高等学校信息安全系列教材

简明信息安全数学基础

陈恭亮

高等教育出版社
HIGHER EDUCATION PRESS

高等学校信息安全系列教材

简明信息安全数学基础

Jianming Xinxi Anquan Shuxue Jichu

陈恭亮

高等教育出版社·北京
HIGHER EDUCATION PRESS BEIJING

内容简介

本书简明而系统地介绍了信息安全所涉及的数论、代数和椭圆曲线论等基本数学理论和方法，以及它们在信息安全实践中的应用。

本书可作为信息安全、通信、计算机和应用数学等专业的本科生、专科生的教科书，也可作为信息专业技术人才知识更新培训课程的教科书，还可作为信息安全从业人员的参考书。

图书在版编目(CIP)数据

简明信息安全数学基础／陈恭亮编著. —北京：高等教育出版社，2011.1

ISBN 978-7-04-031181-5

Ⅰ. ①简… Ⅱ. ①陈… Ⅲ. ①信息安全-应用数学-高等学校-教材 Ⅳ. ①TP309

中国版本图书馆 CIP 数据核字(2010)第 251382 号

策划编辑	武林晓	**责任编辑**	廖肇源	**封面设计**	于文燕
责任绘图	黄建英	**版式设计**	张　岚	**责任校对**	陈旭颖
责任印制	毛斯璐				

出版发行	高等教育出版社	**购书热线**	010-58581118
社　　址	北京市西城区德外大街 4 号	**咨询电话**	800-810-0598
邮政编码	100120	**网　　址**	http://www.hep.edu.cn
			http://www.hep.com.cn
经　　销	蓝色畅想图书发行有限公司	**网上订购**	http://www.landraco.com
印　　刷	国防工业出版社印刷厂		http://www.landraco.com.cn
		畅想教育	http://www.widedu.com
开　　本	787×1092　1/16	**版　　次**	2011 年 1 月第 1 版
印　　张	15.75	**印　　次**	2011 年 1 月第 1 次印刷
字　　数	350 000	**定　　价**	24.00 元

本书如有缺页、倒页、脱页等质量问题，请到所购图书销售部门联系调换。

物料号　31181-00

前　言

信息安全学科是一门新兴的学科，它涉及通信学、计算机科学、信息学和数学等多个学科，其中公钥密码学所基于的三个难解数学问题是：

1. 大整数因数分解问题；

2. 离散对数问题；

3. 椭圆曲线离散对数问题。

这些问题涉及数论、代数和椭圆曲线论等。但应用于信息安全的数学理论和知识只是这些数学理论中的一小部分，而有关数论、代数和椭圆曲线论等方面的书籍多半是针对数学专业的学生。此外，在信息安全研究和应用中所产生的一些新的数学成果也没有在数论、代数和椭圆曲线论等教科书中体现。

信息安全的从业人员需要学习和掌握数论、代数和椭圆曲线论中的一些数学理论和方法，并将它们应用于信息安全的工程实践，跟上信息安全和密码学的最新进展，提高创新能力并做出创新工作。

作者于 2007 年参与上海市信息专业技术人才知识更新培训课程开发项目，深入了解到一些信息技术人员和信息管理人员对信息安全数学基础这类教材的迫切需求：会运用数学语言和方法，通过具体的案例和应用，阐述信息安全的数学理论和方法。

本教材主要特色如下：

1. 基础性　对关于信息安全的重要数学理论和方法以及算法，给出详细的推理过程和说明；

2. 实用性　对信息化建设可能遇到的关于信息安全的数学基础知识，以具体的案例作出简明阐述；

3. 系统性　运用统一的数学语言和符号，形成三大难解数学问题的知识体系。

基于理论和方法的系统性和完整性，同时为方便读者进一步学习，本教材除强调理论和方法的应用性外，还特别注意与《信息安全数学基础》(陈恭亮编著，清华大学出版社，2004 年) 的知识点相对应。

