高等代数 — 引言

张彪

天津师范大学

数学科学学院

zhang@tjnu.edu.cn

提纲

提纲

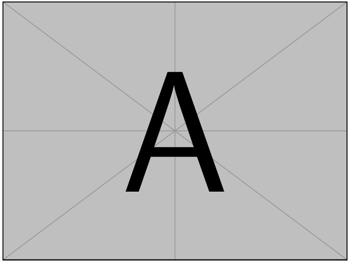
AI 是怎么认出你的？

1. 你拍一张自拍照，电脑看到的不是人脸，而是一张由许多数字组成的“像素表格”.
2. AI 把这些数字放进“数学滤镜”里处理：

$$\text{新图像} = W \times \text{原图像} + b$$

这一步就像用滤镜提取边缘、亮度等特征.

3. 一层层滤镜叠加，AI 就能看出：“这张照片是不是你！”



（原始图像 → 提取特征示意）

关键想法

每一层都在做： **矩阵** × **向量** → **新特征**

这就是 AI 看图、识人的数学基础.

神经网络：一层层的“数学滤镜”

输入：图像数字 → 第 1 层：找出边缘 → 第 2 层：看出眼睛鼻子 → 输出：“是张三！”

- 每一层像一道“滤镜”，从数字中发现更多细节.
- 背后的数学公式：　$\mathbf{y} = W\mathbf{x} + \mathbf{b}$
- W 是 AI 训练出来的“经验”；$\mathbf{x}$ 是输入的数据.

为什么大一就要重视线性代数？

未来你能做什么？

- 算法工程师 → 矩阵运算、矩阵分解、特征值
- 数据分析师 → 主成分分析、降维
- 游戏/图形开发 → 3D 旋转、投影矩阵
- 交叉学科（物理、生物、经济）→ 线性模型、最小二乘

今天的线性代数，
就是明天智能时代的通行证！

建议：认真学好向量、矩阵、特征值；试试用 Python + NumPy 玩转图像！

课程简介

瑞典数学家 Lars Garding 在其名著 Encounter with Mathematics 中说："如果不熟悉线性代数的概念，要去学习自然科学，现在看来就和文盲差不多."

课程简介

瑞典数学家 Lars Garding 在其名著 Encounter with Mathematics 中说：“如果不熟悉线性代数的概念，要去学习自然科学，现在看来就和文盲差不多.”

《高等代数》是数学专业的一门学科基础必修课程，在学生数学素养的培养中发挥着关键作用. 其内容不仅是后续多门数学课程不可或缺的理论基础，其中蕴含的思想方法也广泛渗透于数学的各个分支.

通过本课程的学习，学生将系统掌握高等代数的基本理论与核心方法，具体目标包括：

- 为后续课程（如抽象代数、组合数学、图论、离散数学、数值计算、微分方程、泛函分析等）奠定坚实的代数基础；
- 深入理解代数学的基本特点与研究方式，逐步培养抽象思维能力、逻辑推理能力与数学创新能力，并提升运用代数工具建立数学模型、解决实际问题的综合素养.

代数学起源于人类对于数的理解

代数学习的几个阶段

- 算　术：自然数、正分数的四则运算（小学）
- 初等代数：有理数、无理数、实数、复数、解方程（中学）
- 高等代数：多项式、线性代数（大一）
- 抽象代数：群、环、域（大二）
- ……….

教材

教材

- 北京大学数学系几何与代数教研室代数小组, 高等代数 (第 6 版), 高等教育出版社, 2025.

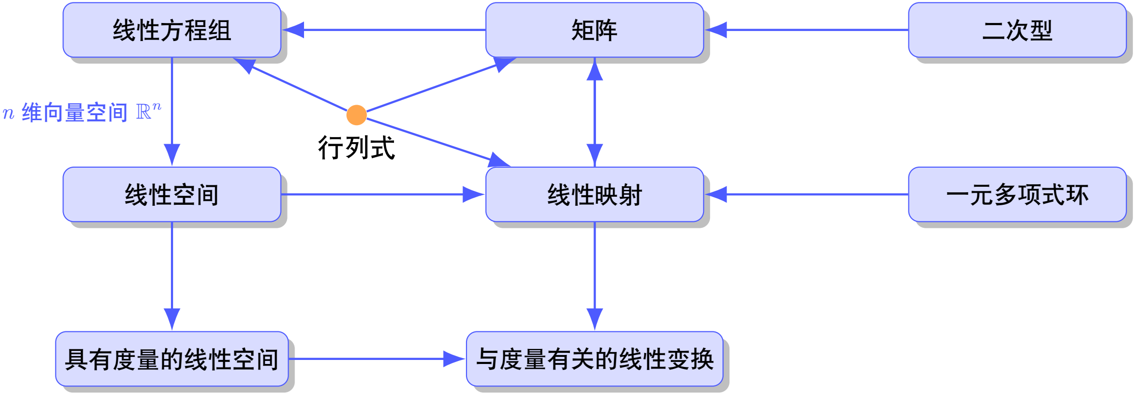
参考书目

- 徐仲等, 高等代数 (北大第四版) 导教导学导考, 西北工业大学出版社, 2014.
- 王萼芳, 石生明, 高等代数辅导与习题解答（北大 · 第 5 版), 高等教育出版社, 2019.

