本科生基础课

初等数论讲义

陆　　俊

谈 胜 利

华东师范大学数学系

二零一八年五月

前　言

这本讲义尝试按照代数几何的观点来介绍初等数论的经典内容. 初等数论的重要内容之一就是研究低次数不定方程的整数解或者有理数解. 从代数几何的观点看, 就是研究底次平面曲线上的整数点或者有理点. 我们希望以解方程为主线, 逐步展开内容, 将初等数论的各个知识点与方程联系统一起来. 另一方面, 我们还希望在教学过程中突出算法的重要性, 比如辗转相除法、连分数方法、椭圆曲线的加法运算等等. 这样可以让学生更好地掌握初等数论这门课程的精髓.

目 录

第一章 导读 1
1.1 一些记号说明 1
1.2 初等数论的主线—求解不定方程 1
本章习题 3
第二章 一次不定方程 4
2.1 整除与素数 4
2.2 公因子和欧几里得算法 5
2.2.1 公因子 5
2.2.2 欧几里得算法 7
2.3 算术基本定理 9
2.3.1 算术基本定理 9
2.3.2 应用 (I): 最大公因子的素因子分解算法 10
2.3.3 应用 (II): 最小公倍数的素因子分解算法 10
2.3.4 应用 (III): 一些无理数的判定 11
2.3.5 应用 (IV): 素数个数无限的证明 13
2.4 一次不定方程 15
2.4.1 二元一次不定方程的求解算法 15
2.4.2 多元一次不定方程的求解算法 17
2.5 同余式 20
2.5.1 同余与完全剩余系 20
2.5.2 既约剩余类与欧拉定理 23
2.5.3 一些简单的应用 25
2.5.4 欧拉函数的公式算法 28
2.6 一次同余方程 (组) 30
2.6.1 一元一次同余方程的求解算法 30
2.6.2 多元一次同余方程的求解算法 33
2.6.3 同余方程组与孙子定理 36
本章习题 39
第三章 二次不定方程 41
3.1 勾股方程及其算法 41
3.1.1 数论证明 42
3.1.2 解析几何证明 42
3.1.3 椭圆或双曲线上的有理点 43
3.1.4 应用: 四次费马方程 45
3.2 平方剩余及其算法 46
3.2.1 勒让德符号与欧拉定理 47
3.2.2 应用 (I): 威尔逊定理 49
3.2.3 应用 (II): 模素数二次同余式求解算法 50
3.2.4 高斯引理 51

3.2.5 二次互反律 53
3.2.6 应用 (III): 梅森素数的判别 56
3.2.7 雅克比符号 57
3.2.8 一般情形的二次同余式的求解算法 60
3.3 平方和问题 61
3.3.1 费马–欧拉定理 62
3.3.2 高斯整数 63
3.3.3 补充材料: 华林问题简介 66
3.4 佩尔方程与连分数算法 67
3.4.1 连分数的基础知识 67
3.4.2 渐近分数的逼近 69
3.4.3 循环连分数 72
3.4.4 佩尔方程的求解算法 75
本章习题 77
第四章 三次不定方程 79
4.1 椭圆曲线上的群结构 79
4.2 有理点的算法 80
4.3 同余数 81
4.4 费马大定理与椭圆曲线 82
4.5 圆锥曲线与二次不定方程 84
本章习题 85
第五章 高次不定方程 86
5.1 高次同余方程的解数 86
5.2 Wolstenholme 定理 88
5.3 原根与指标 89
5.3.1 原根的存在性 89
5.3.2 指标 90
5.3.3 应用 (I): 威尔逊定理的新证明 92
5.3.4 应用 (II): 正多边形尺规作图问题 92
5.4 k 次剩余 94
本章习题 95
参考文献 97

第一章　导读

1.1　一些记号说明

为方便讨论, 我们这里规定一些记号.

(1) 整数集

$$\mathbb{Z} := \{0, \pm 1, \pm 2, \pm 3 \cdots\}.$$

(2) 正整数集

$$\mathbb{Z}^+ := \{n \in \mathbb{Z} \mid n > 0\}.$$

(3) 非负整数集

$$\mathbb{N} := \mathbb{Z}^+ \cup \{0\}.$$

(4) 有理数集

$$\mathbb{Q} = \left\{ \frac{p}{q} \,\middle|\, p, q \in \mathbb{Z},\ q \neq 0 \right\}.$$

(5) 取整函数: 对任何实数 x, 以 $[x]$ 表示不超过 x 的最大整数, 它也称为 x 的整数部分. 比如

$$[2.6] = 2, \quad [0] = 0, \quad [-2.3] = -3, \quad [-3] = -3, \quad [\sqrt{2}] = 1, \quad [-\sqrt{2}] = -2.$$

x 的小数部分定义为

$$\{x\} := x - [x].$$

容易看到, $0 \leq \{x\} < 1$, 因而 $[x] \leq x < [x] + 1$.

1.2　初等数论的主线—求解不定方程

初等数论的主要研究对象就是整数和有理数. 对它们的研究, 主要是通过求解某些特殊的方程作为主线来展开的. 事实上, 你会发现许多重要的经典数学课程都围绕着"解方程" 这一主题. 比如解析几何就是研究方程的几何图形; 线性代数则研究线性方程; 抽象代数最早是从研究代数方程的可解性发展起来的 (我们熟知的尺规作图问题等都与此有关)..... 因此这本讲义也将按照求解方程的主线来介绍初等数论.

首先让我们回忆一下, 在平面解析几何中, 人们主要关心以下多项式方程在平面中所描绘的曲线,

$$C: \quad f(x, y) = 0.$$

比如直线和圆锥曲线 (椭圆、双曲线、抛物线) 等等.

定义 1.2.1　*如果曲线 C 上的点 $p = (x, y)$ 的分量 x, y 都是有理数, 我们就称 p 是 C 的有理点. 如果分量 x, y 都是整数, 我们就称 p 是 C 的整数点.*

一般说来, 曲线 C 上的有理点和整数点是非常稀少的, 有时甚至没有! 数论的主要任务之一就是要求出曲线 C 上的有理点或整数点. 当我们只关心有理点或者整数点的时候, 方程 $f(x,y)=0$ 通常就被称为*丢番图方程*或者*不定方程*. 我们的初等数论主要关心如何求出直线和圆锥曲线等的有理点或整数点. 此外我们也可以考虑变量更多次数更高的不定方程或者不定方程组. 当我们说, 求一个不定方程 (组)的整数解或有理解时, 就相当于说 (从几何角度看), 寻找这个方程定义的几何图形上的整数点或者有理点.

下面我们将逐一简要介绍这本讲义所关心的各类重要的不定方程 (组).

问题 1.2.1　求线性方程组的整数解 $(x_1,\cdots,x_n)$:

$$\begin{cases} a_{11}x_1+a_{12}x_2+\cdots+a_{1n}x_n &= b_1,\\ a_{21}x_1+a_{22}x_2+\cdots+a_{2n}x_n &= b_2,\\ \cdots\quad\cdots\quad\cdots & \\ a_{m1}x_1+a_{m2}x_2+\cdots+a_{mn}x_n &= b_m, \end{cases}$$

这里诸 $a_i,b_i\in\mathbb{Z}$. 这一方程的求解将会引出初等数论中的整除理论和同余理论.

问题 1.2.2　求解单位圆周上的有理点 (x,y):

$$x^2+y^2=1.$$

或者等价地, 我们要求勾股方程

$$X^2+Y^2=Z^2$$

的整数解 (X,Y,Z).

此外, 也希望求解圆周方程

$$x^2+y^2=d$$

的整数解 (x,y), 此处 d 是给定整数.

这些方程的求解将会涉及到近世代数中的一部分内容—事实上, 近世代数的许多内容只不过是初等数论的推广.

问题 1.2.3　求解双曲线上的整数点 (x,y):

$$x^2-dy^2=1,$$

此处 d 是给定的正整数. 该不定方程也称为佩尔方程. 我们将用连分数的方法来巧妙求解.

问题 1.2.4　解抛物线上的整数点 (x,y):

$$x^2-py=q,$$

此处 p,q 是给定的正整数. 该不定方程也称为二次剩余问题或平方剩余问题. 这个问题将会引出是初等数论中最引人入胜的内容之一—高斯的二次互反律.

注 1.2.1　上面的三个问题本质上都是寻找圆锥曲线上的整数点或有理点. 我们也可以研究更一般的不定方程

$$Ax^2+2Bxy+Cy^2=D,$$

这里 A, B, C, D 是给定整数. 这个方程将引出二次型理论和闵可夫斯基的"数的几何". 不过限于本书的篇幅, 我们只能简要介绍其中的部分内容. ■

问题 1.2.5　求解三次方程的有理数解 (x, y):

$$y^2 = x^3 + ax + b.$$

这一方程定义的曲线称作椭圆曲线. 我们将介绍一种巧妙的计算方法, 可以从已知的有理点构造出新的有理点. 此外, 作为应用, 我们将介绍著名的同余数问题等等.

问题 1.2.6　求高次方程的整数解 (x, y):

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 = py,$$

这里诸 $a_i, p \in \mathbb{Z}$. 这一方程的求解在近世代数中有不同程度的推广.

数论中还有许许多多著名的不定方程问题, 其中一些至今未能解决. 我们这里不再一一赘述. 读者将会在此后的章节中看到更多的不定方程的介绍.

本章习题

加 $*$ 号的习题表示有一定难度.

习题 1.1　证明以下各结论:

(1) $[x] \leq x < [x] + 1$, 并给出左边等号成立的条件.

(2) $[x + n] = [x] + n$, $\forall n \in \mathbb{Z}$.

(3) $[x] + [y] \leq [x + y] \leq [x] + [y] + 1$.

(4) $\left[\frac{[nx]}{n}\right] = [x]$, $\forall n \in \mathbb{Z}$.

(5) 如果 $x, y > 0$, $[xy], [x], [y]$ 之间有什么关系吗?

(6) 画出 $y = [x]$ 和 $y = \{x\}$ 的图像.

(7) 对任何实数 x,

$$[-x] + [x] = \begin{cases} 0, & x \in \mathbb{Z}, \\ -1, & x \notin \mathbb{Z}. \end{cases}$$

(8*) (厄尔米特恒等式) 对任何实数 x 恒有:

$$[x] + \left[x + \frac{1}{n}\right] + \cdots + \left[x + \frac{i}{n}\right] + \cdots + \left[x + \frac{n-1}{n}\right] = [nx].$$

第二章　一次不定方程

以下如无特别声明, $a, d, c, \cdots$ 等均指整数.

2.1　整除与素数

最简单的不定方程就是求

$$bx = a, \quad b \neq 0 \tag{2-1}$$

的整数解. 如果该方程有整数解, 我们就称 b 整除 a, 或称 a 被 b 整除, 并记作 $a \mid b$; 否则就称 b 不整除 a, 记作 $b \nmid a$. 显然, $a \mid b$ 等价于说 $\frac{a}{b}$ 是整数.

例 2.1.1

$$1 \mid 2, \quad 3 \mid (-6), \quad 3 \nmid 5, \quad (-2) \nmid 1.$$

命题 2.1.1　设 $a, b, c \in \mathbb{Z}$, $bc \neq 0$, 我们有

(1) (传递性) 若 $b \mid a$ 且 $c \mid b$, 则 $c \mid a$;
(2) (自反性) $b \mid b$;
(3) (消去律) $bc \mid ac$ 当且仅当 $b \mid a$;
(4) (万有性) $\pm 1 \mid a$ 且 $b \mid 0$;
(5) (序关系) 若 $b \mid c$, 则 $|b| \leq |c|$;
(6) (加性) 若 $c \mid a$, $c \mid b$, 则对任何 $m, n \in \mathbb{Z}$, 都有 $c \mid (am + bn)$.

证明　(1)–(4) 是显然的, 留给读者验证.

(5) 设 $x = \frac{c}{b}$. 因为 $b \mid c$ 且 $bc \neq 0$, 所以 x 是非零整数. 因而 $|c| = |x| \cdot |b| \geq |b|$.

(6) 设 $x = \frac{a}{c}, y = \frac{b}{c}$. 由命题条件, $x, y \in \mathbb{Z}$. 因此

$$\frac{am + bn}{c} = xm + yn \in \mathbb{Z},$$

即 $c \mid (am + bn)$. ■

由命题 2.1.1 (5) 以下的常用结论.

推论 2.1.1　设 a, b 是正整数, 若 $a \mid b$ 且 $b \mid a$, 则 $a = b$.

定义 2.1.1　设 $b \mid a$ (要求 $b \neq 0$), 我们称 b 是 a 的因子, a 是 b 的倍数. 进一步, 如果 $1 < |b| < |a|$, 则称 b 是 a 的真因子.

有了整除的概念之后, 我们可以引进“素数”这一重要的对象.

定义 2.1.2　设 $p > 1$ 是整数. 如果 p 没有真因子, 我们就称 p 是素数; 否则就称合数.

正整数中最前面的素数分别是

$$2,\quad 3,\quad 5,\quad 7,\quad 11,\quad 13,\quad 17,\quad 19,\quad 23,\quad 29,\quad 31,\quad 37,\cdots$$

其中 2 是唯一的偶素数.

命题 2.1.2　*设 $n>1$ 是整数, 则 n 必可分解为素数的乘积*

$$n=q_1q_2\cdots q_k$$

这里诸 q_i 是素数 (允许相同).

证明　对 n 施归纳法. $n=2$ 时是显然的. 今假设 $<n$ 的情形已证. 如果 n 是素数, 则命题显然成立. 如果 n 是合数, 那么我们选取 n 的所有真因子中的最小者, 记作 q_1. q_1 必是素数 (否则它将包含更小的真因子).

设 $n'=\frac{n}{q_1}$, 则 $1<n'<n$. 由归纳假设, n' 可以分解为一些素数的乘积 $n'=q_2\dots q_k$. 因此这就得到 $n=q_1q_2\cdots q_k$. ■

有时为了方便, 我们可以将 n 的上述分解中相同的素因子合并起来, 写称方幂形式的乘积

$$n=p_1^{m_1}p_2^{m_2}\cdots p_s^{m_s},\quad p_1<p_2<\cdots<p_s, m_i\geq 1, \tag{2-2}$$

这里诸 q_i 是两两不同的素数. 式 (2-2) 被称为 n 的*标准分解式*. 后面将证明正整数的标准分解式是唯一的.

例 2.1.2　$24=2^3\cdot 3,\quad 120=2^3\cdot 3\cdot 5,\quad 100=2^2\cdot 5^2,\quad 64=2^6.$ ■

2.2　公因子和欧几里得算法

2.2.1　公因子

定义 2.2.1　*设 $a,b,c\in\mathbb{Z}$, 且 $c>0$. 如果 $c\mid a$ 并且 $c\mid b$, 我们就称 c 是 a 和 b 的公因子. 所有公因子中的最大者称作最大公因子, 记作 $\gcd(a,b)$, 或简记作 (a,b). 如果 $(a,b)=1$, 我们就称 a,b 是互质的 (也称互素).*

例 2.2.1　$(2,4)=2,\ (2,3)=1,\ (-4,-6)=2.$ ■

注 2.2.1　我们也可以用方程的语言来叙述公因子的定义, 即如果方程组

$$\begin{cases} cx=a,\\ cy=b \end{cases}$$

存在整数解 (x,y), 则称 c 是 a 和 b 的公因子. ■

进一步, 我们也可以归纳地定义 n 个整数 $a_1,\cdots,a_n$ 的最大公因子

$$(a_1,\cdots,a_n):=((a_1,\cdots,a_{n-1}),a_n).$$

以下我们将介绍求最大公因子的算法. 为此需要先对最大公因子的一些基本性质做一些了解. 首先, 我们回顾基础算术中的带余数除法.

引理 2.2.1 (带余数除法) 设 $a, b \in \mathbb{Z}$, $b > 0$, 则存在唯一的整数 q, r, 使得 $a = qb + r$, 并且 $0 \leq r < b$. r 称为余数, q 称为商.

证明 (1) 存在性. 令 $q = [\frac{a}{b}]$, $r = a - bq$. 由第 1.1 节 (5) 的讨论, 我们有

$$0 \leq r = a - bq = b(\frac{a}{b} - [\frac{a}{b}]) < b.$$

(2) 唯一性. 设 $a = q'b' + r'$ 是另一满足条件的式子. 我们有 $(q' - q)b = r - r'$. 两边取绝对值得

$$|q' - q| \cdot b = |r - r'|.$$

因为 $0 \leq r, r' < b$, 所以 $0 \leq |r - r'| < b$. 这就推出 $0 \leq |q - q'| < 1$, 因而迫使 $q = q'$, 故得 $r = r'$. ■

注 2.2.2 $b \mid a$ 也可以等价定义为: a 除以 b 的余数为零. ■

考虑整数集合中的特殊子集

$$\Sigma_{a,b} = \{am + bn \mid m, n \in \mathbb{Z}\}.$$

引理 2.2.2 (1) (零元) $0 \in \Sigma_{a,b}$;
(2) (封闭性) 对任何 $x, y \in \Sigma_{a,b}$, $s, t \in \mathbb{Z}$, 都有 $sx + ty \in \Sigma_{a,b}$

证明 (1) 取 $m = -b$, $n = a$, 则 $0 = am + bn \in \mathbb{Z}$.
(2) 直接验算即得. ■

引理 2.2.3 设 $d = am_0 + bn_0$ 是 $\Sigma_{a,b}$ 中最小的正整数.
(1) $d = (a, b)$;
(2) 对任何 $x \in \Sigma_{a,b}$, 都有 $d \mid x$;
(3) 设 c 是 a, b 的任一公因子, 则 $c \mid d$.

证明 (1) 因为 $(a, b) \mid a, (a, b) \mid b$, 故由命题 2.1.1 (6) 立知

$$(a, b) \mid d(= am_0 + bn_0).$$

因此由命题 2.1.1 (5) 推出 $(a, b) \leq d$.

另一方面, 设 $a = dq + r$ $(0 \leq r < d)$ 是带余数除法. 我们有

$$r = a - dq = a(1 - qm_0) + b(-qn_0) \in \Sigma_{a,b}.$$

d 的最小性迫使 $r = 0$, 即 $d \mid a$. 同理可证 $d \mid b$. 因此 d 是 a 和 b 的公因子. 由最大公因子的定义得 $d \leq (a, b)$. 这就证明了 $d = (a, b)$.

(2) 显然.

(3) 因 $c \mid a, c \mid b$, 故由命题 2.1.1 (6) 知 $c \mid d(= am_0 + bn_0)$. ■

推论 2.2.1 存在 $x, y \in \mathbb{Z}$, 使得 $ax + by = (a, b)$.

注 2.2.3 我们将在推论 2.2.4 中给出计算上述 x, y 的方法. ■

上述推论有许多应用, 这里我们用它来获得一些求最大公因子的常用技巧.

推论 2.2.2 设 $a,b,c\in\mathbb{Z}$, 且 $c>0$.
(1) (分配律) $(ac,bc)=(a,b)\cdot c$;
(2) (消去律) 若 $(a,b)=1$, 则 $(a,bc)=(a,c)$;
(3) 对任何 $m\in\mathbb{Z}$, 都有 $(a,b-ma)=(a,b)$;
(4) $c\mid b$ 当且仅当 $(c,b)=c$.
(5) 设 p 是素数, 且 $p\nmid a$, 则 $(p,a)=1$.

证明 (1) 设 $x,y\in\mathbb{Z}$ 满足 $ax+by=(a,b)$. 因此 $(a,b)c=acx+bcy\in\Sigma_{ac,bc}$. 由引理 2.2.3 (2) 推知

$$(ac,bc)\mid(a,b)c.$$

另一方面, 由命题 2.1.1 (3) 及公因子的定义, 我们有

$$(a,b)c\mid ac,\quad (a,b)c\mid bc.$$

因此由引理 2.2.3 (3) 可知, $(a,b)c\mid(ac,bc)$. 这就得到 $(a,b)c=(ac,bc)$ (推论 2.1.1).

(2) 此时 $ax+by=1$. 两边乘以 c 得 $a(cx)+bcy=c$. 故由引理 2.2.3 (2) 得 $(a,bc)\mid c$. 显然 $(a,bc)\mid a$, 故 $(a,bc)\mid(a,c)$. 另一方面, 显见 $(a,c)\mid(a,bc)$. 这就证明了 $(a,bc)=(a,c)$ (推论 2.1.1).

(3) 由 $ax+by=(a,b)$ 得 $a(x+my)+(b-am)y=(a,b)$, 故有 $(a,b-am)\mid(a,b)$. 另一方面, 显见 $(a,b)\mid(a,b-am)$, 这就推得等式.

(4) 显然.

(5) 因 $(p,a)\mid p$, 故由素数定义知, $(p,a)=1$ 或 p. 若 $(p,a)=p$, 则由 (4) 得 $p\mid a$, 矛盾! 故 $(p,a)=1$. ■

例 2.2.2 设 $a=1040,b=85$, 求最大公因子 (a,b).

$$(a,b)=5(208,17)=5(52\times4,17)=5(52,17)=5(52-17\times3,17)=5(1,17)=5.$$

事实上, 这种计算方法只不过是下一节将介绍的欧几里得算法的一类特例而已. ■

推论 2.2.3 设 p 是素数, 且 $p\mid ab$, 则要么 $p\mid a$, 要么 $p\mid b$.

证明 由条件, $(p,ab)=p$. 假设 $p\nmid b$, 则由推论 2.2.2 (5), $(p,b)=1$. 进一步由推论 2.2.2 (2) 可得 $(p,a)=1$，从而 $p\nmid a$, 矛盾! ■

注 2.2.4 上述推论显然可以推广到更一般的情形, 即若 $p\mid a_1a_2\cdots a_n$, 则 p 至少整除其中一个 a_i. 这一推论将被用来证明正整数的素因子分解的唯一性 (见算术基本定理 2.3.1). ■

2.2.2 欧几里得算法

这一小节将提供计算最大公因子的算法.

我们考虑带余数除法 $a=bq_1+r_1$, $0\le r_1<q_1$. 假如 $r_1=0$, 即 $b\mid a$, 则显然有 $(a,b)=b$. 如果 $r_1>0$, 则继续考虑带余数除法 $b=r_1q_2+r_2$, $0\le r_2<r_1$,..... 依次类推, 我们得到一系列

带余数除法

$$\begin{cases} a &= bq_1 + r_1, & 0 \le r_1 < b \\ b &= r_1q_2 + r_2, & 0 \le r_2 < r_1 \\ r_1 &= r_2q_3 + r_3, & 0 \le r_3 < r_2 \\ & \cdots & \cdots \\ r_{n-1} &= r_nq_{n+1} + r_{n+1}, & r_{n+1} = 0. \end{cases} \tag{2-3}$$

请注意, 因为余数 r_i 是严格递减的非负整数, 所以我们才能保证上面过程只能出现有限步, 并且最后一式的余数是零.

命题 2.2.1 (欧几里德算法) *在式 (2-3) 的记号下, 我们有 $r_n = (a, b)$.*

证明 由推论 2.2.2 (3), $(a, b) = (a - q_1b, b) = (r_1, b)$. 类似地, 也有 $(r_1, b) = (r_2, r_1) = \cdots = (r_{n-1}, r_n)$. 注意到 $r_n \mid r_{n-1}$, 故 $r_n = (r_{n-1}, r_n)$. 因此 $r_n = (a, b)$. ■

推论 2.2.4 *设*

$$x = (-1)^{n-1}\begin{vmatrix} q_2 & 1 & & & \\ -1 & q_3 & 1 & & \\ & -1 & q_4 & 1 & \\ & & \cdots & \cdots & \\ & & & q_{n-1} & 1 \\ & & & -1 & q_n \end{vmatrix}, \qquad y = (-1)^n\begin{vmatrix} q_1 & 1 & & & \\ -1 & q_2 & 1 & & \\ & -1 & q_3 & 1 & \\ & & \cdots & \cdots & \\ & & & q_{n-1} & 1 \\ & & & -1 & q_n \end{vmatrix}$$

则 $ax + by = (a, b)$.

证明 将式 (2-3) 写成矩阵形式 (请注意最后一个等式不算在内)

$$\begin{pmatrix} q_1 & 1 & & & \\ -1 & q_2 & 1 & & \\ & -1 & q_3 & 1 & \\ & & \cdots & \cdots & \\ & & & q_{n-1} & 1 \\ & & & -1 & q_n \end{pmatrix}\begin{pmatrix} b \\ r_1 \\ r_2 \\ \vdots \\ \vdots \\ r_{n-1} \end{pmatrix} = \begin{pmatrix} a \\ 0 \\ \vdots \\ \vdots \\ 0 \\ -r_n \end{pmatrix}$$

由线性方程的克莱姆法则, 即得

$$b \cdot \begin{vmatrix} q_1 & 1 & & & \\ -1 & q_2 & 1 & & \\ & -1 & q_3 & 1 & \\ & & \cdots & \cdots & \\ & & & q_{n-1} & 1 \\ & & & -1 & q_n \end{vmatrix} = \begin{vmatrix} a & 1 & & & \\ 0 & q_2 & 1 & & \\ 0 & -1 & q_3 & 1 & \\ \vdots & & \cdots & \cdots & \\ 0 & & & q_{n-1} & 1 \\ -r_n & & & -1 & q_n \end{vmatrix}$$

上式右边等于 $(-1)^{n-1}ax + (-1)^n r_n$, 左边等于 $(-1)^n by$. 由此及命题 2.2.1 即得结论. ■

注 2.2.5 请注意, 方程 $ax + by = (a, b)$ 的整数解并不唯一, 上面的结论只是提供了一组特解. ■

例 2.2.3 (1) 设 $a = 323, b = 221$, 求最大公因子 (a,b) 及一组解 (x,y) 满足 $ax + by = (a,b)$.

$$\begin{cases} 323 = 221 \times 1 + 102 \\ 221 = 102 \times 2 + 17 \\ 102 = 17 \times 6. \end{cases}$$

因此 $(a,b) = 17$. 由推论 2.2.4, 可取 $x = -2, y = 3$.

(2) 设 $a = 169, b = 121$, 求最大公因子 (a,b) 及一组解 (x,y) 满足 $ax + by = (a,b)$.

$$\begin{cases} 169 = 121 \times 1 + 48 \\ 121 = 48 \times 2 + 25 \\ 48 = 25 \times 1 + 23 \\ 25 = 23 \times 1 + 2 \\ 23 = 2 \times 11 + 1 \\ 2 = 1 \times 2. \end{cases}$$

因此 $(a,b) = 1$. 由推论 2.2.4, 可取 $x = 58, y = 81$. ■

2.3 算术基本定理

2.3.1 算术基本定理

现在我们要利用推论 2.2.3 来证明素数分解的唯一性, 这就是如下的经典结论

定理 2.3.1 (**算术基本定理**) *任何大于 1 的正整数都有唯一的素因子分解, 即它的标准分解式是唯一的确定的.*

证明 由命题 2.1.2, 我们已经知道任何正整数 $n > 1$ 都可以分解成素数之积. 现在我们要证分解的唯一性. 假设 n 有两种标准分解式

$$n = p_1^{n_1} p_2^{n_2} \cdots p_s^{n_s} = q_1^{m_1} q_2^{m_2} \cdots q_t^{m_t}, \quad p_1 < p_2 < \cdots < p_s, \quad q_1 < q_2 < \cdots < q_t,$$

此处 p_i, q_j 皆素数.

对每个 q_i, 因为

$$q_i \mid p_1^{n_1} p_2^{n_2} \cdots p_s^{n_s},$$

故由推论 2.2.3 可知 q_i 必定整除某个 p_j. 又因为 q_i, p_j 都是素数, 所以这就迫使 $q_i = p_j$. 因此

$$\{q_1, \cdots, q_t\} \subseteq \{p_1, \cdots, p_s\}.$$

同理可证

$$\{p_1, \cdots, p_s\} \subseteq \{q_1, \cdots, q_t\}.$$

从而两个集合相等, 并且由序关系可知 $s = t$, $p_i = q_i$ $(i = 1, \cdots, s)$. 这样, 我们有

$$p_1^{n_1} p_2^{n_2} \cdots p_s^{n_s} = p_1^{m_1} p_2^{m_2} \cdots p_s^{m_s}.$$

如果对某个 i 有 $n_i > m_i$, 则上式两边同时除以 $p_i^{m_i}$, 则右端不含因子 p_i, 故不被 p_i 整除; 而左端却包含 $p_i^{n_i - m_i}$, 矛盾! 因此 $n_i \leq m_i$ 对任何 i 都成立. 同理亦可证 $n_i \geq m_i$, 这就推出 $n_i = m_i$. ■

2.3.2 应用 (I): 最大公因子的素因子分解算法

有了算术基本定理, 我们就可以用标准分解式来计算最大公因子. 不妨设 $a, b > 1$ 是正整数. 它们的素因子分解中可能会出现这样一类情况: a 含有素因子 p, 但 b 不含 p. 此时为方便讨论, 我们可以在 b 的素因子分解中添入 p^0 项, 这样至少在形式上, a, b 的分解式中都出现 p. 因此我们不妨在此意义上考虑"广义"的标准分解式

$$\begin{cases} a = p_1^{\alpha_1} \cdots p_s^{\alpha_s},\ \alpha_i \geq 0, \\ b = p_1^{\beta_1} \cdots p_s^{\beta_s},\ \beta_i \geq 0. \end{cases} \tag{2-4}$$

推论 2.3.1 *在上述记号与假设下, 我们有*

$$(a, b) = p_1^{\gamma_1} \cdots p_s^{\gamma_s},$$

这里 $\gamma_i = \min(\alpha_i, \beta_i)$, $i = 1, \cdots, s$.

证明 设 $c = p_1^{\gamma_1} \cdots p_s^{\gamma_s}$. 由 γ_i 的定义,

$$\frac{a}{c} = p_1^{\alpha_1 - \gamma_1} \cdots p_s^{\alpha_s - \gamma_s}, \quad \frac{b}{c} = p_1^{\beta_1 - \gamma_1} \cdots p_s^{\beta_s - \gamma_s}$$

都是整数, 并且每个 p_i 不可能同时出现在 $\frac{a}{c}, \frac{b}{c}$ 中. 因而 $(\frac{a}{c}, \frac{b}{c}) = 1$. 由推论 2.2.2 (1), 这就推出 $(a, b) = d(\frac{a}{c}, \frac{b}{c}) = d$. ■

例 2.3.1 (1) 设 $a = 12, b = 18$, 求 (a, b).

考虑素因子分解

$$a = 2^2 \cdot 3^1, \quad b = 2^1 \cdot 3^2.$$

由推论 2.3.1 即得 $(a, b) = 2^1 \cdot 3^1 = 6$.

(2) 设 $a = 162, b = 98$, 求 (a, b).

考虑素因子分解

$$a = 2^1 \cdot 3^4 = 2^1 \cdot 3^4 \cdot 7^0, \quad b = 2^1 \cdot 7^2 = 2^1 \cdot 3^0 \cdot 7^2.$$

我们有 $(a, b) = 2^1 \cdot 3^0 \cdot 7^0 = 2$. ■

我们现在有两种方法计算最大公因子:欧几里德算法和素因子分解方法. 第一种方法无需了解整数的素因子是什么, 只需要简单的带余数除法即可求出最大公因子; 而第二种方法却必须先知道每个整数的素因子分解式. 通常来说, 求一个大整数的素因子分解往往是非常困难的, 其计算量可能极其巨大, 因此用后一方法具体计算大整数的最大公因子实际上意义并不大.

2.3.3 应用 (II): 最小公倍数的素因子分解算法

定义 2.3.1 *设 $a, b, c \in \mathbb{Z}$, $ab \neq 0$. 如果 c 满足 $a \mid c, b \mid c$, 我们就称 c 是 a, b 之公倍数. a, b 所有公倍数中的最小正数者称为最小公倍数, 记作 $\mathrm{lcm}(a, b)$, 或简记为 $[a, b]$.*

类似公因子, 我们可以用方程的语言重新叙述公倍数的定义, 即如果方程组

$$\begin{cases} ax = c, \\ by = c \end{cases}$$

有整数解 (x,y), 则称 c 为 a,b 之公倍数.

我们也可以归纳定义 n 个整数 $a_1,\cdots,a_n$ 的公倍数和最小公倍数

$$[a_1,\cdots,a_n]=[[a_1,\cdots,a_{n-1}],a_n].$$

推论 2.3.2 *在式 (2-4) 的记号与假设下, 我们有*

$$[a,b]=p_1^{\delta_1}\cdots p_s^{\delta_s},$$

这里 $\delta_i=\max(\alpha_i,\beta_i)$, $i=1,\cdots,s$. 特别地, 任何公倍数都能被 $[a,b]$ 整除.

证明 设 $c=p_1^{\delta_1}\cdots p_s^{\delta_s}$. 由 δ_i 的定义, 显然有 $a\mid c, b\mid c$. 假设 d 是 a,b 的公倍数, 则 d 的素因子分解中 p_i 的方幂不小于 $\delta_i=\max(\alpha_i,\beta_i)$, 因而 $c\mid d$. 这也蕴含着 $c=[a,b]$. ■

例 2.3.2 (1) 设 $a=12,b=18$, 求 $[a,b]$.

考虑素因子分解

$$a=2^2\cdot 3^1,\quad b=2^1\cdot 3^2.$$

由推论 2.3.2 即得 $[a,b]=2^2\cdot 3^2=36$.

(2) 设 $a=162,b=98$, 求 $[a,b]$.

考虑素因子分解

$$a=2^1\cdot 3^4=2^1\cdot 3^4\cdot 7^0,\quad b=2^1\cdot 7^2=2^1\cdot 3^0\cdot 7^2.$$

我们有 $(a,b)=2^1\cdot 3^4\cdot 7^2=7938$. ■

与求最大公因子一样, 用素因子分解方法来求最小公倍数往往计算量很大. 下面的推论可以将最小公倍数计算归结到最大公因子计算, 从而可以用欧几里得算法有效地计算.

推论 2.3.3 *对任何正整数 a,b, 我们有恒等式*

$$(a,b)\cdot[a,b]=ab.$$

证明 在式 (2-4), 推论 2.3.1 和推论 2.3.2 的记号与假设下, 我们有

$$(a,b)\cdot[a,b]=p_1^{\gamma_1+\delta_1}\cdots p_s^{\gamma_s+\delta_s}.$$

注意到 $\gamma_i+\delta_i=\min(\alpha_i,\beta_i)+\max(\alpha_i,\beta_i)=\alpha_i+\beta_i$, 因此上式就等于 ab. ■

例 2.3.3 设 $a=6,b=15,c=20$. 求 a,b,c 的最大公因子和最小公倍数.

因 $(a,b)=3$, 故 $(a,b,c)=((a,b),c)=(3,20)=1$.

因 $[a,b]=\frac{ab}{(a,b)}=30$, 故 $[a,b,c]=[[a,b],c]=[30,20]=60$. ■

2.3.4 应用 (III): 一些无理数的判定

这一节中, 我们利用算术基本定理来证明一些实数的无理性.

推论 2.3.4 (**毕达哥拉斯**) *$\sqrt{2}$ 是无理数, 即 $\sqrt{2}\notin\mathbb{Q}$.*

证明 反证法. 假设 $\sqrt{2}\in\mathbb{Q}$, 将其写为既约分数 $\sqrt{2}=\frac{a}{b}$, 这里 a,b 是互质的正整数. 两边平方整理得

$$2b^2=a^2.$$

因左边是偶数, 故 a 也是偶数, 设 $a=2c$, 代入上式得 $b^2=2c^2$, 从而 b 也是偶数, 设为 $b=2d$. 这样, $(a,b)=(2c,2d)=2(c,d)>1$, 矛盾! ■

类似地, 我们也可以证明 $\sqrt{n}$ 不是有理数, 这里 n 非完全平方数.

例 2.3.4 $\sqrt{2}+\sqrt{3}$ 也不是有理数.

假设 $x=\sqrt{2}+\sqrt{3}\in\mathbb{Q}$, 则

$$x^2=5+2\sqrt{6}\in\mathbb{Q}.$$

因而 $\sqrt{6}\in\mathbb{Q}$, 矛盾! ■

上面的推论还可以推广到更一般的情形.

