# 网安数学基础
# 期末通关

按教材 13 章 + **全部课后题**整理。**前 5 章按老师说的只做作业级要求，第 6 章往后是笔试主战场。**

目录


00 这门课在讲什么
01 矩阵
02 范数、距离与相似度
03 最优化
04 概率论
05 马尔可夫链与 PageRank
06 整除、最大公因子与欧几里得算法
07 同余、逆元与线性同余式
08 中国剩余定理
09 费马、欧拉、威尔逊三大定理
10 数论函数
11 二次剩余
12 原根与指数
13 群、环、域
14 有限域
15 椭圆曲线基础
16 整卷速查

00

# 这门课在讲什么

约 2 分 · 12 分钟

先看清地图，再决定力气往哪使

> **一句话：**这门课讲的是"密码学背后的数学"：怎么在模运算里造代数结构，再用它做加解密。

? 你可能觉得"网络空间安全"应该是讲攻防、讲漏洞。
可这门课一上来就是整除、同余、群、环、域 —— 看起来像纯数学。
原因很简单：**所有公钥密码都建立在模运算上**。不理解 $a^{p-1}\equiv 1$，就看不懂 RSA 为什么能工作。

先看地图

## 一、老师怎么定的重点

第一节课和讲数论时，老师反复说了几句，直接决定了复习策略：

| 老师原话 | 怎么理解 |
| --- | --- |
| "前 5 章是平时作业，**笔试在后边**" | 矩阵、范数、最优化、概率、马尔可夫不出大题 |
| "欧几里得算法**肯定必考**，分值 10 以上" | 扩展欧几里得是必拿分 |
| "这是唯一用中国命名的定理" | 中国剩余定理必考 |
| "我规定 7 进制，也可能是 13、23 进制" | 进制转换要练 |
| "后边定理的证明会跳过去" | **重计算、轻证明** |

## 二、13 章，分两块

课本有 13 章，但分量完全不同：

| 章 | 内容 | 权重 |
| --- | --- | --- |
| 1–5 | 矩阵、范数、最优化、概率、马尔可夫 | 作业级，不出大题 |

| | | |
|---|---|---|
| **6** | **整数与同余** | ★★★★★ |
| 7 | 数论函数 | ★★★ |
| 8 | 二次剩余 | ★★★★ |
| 9 | 原根与指数 | ★★★★ |
| 10 | 群、环、域 | ★★★★ |
| **11** | **有限域** | ★★★★★ |
| 12 | 椭圆曲线 | ★★★ |

为什么第 6 章这么重？因为**后面所有章节都建在它上面**：二次剩余要用欧拉判别，原根要用欧拉定理，有限域要用模运算。**第 6 章没打通，第 8–11 章全是空中楼阁。**

## 三、这些数学用在哪

每讲一个工具，都对应一个真实的安全技术：

| 数学工具 | 用在哪 |
|---|---|
| 模运算、同余 | 所有公钥密码的运算空间 |
| 扩展欧几里得 | 求模逆元 —— RSA 解密、签名都靠它 |
| 中国剩余定理 | RSA 加速、秘密共享 |
| 费马、欧拉定理 | RSA 正确性、素性检测 |
| 二次剩余 | Rabin 加密、素性检测 |
| 原根 | Diffie-Hellman 密钥交换 |
| 有限域 | AES 的 S 盒、纠错码 |
| 椭圆曲线 | ECC，同强度下密钥更短 |

## 四、怎么用这本材料

每一讲都是"先讲明白，再做题"：正文把概念和推导讲清楚，末尾收着这一讲的课后题，答案默认折叠。

建议走法：先读正文，遇到"停一下"就自己答一遍；然后合上答案做末尾的题；做错的标"不会"，第二轮只看这些。

顶部两个开关：一个切"只看题目"，一个按"会/卡/不会"筛。第二轮、第三轮靠它们省时间。

**先记住 · 四条**

| | |
|---|---|
| 前 5 章作业级，6 章以后是主战场 | 老师原话 |
| 欧几里得必考，10 分以上 | 必拿分 |
| 重计算、轻证明 | 定理证明会跳 |
| 第 6 章是后面所有章的地基 | 先打通它 |

