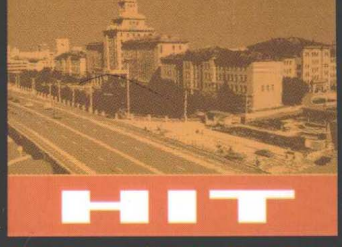
Elementary Number Theory (Ⅱ)



HIT

数论经典著作系列

初等数论(Ⅱ)

陈景润 著

哈爾濱工業大學出版社
HARBIN INSTITUTE OF TECHNOLOGY PRESS

数论经典著作系列

Elementary Number Theory (II)

初等数论 (II)

陈景润 著

哈爾濱工業大學出版社
HARBIN INSTITUTE OF TECHNOLOGY PRESS

内 容 简 介

数论是研究数的性质的一门学科。本书从科学实验的实际经验出发，分析了数论的发生、发展和应用，介绍了数论的初等方法。本书为《初等数论(I)》的后续，介绍了剩余系、数论函数、三角和等方法。每章后有习题，并在书末附有全部习题解答。本书写得深入浅出，通俗易懂，可供广大青年及科技人员阅读。

图书在版编目(CIP)数据

初等数论.2/陈景润著.—哈尔滨:哈尔滨工业大学出版社,2012.2

ISBN 978-7-5603-3494-3

Ⅰ.①初… Ⅱ.①陈… Ⅲ.①初等数论 Ⅳ.①O156.1

中国版本图书馆 CIP 数据核字(2012)第 014349 号

策划编辑 刘培杰 张永芹
责任编辑 尹 凡
封面设计 孙茵艾
出版发行 哈尔滨工业大学出版社
社 址 哈尔滨市南岗区复华四道街 10 号 邮编 150006
传 真 0451-86414749
网 址 http://hitpress.hit.edu.cn
印 刷 黑龙江省教育厅印刷厂
开 本 787mm×1092mm 1/16 印张 9.5 字数 170 千字
版 次 2012 年 2 月第 1 版 2012 年 2 月第 1 次印刷
书 号 ISBN 978-7-5603-3494-3
定 价 18.00 元

哈尔滨工业大学出版社刘培杰数学工作室
已出版(即将出版)图书目录

书　名	出版时间	定　价	编号
新编中学数学解题方法全书(高中版)上卷	2007－09	38.00	7
新编中学数学解题方法全书(高中版)中卷	2007－09	48.00	8
新编中学数学解题方法全书(高中版)下卷(一)	2007－09	42.00	17
新编中学数学解题方法全书(高中版)下卷(二)	2007－09	38.00	18
新编中学数学解题方法全书(高中版)下卷(三)	2010－06	58.00	73
新编中学数学解题方法全书(初中版)上卷	2008－01	28.00	29
新编中学数学解题方法全书(初中版)中卷	2010－07	38.00	75
新编平面解析几何解题方法全书(专题讲座卷)	2010－01	18.00	61
数学眼光透视	2008－01	38.00	24
数学思想领悟	2008－01	38.00	25
数学应用展观	2008－01	38.00	26
数学建模导引	2008－01	28.00	23
数学方法溯源	2008－01	38.00	27
数学史话览胜	2008－01	28.00	28
从毕达哥拉斯到怀尔斯	2007－10	48.00	9
从迪利克雷到维斯卡尔迪	2008－01	48.00	21
从哥德巴赫到陈景润	2008－05	98.00	35
从庞加莱到佩雷尔曼	2011－08	138.00	136
从比勃巴赫到德·布朗斯	即将出版		
数学解题中的物理方法	2011－06	28.00	114
数学解题的特殊方法	2011－06	48.00	115
中学数学计算技巧	2012－01	48.00	116
中学数学证明方法	2012－01	58.00	117
数学趣题巧解	2012－03	28.00	128
数学奥林匹克与数学文化(第一辑)	2006－05	48.00	4
数学奥林匹克与数学文化(第二辑)(竞赛卷)	2008－01	48.00	19
数学奥林匹克与数学文化(第二辑)(文化卷)	2008－07	58.00	36
数学奥林匹克与数学文化(第三辑)(竞赛卷)	2010－01	48.00	59
数学奥林匹克与数学文化(第四辑)(竞赛卷)	2011－08	58.00	87