推论 2.3.5 *考虑以下首一多项式*

$$f(x)=x^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0,\quad a_i\in\mathbb{Z},\quad i=0,1\cdots,n-1,$$

如果方程 $f(x)=0$ 没有整数根, 则它也没有有理根.

证明 反证法, 假设 $x=\frac{p}{q}$ 是有理根 ($(p,q)=1$). 代入方程整理得

$$p^n+a_{n-1}p^{n-1}q+\cdots+a_1pq^{n-1}+a_0q^n=0.$$

注意到上式除了第一项外, 其余项都含有因子 q. 因此 $q\mid p^n$. 但是 $(p,q)=1$, 这就推出 $q=1$, 即 $x=p$ 是整数根, 矛盾! ■

例 2.3.5 (1) 取 $f(x)=x^2-2$. 方程显然没有整数根, 因而由推论 2.3.5, $x=\sqrt{2}$ 不是有理数.

(2) 取 $f(x)=x^4-10x^2+1$. 此时 $f=0$ 无整数根, 且 $x=\sqrt{2}+\sqrt{3}$ 是它的一个根. 因此这就再次证明 $\sqrt{2}+\sqrt{3}$ 是无理数. ■

例 2.3.6 $\log_2 10$ 不是有理数.

反证法. 设 $\log_2 10=\frac{p}{q}$ 是有理数, p,q 互质. 我们有

$$2^p=10^q.$$

上式左边只有素因子 2, 右边却包含素因子 5, 矛盾! ■

命题 2.3.1 *自然对数 e 不是有理数.*

证明 我们使用如下估计式

$$e=1+\frac{1}{1!}+\frac{1}{2!}+\cdots+\frac{1}{n!}+\frac{\theta_n}{n\cdot n!},\quad 0<\theta_n<1.$$

假设 $e=\frac{p}{q}$ 是有理数. 我们取 $n=q$, 并在上式两边乘以 $q!$, 则有

$$p\cdot(q-1)!=e\cdot q!=q!+\frac{q!}{1!}+\frac{q!}{2!}+\cdots+\frac{q!}{q!}+\frac{\theta_q}{q}.$$

这就推出 $\frac{\theta_q}{q}$ 是整数, 因此 θ_q 也是整数, 矛盾! ■

2.3.5 应用 (IV): 素数个数无限的证明

我们将讨论素数个数的无限性.

定理 2.3.2 *素数有无限多个.*

证明 反证法. 假设素数只有有限个 $p_1 < p_2 < \cdots < p_s$. 我们构造整数

$$N = p_1 p_2 \cdots p_s + 1 (> 1).$$

显然 $p_i \nmid N$ (否则将推出 $p_i \mid 1$). 因此 N 的素因子分解中必含有不同于诸 p_i 的素数, 这与假设矛盾! ■

注 2.3.1 这个证明的巧妙之处在于, 它并未具体构造出无限多个素数. 这就是数学中所谓的存在性证明, 即能断言某对象存在, 但却未能提供具体构造的方法. 我们以前学过的介值定理等等都属于存在性证明. ■

类似地, 我们也可以证明如下结论.

推论 2.3.6 *形如 $4n-1$ 的素数有无限多个. 换言之, 等差数列*

$$3, 7, 11, \cdots, 4n-1, \cdots$$

中含有无限多个素数.

证明 反证法. 假设形如 $4n-1$ 的素数只有有限个 $p_1 < p_2 < \cdots < p_s$. 我们构造整数

$$N = 4p_1 p_2 \cdots p_s - 1.$$

易知 N 的素因子中不含诸 p_i 及 2. 因此 N 的素因子只含有形如 $4n+1$ 的素数. 但是任何形如 $4n+1$ 的整数相乘仍然是形如 $4n+1$ 的整数, 即被 4 除余数是 1. 这意味着 N 被 4 除余数是 1, 这与 N 的构造矛盾! ■

狄利克雷给出了以下的一般结果, 但是证明比较困难.

定理 2.3.3 (狄利克雷定理) 设 a, b 是互质的正整数, 则等差数列

$$a, a+b, a+2b, \cdots, a+nb, \cdots$$

中含有无限多个素数.

我们还可以利用*费尔马数*

$$F_n = 2^{2^n} + 1$$

来证明素数个数的无限性. 首先我们有以下恒等式 (留给读者验证)

$$\prod_{k=0}^{n-1} F_k = F_n - 2. \tag{2-5}$$

引理 2.3.1 *任何两个费马数都互质.*

证明 设 $m = (F_k, F_n)$ $(k < n)$. 由式 (2-5), 这意味着 $m = (2, F_k)$. 注意 F_k 是奇数, 所以 $m = 1$. ■

既然任何两个费马数都互质, 所以它们包含的素因子也不相同. 由于我们有无限多个费马数, 所以我们也有无限多个不同的素因子. 这就证明素数有无限多个.

欧拉提供了另一种证明素数无限多的独特证明, 常被看作是解析数论的开端. 这里我们来简单介绍一下. 假设只有有限多个素数 $p_1, p_2, \cdots, p_s$. 我们考虑乘积

$$\left(1+\frac{1}{p_1}+\frac{1}{p_1^2}+\cdots\right)\cdot\left(1+\frac{1}{p_2}+\frac{1}{p_2^2}+\cdots\right)\cdots\left(1+\frac{1}{p_s}+\frac{1}{p_s^2}+\cdots\right) \tag{2-6}$$

的展开式. 显然, (2-6)的展开式中每一项都可以写成

$$\frac{1}{p_1^{m_1}p_2^{m_2}\cdots p_s^{m_s}}.$$

由算术基本定理和假设条件, 对每个整数 n, $\frac{1}{n}$ 恰好出现在 (2-6)的展开式中出现一次. 因此

$$\left(1+\frac{1}{p_1}+\frac{1}{p_1^2}+\cdots\right)\cdot\left(1+\frac{1}{p_2}+\frac{1}{p_2^2}+\cdots\right)\cdots\left(1+\frac{1}{p_s}+\frac{1}{p_s^2}+\cdots\right)=\sum_{n=1}^{\infty}\frac{1}{n}.$$

无论如何, 上式右端是发散的级数. 这就得到矛盾!

欧拉的证明富有很大的启发性. 比如我们考虑以下的无穷连乘积

$$\prod_p\left(1+\frac{1}{p^s}+\frac{1}{p^{2s}}+\frac{1}{p^{3s}}\cdots\right), \tag{2-7}$$

这里 p 取遍所有素数, s 是实部大于 1 的复数. 易知 (2-7) 收敛于一个解析函数, 并且类似上面讨论可知

$$\prod_p\left(1+\frac{1}{p^s}+\frac{1}{p^{2s}}+\frac{1}{p^{3s}}\cdots\right)=\sum_{n=1}^{\infty}\frac{1}{n^s}.$$

注意到

$$\left(1-\frac{1}{p^s}\right)^{-1}=1+\frac{1}{p^s}+\frac{1}{p^{2s}}+\frac{1}{p^{3s}}\cdots$$

所以我们有

$$\prod_p\left(1-\frac{1}{p^s}\right)^{-1}=\sum_{n=1}^{\infty}\frac{1}{n^s}. \tag{2-8}$$

函数

$$\zeta(s)=\sum_{n=1}^{\infty}\frac{1}{n^s}$$

称作*黎曼–ζ 函数*. 它可以延拓到整个复平面上, 并且除了 $s=1$ 是一级极点之外处处解析. 恒等式 (2-8) 将素数和解析函数密切关联起来. 此外, 黎曼函数的零点和素数的性质之间有着深刻的联系. 这一杰出的发现是由天才数学家黎曼首先获得的, 由此开创了解析数论. 他为数论引入了分析这一强大工具, 让我们能用复变函数的方法去有效地解决数论问题.

黎曼提出了如下著名的数学猜想. 这一猜想曾被纳入希尔伯特著名的 23 个问题中, 也是悬赏百万美元的千禧年七大数学难题之一.

问题 2.3.1 (黎曼猜想) $\zeta(s)$ *的非平凡零点都落在复平面上直线* $\mathrm{Re}(s)=\frac{1}{2}$ *上.*

这里所谓的非平凡零点是指那些不容易求出的零点 (易求的零点称为平凡零点). 如果黎曼猜想

能被证明, 那么将有许许多多重要且深刻的数论定理被证明.

解析数论能够解决很多数论难题. 这里我们介绍一个和素数个数有关的定理.

定理 2.3.4 (素数定理) 设 $\pi(x)$ 表示不超过实数 x 的素数的个数, 则

$$\lim_{x\to\infty}\frac{\pi(x)}{\left(\frac{x}{\log x}\right)}=1.$$

这个结论最早由高斯提出猜测. 切比晓夫首先给出突破性进展, 最终由阿达玛和 Paussin 几乎同时独立证明. 后来艾尔多斯和塞尔伯格给出了初等证明.

推论 2.3.7 $\lim_{x\to\infty}\frac{\pi(x)}{x}=0$, 即素数在正整数中出现的几率为零.

2.4 一次不定方程

我们关心以下方程的整数解 $(x_1,\cdots,x_m)$:

$$a_1x_1+a_2x_2+\cdots+a_mx_m=n,$$

这里诸 a_i 和 n 都是给定整数. 如果 $m=1$, 那么这就是我们前面所讨论的整除性. 以下我们先讨论 $m=2$ 的情形, 然后再将它推广到一般情形.

2.4.1 二元一次不定方程的求解算法

考虑不定方程

$$ax+by=n, \tag{2-9}$$

这里 a,b,n 是给定整数.

命题 2.4.1 方程 (2-9) 有整数解的充分必要条件是

$$(a,b)\mid n.$$

证明 ($\Longrightarrow$) 设 (x_0,y_0) 是整数解, 则由引理 2.2.3 得 $(a,b)\mid n(=ax_0+by_0)$.

($\Longleftarrow$) 设 $(a,b)\mid n$. 首先, 由推论 2.2.1, 存在 $s,t\in\mathbb{Z}$ 满足

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

今取 $x_0=s\cdot\frac{n}{(a,b)}$, $y_0=t\cdot\frac{n}{(a,b)}$. 则得方程 (2-9) 的一组解. ■

由上述命题, 我们只需要讨论 $(a,b)=1$ 的情形就足够了. 在这种情形下, 上述命题保证方程总是有解的. 我们甚至可以利用推论 2.2.4 来具体造出方程 (2-9) 的一组特解.

命题 2.4.2 设 $(a,b)=1$, x_0,y_0 满足方程 (2-9), 则方程 (2-9) 的通解公式为

$$\begin{cases}x\ =x_0+bt\\ y\ =y_0-at,\end{cases}$$

这里 t 取遍所有整数.

证明 由

$$ax + by = n, \quad ax_0 + by_0 = n$$

可得

$$a(x - x_0) + b(y - y_0) = 0.$$

因为 $(a, b) = 1$, 所以 $a \mid y - y_0$. 我们令 $t = \frac{y - y_0}{a}$, 则 $y = y_0 - at$, 且 $t \in \mathbb{Z}$. 由此可得 $x = x_0 + bt$.■

上面的讨论总结起来, 提供了求解二元一次不定方程的具体方法:

(1) 先判断 $(a, b) \mid n$ 是否成立.

(2) 将方程 (2-9) 化简成

$$\frac{a}{(a, b)}x + \frac{b}{(a, b)}y = \frac{n}{(a, b)}. \tag{2-10}$$

(3) 求出方程 (2-10) 的特解 (x_0, y_0).

(4) 求出通解.

例 2.4.1 (1) 求不定方程 $3x - 5y = 1$ 的通解.

显见 $(x_0, y_0) = (2, 1)$ 是一组特解. 因 $(3, 5) = 1$, 故由上面引理得通解公式

$$\begin{cases} x = 2 - 5t \\ y = 1 - 3t, \end{cases}$$

这里 t 取遍所有整数.

(2) 求不定方程 $4x + 6y = 10$ 的通解. 因 $(4, 6) \mid 10$, 故方程有解, 且可化简为

$$2x + 3y = 5.$$

$(x_0, y_0) = (1, 1)$ 显然是一组特解. 因此通解公式为

$$\begin{cases} x = 1 + 3t \\ y = 1 - 2t, \end{cases}$$

这里 t 取遍所有整数.

(3) 求方程 $3x + 7y = 46$ 的所有正整数解.

首先求得特解 $(x_0, y_0) = (-1, 7)$. 其次求出整数解通解公式

$$\begin{cases} x = -1 + 7t \\ y = 7 - 3t, \end{cases}$$

这里 t 取遍所有整数. 因为要求 $x > 0$, $y > 0$, 所以

$$-1 + 7t > 0, \quad 7 - 3t > 0$$

这就推出 $t = 1, 2$. 因此正整数解为 $(x, y) = (6, 4), (13, 1)$. ■

一般说来, 二元一次不定方程即使有整数解也未必存在非负整数解或正整数解. 比如 $3x + 5y = 4$ 就没有非负整数解 (为什么?).

推论 2.4.1 *设 $(a, b) = 1$, $a > 0, b > 0$. 如果 $n > ab - a - b$, 则方程 (2-9) 必有非负整数解; 如果 $n = ab - a - b$, 则方程没有非负整数解. 换言之, $ab - a - b$ 是最大的正整数不能由 $ax + by$ $(x \geq 0, y \geq 0)$ 表出者.*

证明 考虑方程 (2-9) 的整数解通解公式

$$x = x_0 + bt, \quad y = y_0 - at.$$

(1) 假设 $n > ab - a - b$. 由带余数除法, 我们可取 t 使得

$$0 \leq y_0 - at < a.$$

从而 $0 \leq y_0 - at \leq a - 1$. 因此

$$(x_0 + bt)a = n - b(y_0 - at) > ab - a - b - b(a - 1) = -a,$$

故 $x_0 + bt > -1$, 从而 $x_0 + bt \geq 0$. 这样, 我们就得到一组非负整数解.

(2) 假设 $n = ab - a - b$, 则方程 (2-9) 可写为

$$ab = (x + 1)a + (y + 1)b.$$

因 $(a, b) = 1$, 所以这就推出

$$a \mid (y + 1), \quad b \mid (x + 1).$$

如果 $x \geq 0, y \geq 0$, 则 $x + 1 \geq b$, $y + 1 \geq a$, 从而

$$ab = (x + 1)a + (y + 1)b \geq 2ab,$$

矛盾! 因此此时方程无非负整数解. ■

命题 2.4.3 *设 a, b 是正整数, c_n 是不定方程 $ax + by = n$ 的非负整数解的个数, 则我们有以下幂级数展式.*

$$\frac{1}{(1 - z^a)(1 - z^b)} = \sum_{n=0}^{\infty} c_n z^n$$

例 2.4.2 上述命题可以用来具体求解方程 (2-9) 的非负整数解个数. 这里举一个简单的例子. 考虑方程 $x + 2y = n$. 注意到

$$\frac{1}{(1 - z)(1 - z^2)} = \frac{1}{(1 - z)^2(1 + z)} = \frac{1}{4(1 - z)} + \frac{1}{2(1 - z)^2} + \frac{1}{4(1 + z)}.$$

因此幂级数展开上式可求得 z^n 的系数为

$$c_n = \frac{1}{4} + \frac{n + 1}{2} + \frac{(-1)^n}{4}.$$

另一方面, 我们也可以直接从方程得到 $c_n = [\frac{n}{2}] + 1$. ■

2.4.2 多元一次不定方程的求解算法

我们考虑不定方程

$$a_1 x_1 + \cdots + a_n x_n = N \tag{2-11}$$

的整数解 $(x_1, \cdots, x_n)$, 这里诸 a_i 和 N 是整数.

定理 2.4.1 *不定方程 (2-11) 有整数解的充分必要条件是*

$$(a_1, \cdots, a_n) \mid N.$$

证明 设 $d = (a_1, \cdots, a_n)$.

($\Longrightarrow$) 如果不定方程 (2-11) 有整数解 $(x_1,\cdots,x_n)$, 则由整除的加性性质可知

$$d \mid a_1x_1+\cdots+a_nx_n=N.$$

($\Longleftarrow$) 今假设 $d \mid N$, 我们要证方程 (2-11) 有整数解. 对 n 施归纳法. $n=1,2$ 时结论已证 (见命题 2.4.1). 今假设 $<n$ 的情形已证.

设 $d'=(a_1,\cdots,a_{n-1})$. 由最大公因子定义, $(d',a_n)=d$. 由命题 2.4.1, 因 $d \mid N$, 故存在整数对 (y,x_n) 满足

$$d'y+a_nx_n=N$$

又由归纳假设, 存在整数组 $(x_1,\cdots,x_{n-1})$, 满足

$$a_1x_1+\cdots+a_{n-1}x_{n-1}=d'y.$$

因此 $(x_1,\cdots,x_n)$ 满足方程 (2-11). ■

注 2.4.1　我们记

$$\langle a_1,\cdots,a_n\rangle=\{a_1x_1+\cdots+a_nx_n \mid x_1,\cdots,x_n\in\mathbb{Z}\}.$$

它称之为整数集 $\mathbb{Z}$ 中由 $a_1,\cdots,a_n$ 生成的理想. 由一个整数生成的理想称为主理想. 定理 2.4.1 就是说

$$\langle a_1,\cdots,a_n\rangle=\langle d\rangle,$$

这里 $d=(a_1,\cdots,a_n)$. 因此 $\mathbb{Z}$ 中任何理想都是主理想. ■

定理 2.4.1 提供了一种计算多元一次不定方程的归纳性解法. 这里我们以三元一次不定方程

$$ax+by+cz=n$$

为例, 来总结一下求解方法.

(1) 先判断 $(a,b,c) \mid n$, 然后将方程化简为 $(a,b,c)=1$ 的情形 (以下各步均作此假设).

(2) 设 $d=(a,b)$, 先求辅助方程

$$ax+by=d$$

的特解 (x_0,y_0).

(3) 再求辅助方程 $dw+cz=n$ 的一组特解 (w_0,z_0).

(4) 原方程通解

$$\begin{cases} x=x_0(w_0+ct)+\frac{b}{d}s,\\ y=y_0(w_0+ct)-\frac{a}{d}s,\\ z=z_0-dt, \end{cases}$$

这里 t,s 跑遍所有整数. 请注意, 一般说来, 通解公式的表达式不唯一, 这取决于参数的选取.

例 2.4.3　求方程 $4x+6y+12z=28$ 的所有整数解, 以及它的所有正整数解.

因为 $(4,6,12)=2 \mid 28$, 所以方程有解, 且可简化为

$$2x+3y+6z=14.$$

先求辅助方程

$$2x+3y=1$$

的特解 $(x_0, y_0) = (-1, 1)$. 再求辅助方程

$$w + 6z = 14$$

的一组特解 $(w_0, z_0) = (2, 2)$. 这就得到原方程组的通解公式

$$\begin{cases} x = -2 - 6t + 3s, \\ y = 2 + 6t - 2s, \\ z = 2 - t, \end{cases}$$

这里 t, s 跑遍所有整数. 如果 x, y, z 皆正整数, 则得不等式

$$-2 - 6t + 3s > 0, \quad 2 + 6t - 2s > 0, \quad 2 - t > 0.$$

因为 t, s 取整数, 所以只能有 $(t, s) = (1, 3)$, 从而 $(x, y, z) = (1, 2, 1)$. ■

类似二元一次方程情形, 我们也关心多元一次不定方程的非负整数解情形. 比如能否求出最大的正整数不能由

$$ax + by + cz$$

表出者 ($(a, b, c$ 是互质的正整数)? 这是至今未能彻底解决之难题. 又比如多元一次不定方程的非负整数解数是多少? (二元情形可精确求之, 亦可见习题 2.8 之近似解答). 仿照命题 2.4.3, 我们有

引理 2.4.1 设 $a_1, a_2, \cdots, a_n$ 皆正整数, 且 $(a_1, \cdots, a_n) = 1$, $A(N)$ 是方程 (2-11) 的非负整数解的个数. 那么

$$\frac{1}{(1 - z^{a_1})(1 - z^{a_2}) \cdots (1 - z^{a_n})} = \sum_{N=0}^{\infty} A(N) z^N.$$

对具体的方程, $A(N)$ 可以利用幂级数展开求得. 具体言之, 我们设

$$1, \zeta_1, \zeta_2, \cdots, \zeta_t$$

是方程 $(1 - z^{a_1})(1 - z^{a_2}) \cdots (1 - z^{a_n}) = 0$ 的所有不同的根, 它们的重数分别是

$$n, l_1, l_2, \cdots, l_n.$$

因为 $(a_1, \cdots, a_n) = 1$, 所以诸 $l_i \leq n - 1$.

由分部分式法得

$$\begin{aligned} &\frac{1}{(1 - z^{a_1})(1 - z^{a_2}) \cdots (1 - z^{a_n})} = \\ &\frac{A_n}{(1 - z)^n} + \cdots + \frac{A_1}{(1 - z)} + \frac{B_{l_1}}{(\zeta_1 - z)^{l_1}} + \cdots + \frac{B_1}{(\zeta_1 - z)} + \\ &\cdots + \cdots + \frac{C_{l_t}}{(\zeta_t - z)^{l_t}} + \cdots + \frac{C_1}{(\zeta_t - z)} \end{aligned} \tag{2-12}$$

注意到

$$\frac{A}{(\alpha - z)^l} = \frac{A}{\alpha^l} \left(1 - \frac{z}{\alpha}\right)^{-l}$$

的幂级数展开中 z^N 的系数

$$\psi(N)=\frac{A}{\alpha^{l+N}}\cdot\binom{N+l-1}{l-1}. \tag{2-13}$$

这样, 我们就可以求出 $A(N)$ 的精确表达式.

例 2.4.4　用上述方法可求得方程 $x+2y+3z=n$ 的非负整数解个数等于

$$\frac{(n+3)^2}{12}-\frac{7}{72}+\frac{(-1)^n}{8}+\frac{2}{9}\cos\frac{2n\pi}{3}.$$

具体验证留给读者. ■

有时候我们并不需要求 $A(N)$ 的精确式, 而只是希望估计 $A(N)$.

定理 2.4.2　*在引理 2.4.1 的条件下,我们有*

$$\lim_{N\to\infty}\frac{A(N)}{N^{n-1}}=\frac{1}{a_1a_2\cdots a_n\cdot(n-1)!}$$

证明　在式 (2-13) 中取 $\alpha=\zeta_i$, $l=l_i$, 则由 $|\alpha|=1$ 及 $l\leq n-1$ 推知

$$\lim_{N\to\infty}\frac{\psi(N)}{N^{n-1}}=0.$$

同理, 如取 $\alpha=1$, $l<n$, 上面的极限式也成立. 因此

$$\lim_{N\to\infty}\frac{A(N)}{N^{n-1}}=\frac{A_n}{(n-1)!},$$

这里 A_n 是分部分式 (2-12) 中 $(1-z)^{-n}$ 的系数. 由简单计算可知

$$A_n=\lim_{z\to1}\frac{(1-z)^n}{(1-z^{a_1})\cdots(1-z^{a_n})}=\frac{1}{a_1\cdots a_n}.$$

这就证明了结论. ■

2.5 同余式

在很多涉及带余数除法的问题中, 我们主要关心余数, 而对商并不太关心. 类似地, 在一次不定方程中, 我们主要关心特解, 因为通解很容易从特解求出. 因此我们可以引进一种便捷的记号—同余, 省略掉那些不太重要的信息, 进一步突出我们所要关心的对象.

2.5.1 同余与完全剩余系

定义 2.5.1　*设 $a,b,m\in\mathbb{Z}$, 且 $m>0$. 如果 $m\mid(a-b)$, 则称 a 与 b 对模 m 同余* (Congruent), *记为*

$$a\equiv b\pmod m.$$

反之, 如果 $m\nmid(a-b)$, 则记 $a\not\equiv b\pmod m$.

引理 2.5.1　*设*

$$a=mq_1+r_1,\quad b=mq_2+r_2,\quad 0\leq r_1,r_2<m$$

是带余数除法, 则 $a\equiv b\pmod m$ 当且仅当 $r_1=r_2$.

证明 由 $(a-b)=m(q_1-q_2)+(r_1-r_2)$, 我们有

$$a\equiv b \pmod m \Longleftrightarrow m\mid a-b \Longleftrightarrow m\mid r_1-r_2.$$

注意到 $0\le|r_1-r_2|<m$, 所以上面的最后一个条件 $m\mid r_1-r_2$ 也等价于 $r_1=r_2$. ■

例 2.5.1 (1) $31\equiv -9 \pmod{10}$. 这等价于说 $10\mid 31-(-9)$.
(2) $a\equiv b \pmod 1$, 对任何 $a,b\in\mathbb{Z}$ 成立. ■

命题 2.5.1 *同余关系是等价关系, 即满足以下三条性质:*
(1) (*自反性*) $a\equiv a \pmod m$.
(2) (*对称性*) $a\equiv b \pmod m$, *则* $b\equiv a \pmod m$.
(3) (*传递性*) *若* $a\equiv b \pmod m$ *且* $b\equiv c \pmod m$, *则* $a\equiv c \pmod m$.

证明 由引理 2.5.1 立得. ■

我们考虑集合

$$\begin{aligned}
\bar 0 &= \{mq+0 \mid q\in\mathbb{Z}\} = \{a \mid a\equiv 0 \pmod m\},\\
\bar 1 &= \{mq+1 \mid q\in\mathbb{Z}\} = \{a \mid a\equiv 1 \pmod m\},\\
&\vdots \qquad\qquad\qquad \vdots\\
\bar r &= \{mq+r \mid q\in\mathbb{Z}\} = \{a \mid a\equiv r \pmod m\},\\
&\vdots \qquad\qquad\qquad \vdots\\
\overline{m-1} &= \{mq+m-1 \mid q\in\mathbb{Z}\} = \{a \mid a\equiv m-1 \pmod m\}.
\end{aligned}$$

这些集合 $\bar 0,\cdots,\overline{m-1}$ 称为模 m 的*剩余类*. 所有剩余类的全体称作*完全剩余系*, 记作 $\mathbb{Z}_m$.

注 2.5.1 有时为方便起见, 我们也可以把剩余类 $\bar a$ 中的任一元素—比如 b, 挑出来作为代表元, 记作 $\bar b$. 它和 $\bar a$ 指代同一个剩余类. 比如模 2 的剩余类中, $\bar 1$ 和 $\bar 3$ 是同一个剩余类, 都表示全体奇数构成的集合; $\bar 0$ 和 $\bar 2$ 指同一剩余类, 即全体偶数构成的集合. 显然 $\bar 0,\bar 1$ 构成完全剩余系 $\mathbb{Z}_2$. ■

推论 2.5.1 *模 m 的剩余类恰好是同余关系诱导的等价类. 换言之, 它们满足以下性质:*
(1) $\bar a=\bar b$ *当且仅当* $a\equiv b \pmod m$.
(2) *若* $\bar a\ne\bar b$, *则* $\bar a\cap\bar b=\emptyset$.
(3) $\mathbb{Z}=\bar 0\cup\bar 1\cup\cdots\cup\overline{m-1}$.

证明 (1) 由引理 2.5.1 及定义即知.

(2) 若存在 $x\in\bar a\cap\bar b$, 则由定义知 $x\equiv a \pmod m, x\equiv b \pmod m$, 由传递性立得 $a\equiv b \pmod m$, 矛盾!

(3) 对任何整数 a, 考虑带余数除法 $a=mq+r$, $0\le r<m$. 因此 $a\in\bar r$. ■

命题 2.5.2 *设* $a_1\equiv b_1 \pmod m, a_2\equiv b_2 \pmod m$, *则*
(1) (*保加减运算*) $a_1\pm a_2\equiv b_1\pm b_2 \pmod m$.
(2) (*保乘法运算*) $a_1a_2\equiv b_1b_2 \pmod m$.
(3) (*保互质性*) *若* $(a_1,m)=1$, *则必有* $(b_1,m)=1$.

(4) (消去律) 若 $(a_1, m) = 1$, 且 $a_1 c \equiv b_1 d \pmod{m}$, 则 $c \equiv d \pmod{m}$.
(5) (乘法逆元) 若 $(a_1, m) = 1$, 则存在 $x \in \mathbb{Z}$, 使得 $a_1 x \equiv 1 \pmod{m}$, 并且 x 在模 m 的同余下是唯一的, 常记作 $a_1^{-1} \pmod{m}$.

证明 (1) 是显然的.

(2) 我们有

$$a_1 a_2 - b_1 b_2 = a_2(a_1 - b_1) + b_1(a_2 - b_2).$$

因 $m \mid a_1 - b_1$, $m \mid a_2 - b_2$, 故得 $m \mid a_1 a_2 - b_1 b_2$, 即 $a_1 a_2 \equiv b_1 b_2 \pmod{m}$.

(3) 设 $a_1 = mq + r$ 是带余数除法, 则 $1 = (a_1, m) = (r, m)$. 因 b_1 被 m 除的余数也是 r, 所以类似也可得 $(b, m) = (r, m) = 1$.

(4) $a_1 c - b_1 d = a_1(c - d) + (a_1 - b_1)d$. 因为 $m \mid a_1 c - b_1 d$, $m \mid a_1 - b_1$, 所以 $m \mid a_1(c - d)$. 又因为 $(a_1, m) = 1$, 故由消去律得 $m \mid c - d$, 即 $c \equiv d \pmod{m}$.

(5) 由推论 2.2.1, 存在 $x, y \in \mathbb{Z}$, 使得 $a_1 x + my = (a_1, m) = 1$, 即 $m(-y) = a_1 x - 1$. 这就推出 $m \mid a_1 x - 1$, 即 $a_1 x \equiv 1 \pmod{m}$. ■

上述命题翻译成剩余类的语言, 即指

推论 2.5.2 模 m 的完全剩余系 $\mathbb{Z}_m$ 上有自然诱导的加减乘运算.
(1) 加法: $\bar{a} + \bar{b} := \overline{a + b}$,
(2) 减法: $\bar{a} - \bar{b} := \overline{a - b}$,
(3) 乘法: $\bar{a} \cdot \bar{b} := \overline{ab}$.

如果 $(m, a) = 1$, 则还有求乘法逆元的运算:
(4) $\bar{a}^{-1} := \overline{a^{-1}}$.
这些运算不依赖于剩余类的代表元选取.

例 2.5.2 模 3 的剩余类有 $\bar{0}$, $\bar{1}$, $\bar{2}$. 我们有以下的剩余类加法和乘法表.

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{0}$	$\bar{1}$

$\times$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{1}$

此外, $\bar{2}^{-1} = \bar{2}$, $\bar{1}^{-1} = \bar{1}$, 但 $\bar{0}$ 没有乘法逆元. ■

推论 2.5.3 设 $k, l, m \in \mathbb{Z}$, 且 $(k, m) = 1$. 设

$$\bar{a}_0, \bar{a}_1, \cdots, \bar{a}_{m-1}$$

是模 m 的完全剩余系, 那么

$$\overline{ka_0 + l}, \overline{ka_1 + l}, \cdots, \overline{ka_{m-1} + l}$$

也是模 m 的完全剩余系.

证明 我们只需要证明诸 $\overline{ka_i + l}$ 两两不相同即可. 首先注意 $(k, m) = 1$, 因而 $\overline{k}^{-1}$ 存在. 假设 $\overline{ka_i + l} = \overline{ka_j + l}$, 则由

$$\bar{a}_i - \bar{a}_j = \overline{a_i - a_j} = \bar{k}^{-1} \cdot \overline{k(a_i - a_j)} = \bar{k}^{-1} \cdot \left(\overline{ka_i + l} - \overline{ka_j + l}\right) = \bar{0}.$$

这就证明了 $i=j$, 因而诸 $\overline{ka_i+l}$ 两两不相同. ■

2.5.2 既约剩余类与欧拉定理

设 $\bar{a}$ 是模 m 的剩余类, 如果 $(a,m)=1$, 则称 $\bar{a}$ 是与模 m 互质的剩余类. 由命题 2.5.2 (3), 上述定义不依赖于代表元 a 的选取. 所有与模 m 互质的剩余类全体构成的集合称作 *既约剩余系* (有时也称为*简化剩余系*), 记为 $\mathbb{Z}_m^*$. 显然 $\mathbb{Z}_m^* \subseteq \mathbb{Z}_m$. 与模 m 互质的剩余类个数记作 $\varphi(m)$, 它可以看成 m 的函数, 称为*欧拉函数*.

我们也可以按如下方式等价定义欧拉函数.

定义 2.5.2 *$\varphi(m)$ 就是指不超过 m, 且与 m 互素的正整数个数.*

例 2.5.3 (1) 取 $m=2$, 则既约剩余系 $\mathbb{Z}_m^*=\{\bar{1}\}$, $\varphi(2)=1$.
(2) 取 $m=6$, 则既约剩余系 $\mathbb{Z}_m^*=\{\bar{1},\bar{5}\}$, $\varphi(6)=2$.
(3) 取 $m=10$, 则既约剩余系 $\mathbb{Z}_m^*=\{\bar{1},\bar{3},\bar{7},\bar{9}\}$, $\varphi(10)=4$.
(4) 取 $m=p$ 是素数, 则既约剩余系 $\mathbb{Z}_m^*=\{\bar{1},\bar{2},\cdots,\overline{p-1}\}=\mathbb{Z}_m-\{\bar{0}\}$, $\varphi(p)=p-1$. ■

前面讨论过, $\mathbb{Z}_m$ 有诱导的加法和乘法运算. 但是该加法运算对 $\mathbb{Z}_m^*$ 不是封闭的. 比如模 3 的既约剩余系 $\mathbb{Z}_3^*=\{\bar{1},\bar{2}\}$, 显然 $\bar{1}+\bar{2}=\bar{0}\notin\mathbb{Z}_3^*$.

命题 2.5.3 *模 m 的既约剩余系 $\mathbb{Z}_m^*$ 关于乘法封闭, 并且对任何 $\bar{a}\in\mathbb{Z}_m^*$, 都有存在逆元 $\bar{a}^{-1}\in\mathbb{Z}_m^*$. 换言之, $\mathbb{Z}_m^*$ 是乘法群. 特别地, $\mathbb{Z}_m^*$ 上可以定义除法运算.*

证明 任取 $\bar{a},\bar{b}\in\mathbb{Z}_m^*$, 由定义知 $(a,m)=(b,m)=1$. 因此由消去律立得 $(ab,m)=1$, 即 $\bar{a}\bar{b}=\overline{ab}\in\mathbb{Z}_m^*$.

由命题 2.5.2 (5), 存在 a 的逆元 $x\in\mathbb{Z}_m$, 满足 $ax\equiv 1 \pmod m$, 因而 $m\mid(ax-1)$. 设 $d=(x,m)$, 则 $d\mid(ax-1)$ 推出 $d\mid 1$, 即 $d=1$. 这表明 $\bar{x}\in\mathbb{Z}_m^*$. ■

例 2.5.4 考虑 $\mathbb{Z}_{10}^*$ 上的乘法表.

$\times$	$\bar{1}$	$\bar{3}$	$\bar{7}$	$\bar{9}$
$\bar{1}$	$\bar{1}$	$\bar{3}$	$\bar{7}$	$\bar{9}$
$\bar{3}$	$\bar{3}$	$\bar{9}$	$\bar{1}$	$\bar{7}$
$\bar{7}$	$\bar{7}$	$\bar{1}$	$\bar{9}$	$\bar{3}$
$\bar{9}$	$\bar{9}$	$\bar{7}$	$\bar{3}$	$\bar{1}$

事实上, 可以验证 $\mathbb{Z}_{10}^*$ 是由 $\bar{3}$ 生成的循环群. 具体言之, $\bar{1}=\bar{3}^0=\bar{3}^4$, $\bar{3}=\bar{3}^1$, $\bar{9}=\bar{3}^2$, $\bar{7}=\bar{3}^3$. ■

类似推论 2.5.3, 我们有以下结论

推论 2.5.4 *设 $k,m\in\mathbb{Z}$, 且 $(k,m)=1$. 设*

$$\bar{a}_1,\bar{a}_2,\cdots,\bar{a}_{\varphi(m)}$$

是模 m 的既约剩余系, 那么

$$\overline{ka_1},\overline{ka_2},\cdots,\overline{ka_{\varphi(m)}}$$

也是模 m 的既约剩余系.

