卡塔兰猜想是 Mih˘ailescu 定理

Martin Klazar
(KAM MFF UK Praha)

arXiv:2601.14900v1 [math.HO] 21 Jan 2026

谨以此书献给我的父母 Blanka 和 Jiˇrˊı

48. 定 ´理 `。**两个连续整数，除 8 和 9 外，不可能是完全幂。（Catalan。）**

参见 [5]。

192

13. Note

摘自一封致编辑的信，作者是巴黎综合理工学院的助教 *E. Catalan* 先生。

“𝕀先生，谨请您在您的文集中刊载下面这个定理：我认为它是正确的，尽管我尚未能完全证明；也许别人会更幸运：两个连续整数，除 8 和 9 外，不可能是完全幂。换言之，未知数为正整数的方程 $x^m - y^n = 1$ 只有一个解。”

参见 [6]。

——根据 [1, 第 1—2] 页撰写。1842年，比利时-法国数学家 Eug`ène Ch. Catalan（1814—1894年）（见 [13]）提出了一条定理，却未给出证明；该定理断言，8 和 9 是仅有的一对连续纯幂。两年后，他修正了自己的说法，将其改为猜想。卡塔兰猜想于 2004年由罗马尼亚数学家 Preda Mih˘ailescu（1955年）证明。本文将给出卡塔兰猜想的完整证明。具体而言，我们将完整呈现 Mih˘ailescu 的证明。

引言

卡塔兰猜想 [6] （1844年）可以表述如下。对于整数 $m,\ n \geq 2$丢番图方程的唯一解

$$x^m - y^n = 1$$

在非零整数中 $x,\ y$ 是 $m = y = 2,\ \ x = \pm 3$ 和 $n = 3$。经过许多作者取得的部分成果，卡塔兰猜想于2004年由 P. Mihˇailescu [25] 证明。

关于这个主题，有三本优秀的书： [30] 由 P. Ribenboim 撰写， [32] 由 R. Schoof 撰写， [1] 由 Yu. Bilu、Y. Bugeaud 和 M. Minotte 撰写。第一本书出版于 Mihˇailescu 之前；另外两本则介绍了 Mihˇailescu 的证明。不过，它们都远非自成一体。本文旨在完整且自成一体地介绍 Mihˇailescu 的证明，实际上也就是卡塔兰猜想的证明（这必须涵盖许多 Mihˇailescu 视为理所当然的内容）。第 1 至?? 章的前半部分对应于我在 2024/25 和 2025/26 学年开设的代数数论课程中的讲课内容。

容易看出，可以假设指数 $m = p$ 和 $n = q$ 是互异素数。卡塔兰猜想的解自然分为两部分：含有 $p = 2$ 或 $q = 2$ 的初等部分，以及含有 $p,\ q \geq 3$ 的非初等部分。“初等”并不意味着容易，“非初等”则意味着困难。前三章讨论初等部分，本文其余内容则专门讨论非初等情形。除非另有说明，解总是指整数解。

在第1章中，我们解方程 $x^2 - y^3 = 1$；其仅有的解为$\langle \pm 3,\ 2\rangle, \langle \pm 1,\ 0\rangle$，以及 $\langle 0,\ -1\rangle$。我们介绍该方程的三种解法。历史上最早的一种由 L. Euler 于 1737 年提出，见第 1.4 节。它利用了这样一个事实：从现代观点来看，$x^2 = y^3 + 1$ 是一条椭圆曲线。欧拉实际上证明了上述五个解是仅有的有理数解。第二种解法见第 1.3 节，由本文作者于 1989年提出；因式分解 $x^2 = (y+1)(y^2 - y + 1)$引导我们研究佩尔方程 $x^2 - 3y^2 = 1$的解的性质。另一种解 $x^2 - y^3 = 1$的方法是从因式分解 $(x+1)(x-1) = y^3$入手；由此可导出方程 $x^3 - 2y^3 = \pm 1$。1957 年，A. Wakulicz 在一篇鲜为人知的文章中给出了更一般方程 $x^3 + y^3 = 2z^3$ 的一种初等解法；我们在第 1.5 节介绍他的结果。$x^2 - y^3 = 1$ 的这三种解法都是完全初等的，也就是说，它们都在域 $\mathbb{Q}$中进行。

布拉格和洛尼，2025年12月至 ??　　Martin Klazar

记号

$\mathbb{N} = \{1, 2, \dots\}$ 是自然数集，且 $\mathbb{N}_0 = \{0, 1, 2, \dots\}$。

目录

（[c] . . . 表示一个相对完整的章节。）

引言 **iv**

记号 **v**

1 欧拉定理： $x^2 - y^3 = 1$ **1**

1.1 [c]佩尔方程.1 1.2 [c]唯一分解整环和 PP.3 1.3 [c]Klazar 对.....的解决 $x^2 - y^3 = 1$ .8 1.4 [c]欧拉论证的现代补充.11 1.5 Wakulicz 的解法 $x^3 + y^3 = 2z^3$ .14

2 V. 勒贝格定理： $x^m - y^2 = 1$ **15**

2.1 [c] p-进阶的性质.15 2.2 [c]V. 勒贝格对 $x^m - y^2 = 1$ 的解.16 2.3 [c]欧几里得整环是唯一分解整环.17

3 Chao Ko定理： $x^2 - y^q = 1$ **，其中** $q \geq 5$ **21**

3.1 [c]两个引理.21 3.2 [c]Chein 对 $x^2 - y^q = 1$ 的求解.22

4 卡塞尔的两个关系： $p \mid y$ **和** $q \mid x$ **24**

4.1 五个引理.24 4.2 [c]关系 $q \mid x$ .26 4.3 关系 $p \mid y$ .27 4.4 推论.28

5 米哈伊莱斯库定理： $x^p - y^q = 1$ **且** $p > q > 2$ **29**

5.1 [c]定理 M0.95–M4.29 5.2 第 6–A 章概述.31

6 障碍群 **32**
6.1 数域.32 6.2 分圆域.33 6.3 障碍群.33

7 超 Cassels 关系： $p^2 \mid y$ **和** $q^2 \mid x$ **347**
.1 The Stickelb ideal 34
.7.2 定理 M0。95 和 M1.34

8 定理 M4： $p = 3,\ 5$ **或** $q = 3,\ 5$ **35**

A 数学分析的结果 36A.1 泰勒级数.36

B 代数中的结果 37B.1 交换群环.37

参考文献 37

较大

第1章

欧拉定理

我们从第一个初等情形开始，踏上证明卡塔兰猜想这一漫长旅程的征途：该方程的唯一整数解为

$$x^2 - y^3 = 1$$

是数对 $\langle \pm 3, 2\rangle$, $\langle \pm 1, 0\rangle$ 和 $\langle 0, -1\rangle$。我们给出三种证明。第1.1节汇集了本章及第3章所需的佩尔方程 $x^2 - dy^2 = 1$ 的辅助结果。第1.2节概述唯一分解整环和幂的原理。第1.3节介绍作者于1989年在 $[18]$, 中找到的 $x^2 - y^3 = 1$ 的解。第1.4节专门介绍一项结果的现代证明：莱昂哈德·欧拉（1707–1783）于1738年在 $[15]$ 中证明，五个数对是该方程仅有的有理解。最后的第1.5节介绍 A. Wakulicz $[34]$ 的初等证明，证明方程 $x^3 + y^3 = 2z^3$ 在 $x \neq \pm y$时无解。因此， $x^3 - 2y^3 = \pm 1$ 的仅有解是 $\langle \pm 1, 0\rangle$和 $\langle \pm 1, \pm 1\rangle$ （等号）。利用因式分解

$$(x - 1)(x + 1) = y^3$$

由此可推得， $x^2 - y^3 = 1$ 恰有上述五个解。非平凡（非零）解 $\langle \pm 3,\ 2\rangle$ 的存在，使这个卡塔兰猜想的初等情形与接下来两章中的初等情形相比，呈现出鲜明的特点。在第 1.3、1.4 和 1.5 节中，我们分别沿用 $[18]$, $[9]$ 和 $[34]$,。

1.1 佩尔方程

佩尔方程是以下形式的丢番图方程

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

未知数为 x, y ，参数 $d \in \mathbb{N}$ 不是平方数： $d = 2$、3、5、6、7、8、10 等。我们称一对 $a, b \in \mathbb{N}$ 为该方程的最小解

方程当且仅当 $a^2 - db^2 = 1$，且不存在解 $x, y \in \mathbb{N}$ 满足 $x < a$。最小解若存在，则唯一。

命题 1.1.1 设 $a, b \in \mathbb{N}$ 是佩尔方程的最小解

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

则方程的自然数解 $x, y \in \mathbb{N}$ 构成一个无限集

$$\{\langle x,\, y\rangle \in \mathbb{N}^2 \colon\ x + y\sqrt{d} = \left(a + b\sqrt{d}\right)^n \ \textit{for some}\ n \in \mathbb{N}\}\,.$$

证明。设 $x_i, y_i \in \mathbb{Z}$, $i = 1,2$ 是方程的两个解，并由下式定义 $x_3, y_3 \in \mathbb{Z}$

$$x_3 + y_3\sqrt{d} = \left(x_1 + y_1\sqrt{d}\right)\left(x_2 + y_2\sqrt{d}\right)\,.$$

那么也有

$$x_3 - y_3\sqrt{d} = \left(x_1 - y_1\sqrt{d}\right)\left(x_2 - y_2\sqrt{d}\right)\,.$$

将所示等式相乘，得到

$$x_3^2 - dy_3^2 = \left(x_1^2 - dy_1^2\right)\left(x_2^2 - dy_2^2\right) = 1 \cdot 1 = 1\,.$$

因此，x_3, y_3 也是方程的一个解。更容易看出，若 x, y 是方程的一个解，则其倒数

$$\frac{1}{x + y\sqrt{d}} = x - y\sqrt{d}$$

得到一个解 x，$-y$。注意，若 x_i，$y_i \in \mathbb{N}$、$i = 1$，2 是该方程的解，那么

$$x_1 < x_2 \iff x_1 + y_1\sqrt{d} < x_2 + y_2\sqrt{d}\,.$$

此外，若 x，$y \in \mathbb{Z}$ 是该方程的一个解，那么 x，$y \in \mathbb{N}$ 当且仅当 $x + y\sqrt{d} > 1$。

现在令 a，b 如上所述，并令 x，$y \in \mathbb{N}$ 满足 $x^2 - dy^2 = 1$。我们取唯一的 $m \in \mathbb{N}_0$，使得

$$\alpha := \left(a + b\sqrt{d}\right)^m < x + y\sqrt{d} \le \left(a + b\sqrt{d}\right)^{m+1}\,.$$

如果最后一个不等式是严格不等式，那么

$$1 < u + v\sqrt{d} := \alpha^{-1} \cdot (x + y\sqrt{d}) < a + b\sqrt{d}$$

将得到该方程的一个解 u，$v \in \mathbb{N}$，这与 a，b的最小性相矛盾。因此 $x + y\sqrt{d} = \left(a + b\sqrt{d}\right)^{m+1}$。□

1770年，拉格朗日证明了每个佩尔方程都有一个最小解，因此有无穷多个解。或许我们不需要这个结果来解决卡塔兰猜想。但我们需要了解佩尔方程 $x^2 - 3y^2 = 1$ 的解的一些性质。

推论 1.1.2 佩尔方程的解

$$x^2 - 3y^2 = 1$$

恰好是以下各对：$\langle \pm x_n、\ \pm y_n \rangle$、$n \in \mathbb{N}_0$，其中

$$x_n + y_n\sqrt{3} = \left(2 + \sqrt{3}\right)^n .$$

此外，$x_0 = 1$、$y_0 = 0$ 以及 $x_{n+1} = 2x_n + 3y_n$、$y_{n+1} = x_n + 2y_n$。

证明。这由命题 1.1.1 得出，因为 $x^2 - 3y^2 = 1$ 具有最小解 $\langle 2,\ 1 \rangle$。□

命题 1.1.3 若 $\langle x_n、\ y_n \rangle$、$n \in \mathbb{N}_0$如前一个推论中所述，则对于每个 $n \in \mathbb{N}_0$，我们有

$$x_{2n} = 2x_n^2 - 1,\ y_{2n} = 2x_n y_n,\ x_{2n+1} = (y_n + y_{n+1})^2 + 1,\ y_{2n+1} = 2x_n y_{n+1} - 1 .$$

