

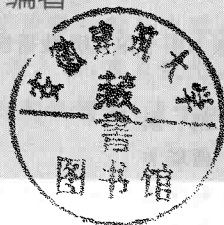
密码学及 信息安全基础

陈小松 编著

清华大学出版社

密码学及 信息安全基础

陈小松 编著



清华大学出版社
北京

内 容 简 介

全书共 5 章和 2 个附录,包含数论和代数基础知识、经典密码、对称密码、公钥密码、数字签名等信息安全知识的内容,还包括课内实验以及实验参考程序(包含用 Java、MATLAB、Maple 实现部分密码系统等)。内容安排循序渐进,由浅入深,重点突出,读者在学习每一部分密码学内容之前,就刚好学完了所需的基础知识,便于读者学习。本书可作为高等院校计算机、信息安全、网络、软件、通信等相关专业本科生以及低年级研究生的教材,也可作为与密码学及信息安全相关的工程技术人员学习的读本。

版权所有,侵权必究。侵权举报电话:010-62782989 13701121933

图书在版编目(CIP)数据

密码学及信息安全基础/陈小松编著. —北京:清华大学出版社,2018
ISBN 978-7-302-51100-7

I. ①密… II. ①陈… III. ①密码学—高等学校—教材②信息安全—安全技术—高等学校—教材 IV. ①TN918.1②TP309

中国版本图书馆 CIP 数据核字(2018)第 195624 号

责任编辑:刘颖
封面设计:傅瑞学
责任校对:赵丽敏
责任印制:丛怀宇

出版发行:清华大学出版社

网 址: <http://www.tup.com.cn>, <http://www.wqbook.com>

地 址:北京清华大学学研大厦 A 座 邮 编:100084

社总机:010-62770175 邮 购:010-62786544

投稿与读者服务:010-62776969, c-service@tup.tsinghua.edu.cn

质量反馈:010-62772015, zhiliang@tup.tsinghua.edu.cn

印 装 者:三河市国英印务有限公司

经 销:全国新华书店

开 本:170mm×240mm

印 张:12 字 数:215 千字

版 次:2018 年 9 月第 1 版

印 次:2018 年 9 月第 1 次印刷

定 价:38.00 元

产品编号:081084-01



随着信息网络的发展,互联网对信息的保密和安全的要求越来越高,信息安全建设不仅关系到个人、单位利益,更重要的是关系到国家的安全和展.很多与计算机相关的专业开设了密码学及信息安全的课程,但是所采用的大部分教材将密码学与数学内容分开,且大多只介绍数学结论,学生很难掌握密码学的思想和算法.本教材按照所需的数学基础知识结构编排,将密码学的内容融入数论和代数中,学生在学习密码学的每一部分内容之前,刚好学完了所需的基础知识.内容编排循序渐进,由浅入深,重点突出,尽可能讲清楚内容的方法和原理,以所需知识和思想方法先做铺垫,使学生更加容易理解,能够学得轻松,记得清楚.

本教材重点介绍密码学的基本思想和基本方法,包含数论和代数基础知识、经典密码、对称密码、公钥密码、数字签名等其他信息安全知识的内容,考虑到很多学校密码学和信息安全课程还包括课内实验,在第5章之后附加了课内实验内容,安排这些实验是为加深学生对算法或操作的理解和认识,也可以提高学生的应用能力和编程解决实际问题的能力.维吉尼亚密码作为经典密码的代表,第1章学完可以开始;RSA公钥作为基于大整数分解密码系统的代表,第2章第2节学完可以开始;Gamal公钥作为基于离散对数密码系统的代表,第2章学完可以开始;流密码密钥生成程序设计第4章学完可以开始;序列码生成程序设计作为认证码的一个应用,第5章第1节讲完可以开始;Windows 7自带防火墙的配置第5章第5节讲完可以开始.又考虑到不同专业学生掌握的编程语言不同,所以附加了用Java、MATLAB、Maple实现部分密码系统的实验参考程序.之所以选择这3种语言是因为:其一,Java是计算机专业最基本的编程语言;其二,MATLAB是理工科学生使用较多的编程语言;其三,Maple是实现一些算法简单高效