目录

图: 课程网页

高等代数内容结构


线性方程组
矩阵
二次型
n 维向量空间 ℝⁿ
行列式
线性空间
线性映射
一元多项式环
具有度量的线性空间
与度量有关的线性变换

为什么要学习数学？

常见学习问题与学习策略

为什么要学习数学？

如何学好大学数学？

常见学习问题与学习策略

为什么要学习数学？

如何学好大学数学？

专业课是否要预习？

常见学习问题与学习策略

为什么要学习数学？

如何学好大学数学？

专业课是否要预习？

怎么学习高等代数？

常见学习问题与学习策略

为什么要学习数学？

如何学好大学数学？

专业课是否要预习？

怎么学习高等代数？

- **多和老师、同学讨论**：讨论是加深理解、发现盲区的最有效方法.
- **拥抱 AI 工具**：多和人工智能交流，尽管有些答案是错的. 它可以帮助你快速梳理概念、提出问题.
- **利用课程资源**：查看课程网页推荐文章，它们能提供更广阔的视野.

怎么学习高等代数？(Qwen 的建议)

1. **重视定义与定理的精确理解**
   高等代数高度抽象，每一个概念（如“线性无关”“不变子空间”“最小多项式”）都必须字斟句酌地理解. 不要死记结论，而要问：为什么这样定义？它解决了什么问题？
2. **动手推导，拒绝“看懂即会”**
   教材中的定理证明和例题演算务必自己重写一遍，必须亲手练习.
3. **精做习题，注重质量而非数量**
   完成教材课后题（如北大版习题质量高）. 对典型题型（如判断矩阵是否可对角化）总结通用解法. 遇到难题，先尝试自己思考，再参考解答，最后复盘思路.
4. **善用几何直观辅助抽象理解**
   例如：将线性变换想象为“空间的拉伸、旋转”；特征向量是“方向不变的向量”. 低维例子可以帮助直观理解高维抽象.

成绩构成

平时成绩 30%		
出勤 30%	作业 45%	月考 25%
期末考试 70%		

注：做出思考题平时成绩有加分.

提纲

充分条件和必要条件

设 A 与 B 为两命题，

- A 的充分条件是 B

  如果 B 成立，那么 A 成立，即 $A \Leftarrow B$（箭头表示能够推导出）
- A 的必要条件是 B

  如果 A 成立，那么 B 成立，即 $A \Rightarrow B$.
- A 的充分必要条件是 B
  - 充分性 $A \Leftarrow B$
  - 必要性 $A \Rightarrow B$

  例如，当 $b \neq 0$ 时，b 是 a 的因数的充分必要条件是 b 除 a 所得的余数为 0.

当且仅当

当且仅当 (英文：if and only if, 或者：iff)，在数学、哲学、逻辑学以及其他一些技术性领域中广泛使用. 在英语中的对应标记为 iff.

设 A 与 B 为两命题，在证明

$$A \text{ 当且仅当 } B$$

时，这相当于去同时证明陈述

- 如果 A 成立，那么 B 成立
- 如果 B 成立，把么 A 成立

公认的其他同样说法还有

$$B \text{ 是 } A \text{ 的充分必要条件 (或称为充要条件)}.$$

注: 在定义中，“如果⋯ 那么⋯” 的意思就是当且仅当.

比如书上两个多项式相等的定义（P3）.

提纲

假定你有一排很长的直立着的多米诺骨牌.

如果你可以确定:

- 第一张骨牌将要倒下.
- 只要某一个骨牌倒了, 与他相临的下一个骨牌也要倒.

那么你就可以推断所有的的骨牌都将要倒.

第一数学归纳法

第一数学归纳法可以概括为:

1. 归纳基础: 证明 $n = n_0$ 时命题成立.
2. 归纳假设: 假设 $n = k$ 时命题成立.
3. 归纳递推: 由归纳假设推出 $n = k + 1$ 时命题也成立.

例 1

证明对于任意正整数 n，下面的公式都成立

$$1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}.$$

例 1

证明对于任意正整数 n，下面的公式都成立

$$1+2+3+\cdots+n=\frac{n(n+1)}{2}.$$

证明

- 这个公式在 $n=1$ 时成立. 左边 $=1$，右边 $=\frac{1\times 2}{2}=1$. 所以这个公式在 $n=1$ 时成立.
- 我们假设 $n=k$ 时公式成立，即

$$1+2+\cdots+k=\frac{k(k+1)}{2}.$$

- 在上式等号两边分别加上 $k+1$ 得到

$$1+2+\cdots+k+(k+1)=\frac{k(k+1)}{2}+(k+1)=\frac{(k+1)(k+2)}{2}.$$

这就是 $n=k+1$ 时的等式.

因此，对于任意正整数等式都成立. ∎

例 2

证明对于任意正整数 n，下面的公式都成立

$$1^2+2^2+3^2+\cdots+n^2=\frac{n(n+1)(2n+1)}{6}.$$

例 2

证明对于任意正整数 n，下面的公式都成立

$$1^2+2^2+3^2+\cdots+n^2=\frac{n(n+1)(2n+1)}{6}.$$

证明

- 这个公式在 $n=1$ 时成立. 左边 $=1$，右边 $=\frac{1\times 2\times 3}{6}=1$.
  所以这个公式在 $n=1$ 时成立.
- 我们假设 $n=k$ 时公式成立，即

$$1^2+2^2+3^2+\cdots+k^2=\frac{k(k+1)(2k+1)}{6}.$$

- 在上式等号两边分别加上 $k+1$ 得到

$$\begin{aligned}1^2+2^2+\cdots+k^2+(k+1)^2&=\frac{k(k+1)(2k+1)}{6}+(k+1)^2\\&=\frac{(k+1)(k+2)(2k+3)}{6}.\end{aligned}$$

例 3

对于任意自然数 n 证明 3^n-1 是 2 的倍数.