数 x_n 和 y_n 具有不同的奇偶性，并且 x_n 为奇数当且仅当 n 为偶数。

证明。由于 $x_n^2 - 3y_n^2 = 1$,

$$\begin{aligned} x_{2n} + y_{2n}\sqrt{3} &= \left(2 + \sqrt{3}\right)^{2n} = \left(x_n + y_n\sqrt{3}\right)^2 \\ &= x_n^2 + 3y_n^2 + 2x_n y_n\sqrt{3} = 2x_n^2 - 1 + 2x_n y_n\sqrt{3} . \end{aligned}$$

同样,

$$\begin{aligned} x_{2n+1} + y_{2n+1}\sqrt{3} &= (2 + \sqrt{3})(x_n^2 + 3y_n^2 + 2x_n y_n\sqrt{3}) \\ &= 2x_n^2 + 6x_n y_n + 6y_n^2 + (x_n^2 + 4x_n y_n + 3y_n^2)\sqrt{3} . \end{aligned}$$

现在 $2x_n^2 + 6x_n y_n + 6y_n^2 = x_n^2 + 6x_n y_n + 9y_n^2 + 1 = (y_n + x_n + 2y_n)^2 + 1 = (y_n + y_{n+1})^2 + 1$和 $x_n^2 + 4y_n y_n + 3y_n^2 = 2x_n^2 + 4x_n y_n - 1 = 2x_n(x_n + 2y_n) - 1 = 2x_n y_{n+1} - 1$。最后一个断言由刚刚证明的公式可立即得出。□

1.2 唯一分解整环和幂原则

这些缩写分别指唯一分解整环 和幂原则。幂原则推动丢番图方程的解，因此值得我们不再像通常那样一带而过。这里我们将对它们进行详细讨论。

命题 1.2.1 (PP0) 设 a、b、$c \in \mathbb{Z}$和 $k \in \mathbb{N}$。若 a 整除 bc^k，且 a、c互素，则 a 整除 b。

命题 1.2.2 (PP1) 设 k、$l \in \mathbb{N}$，其中 k、$l \geq 2$。若 a_i、$b \in \mathbb{N}_0$ 关于 $i \in [k]$是 $k+1$ 个数，且这些数两两互素，并且

$$a_1 a_2 \dots a_k = b^l \,,$$

那么存在 k 两两互素的数 $b_i \in \mathbb{N}_0$，使得对每个 $i \in [k]$,

$$a_i = b_i^l \,.$$

如果 l 是奇数，那么将 $\mathbb{N}_0$ 替换为 $\mathbb{Z}$时，该结果也成立。

命题 1.2.3 (PP2) 设 p是素数，且 $k \in \mathbb{N}$满足 $k \geq 2$。若 a、b、c是$\mathbb{N}_0$ 中的数，使得

$$\gcd(a,b) = p \wedge ab = c^k \,,$$

那么存在互素数 d、$e \in \mathbb{N}_0$，使得

$$\{a,\, b\} = \{pd^k,\, p^{k-1}e^k\} \,.$$

如果 k 是奇数，那么将 $\mathbb{N}_0$ 替换为 $\mathbb{Z}$时，该结果也成立。

为了将 PP0、PP1 和 PP2 推广到整环并证明它们，我们将回顾唯一分解整环的概念。我们还将引入不可约因式分解。回想一下，（整）整环

$$R = \langle R,\, 0_R,\, 1_R,\, +,\, \cdot \rangle$$

是一个带有 1_R 的交换环，使得对每个 a，$b \in R^*$ $(= R \setminus \{0_R\})$，都有 $ab \neq 0_R$。对于 a，$b \in R$，若对某个 $c \in R$ 有 $b = ac (= a \cdot c)$，我们就称 a 整除 b（在 R 中），记作 $a \,|\, b$。若 $a \,|\, 1_R$，则称 $a \in R$ 为单位，也就是说，a 是乘法可逆的。R 中单位的集合记为 $R^\times$。容易看出

$$\langle R^\times,\, 1_R,\, \cdot \rangle$$

是一个阿贝尔群，即整环 R 的单位群。对于 a，$b \in R$，若对某个 $c \in R^\times$ 有 $a = bc$，我们记作 $a \sim b$；称元素 a 和 b 是相伴的。例如，在整数整环中

$$\mathbb{Z} = \langle \mathbb{Z},\, 0,\, 1,\, +,\, \cdot \rangle$$

当且仅当 $m = \pm n$ 时，有 $m \sim n$。容易看出，$\sim$ 是一个等价关系，并且关于乘法是相容的。对于 $a \in R$，我们记为

$$[a]_\sim \;\; (= \{b \in R \colon\; b \sim a\})$$

等价关系 $\sim$中元素 a的等价类。我们得到（交换）等价类幺半群

$$\langle R/\!\sim,\, [1_R]_\sim = R^\times,\, \cdot \rangle \,.$$

命题 1.2.4 在任意整环 R 中，两个元素相伴当且仅当它们彼此整除。

证明。令 $a,b\in R$。假设 $a\sim b$。因此 $a=bc$ 且 $ac^{-1}=b$，其中某个c, $c^{-1}\in R^{\times}$。于是 $b\,|\,a$ 且 $a\,|\,b$。

假设 $a\,|\,b$ 且 $b\,|\,a$。因此 $b=ac$ 且 $a=bd$，其中某个 $c,d\in R$。我们得到等式

$$b\cdot(1_R-d\cdot c)=0_R\,.$$

因此，由于我们处于整环中，$b=a=0_R$ 且 $a\sim b$，或者 $dc=1_R$ 且再次有$a\sim b$。□

两个元素 $a,b\in R$ 互素，记作 $(a,b)=1_R$，若它们同时只能被单位元整除。

定义 1.2.5（最大公因子）设 R 是一个整环，且 $a,b\in R$。若 $c\in R$是 a 和 b的最大公因子，记作 $c=\gcd(a,b)$，则 c 整除a 和 b，并且 a 和 b 的每个公因子都整除 c。

若 $c=\gcd(a,b)$ 且 $c'\sim c$，则 $c'=\gcd(a,b)$。若 $a\sim a'$、$b\sim b'$、$c=\gcd(a,b)$ 且 $c'=\gcd(a',b')$，则 $c\sim c'$。此外，a和 b互素，当且仅当 $\gcd(a,b)=1_R$。

设 R 是一个整环。若元素 $a\in R$ 满足 $a\in R^*\setminus R^{\times}$，且在每个乘法分解 $a=bc$（其中 $b,c\in R$）中，b 或 c 是单位，则称 $a\in R$ 为不可约元。若$a,b\in R$，$a\sim b$ 且 a 是不可约元，则 b也是不可约元。我们用 R^{ir}表示 R 中的不可约元集合。

定义 1.2.6（唯一分解整环 1） R 是唯一分解整环，或称唯一分解整环，若 $R^*\setminus R^{\times}$ 中的每个元素都可以表示为不可约元的乘积，且该乘积在因子的排列顺序以及关系 $\sim$意义下唯一。

更具体地说，如果对每个元素 $a\in R^*\setminus R^{\times}$，都存在 $m\in\mathbb{N}$ 个不可约元 a_i，使得.....，则 R 是唯一分解整环

$$a=a_1\cdot a_2\cdot\ldots\cdot a_m\,,$$

并且，如果任意等式.....

$$c_1\cdot c_2\cdot\ldots\cdot c_l=b_1\cdot b_2\cdot\ldots\cdot b_m\,,$$

其中 l，$m\in\mathbb{N}$ 和 b_i 以及 c_i 均为不可约元，这意味着 $l=m$，并且存在一个对数字 1，2，.....，l的置换 π，使得对每个 $i\in[l]$，都有 $c_i\sim b_{\pi(i)}$。唯一分解整环的一个典型例子是 $\mathbb{Z}$，我们将在第 2.3 节中证明这一点。

回顾一下，如果 A 和 B 是集合，且 $X\subset A\times B$，那么关系 X 是一个偏函数（从 A 到 B），当且仅当对每个 $a\in A$，至多存在一个$b\in B$ 使得 $\langle a,\ b\rangle\in X$。我们将形式化（实际上是集合论化）不可约分解。

定义 1.2.7（不可约分解）设 R 是一个整环，$\mathbb{I}=R^{\mathrm{ir}}/\!\sim$，且 $a\in R^*$。不可约分解（在 R 中）是有限偏函数 X

从 $\mathbb{I}$ 到 $\mathbb{N}$。若 $X \neq \emptyset$，我们称 X 是元素 a 的不可约分解，当且仅当

$$[a]_\sim = \prod_{\langle \alpha,\, m\rangle \in X} \alpha^m .$$

我们称 $X = \emptyset$ 是 a 的不可约分解，当且仅当 $a \in R^\times$。

对于任意不可约分解 X，我们定义

$$(X)_1 = \{\alpha \in \mathbb{I} \colon \exists m \in \mathbb{N} : \langle \alpha, m\rangle \in X\},$$

对于 $\alpha \in (X)_1$，我们用 $X(\alpha)$ 表示满足 $\langle \alpha, m\rangle \in X$ 的唯一 $m \in \mathbb{N}$。

设 $a, b \in R$和 X, Y分别为不可约分解。我们定义 X 整除 Y，记作 $X \,|\, Y$，如果 $(X)_1 \subset (Y)_1$，并且对于每个 $\alpha \in (X)_1$，都有$X(\alpha) \leq Y$({v24)。容易看出，$a \,|\, b$当且仅当 $X \,|\, Y$。我们重述唯一分解整环的定义。

定义 1.2.8（唯一分解整环 2）若整环 R 是唯一因式分解整环，简称唯一分解整环，则 R^* 中的每个元素都有唯一的不可约分解。

命题 1.2.9 在每个唯一分解整环 R 中，任意两个元素 $a, b \in R^*$ 都有最大公因子 c。若 a 和 b 互素，则 $c = 1_R$。否则，分别用 X 和 Y 表示 a 和 b的不可约分解，我们有

$$[c]_\sim = \prod_{\alpha \in X_1 \cap Y_1} \alpha^{\min(X(\alpha),\, Y(\alpha))} .$$

证明。 </style}这可直接由元素在R^* 中的整除关系用其不可约分解来解释。□

对于满足 $ab = 0_R$的数对 a, b，对每个 $a \in R^*$，都有 gcd$(0_R, a) = a$，而 gcd$(0_R, 0_R)$ 不存在。

我们将 PP0、PP1 和 PP2 推广到唯一分解整环。设 R 是唯一分解整环，$a, b \in R^*$，并设X 和 Y 分别是 a 和 b的不可约分解。那么，a 和 b互素当且仅当 $(X)_1 \cap (Y)_1 = \emptyset$。乘积 ab 的不可约分解为

$$\begin{aligned} XY \;:=\; & \{\langle \alpha,\, X(\alpha)\rangle \colon \alpha \in (X)_1 \setminus (Y)_1\} \cup \{\langle \alpha,\, Y(\alpha)\rangle \colon \alpha \in (Y)_1 \setminus (X)_1\} \cup \\ & \cup \{\langle \alpha,\, X(\alpha) + Y(\alpha)\rangle \colon \alpha \in (X)_1 \cap (Y)_1\} . \end{aligned}$$

如果 a 和 b 互素，那么我们有不交并集 $XY = X \cup Y$。对于 $l \in \mathbb{N}$，幂 a^l 具有不可约分解

$$X^l := \{\langle \alpha,\, lX(\alpha)\rangle \colon \alpha \in (X)_1\} .$$

命题 1.2.10 (PP0′) 设 R 是唯一分解整环，a、b、$c \in R$ 且 $k \in \mathbb{N}$。若 a 整除 bc^k，且 a、c 互素，则 a 整除 b。

证明。 </style}不难验证，当 时该命题成立。我们假设 、 b、 $c \in R^*$，并分别用 X、 Y 和 Z 表示它们的不可约分解。由于 $(X)_1 \cap (Z)_1 = \emptyset$，同样有 $(X)_1 \cap (Z^k)_1 = \emptyset$。由前面对不可约分解层面的整除关系的描述可知，由于 $X \mid YZ^k$，实际上有 $(X)_1 \subset (Y)_1 \setminus (Z)_1$ 和 $X \mid Y$。□

