为 a_j 的循环数列.

……

关于各种类型的 l_i 系数不定方程的解法、特性、规律、解的分布及其组成等，这些我们都将在“l_i 系数不定方程”一章中深入探讨和研究.

在一定的数集范围内，无论素数还是合数，我们都可以应用素数的充要条件加以判别；然而，当整数 n 是任意大的整数时，在大于 a_n 而小于 a_{n+1}^2 的整数范围内是否确实存在素数？整数的范围大小有无限制？存在素数的个数有多少？

我们进一步研究得到，存在 m 组正整数：k 和 $s_i \in \{1,2,3,\cdots,a_i-1\}$，$i=1,2,3,\cdots n$，使得下式立：

$$Y = d_1 = l_1 s_1 + l_2 s_2 + l_3 s_3 + \cdots + l_n s_n - kc = l_1 + l_2 s_2 + l_3 s_3 + \cdots + l_n s_n - kc,$$

且满足：$a_n < Y < a_{n+1}^2$，Y 为奇素数.

而 m 为正整数，它的值不小于下式的整数部分：

$$\frac{a_{n+1}^2 - a_n - 3}{a_n} \times \frac{(a_3-1)(a_4-1)(a_5-1)\cdots(a_n-1)}{a_2 a_3 a_4 \cdots a_{n-1}}.$$

从而开拓引申，所得重要特点，我们都将在“Y.M.定理”一章里详尽地分析论证.

最后，为了方便求解素数，我们在“新素数的求法”一章里详细介绍了三种不同求素数的方法。

综上所述，以同余理论，结合数集的性质，研究素数、合数，给我们提出了一个全新的思路和方法，它必将揭示出更宽阔的对整数的研究空间.

为了使广大数学爱好者易于阅读和理解本书的内容，我们首先介绍和阐述“同余的意义和基本性质”与“素数的基本性质”，介绍“Lai集的意义及其基本性质”，接着重点研究“整数的 l_i 表示式和素数的充要条件”，着重研讨“一次不定方程及其解法”与“l_i 系数不定方程及其解法”，详细推证“Y.M.定理”，最后研究得到“新素数的求法”.

全书内容分为七章.每章除给出部分例题外，还备有练习题，供研究、练习.书末附有练习题参考解答，供读者参考.

君利、君良和君昉对“Lai集的意义及其基本性质”、“整数的 l_i 表示式”等章内容颇感兴趣，并参予编写“l_i 系数不定方程”一章.

本书所涉及的内容是一个全新的领域，内容多而广，书中可能存在不妥之处或者错误，诚望广大读者多提宝贵意见，批评指正！

本书的出版，得到了学校领导的关怀与支持，刘金旺教授在百忙中为本书审核、撰写序言，并对本书所具的重要特点给予明示.在本书的撰写过程中，上海华东师范大学校长刘佛年教授、北京科技大学赖和怡教授、北京铁道部科学研究院刘作枢教授、河南省洛阳教育学院陈正廷教授和李滢教授、北京中国原子能科学研究院阳名珠教授和陈学益同志、张淑珍同志等以及许多老同志给予了长期的鼓励，提出了许多宝贵的建议以及多方面的大力支持，在此一并表示由衷的感谢！

赖以明

2002年10月

目　录

第一章　同余的意义和基本性质

§1.1　同余的定义和性质

定义　假设 m 是一个确定的正整数，把它叫做模；a 和 b 是两个整数. 如果用 m 分别去除 a 和 b，若是所得的余数相同，我们就说：a、b 对模 m 同余；或者说：对模 m，a 和 b 同余；记作 $a \equiv b(\mathrm{mod}m)$. 若是所得的余数不相同，我们就说：$a$、$b$ 对模 m 不同余；或者说：对模 m，a 和 b 不同余；记作 $a \not\equiv b(\mathrm{mod}m)$.

依定义，同余显然有如下性质：

性质 1　**设 a 是一个整数，m 是一个正整数，则有** $a \equiv a(\mathrm{mod}m)$.

例 1　下列各式显然都成立：

$$25 \equiv 25(\mathrm{mod}7),\quad 12 \equiv 12(\mathrm{mod}19),\quad 9 \equiv 9(\mathrm{mod}9),$$
$$29 \equiv 29(\mathrm{mod}31),\quad 0 \equiv 0(\mathrm{mod}8),\quad -8 \equiv -8(\mathrm{mod}15).$$

性质 2　**设 a 和 b 是整数，m 是一个正整数，若** $a \equiv b(\mathrm{mod}m)$，**则有** $b \equiv a(\mathrm{mod}m)$.