例 3

对于任意自然数 n 证明 3^n-1 是 2 的倍数.

证明

- $3^0-1=1-1=0$ 是 2 的倍数. 所以, 当 $n=0$ 时命题成立.
- 我们假设 $n=k$ 时命题成立, 即 3^k-1 是 2 的倍数.
- 接下来证明 $n=k+1$ 时命题也成立.

$$3^{k+1}-1=2\cdot 3^k+(3^k-1)$$

$2\cdot 3^k$ 是 2 的倍数. 由归纳假设, 3^k-1 是 2 的倍数.
又因为 $2\cdot 3^k$ 也是 2 的倍数, 所以 $3^{k+1}-1$ 是 2 的倍数.
因此, 对于任意自然数 n, 都有 3^n-1 是 2 的倍数. ∎

错误的归纳证明

命题

世界上所有的马都是同一种颜色。

“证明”过程

- **基础步骤**：当 $n = 1$ 时，只有一匹马，命题成立
- **归纳假设**：假设当 $n \leq k$ 时命题成立
- **归纳步骤**：当 $n = k + 1$ 时：
  - 除去第一匹马，剩下 k 匹马同色
  - 除去第二匹马，剩下 k 匹马同色
  - 因此全部 $k + 1$ 匹马同色
- **结论**：命题对所有 n 成立

问题所在

递推步骤中隐含假设了 $n \geq 3$!

- 当 $n = 2$ 时：
  - 除去第一匹马：剩下的一匹马是”同色”的
  - 除去第二匹马：剩下的一匹马是”同色”的
  - 但这无法证明两匹马颜色相同!
- 实际上，$n = 2$ 时命题为假
- 基础步骤不完整，递推步骤无效

教训

必须验证递推步骤所需的所有初始情况!

课后练习题

请用数学归纳法证明以下命题：

1. **恒等式证明**：对于所有正整数 n，有 $1^2+2^2+3^2+\cdots+n^2=\frac{n(n+1)(2n+1)}{6}$.
2. **不等式证明**：对于所有大于等于 2 的正整数 n，有 $1+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{2^n}\geq 1+\frac{n}{2}$.
3. **整除性证明**：对于所有正整数 n，$4^{2n+1}+3^{n+2}$ 能被 13 整除.

提示

可参考课堂例题的证明思路：恒等式用“凑项”，不等式用“放缩”，整除性用“构造归纳假设形式”.

思考题

证明　平面上有 n 条直线，其中任何两条不平行，任何三条不过同一点. 证明这 n 条直线把平面分成 $\frac{1}{2}(n^2+n+2)$ 个部分.

思考题

给定圆周上任意 n 个点，确定有 $\frac{n(n-1)}{2}$ 条弦划分的圆内的区域数，这里假设任意三条弦在圆内不相交.

第二数学归纳法

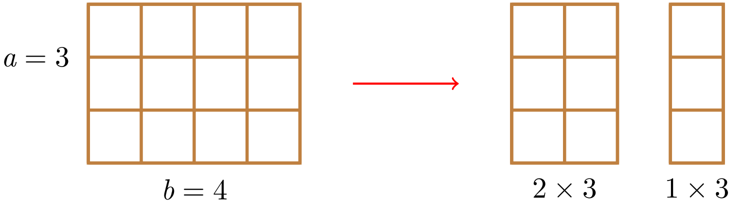
有些命题用第一归纳法证明不大方便，可以用第二归纳法证明.

第二数学归纳法的证明步骤是：

1. 证明当 $n = n_0$ 时命题成立.
2. 假设 $n \geq k$ 时命题都成立.
3. 由归纳假设推出 $n = k + 1$ 时命题也成立.

问题

将一个 $a \times b$ 的巧克力排块掰成 1×1 的小块，需要恰好多少次掰动？

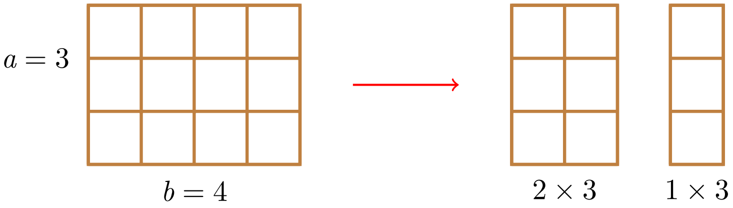


图：巧克力掰动过程示意图：4×3 排块掰成 2×3 和 1×3 两块

第二数学归纳法例题：巧克力排块问题

问题

将一个 $a \times b$ 的巧克力排块掰成 1×1 的小块，需要恰好多少次掰动？



图：巧克力掰动过程示意图：4×3 排块掰成 2×3 和 1×3 两块

命题

将一个 $a \times b$ 的巧克力排块掰成 1×1 的小块，需要恰好 $a \cdot b - 1$ 次掰动.