命题 1.2.11（PP1′）设 R 是一个唯一分解整环，且 $k, l \in \mathbb{N}$ 满足 $k, l \geqslant 2$。若对于 $i \in [k]$，$a_i, b \in R$ 是 $k+1$ 元素，使得 a_i 两两互素，并且

$$a_1 a_2 \dots a_k \sim b^l ,$$

那么存在 k 两两互素元素 $b_i \in R$，使得对于每个 $i \in [k]$,

$$a_i \sim (b_i)^l .$$

证明。设 R, k, l, a_i和 b 如题述。若某个 a_i 是 0_R，则每个满足 $j \neq i$ 的a_j 都是单位。因此命题成立，因为 $0_R = (0_R)^l$，且对于每个 $a \in R^\times$，都有 $a \sim (1_R)^l$。所以我们可以略去所有 $a_i \in R^\times$，并假设 $a_i,\ b \in R^* \setminus R^\times$。设 X_i $(\neq \emptyset)$是 a_i的不可约分解， Y $(\neq \emptyset)$是 b的不可约分解。由于

$$X_1 X_2 \dots X_k = X_1 \cup X_2 \cup \dots \cup X_k = Y^l ,$$

对每个 $i \in [k]$，都有 $X_i \subset Y^l$。因此，对每个 $\langle \alpha,\ m \rangle \in X_i$， l 整除 m，从而对某个 $b_i \in R^* \setminus R^{\mathrm{ir}}$，有 $a_i \sim (b_i)^l$。由于 a_i 两两互素， b_i也两两互素。□

我们使用以下记号。若 R 是一个整环，且 A， $B \subset R$ 是两个等势的有限集，则 $A \sim B$ 表示存在一个双射 $f\colon A \to B$，使得对每个 $a \in A$，都有 $a \sim f(a)$。

命题 1.2.12（PP2′）设 R 是唯一分解整环， $p \in R^{\mathrm{ir}}$ 且设 $k \in \mathbb{N}$ 满足 $k \geqslant 2$。若 a、 b、 c 属于 R，并且满足

$$\gcd(a, b) = p \wedge ab \sim c^k ,$$

那么存在互素元素 d、 $e \in R$，使得

$$\{a, b\} \sim \{pd^k, p^{k-1} e^k\} .$$

证明。设 R、 p、 k、 a、 b 和 c 如前所述。若 a 和 b 中有一个是 0_R，则另一个与 p 相伴。由于 $0_R = p^{k-1}(0_R)^k$ 且 $p = p(1_R)^k$，结论成立。因此，我们可以假设 a, b, $c \in R^*$。设 a、 b 和 c 的不可约分解分别为 X、 Y 和 Z。我们可以假设 $\langle [p]_\sim,\ 1 \rangle \in X$、$\langle [p]_\sim,\ m \rangle \in Y$，其中 $m \in \mathbb{N}$，并且 $(X)_1 \cap (Y)_1 = \{[p]_\sim\}$。由于

$$XY = \big(X \setminus \{\langle [p]_\sim, 1 \rangle\}\big) \cup \big(Y \setminus \{\langle [p]_\sim, m \rangle\}\big) \cup \{\langle [p]_\sim, m+1 \rangle\} = Z^k ,$$

我们得到，对于每个 $\alpha \in ((X)_1 \cup (Y)_1) \setminus \{[p]_\sim\}$， k 都整除 $X(\alpha)$ 和 $Y(\alpha)$，且 k 整除 $m+1$。因此，对于某个 $m_0 \in \mathbb{N}_0$，有 $m = k - 1 + km_0$。由此可得 $a \sim pd^k$ 和 $b \sim p^{k-1}e^k$，其中 d， $e \in R^*$ 互素。□

假设 $\mathbb{Z}$ 是唯一分解整环，留给有兴趣的读者作为简单练习：由 PP0′ 推出 PP0，由 PP1′ 推出 PP1，以及由 PP2′ 推出 PP2。

1.3 Klazar 对 $x^2 - y^3 = 1$ 的解

我们遵循文章 [18]。在下一个结果中，我们得到勾股数的著名公式。这些公式反转了多项式恒等式

$$\left(x^2 - y^2\right)^2 + (2xy)^2 = \left(x^2 + y^2\right)^2 \quad (\text{in } \mathbb{Z}[x, y])\,.$$

命题 1.3.1 若 x、 y、 $z \in \mathbb{N}_0$ 是满足以下条件的数

$$x^2 + y^2 = z^2$$

——它们构成一组勾股数——且两两互素，那么它们可表示为某些互素数 u、 $v \in \mathbb{N}_0$ 的形式：

$$z = u^2 + v^2 \ \ and \ \{x, y\} = \{u^2 - v^2, 2uv\}\,.$$

证明。设 x、 y 和 z 如上所述。模 4 化简可知， z 以及 x 和 y中恰有一个为奇数，设为 x。于是，由于（$z - x$）/2 和（$z + x$）/2 互素，根据等式

$$\left(\frac{y}{2}\right)^2 = \frac{z-x}{2} \cdot \frac{z+x}{2}$$

由 PP1（命题 1.2.2），我们得到互素数 u， $v \in \mathbb{N}_0$，使得 $(z - x)/2 = v^2$，$(z + x)/2 = u^2$ 且 $uv = y/2$。因此 $x = u^2 - v^2$、 $y = 2uv$ 和$z = u^2 + v^2$。□

推论 1.3.2 若 x、 $y \in \mathbb{N}_0$ 是满足以下条件的数

$$2x^2 - y^2 = 1\,,$$

则存在数 a、 $b \in \mathbb{N}_0$，使得 $a^2 - 2b^2 = 1$ 且

$$x \in \{a^2 + 2b^2 + 2ab,\, a^2 + 2b^2 - 2ab\} = \{2a^2 - 1 + 2ab,\, 2a^2 - 1 - 2ab\}\,.$$

证明。设 x， y 如上所述。则 y 是奇数， $y = 2y_0 + 1$ 且 $y_0 \in \mathbb{N}_0$。因此 $x^2 = 2y_0^2 + 2y_0 + 1 = y_0^2 + (y_0 + 1)^2$。根据命题 1.3.1，存在 u， $v \in \mathbb{N}_0$，使得

$$x = u^2 + v^2 \ \text{ and } \{y_0, y_0 + 1\} = \{2uv,\, u^2 - v^2\}\,.$$

因此为 $1 = u^2 - v^2 - 2uv = (u - v)^2 - 2v^2$ 或 $1 = 2uv - u^2 + v^2 = (u + v)^2 - 2u^2$。我们分别设 $a = u - v$、 $b = v$ 为 $a = u + v$、 $b = u$，得到 a， $b \in \mathbb{N}_0$ 如所述。□

我们从 Sierpinski 的书中摘录了以下结果 [**?**]。

命题 1.3.3 丢番图方程的唯一解

$$x^4 - 2y^2 = 1$$

是 $\langle \pm 1、\ 0 \rangle$。

证明。设 $x, y \in \mathbb{Z}$ 是该方程的一个解。那么 x 是奇数，且 $x^2 = 1+4k$，其中 $k \in \mathbb{N}_0$。由因式分解可得

$$(x^2 - 1)(x^2 + 1) = 2y^2$$

即 $4k(2k + 1) = y^2$。由于数 $4k$ 和 $2k + 1$ 互素，根据 PP1（命题 1.2.2），我们有 $4k = a^2$、$a \in \mathbb{N}_0$。因此 $(x - a)(x + a) = 1$ 且$x = \pm 1, y = 0$。□

以下辅助结果本身也具有独立的研究价值。

定理 1.3.4 丢番图方程

$$x^4 - 3y^2 = 1$$

只有平凡解 $\langle \pm 1、\ 0 \rangle$。

证明。我们需要求解 $x_n = m^2$，其中 n，$m \in \mathbb{N}_0$ 且 x_n 如命题 1.1.2 中所述。如果 $n = 2n_0 + 1$ 是奇数，则命题 1.1.3 给出

$$(m - y_{n_0} - y_{n_0+1})(m + y_{n_0} + y_{n_0+1}) = 1\,.$$

因此 $m = \pm 1$ 和 $y_{n_0} + y_{n_0+1} = 0$。这是不可能的，因为总有 $y_{n_0} + y_{n_0+1} > 0$。

设 $n = 2n_0$ $x_n = m^2$ $2x_{n_0}^2 - m^2 = 1$ 1 1 3 $2x_{n_0}^2 - 1 = x_{2n_0} = x_{n_0}$ 4 为偶数。根据命题 . . ，以及 . 对其进行模约简可知其为奇数。由命题 1.1.3，$x_{n_0} = x_{2n_1} = 2x_{n_1}^2 - 1$。推论 1.3.2 表明，存在数 a，$b \in \mathbb{N}_0$ 使得 $a^2 - 2b^2 = 1$ 以及

$$2x_{n_1}^2 - 1 = x_{n_0} = 2a^2 - 1 \pm 2ab\,.$$

因此 $x_{n_1}^2 = a(a \pm b)$。由于 a，b 互素，所以 a，$a \pm b$也互素；根据 PP1（命题 1.2.2），数 a 是一个平方数。由命题 1.3.3 可得$a = 1$。因此 $b = 0$、$x_n = x_{n_0} = 1$ 和 $x = \pm 1$，$y = 0$。□

定理 1.3.5（欧拉，1737）丢番图方程的唯一整数解

$$x^2 - y^3 = 1$$

是 $\langle \pm 3、\ 2 \rangle$、$\langle \pm 1、\ 0 \rangle$ 和 $\langle 0、\ -1 \rangle$。

证明。（Klazar）设 $x, y \in \mathbb{Z}$ 满足 $x^2 - y^3 = 1$。那么

$$x^2 = (y+1) \cdot (y^2 - y + 1) = (y+1) \cdot ((y+1)(y-2) + 3) .$$

由于 $y^2 - y + 1 \geq 0$，我们有 $y + 1 \geq 0$。此外，$y+1$，$y^2 - y + 1$ 的最大公因数为 $\in \{1, 3\}$。若最大公因数为 1，根据 PP1（命题 1.2.2），$y+1$ 和 $y^2 - y + 1$ 都是平方数。因此，对于某个 $a \in \mathbb{N}_0$，有 $4y^2 - 4y + 4 = (2a)^2$。我们得到

$$3 = (2a - 2y + 1)(2a + 2y - 1) .$$

因此，$\langle a,\ y \rangle = \langle \pm 1,\ 1 \rangle$ 或 $\langle \pm 1,\ 0 \rangle$。对于 $y = 1$，数 $y + 1$ 不是平方数；而对于 $y = 0$，我们得到解 $\langle \pm 1,\ 0 \rangle$。

设 $y+1$，$y^2 - y + 1$ 的最大公因数为 $= 3$。根据 PP2（命题 1.2.3），存在数 a，$b \in \mathbb{N}_0$，使得

$$y + 1 = 3a^2 \text{ and } y^2 - y + 1 = 3b^2 .$$

因此，对于某个 $Y \in \mathbb{Z}$，$3(2b)^2 - (2y-1)^2 = 3$ 且 $2y - 1 = 3Y$。结合 $X = 2b (\in \mathbb{N}_0)$，我们得到

$$X^2 - 3Y^2 = 1 \text{ and } Y = 2a^2 - 1 .$$

三元组 $\langle X,\ Y,\ a \rangle = \langle 2,\ -1,\ 0 \rangle$ 是这个方程组的解。我们得到 $y = -1$，解为 $\langle 0,\ -1 \rangle$。

因此，我们可以假设 $Y \geq 0$。我们寻找一个数 $n \in \mathbb{N}_0$，使得$Y = y_n = 2a^2 - 1$，其中 $a \in \mathbb{N}_0$，而 y_n 如命题 1.1.2 所述。由于 y_n 是奇数，n也是奇数。根据命题 1.1.3，我们有

$$2a^2 - 1 = y_n = y_{2m+1} = 2x_m y_{m+1} - 1,\ m \in \mathbb{N}_0 .$$

Thus

$$a^2 = x_m y_{m+1} .$$

我们有

$$\gcd(x_m,\, y_{m+1}) = \gcd(x_m,\, x_m + 2y_m) \in \{1,\, 2\} .$$

若最大公因数$(x_m,\ y_{m+1}) = 1$，根据 PP1（命题 1.2.2），数 x_m 是一个平方数。定理 1.3.4 给出 $x_m = 1$。因此，$m = 0$、$n = 1$、$y_n = Y = 1$ 且 $y = 2$。我们得到解 $\langle \pm 3,\ 2 \rangle$。

最后，令 $\gcd(x_m, y_{m+1}) = 2$。根据 PP2（命题 1.2.3），$y_{m+1} = 2c^2$ for some $c \in \mathbb{N}_0$。根据命题 1.1.3,

$$2c^2 = y_{m+1} = y_{2k} = 2x_k y_k,\ k \in \mathbb{N} .$$

因此 $c^2 = x_k y_k$。由于 x_k, y_k 互素，根据 PP1（命题 1.2.2），数 x_k 是一个平方数。定理 1.3.4 表明这是不可能的，因为$k \geq 1$。我们无法得到 $x^2 - y^3 = 1$ 的其他解，证明完毕。□