证明 与推论 2.5.3 的证明类似, 我们可推出诸 $\overline{ka_i}$ 两两不相同. 因此剩下只需证明 $\overline{ka_i}$ 是与模 m 互质的剩余类. 这是显然的, 因为 $(k,m)=(a_i,m)=1$, 所以 $(ka_i,m)=1$. ■

定理 2.5.1 (欧拉定理) 设 $k,m\in\mathbb{Z}$, $m>0$, 且 $(k,m)=1$, 则

$$k^{\varphi(m)}\equiv 1 \pmod{m}.$$

换言之, 对任何 $\bar{k}\in\mathbb{Z}_m^*$, 都有 $\bar{k}^{\varphi(m)}=\bar{1}$.

证明 考虑模 m 的既约剩余系

$$\bar{a}_1,\bar{a}_2,\cdots,\bar{a}_{\varphi(m)}.$$

由推论 2.5.4,

$$\overline{ka_1},\overline{ka_2},\cdots,\overline{ka_{\varphi(m)}}$$

也是模 m 的既约剩余系. 这就推出

$$\prod_{i=1}^{\varphi(m)} ka_i \equiv \prod_{i=1}^{\varphi(m)} a_i \pmod{m}.$$

因为 $(a_i,m)=1$, 所以由消去律及上式即得

$$k^{\varphi(m)}=\prod_{i=1}^{\varphi(m)} k\equiv 1 \pmod{m}.$$

这就完成了证明. ■

注 2.5.2 我们也可以从群论的角度去证明上述的欧拉定理. 由命题 2.5.3, $\mathbb{Z}_m^*$ 是乘法群, 它的阶数等于 $\varphi(m)$. 根据有限群的简单结果即得 $\bar{a}^{\varphi(m)}=\bar{1}$. ■

推论 2.5.5 (费马小定理) 设 p 是素数, 则对任何 $k\in\mathbb{Z}$, 都有

$$k^p\equiv k \pmod{p}.$$

证明 如果 $(k,p)=1$ (即 $p\nmid k$), 则在定理 2.5.1 中取 $m=p$ 即得

$$k^{p-1}\equiv 1 \pmod{p},$$

即 $k^p\equiv k \pmod{p}$.

如果 $p\mid k$, 即 $k\equiv 0 \pmod{p}$, 则结论是显然的. ■

注 2.5.3 我们后面将证明: 对任何素数 p, 模 p 的既约剩余系 $\mathbb{Z}_p^*=\mathbb{Z}_p-\{0\}$ 是循环群. ■

推论 2.5.6 设 $k,m\in\mathbb{Z}$, $m>0$, 且 $(k,m)=1$, 则 $k^{\varphi(m)-1}$ 在模 m 下是 k 的逆元, 即 $\bar{k}^{-1}=\bar{k}^{\varphi(m)-1}\in\mathbb{Z}_m^*$.

推论 2.5.7 设 $k,n,m\in\mathbb{Z}$, $m>0$, $(m,k)=1$. 设 $n=\varphi(m)q+r$ $(0\le r<q-1)$ 是 n 除以 $\varphi(m)$ 的带余数除法, 则

$$k^n\equiv k^r \pmod{m}.$$

证明

$$k^n\equiv k^{\varphi(m)q+r}\equiv (k^{\varphi(m)})^q\cdot k^r\equiv k^r \pmod{m}.$$

2.5.3 一些简单的应用

这里我们例举一些和同余有关的计算题以及相关的应用.

例 2.5.5 (1) 求 3 在模 10 下的逆元.

因为 $\varphi(10)=4$, 所以由推论 2.5.6 得

$$3^{-1}\equiv 3^{\varphi(10)-1}\equiv 3^3\equiv 7 \pmod{10}.$$

(2) 求 13 在模 17 下的逆元.

因为 17 是素数, 故 $\varphi(17)=16$, 所以由推论 2.5.6 得

$$13^{-1}\equiv 3^{\varphi(17)-1}\equiv 13^{15}\equiv(-4)^{15}\equiv -4\cdot 4^{14}\equiv -4\cdot 16^7\equiv -4\cdot(-1)^7\equiv 4 \pmod{17}.$$

例 2.5.6 设 p 是奇素数.

(1) 求最小的正整数 x, 使得 $2x\equiv 1 \pmod{p}$.

利用带余数除法的唯一性, 我们相当于要求正整数 $x<p$ 使得

$$x\equiv 2^{-1}\equiv 2^{p-2} \pmod{p}.$$

. 由费马小定理知 $2^{p-1}\equiv 1\equiv 1+p \pmod{p}$. 注意到 $1+p$ 是偶数, 所以由消去律得

$$2^{p-2}\equiv \frac{p+1}{2} \pmod{p}.$$

因此有 $x=\frac{p+1}{2}$.

(2) 设 $p>3$, 求最小的正整数 x, 使得 $3x\equiv 1 \pmod{p}$.

由费马小定理知 $3^{p-1}\equiv 1\equiv 1+kp \pmod{p}$. 这里

$$k=\begin{cases} 1, \text{如果 } p\equiv 2 \pmod 3,\\ 2, \text{如果 } p\equiv 1 \pmod 3.\end{cases}$$

显见 $3\mid 1+kp$. 注意到 $(3,p)=1$, 故由消去律可得

$$x\equiv 3^{-1}\equiv 3^{p-2}\equiv \frac{1+kp}{3} \pmod{p}.$$

因而 $x=\frac{1+kp}{3}$. ■

例 2.5.7 (1) 求 3^{103} 的末位数.

这相当于求最小正整数 x, 使得 $x\equiv 3^{103} \pmod{10}$. 注意到 $\varphi(10)=4$, 所以由推论 2.5.7,

$$3^{103}\equiv 3^{4\times 25+3}\equiv 3^3\equiv 7 \pmod{10}.$$

因此末尾数 $x=7$.

(2) 求 2^{103} 的末位数.

这相当于求最小正整数 x, 使得 $x\equiv 2^{103} \pmod{10}$. 此时 $(2,10)=2$, 因而不能直接使用推论 2.5.7. 但我们注意到

$$2^{4k}\equiv (2^4)^k\equiv 6^k\equiv 6 \pmod{10},\quad \forall k\in\mathbb{Z}^+.$$

所以

$$2^{103}=2^{4\times 25+3}=6\cdot 2^3\equiv 8 \pmod{10}.$$

因此末尾数 $x=8$.

(3) 求最小的正整数 x, 使得 $x\equiv 5^{5^{10}} \pmod 7$.

因 $\varphi(7)=6$, 所以由推论 2.5.7, 我们要先求最小的正整数 r, 使得 $r\equiv 5^{10} \pmod 6$. 显见

$$r\equiv (-1)^{10}\equiv 1 \pmod 6,$$

即 $r=1$. 这样, 我们有 $x\equiv 5^r\equiv 5 \pmod 7$, 即 $x=5$. ■

例 2.5.8 (1) 证明: $\frac{1}{5}n^5+\frac{1}{3}n^3+\frac{7}{15}n$ 是整数.

这等价于证明 $15\mid 3n^5+5n^3+7n$. 我们先证 $3\mid 3n^5+5n^3+7n$. 此时

$$3n^5+5n^3+7n\equiv 5n^3+7n\equiv 2n^3-2n\equiv 2(n^3-n)\equiv 0 \pmod 3.$$

上式最后一步使用了费马小定理.

其次证明 $5\mid 3n^5+5n^3+7n$. 此时

$$3n^5+5n^3+7n\equiv 3n^5+7n\equiv 3n^5-3n\equiv 3(n^5-n)\equiv 0 \pmod 5.$$

这就完成了证明.

(2) 证明: $24\mid n(n+1)(n+2)(n+3)$.

我们先证明 $3\mid n(n+1)(n+2)(n+3)$. 此时

$$n(n+1)(n+2)(n+3)\equiv n(n+1)(n-1)n\equiv n^2(n^2-1)\equiv n(n^3-n)\equiv 0 \pmod 3.$$

其次证明 $8\mid n(n+1)(n+2)(n+3)$. 如果 $n=2m$, 则

$$n(n+1)(n+2)(n+3)=4m(m+1)(2m+1)(2m+3),$$

注意到 $2\mid m(m+1)$, 即得结论.

如果 n 是奇数, 则利用 $n^2\equiv 1 \pmod 8$ 得

$$n(n+1)(n+2)(n+3)=(n^2+2n)(n^2+4n+3)\equiv 4(1+2n)(n+1)\equiv 0 \pmod 8.$$

上式最后一步用到 $2\mid n+1$. ■

以下我们介绍同余在 p 进位制表达中的应用. 设 $a,p\in\mathbb{Z}^*$, $p>1$. 考虑 a 的 p 进位制表达式

$$a=a_np^n+a_{n-1}p^{n-1}+\cdots+a_1p+a_0,\quad 0\le a_i\le p-1,\quad i=1,2,\cdots,n.$$

有时也简记做 $a=(\overline{a_na_{n-1}\cdots a_1a_0})_p$. 设

$$s_p(a):=a_n+a_{n-1}+\cdots+a_1+a_0,$$

它称作 a 在 p 进位制下的*位数码和*.

比如

$$2^7=(\overline{128})_{10}=(\overline{10000000})_2.$$

因此 $s_{10}(2^7)=1+2+8=11$, $s_2(2^7)=1$.

日常生活中最常见的是十进制表达, 但在计算机中则以二进制表达为主. 为方便起见, 当我们考虑十进制时, 省略下标 10 以及上划线, 即仍采用通常的写法.

引理 2.5.2　设 a, p 同上.

(1) $a \equiv s_p(a) \pmod{p-1}$, 特别地, 序列

$$a, s_p(a), s_p(s_p(a)), s_p(s_p(s_p(a))), \cdots \tag{2-14}$$

是递减的, 且各项在模 $p-1$ 下彼此同余.

(2) 设 q 是 $(p-1)$ 的任何正因子, 则 $a \equiv s_p(a) \pmod{q}$. 特别地, $q \mid a$ 当且仅当 $q \mid s_p(a)$.

(3) $p+1 \mid a$ 当且仅当 $p+1 \mid \sum_{i=0}^{n}(-1)^i a_i$.

证明　(1) 注意到 $p^i \equiv 1 \pmod{p-1}$, 所以

$$a = a_n p^n + a_{n-1}p^{n-1} + \cdots + a_1 p + a_0 \equiv a_n + a_{n-1} + \cdots + a_1 + a_0 = s_p(a) \pmod{p-1}.$$

此外, $a - s_p(a) = \sum_{i=0}^{n} a_i(p^i - 1) \geq 0$, 从而 $a \geq s_p(a)$.

由递归地证明可知序列 (2-14) 在模 $p-1$ 下彼此同余.

(2) 由 (1) 得 $a \equiv s_p(a) \pmod{q}$. 因此

$$a \equiv 0 \pmod{q} \Longleftrightarrow s_p(a) \equiv 0 \pmod{q}.$$

(3) 注意到 $p^i \equiv (-1)^i \pmod{p+1}$, 所以

$$a \equiv a_n(-1)^n + a_{n-1}(-1)^{n-1} + \cdots - a_1 + a_0 \pmod{p+1}.$$

由此易得结论. ■

例 2.5.9　以下仅讨论十进制表达情形.

(1) 求 $n = 1234567$ 被 3 除的余数.

由引理 2.5.2, 此时 $3 \mid 9(= 10-1)$, 故 $n \equiv s_{10}(n) \pmod{3}$. 易知 $s_{10}(n) = 28 \equiv 1 \pmod{3}$. 因此余数是 1.

(2) (弃九算法) 任给正整数 n, 为求 n 除以 9 的余数, 我们可以考虑递减序列 (2-14), 它最终收敛于所要求的余数.

比如设 $n = 598765432$, 递减序列 (2-14) 如下

$$598765432, \quad 49, \quad 13, \quad 4.$$

因此余数是 4.

(3) 判断 $n = 1234567$ 是否被 11 整除.

由引理 2.5.2 (3), 我们只需求位数码的交错和 $1-2+3-4+5-6+7 = 4$, 即知 $11 \nmid n$. ■

作为同余的另一个应用, 我们证明如下的经典算术结果.

推论 2.5.8　任何正有理数 $r = p/q$ 的十进位制小数表达式一定会出现循环.

证明　不妨设 $(p, q) = 1$, $q = 2^\alpha 5^\beta q'$, $(q', 10) = 1$, $\alpha, \beta \geq 0$. 取

$$r' = 10^{\alpha+\beta} r = \frac{2^\beta 5^\alpha p}{q'}.$$

设 $p' = 2^\beta 5^\alpha p$. 显然 $(p', q') = 1$. 为证 r 的小数表示中会出现循环, 我们只需要证 r' 的小数表示会出现循环即可. 这是因为 r' 无非是将 r 的小数点往右移动了有限位.

因此不失一般性, 我们可以假设 $(q,10)=(p,q)=1$. 因为 $\{r\}=r-[r]$ 与 r 仅相差一个整数, 即在小数表达中只相差小数点前的部分, 所以我们可以不妨假设 $0<r<1$, 即 $0<p<q<1$.

设 $n=\varphi(q)$. 由欧拉定理, $10^n\equiv 1 \pmod q$, 即存在 $u\in\mathbb{Z}$, 使得 $10^n-1=qu$. 因 $p<q$, 所以 $pu<qu=10^n-1$. 现在我们有

$$r=\frac{pu}{10^n-1}=pu\cdot\frac{\frac{1}{10^n}}{1-\frac{1}{10^n}}=pu\sum_{k=1}^{\infty}\frac{1}{10^{kn}}=\sum_{k=1}^{\infty}\frac{pu}{10^{kn}}.$$

如将 pu 写成十进位制表示 $pu=\overline{a_{n-1}a_{n-2}\cdots a_1a_0}$ 代入上式, 即得

$$r=0.\overline{a_{n-1}a_{n-2}\cdots a_1a_0a_{n-1}a_{n-2}\cdots a_1a_0\cdots}.$$

这就证明了 r 的小数表达式是循环的. ■

例 2.5.10　已知 2012 年 1 月 1 日是星期日, 问当年的 1 月 31 日是星期几?

因为 $31\equiv 3 \pmod 7$, 所以 1 月 31 日与 1 月 3 日的星期数一致. 由于 1 月 1 日是星期日, 所以 1 月 3 日是星期二, 因此 1 月 31 日也是星期二. ■

注 2.5.4 (Zeller **公式**)　我们可以按照如下公式计算任何一天是星期几 (要求在 1582 年 10 月 15 日之后). 设公元 $(c+1)$ 世纪 y 年 m 月 d 日是星期 w, 这里要求 $y<100$ (即年数的末两位), $3\le m\le 14$ (一、二月视作 13, 14 月), 则

$$w\equiv y+\left[\frac{y}{4}\right]+\left[\frac{c}{4}\right]-2c+\left[\frac{13(m+1)}{5}\right]+d-1 \pmod 7.$$

比如考虑 2001 年 9 月 11 日. 此时, $c=20$, $y=1$, $m=9$, $d=11$, 我们有 $w=2$, 即当天是星期二. 又比如 1949 年 10 月 1 日是星期六. ■

2.5.4　欧拉函数的公式算法

引理 2.5.3　*设 m,n 是互质的正整数,*

$$\bar{a}_1,\cdots,\bar{a}_m$$

是模 m 的完全剩余系,

$$\bar{b}_1,\cdots,\bar{b}_n$$

是模 n 的完全剩余系, 则

$$\{\overline{mb_i+na_j}\mid i=1,\cdots,n,\quad j=1,\cdots,m\}.$$

恰好构成模 mn 的完全剩余系.

证明　我们只需说明诸 $\overline{mb_i+na_j}$ 两两不同. 假设 $\overline{mb_i+na_j}=\overline{mb_k+na_l}$, 即

$$mb_i+na_j\equiv mb_k+na_l \pmod{mn},$$

因此

$$mb_i+na_j\equiv mb_k+na_l \pmod m.$$

这就推出 $na_j\equiv na_l \pmod m$. 由 $(m,n)=1$ 及消去律得 $a_j\equiv a_l \pmod m$. 同理 $b_i\equiv b_k \pmod n$. ■

引理 2.5.4　设 m,n 是互质的正整数,

$$\bar{a}_1,\cdots,\bar{a}_{\varphi(m)}$$

是模 m 的既约剩余系,

$$\bar{b}_1,\cdots,\bar{b}_{\varphi(n)}$$

是模 n 的既约剩余系, 则

$$\{\overline{mb_i+na_j}\mid i=1,\cdots,\varphi(n),\quad j=1,\cdots,\varphi(m)\}.$$

恰好构成模 mn 的既约剩余系.

证明　由引理 2.5.3, 诸 $\overline{mb_i+na_j}$ 两两不同.

(1) 我们先验证 $(mb_i+na_j,mn)=1$. 首先

$$(mb_i+na_j,m)=(na_j,m)=(a_i,m)=1.$$

同理可证 $(mb_i+na_j,n)=1$. 因此 $\overline{mb_i+na_j}$ 是既约剩余系中的元素.

(2) 设 c 是任一与 mn 互质的整数. 由引理 2.5.3, 存在 a_j,b_i 使得 $c\equiv mb_i+na_j\pmod{mn}$. 因为 $(c,m)=(n,m)=1$, 所以

$$(a_j,m)=(na_j,m)=(mb_i+na_j,m)=1.$$

同理有 $(b_i,n)=1$. 因此既约剩余系中的每个元素都可以表述成形如 $\overline{mb_i+na_j}$ 的形式. ■

注 2.5.5　引理 2.5.3 等价于说 $\mathbb{Z}_m\oplus\mathbb{Z}_n\cong\mathbb{Z}_{mn}$. ■

推论 2.5.9　设 $(m,n)=1$, 则 $\varphi(mn)=\varphi(m)\varphi(n)$.

证明　由引理 2.5.4, 形如 $\overline{mb_i+na_j}$ 的剩余类恰有 $\varphi(m)\varphi(n)$ 个. 另一方面, 既约剩余系有 $\varphi(mn)$ 个元素. 因此得等式. ■

引理 2.5.5　设 p 是素数, $\ell>0$, 则

$$\varphi(p^\ell)=p^\ell-p^{\ell-1}=p^\ell\left(1-\frac{1}{p}\right).$$

证明　不超过 p^ℓ 且与 p^ℓ 互质的正整数就是那些小于 p^ℓ 且与 p 互质的正整数. 由此立得结论. ■

定理 2.5.2　设 $m=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_s^{\alpha_s}$ 是标准分解式, 则

$$\varphi(n)=n\cdot\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_s}\right).$$

证明　由推论 2.5.9 与引理 2.5.5, 我们有

$$\varphi(m)=\prod_{i=1}^{s}\varphi(p_i^{\alpha_i})=\prod_{i=1}^{s}\left(p_i^{\alpha_i}\left(1-\frac{1}{p_i}\right)\right)=n\prod_{i=1}^{s}\left(1-\frac{1}{p_i}\right).$$

这就完成了证明. ■

例 2.5.11 (1) $\varphi(300) = 300(1-\frac{1}{2})(1-\frac{1}{3})(1-\frac{1}{5}) = 80.$

(2) $\varphi(105) = 105(1-\frac{1}{3})(1-\frac{1}{5})(1-\frac{1}{7}) = 48.$ ■

命题 2.5.4

$$n = \sum_{d|n} \varphi(d) = \sum_{d|n} \varphi\left(\frac{n}{d}\right),$$

这里 $\sum_{d|n}$ 指 d 跑遍 n 中所有的正因子.

证明 对 n 的任何因子 d, 设

$$\Sigma_d = \{a \mid d = (a,n), \quad 1 \le a \le n\}.$$

显然诸 Σ_d 两两不相交, 并且它们的并就是集合 $\{1,2,\cdots,n\}$.

另一方面, $d = (a,n)$ 等价于 $(\frac{a}{d}, \frac{n}{d}) = 1$, 因而 $\frac{a}{d}$ 是不超过 $\frac{n}{d}$ 且与 $\frac{n}{d}$ 互质的正整数. 因此 Σ_d 中共有 $\varphi(\frac{n}{d})$ 个元素. 这就得到

$$n = \sum_{d|n} \varphi\left(\frac{n}{d}\right).$$

以 d 代替 $\frac{n}{d}$, 则得另一等式. ■

2.6 一次同余方程 (组)

2.6.1 一元一次同余方程的求解算法

在这一节中, 我们要讨论同余方程

$$ax \equiv b \pmod{m} \tag{2-15}$$

的剩余类解. 从 $\mathbb{Z}_m$ 的角度看, 就是求方程

$$\bar{a}\bar{x} = \bar{b}$$

的解 $\bar{x} \in \mathbb{Z}_m$.

例 2.6.1 (1) $3x \equiv 1 \pmod 5$ 有唯一的剩余类解 $x \equiv 2 \pmod 5$. 换言之, $\bar{2}$ 是 $\bar{3}$ 的逆.

(2) $2x \equiv 1 \pmod 4$ 没有剩余类解. ■

命题 2.6.1 以下条件彼此等价:

(1) 同余方程 $ax \equiv b \pmod m$ 有剩余类解,

(2) 不定方程 $ax + my = b$ 整数解 (x,y),

(3) $(a,m) \mid b$.

证明 由命题 2.4.1, (2) 和 (3) 是等价的.

(1) $\Longleftrightarrow$ (2) 此时 $m \mid ax - b$. 设 $y = -\frac{ax-b}{m}$, 则 (x,y)是方程 $ax + my = b$ 的整数解.

(2) $\Longleftrightarrow$ (1) 此时 $m(-y) = ax - b$ 蕴含着 $m \mid ax - b$, 即 $ax \equiv b \pmod m$. ■

推论 2.6.1 若 $(a,m) = 1$, 则同余方程 $ax \equiv b \pmod m$ 有唯一的剩余类解, $x \equiv a^{-1}b \pmod m$, 这里 a^{-1} 是 a 模 m 的逆元. 换言之, 存在唯一的非负整数 $x < m$, 满足上述同余方程.

例 2.6.2　求 $3x \equiv 4 \pmod{17}$ 的同余解.

解法一: 因为 $(3,17)=1$, 所以

$$x \equiv 3^{-1}\cdot 4 \equiv 3^{16-1}\cdot 4 \equiv 27^5\cdot 4 \equiv 10^5\cdot 4 \equiv 100^2\cdot 10\cdot 4 \equiv (-2)^2\cdot 40 \equiv 160 \equiv 7 \pmod{17}.$$

解法二: 因为 $-14x \equiv 3x \equiv 4 \pmod{17}$, 所以由消去律得 $-7x \equiv 2 \pmod{17}$. 因此

$$x \equiv -2(3x) - (-7x) \equiv -2(4) - 2 \equiv 7 \pmod{17}.$$

命题 2.6.2　*设 $d=(a,m)\mid b$, 则同余方程 (2-15) 在模 m 下恰有 d 个剩余类解. 换言之, 恰好存在 d 个非负整数 $x<m$ 满足上述同余方程.*

证明　由推论 2.6.1, 存在唯一的非负整数 $x_0<m$ 满足 $\frac{a}{d}x_0 \equiv \frac{b}{d} \pmod{\frac{m}{d}}$. 设

$$x_k = x_0 + k\cdot\frac{m}{d},$$

这里 $k=0,1,\cdots,d-1$. 显然

$$ax_k \equiv \frac{a}{d}(dx_0+km) \equiv ax_0 \equiv b \pmod{m}.$$

所以 $x\equiv x_k \pmod{m}$ 是同余方程 (2-15) 的解, 且可验证它们在模 m 下彼此不同余.

设 x 是满足同余方程 (2-15) 及 $x<m$ 的非负整数, 因而它也满足

$$\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{m}{d}}. \tag{2-16}$$

由推论 2.6.1, 我们得到 $x\equiv x_0 \pmod{\frac{m}{d}}$, 因此 $x=x_k$, 对某个整数 k. 由于 $0\le x<m$, 所以 $0\le k<d$. 这表明同余方程 (2-15) 在模 m 下恰有 d 个互不同余的剩余类解

$$x \equiv x_0, x_1, \cdots, x_{d-1} \pmod{m}.$$

至此, 我们完成证明. ■

上面的命题证明提供了求解一元一次同余方程 (2-15) 的方法:

(1) 先判断 $d=(a,m)\mid b$ 是否成立;

(2) 求辅助同余方程

$$\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{m}{d}}$$

在模 $\frac{m}{d}$ 下的剩余类解 $x\equiv x_0 \pmod{\frac{m}{d}}$.

(3) 原同余方程的全部剩余类解为

$$x \equiv x_0,\quad x_0+\frac{m}{d},\cdots,x_0+k\cdot\frac{m}{d},\cdots,x_0+(d-1)\cdot\frac{m}{d}. \pmod{m}$$

例 2.6.3　求同余方程 $12x\equiv 16 \pmod{68}$ 所有剩余类解.

因为 $(12,68)=4\mid 16$, 所以同余方程有解. 先考虑辅助同余方程

$$3x \equiv 4 \pmod{17}.$$

由例 2.6.2, $x\equiv 7 \pmod{17}$. 因此原同余方程的全部剩余类解为

$$x \equiv 7,\quad 7+17,\quad 7+2\cdot 17,\quad 7+3\cdot 17 \pmod{68},$$

即 $x\equiv 7,24,41,58 \pmod{68}$. ■

由命题 2.6.1, 求同余方程的解等价于求一次不定方程的解; 而利用同余方程求解往往比较容易, 比如我们可以利用欧拉定理等等 (见例 2.6.2). 这就提供了求解一次不定方程 $ax+by=n$ 的简便方法:

(1) 设 $d=(a,b)\mid n$. 先简化方程

$$\frac{a}{d}x+\frac{b}{d}y=\frac{n}{d}.$$

(2) 求一整数 x_0 满足同余方程 $\frac{a}{d}x_0\equiv\frac{n}{d}\pmod{\frac{b}{d}}$.

(3) 设 $y_0=\frac{n-ax_0}{b}$, 则得不定方程 $ax+by=0$ 之特解, 并由此得通解

例 2.6.4 (1) 求不定方程 $33x-17y=12$ 的通解.

考虑辅助同余方程

$$33x\equiv 12 \pmod{17}.$$

易知

$$x\equiv -33x\equiv -12\equiv 5 \pmod{17}.$$

故可取特解 $x_0=5, y_0=9$. 由此立得通解公式

$$\begin{cases} x=5+17t,\\ y=9-33t, \end{cases}$$

这里 t 取遍所有整数.

(2) 求不定方程 $14x+26y=10$ 的通解.

首先化简方程

$$7x+13y=5.$$

由辅助同余方程

$$7x\equiv 5 \pmod{13}.$$

可得

$$x\equiv 2(7x)\equiv 10 \pmod{13}.$$

因此可取不定方程的特解 $(x_0,y_0)=(10,-5)$. 由此得通解公式

$$\begin{cases} x=10+13t\\ y=-5-7t, \end{cases}$$

这里 t 取遍所有整数. ■

我们也可以进一步将同余方程方法应用到三元一次不定方程

$$ax+by+cz=n. \tag{2-17}$$

为方便讨论, 不妨假设 $(a,b,c)=1$, 且 $abc\neq 0$. 设 $d=(a,b)$. 我们暂时将 z 视作常数, 这就有二元一次不定方程

$$\frac{a}{d}x+\frac{b}{d}y=\frac{n-cz}{d}. \tag{2-18}$$

以上方程有解当且仅当 $\frac{n-cz}{d}$ 是整数, 即 $cz\equiv n \pmod{d}$. 因为 $(c,d)=1$, 所以该同余方程有唯

一的剩余类解 $z \equiv z_0 \pmod{d}$. 设

$$z = z_0 - dt, \quad w = \frac{n - cz}{d} = \frac{n - cz_0}{d} + dt, \quad t \in \mathbb{Z}, \tag{2-19}$$

代入方程 (2-18), 则得

$$\frac{a}{d}x + \frac{b}{d}y = w. \tag{2-20}$$

将 w 视作常数, 类似前面的方法, 我们可求方程 (2-20) 的通解

$$\begin{cases} x = x_0 + \frac{b}{d}s \\ y = y_0 - \frac{a}{d}s, \end{cases}$$

其中 x_0, y_0 是 w 的线性函数, s 跑遍所有整数. 由此及式 (2-19) 即得原方程 (2-17) 的通解.

例 2.6.5　求方程 $9x + 24y - 5z = 1000$ 的通解公式.

解法一: 将 z 暂视作常数, 得

$$3x + 8y = \frac{1000 + 5z}{3}.$$

因此方程有解的充要条件是 $5z \equiv -1000 \pmod{3}$, 即 $z \equiv 1 \pmod{3}$. 设

$$z = 1 - 3t, w = \frac{1000 + 5}{3} + 3t = 335 + 3t, \quad t \in \mathbb{Z},$$

代入原方程得

$$3x + 8y = w. \tag{2-21}$$

考虑辅助方程 $3x \equiv w \pmod{8}$, 则有

$$x \equiv 3(3x) \equiv 3w \pmod{8}.$$

因而上面的不定方程 (2-21) 有通解公式

$$\begin{cases} x = 3w + 8s, \\ y = -w - 3s, \end{cases}$$

此处 s 跑遍所有整数. 因此原方程通解为

$$\begin{cases} x = 3(335 + 3t) + 8s, \\ y = -(335 + 3t) - 3s, \\ z = 1 - 3t, \end{cases}$$

这里 t, s 取遍所有整数.

解法二: 用第 2.4.2 节介绍的归纳方法, 这里不再赘述. ■

2.6.2　多元一次同余方程的求解算法

上一节的内容很容易推广到多元情形.

命题 2.6.3　以下条件彼此等价:

(1) 同余方程

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n \equiv b \pmod{m} \tag{2-22}$$

有剩余类解,
(2) 不定方程 $a_1x+\cdots+a_nx_n+mx_{n+1}=b$ 整数解 $(x_1,\cdots,x_{n,x_{n+1}})$,
(3) $d:=(a_1,\cdots,a_n,m)\mid b$.

当以上条件之一成立时, 同余方程 (2-22) 在模 m 下恰有 $m^{n-1}d$ 个不同的剩余类解.

证明 这里我们只证明同余方程的剩余类解数在模 m 下恰好是 $m^{n-1}d$. 其余结论的证明与前一节类似, 此处不再赘述.

对变元个数 n 施归纳法. $n=1$ 前面已证, 今假设 $<n$ 的情形已证.

设 $d'=(a_1,\cdots,a_{n-1},m)$. 将 x_n 暂视为常数, 同余方程 (2-22) 有解当且仅当 $d'\mid b-a_nx_n$, 即 $a_nx_n\equiv b\pmod{d'}$, 它也等价于

$$a_n\cdot\frac{m}{d'}x_n\equiv b\cdot\frac{m}{d'}\pmod{m},$$

因此该方程在模 m 下共有 $(a_n\cdot\frac{m}{d'},m)=d\cdot\frac{m}{d'}$ 个剩余类解. 换句话说, 满足 $a_nx_n\equiv b\pmod{d'}$、0 及 $x_n<m$ 的非负整数解恰有 $d\cdot\frac{m}{d'}$ 个. 命 x_n 是其任一解, $b'=\frac{b-a_nx_n}{d'}$, 则由归纳假设, 同余方程

$$a_1x_1+\cdots+a_{n-1}x_{n-1}\equiv b'd'\pmod{m}$$

在模 m 下恰有 $m^{n-2}d'$ 个剩余类解. 综合以上讨论, 原方程 (2-22) 的总解数

$$m^{n-2}d'\cdot\frac{md}{d'}=m^{n-1}d.$$

因此由归纳法可知上述结论对任何 n 成立. ■

例 2.6.6 求同余方程

$$6x+9y\equiv 1\pmod{4}$$

的剩余类解.

因为 $1=(6,9,4)$, 所以方程有解. 先将 y 暂视作常数, 则方程

$$6x\equiv 1-9y\pmod{4}\tag{2-23}$$

有解当且仅当 $2=(6,4)\mid 1-9y$, 即 $y\equiv 1\pmod{2}$, 亦即 $y\equiv 1,3\pmod{4}$. 令 $z=\frac{1-9y}{2}$, 代入方程 (2-23) 得

$$2x\equiv 2z\pmod{4},$$

解得 $x\equiv z,z+2\pmod{4}$. 这样我们得到原方程在模 4 下四组剩余类解:

$$\begin{cases}x\equiv 2\pmod{4},\\ y\equiv 1\pmod{4}.\end{cases}\quad\begin{cases}x\equiv 0\pmod{4},\\ y\equiv 1\pmod{4}.\end{cases}\quad\begin{cases}x\equiv 1\pmod{4},\\ y\equiv 3\pmod{4}.\end{cases}\quad\begin{cases}x\equiv 3\pmod{4},\\ y\equiv 3\pmod{4}.\end{cases}$$ ■

利用多元一次同余方程求解, 我们也可以求多元一次不定方程的通解.

例 2.6.7 (1) 求方程 $9x+24y-5z=1000$ 的通解公式. 例 2.6.5 已经给出了此方程一类解方法. 这里讨论另一解法, 它比前者更为简便.

该方程的求解可转化为同余方程

$$9x+24y\equiv 0\pmod{5}$$

的求解. 将 y 暂视为常数, 则显然有

$$x\equiv-(9x)\equiv 24y\equiv-y\pmod{5}.$$

因此我们令 $y=s, x=-s+5t$, 代入原不定方程即得通解公式

$$\begin{cases} x=-s+5t, \\ y=s, \\ z=-200-3s+9t, \end{cases}$$

这里 s,t 跑遍所有整数.

(2) 求方程 $6x+9y+4z=1$ 的通解公式. 该方程的求解可转化为同余方程

$$6x+9y\equiv 1 \pmod 4 \tag{2-24}$$

的求解. 将 y 暂视为常数, 则方程 (2-24) 有解当且仅当 $y\equiv 1 \pmod 2$. 此时方程 (2-24) 可以约化为

$$3x\equiv \frac{1-9y}{2} \pmod 2.$$

因此 $x\equiv \frac{1-9y}{2}\equiv \frac{1-y}{2} \pmod 2$. 令

$$s=\frac{1-y}{2}, t=\frac{x-s}{2},$$

代入原不定方程即得通解

$$\begin{cases} x=s+2t, \\ y=1-2s, \\ z=-2+3s-3t, \end{cases}$$

这里 s,t 跑遍所有整数. ■

这里总结一下上例中求三元不定方程

$$ax+by+cz=n, \quad abc\neq 0, \quad (a,b,c)=1$$

的方法. 首先考虑辅助同余方程

$$ax+by\equiv n \pmod c.$$

设 $d=(a,c)$. 将 y 暂视为常数, 上述方程有解当且仅当 $by\equiv n \pmod d$. 不妨设 $y\equiv y_0 \pmod d$ 是它的同余类解.

然后求约化的同余方程

$$\frac{a}{d}x\equiv \frac{n-by}{d} \pmod{\frac{c}{d}}$$

的剩余类解 $x\equiv \alpha\cdot\frac{n-by}{d} \pmod{\frac{c}{d}}$ (这里 α 是 $\frac{a}{d}$ 在模 $\frac{c}{d}$ 下的逆元). 令

$$y=y_0+sd, \quad x=\alpha\cdot\frac{n-by}{d}+\frac{c}{d}\cdot t, \quad \beta=-\frac{a\alpha-d}{c}, \quad x_0=\frac{n-by_0}{d}, \quad \forall s,t\in\mathbb{Z},$$

则得原不定方程的通解

$$\begin{cases} x=\alpha(x_0-bs)+\frac{c}{d}\cdot t, \\ y=y_0+ds, \\ z=-\beta(x_0-bs)-\frac{a}{d}t, \end{cases}$$

这里 s,t 跑遍所有整数. 事实上, 这几类求解方法本质上都是一样的, 尽管通解的形式可能有所不同.

2.6.3 同余方程组与孙子定理

上面几节, 我们主要研究了多元一次 (同余) 方程的求解问题, 下面我们将进一步探讨多元一次 (同余) 方程组的求解问题.