基础步骤

当 $a = 1, b = 1$ 时:

- 已经是 1×1 小块
- 掰动次数为 $0 = 1 \cdot 1 - 1$
- 命题成立

归纳假设

假设对于所有面积小于 $a \cdot b$ 的巧克力排块（即所有 $m \times n$，其中 $m \cdot n < a \cdot b$），命题成立.

证明：基础步骤

基础情况

当 $a = 1, b = 1$ 时：

- 已经是 1×1 小块
- 掰动次数为 $0 = 1 \cdot 1 - 1$
- 命题成立

证明：归纳步骤

归纳假设

假设对于所有面积小于 $a \cdot b$ 的巧克力排块（即所有 $m \times n$，其中 $m \cdot n < a \cdot b$），命题成立.

归纳步骤

考虑 $a \times b$ 的巧克力排块，其中 a, b 中至少有一个大于 1.

不妨设 $a > 1$. 将 a 行排块掰成 k 行和 $a - k$ 行两部分：

- 第一次掰动：将排块分成 $k \times b$ 和 $(a-k) \times b$ 两块
- 根据归纳假设：
  - 掰动 $k \times b$ 排块需要 $k \cdot b - 1$ 次
  - 掰动 $(a-k) \times b$ 排块需要 $(a-k) \cdot b - 1$ 次
- 总掰动次数为：

$$1 + (k \cdot b - 1) + ((a-k) \cdot b - 1) = a \cdot b - 1$$

第二数学归纳法例题：素数分解（唯一性不讨论，仅存在性）

例题

证明对任意整数 $n \geq 2$，n 可以表示为若干素数的乘积.

第二数学归纳法例题：素数分解（唯一性不讨论，仅存在性）

例题

证明对任意整数 $n \geq 2$，n 可以表示为若干素数的乘积.

证明（第二数学归纳法）.

- 归纳起点. 当 $n = 2$ 时，2 本身为素数，命题成立.
- 归纳假设. 假设对所有 $2 \leq m \leq k$ 命题成立（$k \geq 2$）.
- 归纳步骤. 考虑 $n = k + 1$:
  - 若 $k + 1$ 为素数，则成立；
  - 若为合数，则存在 a, b 满足 $2 \leq a, b \leq k$ 且 $k + 1 = a\,b$.

  由归纳假设，a 和 b 都可分解为素数乘积，于是 $k + 1$ 亦可分解为素数乘积.

因此，命题对所有 $n \geq 2$ 成立. □

第二数学归纳法（强归纳法）:

$$\text{若命题}P(n)\text{ 满足：}\begin{cases}(1)\ \textbf{起点：}\ P(1), P(2), \ldots, P(k_0)\ \textbf{成立；}\\(2)\ \textbf{归纳：}\ \textbf{若}P(1), P(2), \ldots, P(k)\ \textbf{成立，则}P(k+1)\ \textbf{也成立，}\end{cases}$$

则 $P(n)$ 对所有 $n \geq 1$ 成立.

思考题 1：邮票问题（多基阶归纳）

使用 4 分与 5 分邮票，证明任意 $n \geq 12$ 的面额都能拼成.

思考题 2：铺砖问题（结构归纳）

证明：对于任意 $n \geq 1$，一个 $2^n \times 2^n$ 的棋盘去掉任意一个格子，剩余部分可用 L 型三格砖完全覆盖.

$\rightarrow$ 核心思想：假设的不止一步，而是"到目前为止的全部".

第一数学归纳法

- 归纳假设：仅假设 $P(k)$ 成立.
- 形象理解：推骨牌时，只需要前一块倒.
- 适用场景：递推关系只依赖于前一项.

第二数学归纳法

- 归纳假设：假设 $P(1), P(2), \ldots, P(k)$ 都成立.
- 形象理解：推骨牌时，需要前面所有块都倒.
- 适用场景：递推关系依赖于前面多项.

提纲

在数学中经常碰到若干个数连加的情况

$$a_1 + a_2 + \cdots + a_n. \tag{1}$$

为了简便起见，我们通常记成

$$\sum_{i=1}^{n} a_i \tag{2}$$

称 $\sum$ 为连加号，而连加号上下的写法表示 i 的取值由 1 到 n.

例如

$$1^2 + 2^2 + \cdots + n^2 = \sum_{i=1}^{n} i^2,$$

这里的 i 称为求和指标，它只起一个辅助的作用.

把 (2) 还原成 (1) 时，它是不出现的. 譬如说，(1)也可以记成

$$\sum_{j=1}^{n} a_j.$$

因之，只要不与连加号中出现的其它指标相混，用什么字母作为求和指标是任意的.

提纲

整数的可除性理论

用 $\mathbb{Z}$ 表示全体整数组成的数集.

整数有加法, 减法和乘法等运算, 减法是加法的逆运算.

- 带余除法
- 整除
- 最大公因数
- 辗转相除法
- 互素
- 素数
- 因数分解定理
- 最小公倍数

带余除法

在 $\mathbb{Z}$ 中不能作除法，但是有以下的带余除法.

定理 1

对于任意两个整数 a, b，其中 $b \neq 0$，存在一对整数 q, r 满足

$$a = q \cdot b + r, \quad 0 \leqslant r < |b|$$

而且满足这个条件的整数 q, r 是唯一的.