这是1989年对 $x^2 - y^3 = 1$ 在 [18]中的解。2003年，Ch. Notari 在 [29]中得到了一个类似的解。

1.4 欧拉论证的现代补充

我们给出欧拉在分式域中对方程 $x^2 - y^3 = 1$ 的解的现代版本。我们沿用了（并补全了）Conrad 的写法 [9] 。首先，我们求解一个辅助的丢番图方程。

定理 1.4.1 唯一的三元组 $\langle x, y, z\rangle \in \mathbb{N}^3$ 满足 $(x, y) = 1, (3, x) = 1$并且

$$x^4 - 3x^2y^2 + 3y^4 = z^2\,,$$

是 $\langle 1,1,1\rangle$。等价地说，唯一的互素数 $u, v \in \mathbb{N}$ 满足$(3, u) = 1$，且这三个数

$$u,\ v\ \ and\ \ u^2 - 3uv + 3v^2$$

都是平方数的情形是 $u = v = 1$。

证明。（Conrad）首先，我们证明，在后一个问题中，如果 $v = 1$，那么 $u = 1$。事实上，由于 $u^2 - 3uv + 3v^2$ 是平方数，存在一个 $a \in \mathbb{Z}$ 使得

$$u^2 - 3u + 3 = a^2 \ \text{ and } \ (2a)^2 - (2u - 3)^2 = 3\,.$$

因此 $a = \pm 1$ 和 $u = 1$ 或 2。由于 $u = 2$ 不是平方数，$u = 1$。

因此，我们假设 $u, v \in \mathbb{N}$ 和 $w \in \mathbb{Z}$ 是满足以下条件的数：$(u, v) = 1$，$(3, u) = 1$，u 和 v 都是平方数，

$$u^2 - 3uv + 3v^2 = w^2\,,$$

$v > 1$ 且 v 取可能的最小值（相对于所述性质）。我们得到一个矛盾，并证明这样的三元组 $\langle u, v, w\rangle$ 实际上并不存在。

因此 $(3, w) = 1$，我们可以选择 w 的符号，使得 $w \equiv -u \pmod 3$。令 $r := \frac{w-u}{v} (\in \mathbb{Q})$，于是 $u + rv = w$。根据 w 的选取，我们有 $r \neq 0$。令 $r = \frac{m}{n}$ 为最简分数，于是 $m \in \mathbb{Z}$、$n \in \mathbb{N}$ 且 $(m, n) = 1$。我们看到 $m \mid (w - u)$、$n \mid v$ 且 $(3, m) = 1$。将 $w = u + rv$ 代入前面显示的方程，得到

$$u^2 - 3uv + 3v^2 = u^2 + 2urv + r^2v^2 \ \text{ and } \ (3 - r^2)v^2 = (2r + 3)uv\,.$$

我们可以看到 $2r + 3 \neq 0$。两边除以 $v^2(2r + 3)$，并代入 $r = \frac{m}{n}$，得到

$$\frac{u}{v} = \frac{3n^2 - m^2}{n(2m + 3n)}\,.$$

我们证明右边的分数是最简分数。由（m，n）$= 1$ 可得，n 与 $3n^2 - m^2$互素。为了证明 $3n^2 - m^2$和$2m+3n$ 互素，我们采用反证法。假设素数 p 整除 $3n^2 - m^2$ 和 $2m + 3n$。那么，模 p有 $m^2 \equiv 3n^2$ 和 $2m \equiv -3n$。将第二个同余式平方，并与第一个同余式比较，可得 $4m^2 \equiv 3m^2$ 和

$12n^2 \equiv 9n^2$。因此，p 同时整除 m^2 和 $3n^2$。由于 m 和 n 互素，$p = 3$ 且 p 整除 m，这就产生了矛盾。

Thus

$$u = \varepsilon(3n^2 - m^2) \text{ and } v = \varepsilon n(2m + 3n),\ \varepsilon \in \{-1, 1\}.$$

模 3，$u \equiv -\varepsilon m^2 \equiv -\varepsilon$。由于 u 是平方数，我们得到 $\varepsilon = -1$。因此

$$u = m^2 - 3n^2 \text{ and } v = -n(2m + 3n).$$

由于 u 是平方数，我们有

$$m^2 - 3n^2 = k^2,\ k \in \mathbb{Z}.$$

因此 $(3, k) = 1$，并且我们选择 k 的符号，使得 $k \equiv -m$ 模 3。

令 $s = \frac{k-m}{n} (\in \mathbb{Q})$，使得 $m + sn = k$。由 k的选择可知$s \neq 0$。令 $s = \frac{u'}{v'}$ 为最简分数，使得 $u' \in \mathbb{Z}$、$v' \in \mathbb{N}$ 且 $(u', v') = 1$。我们看到 $u' \mid (k - m)$、$v' \mid n$ 且 $(3, u') = 1$。将 $k = m + sn$ 代入前面显示的方程，得到

$$m^2 - 3n^2 = m^2 + 2mns + s^2n^2 \text{ and } 2mns = -(3 + s^2)n^2.$$

我们知道 $sn \neq 0$。两边除以 sn^2 并代入 $s = \frac{u'}{v'}$，得到

$$\frac{2m}{n} = -\frac{3 + s^2}{s} \text{ and } v = -n^2\Big(\frac{2m}{n} + 3\Big) = n^2 \cdot \frac{(u')^2 - 3u'v' + 3(v')^2}{u'v'}.$$

由于 v 是平方数，两边乘以 $(u'v')^2$，得到

$$u' \cdot v' \cdot \big((u')^2 - 3u'v' + 3(v')^2\big)$$

是平方数。由于 $(u',\ v') = 1$ 且 $(3,\ u') = 1$，所示的三个因子两两互素，由 PP1（命题 1.2.2）可知它们全都是平方数；注意到$v' > 0$ 且 $(u')^2 - 3u'v' + 3(v')^2 > 0$，因此 $u' > 0$也成立。

我们证明 $0 < v' \leq v$。我们有

$$\frac{v}{n} = \frac{n\big((u')^2 - 3u'v' + 3(v')^2\big)}{u'v'}.$$

现在 $n \mid v$，且 u'与 v'互素，并且 $(u')^2 - 3u'v' + 3(v')^2$。因此 $u'v' \mid n$且 $u'v' \mid v$。于是 $0 < u'v' \leq v$ 且 $0 < v' \leq v$。v 的最小性蕴含两种情况：要么 $v' = 1$，要么 $v' = v$。我们证明这两种情况都会导致矛盾，即 $v = 1$。

情形 1，当 $v' = 1$。正如我们一开始所知，$u' = 1$。因此，$s = \frac{u'}{v'} = 1$，$k = m + sn = m + n$, $m^2 - 3n^2 = k^2 = (m + n)^2$ 且 $m = -2n$。所以$r = \frac{m}{n} = -2$ 且 $w = u + rv = u - 2v$。我们得到

$$u^2 - 3uv + 3v^2 = (u - 2v)^2 \text{ and } uv = v^2.$$

因此 $(u-v)v=0$ 且 $u=v$。由于 $(u,v)=1$，我们得到矛盾：$v=1$。

情形 2：当 $v'=v$。因此 $u'=1$。我们有 $s=\frac{k-m}{n}=\frac{u'}{v'}=\frac{1}{n}$。由于 $n\mid u$ 和 $v'\mid n$，可得 $v=v'=n$ 和 $k=m+1$。于是 $m^2-3n^2=k^2=m^2+2m+1$ 和 $2m+1=-3n^2$。但是由

$$n=v=-n(2m+3n)$$

可得 $2m+3n=-1$ 和 $2m+1=-3n$。因此 $-3n^2=-3n$ 和 $n=v=1$，这就构成了矛盾。□

在前一个证明中，我们遵循了 [9],，但修正并补全了证明的结论； [9] 遗漏了情形 1。

由前一个定理，我们可以推出本节的主要结果

定理 1.4.2（欧拉，1737） 方程的有理数解只有 x、$y\in\mathbb{Q}$

$$x^2-y^3=1$$

是数对 $\langle\pm3,2\rangle$, $\langle\pm1,0\rangle$ 和 $\langle0,-1\rangle$。

证明。 (Conrad) 令 $x,y\in\mathbb{Q}$ 满足 $x^2-y^3=1$。由于 $x^2, y^2-y+1=(y-\frac{1}{2})^2+\frac{3}{4}\geq0$，由

$$x^2=y^3+1=(y+1)(y^2-y+1)$$

我们推得 $y\geq-1$。由于 $y=-1$ 给出解 $\langle0,-1\rangle$，因此从现在起假设 $y>-1$。

设 $y=\frac{a}{b}$，其中 $a\in\mathbb{Z}$ 与 $b\in\mathbb{N}$ 互素。由 $y>-1$ 可得 $a+b>0$。由于

$$x^2=y^3+1=\frac{b(a^3+b^3)}{b^4},$$

$b(a^3+b^3)$ 是一个平方数。由 $c=a+b\,(\in\mathbb{N})$，我们写作

$$b(a^3+b^3)=b(a+b)(a^2-ab+b^2)=b\cdot c\cdot(c^2-3bc+3b^2).$$

情形 1，当 $(3,c)=1$. 所示的三个因子两两互素且均为正数。根据 PP1（命题 1.2.2），它们都是平方数。利用定理 1.4.1 可得 $b=c=1$ 和 $a=0$。因此 $y=\frac{a}{b}=0$，从而得到解 $\langle\pm1,0\rangle$。

情况 2，当 $3\mid c$。设 $c=3d$。由 $(b,c)=1$ 可得 $(3,b)=1$ 以及 $(b,d)=1$。于是

$$bc(c^2-3bc+3b^2)=9bd(b^2-3bd+3d^2)$$

是一个平方数。因此

$$b\cdot d\cdot(b^2-3bd+3d^2)$$

是一个平方数。和之前一样，我们利用 PP1（命题 1.2.2）和定理 1.4.1 推得 $b=d=1$。因此，$c=3d=3$、$a=c-b=2$ 和 $y=\frac{a}{b}=2$。我们得到解 $\langle\pm3,2\rangle$。□

1.5 Wakulicz 的解法：$x^3 + y^3 = 2z^3$

Antoni Wakulicz（1902–1988）（[33]）

第2章

V. 勒贝格定理

在第二章中，我们将探讨卡塔兰猜想的第二个初等情形，即奇数指数的方程

$$x^m - y^2 = 1$$

（偶数 m 的情形是一个平凡问题）。第 2.1 节包含关于 p-进阶的结果，我们将在第 2.2 节中用到这些结果；该节将介绍 V. Lebesgue（1791—1875）的定理：该方程的唯一解是 $\langle 1,\ 0\rangle$。关于 V. Lebesgue 的生平，见 [22]。在第 2.3 节中，我们将在定理 2.3.2 中证明，每个欧几里得整环都是唯一分解整环。特别地，$\mathbb{Z}[i]$ 是唯一分解整环，这是 Lebesgue 证明所必需的。该定理在卡塔兰猜想的解中所起的作用，比人们想象的更为重要。借助该定理，我们证明分圆域 $\mathbb{Q}(\zeta_3)$ 和 $\mathbb{Q}(\zeta_5)$ 的类数为 $h_3 = h_5 = 1$；这是第8章中的一个关键结果。在第 2.2 节中，我们遵循 [32, 第 2]。

2.1 p-进赋值的性质

对于素数 p 和 $\alpha \in \mathbb{Q}$，α 的 p-进赋值 $\mathrm{ord}_p(\alpha)$ 在 $\alpha = 0$时为 $+\infty$。对于$\alpha \neq 0$，它是唯一的 $k \in \mathbb{Z}$，使得对于某个 $\beta \in \mathbb{Q}$，有 $\alpha = p^k\beta$，且其分子和分母都与 p互素。

命题 2.1.1 对于每个 $\alpha, \beta \in \mathbb{Q}$，以下结论成立。

1. $\mathrm{ord}_p(\alpha\beta) = \mathrm{ord}_p(\alpha) + \mathrm{ord}_p(\beta)$。这里，对于 $a, b \in \mathbb{Z} \cup \{+\infty\}$，我们定义 $a + b := +\infty$，若 a 或 b 为 $+\infty$。*2.* $\mathrm{ord}_p(\alpha + \beta) \geq \min(\mathrm{ord}_p(\alpha), \mathrm{ord}_p(\beta))$，当 $\mathrm{ord}_p(\alpha) \neq \mathrm{ord}_p(\beta)$ 时取等号。这里，对每个 $m \in \mathbb{Z}$，$+\infty > m$。