承蒙高等教育出版社武林晓编辑的邀请和支持，决定编写这本《简明信息安全数学基础》教材。本书在编写过程中得到了上海市信息专业技术人才知识更新培训课程开发项目和上海交

通大学信息安全工程学院上海市精品课程“信息安全数学基础”教学团队的大力支持,在此表示衷心感谢。此外,特别感谢李建华教授、蒋兴浩、孟魁、张爱新、李银、龚洁中、田芸等教师及本科生和研究生所给予的许多具体帮助。

陈恭亮

2010 年 2 月

目　录

第 1 章　整数的可除性

信息技术的广泛应用需要信息的数字化. 在保证信息的安全性和有效性 (如 RSA 公钥密码系统) 时往往要用到整数的算术性质, 特别是 RSA 公钥密码系统基于大整数因数分解的困难性, 所以我们在本章讨论整数的算术性质.

§1.1　整除的概念

在本节中, 我们讨论整除的基本概念和性质.

我们首先考虑具有一般意义的整除定义, 它只涉及乘法运算.

定义 1.1.1　设 a, b 是任意两个整数, 其中 $b \neq 0$. 如果存在一个整数 q 使得等式

$$a = qb \tag{1.1}$$

成立, 就称 b **整除** a 或者 a 被 b 整除, 记作 $b|a$, 并把 b 叫做 a 的**因数**, 把 a 叫做 b 的**倍数**. 这时, q 也是 a 的因数, 我们常常将 q 写成 a/b 或 $\frac{a}{b}$. 否则, 就称 b 不能整除 a 或者 a 不能被 b 整除, 记作 $b \nmid a$.

注 1　这里整除的定义只涉及乘法运算, 并通过整数 q 的存在性来表述整除性.

注 2　1) 当 b 遍历整数 a 的所有因数时, $-b$ 也遍历整数 a 的所有因数;

2) 当 b 遍历整数 a 的所有因数时, a/b 也遍历整数 a 的所有因数.

例 1.1.1　$30 = 15 \cdot 2 = 10 \cdot 3 = 6 \cdot 5$.

显然 2, 3, 5 分别整除 30 或 30 分别被 2, 3, 5 整除, 记作 2|30, 3|30, 5|30. 这时, 2, 3, 5 都是 30 的因数, 30 是 2, 3, 5 的倍数.

30 的所有因数是 ± 1, ± 2, ± 3, ± 5, ± 6, ± 10, ± 15, ± 30, 或是 ∓ 1, ∓ 2, ∓ 3, ∓ 5, ∓ 6, ∓ 10, ∓ 15, ∓ 30, 或是 $\pm 30 = 30/\pm 1$, $\pm 15 = 30/\pm 2$, $\pm 10 = 30/\pm 3$, $\pm 6 = 30/\pm 5$, $\pm 5 = 30/\pm 6$, $\pm 3 = 30/\pm 10$, $\pm 2 = 30/\pm 15$, $\pm 1 = 30/\pm 30$. 列表就是

d	±1	±2	±3	±5	±6	±10	±15	±30
$-d$	∓1	∓2	∓3	∓5	∓6	∓10	∓15	∓30
$30/d$	±30	±15	±10	±6	±5	±3	±2	±1

又例如: $7|84,\ -7|84,\ 5|20,\ 19|171,\ 3 \nmid 8,\ 5 \nmid 12,\ 13|0,\ 11|11.$

根据定义, 我们有:

0 是任何非零整数的倍数;

1 是任何整数的因数;

任何非零整数 a 是其自身的倍数, 也是其自身的因数.

例 1.1.2 *设 a, b 为整数. 若 $b|a$, 则 $b \mid (-a)$, $(-b)|a$, $(-b)|(-a)$.*

证 设 $b|a$, 则存在整数 q 使得 $a = qb$. 因而

$$(-a) = (-q)b, \quad a = (-q)(-b), \quad (-a) = q(-b).$$

因为 $-q$, q 都是整数, 所以根据整除的定义, 我们有

$$b \mid (-a), \quad (-b)|a, \quad (-b)|(-a).$$ 证毕.