⚠ **三个别做：**

① **别从第 1 章按顺序死磕。**前五章不出大题，顺序读会浪费一半时间。

② **别背定理证明。**老师说会跳过，考试也不会要求完整证明，重点是会用。

③ **别跳过 gcd 和模逆元直接学有限域。**那是没地基盖楼，看不懂是必然的。

## 01 矩阵

约 4 分 · 30 分钟

这一讲不背性质，只搞清一件事：$Ax=b$ 到底在说什么

**一句话：**矩阵只是把一堆线性方程摞起来写省事；解方程就是把矩阵化成上三角，然后回代。

? 初中就学过解二元一次方程组：消元、代入。

三个未知数、五个未知数呢？手写会乱。于是有人想：**能不能把系数单独拎出来排成一个方块，只对这个方块做运算？**

这就是矩阵的来历 —— 它不是什么新数学，只是一种**记账格式**。

**先讲清楚**

### 一、$Ax=b$ 的三种读法

同一个式子，可以按三种方式理解。三种都要会，因为不同的题用不同的读法最快。

| 读法 | 把它看成什么 | 什么时候用 |
|---|---|---|
| **行视角** | 每一行是一个方程，求几条直线的交点 | 解方程 |

| | | |
|---|---|---|
| **列视角** | $x$ 是"各列怎么搭配"的系数 | 判断有没有解 |
| **变换视角** | $A$ 是把向量 $x$ 搬到 $b$ 的动作 | 理解线性变换、特征值 |

列视角最容易被忽略，但它最有用。举例：

$$A=(1,2;3,4)，\ x=(1,1) \Rightarrow Ax=1\cdot(1;3)+1\cdot(2;4)=(3;7)$$

也就是说，**$Ax$ 就是"把 $A$ 的每一列按 $x$ 的分量加权相加"**。

由此立刻得到一条判据：**$Ax=b$ 有解 $\Leftrightarrow$ $b$ 能由 $A$ 的列拼出来 $\Leftrightarrow$ $b$ 在列空间里。**这句话在判断"方程组有没有解"时比消元快得多。

## 二、解方程：消元法的本质

手算消元时做的事，其实是对**整行**做三种操作：交换两行、某行乘一个数、某行加上另一行的倍数。

这三种操作都不改变方程组的解集，所以可以放心做，直到把矩阵化成上三角（左下角全变成 0）。

化成上三角之后，最后一个方程只剩一个未知数，直接解出来，再一层层往上代 —— 这叫**回代**。

## 三、列主元：为什么不能随便选主元

消元时要用主元去除别的行。如果主元很小（比如 0.0001），除出来的乘数会很大，把舍入误差放大，最后结果全错。

所以实际计算时会先在当前列里挑**绝对值最大**的那个，把它换到主元位置再消元。这叫**列主元消元法**。

课本习题里专门放了一个含 1000 和 −100 的矩阵，就是考这一点：**先看列、再动手**。

## 四、LU 分解：把消元过程存起来

消元时，每一步用的"乘数"其实很有价值。把它们记下来放在一个下三角矩阵里，就是 $L$；消完得到的上三角就是 $U$。

$$A=LU$$

有什么用？如果你的 $A$ 不变、$b$ 要换很多次（比如实时信号处理），那消元只做一次，之后每次只需"前代 + 回代"两步，快得多。

> **算一个：** $A=(2,1,3;1,3,2;1,0,1)$，$b=(7,8,9)$。
> 第一列消元：$l_{21}=\frac{1}{2}$、$l_{31}=\frac{1}{2}$；第二列：$l_{32}=-\frac{1}{5}$。
> $L=(1,0,0;\frac{1}{2},1,0;\frac{1}{2},-\frac{1}{5},1)$，$U=(2,1,3;0,\frac{5}{2},\frac{1}{2};0,0,-\frac{2}{5})$。
> 验算 $LU=A$ ✓，再解 $Ly=b$ 得 $y=(7,\frac{9}{2},\frac{32}{5})$，回代得 $x=(25,5,-16)$。