设 $m_1, \cdots, m_n$ 是两两互质的正整数, $a_1, \cdots, a_n$ 是给定的整数, $m = m_1 m_2 \cdots m_n$. 我们要求以下同余方程组在模 m 下的的剩余类解.

$$\begin{cases} x \equiv a_1 \pmod{m_1}, \\ x \equiv a_2 \pmod{m_2}, \\ \cdots \\ x \equiv a_n \pmod{m_n} \end{cases} \tag{2-25}$$

从不定方程的角度看, 这也等价于求解不定方程组

$$\begin{cases} x + m_1 y_1 = a_1, \\ x + m_2 y_2 = a_2, \\ \cdots \\ x + m_n y_n = a_n \end{cases}$$

的整数解 $(x, y_1, \cdots, y_n)$.

我们有著名结论

定理 2.6.1 (孙子定理, 中国剩余定理) 设 $M_i := \frac{m}{m_i}$, 并取整数 M_i' 使得 $M_i' M_i \equiv 1 \pmod{m_i}$, 则方程组 (2-25) 在模 m 下有唯一的剩余类解

$$x \equiv M_1 M_1' a_1 + M_2' M_2 a_2 + \cdots + M_n' M_n a_n \pmod{m}.$$

证明 (1) 令

$$M = M_1 M_1' a_1 + M_2' M_2 a_2 + \cdots + M_n' M_n a_n.$$

我们先证明 $x \equiv M \pmod{m}$ 是一解. 因为 $m_1 \mid M_i$ $(i = 2, 3, \cdots)$, 所以在模 m_1 下有

$$M \equiv M_1' M_1 a_1 \equiv a_1 \pmod{m_1}.$$

同理可证 $M \equiv a_k \pmod{m_k}$ 对任何 k 成立. 因此 $x \equiv M \pmod{m}$ 确实是方程组 (2-25) 的剩余类解.

(2) 设 $x \equiv M' \pmod{m}$ 是 (2-25) 的另一解, 则 $M \equiv a_i \equiv M' \pmod{m_i}$ $(i = 1, \cdots, n)$, 因而 $m_i \mid (M - M')$. 因为诸 m_i 两两互质, 所以 $m = m_1 \cdots m_n \mathrm{id}(M - M')$, 即 $M \equiv M' \pmod{m}$. 这就证明方程组 (2-25) 在模 m 下的的剩余类解是唯一的. ■

注 2.6.1 从代数角度看, 孙子定理等价于如下同构

$$\mathbb{Z}_m \cong \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \cdots \oplus \mathbb{Z}_{m_n}.$$

例 2.6.8 求最小的正整数 x, 满足以下同余方程组

$$\begin{cases} x \equiv 1 \pmod{2}, \\ x \equiv 2 \pmod{3}, \\ x \equiv 3 \pmod{5}, \\ x \equiv 4 \pmod{7}. \end{cases}$$

令 $m = 2 \cdot 3 \cdot 5 \cdot 7 = 210$, $m_1 = 2, m_2 = 3, m_3 = 5, m_4 = 7$,

$$M_1 = \frac{M}{m_1} = 105, \quad M_2 = \frac{M}{m_2} = 70, \quad M_3 = \frac{M}{m_3} = 42, \quad M_4 = \frac{M}{m_4} = 30.$$

然后我们分别取 M_i' 使得 $M_i' M_i \equiv 1 \pmod{m_i}$, 它们分别等于

$$M_1' = 1, \quad M_2' = 1, \quad M_3' = 3, \quad M_4' = 4.$$

因此

$$x \equiv 1 \cdot 105 \cdot 1 + 1 \cdot 70 \cdot 2 + 3 \cdot 42 \cdot 3 + 4 \cdot 30 \cdot 4 \equiv 53 \pmod{210}.$$

因此 $x = 53$. ■

例 2.6.9 我们也可以从不定方程的角度去解同余方程组. 这里仍以例 2.6.8 为例.

因为 $x \equiv 1 \pmod 2$, 故可设 $x = 2y_1 + 1$. 将之代入同余方程 $x \equiv 2 \pmod 3$, 求得

$$y_1 \equiv 2 \pmod 3.$$

因此进一步设 $y_1 = 3y_2 + 2$, 从而 $x = 6y_2 + 5$. 将该式代入同余方程 $x \equiv 3 \pmod 5$, 得

$$6y_2 + 5 \equiv 3 \pmod 5,$$

故 $y_2 \equiv 3 \pmod 5$. 我们设 $y_2 = 5y_3 + 3$, 因而 $x = 30y_3 + 23$. 代入同余式 $x \equiv 4 \pmod 7$, 因而

$$30y_3 + 23 \equiv 4 \pmod 7,$$

求得 $y_3 \equiv 1 \pmod 7$, 故可设 $y_3 = 7y_4 + 1$, 这就得到 $x = 210y_4 + 53$. 进一步, 由题目要求即得 $x = 53$ ($y_4 = 0$). ■

我们还可以反过来, 用同余方程组的求解方法去解单个的同余方程 $ax \equiv b \pmod m$. 设 $m = p_1^{\alpha_1} \cdots p_s^{\alpha_s}$ 是标准分解式, 因而为求该同余方程, 我们只需要求方程组

$$\begin{cases} ax \equiv b \pmod{p_1^{\alpha_1}}, \\ ax \equiv b \pmod{p_2^{\alpha_2}}, \\ \cdots \\ ax \equiv b \pmod{p_s^{\alpha_s}}, \end{cases}$$

再利用孙子定理求出原方程的解.

例 2.6.10 求同余方程 $43x \equiv 1 \pmod{105}$.

这等价于求方程组

$$\begin{cases} 43x \equiv 1 \pmod 3, \\ 43x \equiv 1 \pmod 5, \\ 43x \equiv 1 \pmod 7. \end{cases}$$

化简系数得

$$\begin{cases} x \equiv 1 \pmod 3, \\ 3x \equiv 1 \pmod 5, \\ x \equiv 1 \pmod 7. \end{cases}$$

因此

$$\begin{cases} x \equiv 1 \pmod 3, \\ x \equiv 2 \pmod 5, \\ x \equiv 1 \pmod 7. \end{cases}$$

由孙子定理, $x \equiv 22 \pmod{105}$. ■

类似的想法还可以处理其它问题.

例 2.6.11 求 2^{1000} 的末两位数.

这相当于求最小的正整数 x, 满足 $x \equiv 2^{1000} \pmod{100}$. 此时我们不能直接使用欧拉定理 (因为 2 和 100 不是互质的). 先将方程转化为方程组

$$\begin{cases} x \equiv 2^{1000} \pmod 4, \\ x \equiv 2^{1000} \pmod{25}. \end{cases}$$

因为 $\varphi(25) = 20$, 所以由欧拉定理, 可将上式简化为

$$\begin{cases} x \equiv 0 \pmod 4, \\ x \equiv 1 \pmod{25}. \end{cases}$$

由孙子定理, $x \equiv 76 \pmod{100}$, 从而 $x = 76$, 即 2^{1000} 末两位数是 76. ■

孙子定理还可以用于求解多元一次不定方程组.

例 2.6.12 求不定方程组的整数解与正整数解

$$\begin{cases} 6x + 7y + 14z = 317, \\ 3x - 7y + z = 4. \end{cases}$$

暂将 z 视作常数, 我们解得

$$\begin{cases} x = \frac{107-5z}{3}, \\ y = \frac{103-4z}{7} \end{cases}$$

因此方程组有解当且仅当以下同余方程组有解

$$\begin{cases} 5z \equiv 107 \pmod 3, \\ 4z \equiv 103 \pmod 7. \end{cases}$$

化简得

$$\begin{cases} z \equiv 1 \pmod 3, \\ z \equiv 3 \pmod 7. \end{cases}$$

由孙子定理得 $z \equiv 10 \pmod{21}$. 我们设 $z = 10 + 21t$ ($t \in \mathbb{Z}$), 则得原方程组的通解公式

$$\begin{cases} x = 19 - 35t, \\ y = 9 - 12t, \\ z = 10 + 21t, \end{cases}$$

这里 t 跑遍所有整数. 此时方程的正整数解是 $(x, y, z) = (19, 9, 10)$. ■

进一步, 我们还可以讨论更一般的线性方程组的整数解.

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n &= b_1, \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n &= b_2, \\ \cdots \quad \cdots \quad \cdots & \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n &= b_m, \end{cases}$$

不失一般性, 我们假设上述线性方程组的系数矩阵秩为 $m(< n)$, 且前 m 列系数构成的子阵是满秩的, 其行列式值记为 $M(\neq 0)$. 由线性方程组理论, 我们有

$$\begin{cases} x_1 = \ \frac{1}{M}(c_{1,m+1}x_{m+1} + c_{1,m+2}x_{m+2} + \cdots + c_{1,n}x_n + d_1), \\ x_2 = \ \frac{1}{M}(c_{2,m+1}x_{m+1} + c_{2,m+2}x_{m+2} + \cdots + c_{2,n}x_n + d_2), \\ \qquad\qquad \cdots \qquad \cdots \qquad \cdots \\ x_m = \frac{1}{M}(c_{m,m+1}x_{m+1} + c_{m,m+2}x_{m+2} + \cdots + c_{m,n}x_n + d_m), \end{cases}$$

这里诸 c_{ij}, d_i 和 M 都是整数.

上述方程组有整数解显然等价于以下多元一次同余方程组模 M 的剩余类解

$$\begin{cases} c_{1,m+1}x_{m+1} + c_{1,m+2}x_{m+2} + \cdots + c_{1,n}x_n + d_1 \equiv 0 \pmod{M}, \\ c_{2,m+1}x_{m+1} + c_{2,m+2}x_{m+2} + \cdots + c_{2,n}x_n + d_2 \equiv 0 \pmod{M}, \\ \cdots \quad \cdots \quad \cdots \\ c_{m,m+1}x_{m+1} + c_{m,m+2}x_{m+2} + \cdots + c_{m,n}x_n + d_2 \equiv 0 \pmod{M}. \end{cases}$$

进一步可将上述各同余式进一步分解成模素数方幂的诸同余式. 如果同余方程组有解, 则我们可以分别讨论模素数方幂的同余方程解, 再利用孙子定理得到原始解. 限于篇幅, 这里不再做深入的探讨了.

本章习题

加 $*$ 号的习题表示有一定难度.

习题 2.1　验证命题 2.1.1 (1)–(4).

习题 2.2　证明: (1) 若 $a \mid bc$, 且 $(a,c) = 1$, 则 $a \mid b$.
(2) 若 $c \mid a$, $b \mid a$, 且 $(b,c) = 1$, 则 $bc \mid a$.
(3) 若 $(a,b,c) = 1$, 则 $(a,b)(a,c) \mid a$.

习题 2.3　直接用整除技巧证明以下结论:
(1) $8 \mid (2n+1)^2 - 1$,
(2) $6 \mid n(n+1)(2n+1)$.

习题 2.4　证明: 形如 $6n-1$ 的素数有无限多个.

习题 2.5 (*)　证明: 任取两个正整数是互质的概率等于 $\frac{6}{\pi^2}$.

习题 2.6　证明:

$$\prod_p \left(\frac{p^2-1}{p^2}\right) = \frac{6}{\pi^2},$$

这里 p 跑遍所有素数.

习题 2.7　证明式 (2-5).

习题 2.8　设 (a,b) 是互质的正整数, 证明: 方程 $ax+by=n$ 的非负整数解的个数是 $[\frac{n}{ab}]$ 或者 $[\frac{n}{ab}]+1$.

习题 2.9 (*)　设 a,b,c 是两两互质的正整数, 证明: $2abc-ab-bc-ac$ 是最大的正整数不能由

$$bcx+acy+abz,\quad x\geq 0,y\geq 0,z\geq 0$$

表出者.

习题 2.10 (**五猴分桃问题**)　五猴摘桃若干置于洞. 翌日一猴先至, 食一桃, 余者均分五等, 取走其一. 须臾第二猴至, 不知前者事, 亦先食一桃, 余者均分五等, 取走其一..... 其余诸猴皆如此为之. 试问五猴至少摘桃若干? 诸猴走后, 至少剩桃若干?

习题 2.11 (**泊松分酒问题**)　有一 12 升的酒瓶装满葡萄酒, 另有 8 升和 5 升空酒瓶子各一个, 问如何从中分出 6 升酒来? 试将此问题归结成二元一次不定方程求解, 并将此问题作推广.

习题 2.12 (**百鸡问题—张丘建算经**)　鸡翁一, 值钱五; 鸡母一, 值钱三; 鸡雏三, 值钱一. 百钱买鸡百只, 问鸡翁、母、雏各几何?

习题 2.13　验证例 2.4.4.

习题 2.14　试给出判断一个正整数被 7 整除的方法.

习题 2.15　设 p 是素数, $\nu_p(n)$ 是 $n!$ 的标准分解式中素因子 p 的方幂.
(1) 证明: $v_p(n)=\sum\limits_{i=1}^{\infty}[\frac{n}{p}]$.
(2) 证明: $v_p(n)=\frac{n-s_p(n)}{p-1}$, 这里 $s_p(n)$ 是 n 在 p 进位制表达下的位数码和.
(3*) 证明:

$$s_p(n)+s_p(m)\geq s_p(n+m),\quad s_p(n)s_p(m)\geq s_p(nm),\quad \forall n,m\in\mathbb{Z}^+.$$

试给出等号成立的条件.
(4*) 证明(卢卡斯定理): 组合数 C_{n+m}^n 不被 p 整除当且仅当加法运算 $n+m$ 中不发生进位现象, 即各个对应位置上的数码之和小于 p. 试利用该结论计算杨辉三角中每一行中奇数的个数.

习题 2.16　求所有正整数 n, 使得 $\varphi(n)\mid n$.

习题 2.17　求以下同余方程的剩余类解:
(1) $5x+2\equiv 0\pmod 7$,
(2) $111x\equiv 75\pmod{15}$,
(3) $6x+24\equiv 0\pmod{15}$.

习题 2.18 (**孙子算经**)　今有物不知其数, 三三数之二, 五五数之三, 七七数之二, 问物几何?

第三章　二次不定方程

3.1　勾股方程及其算法

设直角三角形的两条直角边长为 X,Y, 其中斜边长 Z. 一个有趣的问题是: 何时 x,y,z 都是整数? 更一般地, 我们要求如下不定方程的整数解 (X,Y,Z):

$$X^2+Y^2=Z^2.$$

上述不定方程称作*勾股方程*, 其整数解 (X,Y,Z) 称作*勾股数*;

注 3.1.1　设 (X,Y,Z) 是一组勾股数, 那么
(1) $(\pm X,\pm Y,\pm Z)$ 也都是勾股数.
(2) 设 $d=(X,Y)$, 则

$$\left(\frac{Z}{d}\right)^2=\left(\frac{X}{d}\right)^2+\left(\frac{Y}{d}\right)^2$$

也是整数, 所以 $d\mid Z$. 这样, $(\frac{X}{d},\frac{Y}{d},\frac{Z}{d})$ 也是勾股数, 并且它们两两互质.
(3) 如果 X,Y,Z 中有一个等于零, 则我们有平凡解

$$(0,a,\pm a),\quad (a,0,\pm a),\quad (a,\pm a,0),\quad (0,0,0).$$

引理 3.1.1　*设 (X,Y,Z) 是一组勾股数, 则 X,Y 中必有一个是偶数.*

证明　假设 X,Y 都是奇数. 因为 $X+1,X-1$ 都是偶数, 所以 $4\mid X^2-1$, 即 $X^2\equiv 1 \pmod 4$. 同理 $Y^2\equiv 1 \pmod 4$. 这样

$$Z^2\equiv X^2+Y^2\equiv 2 \pmod 4.$$

因此 Z 是偶数, 从而 $Z^2\equiv 0 \pmod 4$, 矛盾! ■

由上面的注记和引理, 以下我们总假设勾股数满足

$$(X,Y)=1,\quad 2\mid X,\quad X,Y,Z>0.$$

这样的勾股数称为*本原勾股数*.

定理 3.1.1 (**商高定理**)　*本原勾股数必可唯一地写为如下形式*

$$\begin{cases} X=2ab,\\ Y=a^2-b^2,\\ Z=a^2+b^2, \end{cases} \tag{3-1}$$

这里 $a>b$ 是两个互质的正整数, 并且 a,b 中一奇一偶.

反过来, 满足以上条件的数组 (a,b) 确定一组本原勾股数.

例 3.1.1　(1) 取 $a=2,b=1$, 则有本原勾股数 $(X,Y,Z)=(4,3,5)$.
(2) 取 $a=3,b=2$, 则有本原勾股数 $(X,Y,Z)=(12,5,13)$. ■

在下面两小节中, 我们将给出两种不同的证明.

3.1.1 数论证明

(1) 先证明本原勾股数都有式 (3-1) 的形式.

由假设条件易知, Y, Z 都是奇数, 所以 $\frac{Z-Y}{2}, \frac{Z+Y}{2}$ 都是整数, 并且

$$\left(\frac{Z-Y}{2}, \frac{Z+Y}{2}\right) = \left(Z, \frac{Z+Y}{2}\right) = (Z, Z+Y) = (Z, Y) = 1. \tag{3-2}$$

由

$$\left(\frac{X}{2}\right)^2 = \frac{Z^2-Y^2}{4} = \left(\frac{Z-Y}{2}\right)\left(\frac{Z+Y}{2}\right)$$

和式 (3-2) 以及算术基本定理, 我们可设

$$\frac{Z+Y}{2} = a^2, \quad \frac{Z-Y}{2} = b^2, \tag{3-3}$$

这里 $a > b$ 是互质的正整数. 由费马小定理

$$a + b \equiv a^2 + b^2 \equiv Z \equiv 1 \pmod 2.$$

这表明 a, b 中一奇一偶. 由式 (3-3), 我们有

$$X = 2ab, \quad Y = a^2 - b^2, \quad Z = a^2 + b^2.$$

(2) 其次证明这样的 a, b 是唯一的.

假设 a', b' 也满足式 (3-1), 则

$$\frac{Z+Y}{2} = a^2 = a'^2, \quad \frac{Z-Y}{2} = b^2 = b'^2.$$

因此 $a = a', b = b'$.

(3) 最后证明任何满足命题条件的数组 (a, b) 对应的解 (X, Y, Z) 是本原勾股数.

注意到 a, b 互质且 $a^2 - b^2$ 是奇数, 所以

$$(a, a^2-b^2) = (a, b^2) = 1, \quad (b, a^2-b^2) = (b, a^2) = 1, \quad (2, a^2-b^2) = 1.$$

这就推出 $(X, Y) = (2ab, a^2 - b^2) = 1$. ■

3.1.2 解析几何证明

我们考虑平面上的单位圆周方程

$$x^2 + y^2 = 1.$$

设 $S = (0, -1)$ 是南极点, $P = (x, y)$ 是单位圆周上的点. 取连接 S, P 的直线 $\overline{SP}$, 其斜率记为 t.

引理 3.1.2 单位圆周上的任一点 $P = (x, y)$ 都可以唯一表达成如下参数形式

$$\begin{cases} x = \frac{2t}{t^2+1}, \\ y = \frac{t^2-1}{t^2+1}, \end{cases} \tag{3-4}$$

这里 t 取遍所有实数或无穷大 ∞ (此时对应北极点 $N = (0, 1)$).

证明 由直线 $\overline{SP}$ 的定义立得 $t = \frac{y+1}{x}$, 即 $y = tx - 1$. 将它代入单位圆周方程得

$$(tx-1)^2 + x^2 = 1.$$

由此即得式 (3-4). ■

引理 3.1.3 $P(x,y)$ 是有理点当且仅当参数式 (3-4) 中的 t 是有理数或者 $t=\infty$.

证明 ($\Longrightarrow$) 已知 P 是有理点, 即 $x,y\in\mathbb{Q}$, 因此 $t=\frac{y+1}{x}\in\mathbb{Q}$ (当 $x\neq 0$ 时) 或者 $t=\infty,0$ (当 $x=0$ 时).

($\Longleftarrow$) 若 $t=\infty$, $P=(0,1)$ 显然是有理点. 若 $t\in\mathbb{Q}$, 则由式 (3-4) 即知 P 是有理点. ■

令 $t=\frac{a}{b}$, a,b 是互质的整数. 当 $b=0$ 时, 我们规定 $t=\infty$. 代入参数式 (3-4) 则有

$$x=\frac{2ab}{a^2+b^2},\quad y=\frac{a^2-b^2}{a^2+b^2}. \tag{3-5}$$

这就得到以下结论.

推论 3.1.1 单位圆上的有理点都可唯一写成式 (3-5), 其中 a,b 是互质的整数.

现在我们考虑勾股方程

$$X^2+Y^2=Z^2$$

的本原勾股解 (X,Y,Z). 设 $x=\frac{X}{Z}$, $y=\frac{Y}{Z}$, 则有

$$x^2+y^2=1.$$

这就是说 $P(x,y)$ 是单位圆周上的有理点, 因而可以表示成式 (3-5).

如果 a,b 一奇一偶, 那么 a^2+b^2 是奇数, 因而

$$(2ab,a^2+b^2)=(ab,a^2+b^2)=(a,a^2+b^2)=1.$$

由式 (3-5) 及既约分式表达的唯一性, 我们得到

$$X=2ab,\quad Z=a^2+b^2,$$

从而 $Y=a^2-b^2$. 这就有式 (3-1).

如果 a,b 都是奇数, 那么 a^2+b^2 是偶数. 此时类似可得

$$X=ab,\quad Z=\frac{a^2+b^2}{2}.$$

因而 X 是奇数, 这与本原勾股解定义矛盾!

至此我们完成了证明. ■

3.1.3 椭圆或双曲线上的有理点

上面的第二种证法富有启发性. 因为它是从几何性质推出了数论的性质. 我们可以用同样的方法讨论椭圆或双曲线上的有理点. 比如考虑以下方程所定义的二次曲线 C:

$$dx^2+y^2=1,$$

这里 d 是给定的非零整数. 取定 C 上一点 $S(0,-1)$,. 对任何 C 上的点 $P(x,y)$, 连接直线 $\overline{SP}$, 其斜率 $t=\frac{y+1}{x}$. 将之代入方程即得 C 的参数表达式

$$\begin{cases} x=\frac{2t}{t^2+d}, \\ y=\frac{t^2-d}{t^2+d}. \end{cases} \tag{3-6}$$

由类似地讨论可知, 当 t 跑遍所有有理数或 ∞ 时, $P(x,y)$ 也恰好跑遍所有的有理点.

上述讨论也可以类似应用于求解不定方程

$$dX^2+Y^2=Z^2. \tag{3-7}$$

为方便讨论, 我们这里考虑 d 是奇素数的情形.

引理 3.1.4 *设 d 是奇素数, (X,Y,Z) 是方程 (3-7) 的解, 则 $(X,Y)=(Y,Z)=(X,Z)$.*

证明 不失一般性, 我们可以假设 $\gcd(X,Y,Z)=1$. 因此我们只需证 X,Y,Z 两两互质.

设 $h=(X,Z)$, 则 $h^2\mid Y^2=Z^2-dX^2$, 从而 $h\mid Y$, 这就推出 $h=1$. 同理可证 $(X,Y)=1$.

设 $c=(Y,Z)$, 则 $c^2\mid dX^2=Z^2-Y^2$. 我们证明 $c\mid X$, 从而 $c=1$. 分两种情形讨论:

(1) 如果 $(c,d)=1$, 那么 $c^2\mid X^2$, 即 $c\mid X$.

(2) 如果 $(c,d)\neq 1$, 即 $d\mid c$, 则 $d^2\mid dX^2$, 因而 $d\mid X^2$, 所以 $d\mid X$. 这就推出 $d\mid(X,Y,Z)$, 因此 $d=1$, 矛盾! ■

由上述引理, 我们只需要讨论方程 (3-7) 的本原解, 即要求 X,Y,Z 是两两互质的正整数.

定理 3.1.2 *设 d 是奇素数, 方程 (3-7) 的所有本原解必可写为如下两种表达式之一:*

$$\begin{cases} X=2ab,\\ Y=|a^2-db^2|, \qquad (a,b)=(a,d)=1, \quad a,b\text{一奇一偶},\\ Z=a^2+db^2, \end{cases}$$

或

$$\begin{cases} X=ab,\\ Y=\frac{|a^2-db^2|}{2}, \qquad (a,b)=(a,d)=1, \quad a,b\text{皆为奇数},\\ Z=\frac{a^2+db^2}{2}. \end{cases}$$

证明 设 $x=\frac{X}{Y}$, $y=\frac{Y}{Z}$, 代入方程 (3-7),即得二次曲线方程

$$dx^2+y^2=1.$$

因此我们等价于求上述椭圆的有理点. 将 $t=\frac{a}{b}$ (a,b 互质) 代入参数表达式 (3-6), 则有

$$x=\frac{2ab}{a^2+db^2}, \quad y=\frac{a^2-db^2}{a^2+db^2}.$$

我们只要将上面式子右边的分数写成既约形式, 就能得到原不定方程的本原解. 由直接计算及 $(a,b)=1$, 我们有 (为什么?)

$$(2ab,a^2+db^2)=(2a,a^2+db^2)=(a,d)(2,a^2+db^2).$$

分情形讨论:

(1) 如果 $(a,d)=1$, 且 a,b 一奇一偶, 则得

$$\begin{cases} X=2ab,\\ Y=a^2-db^2, \qquad (a,b)=1, \quad a,b\text{一奇一偶},\\ Z=a^2+db^2, \end{cases}$$

(2) 如果 $(a,d)=1$, 且 a,b 都是奇数, 则得

$$\begin{cases} X = ab, \\ Y = \frac{a^2-db^2}{2}, \\ Z = \frac{a^2+db^2}{2}, \end{cases} \qquad (a,b)=1, \quad a,b\text{皆为奇数},$$

(3) 如果 $(a,d)=d$, 且 a,b 一奇一偶, 我们设 $a'=\frac{a}{d}$, 从而有

$$\begin{cases} X = 2a'b, \\ Y = da'^2-b^2, \\ Z = da'^2+b^2, \end{cases} \qquad (a',b)=1, \quad a',b\text{一奇一偶},$$

(4) 如果 $(a,d)=d$, 且 a,b 都是奇数, 设 $a'=\frac{a}{d}$, 则得

$$\begin{cases} X = a'b, \\ Y = \frac{da'^2-b^2}{2}, \\ Z = \frac{da'^2+b^2}{2}. \end{cases} \qquad (a',b)=1, \quad a',b\text{皆为奇数},$$

适当替换以上各情形中的参数, 我们可以将本原解统一写成命题所述的两种形式. 此处不再赘述, 留给读者验证. ■

有兴趣的读者也可以类似讨论 d 为其他整数时的不定方程. 比如求 $2X^2+Y^2=Z^2$ 的整数解等等.

3.1.4 应用: 四次费马方程

在这一节中, 我们要利用勾股方程的求解公式以及费马发明的*无穷递降法*, 来证明以下的*四次费马方程*

$$X^4+Y^4=Z^4$$

没有正整数解. 为此, 我们实际上只需要证明以下的不定方程无正整数解即可 (为什么?):

$$X^4+Y^4=Z^2. \tag{3-8}$$

命题 3.1.1 *不定方程 (3-8) 没有正整数解.*

证明 反证法. 假设方程有正整数解. 我们找最小的正整数 Z, 使得不定方程 (3-8) 有正整数解 (X,Y,Z).

(1) 先证 $(X,Y)=1$. 设 $d=(X,Y)>1$, 由

$$\left(\frac{X}{d}\right)^4+\left(\frac{Y}{d}\right)^4=\left(\frac{Z}{d^2}\right)^2$$

可知 $\frac{Z}{d^2}$ 是正整数, $(\frac{X}{d},\frac{Y}{d},\frac{Z}{d^2})$ 是方程 (3-8) 的另一组解. 但 $\frac{Z}{d^2}<Z$, 这与 Z 的极小性矛盾! 所以 $d=1$.

(2) 类似勾股方程的讨论, X,Y 一奇一偶. 因此不妨假设 X 是偶数. 由商高定理, 我们可设

$$X^2=2ab, \quad Y^2=a^2-b^2, \quad Z=a^2+b^2,$$

这里 $(a,b)=1$, $a>b>0$, 且 a,b 一奇一偶. 如果 b 是奇数, 那么因为 Y 也是奇数, 则 $a^2\equiv 2 \pmod 4$, 矛盾! 因此 b 是偶数, a 是奇数.

(3) 设 $b=2c$. 我们得

$$\left(\frac{x}{2}\right)^2 = ac.$$

注意到 $(c,a)=(b,a)=1$, 所以可设

$$a=r^2, \quad c=s^2, \quad (r,s)=1, \quad r \text{ 是奇数}.$$

代入 $Y^2=a^2-b^2$, 得

$$(2s^2)^2+Y^2=(r^2)^2.$$

容易验证 $(2s^2,Y,,r^2)$ 仍是本原勾股数. 再次应用商高定理, 可设

$$2s^2=2pq, \quad Y=p^2-q^2, \quad r^2=p^2+q^2, \quad (p,q)=1, \quad p>q>0,$$

并且 p,q 一奇一偶.

(4) 因为 $s^2=pq$, $(p,q)=1$, 所以可设 $p=u^2, q=v^2$. 将之代入 $r^2=p^2+q^2$ 得

$$u^4+v^4=r^2.$$

因此 (u,v,r) 也是方程 (3-8) 的正整数解. 注意到

$$r \le r^2=a \le a^2 < a^2+b^2=Z,$$

这就与 Z 的最小性矛盾!

因此方程 (3-8) 没有正整数解. ■

注 3.1.2 上面的证明方法称为*无穷递降法*, 乃费马所创. 其原理总结如下:
若命题 $P(n)$ 对若干正整数 n 成立, 则在这些 n 中必有一个最小者, 记作 n_0. 进一步证明, 存在更小的正整数 $n'<n_0$, 使得命题 $P(n')$ 也成立, 这就得到矛盾! 因而可断言 $P(n)$ 不是真命题. ■

注 3.1.3 费马猜测不定方程 (称为*费马方程*)

$$X^n+Y^n=Z^n, \quad XYZ \neq 0, \quad n>2$$

无整数解. 这就是著名的*费马猜想*或*费马大定理*. 费马自己用无穷递降法证明了 $n=4$ 的情形. 欧拉和高斯用不同的方法证明了 $n=3$ 的情形. 此后, 库莫引进理想数的概念, 成功证明了 $n<100$ 的情形. 经过许多数学家的不懈努力, 最终由英国数学家外尔斯于 1995 年前后予以彻底解决—其证明用到了很多艰深的数学工具.

费马猜想被誉为"生金蛋的鸡", 因为它刺激了许多数学理论发展, 产生了许多新的数学思想和方法. 比如近世代数中的理想理论就是从研究这个猜想发展出来的. ■

3.2 平方剩余及其算法

这一节将讨论抛物线方程

$$x^2-my=n$$

的整数解 (x,y), 这里 m,n 是给定的整数. 我们也可以用同余的语言来讨论.

定义 3.2.1 *设 m,n 是整数, $m>1$, $(m,n)=1$. 如果同余方程 $x^2 \equiv n \pmod m$ 有解, 则称 n 是模 m 的平方剩余或二次剩余; 否则称为平方非剩余.*

例 3.2.1　模 7 下的平方剩余有 $\bar{0}, \bar{1}, \bar{2} = \bar{3}^2, \bar{4}$; 平方非剩余则是 $\bar{3}, \bar{5}, \bar{6}$. ■

由孙子定理, 我们只需要讨论整数 n 在模素数方幂时是否为平方剩余即可. 因此我们下面几节先讨论 $m = p$ 是素数的情形.

3.2.1 勒让德符号与欧拉定理

设 p 是素数, $p \nmid n$, 我们定义勒让德符号 (Legendre)

$$\left(\frac{n}{p}\right) = \begin{cases} 1, & \text{如果 } n\text{模 } p \text{ 平方剩余}, \\ -1, & \text{如果 } n\text{模 } p \text{ 平方非剩余}. \end{cases}$$

注 3.2.1　(1) 若 $n \equiv n' \pmod{p}$, 则

$$\left(\frac{n}{p}\right) = \left(\frac{n'}{p}\right).$$

(2) $\left(\frac{n^2}{p}\right) = 1$. 特别地, $\left(\frac{1}{p}\right) = 1$. ■

例 3.2.2

$$\left(\frac{1}{2}\right) = 1, \quad \left(\frac{2}{3}\right) = -1, \quad \left(\frac{2}{7}\right) = 1, \quad \left(\frac{3}{7}\right) = -1.$$

以下我们只关心 $p > 2$ 是奇素数的情形.

命题 3.2.1　*模 p 的既约剩余系 $\mathbb{Z}_p^*$ 中恰有 $\frac{1}{2}(p-1)$ 个平方剩余; 恰有 $\frac{1}{2}(p-1)$ 个平方非剩余. 此外,*

$$1^2, \quad 2^2, \quad , \cdots, \left(\frac{p-1}{2}\right)^2$$

恰为模 p 的所有平方剩余.

证明　(1) 假设 n 是平方剩余, 则存在正整数 $x < p$, 使得 $x^2 \equiv n \pmod{p}$. 显然

$$(p-x)^2 \equiv (-x)^2 \equiv n \pmod{p}.$$

$x, p-x$ 中必有一个不超过 $\frac{1}{2}(p-1)$. 这表明任何平方剩余在模 p 下都可以写成 a^2 的形式, 这里 $1 \le a \le \frac{1}{2}(p-1)$.

假设 $a^2 \equiv b^2 \pmod{p}$, 并且 $1 \le a, b \le \frac{1}{2}(p-1)$. 那么

$$0 \equiv a^2 - b^2 \equiv (a-b)(a+b) \pmod{p},$$

即 $p \mid (a-b)(a+b)$. 因为 $0 < a+b < p$, 所以这就推出 $p \mid a-b$, 从而 $a = b$. 这表明 $1^2, \cdots, \left(\frac{1}{2}(p-1)\right)^2$ 恰好不重复地跑遍所有模 p 的平方剩余. ■

注 3.2.2　上述结论也可以用代数语言去解释. 考虑乘法群之间的同态映射

$$h : \mathbb{Z}_p^* \longrightarrow \mathbb{Z}_p^*, \quad x \to x^2.$$

其像集 $H = \mathrm{Im}h$ 也是 $\mathbb{Z}_p^*$ 中的子群, 它就是所有平方剩余构成的集合, 因此 $|H| = \frac{1}{2}(p-1)$. H 在 $\mathbb{Z}_p^*$ 中的陪集个数等于 2, 也就是说除了 H 本身外, 另一个陪集恰好是所有的平方非剩余. ■

定理 3.2.1 (**欧拉定理**) 设 p 是奇素数, 则

$$n^{\frac{p-1}{2}} \equiv \left(\frac{n}{p}\right) \pmod{p}.$$

证明 (1) 如果 n 是平方剩余, 即存在整数 a, 使得 $a^2 \equiv n \pmod{p}$. 那么由费马小定理

$$n^{\frac{p-1}{2}} \equiv (a^2)^{\frac{p-1}{2}} \equiv a^{p-1} \equiv 1 \equiv \left(\frac{n}{p}\right) \pmod{p}.$$

(2) 由费马小定理, $x^{p-1} - 1 \equiv 0 \pmod{p}$ 恰好有 $p-1$ 个同余解, 它们跑遍 $\mathbb{Z}_p^*$ 中的剩余类. 因为

$$x^{p-1} - 1 = \left(x^{\frac{p-1}{2}} - 1\right)\left(x^{\frac{p-1}{2}} + 1\right),$$

而 $x^{\frac{p-1}{2}} - 1 \equiv 0 \pmod{p}$ 的解恰好就是那些平方剩余 (见 (1) 的讨论), 因此所有非平方剩余都是 $x^{\frac{p-1}{2}} + 1 \equiv 0 \pmod{p}$ 的解. 这就是说, 对任一平方非剩余 n, 有

$$n^{\frac{p-1}{2}} \equiv -1 \equiv \left(\frac{n}{p}\right) \pmod{p}.$$ ■

注 3.2.3 欧拉定理显然推出费马小定理. 反过来, 前者的证明中又用到了费马小定理. 因此这两个定理是彼此等效的. ■

推论 3.2.1 设 p 是奇素数, 则

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}.$$

换言之, 如果 $p \equiv 1 \pmod{4}$, 那么 -1 模 p 平方剩余; 如果 $p \equiv 3 \pmod{4}$, 那么 -1 模 p 平方非剩余.