整除具有传递性, 即

定理 1.1.1 *设 a, $b \neq 0$, $c \neq 0$ 是三个整数. 若 $b|a$, $c|b$, 则 $c|a$.*

证 设 $b|a$, $c|b$, 根据整除的定义, 分别存在整数 q_1, q_2 使得

$$a = q_1 b, \quad b = q_2 c.$$

因此, 我们有

$$a = q_1 b = q_1(q_2 c) = qc.$$

其中 $q = q_1 q_2$ 是整数, 根据整除的定义, 有 $c|a$. 证毕.

例 1.1.3 *因为 $7|42$, $42|84$, 所以 $7|84$.*

在加法、减法运算中, 整除的性质是保持的.

定理 1.1.2 *设 a, b, $c \neq 0$ 是三个整数. 若 $c|a$, $c|b$, 则 $c|a \pm b$.*

证 设 $c|a$, $c|b$, 那么分别存在整数 q_1, q_2 使得

$$a = q_1 c, \quad b = q_2 c.$$

因此

$$a \pm b = q_1 c \pm q_2 c = (q_1 \pm q_2)c.$$

因为 $q_1 \pm q_2$ 是整数, 所以 $a \pm b$ 被 c 整除. 证毕.

例 1.1.4 因为 $7|14$, $7|84$, 所以

$$7|(84 + 14) = 98, \quad 7|(84 - 14) = 70.$$

进一步, 在整数 a, b 的线性组合中, 整除的性质是保持的.

定理 1.1.3 设 a, b, $c \neq 0$ 是三个整数. 若 $c|a$, $c|b$, 则对任意整数 s, t, 有 $c|sa + tb$.

证 设 $c|a$, $c|b$, 那么分别存在整数 q_1, q_2 使得

$$a = q_1 c, \quad b = q_2 c.$$

因此

$$sa + tb = s(q_1 c) + t(q_2 c) = (sq_1 + tq_2)c.$$

因为 $sq_1 + tq_2$ 是整数, 所以 $sa + tb$ 被 c 整除. 证毕.

例 1.1.5 因为 $7|14$, $7|21$, 所以

$$7|(3 \cdot 21 - 4 \cdot 14) = 7, \quad 7|(3 \cdot 21 + 4 \cdot 14) = 119.$$

例 1.1.6 设 a, b, $c \neq 0$ 是三个整数, $c|a$, $c|b$. 如果存在整数 s, t, 使得 $sa + tb = 1$, 则 $c = \pm 1$.

证 设 $c|a$, $c|b$, 因为存在整数 s, t, 使得 $sa + tb = 1$, 根据定理 1.1.3, 我们有

$$c|sa + tb = 1.$$

因此 $c = \pm 1$. 证毕.

前面我们考虑了整除和因数, 现在考虑对于乘法的最小整数, 也就是不能继续分解的整数 (± 1 除外).

定义 1.1.2 设整数 $n \neq 0$, ± 1. 如果除了显然因数 ± 1 和 $\pm n$ 外, n 没有其他因数, 那么 n 叫做**素数** (或**质数**、**不可约数**), 否则 n 叫做**合数**.

当整数 $n \neq 0,\ \pm 1$ 时, n 和 $-n$ 同为素数或合数. 因此, 若没有特别声明, **素数总是指正整数**, 通常写成 p.

奇素数 p 叫做 **安全素数**, 如果 $(p-1)/2$ 也是素数. 例如 $p=23$, $p=47$. 安全素数应用于 §3.3 的 RSA 密码系统中.

例 1.1.7 *整数 2, 3, 5, 7 都是素数; 而整数 4, 6, 10, 15, 21 都是合数.*

下面我们要证明每个合数必有素因数.

定理 1.1.4 *设 n 是一个正合数, p 是 n 的一个大于 1 的最小正因数, 则 p 一定是素数, 且 $p \leqslant \sqrt{n}$.*

证 反证法. 如果 p 不是素数, 则存在整数 q, $1 < q < p$, 使得 $q|p$. 但 $p|n$, 根据定理 1.1.1, 我们有 $q|n$. 这与 p 是 n 的大于 1 的最小正因数矛盾. 所以 p 是素数.