例 2　(1) 23 和 37 对模 7 是同余的，即 $23 \equiv 37(\mathrm{mod}7)$，也有 $37 \equiv 23(\mathrm{mod}7)$.

（因两式都表明 37 和 23 分别被 7 除时，余数相同，同为 2.）

(2) 29 和 13 对模 8 是同余的，即 $29 \equiv 13(\mathrm{mod}8)$，也有 $13 \equiv 29(\mathrm{mod}8)$.

（因两式都表明 13 和 29 分别被 8 除时，余数相同，同为 5.）

(3) 1 和 6 对模 5 是同余的，即 $1 \equiv 6(\mathrm{mod}5)$，也有 $6 \equiv 1(\mathrm{mod}5)$.

（因两式都表明 6 和 1 分别被 5 除时，余数相同，同为 1.）

(4) -7 和 7 对模 7 是同余的，即 $-7 \equiv 7(\mathrm{mod}7)$，也有 $7 \equiv -7(\mathrm{mod}7)$.

（因两式都表明 7 和 -7 分别被 7 除时，余数相同，同为 0.）

(5) -4 和 8 对模 12 是同余的，即 $-4 \equiv 8(\mathrm{mod}12)$，也有 $8 \equiv -4(\mathrm{mod}12)$.

（因两式都表明：8 被 12 除时，余数为 -4；-4 被 12 除时余数也是 -4，余数相同；或 8 被 12 除时余数为 8；-4 被 12 除时商 -1，余数也是 8，相同.）

(6) 0 和 6 对模 6 是同余的，即 $0 \equiv 6(\mathrm{mod}6)$，也有 $6 \equiv 0(\mathrm{mod}6)$.

（因两式都表明 6 和 0 分别被 6 除时，余数相同，同为 0.）

性质 3　**设 a 和 b 是整数，m 是一个正整数，若** $a = b$，**则** $a \equiv b(\mathrm{mod}m)$.

设 a, b, c, d 和 e 都是整数，b 非零，m 和 n 为正整数；

(1) **当** $a + b = c$ **时，则** $a + b \equiv c(\mathrm{mod}m)$；

(2) **当** $a - b = d$ **时，则** $a - b \equiv d(\mathrm{mod}m)$；

(3) 当 $ab = e$ 时，则 $ab \equiv e(\mathrm{mod}m)$；

(4) 当 $\frac{e}{b} = a$ 时，则 $\frac{e}{b} \equiv a(\mathrm{mod}m)$；

(5) 当 $a + b = c + d$ 时，则 $a + b \equiv c + d(\mathrm{mod}m)$；

(6) 当 $a - b = c - d$ 时，则 $a - b \equiv c - d(\mathrm{mod}m)$；

(7) 当 $a + b - c = d + e$ 时，则 $a + b - c \equiv d + e(\mathrm{mod}m)$；

(8) 当 $a + bc = d$ 时，则 $a + bc \equiv d(\mathrm{mod}m)$；

(9) 当 $ab - c = e$ 时，则 $ab - c \equiv e(\mathrm{mod}m)$；

(10) 当 $a^n = b$ 时，则 $a^n \equiv b(\mathrm{mod}m)$.

事实上，当等式成立时，则用正整数 m 去除等式左边所得的余数，与用正整数 m 去除等式右边所得的余数，两者显然是相同的.

反之，同余成立，则对模 m 同余的两数不一定都相等.

例 3 (1) $11 + 8 = 19$，$11 + 8 \equiv 19(\mathrm{mod}13)$.

(2) $17 - 6 = 11$，$17 - 6 \equiv 11(\mathrm{mod}8)$.

(3) $6 \times 5 = 30$，$6 \times 5 \equiv 30(\mathrm{mod}15)$.

(4) $\frac{72}{9} = 8$，$\frac{72}{9} \equiv 8(\mathrm{mod}5)$.

(5) $1 + 20 = 13 + 8$，$1 + 20 \equiv 13 + 8(\mathrm{mod}9)$.

(6) $60 - 47 = 25 - 12$，$60 - 47 \equiv 25 - 12(\mathrm{mod}14)$.

(7) $25 \equiv 11(\mathrm{mod}7)$，$25 \neq 11$.

(8) $13 + 5 \equiv 7 + 11(\mathrm{mod}15)$，$13 + 5 = 7 + 11$.

推论 若 $a \not\equiv b(\mathrm{mod}m)$，则 $a \neq b$.

性质 4 若 $a \equiv b(\mathrm{mod}m)$，$b \equiv c(\mathrm{mod}m)$，则 $a \equiv c(\mathrm{mod}m)$.