哈尔滨工业大学出版社刘培杰数学工作室
已出版(即将出版)图书目录

书　名	出版时间	定　价	编号
发展空间想象力	2010－01	38.00	57
走向国际数学奥林匹克的平面几何试题诠释(上、下)(第2版)	2010－02	98.00	63,64
平面几何证明方法全书	2007－08	35.00	1
平面几何证明方法全书习题解答(第2版)	2006－12	18.00	10
最新世界各国数学奥林匹克中的平面几何试题	2007－09	38.00	14
数学竞赛平面几何典型题及新颖解	2010－07	48.00	74
初等数学复习及研究(平面几何)	2008－09	58.00	38
初等数学复习及研究(立体几何)	2010－06	38.00	71
初等数学复习及研究(平面几何)习题解答	2009－01	48.00	42
世界著名平面几何经典著作钩沉——几何作图专题卷(上)	2009－06	48.00	49
世界著名平面几何经典著作钩沉——几何作图专题卷(下)	2011－01	88.00	80
世界著名平面几何经典著作钩沉(民国平面几何老课本)	2011－03	38.00	113
世界著名数论经典著作钩沉(算术卷)	2012－01	28.00	125
世界著名数学经典著作钩沉——立体几何卷	2011－02	28.00	88
世界著名三角学经典著作钩沉(平面三角卷Ⅰ)	2010－06	28.00	69
世界著名三角学经典著作钩沉(平面三角卷Ⅱ)	2011－01	28.00	78
世界著名初等数论经典著作钩沉(理论和实用算术卷)	2011－07	38.00	126
几何学教程(平面几何卷)	2011－03	68.00	90
几何学教程(立体几何卷)	2011－07	68.00	130
几何变换与几何证题	2010－06	88.00	70
几何瑰宝——平面几何500名题暨1000条定理(上、下)	2010－07	138.00	76,77
三角形的五心	2009－06	28.00	51
俄罗斯平面几何问题集	2009－08	88.00	55
俄罗斯平面几何5000题	2011－03	58.00	89
计算方法与几何证题	2011－06	28.00	129
463个俄罗斯几何老问题	2012－01	28.00	152
近代欧氏几何学	2012－2	38.00	162

哈尔滨工业大学出版社刘培杰数学工作室
已出版(即将出版)图书目录

书　名	出版时间	定　价	编号
超越吉米多维奇——数列的极限	2009－11	48.00	58
初等数论难题集(第一卷)	2009－05	68.00	44
初等数论难题集(第二卷)(上、下)	2011－02	128.00	82,83
谈谈素数	2011－03	18.00	91
平方和	2011－03	18.00	92
数论概貌	2011－03	18.00	93
代数数论	2011－03	48.00	94
初等数论的知识与问题	2011－02	28.00	95
超越数论基础	2011－03	28.00	96
数论初等教程	2011－03	28.00	97
数论基础	2011－03	18.00	98
数论入门	2011－03	38.00	99
解析数论引论	2011－03	48.00	100
基础数论	2011－03	28.00	101
超越数	2011－03	18.00	109
三角和方法	2011－03	18.00	112
谈谈不定方程	2011－05	28.00	119
整数论	2011－05	38.00	120
初等数论100例	2011－05	18.00	122
最新世界各国数学奥林匹克中的初等数论试题(上、下)	2012－01	138.00	144,145
算术探索	2011－12	158.00	148
初等数论(Ⅰ)	2012－01	18.00	156
初等数论(Ⅱ)	2012－01	18.00	157
初等数论(Ⅲ)	2012－01	28.00	158
组合数学浅谈	2012－02	18.00	159
同余理论	2012－02	38.00	163