因为 n 是合数, 所以存在整数 n_1 使得

$$n = n_1 p, \quad 1 < p \leqslant n_1 < n.$$

因此, $p^2 \leqslant n$. 故 $p \leqslant \sqrt{n}$. 证毕.

注 定理 1.1.4 告诉我们, 素数为乘法的最小单元.

下面证明素数有无穷多个.

定理 1.1.5 *素数有无穷多个.*

证 反证法. 假设只有有限个素数, 并设它们为 $p_1,\ p_2,\ \cdots,\ p_k$. 考虑整数

$$n = p_1 \cdot p_2 \cdots p_k + 1.$$

因为 $n > p_i, \quad i = 1, \cdots, k$, 所以 n 一定是合数. 根据定理 1.1.4, n 的大于 1 的最小正因数 p 是素数. 因此, p 是 $p_1,\ p_2,\ \cdots,\ p_k$ 中的某一个, 即存在 j, $1 \leqslant j \leqslant k$, 使得 $p = p_j$. 根据定理 1.1.3, 我们有

$$p \,|\, n - (p_1 \cdots p_{j-1} \cdot p_{j+1} \cdots p_k) \cdot p_j = 1.$$

这是不可能的. 故存在无穷多个素数. 证毕.

用上述方法可证明形为 $4k+3$ 的素数有无穷多个, 也可证明形为 $6k+5$ 的素数有无穷多个. 但无法证明形为 $4k+1$ 的素数有无穷多个.

§1.2 Euclid 除法

本节考虑任意两个整数之间的关系, 我们引进 Euclid 除法或带余数除法.

定理 1.2.1 (Euclid 除法) 设 a, b 是两个整数, 其中 $b>0$, 则存在唯一的整数 q, r 使得

$$a=qb+r, \quad 0\leqslant r<b. \tag{2.1}$$

证 (存在性) 考虑一个整数序列

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

它们将实数轴分成长度为 b 的一系列区间, 而 a 必定落在其中的一个区间上. 因此存在一个整数 q 使得

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

令 $r=a-qb$, 则有

$$a=qb+r, \quad 0\leqslant r<b.$$

(唯一性) 如果分别有整数 q, r 和 q_1, r_1 满足 (2.1) 式, 则

$$\begin{aligned} a &= qb+r, & 0\leqslant r<b,\\ a &= q_1b+r_1, & 0\leqslant r_1<b. \end{aligned}$$

两式相减, 有

$$(q-q_1)b=-(r-r_1).$$

当 $q\neq q_1$ 时, 左边的绝对值 $\geqslant b$, 而右边的绝对值 $<b$, 这是不可能的. 故 $q=q_1$, $r=r_1$.

证毕.

定义 1.2.1 (2.1) 式中的 q 叫做 a 被 b 除所得的**不完全商**, r 叫做 a 被 b 除所得的**余数**.

推论 在定理 1.2.1 的条件下, $b\mid a$ 的充要条件是 a 被 b 除所得的余数 $r=0$.

注 此推论表明: 通过有效运算, 可以判断整数 a 能否被非零整数 b 整除.

为了更好地描述不完全商和余数, 方便今后表述一些数学概念和问题, 我们引进一个数学符号.

定义 1.2.2 设 x 是一个实数, 称小于或等于 x 的最大整数为 x 的整数部分, 记成 $[x]$. 这时, 我们有

$$[x]\leqslant x<[x]+1.$$

注 定理 1.2.1 中的不完全商q 可写为 $q=\left[\dfrac{a}{b}\right]$, 余数 r 可写为 $r=a-qb=a-\left[\dfrac{a}{b}\right]b$. 事实上, 我们也是先计算不完全商 $q=\left[\dfrac{a}{b}\right]$, 再计算余数 $r=a-qb=a-\left[\dfrac{a}{b}\right]b$.

例 1.2.1 $[3.14]=3,\ [-3.14]=-4,\ [3]=3,\ [-3]=-3.$

例 1.2.2 设 $b=15$.