定义

- q 称为 b 除 a 的商，
- r 称为 b 除 a 的余数.

定义

对于整数 a, b, 如果存在一个整数 c 使得 $a = bc$, 则称

- b 是 a 的**因数**,
- a 是 b 的**倍数**.

在定义中我们并不要求 $b \neq 0$.

性质

当 $b \neq 0$ 时， b 是 a 的因数的充分必要条件是 b 除 a 所得的余数为 0.

因此 b 是 a 的因数, 也称 b **整除** a, 记作 $b|a$.

关于整除，有以下一些性质：

性质

1. 如果 $a|b, b|a$, 则 $a = \pm b$.
2. 如果 $a|b, b|c$, 则 $a|c$.
3. 如果 $a|b, a|c$, 则对任意整数 k, l 都有 $a|kb + lc$.

注

- 如果 $a|b$, 则有 $-a|b$ 及 $a|(-b)$，因此以后我们只讨论**非负整数**的**非负因数**和**非负倍数**，不再加以说明.
- 根据定义，每个整数都是 0 的因数，但是 0 不是任何非零整数的因数.

定义

如果 a 既是 b 的因数，又是 c 的因数，则称 a 是 b 和 c 的一个**公因数**.

定义

设 $a, b \in \mathbb{Z}$. 若整数 d 满足

1. $d \mid a$ 且 $d \mid b$（公因数），
2. 对任意 c，若 $c \mid a$ 且 $c \mid b$，则 $c \mid d$（“最大”性），

则称 d 是 a 与 b 的一个**最大公因数**，记作 $\gcd(a, b)$ 或 (a, b).

定义

设 $a, b \in \mathbb{Z}$. 若整数 d 满足

1. $d \mid a$ 且 $d \mid b$（公因数），
2. 对任意 c，若 $c \mid a$ 且 $c \mid b$，则 $c \mid d$（“最大”性），

则称 d 是 a 与 b 的一个**最大公因数**，记作 $\gcd(a, b)$ 或 (a, b).

注：若 d_1, d_2 都是最大公因数，则 $d_1 \mid d_2$ 且 $d_2 \mid d_1$，故 $d_1 = \pm d_2$.
规定最大公因数取非负值，于是 (a, b) **唯一**.

定义

设 $a, b \in \mathbb{Z}$. 若整数 d 满足

1. $d \mid a$ 且 $d \mid b$（公因数），
2. 对任意 c，若 $c \mid a$ 且 $c \mid b$，则 $c \mid d$（“最大”性），

则称 d 是 a 与 b 的一个**最大公因数**，记作 $\gcd(a, b)$ 或 (a, b).

注：若 d_1, d_2 都是最大公因数，则 $d_1 \mid d_2$ 且 $d_2 \mid d_1$，故 $d_1 = \pm d_2$.
规定最大公因数取非负值，于是 (a, b) **唯一**.

思考

- “最大”是指“能被所有公因数整除”.
- 为什么需要“最大”性？只满足条件 1 够不够？
- 如果“最大”性定义为绝对值最大，行不行？

性质 1 ——整除情形

若 $a \mid b$，则 $(a, b) = |a|$. 特别地，$(a, 0) = |a|$ （$a \neq 0$）.

性质 1 ——整除情形

若 $a \mid b$，则 $(a, b) = |a|$. 特别地，$(a, 0) = |a|$（$a \neq 0$）.

性质 2 ——带余除法（核心）

- 若 $a = qb + r$，则 a, b 和 b, r 有相同的公因数.
- 进一步，若 (b, r) 存在，则 (a, b) 也存在，且 $(a, b) = (b, r)$.

性质 1 ——整除情形

若 $a \mid b$，则 $(a, b) = |a|$. 特别地，$(a, 0) = |a|$ （$a \neq 0$） .

性质 2 ——带余除法（核心）

- 若 $a = qb + r$，则 a, b 和 b, r 有相同的公因数.
- 进一步, 若 (b, r) 存在，则 (a, b) 也存在, 且 $(a, b) = (b, r)$.

例如计算 $(48, 18)$:

$$
\begin{aligned}
48 &= 2 \cdot 18 + 12 &\Rightarrow\quad & (48, 18) = (18, 12) \\
18 &= 1 \cdot 12 + 6 &\Rightarrow\quad & (18, 12) = (12, 6) \\
12 &= 2 \cdot 6 + 0 &\Rightarrow\quad & (12, 6) = (6, 0) = 6
\end{aligned}
$$

性质 1 ——整除情形

若 $a \mid b$，则 $(a,b)=|a|$. 特别地，$(a,0)=|a|$（$a\neq 0$）.

性质 2 ——带余除法（核心）

- 若 $a=qb+r$，则 a,b 和 b,r 有相同的公因数.
- 进一步，若 (b,r) 存在，则 (a,b) 也存在，且 $(a,b)=(b,r)$.