事实上，由于 $a \equiv b(\mathrm{mod}m)$，则用 m 分别去除 a 和 b 时，所得的余数相同；设用 m 除 a 得商 q_1，余数为 r，即 $a = q_1 m + r$；用 m 除 b 得商 q_2，余数也是 r，即 $b = q_2 m + r$.

又 $b \equiv c(\mathrm{mod}m)$，则用 m 分别去除 b 和 c 时，所得的余数也相同；既 $b = q_2 m + r$，则用 m 去除 c 时，所得的商设为 q_3，余数便是 r，即 $c = q_3 m + r$.

由于 $a = q_1 m + r$，$c = q_3 m + r$，故用 m 分别去除 a 和 c 时，所得的余数也同是 r；因此，a 和 c 对模 m 同余，所以 $a \equiv c(\mathrm{mod}m)$. 从而有 $a \equiv b \equiv c(\mathrm{mod}m)$.

例 4 下列两式都成立：

(1) 因 $8 \equiv 15(\mathrm{mod}7)$，$15 \equiv 29(\mathrm{mod}7)$，有 $8 \equiv 29(\mathrm{mod}7)$，即 $8 \equiv 15 \equiv 29(\mathrm{mod}7)$.

(2) 因 $5 \equiv -3(\mathrm{mod}8)$，$5 \equiv 21(\mathrm{mod}8)$，有 $21 \equiv -3(\mathrm{mod}8)$.

事实上，在(2)中，因 $5 \equiv 21(\mathrm{mod}8)$，依性质 2，有 $21 \equiv 5(\mathrm{mod}8)$.

于是得 $21 \equiv 5(\mathrm{mod}8)$，$5 \equiv -3(\mathrm{mod}8)$，故 $21 \equiv 5 \equiv -3(\mathrm{mod}8)$，

即有 $21 \equiv -3(\mathrm{mod}8)$，$-3 \equiv 21(\mathrm{mod}8)$.

定理 1 整数 a 和 b 对模 m 同余的充要条件是：m 整除 $a - b$，即 $m \mid (a - b)$[即 $a - b \equiv 0(\mathrm{mod}m)$]，亦即 $a - b = mt$(即 $a = mt + b$)，其中 t 为整数.

证明 先证充分性.

当正整数 m 整除 $a - b$，即 $m \mid (a - b)$，亦即 $a - b \equiv 0(\mathrm{mod}m)$ 时，则 $a - b$ 便是 m 的倍数，于是 $a - b = mt$，因而有 $a = mt + b$，其中 t 为整数.

用正整数 m 除 $mt + b$ 时，应用除法分配律，m 除 mt 得余数 0，m 除 b 得余数设为 r，r 为

小于 m 的非负整数,因而用正整数 m 去除 $mt+b$ 时,得余数 r.

既然 $a=mt+b$,依性质3(1),有 $a\equiv mt+b(\mathrm{mod}m)$.因而用 m 除 a 的余数与用 m 除 $mt+b$ 的余数相同,余数也是 r.从而用正整数 m 分别除 a 和 b 的余数相同,同为 r,依定义,所以 a、b 对模 m 同余,就是 $a\equiv b(\mathrm{mod}m)$.

次证必要性.

既然整数 a 和 b 对模 m 同余,即 $a\equiv b(\mathrm{mod}m)$,依定义,故用正整数 m 分别去除整数 a 和 b 所得的余数相同,设这相同的余数为整数 r.则 $a-r$ 和 $b-r$ 分别被 m 除时余数便同为0,故 $a-r$ 和 $b-r$ 同为 m 的倍数.

因而 $(a-r)-(b-r)$ 也是 m 的倍数,即 $a-b$ 为 m 的倍数.设 $a-b=mt$,其中 t 为整数.

既然 $a-b=mt$,t 为整数,即 $a-b$ 为 m 的倍数,故用 m 除 $a-b$ 时余数为0,依定义,有 $a-b\equiv 0(\mathrm{mod}m)$.

从而 $m\mid(a-b)$,就是 m 能整除 $a-b$. **证毕**

依定理1,对同余这一概念,又可定义为:若 $m\mid(a-b)$,则 a 和 b 叫做对模 m 同余.

依定理1和整除的性质,便得下列性质:

性质5　**若** $a\equiv b(\mathrm{mod}m)$, $c\equiv d(\mathrm{mod}m)$, **则**

$$a+c\equiv b+d(\mathrm{mod}m),\ a-c\equiv b-d(\mathrm{mod}m).$$

证明　因 $a\equiv b(\mathrm{mod}m)$, $c\equiv d(\mathrm{mod}m)$,依定理1,有

$a-b=mt_1$,t_1 为整数;$c-d=mt_2$,t_2 为整数.