当 $a=255$ 时,

$$a=17b+0,\quad q=\left[\frac{255}{15}\right]=17,\ r=255-17\cdot 15=0<15;$$

当 $a=417$ 时,

$$a=27b+12,\quad q=\left[\frac{417}{15}\right]=27,\ 0<r=417-27\cdot 15=12<15;$$

当 $a=-81$ 时,

$$a=-6b+9,\quad q=\left[\frac{-81}{15}\right]=-6,\ 0<r=-81-(-6)\cdot 15=9<15.$$

实际运用 Euclid 除法时, 我们可以根据需要将余数取成其他形式.

定理 1.2.2 (Euclid 除法) 设 a, b 是两个整数, 其中 $b>0$, 则对任意的整数 c, 存在唯一的整数 q, r 使得

$$a=qb+r,\quad c\leqslant r<b+c. \tag{2.2}$$

证 (存在性) 考虑一个整数序列

$$\cdots,\ -3b+c,\ -2b+c,\ -b+c,\ c,\ b+c,\ 2b+c,\ 3b+c,\ \cdots,$$

它们将实数轴分成长度为 b 的一系列区间, 而 a 必定落在其中的一个区间上. 因此存在一个整数 q 使得

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

令 $r=a-qb$, 则有

$$a=qb+r,\quad c\leqslant r<b+c.$$

(唯一性) 如果分别有整数 q, r 和 q_1, r_1 满足 (2.2) 式, 则

$$\begin{aligned} a&=qb+r,\quad c\leqslant r<b+c,\\ a&=q_1b+r_1,\quad c\leqslant r_1<b+c. \end{aligned}$$

两式相减, 有

$$(q-q_1)b=-(r-r_1).$$

当 $q\neq q_1$ 时, 左边的绝对值 $\geqslant b$, 而右边的绝对值 $<b$, 这是不可能的. 故 $q=q_1$, $r=r_1$. 证毕.

注 实际运用 Euclid 除法时, 常采用如下形式的余数:

1. 当 $c=0$ 时, 有 $0\leqslant r<b$. 这时 r 叫做**最小非负余数**.
2. 当 $c=1$ 时, 有 $1\leqslant r\leqslant b$. 这时 r 叫做**最小正余数**.
3. 当 $c=-b+1$ 时, 有 $-b+1\leqslant r\leqslant 0$. 这时 r 叫做**最大非正余数**.
4. 当 $c=-b$ 时, 有 $-b\leqslant r<0$. 这时 r 叫做**最大负余数**.
5. i) 当 $b=2k$, $c=-k$ 时, 有 $-b/2=-k\leqslant r<k=b/2$;

   ii) 当 $b=2k$, $c=-k+1$ 时, 有 $-b/2=-k<r\leqslant k=b/2$;

   iii) 当 $b=2k+1$, $c=-k$ 时, 有 $-(b-1)/2=-k\leqslant r<k+1=(b+1)/2$ 或

$$-b/2<-(b-1)/2=-k\leqslant r\leqslant(b-1)/2<b/2.$$

总之, 我们有

$$-b/2\leqslant r<b/2 \quad 或 \quad -b/2<r\leqslant b/2.$$

这时 r 叫做**绝对值最小余数**.

例 1.2.3 设 $b=7$, 则

余数 $r=0,\ 1,\ 2,\ 3,\ 4,\ 5,\ 6$ 为最小非负余数;

余数 $r=1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7$ 为最小正余数;

余数 $r=0,\ -1,\ -2,\ -3,\ -4,\ -5,\ -6$ 为最大非正余数;

余数 $r=-1,\ -2,\ -3,\ -4,\ -5,\ -6,\ -7$ 为最大负余数;

余数 $r=-3,\ -2,\ -1,\ 0,\ 1,\ 2,\ 3$ 为绝对值最小余数.