## 五、最小二乘：方程多了怎么办

方程个数比未知数多时，一般没有精确解 —— 几条线不会正好交于一点。

这时退一步：找一个 $x$，让"误差的平方和"最小。这就是最小二乘。

它的解满足**正规方程**：

$$A^TAx=A^Tb$$

几何意义：把 $b$ **投影**到 $A$ 的列空间上，投影点就是最优解。投影之后剩下的那一小段垂直于列空间，这就是"误差"。

## 六、秩-1 分解：最简单的结构

如果一个矩阵的每一行都成比例（都是同一个向量的倍数），那它可以写成

$$A=\vec{u}\vec{v}^T$$

这叫秩-1 分解。判断方法：随便挑一行，看其它行是不是它的倍数。

它和第 14 讲的有限域、第 12 讲的椭圆曲线没直接关系，但和后面的 SVD、降维有关 —— 任意矩阵都能拆成若干个秩-1 矩阵之和。

> **停一下：$A=(1,2;2,4)$，$Ax=b$ 对任意 $b$ 都有解吗?**

不是。两行成比例，第二行是第一行的 2 倍，所以两列线性相关。

列空间只有一条直线（一维），而 $b$ 是二维的 —— 大多数 $b$ 不在这条线上，无解。

只有 $b=(t;2t)$ 这种形式的才有解。

**必背 · 五条**

| | |
|---|---|
| $Ax$ = 列的加权和 | 列视角 |
| 有解 ⇔ $b$ 在列空间 | 判据 |
| $A=LU$ | 消元即分解 |
| $A^TAx=A^Tb$ | 最小二乘 |
| 每行成比例 ⇒ rank = 1 | 秩-1 判定 |

**课本 1-2** 6 分 LU 分解与求解

对 $A=(2,1,3;1,3,2;1,0,1)$、$b=(7,8,9)$ 做 LU 分解并解方程。

---

**第一步：老老实实做一遍消元，把乘数记在旁边。**

要消掉第 2 行的第一个 1，用第 1 行乘以 $\frac{1}{2}$ 去减，乘数 $l_{21}=\frac{1}{2}$。

同理 $l_{31}=\frac{1}{2}$。消完之后第 2 行变成 $(0,\frac{5}{2},\frac{1}{2})$，第 3 行变成 $(0,-\frac{1}{2},-\frac{1}{2})$。

**第二步：再消第二列。**第 3 行减去第 2 行的 $(-\frac{1}{5})$ 倍，乘数 $l_{32}=-\frac{1}{5}$。

第 3 行变成 $(0,0,-\frac{2}{5})$。

**第三步：写 $L$ 和 $U$。**$L$ 是单位下三角（对角全 1），把三个乘数填进对应位置；$U$ 就是消完的结果。

$L=(1,0,0;\frac{1}{2},1,0;\frac{1}{2},-\frac{1}{5},1)$，$U=(2,1,3;0,\frac{5}{2},\frac{1}{2};0,0,-\frac{2}{5})$。

**第四步：验算 $LU=A$。**这一步不费时间，但能挡住绝大多数计算错误，一定要做。

**第五步：解 $Ly=b$（前代）。**$y_1=7$；$y_2=8-\frac{1}{2}\times7=\frac{9}{2}$；$y_3=9-\frac{1}{2}\times7+\frac{1}{5}\times\frac{9}{2}=\frac{32}{5}$。

**第六步：解 $Ux=y$（回代）。**从最后一行起：$-\frac{2}{5}x_3=\frac{32}{5}\Rightarrow x_3=-16$；往上算得 $x_2=5$、$x_1=25$。

**第七步：代回验证。**$2\times25+5+3\times(-16)=7$ ✓，$25+15-32=8$ ✓，$25-16=9$ ✓

**答案：$x=(25,5,-16)$。**

LU 分解本身不检查的话，一个乘数抄错，后面全废。所以"验算 $LU=A$"这一步在考试里也值得花 30 秒。

⚠ **三个坑：**

① **把 $L$ 写成上三角。**$L$ 是下三角（Lower），$U$ 是上三角（Upper），按名字记就不会错。

② **最小二乘硬解 $Ax=b$。**方程比未知数多时 $A$ 不可逆，$x=A^{-1}b$ 根本不存在。必须解正规方程。

③ **以为每行成比例就是"所有元素相等"。**成比例是说第 2 行 = $k$ × 第 1 行，$k$ 可以是任何数，不是必须为 1。

**自测 · 3 道**

1. $Ax=b$ 有解的几何条件是什么?
2. LU 分解中 $L$ 的对角线元素是什么?
3. 最小二乘解的方程叫什么?

**1.** $b$ 落在 $A$ 的列空间里。

**2.** 全是 1（单位下三角）。

**3.** 正规方程 $A^TAx=A^Tb$。

## ch01 · 习题 3 道

### ch01 · 1-1

○ 会　○ 卡　○ 不会

**1-1** 用列主元高斯消元解 $Ax=b$：

(1) $A$=(-3,1,4;1000,-5,0;5,-1,0.5)，$b$=(7,4,5)；

(2) $A$=(3,-1,4;-100,2,-2;0.5,-3,-2)，$b$=(7,0,-1).