的编程语言,特别适合研究型读者使用.教师可以根据教学实际情况选取.很多学校密码学和信息安全课程(包括实践环节)为64学时或更少学时,为了适应这种情况,在保证教材内容完整和推导严谨的同时,结合各学校教学的实际情况,将某些内容设置为选讲内容,用星号标注.在教学时可以跳过这些内容.但是对于研究型读者来说,搞清楚这些内容,有助于理解后面的内容.本教材各章节配备了适量习题,还配备了教学课件,需要教学课件的读者可向作者索取.本教材可能会有需要改进的地方,若读者发现其中的问题,请通过邮箱与作者联系,以便在再版时加以完善.

作者

2018年6月



第 1 章 整除性、同余与经典密码	1
1.1 整数的整除性	1
1.1.1 整除的概念	1
1.1.2 最大公因数	2
习题 1.1	6
1.2 不定方程	6
1.2.1 二元一次不定方程	6
1.2.2 三元一次不定方程	8
习题 1.2	8
1.3 素数、取整函数	8
1.3.1 素数、算术基本定理	8
1.3.2 取整函数	10
习题 1.3	11
1.4 同余	11
1.4.1 同余的概念和性质	11
1.4.2 弃九法	12
习题 1.4	13
1.5 完全剩余系、简化剩余系	13
1.5.1 剩余类、完全剩余系	13
1.5.2 欧拉函数、简化剩余系	14
1.5.3 欧拉定理、费马定理	15
习题 1.5	16
1.6 经典密码	17



1.6.1	恺撒密码	17
1.6.2	仿射密码	19
1.6.3	维吉尼亚密码	20
1.6.4	费尔南密码	20
1.6.5	普莱费尔密码	21
1.6.6	希尔密码	22
1.6.7	置换密码	23
	习题 1.6	23
第 2 章	同余式、原根与公钥系统	24
2.1	背包公钥系统	24
2.1.1	背包问题	24
2.1.2	Merkle-Hellman 背包公钥算法	25
* 2.1.3	沙米尔对背包公钥的攻击	26
2.2	RSA 公钥系统	26
2.2.1	RSA 公钥的算法	26
2.2.2	对 RSA 公钥算法的分析	27
	习题 2.2	28
2.3	一次同余式、孙子定理	28
2.3.1	一次同余式求解	28
2.3.2	孙子定理	29
* 2.3.3	一般同余式的求解	30
	习题 2.3	32
2.4	二次同余式	32
2.4.1	奇素数模的二次同余式	32
2.4.2	欧拉判别条件	32
* 2.4.3	勒让德符号	34
* 2.4.4	雅可比符号	37
	习题 2.4	40
2.5	拉宾公钥系统	40
2.5.1	平方剩余的求解	40
2.5.2	拉宾公钥的算法	41
	习题 2.5	41

2.6	原根、指数及 ElGamal 公钥系统	42
2.6.1	原根与指数	42
2.6.2	ElGamal 公钥的算法	43
	习题 2.6	43
第 3 章	代数、多项式及公钥	45
3.1	映射、等价关系	45
3.1.1	映射、单射与满射	45
3.1.2	等价关系与分类	46
	习题 3.1	47
3.2	群	47
3.2.1	群的定义与性质	47
3.2.2	置换	48
3.2.3	加群、子群	49
	习题 3.2	51
3.3	环	51
3.3.1	环的定义	51
3.3.2	域	52
	习题 3.3	53
3.4	域上多项式环	53
3.4.1	域上一元多项式环	53
* 3.4.2	置换多项式及公钥	55
	习题 3.4	57
* 3.5	理想、环的同态	57
3.5.1	理想与剩余类环	57
3.5.2	环的同态映射	58
3.5.3	极大理想	59
	习题 3.5	60
3.6	有限域	60
	习题 3.6	62
第 4 章	对称密码、椭圆曲线公钥密码	63
4.1	对称密码	63
4.1.1	对称密码概述	63