例 1.2.4 设 $b=8$, 则

余数 $r=0,\ 1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7$ 为最小非负余数;

余数 $r=1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8$ 为最小正余数;

余数 $r=0,\ -1,\ -2,\ -3,\ -4,\ -5,\ -6,\ -7$ 为最大非正余数;

余数 $r=-1,\ -2,\ -3,\ -4,\ -5,\ -6,\ -7,\ -8$ 为最大负余数;

余数 $r=-4,\ -3,\ -2,\ -1,\ 0,\ 1,\ 2,\ 3$ 或 $r=-3,\ -2,\ -1,\ 0,\ 1,\ 2,\ 3,\ 4$ 为绝对值最小余数.

作为 Euclid 除法的应用, 我们给出 b 进制的数学表示以及具体计算方法. 运用 Euclid 除法, 我们可得到如下定理:

定理 1.2.3 设 b 是大于 1 的整数, 则每个正整数 n 可唯一地表示成

$$n = a_{k-1}b^{k-1} + a_{k-2}b^{k-2} + \cdots + a_1 b + a_0,$$

其中 a_i 是整数, $0 \leqslant a_i \leqslant b-1$, $i = 0, \cdots, k-1$, 且首项系数 $a_{k-1} \neq 0$.

证 我们先证明 n 有定理中所给的表达式. 具体方法是逐次运用 Euclid 除法, 以得到所期望的表达式.

首先, 用 b 去除 n, 得到

$$n = q_0 b + a_0, \quad 0 \leqslant a_0 \leqslant b-1.$$

再用 b 去除不完全商 q_0, 得到

$$q_0 = q_1 b + a_1, \quad 0 \leqslant a_1 \leqslant b-1.$$

继续这类算法, 依次得到

$$\begin{aligned}
q_1 &= q_2 b + a_2, && 0 \leqslant a_2 \leqslant b-1,\\
q_2 &= q_3 b + a_3, && 0 \leqslant a_3 \leqslant b-1,\\
&\cdots\cdots\cdots\cdots\\
q_{k-3} &= q_{k-2} b + a_{k-2}, && 0 \leqslant a_{k-2} \leqslant b-1,\\
q_{k-2} &= q_{k-1} b + a_{k-1}, && 0 \leqslant a_{k-1} \leqslant b-1.
\end{aligned}$$

因为

$$0 \leqslant q_{k-1} < q_{k-2} < \cdots < q_2 < q_1 < q_0 < n,$$

所以必有整数 k 使得不完全商 $q_{k-1} = 0$.

这样, 我们依次得到

$$\begin{aligned}
n &= q_0 b + a_0,\\
n &= (q_1 b + a_1) b + a_0 = q_1 b^2 + a_1 b + a_0,\\
&\cdots\cdots\cdots\cdots\\
n &= q_{k-3} b^{k-2} + a_{k-3} b^{k-3} + \cdots + a_1 b + a_0,\\
n &= q_{k-2} b^{k-1} + a_{k-2} b^{k-2} + \cdots + a_1 b + a_0\\
&= (q_{k-1} b + a_{k-1}) b^{k-1} + a_{k-2} b^{k-2} + \cdots + a_1 b + a_0\\
&= a_{k-1} b^{k-1} + a_{k-2} b^{k-2} + \cdots + a_1 b + a_0.
\end{aligned}$$

再证明这个表达式是唯一的. 假设有两种不同的表达式:

$$n = a_{k-1}b^{k-1} + a_{k-2}b^{k-2} + \cdots + a_1 b + a_0, \quad 0 \leqslant a_i \leqslant b-1,\ i = 0, \cdots, k-1;$$

$$n = c_{k-1}b^{k-1} + c_{k-2}b^{k-2} + \cdots + c_1 b + c_0, \quad 0 \leqslant c_i \leqslant b-1,\ i = 0, \cdots, k-1.$$

(这里可以取 $a_{k-1} = 0$ 或 $c_{k-1} = 0$.) 两式相减得到

$$(a_{k-1} - c_{k-1})b^{k-1} + (a_{k-2} - c_{k-2})b^{k-2} + \cdots + (a_1 - c_1)b + (a_0 - c_0) = 0.$$

假设 j 是使得 $a_j \neq c_j$ 的最小非负整数, 则

$$[(a_{k-1} - c_{k-1})b^{k-1-j} + (a_{k-2} - c_{k-2})b^{k-2-j} + \cdots + (a_{j+1} - c_{j+1})b + (a_j - c_j)]b^j = 0$$