**套路：每列先挑绝对值最大的当主元再消元；1000 和 -100 就是这两题的全部考点。**

① (1) 第一列 |-3|,|1000|,|5| 中 1000 最大。

② 交换 1、2 行，主元取 1000，避免被 -3 放大舍入误差。

③ 消元后第 2 行是 (0,197/200,4|1753/250)。

④ 第 3 行是 (0,-39/40,1/2|249/50)，乘数 $l_{31}$=1/200。

⑤ 第二列 |197/200|>|-39/40|，不换行，$l_{32}$=-195/197。

⑥ 关键式子：第 3 行化为 (0,0,1757/394|11742/985)，回代。

⑦ 答案：$x$≈(-0.01468,-3.73682,2.67319)。

⑧ 验算：$Ax$=(7,4,5) ✓。

⑨ (2) 第一列 |-100| 最大，交换 1、2 行。

⑩ 消元得 (0,-47/50,197/50|7) 与 (0,-299/100,-201/100|-1)。

⑪ 关键：第二列 |-2.99|>|-0.94|，再交换 2、3 行。

⑫ 答案：$x$≈(-0.04682,-0.74104,1.59985)，代回成立。

**答案：(1) (-0.0147,-3.7368,2.6732)；(2) (-0.0468,-0.7410,1.5999)。**

**易错：不换行硬算时乘数 1/1000 会把误差放大 —— 列主元就是"先看列、再动手"。**

## ch01 · 1-2

○ 会　○ 卡　○ 不会

**1-2** 对下列 $A$ 做 LU 分解，据此解 $Ax=b$：

(1) $A=(2,1,3;1,3,2;1,0,1)$，$b=(7,8,9)$；

(2) $A=(6,2,1;-9,2,-1;1,1,1)$，$b=(15,-15,1)$.