4.1.2	分组密码 DES	63
	习题 4.1	71
4.2	高级加密标准 AES	71
4.2.1	AES 中的基本算法	72
4.2.2	AES 的加密过程	75
4.2.3	AES 的密钥扩展	79
4.2.4	AES 解密算法	81
4.2.5	AES 的安全性	81
	习题 4.2	81
* 4.3	中国商用密码算法 SM4	81
4.4	流密码	87
4.4.1	流密码的加密过程	87
4.4.2	密钥流产生器	88
4.4.3	RC4 算法	90
	习题 4.4	91
4.5	椭圆曲线公钥密码	91
4.5.1	椭圆曲线	91
4.5.2	ElGamal 椭圆曲线公钥算法	93
4.5.3	中国商用公钥算法 SM2	93
	习题 4.5	95
4.6	密码攻击、陷门	95
	习题 4.6	100
第 5 章	其他信息安全知识	101
5.1	消息认证与数字签名	101
5.1.1	消息认证	101
5.1.2	数字签名	106
5.1.3	生日攻击	108
5.1.4	盲签名、代理盲签名	109
5.1.5	零知识证明	111
5.1.6	数字水印	112
	习题 5.1	113
* 5.2	校正码	114

5.2.1	信息码与检定码	114
5.2.2	Hamming 距离与离散度	115
5.2.3	校正码的检定码	117
5.2.4	线性码	117
5.2.5	循环码与 BCH 码	120
	习题 5.2	122
5.3	秘密共享	122
	习题 5.3	124
5.4	公钥基础设施	124
5.4.1	PKI 基础设施	124
5.4.2	密码算法	125
5.4.3	PKI 组成	125
	习题 5.4	127
5.5	访问控制	128
5.5.1	身份认证	128
5.5.2	授权	130
5.5.3	防火墙	131
5.6	协议	132
5.7	病毒和木马	134
附录 A	课程实验	136
A.1	实验 1 维吉尼亚密码的实现	136
A.2	实验 2 RSA 公钥密码的实现	138
A.3	实验 3 ElGamal 公钥密码的实现	139
A.4	实验 4 流密码密钥生成程序设计	141
A.5	实验 5 序列码生成程序设计	141
A.6	实验 6 Windows 7 自带防火墙的配置	142
附录 B	实验参考程序	146
B.1	维吉尼亚密码加密 Java 程序	146
B.2	维吉尼亚密码加密 MATLAB 程序	149
B.3	RSA 公钥密钥生成 Java 程序	153
B.4	RSA 公钥加密 Java 程序	157
B.5	RSA 公钥解密 Java 程序	160



B. 6	RSA 公钥密钥生成 MATLAB 程序	163
B. 7	RSA 公钥加密 MATLAB 程序	164
B. 8	RSA 公钥解密 MATLAB 程序	165
B. 9	RSA 公钥密钥生成 Maple 程序	166
B. 10	RSA 公钥加密 Maple 程序	166
B. 11	RSA 公钥解密 Maple 程序	167
B. 12	ElGamal 公钥密钥生成 Maple 程序	167
B. 13	ElGamal 公钥加密 Maple 程序	167
B. 14	ElGamal 公钥解密 Maple 程序	168
B. 15	ElGamal 公钥密钥生成 MATLAB 程序	168
B. 16	ElGamal 公钥加密 MATLAB 程序	170
B. 17	ElGamal 公钥解密 MATLAB 程序	170
B. 18	序列码生成 Java 程序	171
B. 19	序列码生成 MATLAB 程序	175
参考文献		181

第 1 章

整除性、同余与经典密码

1.1 整数的整除性

1.1.1 整除的概念

本书中,用 $\mathbf{N}=\{0,1,2,3,\dots\}$ 表示自然数的集合, $\mathbf{Z}^+=\{1,2,3,\dots\}$ 表示正整数的集合, $\mathbf{Z}=\{\dots,-2,-1,0,1,2,\dots\}$ 表示全体整数的集合.

两个整数相加、相减、相乘的结果仍然是整数,但是两个整数相除却不一定是整数.

定义 1.1 设 $a, b \in \mathbf{Z}, b \neq 0$, 若 $\frac{a}{b} \in \mathbf{Z}$, 则说 b 整除 a , 记作 $b|a$, 也说 b 是 a 的因数或 a 是 b 的倍数; 若 $\frac{a}{b} \notin \mathbf{Z}$, 则说 b 不能整除 a .