于是 $(a-b)+(c-d)=mt_1+mt_2=m(t_1+t_2)$,

即 $(a+c)-(b+d)=m(t_1+t_2)$.

由于 t_1+t_2 为整数,依定理1,故得 $a+c\equiv b+d(\mathrm{mod}m)$.

又 $(a-b)-(c-d)=mt_1-mt_2=m(t_1-t_2)$,

即 $(a-c)-(b-d)=m(t_1-t_2)$.

由于 t_1-t_2 为整数,依定理1,故得 $a-c\equiv b-d(\mathrm{mod}m)$. **证毕**

性质6　**若** $a+b\equiv c(\mathrm{mod}m)$,**则** $a\equiv c-b(\mathrm{mod}m)$, $a-c\equiv -b(\mathrm{mod}m)$.

证明　因 $a+b\equiv c(\mathrm{mod}m)$,又依性质1,有 $b\equiv b(\mathrm{mod}m)$,故依性质5,有

$(a+b)-b\equiv c-b(\mathrm{mod}m)$,即 $a\equiv c-b(\mathrm{mod}m)$.

再 $a+b\equiv c(\mathrm{mod}m)$,又依性质1,有 $b+c\equiv b+c(\mathrm{mod}m)$.

故依性质5,有 $(a+b)-(b+c)\equiv c-(b+c)(\mathrm{mod}m)$,

即 $$a-c\equiv -b(\mathrm{mod}m).$$ **证毕**

推论　**若** $a-b\not\equiv 0(\mathrm{mod}m)$,**则** $a\not\equiv b(\mathrm{mod}m)$,**反之亦然**.

性质7　**若** $a\equiv b(\mathrm{mod}m)$, c **是一个整数,则** $ac\equiv bc(\mathrm{mod}m)$.

证明　因 $a\equiv b(\mathrm{mod}m)$,依定理1,有 $a-b=mt$,t 为整数.又 c 是一个整数,于是有

$$(a-b)c=mt\cdot c,\text{即 } ac-bc=m\cdot(ct).$$

从而依定理1,得 $$ac\equiv bc(\mathrm{mod}m).$$ **证毕**

性质8　**若** $a\equiv b(\mathrm{mod}m)$,$c\equiv d(\mathrm{mod}m)$,**则** $ac\equiv bd(\mathrm{mod}m)$.

证明　因 $a\equiv b(\mathrm{mod}m)$,依性质7,有 $ac\equiv bc(\mathrm{mod}m)$. (a)

又 $c\equiv d(\mathrm{mod}m)$,同理有 $bc\equiv bd(\mathrm{mod}m)$. (b)

由(a)和(b),依性质4,有 $ac \equiv bc \equiv bd(\mathrm{mod}m)$.

所以 $ac \equiv bd(\mathrm{mod}m)$. 证毕

性质9 若 $a \equiv b(\mathrm{mod}m)$,$n$ 正整数,则 $a^n \equiv b^n(\mathrm{mod}m)$.

证明 当 $n = 1$ 时,显然有 $a \equiv b(\mathrm{mod}m)$. (1)

当 $n = 2$ 时,由(1)和(1),依性质8,有 $a^2 \equiv b^2(\mathrm{mod}m)$. (2)

由(1)和(2),依性质8,得 $a^3 \equiv b^3(\mathrm{mod}m)$. (3)

由(1)和(3),同理,得 $a^4 \equiv b^4(\mathrm{mod}m)$. (4)

同理类推,得 $a^n \equiv b^n(\mathrm{mod}m)$. 证毕

性质10 设 n 为正整数,c_i 为整数,则当 $a_i \equiv b_i(\mathrm{mod}m), i = 1,2,3,\cdots,n$ 时,有

$$a_1c_1 + a_2c_2 + a_3c_3 + \cdots + a_nc_n \equiv b_1c_1 + b_2c_2 + b_3c_3 + \cdots + b_nc_n(\mathrm{mod}m),$$

即
$$\sum_{i=1}^{n} a_ic_i \equiv \sum_{i=1}^{n} b_ic_i(\mathrm{mod}m).$$

证明 因 c_i 为整数,$a_i \equiv b_i(\mathrm{mod}m), i = 1,2,3,\cdots,n$.

依性质7,有 $a_ic_i \equiv b_ic_i(\mathrm{mod}m), i = 1,2,3,\cdots,n$.