哈尔滨工业大学出版社刘培杰数学工作室
已出版(即将出版)图书目录

书　名	出版时间	定　价	编号
历届 IMO 试题集(1959—2005)	2006—05	58.00	5
历届 CMO 试题集	2008—09	28.00	40
历届国际大学生数学竞赛试题集(1994—2010)	2012—01	28.00	143
全国大学生数学夏令营数学竞赛试题及解答	2007—03	28.00	15
历届美国大学生数学竞赛试题集	2009—03	88.00	43
前苏联大学生数学竞赛试题及解答(上)	2012—03	28.00	169
前苏联大学生数学竞赛试题及解答(下)	2012—03	38.00	170
整函数	2012—1		161
俄罗斯函数问题集	2011—03	38.00	103
俄罗斯组合分析问题集	2011—01	48.00	79
博弈论精粹	2008—03	58.00	30
多项式和无理数	2008—01	68.00	22
模糊数据统计学	2008—03	48.00	31
受控理论与解析不等式	2012—03		165
解析不等式新论	2009—06	68.00	48
反问题的计算方法及应用	2011—11	28.00	147
建立不等式的方法	2011—03	98.00	104
数学奥林匹克不等式研究	2009—08	68.00	56
不等式研究(第二辑)	2012—02	68.00	153
初等数学研究(Ⅰ)	2008—09	68.00	37
初等数学研究(Ⅱ)(上、下)	2009—05	118.00	46,47
中国初等数学研究　2009 卷(第 1 辑)	2009—05	20.00	45
中国初等数学研究　2010 卷(第 2 辑)	2010—05	30.00	68
中国初等数学研究　2011 卷(第 3 辑)	2011—07	60.00	127
数阵及其应用	2012—02	28.00	164
不等式的秘密(第一卷)	2012—02	28.00	154
初等不等式的证明方法	2010—06	38.00	123
数学奥林匹克不等式散论	2010—06	38.00	124
数学奥林匹克不等式欣赏	2011—09	38.00	138
数学奥林匹克超级题库(初中卷上)	2010—01	58.00	66
数学奥林匹克不等式证明方法和技巧(上、下)	2011—08	158.00	134,135

哈尔滨工业大学出版社刘培杰数学工作室
已出版(即将出版)图书目录

书　名	出版时间	定　价	编号
500个最新世界著名数学智力趣题	2008－06	48.00	3
400个最新世界著名数学最值问题	2008－09	48.00	36
500个世界著名数学征解问题	2009－06	48.00	52
400个中国最佳初等数学征解老问题	2010－01	48.00	60
500个俄罗斯数学经典老题	2011－01	28.00	81
数学 我爱你	2008－01	28.00	20
精神的圣徒　别样的人生——60位中国数学家成长的历程	2008－09	48.00	39
数学史概论	2009－06	78.00	50
斐波那契数列	2010－02	28.00	65
数学拼盘和斐波那契魔方	2010－07	38.00	72
斐波那契数列欣赏	2011－01	28.00	160
数学的创造	2011－02	48.00	85
数学中的美	2011－02	38.00	84
最新全国及各省市高考数学试卷解法研究及点拨评析	2009－02	38.00	41
高考数学的理论与实践	2009－08	38.00	53
中考数学专题总复习	2007－04	28.00	6
向量法巧解数学高考题	2009－08	28.00	54
新编中学数学解题方法全书(高考复习卷)	2010－01	48.00	67
新编中学数学解题方法全书(高考真题卷)	2010－01	38.00	62
新编中学数学解题方法全书(高考精华卷)	2011－03	68.00	118
高考数学核心题型解题方法与技巧	2010－01	28.00	86
数学解题——靠数学思想给力(上)	2011－07	38.00	131
数学解题——靠数学思想给力(中)	2011－07	48.00	132
数学解题——靠数学思想给力(下)	2011－07	38.00	133
2011年全国及各省市高考数学试题审题要津与解法研究	2011－10	48.00	139
新课标高考数学——五年试题分章详解(2007～2011)(上、下)	2011－10	78.00	140,141
30分钟拿下高考数学选择题、填空题	2012－01	48.00	146
高考数学压轴题解题诀窍(上)	2012－02	78.00	166
高考数学压轴题解题诀窍(下)	2012－03	28.00	167
300个日本高考数学题	2012－03		142