为了使表达简洁, 用 \forall 表示“对于一切”, 用 \Rightarrow 表示“蕴含”, \Leftrightarrow 表示“当且仅当”.

定理 1.1 $b|a \Leftrightarrow$ 存在 $q \in \mathbf{Z}$, 使得 $a=bq (b \neq 0)$.

证 若 $b|a$, $\frac{a}{b}=q \in \mathbf{Z}$, 即 $a=bq (b \neq 0)$; 反过来, 若 $a=bq (b \neq 0)$, 两边同除以 b , 则得 $\frac{a}{b}=q \in \mathbf{Z}$.

当 $q \neq \pm 1, \pm a$ 时, 则说 b 是 a 的真因数.

整除有以下基本性质.

定理 1.2 (1) $c|b, b|a \Rightarrow c|a$.

(2) $d|a, d|b \Rightarrow \forall p, q \in \mathbf{Z}, d|(pa+qb)$.

(3) $b|a, a \neq 0 \Rightarrow |b| \leq |a|$.

(4) $b|a, c \neq 0 \Leftrightarrow cb|ca$.

证 (1) $c|b, b|a \Rightarrow b=cs, a=bt \Rightarrow a=(cs)t=c(st) \Rightarrow c|a$.

$$(2) a=ds, b=dt, pa+qb=dps+dqt=d(ps+qt)\Rightarrow d|(pa+qb).$$

$$(3) a=bc\Rightarrow |a|=|b||c|, a\neq 0\Rightarrow |a|\neq 0. \text{ 又 } |c|\geq 1\Rightarrow |b|\leq |a|.$$

$$(4) a=bs\Rightarrow ca=cbs\Rightarrow cb|ca.$$

例 1.1 k 个连续整数的乘积能被 $k!$ 整除.

证 考查 $n(n-1)\cdots(n-k+1)$.

(1) 若 $(n-k+1)>0$, 则

$$C_n^k = \frac{n(n-1)\cdots(n-k+1)}{k!} \in \mathbf{Z} \Rightarrow k! | n(n-1)\cdots(n-k+1).$$

(2) 若 $n(n-1)\cdots(n-k+1)=0$, 则 $k!|0$.

(3) 若 $n<0$, 则 $-n=n'>0$. 令 $n=-n'$, 则 $n(n-1)\cdots(n-k+1)=(-n')(-n'-1)\cdots(-n'-k+1)=(-1)^k n'(n'+1)\cdots(n'+k-1)$, 归结为第一种情况.

因此, $k!|n'(n'+1)\cdots(n'+k-1)$, 所以, $k!|(-1)^k n'(n'+1)\cdots(n'+k-1)$, 即 $k!|n(n-1)\cdots(n-k+1)$.

例 1.2 证明 对于任何正整数 $n, 6|n(n+1)(2n+1)$.

$$\begin{aligned} \text{证} \quad n(n+1)(2n+1) &= n(n+1)(n-1+n+2) \\ &= (n-1)n(n+1)+n(n+1)(n+2), \end{aligned}$$

由例 1.1,

$$3!|(n-1)n(n+1), \quad 3!|n(n+1)(n+2),$$

因此, $6|n(n+1)(2n+1)$.

定理 1.3(带余除法) 设 $a, b \in \mathbf{Z}, b>0$, 则存在唯一的 q, r , 使得

$$a=bq+r, \quad 0\leq r<b.$$

证 作数列 $\cdots, -2b, -b, 0, b, 2b, \cdots$, 则 a 必落在某一区间且只能落在一个区间, 即存在 q , 使

$qb\leq a<(q+1)b\Rightarrow 0\leq a-qb<b$. 令 $r=a-qb$, 则有 $a=qb+r, 0\leq r<b$. 由于只能在一个区间, 所以 q 唯一, 从而 r 唯一.

1.1.2 最大公因数

定义 1.2 设 $a, b \in \mathbf{Z}, a, b$ 不全为 0, 如果 $d|a$ 且 $d|b$, 则称 d 为 a 和 b 的公因数. 而把 a 和 b 的所有公因数中最大的称为 a 和 b 的最大公因数, 记为 (a, b) 或 $\gcd(a, b)$.