证明。1. 如果 α 或 β 为 0，则等式成立，因此我们可以假设$\alpha, \beta \neq 0$。设 $\alpha = p^k\alpha_0$ 和 $\beta = p^l\beta_0$ 是 $\mathbb{Q}^*$ 中的任意两个分数，其中

$k = \mathrm{ord}_p(\alpha)$，$l = \mathrm{ord}_p(\beta)$，且分数 α_0 和 β_0 的分子和分母都与 p互素。那么

$$\alpha\beta = p^{k+l}\alpha_0\beta_0 =: p^{k+l}\gamma$$

其中 $\gamma \in \mathbb{Q}^*$ 分子和分母都与 p 互素。 Thus

$$\mathrm{ord}_p(\alpha\beta) = k + l = \mathrm{ord}_p(\alpha) + \mathrm{ord}_p(\beta)\,.$$

2. 同样，若 α 或 β 为 0，则结论成立。取 α，$\beta \in \mathbb{Q}^*$ 如第 1 项所示，并且不失一般性地假设 $k \le l$。于是

$$k = \min(\mathrm{ord}_p(\alpha), \mathrm{ord}_p(\beta))$$

and

$$\alpha + \beta = p^k(\alpha_0 + p^{l-k}\beta_0) =: p^k\gamma\,.$$

若 $k < l$，则 γ 可写成分子和分母都与 p 互素的分数，因此 $\mathrm{ord}_p(\alpha+\beta) = k$。若 $k = l$，则 γ 可写成分母与 p 互素的分数，由此可得 $\mathrm{ord}_p(\alpha+\beta) \ge k$。□

推论 2.1.2 若 p 是素数，且 α_1、……、α_n 是 $n \ge 2$ 分数，使得

$$\mathrm{ord}_p(\alpha_n) < \mathrm{ord}_p(\alpha_i) \ \textit{for every}\ i \in [n-1]\,,$$

则 $\sum_{j=1}^n \alpha_j \neq 0$。

证明。令 $k := \min(\{\mathrm{ord}_p(\alpha_i)\colon\ i \in [n-1]\})$ $(\in \mathbb{Z} \cup \{+\infty\})$，并令 $\alpha := \sum_{j=1}^{n-1}\alpha_j$。反复应用命题 1 的第 2 项，我们得到 $\mathrm{ord}_p(\alpha) \ge k$。由于 $\mathrm{ord}_p(\alpha_n) < k$，因此 $\mathrm{ord}_p(\alpha_n) < +\infty$ 且

$$\mathrm{ord}_p\big(\textstyle\sum_{j=1}^n \alpha_j\big) = \mathrm{ord}_p(\alpha + \alpha_n) = \mathrm{ord}_p(\alpha_n) < +\infty\,.$$

因此 $\sum_{j=1}^n \alpha_j \neq 0$。 □

2.2 V. 勒贝格对 $x^m - y^2 = 1$ 的解答

我们在整环

$$\mathbb{Z}[i] = \langle \mathbb{Z}[i],\, 0,\, 1,\, +,\, \cdot,\, \rangle\,,$$

其中基集 $\mathbb{Z}[i] = \{a + bi\colon\ a,\ b \in \mathbb{Z}\}$ 是实部和虚部均为整数的复数集合。

定理 2.2.1（V. Lebesgue，1850） 设 $m \ge 3$ 为奇整数。丢番图方程

$$x^m - y^2 = 1$$

只有解 $\langle 1, 0\rangle$。

证明。 (V. Lebesgue) 设 m 如题所述，且 $a, b \in \mathbb{Z}$ 满足 $b \neq 0$，使得 $a^m - b^2 = 1$。我们推出矛盾。若 b 是奇数，则 $a^m \equiv 2$ 模 4，这是不可能的。因此 b 是偶数， $b \neq 0$ 且 a 是奇数。在 $\mathbb{Z}[i]$中，我们考虑因式分解

$$a^m = (1 + bi)(1 - bi)\,.$$

元素 $1 + bi$ 和 $1 - bi$ 互素：若 $\alpha \in \mathbb{Z}[i]$ 同时整除 $1 + bi$和 $1 - bi$，则 $n = \alpha\alpha\ (\in \mathbb{N})$在 $\mathbb{Z}$中整除数 $2 \cdot 2 = 4$ 和奇数 $(1 + bi)(1 - bi) = a^m$。因此 $n = 1$, α 是单位元，且 $1 + bi$ 和$1 - bi$ 互素。由于 $\mathbb{Z}[i]$ 是唯一分解整环（下一节的推论 2.3.3），根据 PP1′（命题 1.2.11），存在元素 $\alpha \in \mathbb{Z}[i]$、单位元 ϵ, $\epsilon' \in \mathbb{Z}[i]^\times$ 以及数 $u, v \in \mathbb{Z}$，使得

$$1 + bi = \epsilon\alpha^m = (\epsilon'\alpha)^m = (u + vi)^m \text{ and } 1 - bi = \overline{\epsilon}(\overline{\alpha})^m = (\overline{\epsilon'\alpha})^m = (u - vi)^m\,,$$

因为 $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$ 中的每个单位元（下一节的命题 2.3.4）都是一个 m 次幂。由于 m 是奇数，我们有

$$2 = (u + vi)^m + (u - vi)^m = 2u \cdot \beta,\ \beta \in \mathbb{Z}[i]\,,$$

并推导出 $u = \pm 1$。我们排除 $u = -1$ 的可能性。由于 $(1 + v^2)^m = (u^2 + v^2)^m = 1 + b^2$ 为奇数，数 v 为偶数。从

$$1 + bi = (u + vi)^m = \textstyle\sum_{j=0}^{m} \binom{m}{j} u^{m-j}(vi)^j \equiv u^m + mu^{m-1}vi \pmod 4$$

（$\mathbb{Z}[i]$ 中的同余）我们推导出 $u^m \equiv 1$ 模 4（$\mathbb{Z}$ 中的同余），从而排除 $u = -1$。

因此， $u + vi = 1 + vi$，其中 v 为偶数且非零（因为 $b \neq 0$）。比较 $1 + bi = (1 + vi)^m$ 中的实部，我们得到 $\mathbb{Z}$ 中的一个恒等式，

$$1 = \textstyle\sum_{j=0}^{(m-1)/2} (-1)^j \binom{m}{2j} v^{2j},\ \text{or}\ -\binom{m}{2}v^2 + \sum_{j=2}^{(m-1)/2} (-1)^j \binom{m}{2j} v^{2j} = 0\,.$$

对于 $m = 3$，最后一个和为空（即为零），且等式不可能成立，因为 $v \neq 0$。对于奇数 $m \geq 5$, 我们利用推论 2.1.2 和素数 $p = 2$ 证明该等式不成立。对于 $j = 2$, 我们令 $A = \binom{m}{2}v^2$ 和 $B_j = \binom{m}{2j} \cdot v^{2j}$， 3，……， $\frac{m-1}{2}$，并证明对于每个 j, $\mathrm{ord}_2(A) < \mathrm{ord}_2(B_j)$。事实上，

$$B_j = A \cdot \tfrac{1}{j(2j-1)} \tbinom{m-2}{2j-2} v^{2j-2} =: A \cdot C_j$$

且 $\mathrm{ord}_2(C_j) \geq 2j - 2 - \lfloor \log_2(j) \rfloor > 0$, 因此根据 $\mathrm{ord}_2(\cdot)$ 的可加性（命题 2.1.1 的第 1 项），我们有 $\mathrm{ord}_2(A) = \mathrm{ord}_2(B_j) - \mathrm{ord}_2(C_j) < \mathrm{ord}_2(B_j)$。由此得到矛盾 □

2.3 欧几里得整环是唯一分解整环

我们先回顾欧几里得整环。良序 $\langle W, \prec \rangle$ 是集合 W 上的线性序 $\prec$，满足每个非空集合 $V \subset W$ 都有最小元素 $m \in V$，即一个满足 $m \preceq x$ 对每个 $x \in V$都成立的元素。最小元素是唯一的。

D定义 2.3.1（欧几里得整环） 一个整环 $main$

$$R = \langle R,\, 0_R,\, 1_R,\, +,\, \cdot \rangle$$

若存在一个良序 $\langle W, \prec \rangle$ 以及一个函数 $f\colon R^* \to W$，使得

$$\forall\, a,\, b \in R,\, b \neq 0_R\, \exists\, c,\, d \in R\, \big(a = b \cdot c + d \wedge (d = 0_R \vee f(d) \prec f(b))\big)\,.$$

注意，最后一个析取是异或。例如，整数整环 $\mathbb{Z}$ 是欧几里得整环：$\langle W,\ \prec \rangle$ 是 $\langle \mathbb{N},\ <\rangle$ 且 $f(n) = |n|$。通常可以利用下面这个经典定理证明一个整环是唯一分解整环。

定理 2.3.2 每个欧几里得整环都是唯一分解整环。

证明。设 R 是一个欧几里得整环，具有良序 $\langle W,\ \prec \rangle$ 以及映射$f\colon R^* \to W$，如定义 2.3.1 所述。

不可约分解的存在性。我们证明每个 $x \in R^* \setminus R^\times$ 都是不可约元的乘积。反设集合

$$A \subset R^* \setminus R^\times$$

中包含的元素都不能写成不可约元的乘积。取 $a \in R^*$ 使得 a 有一个因子 $b \in A$，且值 $f(a)$在 W中所有这类值里是 $\prec$-最小的。因此 $a = bc$，其中 $b \in A$ 且 $c \in R^*$。由于 b 不是不可约元，故 $b = de$，且 $d,\ e \in R^* \setminus R^\times$。但是 $b \in A$，因此 d或 e 属于 A。我们假设 $d \in A$；$e \in A$ 的情形类似。因此 $a = d(ec)$，其中 $d \in A$且 $ec \in R^* \setminus R^\times$（因为 $e \in R^* \setminus R^\times$）。由命题 1.2.4 可知，这意味着$a$ 不整除 d；若用 a除 d 并求余数，则得到

$$d = ag + h \ \text{ where } g \in R,\, h \in R^* \text{ and } f(h) \prec f(a)\,.$$

由于 d整除 a，它也整除 h。因此 $d \in A$且整除 h，并且 $f(h) \prec f(a)$。这与 a的选取矛盾。

贝祖等式。我们证明，若 $a,\ b \in R$ 互素，则存在$c,\ d \in R$ 使得 $ca + db = 1_R$。我们考虑集合

$$I = \{ca + db :\ c,\, d \in R\}\ (\subset R)\,,$$

它是 R 中由元素 $a,\ b$生成的理想。令 $e \in I \setminus \{0_R\}$ 取$\prec$-最小值 $f(e)$。显然，$I \neq \emptyset$。注意，由于不存在 $a = b = 0_R$，所以 $I \neq \{0_R\}$，元素 0_R 不是单位，因此 $0_R,\ 0_R$ 不互素。我们证明 e 整除每个 $x \in I$。事实上，我们可以将任意 $x \in I$ 表示为 $x = ec + d$，其中 $c,\ d \in R$且 $d = 0_R$，或者 $f(d) \prec f(e)$。由于 $d = x - ec \in I$，我们有 $d = 0_R$。因此 e 整除 I 中的每个元素；又因为 $a,\ b \in I$ 互素，所以 $e \in R^\times$。由此可知 $1_R \in I$，存在 $c,\ d \in R$ 使得$1_R = ca + db$。

素数即素因子。我们证明，若 $a, b, c \in R$, $a \,|\, bc$ and $a \in R^{\mathrm{ir}}$，则 $a \,|\, b$或 $a \,|\, c$。设 $a, b, c \in R$，且 a 是不可约元，整除 bc