证明 将 $n = -1$ 代入欧拉定理中的同余式即得. ■

推论 3.2.2 $n^2 + 1$ 中的奇素因子 p 必定满足 $p \equiv 1 \pmod{4}$.

证明 设 $p \mid n^2 + 1$, 则 $n^2 \equiv -1 \pmod{p}$. 这表明 -1 在模 p 下是平方剩余, 因而

$$1 = \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}.$$

这意味着 $p \equiv 1 \pmod{4}$. ■

推论 3.2.3 设 $p \nmid mn$, 则

$$\left(\frac{mn}{p}\right) = \left(\frac{m}{p}\right) \cdot \left(\frac{n}{p}\right)$$

证明 由

$$\left(\frac{mn}{p}\right) \equiv (mn)^{\frac{p-1}{2}} \equiv m^{\frac{p-1}{2}} n^{\frac{p-1}{2}} \equiv \left(\frac{m}{p}\right) \cdot \left(\frac{n}{p}\right) \pmod{p}$$

立得结论. ■

推论 3.2.4 在模 p 下,

(1) 两平方剩余之积仍是平方剩余;

(2) 两平方非剩余之积是平方剩余;

(3) 平方剩余和平方非剩余之积是平方非剩余.

3.2.2 应用 (I): 威尔逊定理

我们证明如下的著名结论.

定理 3.2.2 (威尔逊定理) *n 是素数的充分必要条件是*

$$(n-1)! \equiv -1 \pmod{n}.$$

证明 ($\Longleftarrow$) 已知 $(n-1)! \equiv -1 \pmod{n}$, 即 $n \mid (n-1)!+1$.

假设 n 不是素数, p 是 n 中的素因子, 则 $p \leq n-1$, 从而 $p \mid (n-1)!$. 这就推出 $p \nmid (n-1)!+1$, 所以 $n \nmid (n-1)!+1$, 矛盾! 因此 n 是素数.

($\Longrightarrow$) 设 $n=p$ 是素数. 我们取模 p 的任一平方非剩余 a. 由命题 3.2.1 和推论 3.2.4,

$$a \cdot 1^2, \quad a \cdot 2^2, \quad \cdots, \quad a \cdot \left(\frac{p-1}{2}\right)^2$$

恰好跑遍所有的平方非剩余. 因此上述序列连同

$$1^2, \quad 2^2, \quad \cdots, \quad \left(\frac{p-1}{2}\right)^2$$

恰好构成模 p 的既约剩余系. 将这两列元素乘起来, 这就推出

$$a^{\frac{p-1}{2}} \left(\left(\frac{p-1}{2}\right)!\right)^4 \equiv (p-1)! \pmod{p}$$

由欧拉定理, $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$, 因此

$$\left(\left(\frac{p-1}{2}\right)!\right)^4 \equiv -(p-1)! \pmod{p}. \tag{3-9}$$

另一方面,

$$-\frac{p-1}{2}, \quad \cdots, \quad -2, \quad -1, \quad 1, \quad 2, \quad \cdots, \quad \frac{p-1}{2}$$

也构成完全剩余系, 因此将它们乘起来就得到

$$(-1)^{\frac{p-1}{2}} \left(\left(\frac{p-1}{2}\right)!\right)^2 \equiv (p-1)! \pmod{p}. \tag{3-10}$$

结合上式与式 (3-9), 我们就得到

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

这就完成了证明. ■

我们这里再提供一种证明. 设 r 是不超过 $p-1$ 的正整数. 我们可以找到唯一的正整数 $r^* \leq p-1$ 使得 $rr^* \equiv 1 \pmod{p}$. 除了 $r=1, p-1$ 外, 我们总有$r \neq r^*$. 现在我们将模 p 的既约剩余系

$$\bar{1}, \quad \bar{2}, \quad \cdots, \quad \overline{p-1}$$

做一个分划, 将 $\{\bar{r}, \overline{r^*}\}$ (如果 $r \neq 1, p-1$) 归一个子集合, $\{\bar{1}\}$, $\{\overline{p-1}\}$ 分别归为单元集. 将所有剩余类相乘, 由每个双元集内的元素相乘等于 1, 所以

$$\overline{(p-1)!} = \bar{1} \cdot \overline{p-1} = \overline{-1}.$$

这就推出 $(p-1)! \equiv -1 \pmod{p}$.

3.2.3 应用 (II): 模素数二次同余式求解算法

我们现在来具体求解一些二次同余方程

$$x^2 \equiv n \pmod{p}, \tag{3-11}$$

这里 p 是奇素数.

推论 3.2.5 如果 $p \equiv 3 \pmod 4$, 那么方程 (3-11) 的剩余类解为

$$x \equiv \pm n^{\frac{p+1}{4}} \pmod{p}.$$

证明 由欧拉定理得

$$\left(\pm n^{\frac{p+1}{4}}\right)^2 \equiv n^{\frac{p+1}{2}} \equiv n^{\frac{p-1}{2}} \cdot n \equiv n \pmod{p}.$$

这就得到结论. ■

推论 3.2.6 如果 $p \equiv 5 \pmod 8$, 那么

(1) $n = -1$ 是平方剩余, 此时方程 (3-11) 的剩余类解为

$$x \equiv \pm \left(\frac{p-1}{2}\right)! \pmod{p}.$$

(2) 假设 n 是平方剩余, 则

$$n^{\frac{p-1}{4}} \equiv \pm 1 \pmod{p}.$$

进一步, 方程 (3-11) 的剩余类解为

$$x \equiv \begin{cases} \pm n^{\frac{p+3}{8}}, & \text{如果 } n^{\frac{p-1}{4}} \equiv 1 \pmod{p}, \\ \pm \left(\frac{p-1}{2}\right)! \cdot n^{\frac{p+3}{8}}, & \text{如果 } n^{\frac{p-1}{4}} \equiv -1 \pmod{p} \end{cases}$$

证明 (1) 由式 (3-10) 以及威尔逊定理立得.

(2) 设 n 是平方剩余, 则由欧拉定理

$$\left(n^{\frac{p-1}{4}} - 1\right)\left(n^{\frac{p-1}{4}} + 1\right) \equiv n^{\frac{p-1}{2}} - 1 \equiv 0 \pmod{p}.$$

这就推出$n^{\frac{p-1}{4}} \equiv \pm 1 \pmod{p}$.

如果 $n^{\frac{p-1}{4}} \equiv 1 \pmod{p}$, 那么

$$\left(\pm n^{\frac{p+3}{8}}\right)^2 \equiv n^{\frac{p+3}{4}} \equiv n^{\frac{p-1}{4}} \cdot n \equiv n \pmod{p}.$$

如果 $n^{\frac{p-1}{4}} \equiv -1 \pmod{p}$, 那么

$$\left(\pm \left(\frac{p-1}{2}\right)! \cdot n^{\frac{p+3}{8}}\right)^2 \equiv \left(\left(\frac{p-1}{2}\right)!\right)^2 \cdot n^{\frac{p+3}{4}} \equiv -n^{\frac{p-1}{4}} \cdot n \equiv n \pmod{p}.$$

这就完成了证明. ■

对于 $p \equiv 1 \pmod 8$ 的情形, 求二次同余式通常比较困难, 没有直接的结果. 这里提供一种简化计算量的思路. 假设已知 $x^2 \equiv n \pmod m$ 有解, 这等价于说不定方程 $x^2 = n + py$ 有解. 不失一般性, 我们可以假设 $0 < n < p$, $0 < x < \frac{p}{2}$, 因而$0 < y < \frac{p}{4}$. 今取一个与 p 互质的奇素数 e, 则 $x^2 \equiv n + py \pmod e$ 意味着 $n + py$ 在模 e 下是平方剩余. 这样我们就能将 y 的取值范围进一

步缩小. 选取不同的 e, 我们可以逐步缩小 y 的取值范围直至求出满足条件的 y, 从而得到 x 的值.

例 3.2.3 求最小的正整数 x, 满足 $x^2 \equiv 2 \pmod{73}$.

由上面的讨论, 这等价于求不定方程

$$x^2 = 2 + 73y, \quad 1 \leq x \leq 36, \quad 1 \leq y \leq 18.$$

取素数 $e_1 = 3$, 因为 $2 + 73y$ 在模 e_1 下平方剩余, 所以有以下几种可能

$$2 + 73y \equiv 0,\ 1 \pmod{3},$$

即 $y \equiv 1,\ 2 \pmod{3}$, 亦即 y 不是 3 的倍数. 这样, y 的取值范围缩减为

$$1, \quad 2, \quad 4, \quad 5, \quad 7, \quad 8, \quad 10, \quad 11, \quad 13, \quad 14, \quad 16, \quad 17.$$

取素数 $e_2 = 5$, 因为 $2 + 73y$ 在模 e_2 下也是平方剩余, 所以有以下几种可能

$$2 + 73y \equiv 0,\ 1,\ 4 \pmod{5},$$

即 $y \equiv 1,\ 3,\ 4 \pmod{5}$, 亦即 $y \not\equiv 0,\ 2 \pmod{5}$. 这样, y 的取值范围缩减为

$$1, \quad 4, \quad 8, \quad 11, \quad 13, \quad 14, \quad 16.$$

同样地, 取素数 $e_3 = 7$, 可将 y 的范围进一步缩减为

$$4, \quad 11, \quad 14, \quad 16.$$

由此验算可得 $y = 14, x = 32$. ■

3.2.4 高斯引理

引理 3.2.1 (高斯引理) 设 p 是奇素数, $p \nmid n$, 设 $\frac{1}{2}(p-1)$ 个数

$$n, \quad 2n, \quad 3n, \quad \cdots, \quad \left(\frac{p-1}{2}\right)n \pmod{p} \tag{3-12}$$

之最小正余数中有 m 个大于 $\frac{1}{2}p$, 则

$$\left(\frac{n}{p}\right) = (-1)^m. \tag{3-13}$$

例 3.2.4 (1) 取 $p = 7$, $n = 10$, 以下三个数

$$10, \quad 20, \quad 30 \pmod{7}$$

的最小正余数分别是 $3, 6, 2$, 其中大于 $\frac{7}{2}$ 的有一个, 即 $m = 1$. 因而

$$\left(\frac{10}{7}\right) = -1,$$

即 10 在模 7 下平方非剩余.

(2) 取 $p = 11$, $n = 2$, 以下五个数

$$2, \quad 4, \quad 6, \quad 8, \quad 10 \pmod{11}$$

的最小正余数中大于 $\frac{11}{2}$ 的有 3 个, 即 $m=3$. 因而

$$\left(\frac{2}{11}\right)=-1,$$

即 2 在模 11 下平方非剩余. ■

高斯引理的证明: 将数组 (3-12) 在模 p 下的最小正余数分为两类:

$a_1,\cdots,a_l$ 是所有小于 $\frac{1}{2}p$ 者;

$b_1,\cdots,b_m$ 是所有大于 $\frac{1}{2}p$ 者 ($l+m=\frac{p-1}{2}$).

注意到 $1\leq p-b_i\leq\frac{1}{2}(p-1)$, 所以诸 a_j 与 $p-b_i$ 皆落在 1 及 $\frac{1}{2}(p-1)$ 之间.

第一步: 我们证明 $a_j\neq p-b_i$, 对任何 i,j.

假设 $a_j=p-b_i$ 对某 i,j 成立. 由 a_j,b_i 的定义, 存在 $x,y\in\mathbb{Z}$, 满足 $1\leq x,y\leq\frac{1}{2}(p-1)$, 且

$$xn\equiv a_j,\quad yn\equiv b_i\pmod p.$$

因此

$$xn+yn\equiv a_j+b_i\equiv p\equiv 0\pmod p.$$

这就推出 $x+y\equiv 0\pmod p$, 从而与 $1\leq x,y\leq\frac{1}{2}(p-1)$ 矛盾!

第二步: 我们证明

$$\prod_{j=1}^{l}a_j\prod_{i=1}^{m}(p-b_i)\equiv\left(\frac{p-1}{2}\right)!\pmod p. \tag{3-14}$$

由第一步, 诸 a_j 与 $p-b_i$ 恰好无重复且无遗漏地跑遍 1 及 $\frac{1}{2}(p-1)$ 之间所有的整数, 由此立得式 (3-14).

第三步: 我们证明

$$\prod_{j=1}^{l}a_j\prod_{i=1}^{m}b_i\equiv\left(\frac{p-1}{2}\right)!\cdot n^{\frac{p-1}{2}}\pmod p. \tag{3-15}$$

由 a_j 与 b_i 的定义,

$$\prod_{j=1}^{l}a_j\prod_{i=1}^{m}b_i=\prod_{k=1}^{\frac{1}{2}(p-1)}(kn)\pmod p.$$

由此立得式 (3-15).

第四步: 证明式 (3-13).

结合式 (3-14) 和式 (3-15), 我们有

$$n^{\frac{p-1}{2}}\equiv(-1)^m\pmod p.$$

再由欧拉定理即得式 (3-13). ■

推论 3.2.7 *设 P 是奇素数, 则*

$$\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}.$$

证明 在数组 (3-12) 中取 $n=2$, 则有

$$2,4,6,\cdots,(p-1)\pmod p.$$

上述序列中最小正余数大于 $\frac{1}{2}p$ 者的个数等于

$$m=\begin{cases}\frac{p-1}{4}, & \text{如果 } p\equiv 1 \pmod 4,\\ \frac{p+1}{4}, & \text{如果 } p\equiv 3 \pmod 4.\end{cases}$$

由高斯引理,

$$\left(\frac{2}{p}\right)=(-1)^m.$$

容易验证,

$$(-1)^m=(-1)^{\frac{p^2-1}{8}}=\begin{cases}1 & \text{如果 } p\equiv \pm 1 \pmod 8,\\ -1 & \text{如果 } p\equiv \pm 3 \pmod 8.\end{cases}$$ ■

例 3.2.5 (1)

$$\left(\frac{2}{7}\right)=(-1)^{\frac{7^2-1}{8}}=1,\quad \left(\frac{2}{41}\right)=(-1)^{\frac{41^2-1}{8}}=1,\quad \left(\frac{-29}{31}\right)=\left(\frac{2}{31}\right)=(-1)^{\frac{31^2-1}{8}}=1.$$

(2)

$$\left(\frac{8}{37}\right)=\left(\frac{2}{37}\right)^3=\left(\frac{2}{37}\right)=(-1)^{\frac{37^2-1}{8}}=-1.$$

例 3.2.6 对奇素数 p, 我们有

$$\left(\frac{-2}{p}\right)=\left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)=(-1)^{\frac{p-1}{2}}\cdot(-1)^{\frac{p^2-1}{8}}=\begin{cases}1, & \text{如果 } p\equiv 1,3 \pmod 8,\\ -1, & \text{如果 } p\equiv -1,-3 \pmod 8.\end{cases}$$ ■

比如

$$\left(\frac{15}{17}\right)=\left(\frac{-2}{17}\right)=1,\quad \left(\frac{-2}{37}\right)=-1.$$

推论 3.2.8 n^2-2 中的奇素因子 p 必满足 $p\equiv\pm 1 \pmod 8$.

3.2.5 二次互反律

我们要在这一节介绍最重要的定理—高斯二次互反律.

定理 3.2.3 (**二次互反律**) 设 p,q 是奇素数, 则

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

换言之, 如果 $p\equiv q\equiv 3 \pmod 4$, 则两同余式

$$x^2\equiv p \pmod q,\quad y^2\equiv q \pmod p$$

中一个可解, 一个无解; 否则, 都可解或都不可解.

例 3.2.7 (1)

$$\left(\frac{17}{73}\right)=(-1)^{\frac{17-1}{2}\cdot\frac{73-1}{2}}\left(\frac{73}{17}\right)=\left(\frac{73}{17}\right)=\left(\frac{5}{17}\right)=(-1)^{\frac{17-1}{2}\cdot\frac{5-1}{2}}\left(\frac{17}{5}\right)=\left(\frac{2}{5}\right)=(-1)^{\frac{5^2-1}{8}}=-1.$$

(2)

$$\left(\frac{24}{101}\right)=\left(\frac{6}{101}\right)=\left(\frac{2}{101}\right)\left(\frac{3}{101}\right).$$

注意到

$$\left(\frac{2}{101}\right)=(-1)^{\frac{101^2-1}{8}}=-1,\quad \left(\frac{3}{101}\right)=(-1)^{\frac{101-1}{2}\cdot\frac{3-1}{2}}\left(\frac{101}{3}\right)=\left(\frac{101}{3}\right)=\left(\frac{2}{3}\right)=-1.$$

因此 $\left(\frac{24}{101}\right)=1$. ■

例 3.2.8 (1) 设 $p>3$ 是奇素数, 则

$$\left(\frac{3}{p}\right)=(-1)^{\frac{p-1}{2}\cdot\frac{3-1}{2}}\left(\frac{p}{3}\right)=(-1)^{\frac{p-1}{2}}\left(\frac{p}{3}\right).$$

由简单计算可知

$$\left(\frac{p}{3}\right)=\begin{cases}1 & \text{如果 } p\equiv 1 \pmod 3,\\ -1 & \text{如果 } p\equiv -1 \pmod 3.\end{cases}$$

另一方面

$$(-1)^{\frac{p-1}{2}}=\begin{cases}1 & \text{如果 } p\equiv 1 \pmod 4,\\ -1 & \text{如果 } p\equiv -1 \pmod 4.\end{cases}$$

由此得

$$\left(\frac{3}{p}\right)=\begin{cases}1 & \text{如果 } p\equiv \pm 1 \pmod{12},\\ -1 & \text{如果 } p\equiv \pm 5 \pmod{12}.\end{cases}$$

(2) 设 $p>5$ 是奇素数,

$$\left(\frac{5}{p}\right)=(-1)^{\frac{p-1}{2}\cdot\frac{5-1}{2}}\left(\frac{p}{5}\right)=\left(\frac{p}{5}\right)=\begin{cases}1 & \text{如果 } p\equiv \pm 1 \pmod 5,\\ -1 & \text{如果 } p\equiv \pm 2 \pmod 5.\end{cases}$$

■

为证明二次互反律, 我们需要一些准备工作. 设 p,q 是奇素数. 考虑 $\frac{1}{2}(p-1)$ 个数

$$q,\quad 2q,\quad \cdots,\quad \left(\frac{p-1}{2}\right)q$$

除以 p 的带余数除法

$$kq=q_kp+r_k,\quad 1\le r_k\le p-1,\quad q_k=\left[\frac{kq}{p}\right].$$

诸 r_k 中有 l 个小于 $\frac{p}{2}$, 我们重新记作 $a_1,\cdots,a_l$; 有 m 个大于 $\frac{p}{2}$, 重新记作 $b_1,\cdots,b_m$ (这里 $l+m=\frac{p-1}{2}$). 为计算方便, 我们令

$$a=\sum_{j=1}^{l}a_j,\quad b=\sum_{i=1}^{m}b_i. \tag{3-16}$$

显然

$$\sum_{k=1}^{\frac{p-1}{2}}r_k=a+b.$$

另一方面, 由上一节的证明可知, 诸 a_j 和 $p-b_i$ 恰好无重复地跑遍 1 到 $\frac{1}{2}(p-1)$ 之间所有整数, 因此

$$\frac{p^2-1}{8}=1+2+\cdots+\frac{1}{2}(p-1)=a+pm-b. \tag{3-17}$$

注意到

$$\sum_{k=1}^{\frac{p-1}{2}}r_k\equiv\sum_{k=1}^{\frac{p-1}{2}}kq-p\sum_{k=1}^{\frac{p-1}{2}}q_k\equiv\sum_{k=1}^{\frac{p-1}{2}}k-\sum_{k=1}^{\frac{p-1}{2}}q_k\equiv\frac{p^2-1}{8}-\sum_{k=1}^{\frac{1}{2}(p-1)}q_k\pmod 2.$$

将 (3-16) 和 (3-17) 代入上式得

$$m\equiv\sum_{k=1}^{\frac{p-1}{2}}q_k\pmod 2.$$

因此由高斯引理得

$$\left(\frac{q}{p}\right)=(-1)^m=(-1)^{\sum\limits_{k=1}^{\frac{1}{2}(p-1)}q_k}=(-1)^{\sum\limits_{k=1}^{\frac{1}{2}(p-1)}\left[\frac{kq}{p}\right]}. \tag{3-18}$$

同理也有

$$\left(\frac{p}{q}\right)=(-1)^{\sum\limits_{l=1}^{\frac{1}{2}(q-1)}\left[\frac{lp}{q}\right]}. \tag{3-19}$$

由式 (3-18) 和式 (3-19) 得

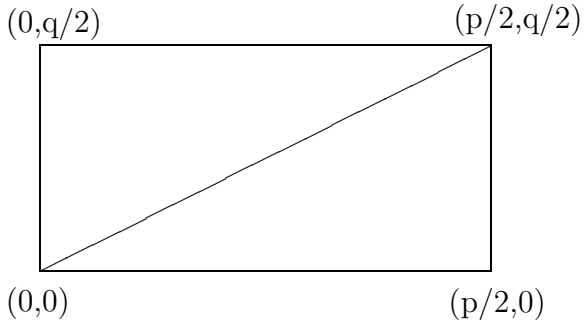
$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right)=(-1)^{\sum\limits_{k=1}^{\frac{1}{2}(p-1)}\left[\frac{kq}{p}\right]+\sum\limits_{l=1}^{\frac{1}{2}(q-1)}\left[\frac{lp}{q}\right]}. \tag{3-20}$$

因此我们只需要证明以下引理即得互反律.

引理 3.2.2 (**爱森斯坦**)

$$\sum_{k=1}^{\frac{1}{2}(p-1)}\left[\frac{kq}{p}\right]+\sum_{l=1}^{\frac{1}{2}(q-1)}\left[\frac{lp}{q}\right]=\frac{p-1}{2}\cdot\frac{q-1}{2}.$$

证明 作一长方形以 $(0,0),(0,q/2),(p/2,q/2),(p/2,0)$ 为顶点.



此长方形内整数点个数为

$$\frac{p-1}{2}\cdot\frac{q-1}{2}.$$

长方形对角线方程 $qx-py=0$. 若该对角线上含有整数点, 则推知 $p\mid x, q\mid y$, 但这样的点

不在长方形内. 由直接计算可知, 对角线之下的三角形内整数点个数为

$$\sum_{k=1}^{\frac{1}{2}(p-1)} \left[\frac{kq}{p}\right],$$

对角线之上的三角形内整数点个数为

$$\sum_{l=1}^{\frac{1}{2}(q-1)} \left[\frac{lp}{q}\right]$$

由此立得结论. ■

二次互反律的证明: 由引理 3.2.2 和式 (3-20) 立得. ■

3.2.6 应用 (III): 梅森素数的判别

我们定义*梅森数列*

$$M_p = 2^p - 1,$$

这里 p 跑遍所有的素数. 开头的几个梅森数是

$$M_2 = 3, \quad M_3 = 7, \quad M_5 = 31, \quad M_7 = 127, \quad M_{11} = 2047 = 23 \times 89, \cdots$$

如果一个梅森数是素数, 则称之为*梅森素数*.

我们利用平方剩余的知识来证明如下结论.

命题 3.2.2 *假设 p 是奇素数, 如果 $p \equiv 3 \pmod 4$ 且 $2p+1$ 也是素数, 则*

$$2p+1 \mid M_p,$$

因而 M_p 不是素数.

证明 设 $q = 2p+1$. 由 $q \equiv 7 \pmod 8$ 及推论 3.2.7,

$$\left(\frac{2}{q}\right) = (-1)^{\frac{q^2-1}{8}} = 1.$$

再由欧拉定理,

$$2^p = 2^{\frac{q-1}{2}} \equiv 1 \pmod q,$$

即 $q \mid M_p$. ■

例 3.2.9 分别取 $p = 11, 23, 83$, 我们有

$$23 \mid M_{11}, \quad 47 \mid M_{23}, \quad 167 \mid M_{83}.$$

梅森素数和偶完全数关系密切. 设 n 是正整数, 我们用

$$\sigma(n) = \sum_{d \mid n} d$$

来表示 n 的所有正因子之和. 如果 $\sigma(n) = 2n$, 则称之为*完全数*.

命题 3.2.3 *一个正偶数 n 是完全数的充分必要条件为: n 可写成以下形式*

$$n = \frac{1}{2}p(p+1),$$

这里 p 是梅森素数.

证明 ($\Longleftarrow$) 设 $p=2^r-1$ 是梅森素数, $n=\frac{1}{2}p(p+1)$, 则 $n=2^{r-1}(2^r-1)$ 的所有正因子如下:

$$1,\quad 2,\quad 2^2,\quad \cdots,\quad 2^{r-1},\quad 2^r-1,\quad 2(2^r-1),\quad 2^2(2^r-1),\quad \cdots,\quad 2^{r-1}(2^r-1).$$

因此 $\sigma(n)=2n$.

($\Longrightarrow$) 假设 n 是偶完全数. 容易验证 n 不是 2 的方幂. 不妨设 $n=2^{r-1}u$, 这里 $u>1$ 是奇数, $r\geq 2$. n 中的因子都可以写为 2^id $(i=0,1,\cdots,r-1)$, 这里d 是 u 的正因子. 因此

$$\sigma(n)=\sum_{i=0}^{r-1}\sum_{d|u}2^id=\sum_{i=0}^{r-1}2^i\sigma(u)=(2^r-1)\sigma(u).$$

由假设条件及以上等式, 我们有

$$2^ru=2n=\sigma(n)=(2^r-1)\sigma(u).$$

因此

$$\sigma(u)=\frac{2^ru}{(2^r-1)}=u+\frac{u}{2^r-1}. \tag{3-21}$$

这表明 $2^r-1,\frac{u}{2^r-1},u$ 都是 u 的正因子. 如果 $\frac{u}{2^r-1}>1$, 则由 σ 的定义可知

$$\sigma(u)\geq u+1+\frac{u}{2^r-1},$$

与 (3-21) 矛盾! 因此 $u=2^r-1$. 如果 u 不是素数, 则 $\sigma(u)>1+u$, 仍与 (3-21) 矛盾! 因此 u 是梅森素数. ■

3.2.7 雅克比符号

在使用二次互反律时, 我们要求分子分母都是奇素数. 但在平时计算中, 分子往往是合数, 所以需要先做素因子分解, 这样非常不便于计算. 为此我们引进雅克比符号.

定义 3.2.2 设 $m>1$ 是奇数, $m=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_s^{\alpha_s}$ 是标准素因子分解式, n 是与 m 互质的整数, 我们定义雅克比符号

$$\left(\frac{n}{m}\right):=\left(\frac{n}{p_1}\right)^{\alpha_1}\left(\frac{n}{p_2}\right)^{\alpha_2}\cdots\left(\frac{n}{p_s}\right)^{\alpha_s}.$$

例 3.2.10 由定义, 我们总是有 $\left(\frac{n^2}{m}\right)=1$. 特别地, $\left(\frac{1}{m}\right)=1$. ■

例 3.2.11 (1) $\left(\frac{n}{m}\right)=1$ 不表示同余方程 $x^2\equiv n\pmod m$ 一定有解, 比如

$$\left(\frac{-1}{49}\right)=\left(\frac{-1}{7}\right)^2=1.$$

但是 $x^2\equiv -1\pmod{49}$ 无解. 这是因为若它有解则推知 $x^2\equiv -1\pmod 7$ 有解, 但 -1 在模 7 是平方非剩余.

(2) $\left(\frac{n}{m}\right)=-1$ 则能推出同余方程 $x^2\equiv n\pmod m$ 必定无解. 这是因为, 由雅克比符号定义可知, 存在素因子 p_i 使得 $\left(\frac{n}{p_i}\right)=-1$, 即 n 在模 p_i 下平方非剩余. 倘若方程 $x^2\equiv n\pmod m$ 有解, 则 $x^2\equiv n\pmod{p_i}$ 亦有解, 矛盾! ■

上例表明雅克比符号并不像勒让德符号那样具有明确的意义, 它仅仅是为了计算方便才引入了. 下面我们罗列一些雅克比符号的性质.

命题 3.2.4 设 $m, m' > 1$ 是奇数, n 是与 m, m' 互质的整数, 那么

(1) 若 $n \equiv n' \pmod{m}$, 则 $\left(\frac{n}{m}\right) = \left(\frac{n'}{m}\right)$.

(2)
$$\left(\frac{n}{m}\right)\left(\frac{n}{m'}\right) = \left(\frac{n}{mm'}\right).$$

(3) 设 $(n', m) = 1$, 则
$$\left(\frac{n}{m}\right)\left(\frac{n'}{m}\right) = \left(\frac{nn'}{m}\right).$$

(4) $\left(\frac{-1}{m}\right) = (-1)^{\frac{m-1}{2}}$.

(5) $\left(\frac{2}{m}\right) = (-1)^{\frac{m^2-1}{8}}$.

(6) 设 $n > 1$ 是奇数, 则
$$\left(\frac{n}{m}\right)\left(\frac{m}{n}\right) = (-1)^{\frac{m-1}{2}\cdot\frac{n-1}{2}}.$$

为证明上述结论, 我们需要一些准备工作.

引理 3.2.3 对任何奇数 u, v, 我们有

(1)
$$\frac{u-1}{2} + \frac{v-1}{2} \equiv \frac{uv-1}{2} \pmod{2},$$

(2)
$$\frac{u^2-1}{8} + \frac{v^2-1}{8} \equiv \frac{u^2v^2-1}{8} \pmod{2}.$$

证明 (1)
$$\frac{uv-1}{2} - \left(\frac{u-1}{2} + \frac{v-1}{2}\right) = \frac{(u-1)(v-1)}{2} = 2\left(\frac{u-1}{2}\cdot\frac{v-1}{2}\right),$$

由此即得第一个等式.

(2)
$$\frac{u^2v^2-1}{8} - \left(\frac{u^2-1}{8} + \frac{v^2-1}{8}\right) = \frac{(u^2-1)(v^2-1)}{8} = 2\left(\frac{u^2-1}{4}\cdot\frac{v^2-1}{4}\right),$$

这就推得第二个等式. ■

由归纳法及以上引理立得如下结论.

推论 3.2.9 设 $q_1, \cdots, q_t$ 是奇数, 则

(1)
$$\sum_{k=1}^{t}\frac{q_k-1}{2} \equiv \frac{\prod_{k=1}^{t} q_k - 1}{2} \pmod{2}.$$

(2)

$$\sum_{k=1}^{t}\frac{q_k^2-1}{8}\equiv\frac{\prod\limits_{k=1}^{t}q_k^2-1}{8}\pmod 2.$$

命题 3.2.4 的证明: (1) (2) (3) 直接来自于雅克比符号定义和勒让德符号的基本性质.

(4) 设 $m=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_s^{\alpha_s}$ 是标准素因子分解式.

$$\left(\frac{-1}{m}\right)=\left(\frac{-1}{p_1}\right)^{\alpha_1}\cdots\left(\frac{-1}{p_s}\right)^{\alpha_s}=(-1)^{\alpha_1\frac{p_1-1}{2}+\cdots+\alpha_s\frac{p_s-1}{2}}$$

由推论 3.2.9 (1) 得

$$\alpha_1\frac{p_1-1}{2}+\cdots+\alpha_s\frac{p_s-1}{2}\equiv\frac{m-1}{2}\pmod 2.$$

这就得到了结论.

应用推论 3.2.9 (2) 也可以类似得到 (5). 我们留给读者完成证明.

(6) 设 $n=q_1^{\beta_1}\cdots q_t^{\beta_t}$ 是标准素因子分解式.

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right)=\left(\prod_{i=1}^{s}\prod_{j=1}^{t}\left(\frac{p_i}{q_j}\right)^{\alpha_i\beta_j}\right)\cdot\left(\prod_{i=1}^{s}\prod_{j=1}^{t}\left(\frac{q_j}{p_i}\right)^{\alpha_i\beta_j}\right)=\prod_{i=1}^{s}\prod_{j=1}^{t}\left(\left(\frac{p_i}{q_j}\right)\left(\frac{q_j}{p_i}\right)\right)^{\alpha_i\beta_j}.$$

由二次互反律, 上式可进一步化简为

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right)=\prod_{i=1}^{s}\prod_{j=1}^{t}(-1)^{\frac{p_i-1}{2}\cdot\frac{q_j-1}{2}\cdot\alpha_i\beta_j}$$

这样, 我们只需要验证

$$\sum_{i=1}^{s}\sum_{j=1}^{t}\frac{p_i-1}{2}\cdot\frac{q_j-1}{2}\cdot\alpha_i\beta_j\equiv\frac{m-1}{2}\cdot\frac{n-1}{2}\pmod 2.\tag{3-22}$$

由推论 3.2.9 (1), 上式左端在模 2 下同余于

$$\sum_{i=1}^{s}\alpha_i\cdot\frac{p_i-1}{2}\left(\sum_{j=1}^{t}\beta_j\cdot\frac{q_j-1}{2}\right)\equiv\sum_{i=1}^{s}\alpha_i\cdot\frac{p_i-1}{2}\cdot\left(\frac{n-1}{2}\right)\equiv\left(\frac{m-1}{2}\right)\left(\frac{n-1}{2}\right)\pmod 2.$$

这就证明了式 (3-22). ■

例 3.2.12 已知 $383, 443$ 是素数, 求勒让德符号 $\left(\frac{383}{443}\right)$.

$$\left(\frac{383}{443}\right)=-\left(\frac{443}{383}\right)=-\left(\frac{60}{383}\right)=-\left(\frac{4}{383}\right)\left(\frac{15}{383}\right)=-\left(\frac{15}{383}\right).$$

上式右端视作雅克比符号, 则可进一步应用互反律, 而无需进一步分解分子的素因子,

$$-\left(\frac{15}{383}\right)=\left(\frac{383}{15}\right)=\left(\frac{8}{15}\right)=\left(\frac{2}{15}\right)=1.$$

这就推知勒让德符号 $\left(\frac{383}{443}\right)=1$. ■

3.2.8 一般情形的二次同余式的求解算法

设 p 是奇素数, $\ell > 0$. 我们考虑求解如下方程

$$x^2 \equiv n \pmod{p^\ell}, \quad p \nmid n.$$

如果 $\ell = 1$, 那么由第 3.2.3 节的讨论, 我们已经知道如何求解上述同余方程. 此时同余解数为 2. 今讨论 $\ell = 2$ 的情形. 假设 x 为一解, 满足

$$x^2 \equiv n \pmod{p^2}, \tag{3-23}$$

则 x 显然也满足

$$x^2 \equiv n \pmod{p}. \tag{3-24}$$

不妨设 $x \equiv a_0 \pmod{p}$ 是方程 (3-24) 的同余解. 令 $x = a_0 + py$ 代入方程 (3-23),

$$a_0^2 + 2pa_0y + p^2y^2 \equiv n \pmod{p^2}.$$

进一步简化上式即得

$$\frac{a_0^2 - n}{p} + 2a_0y \equiv 0 \pmod{p}, \tag{3-25}$$

式 (3-25) 是一次同余方程, 它有唯一的剩余类解 $y \equiv a_1 \pmod{p}$, 这样我们就得到原方程 (3-23) 的解 $x \equiv a_0 + a_1p \pmod{p^2}$. 注意到方程 (3-24) 恰有两解, 所以方程 (3-23) 的解数仍是 2. 显然另一解就是 $x \equiv -(a_0 + a_1p) \pmod{p^2}$.

例 3.2.13 求同余方程 $x^2 \equiv -7 \pmod{37^2}$ 的剩余类解.

首先解方程

$$x^2 \equiv -7 \pmod{37}.$$

由第 3.2.3 节的讨论, 可得 $x \equiv \pm 17 \pmod{37}$.

令 $x = 17 + 37y$ 代入原方程化简得

$$8 + 34y \equiv 0 \pmod{37},$$

其解为 $y \equiv 15 \pmod{37}$.

这样, 我们得到原方程的解 $x \equiv \pm(17 + 37 \cdot 15) \equiv \pm 572 \pmod{37^2}$. ■

例 3.2.14 $p = 2$ 与奇素数的情形略有不同.