例如计算 $(48,18)$：

$$\begin{aligned}
48 &= 2\cdot 18+12 &&\Rightarrow\quad (48,18)=(18,12)\\
18 &= 1\cdot 12+6 &&\Rightarrow\quad (18,12)=(12,6)\\
12 &= 2\cdot 6+0 &&\Rightarrow\quad (12,6)=(6,0)=6
\end{aligned}$$

为什么重要？

它把“大数”$\to$“小数”$\to$“整除”一步步化简，正是辗转相除法的理论基础！

辗转相除法（Euclidean Algorithm）

设 $b \neq 0$（即 $b > 0$）. 通过**带余除法**反复进行如下操作：

$$
\begin{aligned}
a &= q_1 b + r_1, & 0 < r_1 < b,\\
b &= q_2 r_1 + r_2, & 0 < r_2 < r_1,\\
&\cdots & \cdots\\
r_{k-2} &= q_k r_{k-1} + r_k, & 0 < r_k < r_{k-1},\\
r_{k-1} &= q_{k+1} r_k + 0.
\end{aligned}
$$

当余数为零时，算法终止. 此时有：

$$(a, b) = (b, r_1) = (r_1, r_2) = \cdots = (r_{k-1}, r_k) = r_k.$$

此外，通过上述过程，还可以找到整数 u, v，使得

$$(a, b) = ua + vb.$$ 贝祖等式（Bézout's identity）

例 4

使用辗转相除法求 $(252, 105)$.

解

$$252 = 2 \times 105 + 42$$

例 4

使用辗转相除法求 $(252, 105)$.

解

$$252 = 2 \times 105 + 42$$

$$105 = 2 \times 42 + 21$$

例 4

使用辗转相除法求 $(252, 105)$.

解

$$252 = 2 \times 105 + 42$$

$$105 = 2 \times 42 + 21$$

$$42 = 2 \times 21 + 0$$

例 4

使用辗转相除法求 $(252, 105)$.

解

$$252 = 2 \times 105 + 42$$

$$105 = 2 \times 42 + 21$$

$$42 = 2 \times 21 + 0$$

$$(252, 105) = 21.$$

例 4

使用辗转相除法求 $(252, 105)$.

解

$$252 = 2 \times 105 + 42$$

$$105 = 2 \times 42 + 21$$

$$42 = 2 \times 21 + 0$$

$$(252, 105) = 21.$$

求贝祖等式：找整数 u, v **使得** $21 = u \times 252 + v \times 105.$

例 4

使用辗转相除法求 $(252, 105)$.

解

$$
\begin{aligned}
252 &= 2 \times 105 + 42 \\
105 &= 2 \times 42 + 21 \\
42 &= 2 \times 21 + 0
\end{aligned}
$$

$$(252, 105) = 21.$$

求贝祖等式：找整数 u, v 使得 $21 = u \times 252 + v \times 105$.

由第二步 $21 = 105 - 2 \times 42$. 代入第一步 $42 = 252 - 2 \times 105$, 得

例 4

使用辗转相除法求 $(252, 105)$.

解

$$252 = 2 \times 105 + 42$$

$$105 = 2 \times 42 + 21$$

$$42 = 2 \times 21 + 0$$

$$(252, 105) = 21.$$

求贝祖等式：找整数 u, v 使得 $21 = u \times 252 + v \times 105$.

由第二步 $21 = 105 - 2 \times 42$. 代入第一步 $42 = 252 - 2 \times 105$, 得

注: 对于整数 $c \neq 1$, 如果存在整数 u, v 使 $u\,a + v\,b = c$, 这不意味着 c 是 a 和 b 的最大公因数. 试试自己举出反例.

例 4

使用辗转相除法求 $(252, 105)$.

解

$$252 = 2 \times 105 + 42$$

$$105 = 2 \times 42 + 21$$

$$42 = 2 \times 21 + 0$$

$$(252, 105) = 21.$$

求贝祖等式：找整数 u, v 使得 $21 = u \times 252 + v \times 105$.

由第二步 $21 = 105 - 2 \times 42$. 代入第一步 $42 = 252 - 2 \times 105$, 得

$$21 = 105 - 2 \times (252 - 2 \times 105) = (-2) \times 252 + 5 \times 105.$$

注: 对于整数 $c \neq 1$, 如果存在整数 u, v 使 $u\,a + v\,b = c$, 这不意味着 c 是 a 和 b 的最大公因数. 试试自己举出反例.

定义

如果整数 a, b 的最大公因数等于 1, 则称 a, b **互素** (也称互质).

例如, 3 与 5 互素, 21 与 40 互素.

互素有以下一些重要性质:

1. a, b 互素的充分必要条件是存在整数 u, v 使
$$u\,a + v\,b = 1$$
2. 如果 $a|bc$, 且 $(a, b) = 1$, 则 $a|c$.
3. 如果 $a|c$, $b|c$ 且 $(a, b) = 1$, 则 $ab|c$
4. 如果 $(a, c) = 1, (b, c) = 1$, 则 $(ab, c) = 1$

定义

设 a 是一个大于 1 的整数.

如果除去 1 和本身外, a 没有其它因数, 那么称 a 是一个**素数**(也称质数).

例如 2, 3, 5, 23 等都是素数.

从定义可知, 如果 p 表示成 $p = a \cdot b$, 则必有 $a = 1, b = p$ 或 $a = p, b = 1$

性质

1. 一个素数 p 和任一个整数 a 都有 $p|a$ 或 $(p, a) = 1$.
2. 如果素数 $p|ab$, 那么 $p|a$ 或 $p|b$.
3. 如果一个大于 1 的整数 p 和任何整数 a 都有 $p|a$ 或$(p, a) = 1$, 则 p 是一个素数.
4. 如果大于 1 的整数 p 具有下述性质: 对任何整数 a, b 从 $p|ab$ 可推出 $p|a$ 或 $p|b$, 则 p 是一个素数.