但不整除 b。那么 a, b 互素，根据第二步，存在 $d, e \in R$ 使得

$$da + eb = 1_R \,.$$

将它乘以 c，得到 $dac + ebc = c$。因此 a 整除 c。

最后，我们证明，在 R 中，每个元素 $a \in R^*$ 都有唯一的不可约分解 X（$\subset \mathbb{I} \times \mathbb{N}$）。这意味着要证明：如果

$$a_1 a_2 \dots a_k \sim b_1 b_2 \dots b_l \,,$$

其中 $a_i,\ b_i \in R^{\mathrm{ir}}$ 和 $k,\ l \in \mathbb{N}$，那么总有 $k = l$，并且总存在一个双射 $f\colon [k] \to [l]$，使得

$$a_i \sim b_{f(i)},\ i \in [k] \,.$$

假设上面所示的等式是一个最短的反例。那么$k,\ l \geq 2$，并且根据上一步，存在某个 $m \in [l]$，使得 $a_k \sim b_m$。约去 a_k 和b_m，得到

$$a_1 a_2 \dots a_{k-1} \sim b_1 b_2 \dots b_{m-1} b_{m+1} \dots b_l \,.$$

现在我们有 $k - 1 = l - 1$ 以及一个映射 $g\colon [k-1] \to [l] \setminus \{m\}$，它具有上述性质。但此时 $k = l$，我们很容易将 g 扩展为 $f\colon [k] \to [l]$，使得 f 具有上述性质。由此得到矛盾，并推断实际上不存在反例。□

推论 2.3.3 整环 $\mathbb{Z}[i]$ 是欧几里得整环，因此是唯一分解整环。

证明。回忆一下，对于 $z = u + vi$（$\in \mathbb{C}$），z 的范数（绝对值）为 $|z| = \sqrt{z \cdot \overline{z}} = \sqrt{u^2 + v^2}$。我们有 $|z \cdot z'| = |z| \cdot |z'|$ 和 $|z + z'| \leq |z| + |z'|$。取良序 $\langle \mathbb{N}, < \rangle$，即自然数上的通常线性序，以及映射

$$f\colon \mathbb{Z}[i]^* \to \mathbb{N},\ f(z) = |z|^2 \,.$$

设 $z, z' \in \mathbb{Z}[i]$ 满足 $z' \neq 0$。我们定义 $\alpha, \beta \in \mathbb{Q}$ 为

$$\frac{z}{z'} = \alpha + \beta i \,.$$

设 $a, b \in \mathbb{Z}$ 满足 $|a - \alpha| \leq \frac{1}{2}$ 且 $|b - \beta| \leq \frac{1}{2}$。令 $w := a + bi$ 和 $w' = z - z' \cdot w$。那么显然有 $z = z' \cdot w + w'$，并且

$$f(w') = |w'|^2 = |z'|^2 \cdot \left| \frac{z}{z'} - w \right|^2 \leq f(z') \Big(\frac{1}{4} + \frac{1}{4} \Big) < f(z') \,.$$

□

命题 2.3.4 $\mathbb{Z}[i]^\times = \{-1, 1, -i, i\}$。

证明。令 $f(z) = |z|^2 \colon \mathbb{Z}[i]^* \to \mathbb{N}$ 为前一个证明中的映射。如果$z = a + bi$, $z' \in \mathbb{Z}[i]$ 满足 $zz' = 1$，那么

$$1 = f(1) = f(z)f(z') = (a^2 + b^2)f(z')$$

以及 $a^2 + b^2 = 1$。因此 $a = \pm 1$, $b = 0$ 或 $a = 0$, $b = \pm 1$，由此得到所述单位元。□

第3章

Chao Ko定理

第三章专门讨论 Catalan 猜想最后一个初等情形，即以下方程的情形

$$x^2 - y^q = 1$$

其中 $q \geq 5$ 是一个素数。1965年，中国数学家 Chao Ko（1910–2002）（[17]）在 [19] 中证明，对于每个 q，唯一的解是 $\langle \pm 1,\ 0\rangle$和 $\langle 0,\ -1\rangle$。Chao Ko的另一项著名数学成果是极值组合学中的 Erd˝os–Ko–Rado 定理 [10, 11]。

第3.1节包含两个辅助引理。在第3.2节中，我们将介绍 E. Z. Chein 关于该方程的一个解法 [7]。本章遵循 [32,第 3]章。

3.1 两个引理

引理 3.1.1 设 q 是一个素数，且 a、$b \in \mathbb{Z}$、$a \neq b$ 互素。那么

$$d := \gcd\left(\tfrac{a^q - b^q}{a-b},\, a-b\right) = \gcd\left(\textstyle\sum_{i=0}^{q-1} a^i b^{q-1-i},\, a-b\right)$$

整除 q。

证明。根据二项式定理，$\frac{a^q-b^q}{a-b} = \frac{(a-b+b)^q-b^q}{a-b}$ 等于

$$\textstyle\sum_{i=1}^{q} \binom{q}{i}(a-b)^{i-1}b^{q-i} = qb^{q-1} + \sum_{i=2}^{q} \binom{q}{i}(a-b)^{i-1}b^{q-i}\,.$$

因此 $d \mid qb^{q-1}$。由于 a，b互素，所以 b，$a-b$与 $(d,\ b) = 1$也互素。根据 PP0（命题 1.2.1），数 d 整除 q。□

引理 3.1.2 设 $q \in \mathbb{N}$，其中 $q \geq 3$ 为奇数，且 x、y 为满足 $x^2 - y^q = 1$ 的非零整数。那么 y 为偶数；必要时将 x 替换为 $-x$，我们便有如下表达式

$$x - 1 = 2^{q-1}a^q \ \ and \ \ x + 1 = 2b^q\,,$$

其中 a、$b \in \mathbb{Z}$ 互素，且 b 为奇数。

证明。在因式分解 $(x-1)(x+1) = y^q$ 中，两个因子互素，或它们的最大公因数为 2。前一种情况下，由 PP1（命题 1.2.2）可得两个相差 2 的 q 次幂。唯一满足条件的幂是 -1 和 1，而 $x = 0$。这不可能，因此我们看到 $\gcd(x-1, x+1) = 2$ 且 y 为偶数。因此 x 为奇数。改变 x的符号后，我们可以假设 $\frac{x+1}{2}$ 为奇数。应用 PP2（命题 1.2.3），即可得到所述表达式。□

3.2 Chein 对 $x^2 - y^q = 1$ 的求解

命题 3.2.1 设 $q \geq 3$ 为素数，x、y 为非零整数，且满足$x^2 - y^q = 1$。则 q 整除 x。

证明。我们不妨假设 $y \in \mathbb{N}$。假设 $\neg(q \mid x)$，从而得到矛盾。由引理 3.1.1，在因式分解中

$$x^2 = (y+1) \cdot \tfrac{y^q-(-1)}{y-(-1)}$$

两个因子的最大公因数整除 q。根据关于 x 的假设，它们因此互素。由 PP1（命题 1.2.2），对于 $u \in \mathbb{N}$，我们有 $y+1 = u^2$。由于 y 是偶数，u 是奇数。由等式

$$x^2 - y \cdot \left(y^{(q-1)/2}\right)^2 = 1 \text{ and } u^2 - y \cdot 1^2 = 1$$

我们看到，$\langle x,\ y^{(q-1)/2}\rangle$ 和 $\langle u,\ 1\rangle$ 是佩尔方程的两个解

$$X^2 - yY^2 = 1\,.$$

（由于 $y = u^2 - 1 \geq 3$ 且不是平方数，这确实是一个佩尔方程。）显然，$\langle u, 1\rangle \in \mathbb{N}^2$ 是最小解。由命题 1.1.1，存在一个 $m \in \mathbb{N}$，使得在整环 $\mathbb{Z}[\sqrt{y}]$ 中有等式

$$x + y^{(q-1)/2}\sqrt{y} = \left(u + \sqrt{y}\right)^m\,.$$

因此在 $\mathbb{Z}[\sqrt{y}]$ 中，我们有同余关系

$$x \equiv u^m + mu^{m-1}\sqrt{y} \pmod{y}\,.$$

因此，在 $\mathbb{Z}$ 中，数 y 整除 mu^{m-1}。但是 y 是偶数，而 u 是奇数，所以 m 是偶数。因此在 $\mathbb{Z}[\sqrt{y}]$ 中，我们有等式

$$x + y^{(q-1)/2}\sqrt{y} = \left(u^2 + y + 2u\sqrt{y}\right)^{m/2}\,,$$

由此得到同余式 $x + y^{(q-1)/2}\sqrt{y} \equiv y^{m/2}$（模 u）。因此，在 $\mathbb{Z}$中，数 u整除 $y^{(q-1)/2}$。但是 $y+1 = u^2$，所以 y, u互素，且 $u = \pm 1$。因此 $y = 0$，这与假设矛盾。□

命题 3.2.2 设 $q \geq 3$ 为素数， x、 y 为非零整数，且满足$x^2 - y^q = 1$。则 $x \equiv \pm 3 \pmod{q}$。

证明。设 q、 x 和 y 如所述。必要时改变 x 的符号，根据引理 3.1.2，我们有互素的 a， $b \in \mathbb{Z}$，其中 b为奇数，且满足 $x - 1 = 2^{q-1}a^q$和$x + 1 = 2b^q$。因此

$$b^{2q} - (2a)^q = \left(\frac{x+1}{2}\right)^2 - 2(x-1) = \left(\frac{x-3}{2}\right)^2$$

and

$$(b^2 - 2a) \cdot \left(\frac{b^{2q} - (2a)^q}{b^2 - 2a}\right) = \left(\frac{x-3}{2}\right)^2 .$$

数 $2a$， b^2 互素，根据引理 3.1.1，最后两个因子的最大公因数整除 q。

如果是 q，那么 $x \equiv 3$ （mod q），而对于原来的 x，在可能改变符号之前，我们有 $x \equiv \pm 3$ （mod q）。反设最大公因数为 1。因此我们假设 $b^2 - 2a$ 和 $b^{2q} - (2a)^q$ 是互素数。由$b^{2q} - (2a)^q \geq 0$ （这是一个平方数），我们得到 $b^2 - 2a \geq 0$ （f（X） $= X^q$是一个递增函数），根据 PP1（命题 1.2.2），存在一个 $c \in \mathbb{N}$ 使得 $b^2 - 2a = c^2$。由于 $y \neq 0$，也有 $a \neq 0$ 和 $c^2 \neq b^2$。与 b^2 不同的最近平方数是 $(b \pm 1)^2$。因此 $2|a| = |b^2 - c^2| \geq 2|b| - 1$，从而 $|a| \geq |b|$。另一方面，

$$|a|^q = \frac{|x-1|}{2^{q-1}} \leq \frac{|x-1|}{16} < \frac{|x+1|}{2} = |b|^q .$$

对于 $x \in \mathbb{Z}$，关键的不等式 $|x - 1| < 8|x + 1|$ 仅在$x = -1$时不成立。根据 $y \neq 0$， x 的这个取值不可能。因此 $|a| < |b|$也成立，于是我们得到矛盾。□

定理 3.2.3（Chao Ko，1965年）设 $q \geq 5$ 为素数。丢番图方程

$$x^2 - y^q = 1$$

只有以下解： $\langle \pm 1, 0 \rangle$ 和 $\langle 0, -1 \rangle$。

证明。(Chein) 假设 q 如所述，且 x， $y \in \mathbb{Z}^*$ 满足 $x^2 - y^q = 1$。根据命题 3.2.1，我们有 $x \equiv 0$ (模 q)。此外，根据命题 3.2.2， $x \equiv \pm 3$ (模 q)。对于 $q > 3$，这些同余式互相矛盾。□

第4章

卡塞尔的两个关系

在第4.2节和第4.3节中，我们推导出方程的假设非零解 x， $y \in \mathbb{Z}^*$ 所满足的两个整除关系

$$x^p - y^q = 1\,,$$

其中 $p > q > 2$ 是素数： q 整除 x ，且 p 整除 y。由于我们最终将证明不存在这样的数 x和 y ，因此这些是关于不存在对象的性质。这些关系在 Mihˇailescu 的证明中十分重要，分别由英国数学家 John W. S. Cassels（1922—2015）于 [3]和 [4], 提出（[2]）。第4.1节包含辅助结果。在第4.4节中，我们将得到这两个关系的推论。本章遵循 [32, 第 6]章。

4.1 五个引理

引理 4.1.1 对于 $u \in \mathbb{R}$ ，以下结论成立。

1. 若 $u \geq 1$ ，则函数

$$f(x) = \big(u^x + 1\big)^{1/x} \colon (0,\, +\infty) \to (0,\, +\infty)$$

递减。

2. 如果 $u > 1$ ，那么函数

$$f(x) = \big(u^x - 1\big)^{1/x} \colon (0,\, +\infty) \to (0,\, +\infty)$$

递增。

证明。 1. 我们有

$$f'(x) = f(x)\Big(\frac{u^x \log u}{x(u^x+1)} - \frac{\log(u^x+1)}{x^2}\Big)$$

并且（$\cdots$） < 0 因为 $xu^x \log\, u = u^x \log(u^x) <$ （$u^x + 1$） $\log(u^x + 1)$ 。