(1) 当 $\ell = 1$ 时, 方程 $x^2 \equiv 1 \pmod{2}$ 显然仅有一解.

(2) 当 $\ell = 2$ 时, 方程 $x^2 \equiv 1 \pmod{4}$ 有两解 $x \equiv 1, 3 \pmod{4}$.

(3) 当 $\ell \geq 3$ 且 $n \equiv 1 \pmod{8}$ 时, 方程 $x^2 \equiv 1 \pmod{2^\ell}$ 有四个解.

(4) 当 $\ell \geq 3$ 且 $n \not\equiv 1 \pmod{8}$ 时, 方程 $x^2 \equiv 1 \pmod{2^\ell}$ 无解.

比如 $x^2 \equiv 9 \pmod{16}$ 有四个解

$$x \equiv \pm 3, \pm 5 \pmod{16}.$$

我们也可以考虑更一般的情形. 假设已经求出

$$x^2 \equiv n \pmod{p^{\ell-1}}$$

的解 $x \equiv \pm x_0 \pmod{p^{\ell-1}}$. 设 $x = x_0 + p^{\ell-1}y$ 代入方程

$$x^2 \equiv n \pmod{p^\ell} \tag{3-26}$$

化简得

$$\frac{x_0^2 - n}{p^\ell} + 2x_0 y \equiv 0 \pmod{p}.$$

由此可求出唯一的 y 满足 $0 < y < p$, 从而可求得方程 (3-26) 的解.

进一步, 我们可以求解更一般情形的二次同余式

$$x^2 \equiv n \pmod{m}. \tag{3-27}$$

设 $m = p_1^{\alpha_1} \cdots p_s^{\alpha_s}$ 是标准素因子分解式. 上述方程等价于求方程组

$$\begin{cases} x^2 \equiv n \pmod{p_1^{\alpha_1}}, \\ \cdots \quad \cdots \quad \cdots \\ x^2 \equiv n \pmod{p_s^{\alpha_s}}. \end{cases}$$

假设每个方程的解存在. 设 $x \equiv \pm a_i \pmod{p_i^{\alpha_i}}$ 是方程 $x^2 \equiv n \pmod{p_i^{\alpha_i}}$ 的任一解. 那么方程组 (3-27) 进一步归结为

$$\begin{cases} x \equiv a_1 \pmod{p_1^{\alpha_1}}, \\ \cdots \quad \cdots \quad \cdots \\ x \equiv a_s \pmod{p_s^{\alpha_s}}. \end{cases}$$

由孙子定理, 即可求出方程组 (3-27) 的一个解. 其余解可类似求出.

例 3.2.15 求 $x^2 \equiv 11 \pmod{35}$ 的剩余类解.

这等价于求

$$\begin{cases} x^2 \equiv 11 \pmod{5}, \\ x^2 \equiv 11 \pmod{7}. \end{cases}$$

进一步可简化为

$$\begin{cases} x \equiv \pm 1 \pmod{5}, \\ x^2 \equiv \pm 2 \pmod{7}. \end{cases}$$

因此由孙子定理得解 $x \equiv \pm 16, \pm 9 \pmod{35}$. ■

3.3 平方和问题

这一节将讨论如下不定方程

$$n = x^2 + y^2$$

的整数解 (x, y), 这里 n 是给定的正整数. 如果方程有解, 我们就说 n 能表为两个整数的平方和. 从几何个角度看, 我们相当于要在半径为 $\sqrt{n}$, 圆心在原点的圆周上寻找整数点.

例 3.3.1

$$1 = 1^2 + 0^2, \quad 2 = 1^2 + 1^2, \quad 5 = 1^2 + 2^2, \quad 13 = 2^2 + 3^2, \quad 17 = 1^2 + 4^2, \cdots$$

然而不是所有正整数都能表为两个整数的平方和, 比如 $n=3,7,11$ 等. ■

3.3.1 费马–欧拉定理

我们要证明如下著名结论—费马平方和定理. 这个结果由费马最早发现, 欧拉后来给出了严格证明.

定理 3.3.1 (费马–欧拉定理) *正整数 n 可表为两个数的平方和当且仅当 n 的每个形如 $4m+3$ 的素因子在 n 的标准分解式中的方幂都是偶数.*

首先讨论 $n=p$ 是奇素数的情形.

引理 3.3.1 *如果奇素数 $p\equiv 3 \pmod 4$, 则它不能表为两个平方数之和.*

证明 假设 $p=x^2+y^2$, 则 x,y 一奇一偶, 从而

$$p\equiv x^2+y^2\equiv 1^2+0^2\equiv 1 \pmod 4.$$

这就与命题条件矛盾! ■

引理 3.3.2 *如果奇素数 $p\equiv 1 \pmod 4$, 则它可表为两个平方数之和.*

证明 此时 $\left(\frac{-1}{p}\right)=1$, 因此存在整数 s 使得 $s^2\equiv -1 \pmod p$.
今考虑集合

$$X=\{(a,b)\mid a,b\in\mathbb{Z},\ 0\le a,b\le\sqrt{p}\}.$$

易知 X 中的元素个数是 $|X|=([\sqrt{p}]+1)^2$. 注意到 $|X|>p$, 所以由抽屉原理可知, 必定存在两个不同的数对

$$(a,b),(c,d)\in X,$$

使得 $a-sb\equiv c-sd \pmod p$. 令

$$x=|a-c|,\quad y=|b-d|,$$

这就有 $x\equiv\pm sy \pmod p$ ($\pm$ 号取决于 $b-d$ 的正负). 因而

$$x^2\equiv s^2y^2\equiv -y^2 \pmod p.$$

这就推出 $p\mid x^2+y^2$. 因为 $x,y<\sqrt{p}$, 所以 $0<x^2+y^2<2p$, 因此

$$p=x^2+y^2.$$

至此, 我们完成证明. ■

注 3.3.1 事实上, 形如 $4m+1$ 的素数的平方和表示是唯一的. ■

引理 3.3.3 *设奇素数 p 满足 $p\equiv 3 \pmod 4$, 正整数 n 可表为两个整数的平方和, 且 $p\mid n$, 那么必有 $p^2\mid n$, 并且 $\frac{n}{p^2}$ 也能表为两平方数之和.*

证明 设 $n=x^2+y^2$. 如果 $p\nmid x$, 则存在整数 x^* 使得 $xx^*\equiv 1 \pmod p$. 因为 $x^2+y^2\equiv 0 \pmod p$, 所以

$$y^2x^{*2}\equiv(-x^2)x^{*2}\equiv -1 \pmod p.$$

这意味着 -1 在模 p 下是平方剩余, 即 $1 = (\frac{-1}{p}) = (-1)^{\frac{p-1}{2}}$, 这与 $p \equiv 3 \pmod 4$ 矛盾! 因此 $p \mid x$, 从而 $p \mid y$. 这样,

$$\frac{n}{p^2} = \left(\frac{x}{p}\right)^2 + \left(\frac{y}{p}\right)^2 \in \mathbb{Z}.$$

由此即得结论. ■

引理 3.3.4 设 $n = a^2 + b^2$, $m = c^2 + d^2$, 则

$$mn = (ac - bd)^2 + (ad + bc)^2.$$

特别地, 对任何整数 z, nz^2 也能表为两平方和: $nz^2 = (az)^2 + (bz)^2$.

费马–欧拉定理的证明:

充分性. 已知 n 的素因子分解中所有形如 $4m + 3$ 的素因子的方幂都是偶数. 这样我们能将 n 写为

$$n = 2^r \cdot u^2 \cdot v, \quad 2 \nmid uv, \quad r \geq 0,$$

其中 u 是那些形如 $4m+3$ 的素因子乘积; v 是那些形如 $4m+1$ 的素因子乘积. 注意到 $2 = 1^2+1^2$, 每个形如 $4m + 1$ 的素因子也能表为平方和 (引理 3.3.2), 所有由引理 3.3.4 可知 n 也能表为两个整数的平方和.

必要性. 已知 n 能表为两个整数的平方和. 假设存在这样的正整数 n, 使得某个形如 $4m + 3$ 的素因子 p 在 n 的标准分解式中方幂是奇数. 我们不妨设 n 是满足上述条件的最小正整数. 那么由引理 3.3.3, $\frac{n}{p^2}$ 是整数, 并且也可表为两平方和. 但显然 $\frac{n}{p^2}$ 的分解式中 p 的方幂仍是奇数. 这就和 n 的最小性矛盾! ■

设 $r(n)$ 是方程 $n = x^2 + y^2$ 的整数解个数. 我们罗列如下优美结果. 它的证明可以参看 [Hua57].

命题 3.3.1

$$r(n) = 4 \sum_{\substack{d \mid n, \\ 2 \nmid d}} (-1)^{\frac{d-1}{2}},$$

这里 d 跑遍 n 的所有正的奇数因子.

特别地, 当 p 是形如 $4m + 1$ 的奇素数时, 方程恰有 8 解. 如果不考虑正负号以及顺序的话, 这表明 p 能唯一分解成两个平方数之和. 我们将在下一小节中用其他方法来直接证明这个结论.

3.3.2 高斯整数

费马平方和问题也可以用更高的代数观点去处理. 我们简要介绍一下这方面的内容.

首先考虑如下的复数集合

$$\mathbb{Z}[i] := \{a + bi \mid a, b \in \mathbb{Z}\},$$

这里 $i = \sqrt{-1}$ 是虚数单位. 这个集合通常叫做高斯整数环, 其中的元素叫做高斯整数. 显然 $\mathbb{Z} \subseteq \mathbb{Z}[i]$, $\mathbb{Z}[i]$ 上有自然的加减乘运算. 事实上, 我们还能类似整数情形那样定义高斯整数间的带余数除法.

命题 3.3.2　设 $\alpha,\beta\in\mathbb{Z}[i]$, $\beta\neq 0$, 则存在高斯整数 γ,ρ, 满足

$$\alpha=\gamma\beta+\rho,\quad |\rho|^2<|\beta|^2. \tag{3-28}$$

证明　设 $\frac{\alpha}{\beta}=x+yi$. 我们可以找到整数 s,t, 使得

$$|x-s|\leq\frac{1}{2},\quad |y-t|\leq\frac{1}{2}.$$

令 $\gamma=s+it\in\mathbb{Z}[i]$, 则

$$\left|\frac{\alpha}{\beta}-\gamma\right|\leq\frac{\sqrt{2}}{2}<1.$$

设 $\rho=\alpha-\gamma\beta$, 由上面不等式即得 $|\rho|<|\beta|$. ■

注 3.3.2　一般说来, 上面的带余数除法中的商和余数不一定是唯一的. 比如设 $\alpha=1+i$, $\beta=2$, 我们有两种带余数除法

$$\alpha=i\beta+(1-i),\quad \alpha=\beta+(-1+i).$$

我们也可以定义如下一些概念.

定义 3.3.1　设 $\alpha,\beta\in\mathbb{Z}[i]$, $\beta\neq 0$.
(1) 如果 $\frac{\alpha}{\beta}\in\mathbb{Z}[i]$, 那么我们说 β 整除 α, 记作 $\beta\mid\alpha$, β 称为 α 的因子.
(2) 如果 $\beta\mid\alpha$ 并且 $\alpha\mid\beta$, 那么我们称 α,β 是相伴的.
(3) $1,-1,i,-i$ 称作 $\mathbb{Z}[i]$ 中的单位元或者可逆元.
(4) $N(\alpha):=|\alpha|^2=\alpha\bar{\alpha}\in\mathbb{Z}$ 称作 α 的范数.

容易验证以下事实.

引理 3.3.5　设 $\alpha,\beta\in\mathbb{Z}[i]$,
(1) $\beta\mid\alpha$ 当且仅当带余除法 (3-28) 中的余数是零.
(2) α,β 相伴当且仅当 $\frac{\alpha}{\beta}$ 是 $\mathbb{Z}[i]$ 中的单位元.
(3) α 是单位元当且仅当 $N(\alpha)=1$, 也当且仅当 α 与 1 相伴.
(4) 如果 $\beta\mid\alpha$, 那么 $N(\beta)\mid N(\alpha)$. 特别地, α,β 相伴 当且仅当 $N(\alpha)=N(\beta)$.
(5) $N(\alpha\beta)=N(\alpha)N(\beta)$.

由带余数除法, 我们可以引进欧几里得算法 与公因子等等概念. 此外, 我们还可以定义 $\mathbb{Z}[i]$ 中类似"素数"的概念.

定义 3.3.2　如果高斯整数 α 除了自身与 1 的诸相伴元之外没有其他因子, 就称 α 是 $\mathbb{Z}[i]$ 中的不可约元.

进一步, 我们能得到 $\mathbb{Z}[i]$ 中的算术基本定理.

定理 3.3.2 (**算术基本定理**)　设 $\alpha\in\mathbb{Z}$ 不是单位元, 则存在分解式

$$\alpha=\varepsilon p_1^{\alpha_1}\cdots p_s^{\alpha_s},\quad \alpha_i\geq 1,$$

这里 ε 是单位元, 诸 p_i 是互不相伴的不可约元. 进一步, 这个表达式在相伴意义下是唯一的.

上面的这些讨论可以在很多代数数论或者抽象代数的书籍中找到, 有兴趣的读者可以查阅更多的相关内容. 我们这里不再赘述.

引理 3.3.6　*设奇素数 p 满足 $p \equiv 1 \pmod 4$, 则 p 不可能是 $\mathbb{Z}[i]$ 中的不可约元.*

证明　反证法. 假设 $p \in \mathbb{Z}[i]$ 是不可约元.

此时同余方程 $x^2 \equiv -1 \mod p$ 有解, 即存在整数 x 使得 $p \mid x^2+1$. 因为

$$x^2+1 = (x+i)(x-i),$$

所以由算术基本定理, 要么 $p \mid x+i$, 要么 $p \mid x-i$. 这等价于说 $\frac{x}{p} \pm \frac{i}{p}$ 中有一个是高斯整数, 但是注意到 $p \nmid x$, 这就得到矛盾! ■

现在我们可以重新证明比引理 3.3.2 稍强的结论.

命题 3.3.3　*设奇素数 p 满足 $p \equiv 1 \pmod 4$, 则 p 可以唯一地表达成两个正整数的平方和 (不考虑顺序).*

证明　由引理 3.3.6, 我们可以写

$$p = \alpha \cdot \beta,$$

这里 $\alpha, \beta \in \mathbb{Z}[i]$ 不与 1 或者 p 相伴. 因此 $N(\alpha), N(\beta) > 1$. 注意到

$$p^2 = N(p) = N(\alpha)N(\beta),$$

所以这就迫使 $p = N(\alpha) = N(\beta)$. 设 $\alpha = a+bi$, 则立得

$$p = a^2+b^2, \quad \beta = \bar{\alpha} = a-bi.$$

进一步, 我们可以证明 α, β 不可约. 若不然可设 $\alpha = \gamma \cdot \lambda$, 这里 $\gamma, \lambda \in \mathbb{Z}[i]$ 不与 1 或者 α 相伴. 因而 $p = N(\alpha) = N(\gamma)N(\lambda)$. 这意味着 $N(\gamma), N(\lambda)$ 中的一个等于 1, 矛盾!

假如存在另一分解 $p = c^2+d^2$, 则

$$p = (c+di)(c-di) = (a+bi)(a-bi).$$

由算术基本定理, 这意味着 $a+bi$ 与 $c \pm di$ 中的一个相伴. 这就推出要么 $|a| = |c|, |b| = |d|$, 要么 $|a| = |d|, |b| = |c|$. 因此 p 只能唯一分解为两个正整数的平方和. ■

结合上面的讨论, 我们可以完整地刻画所有 $\mathbb{Z}[i]$ 中的不可约元.

定理 3.3.3　*$\mathbb{Z}[i]$ 中的任何不可约元 π 必定相伴于以下某类不可约元:*
(1) $1+i$,
(2) $a+bi$, *这里要求 $p = a^2+b^2$ 是满足 $p \equiv 1 \pmod 4$ 的奇素数, 且 $a > |b| > 0$,*
(3) p, *这里 p 是满足 $p \equiv 3 \pmod 4$ 的奇素数.*

证明　首先验证上面三类高斯整数是不可约的. 设 π 是 (1)(2) 类型. 如果 $\pi = \alpha \cdot \beta$, 则

$$p = N(\pi) = N(\alpha)N(\beta)$$

蕴含着 $N(\alpha), N(\beta)$ 中的一个等于 1, 也就是说 α, β 中有一个是单位元. 因此 π 是不可约的.

设 π 是类型 (3), $\pi = \alpha \cdot \beta$, 则

$$p^2 = N(\pi) = N(\alpha)N(\beta).$$

如果 $p = N(\alpha) = N(\beta)$, 这就推出 p 可以表为两整数的平方和, 因而 $p \equiv 1 \pmod 4$, 矛盾! 因此 $N(\alpha), N(\beta)$ 中的一个等于 1, 再次推出 π 是不可约的.

其次证明每个不可约元必相伴于其中一类. 设 π 是不可约元. 将 $N(\pi)$ 在整数内分解为素数乘积

$$N(\pi) = \pi\bar{\pi} = p_1 p_2 \cdots p_s,$$

这里诸 p_k 是素数 (允许相同). 在 $\mathbb{Z}[i]$ 里看, 由算术基本定理可得 $\pi \mid p_k$ 对某个 p_k 成立. 因此 $N(\pi) \mid N(p_k) = p_k^2$. 如果 $N(\pi) = p_k$, 设 $\pi = a + bi$, 则 $p = a^2 + b^2$, 这表明 π 相伴于类型 (1)(2) 的不可约元.

如果 $N(\pi) = p_k^2$, 那么由 $N(p_k) = p_k^2$ 可知 π, p_k 相伴. 因而 p_k 必须是类型 (3) 的不可约元 (否则由前面讨论, 它可以被前两类不可约元整除). ■

3.3.3 补充材料: 华林问题简介

虽然并非每个正整数都能写成两个整数的平方和, 但我们有如下漂亮的结论.

定理 3.3.4 (**拉格朗日**) 任何正整数可以写成四个平方数之和.

华林 (Waring) 于 1770 年提出如下猜想:

任何正整数必可表为 9 个立方数之和; 19 个四次方数之和; 37 个五次方数之和.....

更一般地, 给定正整数 k, 是否存在正整数 $s = s(k)$, 使得对任何正整数 n, 方程

$$n = x_1^k + \cdots + x_s^k$$

总是整数解? 这就是著名的华林问题. 希尔伯特最早证明了这个结论, 故称之为华林-希尔伯特定理.

设 $g(k)$ 是华林问题中满足性质的最小 s. 华林问题可等价表述为

$$g(2) = 4, \quad g(3) = 9, \quad g(4) = 19, \quad g(5) = 37, \cdots$$

我们这里证明一个初等的结果.

命题 3.3.4

$$g(k) \geq 2^k + \left[\left(\frac{3}{2}\right)^k\right] - 2.$$

特别地, $g(2) \geq 4$, $g(3) \geq 9$, $g(4) \geq 19$, $g(5) \geq 37$.

证明 令 $q = \left[\left(\frac{3}{2}\right)^k\right]$, $n = 2^k q - 1$, 则 $n < 3^k$. 因此如果将 n 分解为 k 次方幂之和, 则其中每个方幂要么是 1^k, 要么是 2^k. 所有可能的这类分解中,

$$n = \underbrace{2^k + \cdots + 2^k}_{q-1} + \underbrace{1^k + \cdots + 1^k}_{2^k - 1}$$

的分解项数达到最小. 因此

$$g(k) \geq (q-1) + (2^k - 1).$$

这就得到了所需结论. ■

一个有趣的问题是, 上述不等式的等号何时成立? 华罗庚及 K. Mahler 的结果证明, 存在整数 k_0, 当 $k > k_0$ 时, 等号成立, 即有

$$g(k) = 2^k + \left[\left(\frac{3}{2}\right)^k\right] - 2.$$

那么 k_0 具体可以是多少? 人们却无法计算出来.

3.4 佩尔方程与连分数算法

这一节将讨论如下的双曲线方程的整数解:

$$x^2 - dy^2 = 1,$$

这里 $d > 1$ 是正整数. 该不定方程称为*佩尔方程*, 实际上与佩尔无关, 乃是因欧拉所著一书误传所致. 此方程最早的系统研究者实可追溯至古印度的 Brahmagupta.

为方便讨论, 以下不妨假设 d 不含平方因子 (即 d 的任何素因子在分解式中都是 1 重的). 求解佩尔方程的技巧与所谓的连分数理论有着极为密切的关系. 因此我们首先介绍连分数的一些基础知识.

3.4.1 连分数的基础知识

考虑分数

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots + \cfrac{1}{a_N}}}}$$

如果 N 是有限数, 则该分数称为*有限连分数*, 若 $N = \infty$, 则简称为*连分数*. 有时为了书写方便, 我们也简记连分数为

$$[a_0, a_1, \cdots, a_N].$$

无限连分数相当于以下极限 (如果存在的话)

$$\lim_{n\to\infty} [a_0, \cdots, a_n].$$

例 3.4.1 (1) $2 = [1,1] = [2]$, $3/2 = [1,1,1] = [1,2]$, 更一般地,

$$\frac{F_n}{F_{n-1}} = [\underbrace{1,1,\cdots,1}_{n}] = [\underbrace{1,1,\cdots,1}_{n-2},2] = [1, \frac{F_{n-1}}{F_{n-2}}],$$

这里 F_n 是斐波那契数, $F_0 = 1$, $F_1 = 1$, $F_n = F_{n-1} + F_{n-2}$.

(2) 无限连分数

$$\frac{1+\sqrt{5}}{2}=[1,1,1,\cdots,1\cdots].$$

求法如下: 设 $\alpha=[1,1,1,\cdots,1\cdots]$, 则得 $\alpha=[1,\alpha]$, 由此解出上述值. ■

我们记

$$[a_0,\cdots,a_n]=\frac{p_n}{q_n},\quad n=0,\cdots,N.$$

它称为 $[a_0,\cdots,a_N]$ 的第 n 个渐近分数或渐近值.

命题 3.4.1 p_n,q_n 满足以下递推关系:

$$p_0=a_0,\quad p_1=a_1a_0+1,\quad p_n=a_np_{n-1}+p_{n-2},$$

及

$$q_0=1,\quad p_1=a_1,\quad q_n=a_nq_{n-1}+q_{n-2}.$$

证明 我们以归纳法证明. $n=0,1$ 时可直接验证. 假设 $n\le m$ 情形已证.

$$\begin{aligned}\frac{p_{m+1}}{q_{m+1}}&=[a_0,\cdots,a_{m+1}]=[a_0,\cdots,a_{m-1},a_m+\frac{1}{a_{m+1}}]\\&=\frac{\left(a_m+\frac{1}{a_{m+1}}\right)p_{m-1}+p_{m-2}}{\left(a_m+\frac{1}{a_{m+1}}\right)q_{m-1}+q_{m-2}}=\frac{a_{m+1}\left(a_mp_{m-1}+p_{m-2}\right)+p_{m-1}}{a_{m+1}\left(a_mq_{m-1}+q_{m-2}\right)+q_{m-1}}\\&=\frac{a_{m+1}p_m+p_{m-1}}{a_{m+1}q_m+q_{m-1}}\end{aligned}$$

由此即得结论. ■

推论 3.4.1 设 p_n,q_n 同上, 则有

$$p_nq_{n-1}-p_{n-1}q_n=(-1)^{n-1},\quad n\ge 1,$$

及

$$p_nq_{n-2}-p_{n-2}q_n=(-1)^na_n,\quad n\ge 2.$$

证明 $n=1$ 时, 第一式显然成立. 注意到

$$p_nq_{n-1}-p_{n-1}q_n=(a_np_{n-1}+p_{n-2})q_{n-1}-p_{n-1}(a_nq_{n-1}+q_{n-2})=-(p_{n-1}q_{n-2}-p_{n-2}q_{n-1}),$$

则由归纳法立得第一式.

因为

$$p_nq_{n-2}-p_{n-2}q_n=(a_np_{n-1}+p_{n-2})q_{n-2}-p_{n-2}(a_nq_{n-1}+q_{n-2})=a_n(p_{n-1}q_{n-2}-p_{n-2}q_{n-1}),$$

故由第一式即得后一等式. ■

定义 3.4.1 如果 $a_0\in\mathbb{Z}$, 且其余诸 a_i 是正整数, 则称连分数 $[a_0,a_1,\cdots]$ 为简单连分数.

以下如无特别声明, 我们只考虑简单连分数.

推论 3.4.2　对简单连分数, 我们有

(1) $q_n > q_{n-1}$, 因此 $q_n \geq n$.

(2) $\frac{p_{2n+1}}{q_{2n+1}} < \frac{p_{2n-1}}{q_{2n-1}}$, $\frac{p_{2n}}{q_{2n}} > \frac{p_{2n-2}}{q_{2n-2}}$.

(3) $(p_n, q_n) = 1$.

证明　(1) 直接来自于递推关系式.

(2) (3) 直接来自于推论 3.4.1. ■

下面的初等结论解释了有限简单连分数和欧几里得算法的关系.

推论 3.4.3　考虑正整数 a, b 的欧几里德算法

$$\begin{cases} a &= ba_0 + r_1, & 0 \leq r_1 < b \\ b &= r_1a_1 + r_2, & 0 \leq r_2 < r_1 \\ r_1 &= r_2a_2 + r_3, & 0 \leq r_3 < r_2 \\ &\cdots & \cdots \\ r_{n-1} &= r_na_n + r_{n+1}, & r_{n+1} = 0, \end{cases} \tag{3-29}$$

这里 $r_n = (a, b)$, 则 $\frac{a}{b}$ 可展开成如下的简单连分数

$$\frac{a}{b} = [a_0, a_1, \cdots, a_n].$$

设 $\frac{p_{n-1}}{q_{n-1}} = [a_0, \cdots, a_{n-1}]$ 是第 $n-1$ 个渐近分数, 则

$$aq_{n-1} - bp_{n-1} = (-1)^{n-1}(a, b).$$

利用上面推论, 我们可以快速求出一次不定方程 $ax + by = (a, b)$ 的特解 (比较推论 2.2.4), 即

$$x = (-1)^{n-1}q_{n-1}, \quad y = (-1)^n p_{n-1}.$$

例 3.4.2　(1) 求不定方程 $39x + 23y = 1$ 的整数解.

用欧几里得算法展开 $\frac{39}{23}$ 成简单连分数

$$\frac{39}{23} = [1, 1, 2, 2, 2],$$

它的第 3 个渐近分数 $[1, 1, 2, 2] = \frac{17}{10}$. 这就得到特解 $(x_0, y_0) = (-10, 17)$. 因此通解公式为

$$\begin{cases} x = -10 - 23t, \\ y = 17 + 39t, \end{cases}$$

这里 t 取遍所有整数.

(2) 求 23 在模 39 下的逆元.

这相当于求 (1) 的特解, 因此该逆元为 17 (mod 39). ■

3.4.2　渐近分数的逼近

我们把

$$\alpha_n' = [a_n, a_{n+1}, \cdots]$$

称为连分数 $\alpha = [a_0, a_1, \cdots, a_n, \cdots]$ 的第 $n+1$ 个完全商.

命题 3.4.2　在以上诸记号下, 我们有

(1)

$$\alpha=\alpha_0',\quad \alpha=\frac{\alpha_1'+a_0}{\alpha_1'},\quad \alpha=\frac{\alpha_n'p_{n-1}+p_{n-2}}{\alpha_n'q_{n-1}+q_{n-2}},\quad n\geq 2.$$

(2) $a_n=[\alpha_n]$ 对任何 n 成立, 除了以下的例外情形: $\alpha=[a_0,a_1,\cdots,a_N]$ 是有理数, 且 $a_N=1$, 此时有 $a_{N-1}=[\alpha_{N-1}']-1$.

(3) 无理数的简单连分数表达式唯一.

(4) 存在小于 1 的正数 δ_n, 使得

$$q_n\alpha-p_n=\frac{(-1)^n\delta_n}{q_{n+1}},$$

且 $\{\frac{\delta_n}{q_{n+1}}\}$ 是递减数列, 除了以下例外情形: $\alpha=[a_0,a_1,\cdots,a_N]$ 是有理数, $n=N-1$, 此时有 $\delta_{N-1}=1$.

(5)

$$\left|\alpha-\frac{p_n}{q_n}\right|\leq\frac{1}{q_nq_{n+1}}<\frac{1}{q_n^2}.$$

特别地, 当 α 是无理数时, 我们 $\lim_{n\to\infty}\frac{p_n}{q_n}=\alpha$.

证明　(1) 对 n 施归纳法. $n=2$ 时可直接验证其成立. 注意到 $\alpha_{n-1}'=a_{n-1}+\frac{1}{\alpha_n'}$, 故由归纳假设可得

$$\begin{aligned}\alpha&=\frac{\alpha_{n-1}'p_{n-2}+p_{n-3}}{\alpha_{n-1}'q_{n-2}+q_{n-3}}=\frac{\left(a_{n-1}+\frac{1}{\alpha_n'}\right)p_{n-2}+p_{n-3}}{\left(a_{n-1}+\frac{1}{\alpha_n'}\right)q_{n-2}+q_{n-3}}\\&=\frac{(a_{n-1}p_{n-2}+p_{n-3})\alpha_n'+p_{n-2}}{(a_{n-1}q_{n-2}+q_{n-3})\alpha_n'+q_{n-2}}=\frac{p_{n-1}\alpha_n'+p_{n-2}}{q_{n-1}\alpha_n'+q_{n-2}}.\end{aligned}$$

(2) 假设 α 不满足例外情形. 因为 $\alpha_{n+1}'>1$ 并且 $\alpha_n'=a_n+\frac{1}{\alpha_{n+1}}$, 所以 $a_m<\alpha_n'<a_n+1$, 由此即得结论. 例外情形留给读者验证.

(3) 假设

$$\alpha=[a_0,a_1,a_2\cdots]=[b_0,b_1,b_2,\cdots].$$

首先, 由 (2) 知, $[\alpha]=a_0=b_0$. 同理有 $a_1=b_1$. 假设已知 $a_i=b_i$ $(i=0,1,\cdots,n-1)$. 设

$$\alpha=[a_0,a_1,\cdots,a_{n-1},\alpha_n']=[a_0,a_1,\cdots,a_{n-1},\beta_n'].$$

由 (1) 得

$$\alpha=\frac{\alpha_n'p_{n-1}+p_{n-2}}{\alpha_n'q_{n-1}+q_{n-2}}=\frac{\beta_n'p_{n-1}+p_{n-2}}{\beta_n'q_{n-1}+q_{n-2}}.$$

整理即得

$$(\alpha_n'-\beta_n')(p_{n-1}q_{n-2}-p_{n-2}q_{n-1})=0.$$

由推论 3.4.1 立知 $\alpha_n'=\beta_n'$, 故 $a_n=[\alpha_n']=[\beta_n']=b_n$. 归纳法得证.

(4) 由 (1) 及推论 3.4.1, 我们有

$$\alpha-\frac{p_n}{q_n}=\frac{\alpha_{n+1}'p_n+p_{n-1}}{\alpha_{n+1}'q_n+q_{n-1}}-\frac{p_n}{q_n}=\frac{-(p_nq_{n-1}-q_np_{n-1})}{q_n(\alpha_{n+1}'q_n+q_{n-1})}=\frac{(-1)^n}{q_n(\alpha_{n+1}q_n+q_{n-1})}.$$

我们令

$$\delta_n = \frac{q_{n+1}}{\alpha'_{n+1}q_n + q_{n-1}} = \frac{a_{n+1}q_n + q_{n-1}}{\alpha'_{n+1}q_n + q_{n-1}}.$$

除了例外情形, 我们显然有 $0 < \delta_n < 1$.

注意到 $\alpha'_n = a_n + \frac{1}{\alpha'_{n+1}}$, 因而

$$\frac{\delta_n}{q_{n+1}} = \frac{q_{n+1}}{\alpha'_{n+1}q_n + q_{n-1}} \geq \frac{1}{(a_{n+1}+1)q_n + q_{n-1}} = \frac{1}{q_{n+1}+q_n} \geq \frac{1}{a_{n+2}q_{n+1}+q_n} = \frac{1}{q_{n+2}} \geq \frac{\delta_{n+1}}{q_{n+2}}.$$

(5) 由 (4) 立得. ■

注 3.4.1　推论 3.4.3 实际上是命题 3.4.2 (4) 的特殊情形. ■

推论 3.4.4　*设 α 是无理数, 展为无限的简单连分数*

$$\alpha = [a_0, a_1, \cdots, a_n, \cdots].$$

设 $\alpha_n = [a_0, \cdots, a_n] = \frac{p_n}{q_n}$ 是第 n 个渐近分数, 则对任何 $n \geq 1$, α_n, α_{n+1} 中至少有一个满足

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{2q^2}.$$

证明　由推论 3.4.2 (4), α_n, α_{n+1} 中一个大于 α, 一个小于 α, 因此

$$\frac{1}{q_n q_{n+1}} = |\alpha_{n+1} - \alpha_n| = |\alpha_{n+1} - \alpha| + |\alpha - \alpha_n|.$$

如果 $|\alpha_n - \alpha| \geq \frac{1}{2q_n^2}$, $|\alpha_{n+1} - \alpha| \geq \frac{1}{2q_{n+1}^2}$, 这就推出

$$\frac{1}{q_n q_{n+1}} \geq \frac{1}{2q_n^2} + \frac{1}{2q_{n+1}^2},$$

即 $(q_n - q_{n+1})^2 \leq 0$, 矛盾! 因此 (1) 成立. ■

上述推论表明, 存在无穷多个渐近分数满足

$$|\alpha - \frac{p}{q}| < \frac{1}{2q^2}. \tag{3-30}$$

事实上, 我们还有更佳的逼近

定理 3.4.1 (Hurwitz)　*设 α 是无理数, 则 α 的三个相邻的渐近值中必有一个适合*

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{\sqrt{5}q^2}.$$

限于篇幅, 我们不再证明它. 有兴趣的读者, 可以参考 [Hua57, 第十章, 第四节].

上面我们已证明, 无理数 α 的渐近分数 $\frac{p}{q}$ 总满足

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}.$$

一个反问题是: 满足上面不等式的分数是否一定为 α 的某个渐近分数? 答案是否定的. 下面介绍如何判定这样的分数是否为渐近分数. 具体证明参看 [Hua57, 第十章, 第七节].

定理 3.4.2 (Legendre)　设有理数 $\frac{p}{q}$ 的简单连分数展开为

$$\frac{p}{q} = [a_0, a_1, \cdots, a_{n-1}],$$

那么 $\frac{p}{q}$ 是 α 的渐近分数的充要条件是

$$\left|q^2\alpha - pq\right| < \frac{q_{n-1}}{q_{n-1} + q_{n-2}} < 1.$$

推论 3.4.5　如果有理数 $\frac{p}{q}$ 满足

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{2q^2},$$

则其必为 α 的渐近分数.

证明　由

$$\frac{q_{n-1}}{q_{n-1} + q_{n-2}} > \frac{1}{2}$$

及定理 3.4.2 立得. ■

推论 3.4.6　如果有理数 $\frac{p}{q}$ 满足

$$\left|p^2\alpha - q^2\right| < \alpha,$$

则其必为 α 的渐近分数.