**套路：Doolittle 分解 $A=LU$（$L$ 单位下三角），先解 $Ly=b$ 再解 $Ux=y$。**

① (1) 第一列乘数 $l_{21}=1/2$、$l_{31}=1/2$。

② 第二列乘数 $l_{32}=(-1/2)/(5/2)=-1/5$。

③ 关键式子：$L=(1,0,0;1/2,1,0;1/2,-1/5,1)$，$U=(2,1,3;0,5/2,1/2;0,0,-2/5)$。

④ 验算 $LU=A$ ✓。

⑤ 解 $Ly=b$ 得 $y=(7,9/2,32/5)$。

⑥ 回代得 $x=(25,5,-16)$，代回 $Ax=(7,8,9)$ ✓。

⑦ (2) 乘数 $l_{21}=-3/2$、$l_{31}=1/6$、$l_{32}=2/15$。

⑧ 关键式子：$U$ 最后一行为 $(0,0,23/30)$。

⑨ 解 $Ly=b$ 得 $y=(15,15/2,-5/2)$。

⑩ 关键：回代得 $x=(56/23,42/23,-75/23)\approx(2.4348,1.8261,-3.2609)$。

**答案：(1) $x=(25,5,-16)$；(2) $x\approx(2.435,1.826,-3.261)$。**

**易错：LU 不换行要求主元全程非零；碰上 0 主元只能改用 $PA=LU$。**

## ch01 · 1-4~1-5

○ 会　○ 卡　○ 不会

**1-4**（水印嵌入）取彩色载体 $A$ 与水印 $W$，用 SVD 以强度 $a$ 把 $W$ 嵌入 $A$，给出数据并验证.

**1-5**（自适应降维）还原例 1.6.4，并给出判据来自适应选降维参数 $k$.

**套路：SVD 把 $A$ 拆成秩 1 片之和；$\sigma_i$ 是 $A^TA$ 特征值的算术平方根，砍小的 $\sigma$ 就是降维。**

① 1-4 的模型：$A_w \approx A+aW$，$a$ 是强度。

② 关键式子：$|\sigma_i(A_w)-\sigma_i(A)| \le a\|W\|_2$，奇异值对扰动是 Lip 连续的。

③ 数值例：$A=(3,0;0,1)$，$W=(0,1;1,0)$，$a=0.1$。

④ 得 $A_w=(3,0.1;0.1,1)$，$\sigma(A)=(3,1)$。

⑤ 关键：$\sigma(A_w)\approx(3.0050,0.9950)$，偏差 0.005 远小于上界 0.1。

⑥ 结论：$a$ 越大越抗攻击，失真上界就是 $a\|W\|_2$。

⑦ 1-5：$A=\Sigma_i\sigma_i u_i v_i^T$，截断 $A_k=\Sigma_{i\le k}\sigma_i u_i v_i^T$。

⑧ 关键：Eckart-Young —— $A_k$ 是最优秩 $k$ 逼近。

⑨ 误差 $\|A-A_k\|_F=\sqrt{\Sigma_{i>k}\sigma_i^2}$，谱范数误差正是 $\sigma_{k+1}$。

⑩ 例 1.6.4：402×600 灰度图，$\sigma_1=42409$，最小 3.3。

⑪ 前 41 个 $\sigma$ 在 $10^3$ 以上，第 42 个起掉下去。

⑫ 关键判据：取最小 $k$ 使能量占比 $\Sigma_{i\le k}\sigma_i^2/\Sigma\sigma_i^2 \ge 1-\varepsilon$（常取 0.99）。

⑬ 按 $\sigma \ge 10^3$ 得 $k=41$；书里取 $k=30$ 已近似原图。

⑭ 存储：$A_k$ 只需 $k(402+600+1)=1003k$ 个数。

⑮ 关键：$k=30$ 时约 12.5% 的数据量，这就是降维收益。

**答案：判据用奇异值能量占比或 $\sigma_{k+1}$ 阈值，本例 $k$ 取 30~41；水印失真由 $a\|W\|_2$ 控制。**

## 02 范数、距离与相似度

约 4 分 · 25 分钟

这一讲定三把尺子：多长、多远、多像

> **一句话：** 范数是"一个向量的长度"，距离是"两个向量之间有多远"，相似度是"两个方向有多接近"。

? 问一个向量有多长，你会想到勾股定理。可如果数据是"某地房价、收入、人口"三个数，长度有意义吗？
不同的量纲（元、万人）直接平方相加，明显不合理，可数学上还得算下去。
这一讲告诉你：**长度不止一种定义法，选哪种取决于你想强调什么。**

先讲清楚

## 一、三种长度：为什么会有三种

拿向量 $x=(3,4)$ 举例。三种范数算出来不一样：

| 范数 | 公式 | $x=(3,4)$ 时 |
|---|---|---|
| 1-范数 | $\|x\|_1=\Sigma\|x_i\|$ | 7 |
| **2-范数** | $\|x\|_2=\sqrt{\Sigma x_i^2}$ | 5 |
| ∞-范数 | $\|x\|_\infty=\max\|x_i\|$ | 4 |