或者

$$(a_{k-1} - c_{k-1})b^{k-1-j} + (a_{k-2} - c_{k-2})b^{k-2-j} + \cdots + (a_{j+1} - c_{j+1})b + (a_j - c_j) = 0.$$

因此

$$a_j - c_j = -[(a_{k-1} - c_{k-1})b^{k-j-2} + (a_{k-2} - c_{k-2})b^{k-j-3} + \cdots + (a_{j+1} - c_{j+1})]b.$$

故

$$b \mid (a_j - c_j), \quad |a_j - c_j| \geqslant b.$$

但

$$0 \leqslant a_j \leqslant b-1, \quad 0 \leqslant c_j \leqslant b-1,$$

从而又有 $|a_j - c_j| < b$. 得出矛盾, 也就是说 n 的表达式是唯一的. 证毕.

根据定理 1.2.3, 我们有

定义 1.2.3 用 $n = (a_{k-1}a_{k-2}\cdots a_1 a_0)_b$ 表示展开式

$$n = a_{k-1}b^{k-1} + a_{k-2}b^{k-2} + \cdots + a_1 b + a_0,$$

其中 $0 \leqslant a_i \leqslant b-1$, $i = 0, \cdots, k-1$, $a_{k-1} \neq 0$, 并称其为整数 n 的 b **进制表示**. 这时, n 的 b 进制位数是 $k = [\log_b n] + 1$. 事实上,

$$b^{k-1} \leqslant n < b^k \quad \text{或} \quad k - 1 \leqslant \log_b n < k.$$

因此, $k - 1 = [\log_b n]$.

当 $b = 2$ 时, 系数 a_i 为 0 或 1, 因此我们有

推论 每个正整数都可以表示成 2 的不同的幂之和.

例 1.2.5 表示整数 642 为 2 进制.

解 逐次运用 Euclid 除法, 我们有

$$\begin{aligned}
642 &= 321\cdot 2 + 0,\\
321 &= 160\cdot 2 + 1,\\
160 &= 80\cdot 2 + 0,\\
80 &= 40\cdot 2 + 0,\\
40 &= 20\cdot 2 + 0,\\
20 &= 10\cdot 2 + 0,\\
10 &= 5\cdot 2 + 0,\\
5 &= 2\cdot 2 + 1,\\
2 &= 1\cdot 2 + 0,\\
1 &= 0\cdot 2 + 1.
\end{aligned}$$

因此, $642 = (1010000010)_2$ 或者

$$\begin{aligned}
642 = {} & 1\cdot 2^9 + 0\cdot 2^8 + 1\cdot 2^7 + 0\cdot 2^6 + 0\cdot 2^5 +\\
& 0\cdot 2^4 + 0\cdot 2^3 + 0\cdot 2^2 + 1\cdot 2^1 + 0\cdot 2^0.
\end{aligned}$$

计算机也常用 8 进制、 16 进制或 64 进制. 在 16 进制中, 我们用 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F 分别表示 0, 1, $\cdots$, 15 等 16 个数, 其中 A, B, C, D, E, F 分别对应于 10, 11, 12, 13, 14, 15.

例 1.2.6 转换 16 进制 $(ABC8)_{16}$ 为 10 进制.

解 $(ABC8)_{16} = 10\cdot 16^3 + 11\cdot 16^2 + 12\cdot 16 + 8 = (43976)_{10}$.

为了方便各进制之间的转换, 提高转换效率, 我们可以预先制作一个换算表, 再根据换算表作转换. 以下就是 10 进制、 16 进制和 2 进制之间的换算表:

10 进制	16 进制	2 进制	10 进制	16 进制	2 进制
0	0	0000	8	8	1000
1	1	0001	9	9	1001
2	2	0010	10	A	1010
3	3	0011	11	B	1011
4	4	0100	12	C	1100
5	5	0101	13	D	1101
6	6	0110	14	E	1110
7	7	0111	15	F	1111