证明　设 $|q^2\alpha^2 - p^2| = \delta\alpha$, 这里 $0 \le \delta < 1$. 由定理 3.4.2, $\frac{p}{q}$ 为 α 的渐近分数当且仅当

$$\left|q^2\alpha - pq\right| = \frac{\delta q\alpha}{\alpha q + p} = \frac{\delta\alpha q_{n-1}}{\alpha q_{n-1} + p_{n-1}} < \frac{q_{n-1}}{q_{n-1} + q_{n-2}}.$$

因此我们只需要证明

$$\frac{\alpha q_{n-1}}{\alpha q_{n-1} + p_{n-1}} < \frac{q_{n-1}}{q_{n-1} + q_{n-2}}$$

即可, 亦即

$$\alpha q_{n-1} - p_{n-1} < \alpha(q_{n-1} - q_{n-2}).$$

注意到

$$|\alpha q_{n-1} - p_{n-1}| = \frac{\delta\alpha}{\alpha q_{n-1} + p_{n-1}},$$

所以我们只需证明

$$\frac{\delta}{\alpha q_{n-1} + p_{n-1}} < q_{n-1} - q_{n-2}.$$

但这是显然的, 因为上不等式左边严格小于 1, 而右边是正整数. ■

3.4.3　循环连分数

定义 3.4.2　设 $\alpha = [a_0, a_1, \cdots]$ 是简单连分数. 如果当 $i \ge L$ 时, 总有 $a_i = a_{i+k}$, 则称此连分数为以 k 为周期的循环连分数, 写为

$$[a_0, a_1, \cdots, \dot{a}_L, \cdots, \dot{a}_{L+k-1}].$$

例 3.4.3 (1)

$$\sqrt{2}+1=2+(\sqrt{2}-1)=2+\frac{1}{\sqrt{2}+1}=2+\frac{1}{2+(\sqrt{2}-1)}=2+\cfrac{1}{2+\cfrac{1}{2+\cfrac{1}{\ddots}}}=[\dot{2}].$$

由此得 $\sqrt{2}=[1,\dot{2}]$.
(2) 类似地, 我们有 $\sqrt{3}=[1,\dot{1},\dot{2}]$, $\sqrt{5}=[2,\dot{4}]$. ■

我们要证明如下重要结论.

定理 3.4.3 $\alpha=[a_0,a_1,\cdots]$ 是循环连分数当且仅当 α 是某不可约有理系数二次方程的根.

证明 仍采用前面的记号.

($\Longrightarrow$) 考虑第 $L+1$ 个完全商

$$\alpha'_L=[\dot{a}_L,\cdots,\dot{a}_{L+k-1}]=[a_L,\cdots,a_{L+k-1},\alpha'_L].$$

由此得

$$\alpha'_L=\frac{p'\alpha'_L+p''}{q'\alpha'_L+q''},$$

这里 $\frac{p'}{q'},\frac{p''}{q''}$ 是 $[a_L,\cdots,a_{L+k-1}]$ 是最后两个渐近分数. 整理上式即知, α'_L 满足二次方程

$$q'\alpha'^2_L+(q''-p')\alpha'_L-p''=0.$$

又因为

$$\alpha=\frac{p_{L-1}\alpha'_L+p_{L-2}}{q_{L-1}\alpha'_L+q_{L-2}},$$

所以这就推出, α 也满足某个二次有理系数多项式方程的根. 注意到 α 是无理数, 所以该方程在有理数域上不可约.

($\Longleftarrow$) 假设 $a\alpha^2+b\alpha+c=0$, $a,b,c\in\mathbb{Z}$, $a\neq 0$. 由

$$\alpha=\frac{\alpha'_n p_{n-1}+p_{n-2}}{\alpha'_n q_{n-1}+q_{n-2}},$$

我们得到

$$A_n\alpha'^2_n+B_n\alpha'_n+C_n=0,$$

这里系数

$$\begin{cases} A_n=ap^2_{n-1}+bp_{n-1}q_{n-1}+cq^2_{n-1},\\ B_n=2ap_{n-1}p_{n-2}+b(p_{n-1}q_{n-2}+p_{n-2}q_{n-1})+2cq_{n-1}q_{n-2},\\ C_n=ap^2_{n-2}+bp_{n-2}q_{n-2}+cq^2_{n-2}. \end{cases}\tag{3-31}$$

因为 α'_n 是无理数, 所以 A_n 不可能为零. 此外由直接计算可得

$$B^2_n-4A_nC^2_n=b^2-4ac.\tag{3-32}$$

由命题 3.4.2 (4) 可得

$$p_{n-1}=\alpha q_{n-1}+\frac{\epsilon_{n-1}}{q_{n-1}},\quad |\epsilon_{n-1}|<1.$$

将之代入 A_n 得

$$A_n = 2a\alpha\epsilon_{n-1} + a\frac{\epsilon_{n-1}^2}{q_{n-1}^2} + b\epsilon_{n-1}. \tag{3-33}$$

因而

$$|A_n| < 2|a\alpha| + |a| + |b|.$$

由于 $C_n = A_{n-1}$, 所以也有

$$|C_n| < 2|a\alpha| + |a| + |b|.$$

再由式 (3-32) 得

$$B_n^2 \le 4|A_nC_n| + |b^2 - 4ac|.$$

这样, 整数 A_n, B_n, C_n 的绝对值有上界, 因而只有有限种取值. 因此至少有一组 (A_n, B_n, C_n) 出现三次. 设 $n = n_1, n_2, n_3$ 对应同一组 (A_n, B_n, C_n), 则 $\alpha'_{n_1}, \alpha'_{n_2}, \alpha'_{n_3}$ 都是

$$A_ny^2 + B_ny + C_n = 0$$

的根, 从而必有两个相等, 比如 $\alpha'_{n_1} = \alpha'_{n_3}$. 由简单连分数表达的唯一性即知

$$a_{n_1} = a_{n_2}, \quad a_{n_1+1} = a_{n_2+1}, \cdots,$$

故连分数循环. ■

设 d 是正整数, 并且不是某个整数的平方.

命题 3.4.3 *考虑 $\alpha = \sqrt{d}$ 的连分数展开*

$$[a_0, a_1, \cdots, \dot{a}_L, \cdots, \dot{a}_{L+k-1}],$$

设 α'_n 是第 $n+1$ 个完全商, 则
(1) *α'_n 必可写为如下形式:*

$$\alpha'_n = \frac{\sqrt{d} + P_n}{Q_n}, \quad P_n^2 \equiv d \pmod{Q_n},$$

这里 P_n, Q_n 是整数.
(2) $p_{n-1}^2 - dq_{n-1}^2 = (-1)^nQ_n$, *这里 p_{n-1}/q_{n-1} 是渐近分数.*
(3) $p_{n-1+lk}^2 - dq_{n-1+lk}^2 = (-1)^{n+lk}Q_n$, $\forall l \ge 0$.

证明 (1) 因为 $\sqrt{d} - [\sqrt{d}] = \frac{1}{\alpha'_1}$, 所以

$$\alpha'_1 = \frac{\sqrt{d} + [\sqrt{d}]}{d - [\sqrt{d}]^2}.$$

因此可取 $P_1 = [\sqrt{d}]$, $Q_1 = d - [\sqrt{d}]^2$. 它们显然满足条件. 今对 n 施归纳法, 假设对 $\le n$ 的情形均已证. 我们令

$$P_{n+1} = a_nQ_n - P_n, \quad Q_{n+1} = \frac{d - P_{n+1}^2}{Q_n}.$$

因为 $P_n^2 \equiv P_{n+1}^2 \pmod{Q_n}$, 及归纳假设 $d \equiv P_n^2 \pmod{Q_n}$, 所以 Q_n 也是整数. 此外容易验证,

$$\alpha'_n = \frac{\sqrt{d} + P_n}{Q_n} = a_n + \frac{Q_{n+1}}{\sqrt{d} + P_{n+1}}.$$

结合 $\alpha'_n = a_n + \frac{1}{\alpha'_{n+1}}$ 即得结论.

(2) 首先

$$\sqrt{d} = \frac{p_{n-1}\alpha'_n + p_{n-2}}{q_{n-1}\alpha'_n + q_{n-2}} = \frac{p_{n-1}(\sqrt{d}+P_n) + p_{n-2}Q_n}{q_{n-1}(\sqrt{d}+P_n) + q_{n-2}Q_n}.$$

整理上式, 由 $\sqrt{d}$ 的无理性即得

$$\begin{cases} p_{n-1} &= q_{n-1}P_n + q_{n-2}Q_n, \\ dq_{n-1} &= p_{n-1}P_n + p_{n-2}Q_n. \end{cases}$$

由此可得

$$\begin{aligned} p_{n-1}^2 - dq_{n-1}^2 &= (q_{n-1}P_n + q_{n-2}Q_n)p_{n-1} - (p_{n-1}P_n + p_{n-2}Q_n)q_{n-1} \\ &= (p_{n-1}q_{n-2} - p_{n-2}q_{n-1})Q_n = (-1)^n Q_n. \end{aligned}$$

(3) 由于循环连分数周期是 k, 所以

$$\frac{\sqrt{d}+P_n}{Q_n} = \frac{\sqrt{d}+P_{n+lk}}{Q_{n+lk}}.$$

由此立得结论. ■

推论 3.4.7 *假设整数 ℓ 满足 $0 < |\ell| < \sqrt{d}$, 且 $\ell \neq (-1)^n Q_n$ (记号同上), 那么二次不定方程 $x^2 - dy^2 = \ell$ 无整数解.*

证明 如有解, 则由推论 3.4.6 知, $\frac{x}{y}$ 是 $\sqrt{d}$ 的渐近分数, 因而由推论 3.4.3 知, $\ell = (-1)^n Q_n$, 对某个 n 成立. 这与假设矛盾! ■

3.4.4 佩尔方程的求解算法

这一节, 我们求佩尔方程

$$x^2 - dy^2 = 1. \tag{3-34}$$

的整数解. 由命题 3.4.3, 存在整数 Q, 使得方程 $x^2 - dy^2 = Q$ 有无穷多组解. 由抽屉原理, 在模 $|Q|$ 下必有两组解在同一剩余类中, 即存在正整数 x_1, y_1, x_2, y_2 满足

$$x_1^2 - dy_1^2 = x_2^2 - dy_2^2 = Q, \quad x_1 \equiv x_2 \pmod{|Q|}, \quad y_1 \equiv y_2 \pmod{|Q|}, \quad x_1 \neq x_2.$$

引理 3.4.1 *在上述记号与假设下, 令*

$$x = \frac{x_1x_2 - y_1y_2}{Q}, \quad y = \frac{x_1x_2 - x_2y_1}{Q},$$

这 (x, y) 是佩尔方程 (3-34) 的一组整数解, 且 $(x, y) \neq (\pm 1, 0)$.

证明 首先, 注意到

$$\begin{cases} x_1x_2 - y_1y_2 \equiv x_1^2 - dy_1^2 \equiv Q \equiv 0 \pmod{|Q|}, \\ x_1y_2 - x_2y_1 \equiv x_1y_1 - x_2y_2 \equiv 0 \pmod{|Q|}. \end{cases}$$

因此 x, y 是整数.

其次,

$$x^2 - dy^2 = \frac{(x_1x_2 - y_1y_2)^2 - d(x_1y_2 - x_2y_1)^2}{Q^2} = \frac{1}{Q^2}(x_1^2 - dy_1^2)(x_2^2 - dy_2^2) = 1.$$

最后, 假如 $y = 0$, 则 $x_1y_2 = x_2y_1$. 因为 $(x_1, y_1) = (x_2, y_2) = 1$, 所以 $x_1 = x_2$, $y_1 = y_2$, 与假设矛盾! 因此 $y \neq 0$. ■

由推论 3.4.7 及上面的引理可知, 必存在 n 使得 $(-1)^nQ_n = 1$. 我们以下不妨取满足此条件的最小的 n.

定理 3.4.4 佩尔方程 (3-34) 的全部解都由如下展式得到:

$$x + y\sqrt{d}y = \pm(p_{n-1} + \sqrt{d}q_{n-1})^l, \quad \forall l \in \mathbb{Z}.$$

证明 设 $\epsilon = p_{n-1} + \sqrt{d}q_{n-1}$. 注意到

$$\frac{1}{x + \sqrt{d}y} = x - \sqrt{d}y,$$

因此我们只需要证明任何正整数解都能表为 $x + \sqrt{d}y = \epsilon^m$ $(m > 0)$. 设 (x, y) 为一解. 由于 $\epsilon > 1$, 所以存在 $m > 0$, 使得

$$\epsilon^m \leq x + \sqrt{d}y < \epsilon^{m+1},$$

即

$$1 \leq \epsilon^{-m}(x + \sqrt{d}y) < \epsilon.$$

设 $\epsilon^{-m} = x_0 - \sqrt{d}y_0$ 及

$$\epsilon^{-m}(x + \sqrt{d}y) = (x_0 - \sqrt{d}y_0)(x + y\sqrt{d}) = X + \sqrt{d}Y.$$

由 d 的无理性, 上式也推出

$$(x_0 + \sqrt{d}y_0)(x - y\sqrt{d}) = X - \sqrt{d}Y$$

两式相乘即得

$$X^2 - dY^2 = 1,$$

并且 $1 < X + \sqrt{d}Y < \epsilon$. 因此

$$0 < \epsilon^{-1} < (X + \sqrt{d}Y)^{-1} = X - \sqrt{d}Y < 1.$$

这就推出

$$2X = (X + \sqrt{d}Y) + (X - \sqrt{d}Y) > 1 + \epsilon^{-1} > 0,$$
$$2Y = (X + \sqrt{d}Y) - (X - \sqrt{d}Y) > 1 - 1 = 0.$$

因此 (X, Y) 也是佩尔方程 (3-34) 的正整数解, 并且

$$1 < X + \sqrt{d}Y < p_{n-1} + \sqrt{d}q_{n-1}.$$

注意到 $x = \sqrt{1 + dy^2}$ 是关于 y 的递增函数, 所以上面不等式推出 $X < p_{n-1}$, $Y < q_{n-1}$. 由推论 3.4.6 知, $\frac{X}{Y}$ 是 $\sqrt{d}$ 的渐近分数, 但其分母比 q_{n-1} 小, 这就与 n 的最小性矛盾! ■

从上面的证明可以看到, 在所有正整数解中, 特解 (p_{n-1}, q_{n-1}) 其实就是满足 $x + \sqrt{d}y$ 最小解.

例 3.4.4　求佩尔方程 $x^2-2y^2=1$ 的整数解.

因为 $[\sqrt{2}=1,\dot{2}]$, 所以其最小特解 $(x_0,y_0)=(3,2)$, 因此全部整数解可为

$$x+y\sqrt{2}=(3+2\sqrt{2})^l=(1+\sqrt{2})^{2l},\quad l\in\mathbb{Z}.$$

比如 $l=2$ 时, 有解 $(x,y)=(17,12)$; $l=3$ 时, 有解 $(x,y)=(99,70)$, 等等. ■

注 3.4.2　(1) 一般说来, 方程 $x^2-dy^2=-1$ 未必有整数解. 比如 $x^2-3y^2=-1$ 无解 (考察模 4 下的剩余即得). 若该佩尔方程有解, 我们也可以仿照上面的定理求出所有的解 (参见习题 3.15).

(2) 佩尔方程 $x^2-dy^2=4$ 的全部整数解也能类似求出 (习题 3.16).

(3) 我们也可以讨论一般的佩尔方程 $x^2-dy^2=l$. 当 $|l|<\sqrt{d}$ 时, 由推论 3.4.7, 我们可以用连分数逐一试出特解, 并利用循环连分数的周期性, 求出所有的解. 当 $|l|>\sqrt{d}$ 时,则可通过一些技巧将它归结到上面的情形.

(4) 更一般地, 我们也可以讨论二次曲线方程

$$ax^2+bxy+cy^2+dx+ey+f=0$$

的整数解. 由仿射变换, 我们可以把主要问题归结为求解

$$ax^2+bxy+cy^2=k.$$

它又可以进一步归结到椭圆方程和双曲线方程 (即广义佩尔方程) 的求解问题.

限于篇幅, 我们这里不再详细展开介绍. 有兴趣的读者可以参看 [Hua57, 第十章] ■

本章习题

加 $*$ 号的习题表示有一定难度.

习题 3.1　求不定方程 $2X^2+Y^2=Z^2$ 的正整数解, 这里要求 $(X,Y)=1$.

习题 3.2　求不定方程 $X^2+Y^2+Z^2=W^2$ 的正整数解 (X,Y,Z,W).

习题 3.3　证明以下各不定方程均无正整数解.

(1) $X^4+4Y^4=Z^2$;
(2) $X^4-Y^4=Z^2$;
(3) $X^4-Y^4=2Z^2$;
(4) $X^4-Y^4=11Z^2$.

习题 3.4　求解不定方程 $X^2+Y^2=Z^4$ 的正整数解, 这里要求 $(X,Y)=1$, X 是偶数.

习题 3.5　(1) 证明以下方程组无正整数解

$$\begin{cases}X^2+Y^2=Z^2\\ Z^2+Y^2=W^2.\end{cases}$$

(2) 利用上小题证明: 三条边长都是正整数的直角三角形面积不可能是完全平方数.

习题 3.6 (*)　设 l,m,n 是正整数, 且 $(lm,n)=(ln,m)=(mn,l)=1$, 证明: 不定方程

$$X^l+Y^m=Z^n$$

有无穷多组正整数解.

习题 3.7　求以下二次同余式的解.

(1) $x^2\equiv 73 \pmod{127}$,

(2) $x^2\equiv 7 \pmod{53}$,

(3) $x^2\equiv 32 \pmod{47}$,

(4) $x^2\equiv 46 \pmod{105}$,

(5) $x^2\equiv 37 \pmod{81}$,

(6*) (高斯) $x^2\equiv -286 \pmod{4272943}$, 这里已知 4272943 是素数.

习题 3.8　设 $a>1,n>1$, 证明: 如果 a^n-1 是素数, 则 $a=2$, n 也是素数.

习题 3.9　分别求以下勒让德符号:

$$\left(\frac{286}{563}\right),\quad \left(\frac{-1457}{2389}\right),\quad \left(\frac{74}{101}\right),\quad \left(\frac{195}{1901}\right),\quad \left(\frac{365}{1847}\right)$$

习题 3.10　利用推论 3.2.2 证明形如 $4m+1$ 的奇素数有无穷多个.

习题 3.11　设 a 是正整数, 并且对任何正整数 n, 同余方程 $x^2\equiv a \pmod{n}$ 都有解. 证明: a 一定是完全平方数.

习题 3.12　证明引理 3.3.5.

习题 3.13　设 p_n,q_n,a_i 等同命题 3.4.1 的定义, 证明:

$$p_n=\begin{vmatrix} a_0 & 1 & 0 & 0 & \cdots & 0 & 0 & 0\\ -1 & a_1 & 1 & 0 & \cdots & 0 & 0 & 0\\ 0 & -1 & a_2 & 1 & \cdots & 0 & 0 & 0\\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots\\ 0 & 0 & 0 & 0 & \cdots & -1 & a_{n-1} & 1\\ 0 & 0 & 0 & 0 & \cdots & 0 & -1 & a_n \end{vmatrix},\quad q_n=\begin{vmatrix} a_1 & 1 & 0 & 0 & \cdots & 0 & 0 & 0\\ -1 & a_2 & 1 & 0 & \cdots & 0 & 0 & 0\\ 0 & -1 & a_3 & 1 & \cdots & 0 & 0 & 0\\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots\\ 0 & 0 & 0 & 0 & \cdots & -1 & a_{n-1} & 1\\ 0 & 0 & 0 & 0 & \cdots & 0 & -1 & a_n \end{vmatrix}.$$

习题 3.14　验证式 (3-31), 式 (3-32) 和式 (3-33).

习题 3.15　仿照定理 3.4.4, 证明: 若不定方程 $x^2-dy^2=-1$ 有解, 则所有解都由如下展式得到:

$$x+\sqrt{d}y=\pm\left(p_{n-1}+\sqrt{d}q_{n-1}\right)^l,\quad \forall l\in\mathbb{Z},$$

这里 p_n/q_n 是使得 $(-1)^nQ_n=-1$ 的渐近分数, 且 n 达到最小.

习题 3.16　仿照定理 3.4.4, 证明不定方程 $x^2-dy^2=4$ 的诸解都由如下展式得到:

$$\frac{x+\sqrt{d}y}{2}=\pm\left(\frac{x_0+\sqrt{d}y_0}{2}\right)^l,\quad \forall l\in\mathbb{Z},$$

这里 (x_0,y_0) 是使得 $x_0+\sqrt{d}y_0$ 最小的正整数解.

第四章　三次不定方程

这一章节我们将简单讨论三次不定方程的求解. 费马在研读丢番图的著作时, 实际上已经讨论了一部分三次不定方程的求解问题. 比如他曾断言

(1) 除了 1 之外, 任何三角数都不可能是立方数. 换成方程的语言, 即

$$\frac{y(y+1)}{2} = x^3$$

只有唯一的正整数解 $(1,1)$.

(2) 一个立方数减去 2 不可能是平方数, 除非是以下特例: $5^2 = 3^3 - 2$. 也就是说,

$$y^2 = x^3 - 2$$

只有唯一的正整数解 $(3,5)$.

(3) 一个立方数减去4不可能是平方数, 除非是以下特例: $2^2 = 2^3 - 4$, $11^2 = 5^3 - 4$. 换言之,

$$y^2 = x^3 - 4$$

仅有两组正整数解 $(2,2)$, $(5,11)$.

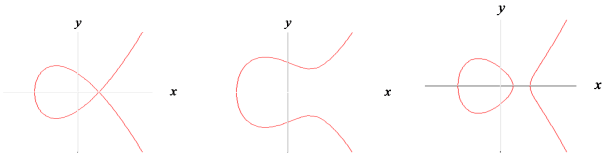
事实上, 椭圆曲线和许多数学问题以及数学理论有着极为密切的联系–比如同余数问题和费马最后的猜想等. 它是一只“生金蛋的鸡”!

4.1　椭圆曲线上的群结构

一个三次方程通过适当的坐标变换, 可以写成如下标准形式:

$$y^2 = x^3 + ax + b. \tag{4-1}$$

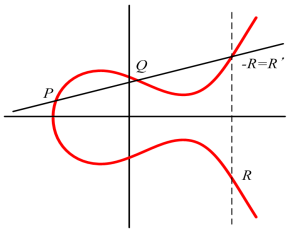
它在坐标平面上定义了一条三次曲线 C. 它显然关于 x 轴对称. 以下是几类三次曲线在实坐标平面中的图像.

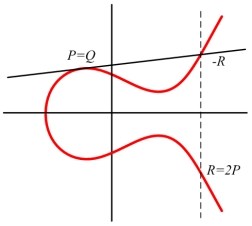


如果 $4a^3 + 27b^2 \neq 0$, 我们就称 C 是椭圆曲线; 如果 $4a^3 + 27b^2 = 0$, 则称之为奇异有理曲线. 上面的第一个图就是奇异的有理曲线. 通过方程容易验证, 任何直线与 C 相交三个点 (允许重合).

我们求解三次不定方程的整数 (有理数) 解, 相当于寻找椭圆曲线上的整数点 (有理点). 对奇异有理曲线来说, 寻找有理点的方法其实求解单位圆上的有理点完全类似, 我们这里不再具体介绍这类情形.

我们将 C 看作点的集合. 这一节的主要任务就是在这个集合上引进一种“加法”运算, 使得 C 成为一个群. 任取两点 $P, Q \in E$ (允许重合), 设 $\overline{PQ}$ 是连接 P, Q 的直线 (若重合, 则取切线), 则该直线与 C 相交于第三个点, 我们记作 $R' := P * Q$. 设 R' 是 R 关于 x 轴的对称点, 记作 $R = P + Q$.





下面为了讨论方便, 我们把无穷远点 $O=(0,\infty)$ 也放入曲线 C 内. 我们先承认以下的结果 (并非显而易见).

定理 4.1.1　设 C 是椭圆曲线. 在上述定义的 $+$ 运算下, $(C,+,O)$ 成为一个交换群, 且
(1) 无穷远点 $O=(0,\infty)$ 为零元.
(2) 点 $P\in C$ 的逆元 $-P$ 就是 P 关于 x 轴的对称点.
(3) P,Q,R 三点共线当且仅当 $P+Q+R=O$.
设 $P\neq O$, 则 $2P=0$ 当且仅当 C 在 P 落在 x 轴上.

请注意, 这里的$+$ 运算并非通常的坐标相加. 事实上, 从上面的定理, 我们可以得到这种运算下的坐标计算公式 (留给读者验证).

定理 4.1.2　考虑椭圆曲线 $(C,+,O)$ 上的两点 $P=(t,u),Q=(v,w)$, 且假设 P,Q,O 不共线. 设 $P+Q=(g,h)$, 则

$$\begin{cases} g=m^2-a_1-t-v,\\ h=m(t-g)-u, \end{cases}\qquad \text{其中}\quad m=\begin{cases} \frac{u-w}{t-v}, & P\neq Q,\\ \frac{3t^2+2a_1t+a_2}{2u}, & P=Q. \end{cases}$$

4.2　有理点的算法

以下假设方程 (4-1) 的系数 a,b 均是有理数. C 上的有理点集 (包括 O 点) 记作 $C(\mathbb{Q})$. 由定理 4.1.2 立得如下推论.

推论 4.2.1　设 $P,Q\in C$ 为有理点, 则 $P+Q$ 也为有理点. 特别地, $C(\mathbb{Q})$ 是 $(C,+,O)$ 的子群.

利用上述性质, 我们可以从已知的有理点出发, 通过加法运算, 不断地找到新的有理点.

我们有以下的深刻结果–它们已超出了本书的范围.

定理 4.2.1 (Mordell **定理**)　$C(\mathbb{Q})$ 是有限生成交换群, $C(\mathbb{Q})\cong\mathbb{Z}^r\oplus C(\mathbb{Q})_{\rm tor}$. 这里 $C(\mathbb{Q})_{\rm tor}$ 是有限交换群.

定理 4.2.2 (Mazur **定理**)　$C(\mathbb{Q})_{\rm tor}$ 必是以下情形之一:
(1) $\mathbb{Z}/n\mathbb{Z}$, $n\leq 10$ 或者 $n=12$,
(2) $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2n\mathbb{Z}$, $n\leq 4$.

例 4.2.1　如何求出 $C(\mathbb{Q})$ 是个较难的问题. 这里有两个已知的例子.
(1) $y^2=x^3+1$, 此时 $C(\mathbb{Q})\cong\mathbb{Z}/6\mathbb{Z}$. 精确言之, 它由以下六个解构成

$$(2,3),\quad (0,1),\quad (-1,0),\quad (0,-1),\quad (2,-3),\quad O=[0,1,0].$$

(2) $y^2=x^3-6x-4$, 此时 $C(\mathbb{Q})\cong\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}$. ■

注 4.2.1　一个未解决的问题是: $C(\mathbb{Q})$ 的秩 r 是否有上界? Martin-Mimillen 在 2000 年给出一个 $r \geq 24$ 的例子. ■

例 4.2.2　$y^2 = x^3 + 3x$, $P = (1, 2)$. 此时 $a = 3, b = 0$.

(1) 求 $2P$ 的坐标, 即 $P = Q$ 情形. 此时有 $t = 1, u = 2, v = 1, w = 2$, 利用定理 4.1.2 计算得

$$m = \frac{3t^2 + 2a_1 t + a_2}{2u} = \frac{3 \times 1 + 2 \times 0 + 3}{4} = \frac{3}{2}$$

$$g = m^2 - a_1 - t - v = \frac{3}{2}^2 - 0 - 1 - 1 = \frac{1}{4}$$

$$h = m(t - g) - u = \frac{3}{2} \times (1 - \frac{1}{4}) - 2 = -\frac{7}{8}$$

所以 $2P = (\frac{1}{4}, -\frac{7}{8})$.

(2) 求 $3P$ 的坐标. 此时 $3P = P + 2P, P \neq 2P$. 利用 (1)的结果, 此时有 $t = 1, u = 2, v = \frac{1}{4}, w = -\frac{7}{8}$, 由定理 4.1.2 计算得

$$m = \frac{u - w}{t - v} = \frac{2 + \frac{7}{8}}{1 - \frac{1}{4}} = \frac{23}{6}$$

$$g = m^2 - a_1 - t - v = \frac{23}{6}^2 - 0 - 1 - \frac{1}{4} = \frac{121}{9}$$

$$h = m(t - g) - u = \frac{23}{6} \times (1 - \frac{121}{4}) - 2 = -\frac{1342}{27}$$

所以 $3P = (\frac{121}{9}, -\frac{1342}{27})$. ■

例 4.2.3　读者也可以尝试计算以下例子.

(1) $y^2 = x^3 + 8$, $p = (2, 4)$ 的有理点 np. 比如

$$2p = (-\frac{7}{4}, \frac{13}{8}), \qquad 3p = (\frac{34}{225}, -\frac{9548}{3375}).$$

(2) $y^2 = x^3 - 2x$, $p = (2, 2)$. 比如

$$2p = (\frac{9}{4}, -\frac{21}{8}).$$

4.3 同余数

同余数问题是指如下的数论问题:

给定正整数 n, 是否存在一个直角三角形, 它的三条边长是有理数, 并且面积正好等于 n? 满足此条件的 n 称为同余数 (Congruent number).

例 4.3.1　(1) 5 是同余数, 因为存在直角三角形三边长为 $(\frac{20}{3}, \frac{3}{2}, \frac{41}{6})$, 其面积恰好是 5.

(2) 6 也是同余数, 因为它恰好是直角边长为 $(3, 4, 5)$ 的三角形面积.

(3) (费马) $1, 2$ 不是同余数.

(4) 目前已知的最前面的同余数是:

$$5, 6, 7, 13, 14, 15, 20, 21, 22, 23, 24, 28, 29, 30, 31, 34, 37, 38, 39, 41, 45, 46, 47$$

判断一个正整数 n 是否是同余数, 等价于判断以下方程是否有正有理数解 (a,b,c).

$$\begin{cases} a^2+b^2 &= c^2 \\ \frac{1}{2}ab &= n. \end{cases}$$

我们令

$$x=\frac{n(a+c)}{b}, \qquad y=\frac{2n^2(a+c)}{b^2}.$$

这样就得到椭圆曲线

$$y^2=x^3-n^2x.$$

上述变换是可逆的,

$$a=\frac{x^2-n^2}{y}, \qquad c=\frac{x^2+n^2}{y}.$$

由此易得以下结论.

命题 4.3.1 *n 是同余数当且仅当椭圆曲线 $y^2=x^3-n^2x$ 有有理点 (x,y) 使得 $y\neq 0$.*

例 4.3.2 以同余数 $n=5$ 为例, 椭圆曲线 $y^2=x^3-25x$ 显然有理点 $P=(-4,6)$. 我们求得 $2P=(\frac{1681}{144},\frac{62279}{1728})$. 这样, 我们得到直角三角边长 $(\frac{1519}{492},\frac{4920}{1519},\frac{3344161}{747348})$. ■

关于同余数, 我们有以下著名猜想 (Tunnell):

假设 n 是奇数, 且不含平方因子, 那么 n 是同余数当且仅当以下两个集合的元素个数满足关系式

$$\sharp\{(a,b,c)\mid 2a^2+b^2+8c^2=n\}=2\sharp\{(a,b,c)\mid 2a^2+b^2+32c^2=n\}.$$

4.4 费马大定理与椭圆曲线

费马曾猜测, 当 $n\geq 3$ 时, 以下不定方程没有整数解 (a,b,c).

$$a^n+b^n=c^n, \qquad abc\neq 0.$$

费马本人用无穷递降方法证明了 $n=4$ 的情形. 这样, 人们只需要验证 n 是素数的情形无解即可.

假设对某个素数 n, 存在非零整数解 (a,b,c) 满足费马方程, 那么可以构造如下的椭圆曲线:

$$y^2=x(x+a^p)(x-b^p).$$

这条曲线称为 Frey 曲线, 由 Frey 于 1985 年 构造. Ribet 于 1986 年证明 Frey 曲线不可能是模曲线.

另一方面, 人们曾有如下猜测 (Taniyama-Shimura):

任何椭圆曲线都是模曲线.

直到 1995 年, Wiles 证明了上述猜测成立. 这就彻底证明了费马方程无解.

对于 $n=3,4$ 的情形, 上述方程可以在某种变量替换下自动变成椭圆曲线方程. 比如 $n=3$ 的情形, 令

$$x=\frac{12c}{a+b}, \qquad y=\frac{36(a-b)}{a+b}.$$

由此可得关系式

$$y^2 = x^3 - 432.$$

这条椭圆曲线只有两个有理点 $(12, 36)$, $(12, -36)$—它们恰好对应费马方程的平凡解 $a = 0$ 或 $b = 0$. 如果费马方程有解, 那么上述椭圆曲线除了这两个有理点外必须还有其他有理点, 这就导致矛盾! 因此三次费马方程无非平凡解.

又比如对 $n = 4$ 的情形, 令

$$x = \frac{2(b^2 + c^2)}{a^2}, \qquad y = \frac{4b(b^2 + c^2)}{a^3}.$$

这就得到椭圆曲线

$$y^2 = x^3 - 4x.$$

这条曲线只有三个有理点 $(0, 0)$, $(-2, 0)$, $(2, 0)$. 它们都对应原方程 $b = 0$ 的平凡解. 因此这就推出费马方程无解.

注 4.4.1 $n = 3, 4$ 的情形在代数数论中的证明很有意思. 比如 $n = 3$ 的情形, 高斯将费马方程的解置入 3 次扩域 $\mathbb{Q}(\omega)$ 中来考虑, 这里 $\omega = \frac{1}{2} + \frac{\sqrt{-3}}{2}$ 是三次单位根. 在 $\mathbb{Q}(\omega)$ 中, 高斯利用了该扩域的代数数论性质, 十分简洁地证明了费马方程无解. 尽管 $n = 3$ 情形也曾由欧拉获得, 但其证明很冗长繁琐.

$n = 4$ 情形则可置入高斯数域 $\mathbb{Q}(\sqrt{-1})$ 中, 类似证明. 为研究一般情形, 库莫引进了理想数的概念, 从而极大促进了代数数论和割圆域论的发展. 当然这样的方法仍然不足以彻底解决费马猜想. ■

人们也感兴趣如下形式的不定方程

$$a^3 + b^3 = dc^3,$$

这里 d 是给定的正整数. $d = 1$ 时就是三次费马方程. 考虑射影变换

$$\begin{cases} X = dc, \\ Y = \frac{d}{2}(a - b), \\ Z = 3(a + b) \end{cases} \quad \text{等价地} \quad \begin{cases} a = \frac{Y}{d} + \frac{Z}{6}, \\ b = -\frac{Y}{d} + \frac{Z}{6}, \\ c = \frac{X}{d} \end{cases}$$

这就得到

$$Y^2 Z = X^3 - \frac{d^2}{108} Z^3.$$

令 $x = X/Z$, $y = Y/Z$, 则得

$$y^2 = x^3 - \frac{d^2}{108}.$$

无穷远点 O 对应了原方程的平凡解 $c = 0$.

当 $d = 1$ 时, 我们已经知道 $C(\mathbb{Q}) = \mathbb{Z}/3\mathbb{Z}$. 一般情形则仍未完全解决. 人们验证了 $6 \le d \le 500$ 的情形, 证明当 d 是以下整数时, $C(\mathbb{Q})$ 中的非挠部分是秩 1 的:

$$d = 6, 7, 9, 12, 13, 15, 17.$$

例 4.4.1 考虑不定方程 $a^3 + b^3 = 9c^3$. 由上面的坐标变换, 我们得到椭圆曲线 C:

$$y^2 = x^3 - \frac{3}{4}.$$

显见 $p=(1,-\frac{1}{2})$ 是 C 的有理点. 我们计算出 $2p=(7,\frac{37}{2})$, $3p=(\frac{73}{36},-\frac{6067}{216})$. 代回到原来的不定方程, $p,2p,3p$ 分别对应了本原解

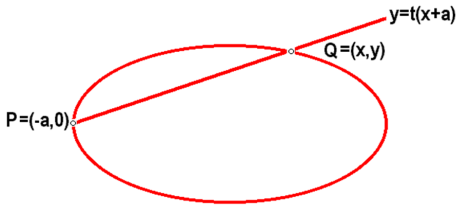
$$(1,2,1),\quad (20,-17,7),\quad (-5743,6391,438).$$

4.5 圆锥曲线与二次不定方程

三次曲线可以退化为圆锥曲线和无穷远直线的并. 因此我们可以将三次曲线上的群结构搬到圆锥曲线上. 具体言之, 设 C 是圆锥曲线, $O\in C$ 是给定的基点. 对任何 $P,Q\in C$, 我们做一条从 O 出发, 并与 $\overline{PQ}$ 平行的直线 (即通过 $\overline{PQ}$ 与无穷远直线的交点). 这条直线与 C 交另一点, 记作 $P+Q$. 类似可证, $(C,+)$ 是群, 并且有理点构成子群 $C(\mathbb{Q})$.