2. 同理,

$$f'(x) = f(x)\Big(\frac{u^x \log u}{x(u^x-1)} - \frac{\log(u^x-1)}{x^2}\Big)$$

且 $(\cdots) > 0$ 因为 $xu^x \log u = u^x \log(u^x) > (u^x-1)\log(u^x-1)$。 □

定义 4.1.2 ($F_{m,\,n}(X)$) 设 m、$n \in \mathbb{N}$，且 n 为奇数。我们定义函数

$$F_{m,n}(X) = \big((1+X)^m - X^m\big)^{1/n} \colon \mathbb{R} \to \mathbb{R}\,.$$

引理 4.1.3 设 l、m、$n \in \mathbb{N}$ 和 $l < m$。则

$$F_{m,\,n}(X) = \sum_{j=0}^{l} \binom{m/n}{j} X^j + o(X^l) \quad (X \to 0)\,.$$

证明。

□

引理 4.1.4 设 $a \in \mathbb{Z}$、m、$d \in \mathbb{N}$、p 为满足 $(p,\ d) = 1$ 的素数，并设

$$P_m(a,\,d) := \prod_{j=0}^{m-1} (a + jd)\,.$$

Then

$$\operatorname{ord}_p\big(P_m(a,\,d)\big) = \sum_{j\geq 1} \Big(\Big\lfloor \frac{m}{p^j} \Big\rfloor + \varepsilon_j \Big),\ \varepsilon_j \in \{0,\,1\}\,.$$

如果 $P_m(a,\ d) = m!$ 那么对每个 j，都有 $\varepsilon_j = 0$。

证明。设 a、m、d 和 p 如所述。对于 $j \in \mathbb{N}$，令 $m_j\,(\in \mathbb{N}_0)$ 表示 $a + id$、$i = 0,\ 1,\ \ldots\ldots,\ m-1$ 中 p^j 的倍数的个数。由双重计数论证可得

$$\operatorname{ord}_p\big(P_m(a,\,d)\big) = \sum_{j\geq 1} m_j\,.$$

如果整数 i 和 i' 模 p^j不同余，那么 $a + id$ 和 $a + i'd$也不同余。因此，如果 $I \subset \{0, 1, \ldots, m-1\}$ 是长度为 $|I| \leq p^j$的区间，那么至多有一个 $i \in I$ 使数 $a + id$ 能被 p^j整除；而如果 $|I| = p^j$，则恰好有一个这样的数。因此

$$m_j = \Big\lfloor \frac{m}{p^j} \Big\rfloor + \varepsilon_j$$

其中 ε_j 等于 0 或 1，因为我们有如下划分

$$\{0,1,\dots,m-1\} = I_1 \cup I_2 \cup \cdots \cup I_k \cup I_0$$

分成区间 $I_1 < I_2 < \cdots < I_k < I_0$，使得 $k = \lfloor m/p^j \rfloor$、$|I_i| = p^j$，对于 $i > 0$ 和 $|I_0| < p^j$。这证明了第一个断言。□

引理 4.1.5 设 q 为素数，$a \in \mathbb{Z}$ 满足 $(q,a) = 1$ 且 $k \in \mathbb{N}_0$。那么存在 $b \in \mathbb{Z}$，满足 $(q,b) = 1$，使得

$$\binom{a/q}{k} = \frac{b}{q^{k+\mathrm{ord}_q(k!)}}\,.$$

4.2 关系 $q \mid x$

以下定理由 Cassels 于 [3]证明。我们遵循 [32, 第 6] 章。

定理 4.2.1（Cassels，1953 年）若 $p > q > 2$ 是素数，且 x、$y \in \mathbb{Z}^*$ 是满足以下条件的数

$$x^p - y^q = 1\,,$$

那么 q 整除 x。

证明。假设 p、q、x 和 y 如所述，且 $(q,x) = 1$。那么根据引理 3.1.1，这两个因子

$$(y+1)\cdot\frac{y^q+1}{y+1} = x^p$$

互素。根据 PP1（命题 1.2.2），我们有 $y+1 = b^p$，其中某个 $b \in \mathbb{Z}$。由于 $x \neq 0$，也有 $b \neq 0$。因此

$$x^p - (b^p-1)^q = 1\,.$$

我们证明这个等式不可能成立。

对于 $X \in \mathbb{R}$，我们考虑函数

$$g(X) = X^p - (b^p-1)^q$$

并证明对于每个 $X \in \mathbb{Z}$，都有 $g(X) \neq 1$。设 $b > 0$。由于 $y \neq 0$，我们有 $b \geq 2$。于是

$$g(b^q) = \sum_{j=0}^{q-1} b^{jp}(b^p-1)^{q-1-j} \geq q > 1$$

and

$$g(b^q-1) = (b^q-1)^p - (b^p-1)^q < 0\,,$$

因为，由于 $q<p$，根据引理 4.1.1 的第 2 项，我们有

$$\left((b^q-1)^p\right)^{\frac{1}{pq}}=(b^q-1)^{\frac{1}{q}}<(b^p-1)^{\frac{1}{p}}=\left((b^p-1)^q\right)^{\frac{1}{pq}}.$$

函数 $g(X)$ 在 $\mathbb{R}$ 上递增，因此我们看到，不存在满足 $g(X)=1$ 的 $X\in\mathbb{Z}$。

假设 $b<0$，于是 $b\le -1$。那么，同理，

$$g(b^q)=\sum_{j=0}^{q-1}(b^p)^j(b^p-1)^{q-1-j}\ge q>1$$

（每一项的符号均为 $(-1)^{q-1}=1$），并且

$$g(b^q-1)=-((-b)^q+1)^p+((-b)^p+1)^q<0\,,$$

因为，既然 $q<p$，由引理 4.1.1 的第 1 项可知

$$\left(((-b)^q+1)^p\right)^{\frac{1}{pq}}=((-b)^q+1)^{\frac{1}{q}}>((-b)^p+1)^{\frac{1}{p}}=\left(((-b)^p+1)^q\right)^{\frac{1}{pq}}.$$

同样，$g(X)$ 在 $\mathbb{R}$ 上递增，因此我们看到，不存在满足 $g(X)=1$ 的 $X\in\mathbb{Z}$。这就得到了一个矛盾，并且可知 q 整除 x。□

4.3 关系 $p\,|\,y$

下述定理由 Cassels 于 [4]证明。我们遵循 [32, 第 6]章。

定理 4.3.1（Cassels，1960）若 $p>q>2$ 是素数，且 x、$y\in\mathbb{Z}^*$ 是满足下述条件的数

$$x^p-y^q=1\,,$$

则 p 整除 y。

证明。设 p、q、x 和 y 如上所述，并设 $(p,y)=1$。由引理 3.1.1，以下两个因子

$$(x-1)\cdot\frac{x^p-1}{x-1}=y^q$$

互素。由此我们得到一个矛盾。根据 PP1（命题 1.2.2），$x-1=a^q$ 与 $a\in\mathbb{Z}$。显然 $a\neq 0$。因此，$y^q=(a^q+1)^p-1$，并按照定义 4.1.2 中的 $F_{p,q}(X)$，将 y 表示为

$$y=a^p\cdot F_{p,q}(1/a^q)\,.$$

我们设 $m=\lfloor p/q\rfloor+1\,(\ge 2)$，$D=q^{m+\mathrm{ord}_q(m!)}$ 并且

$$z=a^{mq-p}y-a^{mq}\cdot T_0^m(F_{p,q})(1/a^q)\ \ (\in\mathbb{Q})\,.$$

利用引理 4.1.3 和 4.1.5 以及不等式 $mq-p\geq 0$ （由$m>\frac{p}{q}$ 可得），我们得到 –

$$Dz = Da^{mq-p}y - \sum_{k=0}^{m} D\tbinom{p/q}{k} a^{mq-qk} \in \mathbb{Z}\,.$$

我们通过证明整数 $Dz\neq 0$，但同时 $|Dz|<1$，得出一个矛盾。Dz 的非零性源于不可整除性¬($q\,|\,Dz$)：在 Dz 的展开式中，除了含有 $k=m$ 的项之外，所有项都能被 q 整除；根据引理 4.1.5，该项是整数 $D\binom{p/q}{m}$，不能被 q 整除。

我们证明 $|Dz|<1$。我们有 $z=a^{mq}\big(F_{p.q}(1/a^q)-T_0^m(F_{p.q})(1/a^q)\big)$。由于 $x\neq 0$，但根据定理 4.2.1，$q\,|\,x$ $a\neq 0$，± 1 且 $|a|\geq 2$。我们可以对 $X=1/a^q$ 使用引理 **??**，并得到界

$$|z| \leq \frac{|a|^{mq}\cdot|a|^{-(m+1)q}}{(1-|a|^{-q})^2} = \frac{|a|^q}{(|a|^q-1)^2} \leq \frac{1}{|a|^q-2} \leq \frac{1}{|x|-3}\,.$$

根据命题 **??**，$|x|\geq q^{p-1}+q$。因此

$$|Dz| \leq q^{m+\mathrm{ord}_q(m!)-(p-1)}\,.$$

如果指数为负数，我们就完成了。事实上，根据引理 **??**，不等式 $m<\frac{p}{q}+1$，且由于 $p\geq 5$ 和 $q\geq 3$，它为负数：

$$\begin{aligned} m+\mathrm{ord}_q(m!)-(p-1) &\leq m\big(1+\tfrac{1}{q-1}\big)-(p-1)\\ &< \big(\tfrac{p}{q}+1\big)\big(1+\tfrac{1}{q-1}\big)-(p-1)\\ &= \tfrac{3-(p-2)(q-2)}{q-1}\leq 0\,. \end{aligned}$$

□

4.4 推论

第5章

Mih˘ailescu 定理：证明概要

5.1 定理 M0.95–M4

Catalan 猜想断言，对于整数 $m, n \geq 2$，丢番图方程的唯一非零解$x, y \in \mathbb{Z}^*$ 为

$$x^m - y^n = 1$$

当 $m = 2$ 和 $n = 3$ 取 $\langle x、\ y\rangle = \langle \pm 3、\ 2\rangle$ 时出现。在前三章中，我们描述了在 $m = 2$ 或 $n = 2$ 的情况下如何解出这一猜想。显然，要证明整个猜想，还需要证明：对于任意两个不同的奇素数 p 和 q，丢番图方程

$$x^p - y^q = 1$$

没有非零解。P. Mih˘ailescu 于 2004年完成了这一证明，本章将概述他的解法。我们还将介绍本书其余各章的内容。回想一下，如果 $x、\ y \in \mathbb{Z}$ 和 $m、\ n \in \mathbb{N}$ 是奇数，那么

$$x^m - y^n = 1 \iff (-y)^n - (-x)^m = 1\,,$$

因此，如有需要，我们可以假设 $p > q$。

在本章的第一部分，我们沿用 [32, 第 1], 章的内容，但对定理 M1–M4 中的假设作了更精确、清晰的说明。这样做很有帮助，因为与 [32, 第 5]页给出的论证相比，我们可以简化从这四个定理推导定理 5.1.1 的过程。

定理 5.1.1（米哈伊莱斯库˘，2004年）若 p 和 q 是不同的奇素数，则丢番图方程

$$x^p - y^q = 1$$

没有非零解 $x, y \in \mathbb{Z}^*$。

定理 5.1.1、1.3.5（或 1.4.2）、2.2.1 和 3.2.3 共同证明了 Catalan 猜想。

定理 5.1.1 可由接下来的四个定理 M1–M4 推出，这些定理均归功于 P. Mih˘ailescu。

定理 5.1.2 (M1, [24]) 若 $p > q > 2$ 是素数，且对于某些数 x、$y \in \mathbb{Z}^*$，有 $x^p - y^q = 1$，则