它们只在强调不同的东西：

- **1-范数**像走街区：只能横着走竖着走，走的总路程；
- **2-范数**像走直线：两点间最短的路；
- **∞-范数**只看最大的那个分量，其它忽略。

三条要满足的规矩叫范数公理：**非负、齐次（乘倍数长度跟着变）、三角不等式**。满足这三条的都能叫范数。

## 二、距离：两个向量之差有多长

距离就是把范数用在"差"上：$d(x,y)=\|x-y\|$。

所以有三种范数，就有三种距离。聚类、分类里选哪种，会直接影响结果。

两个特殊距离要认识：**汉明距离**（不同的位数），**编辑距离**（改几个字符能变成另一个）。

## 三、相似度：只看方向，不看长短

余弦相似度：

$$\cos\theta=\frac{\langle x,y\rangle}{\|x\|_2\|y\|_2}$$

值域是 [-1,1]，1 表示同向，0 表示垂直（无关），−1 表示反向。

它的好处是**不受长度影响**：文章 A 是文章 B 的两倍长，只要用词比例一样，余弦相似度就是 1。所以文本相似度几乎都用它。

另一个常用的是**杰卡德相似度**，专用于集合：

$$J=\frac{|A\cap B|}{|A\cup B|}$$

它只看"有哪些"，不看"有多少个"。

## 四、矩阵也有范数，还多一条要求

矩阵的范数是"它能把向量放大多少倍"。除了向量那三条，还要多一条**相容性**：

$$\|Ax\| \le \|A\| \cdot \|x\|$$

意思是"乘一次矩阵，长度最多放大 $\|A\|$ 倍"。

这条要求就淘汰了一堆看起来像范数但其实是向量的东西 —— 比如 $\max|a_{ij}|$，它满足前三条，但不满足相容性，所以**不是**矩阵范数。

## 五、相似度和安全的关系

恶意代码家族分类就靠这个：把每个样本抽成"特征词集合"，两两算相似度，相似的聚成一堆，一堆就是一个家族。

这里有个坑：如果只用"出现过没有"（0/1 向量），词频信息就丢了 —— 一个词出现 1 次和 100 次被当成一样。改进办法是换成词频向量再算余弦。

> **停一下：** $x=(3,4)$ 的 1-范数、2-范数、∞-范数分别是多少？

1-范数：$3+4=7$。

2-范数：$\sqrt{9+16}=5$。

∞-范数：$\max(3,4)=4$。

关系：$4 \le 5 \le 7$，永远是 $\infty \le 2 \le 1$。

**必背 · 五条**

| | |
|---|---|
| $\|x\|_1=\Sigma\|x_i\|$ | 曼哈顿 |
| $\|x\|_2=\sqrt{\Sigma x_i^2}$ | 欧氏 |
| $\|x\|_\infty=\max\|x_i\|$ | 最大分量 |
| $\cos\theta=\frac{\langle x,y\rangle}{\|x\|\|y\|}$ | 只看方向 |
| $\|Ax\| \le \|A\|\|x\|$ | 矩阵范数多这一条 |

**课本 2-2** 6 分 判定是不是范数

$\|A\|=\max|a_{ij}|$ 是矩阵范数吗?

---

**第一步：先看它是什么。**$\max|a_{ij}|$ 是把矩阵所有元素摊平成一个长向量，取 ∞-范数。

**第二步：查向量范数的三条。**非负 ✓、齐次 ✓、三角不等式 ✓ —— 三条都过，所以它**是向量范数**。

**第三步：再查矩阵范数多出来的相容性。**要求 $\|AB\|\le\|A\|\|B\|$。

**第四步：找反例。**取 $A=B=(1,1;1,1)$。

那么 $\|A\|=1$，$\|B\|=1$；可 $AB=(2,2;2,2)$，$\|AB\|=2$。

$2>1\times1$，**相容性失败**。

**答案：不是矩阵范数，只是 $\mathbb{R}^{mn}$ 上的向量范数。**

这题教一件事：**三条公理都过，不等于就是矩阵范数**。乘法这一条才是分界线。

⚠ **三个坑：**

① **以为范数只有欧氏一种。**题目里说"某种范数"，就要考虑 1、2、∞ 三种，结论可能不同（比如怎么算距离最近）。

② **把余弦相似度和距离混用。**余弦是"越大越像"，距离是"越小越像"。混了方向就全反。

③ **忘了矩阵范数要相容性。**很多判断题就是靠这一条排除选项。

**自测 · 3 道**

1. $x=(1,2,2)$ 的 2-范数是多少?
2. 两个向量同向但长度差 10 倍，余弦相似度是多少?
3. 杰卡德相似度适合什么数据?