例 4.5.1　单位圆上的群结构就是通常的复数乘法. ■

圆锥曲线都可以有理参数化, 即存在有理函数 $\varphi(t),\psi(t)$ 使得 $(x,y)=(\varphi(t),\psi(t))$ 就是 C 的定义方程的参数解.



具体言之, 就是从基点 O 出发斜率为 t 的射线 L_t. 对任何点 $P\in C$, 总有唯一的射线 L_t 经过 P, 由此可以求出P 的关于参数 t 的坐标. 下面举几例说明 (参见第 3.1.2 节).

例 4.5.2　设 C 由方程 $x^2-dy^2=1$ 定义, $O=(1,0)$, d 是整数. 此时 $P\in C$ 的参数表达式为

$$P=\left(\frac{dt^2+1}{dt^2-1},\frac{2t}{1-dt^2}\right).$$

P 是有理点当且仅当 $t\in\mathbb{Q}$ 或 ∞. ■

如果我们从一个有理点 P出发, 通过加法运算求 nP, 就能得到一系列的有理点.

推论 4.5.1　设 C 形如例 4.5.2 (2). $P=(x_0,y_0)\in C$. 那么

$$nP:=(x_n,y_n)=\left(\frac{(x_0+y_0\sqrt{d})^n+(x_0-y_0\sqrt{d})^n}{2},\frac{(x_0+y_0\sqrt{d})^n-(x_0-y_0\sqrt{d})^n}{2\sqrt{d}}\right),$$

换言之,

$$x_n+y_n\sqrt{d}=(x_0+\sqrt{d}y_0)^n.$$

特别地, 如果 P 是整数点, 即 $x_0,y_0\in\mathbb{Z}$, 那么对任何 $n\in\mathbb{Z}$, nP 也是整数点. 进一步, 所有整数点构成子群 $C(\mathbb{Z})\cong\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}$.

这样, 我们就给出了定理 3.4.4 的几何解释.

本章习题

加 $*$ 号的习题表示有一定难度.

习题 4.1　尝试求出三次奇异有理曲线上的全部有理点 (假设方程系数都是有理数).

习题 4.2　验证定理 4.1.2.

习题 4.3　验证例 4.2.3 的结果.

第五章　高次不定方程

考虑 n 次整系数多项式.

$$f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0,\quad a_i\in\mathbb{Z},\quad a_n\neq 0.$$

我们关心如下高次同余方程的求解

$$f(x)\equiv 0\pmod m. \tag{5-1}$$

它也等价于求解不定方程

$$f(x)=my$$

的整数解.

5.1　高次同余方程的解数

这一节, 我们讨论同余方程 (5-1) 在模 m 下的剩余类解个数. 我们知道, 在复数域上, $f(x)=0$ 恰好有 $n=\deg f$ 个解. 但是在模 m 下, 同余方程 (5-1) 的剩余类解数未必恰好是 n.

例 5.1.1　(1) $x^3-x=x(x-1)(x+1)\equiv 0\pmod 6$ 有六个剩余类解, 即

$$x\equiv 0,1,2,3,4,5\pmod 6.$$

(2) $x^2+1\equiv 0\pmod 3$ 无剩余类解.
(3) 设 p 是素数, 方程

$$(x-1)(x-p-1)\equiv 0\pmod{p^2}$$

恰有 p 个剩余类解

$$x\equiv 1,p+1,2p+1,\cdots,(p-1)p+1\pmod{p^2}.$$

这几个例子表明, 高次同余方程的剩余类解个数有比较复杂的情况. ■

命题 5.1.1　*设 m_1,m_2 是互质的正整数, 则同余方程*

$$f(x)\equiv 0\pmod{m_1m_2} \tag{5-2}$$

的剩余类解数恰好等于以下两个同余方程剩余类解数之积:

$$f(x)\equiv 0\pmod{m_i},\quad i=1,2.$$

证明　若 x 是 (5-2) 的解, 则显然它也分别是 $f(x)\equiv 0\pmod{m_i}$ 的解.

反过来, 设 c_i 是 $f(x)\equiv 0\pmod{m_i}$ 的解 $(i=1,2)$, 则由孙子定理, 存在模 m_1m_2 中唯一的剩余类 c, 使得 $c\equiv c_i\pmod{m_i}$. 因此 $f(c)\equiv f(c_i)\equiv 0\pmod{m_i}$, 即 $m_i\mid f(c)$. 由于 $(m_1,m_2)=1$, 所以 $m_1m_2\mid f(c)$, 即

$$f(c)\equiv 0\pmod{m_1m_2}.$$

这就证明了结论. ■

结合上面的结论和算术基本定理, 我们只需要讨论模素数方幂的同余方程的剩余类解数.

定理 5.1.1 设 p 是素数, 且 $p\nmid a_n$, 则方程 (5-1) 的剩余类解个数不超过 $n=\deg f$ (包括重根).

证明 今对 n 施归纳法. $n=1$ 时是显然的, 假设 $<n$ 的情形均已证. 设 $x\equiv a \pmod p$ 是一剩余类解. 考虑多项式的带余除法

$$f(x)=(x-a)f_1(x)+r_1.$$

因为 $r_1=f(a)\equiv 0 \pmod p$, 所以

$$f(x)\equiv (x-a)f_1(x) \pmod p.$$

若 a 仍是 $f_1(x)\equiv 0 \pmod p$ 的剩余类解, 则类似可得 $f_1(x)\equiv (x-a)f_2(x) \pmod p$. 此时我们称 a 是方程 (5-1) 的重根. 在有限步后, 我们有

$$f(x)\equiv (x-a)^h g_1(x) \pmod p,\quad \deg g_1=n-h,\quad g_1(a)\not\equiv 0 \pmod p.$$

若有另外一解 b, 则 $0\equiv f(b)\equiv (b-a)^h g_1(b) \pmod p$, 因而推知 $g_1(b)\equiv 0 \pmod p$. 因为 $\deg g_1=n-h<n$, 所以由归纳假设, $g_1(x)\equiv 0 \pmod p$ 的解数不超过 $n-h$. 因此同余方程 (5-1) 的剩余类解个数不超过 n. ■

注 5.1.1 上面的结论告诉我们, 多项式 $f(x)$ 在模素数 p 下可以分解成

$$f(x)\equiv (x-a)^h(x-b)^k\cdots(x-c)^l g(x) \pmod p,$$

这里 $\deg g=n-h-k-\cdots-l$, 且 $g(x)\equiv 0 \pmod p$ 没有剩余类解. ■

例 5.1.2 设 $f(x)=x^4+2x^3+8x+9$, 求同余方程 $f(x)\equiv 0 \pmod{35}$ 的剩余类解.

这等价于求方程组

$$\begin{cases} f(x)\equiv 0 \pmod 5,\\ f(x)\equiv 0 \pmod 7. \end{cases}$$

由逐步检验可知,

$$\begin{cases} f(x)\equiv (x-1)(x+1)^3 \pmod 5,\\ f(x)\equiv (x-3)(x+1)(x+2)^2 \pmod 7. \end{cases}$$

因此原方程的解等价于

$$\begin{cases} x\equiv 1,4 \pmod 5,\\ x\equiv 3,5,6 \pmod 7. \end{cases}$$

■

由孙子定理, $x\equiv 21b_1+15b_2 \pmod{35}$, 这里 b_1 取值 $1,4$, b_2 取值 $3,5,6$. 最终得解

$$x\equiv 6,19,24,26,31,34 \pmod{35}.$$

例 5.1.3 设 $f(x)=x^4+7x+4$, 求 $f(x)\equiv 0 \pmod{27}$ 的剩余类解.

先讨论同余方程 $f(x)\equiv 0 \pmod 3$, 它有唯一解 $x\equiv 1 \pmod 3$. 设 $x=1+3y$, 代入方程

$$f(x)=f(1+3y)\equiv 0 \pmod 9,$$

则可化简得

$$4+11y\equiv 0 \pmod 3.$$

因此 $y\equiv 1 \pmod 3$.

设 $y=1+3z$, 则 $x=4+9z$, 代入到原方程得 $z\equiv 2 \pmod 3$, 令 $z=2+3w$, 从而 $x=22+27w$, 这就得到原方程的唯一剩余类解 $x\equiv 22 \pmod{27}$. ■

5.2 Wolstenholme 定理

由费马小定理, 定理 5.1.1 以及注记 5.1.1, 我们立刻有

推论 5.2.1 $x^{p-1}-1\equiv (x-1)(x-2)\cdots(x-(p-1)) \pmod p$. 换言之, 考虑展开式

$$(x-1)(x-2)\cdots(x-(p-1))=x^{p-1}-s_1x^{p-2}+\cdots+s_{p-1}, \tag{5-3}$$

则 $s_i\equiv 0 \pmod p$ $(1\le i\le p-2)$, $s_{p-1}\equiv -1$.

注意到 $s_{p-1}=(p-1)!$, 故由以上推论直接得到威尔逊定理

$$(p-1)!\equiv -1 \pmod p.$$

这就给出了威尔逊定理的另一证明.

利用上述推论, 我们还能得到如下有趣结果.

定理 5.2.1 (Wolstenholme) 设 $p>3$ 是素数, 取整数 s^* 使得它是 s 在模 p^2 下的逆元, 则

$$1^*+2^*+\cdots+(p-1)^*\equiv 0 \pmod{p^2}.$$

证明 注意到

$$(p-1)!s^*\equiv\frac{(p-1)!}{s} \pmod{p^2},$$

所以我们相当于要证明

$$p^2\mid (p-1)!\left(1+\frac12+\cdots+\frac{1}{p-1}\right).$$

在展开式 (5-3) 中系数

$$s_{p-2}=(p-1)!\left(1+\frac12+\cdots+\frac{1}{p-1}\right).$$

因此我们只需证明 $p^2\mid s_{p-2}$ 即可.

将 $x=p$ 代入式 (5-3) 中, 并注意 $s_{p-1}=(p-1)!$, 我们得到

$$p^{p-2}-s_1p^{p-3}+\cdots+s_{p-3}p-s_{p-2}=0.$$

因为 $p\mid(s_1,s_2,\cdots,s_{p-2})$, 所以上式除了最后一项, 其余项都被 p^2 整除. 因而 $p^2\mid s_{p-2}$. ■

Wolstenholme 定理还有一种证明方法, 这里简单介绍一下. 如上讨论, 我们只需证明

$$p^2\mid (p-1)!\sum_{k=1}^{p-1}\frac1k.$$

因为

$$(p-1)!\sum_{k=1}^{p-1}\frac{1}{k}=(p-1)!\sum_{k=1}^{\frac{p-1}{2}}\left(\frac{1}{k}+\frac{1}{p-k}\right)=p!\sum_{k=1}^{\frac{p-1}{2}}\frac{1}{k(p-k)}.$$

所以我们只要证明

$$p\mid(p-1)!\sum_{k=1}^{\frac{p-1}{2}}\frac{1}{k(p-k)}.$$

我们取整数 $\bar{k}$ 使得它是 k 在模 p 下的逆元. 注意到

$$(p-1)!\cdot\frac{1}{k(p-k)}\equiv-(p-1)!\cdot\bar{k}^2\pmod{p},$$

并且当 k 从 1 取到 $\frac{p-1}{2}$ 时, $\bar{k}^2$ 在模 p 下不重复地跑遍所有平方剩余. 因此

$$(p-1)!\sum_{k=1}^{\frac{p-1}{2}}\frac{1}{k(p-k)}\equiv-(p-1)!\sum_{k=1}^{\frac{p-1}{2}}\bar{k}^2\equiv-(p-1)!\sum_{k=1}^{\frac{p-1}{2}}k^2\equiv0\pmod{p}.$$

5.3 原根与指标

5.3.1 原根的存在性

设 p 是奇素数, a 是整数, 且 $p\nmid a$. 我们可以取最小的正整数 d, 使得 $a^d\equiv1\pmod{p}$. 我们将 d 称作 a 在模 p 中的指数, 记作 $d:=\mathrm{ord}_pa$. 请注意, 费马小定理保证了指数的存在性.

定理 5.3.1 *在模 p 下, 我们有*

(1) *任何既约剩余类的指数都整除 $p-1$;*

(2) *指数等于 d 的既约剩余类恰有 $\varphi(d)$ 个, 这里要求 $d\mid p-1$.*

证明 (1) 设 $\bar{a}\in\mathbb{Z}_p^*$ 的指数等于 d. 考虑带余数除法 $p-1=dk+r$, $0\le r<d$, 则有

$$a^r\equiv(a^d)^k\cdot a^r\equiv a^{p-1}\equiv1\pmod{p}.$$

由 d 的最小性可知, $r=0$, 即 $d\mid p-1$.

(2) 首先证明指数等于 d 的既约剩余类最多只有 $\varphi(d)$ 个. 若不存在指数等于 d 的既约剩余类, 则此结论显然. 假设存在 $\bar{a}\in\mathbb{Z}_p^*$, 使得 $\mathrm{ord}_pa=d$. 很显然, a^k $(k=1,2,\cdots,d)$ 是方程

$$x^d\equiv1\pmod{p}$$

的 d 个不同的剩余类解. 由定理 5.1.1, 上述方程最多有 d 个解, 因而它恰有这 d 个解. 设 $\bar{b}\in\mathbb{Z}_p^*$ 也有指数 d. 由上面讨论可知, $\bar{b}=\bar{a}^k$, 对某个正整数 $k(\le d)$ 成立. 若 $(k,d)>1$, 则

$$b^{\frac{d}{(k,d)}}\equiv(a^d)^{\frac{k}{(k,d)}}\equiv1\pmod{p}.$$

这与 d 的最小性矛盾! 故 $(k,d)=1$. 因此这样的剩余类 b 最多有 $\varphi(d)$ 个.

假设 $h(d)$ 是指数等于 d 的既约剩余类个数. 上面已证 $h(d)\le\varphi(d)$. 另一方面,

$$\sum_{d\mid p-1}h(d)=n=\sum_{d\mid p-1}\varphi(d),$$

后一等式来自于命题 2.5.4. 这就迫使 $h(d)=\varphi(d)$. ■

推论 5.3.1　模 p 中指数为 $p-1$ 的既约剩余类恰有 $\varphi(p-1)$ 个.

我们把指数为 $p-1$ 的既约剩余类称作模 p 中的原根. 上面的推论告诉我们模 p 中的原根存在, 且有 $\varphi(p-1)$ 个. 设 $\bar{g}\in\mathbb{Z}_p^*$ 是原根, 则

$$\bar{g},\quad \bar{g}^2,\quad \cdots,\quad \bar{g}^{p-2},\quad \bar{g}^{p-1}=\bar{1}$$

恰好不重复地跑遍所有既约剩余类. 因此我们有以下结论.

推论 5.3.2　模 p 的既约剩余系 $\mathbb{Z}_p^*$ 作为乘法群是 $p-1$ 阶循环群, 其生成元就是那些原根, 因而恰有 $\varphi(p-1)$ 个生成元.

例 5.3.1　我们通常没有统一的方法来构造模 p 的原根. 这里罗列一些小素数情形的原根.
(1) 当 $p=3,5,11,13,19,29,37,53,59,61,67$ 时, $g=2$ 都是模 p 的原根.
(2) 当 $p=7,17,31,43$ 时, $g=3$ 都是模 p 的原根.
(3) 当 $p=23,47$ 时, $g=5$ 都是模 p 的原根.
(4) 当 $p=41$ 时, $g=6$ 是模 p 的原根. ■

一个有趣的问题是: 如果 m 不是素数, 则在模 m 的既约剩余系中下是否存在原根? 即 $\mathbb{Z}_m^*$ 是否为循环群? 一般来说, 答案是否定的. 比如

$$\mathbb{Z}_8^*=\{\bar{1},\bar{3},\bar{5},\bar{7}\}\cong\mathbb{Z}_2\oplus\mathbb{Z}_2.$$

定理 5.3.2　模 m 的既约剩余系有原根存在当且仅当 $m=2,4,p^l,2p^l$ (此处 p 是奇素数).

限于篇幅, 我们这里不再证明这个定理. 读者可以参考 [Hua57, 第三章, 第九节].

5.3.2　指标

设 $\bar{g}\in\mathbb{Z}_p^*$ 是原根. 对任何 $\bar{n}\in\mathbb{Z}_p^*$, 显然存在唯一的正整数 $k\le p-1$, 使得 $\bar{n}=\bar{g}^k$. 我们称 k 为 $\bar{n}$ 关于 $\bar{g}$ 的指标, 并记作 $k=\mathrm{ind}_g n$.

例 5.3.2　(1) 在模 17 的既约剩余系中, 取原根 $g=3$. 我们有

$$\mathrm{ind}_3 2=14,\quad \mathrm{ind}_3 5=5,\quad \mathrm{ind}_3 7=11,\quad \mathrm{ind}_3 11=7,\quad \mathrm{ind}_3 13=4.$$

(2) 在模 7 的既约剩余系中, 取原根 $g=3$. 我们有

$$\mathrm{ind}_3 2=2,\quad \mathrm{ind}_3 6=3.$$

如取原根 $g=5$, 则

$$\mathrm{ind}_5 2=4,\quad \mathrm{ind}_5 6=3.$$

命题 5.3.1　设 g 是模 p 的原根, 则
(1) $\mathrm{ind}_g ab\equiv\mathrm{ind}_g a+\mathrm{ind}_g b\pmod{p-1}$.
(2) $\mathrm{ind}_g(a^n)\equiv n\mathrm{ind}_g a\pmod{p-1}$.
(3) 设 g' 是另一原根, 则 $\mathrm{ind}_g a\equiv\mathrm{ind}_g g'\cdot\mathrm{ind}_{g'}a\pmod{p-1}$.
(4)

$$\mathrm{ord}_p a=\frac{p-1}{(\mathrm{ind}_g a,p-1)}.$$

(5) a 是原根当且仅当 $(\mathrm{ind}_g a, p-1)=1$.

证明 (1) 设 $n=\mathrm{ind}_g a$, $m=\mathrm{ind}_g b$. 我们有

$$g^{\mathrm{ind}_g ab}\equiv ab\equiv g^{n+m} \pmod p.$$

因此 $g^{\mathrm{ind}_g ab-n-m}\equiv 1 \pmod p$. 由定理 5.3.1 (1), $p-1\mid \mathrm{ind}_g ab-n-m$.

(2) 是 (1) 的直接推论.

(3) 设 $k=\mathrm{ind}_g g'$. 我们有

$$g^{\mathrm{ind}_g a}\equiv a\equiv g'^{\mathrm{ind}'_g a}\equiv (g^k)^{\mathrm{ind}'_g a}\equiv g^{k\mathrm{ind}'_g a} \pmod p.$$

类似地, 由定理 5.3.1 (1) 即得结论.

(4) 由 (2) 可知

$$p-1=\mathrm{ind}_g a^{\mathrm{ord}_p a}\equiv \mathrm{ord}_p a\cdot \mathrm{ind}_g a \pmod{p-1},$$

即 $p-1|\mathrm{ord}_p a\cdot \mathrm{ind}_g a$, 从而

$$\frac{p-1}{(\mathrm{ind}_g a, p-1)}\mid \mathrm{ord}_p a.$$

另一方面

$$a^{\frac{p-1}{(\mathrm{ind}_g a,p-1)}}\equiv g^{\frac{(p-1)\mathrm{ind}_g a}{(\mathrm{ind}_g a,p-1)}}\equiv (g^{p-1})^{\frac{\mathrm{ind}_g a}{(\mathrm{ind}_g a,p-1)}}\equiv 1 \pmod p.$$

因此 (为什么?)

$$\mathrm{ord}_p a\mid \frac{p-1}{(\mathrm{ind}_g a, p-1)}.$$

这就证明了等式.

(5) 如果 a 是原根, 则由 (3) 得

$$1=\mathrm{ind}_g g\equiv \mathrm{ind}_g a\cdot \mathrm{ind}_a g \pmod{p-1}.$$

因此 $(\mathrm{ind}_g a, p-1)=1$.

反过来, 若已知 $(\mathrm{ind}_g a, p-1)=1$, 则由 (4) 知, $\mathrm{ord}_p a=p-1$, 即 a 是原根. ■

例 5.3.3 (1) 已知模 17 有原根 $g=3$, 求出全部原根.

根据命题 5.3.1 (5), 我们只要找出所有指标 $\mathrm{ind}_3 a$ 与 16 互质的既约剩余类 $\bar{a}$ 即可. 换言之, 所有的原根可写为 $\bar{3}^{2k+1}$, $k=0,1,\cdots,7$. 具体计算得

$$\bar{3},\quad 1\bar{0},\quad \bar{5},\quad 1\bar{1},\quad 1\bar{4},\quad \bar{7},\quad 1\bar{2},\quad \bar{6}.$$

(2) 已知模 13 有原根 $g=2$, 求出全部原根.

类似地, a 是原根当且仅当 $(\mathrm{ind}_2 a, 12)=1$, 这表明 $\mathrm{ind}_2=1,5,7,11$. 因此全部原根为

$$\bar{2},\quad \bar{6},\quad 1\bar{1},\quad \bar{7}.$$

例 5.3.4 求 -1 在模 p 下关于原根 g 的指标.

注意到 $\mathrm{ord}_p(-1)=2$, 故由命题 5.3.1 (4) 得 $\frac{p-1}{2}\mid \mathrm{ind}_g(-1)$. 又因为 $0<\mathrm{ind}_g(-1)<p-1$, 所以 $\mathrm{ind}_g(-1)=\frac{p-1}{2}$. ■

在求指标时, 利用命题 5.3.1 (1)(2) 及例 5.3.4, 常可化简计算.

例 5.3.5　已知模 13 有原根 $g=2$,

(1) 求 $\mathrm{ind}_g 6$, $\mathrm{ind}_g 7$, $\mathrm{ind}_g 11$

首先,

$$\mathrm{ind}_g 6 \equiv \mathrm{ind}_g 2 + \mathrm{ind}_g 3 \equiv 1 + \mathrm{ind}_g 3 \equiv 1 + \mathrm{ind}_g 16 \equiv 1 + 4\mathrm{ind}_g 2 \equiv 5 \pmod{12},$$

故 $\mathrm{ind}_g 6 = 5$.

其次

$$\mathrm{ind}_g 7 \equiv \mathrm{ind}_g(-6) \equiv \mathrm{ind}_g(-1) + \mathrm{ind}_g 6 \equiv 6 + 5 \pmod{12},$$

因而 $\mathrm{ind}_g 7 = 11$.

类似地,

$$\mathrm{ind}_g 11 \equiv \mathrm{ind}_g(-2) \equiv \mathrm{ind}_g(-1) + \mathrm{ind}_g 2 \equiv 7 \pmod{12},$$

所以 $\mathrm{ind}_g 11 = 7$.

(2) 求 $\mathrm{ord}_{13} 6$, $\mathrm{ord}_{13} 7$, $\mathrm{ord}_{13} 11$.

由上一小题及命题 5.3.1 (4), 我们得到 $\mathrm{ord}_{13} 6 = \mathrm{ord}_{13} 7 = \mathrm{ord}_{13} 11 = 12$.

(3) 求出所有满足 $\mathrm{ord}_{13} a = 3$ 的剩余类.

由命题 5.3.1 (4), 这等价于求满足以下条件的剩余类:

$$3 = \frac{13-1}{(13-1, \mathrm{ind}_2 a)},$$

即 $(12, \mathrm{ind}_2 a) = 4$, 亦即 $\mathrm{ind}_2 a = 4, 8$. 所以 $a \equiv 2^4, 2^8 \pmod{13}$, 也就是 $a \equiv 3, 9$. ■

例 5.3.6　已知 g 是模 19 下的原根, 并且 $\mathrm{ind}_g 3 = 5$, $\mathrm{ind}_g 17 = 8$, 试求 g 的最小非负剩余.

先求整数 u, v 使得 $5u + 8v = 1$. 比如取 $u = -3, v = 2$. 于是

$$g \equiv g^{5u+8v} \equiv 3^u \cdot 17^v \equiv 27^{-1} \cdot 289 \equiv 8^{-1} \cdot 4 \equiv 12 \cdot 4 \equiv 10 \pmod{19}.$$

5.3.3　应用 (I): 威尔逊定理的新证明

设 p 是奇素数. 我们用原根重新证明威尔逊定理

$$(p-1)! + 1 \equiv 0 \pmod{p}.$$

设 g 是模 p 下的原根. 我们只需注意到以下的同余式

$$(p-1)! \equiv g \cdot g^2 \cdot \cdots \cdot g^{p-2} \cdot g^{p-1} \pmod{p}.$$

上式右边在模 p 下同余于

$$g^{\sum_{k=1}^{p-1} k} \equiv g^{\frac{(p-1)p}{2}} \equiv (g^{\frac{p-1}{2}})^p \equiv g^{\frac{p-1}{2}} \equiv -1 \pmod{p}.$$

后面两个同余式来自于费马小定理和例 5.3.4. 这就完成了证明.

5.3.4　应用 (II): 正多边形尺规作图问题

这里我们介绍高斯关于正多边形作图的漂亮结果.

定理 5.3.3 (**高斯**)　一个正 m 边形能用尺规作图得到的充分必要条件是:

$$m = 2^e p_1 p_2 \cdots p_s,$$

这里诸 p_i 是费马素数, 且两两不同.

我们已经知道前几个费马素数

$$F_0 = 3, \quad F_1 = 5, \quad F_2 = 17, F_3 = 257.$$

正三角形和正五边形的尺规作图是比较容易的. 但正十七边形尺规作图则是一个让人吃惊的结果. 我们这里就讨论正 17 边形的尺规作图问题.

设

$$\omega = e^{\frac{2\pi\sqrt{-1}}{17}} = \cos\frac{2\pi}{17} + \sqrt{-1}\sin\frac{2\pi}{17}.$$

它是 $z^17 = 1$ 的本原单位根. ω^k $(k = 0, 1, 2, \cdots, 16)$ 恰好构成了正十七边形的顶点. 因此我们只需要用尺规作出 ω 对应的点的位置即可.

取模 17 下的原根 $g = 3$. 令

$$z_k = \omega^{3^k}, \quad k = 0, 1, \cdots, 15.$$

设

$$\begin{cases} X &= \sum\limits_{k=0}^{7} z_{2k}, \\ x &= \sum\limits_{k=0}^{7} z_{2k+1}. \end{cases}$$

容易验证

$$X + x = \sum_{k=1}^{15} \omega^k = -1, \quad Xx = 4(\sum_{k=1}^{15} \omega^k) = -4.$$

换言之, X, x 是方程 $t^2 + t - 4 = 0$ 的两个根. 因此

$$X = \frac{\sqrt{17} - 1}{2}, \quad x = \frac{-1 - \sqrt{17}}{2}.$$

设

$$\begin{cases} U &= \sum\limits_{k=0}^{3} z_{4k}, \\ u &= \sum\limits_{k=0}^{3} z_{4k+2}, \end{cases} \qquad \begin{cases} V = \sum\limits_{k=0}^{3} z_{4k+1}, \\ v = \sum\limits_{k=0}^{3} z_{4k+3}. \end{cases}$$

我们有

$$U + u = X, \quad Uu = -1, \quad V + v = x, \quad Vv = -1.$$

因此 U, u 是方程 $t^2 - Xt - 1 = 0$ 的两个根; V, v 是方程 $t^2 - xt - 1 = 0$ 的两个根. 因此

$$U = \frac{\sqrt{X^2+4} + X}{2}, \quad u = \frac{X - \sqrt{X^2+4}}{2}, \quad V = \frac{\sqrt{x^2+4} + x}{2}, \quad v = \frac{x - \sqrt{x^2+4}}{2}.$$

最后设 $W = z_0 + z_8$, $w = z_4 + z_{12}$, 则有

$$W + w = U, \quad Ww = V,$$

因而解得

$$W=\frac{\sqrt{U^2-4V}+U}{2},\quad w=\frac{U-\sqrt{U^2-4V}}{2}.$$

另一方面, 由 W 的直接定义可知 $W=\omega+\omega^{16}=\omega+\omega^{-1}=2\mathrm{Re}\omega$, 所以通过二次方程

$$\omega^2-W\omega+1=0$$

可求出 ω 的根式表达.

总结起来, 正十七边形的作图可以分为几步:

(1) 作出长度为 X,x 的线段.

(2) 作出长度为 U,V 的线段.

(3) 作出长度为 W,w 的线段.

(4) 在实轴上作出 ω 的实部长度的线段, 并由此求出 ω 的位置.

5.4 k 次剩余

设 p 是奇素数. 我们考虑同余方程

$$x^k\equiv n\pmod p,\tag{5-4}$$

这里 $p\nmid n$. 如果该方程有解, 则称 n 在模 p 下是 k 次剩余的; 否则就称它是k 次非剩余. 当 $k=2$ 时, 这就是我们讨论的平方剩余.

今取模 p 的任一原根 g. 设 $y=\mathrm{ind}_g x$, $m=\mathrm{ind}_g n$. 方程 (5-4) 等价于

$$g^{ky}\equiv g^m\pmod p.$$

这又等价于求

$$ky\equiv m\pmod{p-1}$$

的剩余类解 $y\pmod{p-1}$. 由命题 2.6.1 和命题 2.6.2, 这就得到如下结论.

定理 5.4.1 *n 在模 p 下是 k 次剩余的充分必要条件是*

$$(k,p-1)\mid \mathrm{ind}_g n.$$

条件成立时, 方程 (5-4)在模 p 下恰有 $(k,p-1)$ 个剩余类解.

注 5.4.1 上述结论不依赖于原根的选取. 这一点可以从命题 5.3.1 (3) (5) 看到. ■

推论 5.4.1 *模 p 下的 k 次剩余类恰有 $\frac{p-1}{(k,p-1)}$ 个.*

证明 这相当于指标被 $(k,p-1)$ 整除的既约剩余类个数. 这样的指标显然有 $\frac{p-1}{(k,p-1)}$ 个. ■

上述推论显然是命题 3.2.1 的推广.

推论 5.4.2 *n 在模 p 下是平方剩余的充分必要条件是 $\mathrm{ind}_g n$ 是偶数, 这里 g 是模 p 的原根. 特别地, -1 是平方剩余的充分必要条件为 $p\equiv 1\pmod 4$.*

证明 前半部分来自于定理 5.4.1, 后半部分来自于例 5.3.4. ■

从近世代数的观点看, 上面的讨论可以归结为群同态

$$\Phi_k : \mathbb{Z}_p^* \longrightarrow \mathbb{Z}_p^*, \quad \bar{x} \to \bar{x}^k.$$

其中核

$$\mathrm{Ker}\Phi_k = \{\bar{x} \in \mathbb{Z}_p^* \mid \bar{x}^k = \bar{1}\}$$

是阶数为 $(k, p-1)$ 的循环子群, 生成元为 $\bar{g}^{\frac{p-1}{(k,p-1)}}$, 这里 $\bar{g}$ 是原根; 像 $\mathrm{Im}\Phi_k$ 则由所有 k 次剩余构成, 它是阶数为 $\frac{p-1}{(k,p-1)}$ 的循环子群–这一点也可以从自然同态看出来:

$$\mathbb{Z}_p^*/\mathrm{Ker}\Phi_k \cong \mathrm{Im}\Phi_k.$$

当 $k = p$ 时, 我们也可以定义环同态

$$F_p : \mathbb{Z}_p \longrightarrow \mathbb{Z}_p, \quad \bar{x} \to \bar{x}^p.$$

当然, 读者需要验证恒等式

$$(\bar{x} + \bar{y})^p = \bar{x}^p + \bar{y}^p, \quad \bar{x}, \bar{y} \in \mathbb{Z}_p. \tag{5-5}$$

上述同态被称为 Frobenius 同态.

例 5.4.1　已知 $g = 2$ 是模 13 的原根, 求方程

$$x^4 \equiv 3 \pmod{13}$$

的剩余类解.

前面已算得 $\mathrm{ind}_2 3 = \mathrm{ind}_2 16 = 4$. 设 $r = \mathrm{ind}_2 x$. 因此由定理 5.4.1 知, 原方程等价于求

$$4r \equiv 4 \pmod{12}.$$

此时 $r \equiv 1, 4, 7, 10 \pmod{12}$, 故原方程的解为

$$x \equiv 2, 2^4, 2^7, 2^{10} \equiv 2, 3, 11, 10 \pmod{13}.$$

推论 5.4.3　设 $p \equiv 3 \pmod 4$, 那么在模 p 下, n 是平方剩余当且仅当 n 是四次剩余.

证明　由定理 5.4.1, n 是四次剩余的充分必要条件是

$$2 = (4, p-1) \big| \mathrm{ind}_g n,$$

这里 g 是原根. 又由推论 5.4.2, 上述条件也等价于平方剩余. ■

本章习题

加 $*$ 号的习题表示有一定难度.

习题 5.1　求出模 11 下的全部原根.

习题 5.2　已知 $g = 5$ 是模 23 下的原根, 试求指标

$$\mathrm{ind}_g 2, \quad \mathrm{ind}_g 3, \quad \mathrm{ind}_g 7, \quad \mathrm{ind}_g 11, \quad \mathrm{ind}_g 13.$$

习题 5.3　已知 $g = 10$ 是模 29 下的原根, 试求指数

$$\mathrm{ord}_{29} 2, \quad \mathrm{ord}_{29} 3, \quad \mathrm{ord}_{29} 7,$$

并求出所有满足 $\mathrm{ord}_{29}a = 3$ 的剩余类.

习题 5.4　已知 g 是模 37 下的原根, 且 $\mathrm{ind}_g 31 = 9$, $\mathrm{ind}_g 30 = 14$, 求 g 的最小非负剩余.

习题 5.5　设 p 是奇素数, $p \nmid n$. 证明或否定如下断言: 如果 $\mathrm{ind}_g n$ 的值不依赖于任何原根 g 的选取, 那么 $n \equiv \pm 1 \pmod{p}$.

习题 5.6　模仿第 5.3.4 节的方法, 讨论正五边形的尺规作图.

习题 5.7　验证等式 (5-5).

参 考 文 献

[Hua57] 华罗庚: *数论导引*, 科学出版社, 1957.

[HW10] G. H. Hardy, E. M. Wright: *哈代数论* (第 6 版), 人民邮电出版社, 2010.

索 引

k 次剩余, 94

带余数除法, 63

Frobenius 同态, 95

Hurwitz 最佳逼近定理, 71

Legendre 渐近分数判定条件, 72

Mazur 定理, 80
Mordell 定理, 80

Wolstenholme 定理, 88

Zeller 公式, 28

爱森斯坦恒等式, 55

倍数, 4
本原勾股数, 41
标准分解式, 5

不定方程, 2
不可约元, 64

带余数除法, 6

单位元, 64

丢番图方程, 2
二次互反律, 53
二次剩余, 2, 46

范数, 64
费尔马数, 13
费马大定理, 46
费马方程, 46
费马平方和定理, 62
费马小定理, 24

高斯整数, 63
高斯整数环, 63
高斯正多边形作图问题, 93

公倍数, 10
公因子, 5
勾股方程, 2, 41
勾股数, 41

合数, 4

互素, 5
互质, 5
华林问题, 66

既约剩余系, 23
简单连分数, 68
简化剩余系, 23

渐近分数, 68
进位制, 26

可逆元, 64

勒让德符号, 47
黎曼猜想, 14
黎曼函数, 14
理想, 18

连分数, 67

梅森素数, 56

欧几里德算法, 8
欧几里得算法, 64
欧拉定理, 24, 48
欧拉函数, 23
佩尔方程, 2, 67

平方剩余, 2, 46
奇异有理曲线, 79
弃九算法, 27

商, 6
商高定理, 41

剩余类, 21

素数, 4

素数定理, 15
算术基本定理, 9, 64
孙子定理, 36

同余, 20
同余数, 81
椭圆曲线, 3, 79
完全商, 69
完全数, 56
威尔逊定理, 49

位数码和, 26
无穷递降法, 46

相伴, 64

小数部分, 1

循环连分数, 72
雅克比符号, 57

因子, 4

有理点, 1
有限连分数, 67
余数, 6

原根, 90

整除, 4, 64
整数部分, 1
整数点, 1

指标, 90
指数, 89
中国剩余定理, 36
主理想, 18

最大公因子, 5
最小公倍数, 10