如果一个素数 p 是整数 a 的一个因数, 则 p 称为 a 的一个**素因数**.

根据互素及素数的性质，应用数学归纳法可以证明整数的一个基本定理.

定理 2 (因数分解及唯一性定理)

任一个大于 *1* 的整数 a 可以分解成有限多个素因数的乘积:

$$a = p_1 p_2 \cdots p_s$$

而且分解法是唯一的，即如果有两种分解法:

$$a = p_1 p_2 \cdots p_s = q_1 q_2 \cdots q_t$$

其中 $p_1, \cdots, p_s; q_1, \cdots, q_t$ 都是素数，那么有 $s = t$,
并且重新将 $q_1, \cdots, q_t$ 适当排序后，可得 $p_i = q_i, \quad i = 1, 2, \cdots, s.$

大数质因子分解是当代密码体制的基础. 比如常见的 RSA 加密体系，如果想破解就需要对大数进行质因子分解.

- 在 a 的分解式中，将同一个素因数合并写成方幂，并且将素因数按大小排列，得到

$$a = p_1^{\ell_1} p_2^{\ell_2} \cdots p_r^{\ell_r}, \quad p_1 < p_2 < \cdots < p_r, l_i > 0, i = 1, \cdots, r.$$

  这种表示法称为 a 的标准分解式.

可以应用整数的分解式来判断整除性及计算最大公因数.

- 现在将整数 a 和 b 的因数合在一起，设为 $p_1, p_2, \cdots, p_t$，并设

$$\begin{cases} a = p_1^{\ell_1} p_2^{\ell_2} \cdots p_t^{\ell_t}, & \ell_i \geqslant 0, \quad i = 1, 2, \cdots, t \\ b = p_1^{d_1} p_2^{d_2} \cdots p_t^{d_t}, & d_i \geqslant 0, \quad i = 1, 2, \cdots, t \end{cases} \tag{3}$$

  则

  1. a 能整除 b 的充分必要条件为 $\ell_i \leqslant d_i$, $i = 1, 2, \cdots, t$
  2. $(a, b) = p_1^{\min(\ell_1, d_1)} p_2^{\min(\ell_2, d_2)} \cdots p_t^{\min(\ell_t, d_t)}$

定义

设 a, b 是两个非负整数. m 是 a, b 的一个公倍数 (按前面约定, 也是非负的). 如果 a, b 的任一个公倍数都是 m 的倍数, 则 m 称为 a, b 的一个最小公倍数.

注

- 由定义可看出 a, b 的最小公倍数是唯一的, 记作 $[a, b]$.
- 当 a, b 是正整数时, 从它们的标准分解式可以求出最小公倍数.
  设 a , b 的分解如 (3), 则

$$[a, b] = p_1^{\max(l_1, d_1)} p_2^{\max(l_2, d_2)} \cdots p_t^{\max(p_t, d_t)}$$

- 由此还可看出

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

例 5 (思考题)

一个整数能被 3 整除当且仅当这个数的数字和能被 3 整除.

例 6 (思考题)

一个数字能被 7 整除当且仅当其末 3 位与末 3 位之前的数字之差能被 7 整除.

提纲

高中的时候，定义了

$$\mathrm{i} = \sqrt{-1}$$

然后形如：

$$a + b\,\mathrm{i} \quad (a, b \in \mathbb{R})$$

这样的数就是复数. 全体复数的集合记为

$$\mathbb{C} = \{a + b\,\mathrm{i} \,|\, a, b \in \mathbb{R}\}$$

有了复数之后，开方运算就不再局限于大于零的数了，这样一元二次方程

$$ax^2 + bx + c = 0 \quad (a \neq 0)$$

就总是有解了：

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

- 定义 $\mathbb{C}$ 内的加法

$$(a+bi)+(c+d\mathrm{i}):=(a+c)+(b+d)\,\mathrm{i}$$

- 定义 $a+b\,\mathrm{i}$ 的负数 $-(a+b\,\mathrm{i})$ 是 $(-a)+(-b)\,\mathrm{i}$
- 定义 $\mathbb{C}$ 内的减法

$$(a+b\,\mathrm{i})-(c+d\,\mathrm{i})=(a-c)+(b-d)\,\mathrm{i}$$

- 定义 $\mathbb{C}$ 内的乘法

$$(a+b\,\mathrm{i})(c+d\,\mathrm{i})=(ac-bd)+(ad+bc)\,\mathrm{i}$$

- 定义 $a+b\,\mathrm{i}$ 的倒数或逆

$$\frac{1}{a+b\,\mathrm{i}}=\frac{1}{a^2+b^2}(a-b\,\mathrm{i})=\frac{a-b\,\mathrm{i}}{a^2+b^2}$$

- $\mathbb{C}$ 内的除法是 (设 $c+d\,\mathrm{i}\neq 0$)

$$\frac{a+b\,\mathrm{i}}{c+d\,\mathrm{i}}=(a+b\,\mathrm{i})\frac{1}{c+d\,\mathrm{i}}=(a+b\,\mathrm{i})\frac{c-d\,\mathrm{i}}{c^2+d^2}$$

复数：实部、虚部、共轭、模

我们知道，实数与数轴上的点一一对应，实数可用数轴上的点来表示.