最大公因数的概念可以推广到多个, 即 n 个不全为 0 的整数 a_1, a_2, \cdots, a_n 的所有公因数中最大的称为 a_1, a_2, \cdots, a_n 的最大公因数, 记为 (a_1, a_2, \cdots, a_n) , 或

$\gcd(a_1, a_2, \dots, a_n)$.

定理 1.4 $(a, b) = (|a|, |b|)$.

证 $d|a, d|b \Leftrightarrow d||a|, d||b|$, 即 a, b 的公因数集与 $|a|, |b|$ 的公因数集相同, 因此最大的也就相同.

定理 1.4 表明, 求两个整数的最大公因数归结为求两个正整数的最大公因数, 故求 a 的公因数时, 若 a 是负数, 则可以去掉 a 的负号.

定理 1.5 如果 $a = bq + c$, 则 $(a, b) = (b, c)$.

证 若 $d|a, d|b \Rightarrow d|b, d|(a - bq)$, 即 $d|c$; 反过来, 若 $d|b, d|c \Rightarrow d|b, d|(bq + c)$, 即 $d|a$. 这表明 a, b 的公因数集与 b, c 的公因数集相同, 最大的也就相同.

例 1.3 $c|(a+b)$, 则 $(a, c) = (b, c)$.

证 $a+b=cs \Rightarrow a=cs-b$, 由定理 1.4、定理 1.5, $(a, c) = (b, c)$.

求两个正整数的最大公因数的方法称为辗转相除法, 又称为欧几里得除法.

定理 1.6 设 $a, b \in \mathbf{Z}^+$, 反复用带余除法, 即用每次的余数为除数去除上一一次的除数, 直到余数为 0, 可得

$$\begin{aligned} a &= bq_1 + r_1, & 0 < r_1 < b, \\ b &= r_1q_2 + r_2, & 0 < r_2 < r_1, \\ r_1 &= r_2q_3 + r_3, & 0 < r_3 < r_2, \\ &\vdots \\ r_{n-2} &= r_{n-1}q_n + r_n, & 0 < r_n < r_{n-1}, \\ r_{n-1} &= r_nq_{n+1} + r_{n+1}, & r_{n+1} = 0. \end{aligned}$$

最后一个不为 0 的余数 r_n 就是 a 和 b 的最大公因数.

证 由定理 1.5

$$(a, b) = (b, r_1) = (r_1, r_2) = \dots = (r_{n-1}, r_n) = (r_n, r_{n+1}) = (r_n, 0) = r_n.$$

例 1.4 求 $(525, 231)$.

解 将 525 和 231 辗转相除, 得

$$\begin{aligned} 525 &= 2 \times 231 + 63, \\ 231 &= 3 \times 63 + 42, \\ 63 &= 1 \times 42 + 21, \\ 42 &= 2 \times 21 + 0. \end{aligned}$$

这个过程可以按如下竖式计算出来:

2	525	231	3
	462	189	
1	63	42	2
	42	42	
	21	0	

所以 $(525, 231) = 21$.

定理 1.7 a, b 的公因数集与 (a, b) 的因数集合相同.

证 设 d 是 a, b 的公因数, 即 $d|a, d|b$, 则由辗转相除法的过程, 得 $d|r_n = (a, b)$, 即 a, b 的公因数是 (a, b) 的因数; 反过来, 设 d 是 (a, b) 的因数, 则 $d|(a, b)$. 而 $(a, b)|a, (a, b)|b$, 于是 $d|a, d|b$, 即 (a, b) 的因数是 a, b 的公因数.

推论 1.1 $\forall k \in \mathbf{Z}, (a, b) = (a, b+ka)$.

证 $(a, b)|a, (a, b)|b$, 由定理 1.5 $\Rightarrow (a, b)|(b+ka)$, 从而 $(a, b)|(a, b+ka)$; 令 $d = (a, b+ka)$, 则 $d|a, d|ka+b \Rightarrow d|(b+ka) - ka$, 即 $d|b \Rightarrow d|(a, b)$.

将推论 1.1 用于例 1.4, 有 $(525, 231) = (525 + (-2) \cdot 231, 231) = (63, 231) = (63, (-4) \cdot 63 + 231) = (63, 21) = 21$.