哈尔滨工业大学出版社刘培杰数学工作室
已出版(即将出版)图书目录

书　名	出版时间	定　价	编号
中等数学英语阅读文选	2006－12	38.00	13
统计学专业英语	2007－03	28.00	16
方程式论	2011－03	38.00	105
初级方程式论	2011－03	28.00	106
Galois 理论	2011－03	18.00	107
代数方程的根式解及伽罗瓦理论	2011－03	28.00	108
线性偏微分方程讲义	2011－03	18.00	110
N 体问题的周期解	2011－03	28.00	111
代数方程式论	2011－05	28.00	121
动力系统的不变量与函数方程	2011－07	48.00	137
基于短语评价的翻译知识获取	2012－02	48.00	168
闵嗣鹤文集	2011－03	98.00	102
吴从炘数学活动三十年(1951～1980)	2010－07	99.00	32
吴振奎高等数学解题真经(概率统计卷)	2012－01	38.00	149
吴振奎高等数学解题真经(微积分卷)	2012－01	68.00	150
吴振奎高等数学解题真经(线性代数卷)	2012－01	58.00	151
钱昌本教你快乐学数学(上)	2011－12	48.00	155

联系地址:哈尔滨市南岗区复华四道街 10 号　哈尔滨工业大学出版社刘培杰数学工作室
网　　址:http://lpj.hit.edu.cn/
邮　　编:150006
联系电话:0451－86281378　　13904613167
E-mail:lpj1378@yahoo.com.cn

◎目录

剩余系,欧拉定理,费马定理及其应用

第5章

5.1 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 $3^4=3\times3\times3\times3=81$,所以有

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

由于 $4^5=1\ 024$,所以有

$$3^{4^5}=3^{1\ 024}>10^{488}>(81)^5=(3^4)^5$$

因而

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

由于 $5^6=15\ 625,6^7=279\ 936$,所以有

$$4^{5^6}=4^{15\ 625}>10^{9\ 407},5^{6^7}=5^{279\ 936}>10^{195\ 666}$$

但是

$$(4^5)^6=(1\ 024)^6<10^{19},(5^6)^7=(15\ 625)^7<10^{30}$$

因而

$$4^{5^6}>10^{9\ 388}\times(4^5)^6,5^{6^7}>10^{195\ 636}\times(5^6)^7$$

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

$$3^{4^{5^6}} = 3^{4^{15\,625}} \geqslant 10^{10^{9\,406}}, 4^{5^{6^7}} > 10^{10^{193\,665}}$$

$$(3^{4^5})^6 = 3^{1\,024\times 6} = 3^{6\,144} \leqslant 10^{2\,932}$$

$$(4^{5^6})^7 = 4^{15\,625\times 7} = 44^{109\,375} \leqslant 10^{65\,851}$$

我们又有

$$(12\,345^{56} + 50)^{40} \leqslant (10^{230})^{40} = 10^{9\,200} \leqslant 10^{9\,407} \leqslant 4^{56}$$

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 $773^{3\,169^c}$ 天后,应该是星期四.

在本章第5.5节中将对例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 $(12\,371^{56} + 34)^{28+72c}$ 被 111 除的余数等于 70,其中 c 是任意非负整数.

在本章第5.5节中将给出例2的证明. 我们将在第6章说明欧拉定理、费马定理在研究循环小数时的作用.