根据复数相等的定义，复数 $a+b\mathrm{i}$ 与直角坐标系中的点 (a,b) 一一对应. 因此，复数可用直角坐标系中的点来表示.

通常把建立了直角坐标系来表示复数的平面叫做复平面.

定义

对于复数 $z=a+b\mathrm{i}$，其中 a,b 是实数.

- a 称为 z 的实部，记为 $\mathrm{Re}\,z$
- b 称为 z 的虚部，记为 $\mathrm{Im}\,z$
- 复数 $z=a+b\mathrm{i}$ 的共轭 $\bar{z}:=a-b\mathrm{i}$
- $|z|=\sqrt{a^2+b^2}$ 称为 $a+b\mathrm{i}$ 的模或绝对值.

性质

- $z\bar{z}=(a+b\mathrm{i})(a-b\mathrm{i})=a^2+b^2$.
- $z+\bar{z}=(a+b\mathrm{i})+(a-b\mathrm{i})=2a$.
- $z-\bar{z}=(a+b\mathrm{i})-(a-b\mathrm{i})=2b\mathrm{i}$.

复数的三角表示

定义

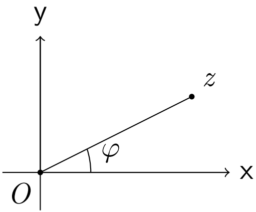
一个复数 $z = a + b\,\mathrm{i}$ 的辐角是指将 Ox 轴正方向沿逆时针方向旋转到 Oz 的旋转角 φ .

辐角的值不是唯一确定的，可以加上 2π 的任意整数倍.

因为 $a = |z|\cos\varphi, b = |z|\sin\varphi$, 故有

$$z = a + b\,\mathrm{i} = |z|(\cos\varphi + i\sin\varphi)$$

上式称为复数的三角表示.



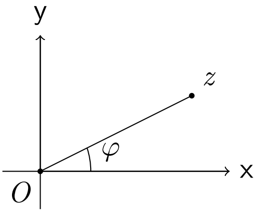
复数 z 的指数表示

- 令模为 1 的复数

$$e^{i\varphi} := \cos\varphi + i\sin\varphi,$$

这个复数位于以坐标原点 O 为中心的单位圆上，其辐角为 φ.
以后我们会看到, $e^{i\varphi}$ 不仅是一个记号, 也有实际的意义.

- 因此，任一复数 z 可以表示为 $z = |z|e^{i\varphi}$ ，其中 φ 为 z 的辐角，这种表示称为复数 z 的指数表示.



如果复数

$$z_1 = |\alpha|(\cos\varphi + \,\mathrm{i}\sin\varphi), \quad z_2 = |\beta|(\cos\psi + \,\mathrm{i}\sin\psi),$$

那么它们的乘积

$$\begin{aligned} z_1\, z_2 &= |z_1||z_2|(\cos\varphi + \,\mathrm{i}\sin\varphi)(\cos\psi + i\sin\psi) \\ &= |z_1||z_2|(\cos\varphi\cos\psi - \sin\varphi\sin\psi) + (\sin\varphi\cos\psi + \cos\varphi\sin\psi)\,\mathrm{i}) \\ &= |z_1||z_2|(\cos(\varphi + \psi) + \,\mathrm{i}\sin(\varphi + \psi)) \end{aligned}$$

上式表示，两个复数相乘时，

- 其模为这两个复数的模相乘，
- 其辐角相加 (因为三角函数以 $2\,\pi$ 为周期，故把相差 $2\,\pi$ 的整数倍的角认为是相同的).

若 n 为正整数，$z=|z|(\cos\theta+\mathrm{i}\sin\theta)$ 为复数 z 的三角表示，则

$$z^n=|z|^n(\cos(n\theta)+\mathrm{i}\sin(n\theta))$$

特别地，取 $z=\cos\theta+\mathrm{i}\sin\theta$ ，则

$$(\cos\theta+\mathrm{i}\sin\theta)^n=\cos(n\theta)+\mathrm{i}\sin(n\theta)$$

称之为棣莫弗公式（De Moivre formula).

方程 $x^n - 1 = 0$ 的根

给定一个正整数 n, 考虑下面 n 个复数

$$\mathrm{e}^{\frac{2k\pi}{n}\mathrm{i}} = \cos\frac{2k\pi}{n} + \mathrm{i}\sin\frac{2k\pi}{n},$$

其中 $k = 0, 1, 2, \cdots, n-1$.

这 n 个复数就是以原点 O 为中心的单位圆的内接正 n 边形的 n 个顶点. 由欧拉公式可知,

$$\left(\mathrm{e}^{\frac{2k\pi}{n}i}\right)^n = \left(\cos\frac{2k\pi}{n} + \mathrm{i}\sin\frac{2k\pi}{n}\right)^n = \cos 2k\pi + \mathrm{i}\sin 2k\pi = 1.$$

因此，这 n 个复数恰为 n 次代数方程

$$x^n - 1 = 0$$

在复数系 $\mathbb{C}$ 内的 n 个根, 称为 n **次单位根**.