《九章算术》中的更相减损术, 相当于 $a > b > 0, k = -1$ 的情况下的推论 1.1.

引理 1.1 设 $a, b \in \mathbf{Z}, q_i$ 由辗转相除法得到, 则

$Q_k a - P_k b = (-1)^{k-1} r_k$, 这里

$$P_0 = 1, \quad P_1 = q_1, \quad P_k = q_k P_{k-1} + P_{k-2},$$

$$Q_0 = 0, \quad Q_1 = 1, \quad Q_k = q_k Q_{k-1} + Q_{k-2}, \quad k = 2, 3, \dots, n.$$

证 对 k 用数学归纳法. 当 $k=1$ 时, $Q_1 a - P_1 b = a - q_1 b = r_1$, 结论成立;

当 $k=2$ 时, $Q_2 a - P_2 b = a(q_2 Q_1 + Q_0) - (q_2 P_1 + P_0) b = -r_2$.

假定对于小于 k 结论成立, 则

$$\begin{aligned} Q_k a - P_k b &= (q_k Q_{k-1} + Q_{k-2}) a - (q_k P_{k-1} + P_{k-2}) b \\ &= q_k (Q_{k-1} a - P_{k-1} b) + Q_{k-2} a - P_{k-2} b \\ &= q_k (-1)^{k-2} r_{k-1} + (-1)^{k-3} r_{k-2} = (-1)^{k-2} (q_k r_{k-1} - r_{k-2}) \\ &= (-1)^{k-2} (q_k r_{k-1} - (r_{k-1} q_k + r_k)) \\ &= (-1)^{k-2} (-r_k) = (-1)^{k-1} r_k, \end{aligned}$$

即结论对于 k 成立.

定理 1.8 $ax + by = (a, b), a > 0, b > 0$ 的一个解为

$$x_0 = (-1)^{n-1} Q_n, \quad y_0 = (-1)^n P_n.$$

证 在引理 1.1 中取 $k=n$, 即得.

推论 1.2 设 a, b 不全为 0, $a, b \in \mathbf{Z}$, 则存在 $x, y \in \mathbf{Z}$, 使 $(a, b) = xa + yb$.

证 不妨设 $a \neq 0$. 若 x, y 满足 $|a|x + by = (a, b)$, 当 $a < 0$ 时, $-x, y$ 满足 $ax + by = (a, b)$.

定义 1.3 如果整数 a 与整数 b 的最大公因数为 1, 则称 a 与 b 互素, 记为 $(a, b) = 1$.

互素的概念可以推广到多个,即若 n 个整数 a_1, a_2, \dots, a_n 的最大公因数为 1, 则称 a_1, a_2, \dots, a_n 互素, 记为 $(a_1, a_2, \dots, a_n) = 1$.

如果 a_1, a_2, \dots, a_n 中任意两个都互素, 则称 a_1, a_2, \dots, a_n 两两互素.

例如 2, 3, 6 互素, 2, 3 互素, 但 2, 6 不互素, 所以 2, 3, 6 不是两两互素.

推论 1.3 $(a, b) = 1 \Leftrightarrow$ 存在 $s, t \in \mathbf{Z}$, 使得 $sa + tb = 1$.

证 “ \Rightarrow ” $(a, b) = 1$, 由推论 1.2 直接得出;

“ \Leftarrow ”若有 $s, t \in \mathbf{Z}$, 使 $sa + tb = 1$, 若 $d|a, d|b$, 则 $d|(sa + tb) = 1$, 即 $(a, b) = 1$.

定理 1.9 设 $a, b \in \mathbf{Z}$, a, b 不全为 0, 则 $\forall m \in \mathbf{Z}^+$, 有 $(ma, mb) = m(a, b)$.

证 将辗转相除法的等式乘以 m , 有

$$\begin{aligned} am &= bmq_1 + r_1m, & 0 < r_1m < bm, \\ bm &= r_1mq_2 + r_2m, & 0 < r_2m < r_1m, \\ r_1m &= r_2mq_3 + r_3m, & 0 < r_3m < r_2m, \\ & \vdots \\ r_{n-2}m &= r_{n-1}mq_n + r_nm, & 0 < r_nm < r_{n-1}m, \\ r_{n-1}m &= r_nmq_{n+1} + r_{n+1}m, & r_{n+1}m = 0, \end{aligned}$$

所以 $(am, bm) = r_nm = (a, b)m$.