**1.** $\sqrt{1+4+4}=3$。

**2.** 1（余弦只看方向）。

**3.** 集合型数据，比如"包含哪些关键词"。

## ch02 · 习题 3 道

### ch02 · 2-1~2-2

○ 会　○ 卡　○ 不会

**2-1** 设 $\|\cdot\|$ 是向量范数、$P$ 非奇异，定义 $\|x\|_P=\|Px\|$，证明它也是向量范数.

**2-2** $\|A\|=\max|a_{ij}|$ 是矩阵范数吗?

---

**套路：判范数只查非负、齐次、三角三条；矩阵范数还多一条乘法相容性。**

① 2-1 非负：$\|Px\|\geq 0$，且为 0 时 $Px=0$。

② 关键：$P$ 非奇异 $\Rightarrow x=0$，非负性成立。

③ 齐次：$\|P(kx)\|=|k|\|Px\|$。

④ 三角：$\|P(x+y)\|\leq\|Px\|+\|Py\|$。

⑤ 故 $\|x\|_P$ 是向量范数，"$P$ 可逆"这一步不能省。

⑥ 2-2：$\max|a_{ij}|$ 是 $\mathrm{vec}(A)$ 的 $\infty$-范数，三条公理都过。

⑦ 关键：矩阵范数要求 $\|AB\|\leq\|A\|\|B\|$，这条会失败。

⑧ 反例：$A=B=(1,1;1,1)$，$\|A\|=\|B\|=1$。

⑨ 关键式子：$AB=(2,2;2,2)$，$\|AB\|=2>1\times 1$。

**答案：2-1 得证；2-2 不是矩阵范数（乘性失败），只是向量范数。**

**易错：非负、齐次、三角都过 ≠ 矩阵范数，乘性才是分界线。**

## ch02 · 2-3~2-5

○ 会 ○ 卡 ○ 不会

**2-3** 实现例 2.5.4，给出恶意软件家族归属.

**2-4** 用别的方法替换 Jaccard 并比较结果.

**2-5** 相同特征词只计一次是否有缺陷？给改进方案.

**套路：相似度 = 向量化 + 度量；0/1 集合配 Jaccard，词频向量配余弦。**

① 2-3：每个样本抽特征词集合 $X$，两两算相似度。

② 关键式子：$J=|X\cap Y|/|X\cup Y|$，值域 $[0,1]$，越大越像。

③ 相似矩阵做阈值或聚类，同族样本聚成一堆。

④ 注意书里把"Jaccard 指数"写成 $1-|X\cap Y|/|X\cup Y|$，那是**距离**。

⑤ 小例：$X=\{a,b,c\}$，$Y=\{b,c,d\}$，$J=2/4=0.5$。

⑥ 2-4 换余弦：集合写成 0/1 向量。

⑦ 关键式子：$\mathrm{Sim}=\dfrac{x^Ty}{\|x\|_2\|y\|_2}$。

⑧ 同例 $x=(1,1,1,0)$、$y=(0,1,1,1)$，$\mathrm{Sim}=2/3\approx0.667$。

⑨ 两法排序大体一致：余弦奖励"共同多"，Jaccard 惩罚"独有多"。

⑩ 比较方法：两套排序算秩相关（斯皮尔曼）。

⑪ 2-5 缺陷：0/1 丢掉词频，出现 1 次与 100 次同权。

⑫ 改进一：改 tf 或 tf-idf 向量再配余弦。

⑬ 改进二：加权 Jaccard，交集按 $\min$(频次) 计。

**答案：向量化决定相似度上限；重复词必须进权重。**

**易错：Jaccard 指数、距离、相似度三个名字常混，答题先写清用哪个。**

## ch02 · 2-6

○ 会 ○ 卡 ○ 不会

**2-6** 证明：秩距离满足距离的三条公理与对称性.

**套路：秩距离 $d(A,B)=\text{rank}(A-B)$；先证距离公理，再查齐次性会发现它不是范数。**

① 非负：rank 是非负整数，$d(A,A)=\text{rank}(0)=0$。

② 对称：$A-B$ 与 $B-A$ 只差 -1 倍，秩不变。

③ 三角：把 $A-B$ 拆成 $(A-C)+(C-B)$。

④ 关键式子：$\text{rank}(X+Y)\le\text{rank}X+\text{rank}Y$。

⑤ 故 $d(A,B)\le d(A,C)+d(C,B)$，可作纠错码的度量。

⑥ 但范数还要齐次性 $\|kA\|=|k|\|A\|$，这条不成立。

⑦ 关键：$k\neq0$ 时 $\text{rank}(kA)=\text{rank}(A)$，对缩放不敏感。

⑧ 反例：$A=(1,0;0,0)$，$d(2A,0)=1$ 而 $2d(A,0)=2$。

**答案：秩距离是"距离"不是"范数"；题中"范数的 3 个定义"应读作距离三公理。**

**易错：只答"满足范数定义"会被扣分，要补一句齐次性缺失。**

# 03 最优化

约 4 分 · 25 分钟

这一讲讲两件事：怎么下山，和有约束时怎么下山

> **一句话：**最优化就是"找最低点"：没约束就看梯度为零，有约束就把约束塞进目标函数。

? 你站在雾蒙蒙的山上，看不见四周，只能用脚试探坡度。
往哪走能最快到谷底？**往最陡的下坡方向走。**这就是梯度下降。
可如果山谷外有围栏，你不能乱走，怎么办？这一讲就解决这两件事。