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

这些同余式很容易从实际的定理推出，我们将其称为 M0.95 定理。

定理 5.1.3 (M0.95, [24]) 若 $p > q > 2$ 是素数，且对于某些数 x、$y \in \mathbb{Z}^*$，有 $x^p - y^q = 1$，则

$$p^2 \mid y \ \ and \ \ q^2 \mid x.$$

定理 5.1.4 (M2, [25]) 若 p、$q \geq 7$ 是互异素数，且对于某些数 x、$y \in \mathbb{Z}^*$，有 $x^p - y^q = 1$，则

$$p \equiv 1 \pmod{q} \ \ or \ \ q \equiv 1 \pmod{p}.$$

这是 M1–M4 中最难证明的定理。 [25] 中的原始定理对素数 3 和 5 也成立，但当前这个略加限制的版本证明起来更简单，且足以证明定理 5.1.1。

定理 5.1.5（M3, [26]） 若 p、$q \geq 7$ 是互异素数，且 $x^p - y^q = 1$ 对某些数 x、$y \in \mathbb{Z}^*$ 成立，则

$$p < 4q^2 \ \ and \ \ q < 4p^2.$$

同样， [26] 中的原定理对素数 3 和 5 也成立。

定理 5.1.6（M4, [26]） 若 p 和 q 是互异奇素数，且 $p \in \{3, 5\}$ 或 $q \in \{3, 5\}$，则丢番图方程

$$x^p - y^q = 1$$

没有非零解 x、$y \in \mathbb{Z}^*$。

在 $[26, 32]$ 中，该定理对更大的素数集合 $\{3, 5, 7, 11, \ldots, 41\}$ 得到了证明，但这个受限版本已足以满足我们的需要。

要从定理 M1–M4 推出定理 5.1.1，我们需要一个简单的引理。

引理 5.1.7 设 q 是素数， $x \in \mathbb{Z}$, $x \equiv 1$ (模 q) 且 $x^{q-1} \equiv 1$ (模 q^2)。则 $x \equiv 1$ (模 q^2)。

证明。 我们有 $x = 1 + kq$，其中 $k \in \mathbb{Z}$。由 om

$$x^{q-1} = (1 + kq)^{q-1} = 1 + \sum_{j=1}^{q-1} \binom{q-1}{j} (kq)^j \equiv 1 \pmod{q^2}$$

我们推得 $q^2 \mid (q-1)kq$。因此， $q \mid k$，如前所述。 □

由定理 M1–M4 推导定理 5.1.1。 根据定理 M4（定理 5.1.6），我们可以假设 p, $q \geq 7$ 是互异素数，且$x^p - y^q = 1$ 对某些非零整数 x 和 y成立。由此推出矛盾。根据定理 M1（定理 5.1.2）、定理 M2（定理 5.1.4）、引理 5.1.7 以及对称性，我们有 $p = 1+kq^2$，其中 $k \in \mathbb{N}$。根据定理 M3（定理 5.1.5），$k \in \{1, 2, 3\}$。由于 $k = 1$和 3 会导致一个偶数，因此排除这两个值。于是 $p = 1 + 2q^2$。由于 $q \neq 3$ 会导致一个被 3 整除的 p，因此排除这些值。剩下唯一的一对 $\langle p, q\rangle = \langle 19, 3\rangle$。根据假设 $p, q \geq 7$（即根据定理 5.1.6），可以排除这一对。□

5.2 第 6–A 章概述

第6章

一个障碍群

6.1 数域

如果一个域 L 是另一个域 K 的扩张，记作 L/K，那么 K 的基集是 L 的基集的子集，两个域共享单位元，也就是说， $0_K = 0_L$ 和 $1_K = 1_L$，并且 L 中的加法和乘法扩张了 K 中的这些运算。在这种情况下， L 是一个 K- 向量空间。我们将其维数记为$[L : K]$。

定义 6.1.1（数域）若域扩张 K 的分式域$\mathbb{Q}_{\text{fi}}$ 具有有限维数 $d := [K : \mathbb{Q}_{\text{fi}}]$ *(*$\in \mathbb{N}$*)*，则称其为数域（次数为 d）。

设 K是一个次数为 d的数域，并设 $\alpha \in K$。那么， $d+1$幂1_K、 α、 α^2、<style id="8">.....、 α^d 在 $\mathbb{Q}$上是线性相关的，并且 α 是 $\mathbb{Q}[x]$ 中的一个非零多项式的根，其次数至多为 d。

定义 6.1.2（整数环）设 K 是一个数域。我们定义子集

$$\mathcal{O}_K = \{\alpha \in K \colon\ p(\alpha) = 0_K \ \textit{for a monic polynomial}\ p(x) \in \mathbb{Z}[x]\}\,.$$

我们称 $\mathcal{O}_K$ 为 K的整数环（的基集）。

命题 6.1.3 集合 $\mathcal{O}_K$ 包含单位元 0_K 和 1_K，并且在 K中对加法和乘法封闭。它是 K的子整环。

证明。

□

命题 6.1.4 对于每个数域 K ， 其整数环是唯一分解整环 当且仅当类数为 $h_K = 1$。

证明。

□

6.2 分圆域

命题 6.2.1 对于每个素数 p ，分圆域 $\mathbb{Q}$的整数环$(\zeta_p)_{\mathrm{fi}}$ 等于 $\mathbb{Z}[\zeta_p]_{\mathrm{do}}$。

证明。

□

定理 6.2.2 这些整环

$$\mathbb{Z}[\zeta_3]_{\mathrm{do}} \ \ and \ \ \mathbb{Z}[\zeta_5]_{\mathrm{do}}$$

是欧几里得整环。鉴于命题 *6.1.4* 和 *6.2.1*，以及定理 *2.3.2*，分圆域 $\mathbb{Q}$（ζ_3）$_{\mathrm{fi}}$ 和 $\mathbb{Q}$（ζ_5）$_{\mathrm{fi}}$ 的类数为

$$h_3 = h_5 = 1\,.$$

证明。

□

6.3 障碍群

第7章

超 Cassels 关系

7.1 斯蒂克尔贝格理想

7.2 定理M0.95 和M1

第8章

定理 M4

定理8.0.1 (M4) 若 p 和 q 是不同的奇素数，且 $p \in \{3,5\}$ 或$q \in \{3,5\}$，则丢番图方程

$$x^p - y^q = 1$$

没有非零解 $x, y \in \mathbb{Z}^*$。

证明。

□

附录 A

数学分析中的结果

A.1 泰勒级数

定理 A.1.1（关于泰勒多项式）设 $n \in \mathbb{N}$，$I \subset \mathbb{R}$ 是一个开区间，$a \in I$ 且 $f\colon I \to \mathbb{R}$ 是一个具有 n 阶导数的函数

$$f', f'', \ldots, f^{(n)}\colon I \to \mathbb{R}\,.$$

那么这个（泰勒）多项式

$$T_f^{n,\,a}(x) := \sum_{j=0}^{n} \frac{f^{(j)}(a)}{j!}(x-a)^j$$

是一个次数至多为 $P \in \mathbb{R}[x]$ 且具有如下性质的唯一多项式：

$$f(x) = P(x) + o((x-a)^n) \quad (x \to a)\,.$$

证明。

□

附录 B

代数中的结果

B.1 交换群环

我们所说的群，是指交换群，并采用乘法记号书写。

$$G = \langle G, 1_G, \cdot \rangle$$

这里的环指交换含幺环

$$R = \langle R, 0_R, 1_R, +, \cdot \rangle .$$

定义 B.1.1（群环）设 R 是一个环，G 是一个群。由 R 和 G 生成的群环 $R[G]$ 是如下代数结构：

$$R[G] = \langle S, 0_S, 1_S, +, \cdot \rangle ,$$

其基集、单位元和运算定义如下。S 是映射 $F\colon\ G \to R$ 的集合，其中只有有限多个 $g \in G$ 满足 $F(g) \neq 0_R$。0_S 是满足对每个 $g \in G$ 都有 $0_S(g) = 0_R$ 的零映射。1_S 是满足对每个 $g \in G \setminus \{1_G\}$ 都有 $1_S(1_G) = 1_R$ 且 $1_S(g) = 0_R$ 的映射。加法按分量定义为

$$(F + F')(g) = F(g) + F'(g),\ g \in G .$$

最后，乘法由卷积定义

$$(F \cdot F')(g) = \sum_{\substack{e,\, f \in G \\ e \cdot f = g}} F(e) \cdot F'(f),\ g \in G ,$$

其中，可能的无限和定义为 R 中有限多个不等于 0_R 的项之和。

定理 B.1。2 $R[G]$ 是一个交换含幺环。

证明。

□

参考文献

[1] Yu. Bilu、Y. Bugeaud 和 M. Mignotte，《卡塔兰问题》，施普林格，沙姆，2014 年[2] J. W. S. Cassels，维基百科词条，https://en.wikipedia.org/wiki/ J._W._S._Cassels[3] J. W. S. Cassels，关于方程 $a^x - b^y = 1$，《美国数学杂志》75（1953 年），159–162[4] J. W. S. Cassels，关于方程 $a^x - b^y = 1$。II，《剑桥哲学学会会刊》56（1960），97–103；勘误：同上，57（1961），187[5] E. Catalan，问题 48，《新数学年刊》1（1842年），520[6] E. Catalan，摘自一封致编辑的信，《纯粹与应用数学杂志》27（1844），192[7] E. Z. Chein，关于方程 $x^2 = y^q + 1$ 的一则注记，《美国数学学会会刊》56（1976），83–84[8] H. Cohen，《数论。第一卷：工具与丢番图方程》，施普林格，纽约，2007[9] B. Conrad，欧拉下降法的一个例子，5 页，https://kconrad.math.uconn.edu/blurbs/ugradnumthy/descentbyeuler.pdf（访问于2025年12月4日）[10] P. Erd˝os、Chao Ko 和 R. Rado，有限集系统的交定理，《牛津数学季刊》，第2辑，12（1961），313–320[11]Erd˝os–Ko–Rado 定理，维基百科词条，https://en.wikipedia. org/wiki/Erd%C5%91s%E2%80%93Ko%E2%80%93Rado_定理[12]欧几里得整环，维基百科词条，https://en.wikipedia.org/ wiki/Euclidean_整环[13] Eug`ene Charles Catalan，维基百科词条，https://en.wikipedia.org/ wiki/Eug%C3%A8ne_Charles_Catalan

[14] 莱昂哈德·欧拉，维基百科词条，https://en.wikipedia.org/wiki/Leonhard_Euler[15]L. Euler，《某些算术定理的证明》，《彼得堡科学院通讯》10（1738），125–146[16] G. H. Hardy 和 E. M. Wright，《数论导引》第四版，牛津克拉伦登出版社，牛津，1960[17] 赵可，维基百科词条，https://en.wikipedia.org/wiki/Ke_Zhao[18] M. 克拉扎尔，《关于丢番图方程 $´ ´$ 的求解》，《数学视野》32（1989），47–53（求解丢番图方程 $x^2 - y^3 = \pm 1$）[19] Chao Ko，《关于丢番图方程 $x^2 = y^n + 1$、$xy \neq 0$》，《中国科学》14（1965），457–460[20] S. 兰，《代数》，修订第三版，施普林格出版社，纽约，2002[21] V. Lebesgue，《关于整数范围内方程 $x^m = y^2 + 1$ 不可能成立》，《新数学年刊》8（1850），178–181[22]Victor Am´ed´ee Lebesgue，Mac Tutor数学史档案词条，https://mathshistory.st-andrews.ac.uk/Biographies/Lebesgue_Victor/[23] T. Mets¨ankyl¨a，《卡塔兰猜想：另一个得到解决的古老丢番图问题》，《美国数学会通报》41（2003），43–57[24]P. Mih˘ailescu，《卡塔兰猜想的一个无需类数的判据》，《数论杂志》99（2003），225–231[25] P. Mih˘ailescu，《基本圆分单位与卡塔兰猜想的证明》，《纯粹与应用数学杂志》572（2004），167–195[26] P. Mih˘ailescu，《存在卡塔兰方程解时圆分扩˘张的类群》，《数论杂志》118（2006），123–144[27] L. J. 莫德尔，《丢番图方程》，学术出版社，伦敦和纽约，1969[28] T. 纳格尔，《关于不定方程 $z^p + 1 = y^2$ 不可能成立》，《挪威数学学会文集》4（1921），14页[29] Ch. Notari，《丢番图方程 $x^3 = y^2 - 1$ 的一个初等解法》，《数学展示》21（2003），279–283[30] P. Ribenboim，《卡塔兰猜想：8和9是仅有的一对连续幂吗？》，学术出版社，波士顿，马萨诸塞州，1994[31] K. 罗杰斯，《欧几里得整环公理》，《美国数学月刊》78（1971），1127–1128

[32] R. Schoof，卡塔兰猜想，Springer-Verlag London, Ltd.，伦敦，2008

[33] Antoni Wakulicz，维基百科条目，https://pl.wikipedia.org/wiki/Antoni_Wakulicz（波兰语）

[34] A. Wakulicz，关于方程 $x^3 + y^3 = 2z^3$，《数学杂志》**5**（1957），11–15

[35] A. Weil，《数论：历史视角——从汉谟拉比到勒让德》，Birhkh¨auser，波士顿 1984