定理 1.10 $a, b, c \in \mathbf{Z}$, b, c 不全为 0, 且 $(a, c) = 1$, 则 $(ab, c) = (b, c)$.

证 $(a, c) = 1$, 故存在 $s, t \in \mathbf{Z}$, 使得 $sa + tc = 1$, 两边乘以 b , 得 $s(ab) + tbc = b$. 若 $d|ab, d|c$, 则 $d|b$. 反之, 若 $d|b, d|c$, 则 $d|ab$, 故 ab, c 与 b, c 有相同的公因数, 由有限数集的最大数唯一, 得 $(ab, c) = (b, c)$.

推论 1.4 若 $(a, c) = 1, (b, c) = 1$, 则 $(ab, c) = 1$.

推论 1.5 若 $c|ab, (a, c) = 1$, 则 $c|b$.

证 $c|ab, |c| = (c, ab) = (c, b)$, 由定理 1.10, 得 $c|b$.

定义 1.4 设 $a|m, b|m$, 则说 m 是 a, b 的一个公倍数, 最小的正公倍数称为最小公倍数, 记作 $[a, b]$ 或 $\text{lcm}(a, b)$.

定理 1.11 设 $a, b \in \mathbf{Z}^+$, 则 $[a, b] = \frac{ab}{(a, b)}$.

证 设 $a|m, b|m \Rightarrow m = ak = bs$. 令 $a = (a, b)a_1, b = (a, b)b_1$, 则

$$m = (a, b)a_1k = (a, b)b_1s \Rightarrow a_1k = b_1s, \quad (a_1, b_1) = \left(\frac{a}{(a, b)}, \frac{b}{(a, b)} \right) = 1,$$

$$b_1|k, \text{ 即 } k = b_1t \Rightarrow m = (a, b)a_1b_1t = \frac{ab}{(a, b)}t,$$

$t=1$ 时最小, 即 $[a, b] = \frac{ab}{(a, b)}$.

例如, $a=18=2 \times 3^2$, $b=12=2^2 \times 3$, $(a,b)=6$, $[a,b]=\frac{ab}{(a,b)}=\frac{18 \times 12}{(18,12)}=36$.

习题 1.1

1. 对任意整数 n , 证明 $30 \mid n^5 - n$.

2. 求 $(39, 63)$.

3. 设 $a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$ 是一个整系数多项式, 则它的有理根 $\frac{p}{q}$ 一定满足 $p \mid a_0, q \mid a_n$, 从而证明 $\sqrt{2}$ 不是有理数.

1.2 不定方程

1.2.1 二元一次不定方程

公元 5 世纪《张丘建算经》里, 有一道百鸡问题:

鸡翁一, 值钱五,

鸡母一, 值钱三,

鸡雏三, 值钱一,

百钱买百鸡,

问鸡翁、鸡母、鸡雏各几何?

设买公鸡 x 只, 买母鸡 y 只, 买小鸡 z 只, 那么

$$\begin{cases} x+y+z=100, & (1-1) \end{cases}$$

$$\begin{cases} 5x+3y+z/3=100. & (1-2) \end{cases}$$

$(1-2) \times 3 - (1-1)$, 得 $14x+8y=200$, 即

$$7x+4y=100.$$

设 a, b, c 是整数,

$$ax+by=c \quad (1-3)$$

称为二元一次不定方程. 适合方程(1-3)的整数 x, y 称为该不定方程解.

并不是所有二元一次方程都有解, 例如方程 $4x+12y=15$ 无解, 因为对任意整数 x, y , $4x+12y$ 永远是偶数.

定理 1.12 设 $ab \neq 0$, 则 $ax+by=c$ 有解 $\Leftrightarrow (a,b) \mid c$.

证 “ \Rightarrow ”若方程(1-3)有解 x, y , 即 $ax+by=c$, 则 $(a,b) \mid a, (a,b) \mid b$, 因此