于是,当 $i = 1$ 时,有 $a_1c_1 \equiv b_1c_1(\mathrm{mod}m)$; (1)

当 $i = 2$ 时,有 $a_2c_2 \equiv b_2c_2(\mathrm{mod}m)$; (2)

当 $i = 3$ 时,有 $a_3c_3 \equiv b_3c_3(\mathrm{mod}m)$; (3)

……

当 $i = n$ 时,有 $a_nc_n \equiv b_nc_n(\mathrm{mod}m)$. (n)

由(1)和(2),依性质5,得 $a_1c_1 + a_2c_2 \equiv b_1c_1 + b_2c_2(\mathrm{mod}m)$. (2′)

由(2′)和(3),同理得 $a_1c_1 + a_2c_2 + a_3c_3 \equiv b_1c_1 + b_2c_2 + b_3c_3(\mathrm{mod}m)$, (3′)

……

照样继续进行,最后得 $a_1c_1 + a_2c_2 + a_3c_3 + \cdots + a_nc_n \equiv$

$$b_1c_1 + b_2c_2 + b_3c_3 + \cdots + b_nc_n(\mathrm{mod}m),$$

即得
$$\sum_{i=1}^{n} a_ic_i \equiv \sum_{i=1}^{n} b_ic_i(\mathrm{mod}m).$$ 证毕

一般地,我们有

定理2 设 n 为正整数,$i = 1,2,3,\cdots,n$. 若 $a_i, b_i, c_i, \cdots, f_i$ 都是正整数;$A_{i_1}, A_{i_2}, B_{i_1}, B_{i_2}, C_{i_1}, C_{i_2}, \cdots, F_{i_1}$ 和 F_{i_2},以及 $Xa_ib_ic_i\cdots f_i$ 和 $Ya_ib_ic_i\cdots f_i$ 都是整数,且

$A_{i_1} \equiv A_{i_2}(\mathrm{mod}m)$, $B_{i_1} \equiv B_{i_2}(\mathrm{mod}m)$, $C_{i_1} \equiv C_{i_2}(\mathrm{mod}m)$, $\cdots$, $F_{i_1} \equiv F_{i_2}(\mathrm{mod}m)$;

$Xa_ib_ic_i\cdots f_i \equiv Ya_ib_ic_i\cdots f_i(\mathrm{mod}m)$.

则 $Xa_1b_1c_1\cdots f_1A_{1_1}^{a_1}B_{1_1}^{b_1}C_{1_1}^{c_1}\cdots F_{1_1}^{f_1} + Xa_2b_2c_2\cdots f_2A_{2_1}^{a_2}B_{2_1}^{b_2}C_{2_1}^{c_2}\cdots F_{2_1}^{f_2} +$

$Xa_3b_3c_3\cdots f_3A_{3_1}^{a_3}B_{3_1}^{b_3}C_{3_1}^{c_3}\cdots F_{3_1}^{f_3} + \cdots + Xa_nb_nc_n\cdots f_nA_{n_1}^{a_n}B_{n_1}^{b_n}C_{n_1}^{c_n}\cdots F_{n_1}^{f_n} \equiv$

$Ya_1b_1c_1\cdots f_1A_{1_2}^{a_1}B_{1_2}^{b_1}C_{1_2}^{c_1}\cdots F_{1_2}^{f_1} + Ya_2b_2c_2\cdots f_2A_{2_2}^{a_2}B_{2_2}^{b_2}C_{2_2}^{c_2}\cdots F_{2_2}^{f_2} +$

$Ya_3b_3c_3\cdots f_3A_{3_2}^{a_3}B_{3_2}^{b_3}C_{3_2}^{c_3}\cdots F_{3_2}^{f_3} + \cdots + Ya_nb_nc_n\cdots f_nA_{n_2}^{a_n}B_{n_2}^{b_n}C_{n_2}^{c_n}\cdots F_{n_2}^{f_n}(\mathrm{mod}m)$.

证明 由于 $A_{i_1} \equiv A_{i_2}(\mathrm{mod}m), B_{i_1} \equiv B_{i_2}(\mathrm{mod}m), C_{i_1} \equiv C_{i_2}(\mathrm{mod}m), \cdots, F_{i_1} \equiv F_{i_2}(\mathrm{mod}m)$,又 $a_i, b_i, c_i, \cdots, f_i$ 都是正整数,依性质9,分别有

$$A_{i_1}^{a_i} \equiv A_{i_2}^{a_i}(\mathrm{mod}m),\ B_{i_1}^{b_i} \equiv B_{i_2}^{b_i}(\mathrm{mod}m),$$