5.2 完全剩余系

设 a,b 是任意两个整数,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 对模同余,记作 $a \equiv b(\bmod m)$.

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

$$a \equiv c(\bmod m)$$

证 $a - b = mq_1$,$b - c = mq_2$,其中 q_1,q_2 是两个整数,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 $ac \equiv bc(\bmod m)$ 时,有

$$a \equiv b(\bmod m)$$

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 是任意两个整数,而 m,n 是两个正整数,则当 $a \equiv b(\bmod m)$ 时,有

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

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

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

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两类,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 $n = 0, \pm 1, \pm 2, \cdots$)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

$$-10 \equiv 4(\mathrm{mod}\ 7), -6 \equiv 1(\mathrm{mod}\ 7), -1 \equiv 6(\mathrm{mod}\ 7)$$

$$2 \equiv 2(\mathrm{mod}\ 7), 10 \equiv 3(\mathrm{mod}\ 7), 12 \equiv 5(\mathrm{mod}\ 7)$$

$$14 \equiv 0(\mathrm{mod}\ 7)$$

而4,1,6,2,3,5,0和0,1,2,3,4,5,6只有在次序上有不同,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

$$6 \equiv 6(\mathrm{mod}\ 8), 9 \equiv 1(\mathrm{mod}\ 8), 12 \equiv 4(\mathrm{mod}\ 8)$$

$$15 \equiv 7(\mathrm{mod}\ 8), 18 \equiv 2(\mathrm{mod}\ 8), 21 \equiv 5(\mathrm{mod}\ 8)$$

$$24 \equiv 0(\mathrm{mod}\ 8), 27 \equiv 3(\mathrm{mod}\ 8)$$

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 $a_1,a_2,\cdots,a_m$ 中任取出两个整数,则这两个整数对模 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

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

则我们有

$$a_1 \equiv r_1(\bmod m),a_2 \equiv r_2(\bmod m),\cdots,a_m \equiv r_m(\bmod m) \tag{2}$$

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,任取出两个整数,这两个整数对模 m 是不同的,所以在 $r_1,r_2,\cdots,r_m$ 中任取出两个整数,这两个整数对模 m 是不同余的. 故由式(2)知道,在 $a_1,a_2,\cdots,a_m$ 中任取出两个整数,则这两个整数对模 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 $a_1,a_2,\cdots,a_m$ 中任取出两个整数时,这两个整数对模 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

$$a_i \equiv r_i(\bmod m),0 \leqslant r_i \leqslant m-1$$

则我们有

$$a_1 \equiv r_1(\bmod m),a_2 \equiv r_2(\bmod m),\cdots,a_m \equiv r_m(\bmod m) \tag{3}$$

其中 $0 \leqslant r_1 \leqslant m-1,0 \leqslant r_2 \leqslant m-1,\cdots,0 \leqslant r_m \leqslant m-1$. 由于式(3)和假设在 $a_1,a_2,\cdots,a_m$ 中任取出两个整数时,这两个整数对模 m 不同余,所以当我们在 $r_1,r_2,\cdots,r_m$ 中任取出两个整数时,这两个整数对模 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 $a_1+b,a_2+b,\cdots,a_m+b$ 中存在两个整数 $a_k+b,a_\lambda+b$(其中 $1 \leqslant k<\lambda \leqslant m$),使得

$$a_k+b \equiv a_\lambda+b(\bmod m) \tag{4}$$

成立. 我们又有

$$b \equiv b(\bmod m) \tag{5}$$

由式(4)减去式(5),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,知道式(4)是不可能成立的. 所以在$a_1+b,a_2+b,\cdots,a_m+b$中任取出两个整数时,这两个整数对模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$ba_1,ba_2,\cdots,ba_m$中存在两个整数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,知道式(7)是不可能成立的. 所以在$ba_1,ba_2,\cdots,ba_m$中任取出两个整数时,这两个整数对模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是两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是任意的两个整数,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$(a,m)=(b,m)$.

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

5.4 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