先讲清楚

### 一、没有约束：梯度为零就是最低点

梯度是"各方向斜率组成的向量"。在最低点，往任何方向走都是上坡，所以梯度必须是零向量。

$$\nabla f(x)=0$$

解出这个方程，就得到候选极值点。但要注意：**梯度为零只是必要条件** —— 山顶、鞍点也是零。要确认是极小，还得看二阶导（或者用凸性判断）。

## 二、凸性：为什么它让事情变简单

如果函数是凸的（图像像个碗），那**局部最小就是全局最小**，不会卡在别的坑里。

判断凸的几个办法：二阶导非负；或者任取两点，连线在曲线上方。

所以做题看到"凸函数"，就可以放心：找到的那个极小点就是答案。

## 三、有等式约束：拉格朗日乘子

要最小化 $f(x)$，但 $x$ 必须满足 $g(x)=0$（比如"在圆周上"）。

办法是造一个新函数，把约束"罚"进去：

$$L(x,\lambda)=f(x)+\lambda\, g(x)$$

然后对 $x$ 和 $\lambda$ **都**求偏导，令它们为零，解方程组。

几何上是什么意思？**在最优点，$f$ 的梯度必须和约束曲面的法向量平行。**否则你还能沿着约束面再挪一点，让 $f$ 更小。$\lambda$ 就是这两个向量的比例。

> **算一个：**最小化 $f=x_1^2+x_2^2$，约束 $x_1+x_2=1$。
> $L=x_1^2+x_2^2+\lambda(x_1+x_2-1)$。
> 对 $x_1$：$2x_1+\lambda=0$；对 $x_2$：$2x_2+\lambda=0$；对 $\lambda$：$x_1+x_2-1=0$。
> 前两式给出 $x_1=x_2$，代入第三式得 $x_1=x_2=\frac{1}{2}$。
> 最小值 $f=\frac{1}{4}+\frac{1}{4}=\frac{1}{2}$，$\lambda=-1$。

## 四、不等式约束：KKT 条件

约束变成 $g(x)\le 0$ 时，情况复杂一点：约束可能**起作用**（正好卡在边界上），也可能**不起作用**（最优点在内部）。

KKT 条件把这两种情况统一写出来：

- 梯度条件：$\nabla f=\lambda\nabla g$；
- 互补松弛：$\lambda\, g(x)=0$；
- 对偶可行：$\lambda\ge 0$。

**互补松弛是最妙的一条**：如果约束没起作用（$g<0$），那 $\lambda$ 必须为 0；如果 $\lambda>0$，那约束一定卡在边界（$g=0$）。

做题时就是分情况：先假设约束不起作用（$\lambda=0$），解出来看是否满足 $g\le 0$；不满足就假设起作用（$g=0$），再解。

## 五、迭代法：梯度下降和牛顿法

实际问题很少能解析求解，都是一步一步挪：

$$x_{k+1}=x_k-\alpha\nabla f(x_k)$$

$\alpha$ 叫步长。太大了会越过谷底来回震荡，太小了走得慢。

**牛顿法**更聪明：它用二阶导（Hessian 矩阵）估计曲率，方向选得更准，通常几步就到。代价是每步要算 Hessian 的逆，计算量大。

而且牛顿法对正定二次函数**一步到位** —— 因为二次函数的曲率是常数，它一次就猜中了。

> **停一下：拉格朗日乘子 $\lambda$ 有符号限制吗?**

等式约束时 $\lambda$ 可正可负，没有限制。

不等式约束（$g \le 0$ 形式）时，KKT 要求 $\lambda \ge 0$。

这个差别常考：**等式自由，不等式非负。**

**必背 · 五条**

| | |
|---|---|
| $\nabla f = 0$ 是最优的必要条件 | 不是充分 |
| 凸 $\Rightarrow$ 局部最小即全局最小 | 碗形 |
| $L = f + \lambda g$，对两者求偏导 | 等式约束 |
| $\lambda g = 0$，$\lambda \ge 0$ | 互补松弛 |
| 牛顿法对二次函数一步到位 | 曲率是常数 |

**课本 3-3** 6 分 牛顿法的收敛

用牛顿法解 $\min f(x)=\frac{1}{2}x_1^2+\frac{9}{2}x_2^2$，比较不同初值的迭代次数。

---

**第一步：求梯度。**$\nabla f=(x_1, 9x_2)$。

**第二步：求 Hessian。**对各分量再求一次偏导：$H=(1,0;0,9)$，这里是常数矩阵。

**第三步：写牛顿迭代式。**$x\leftarrow x-H^{-1}\nabla f$。

$H^{-1}=(1,0;0,\frac{1}{9})$，所以 $H^{-1}\nabla f=(x_1, x_2)$。

**第四步：代入。**$x\leftarrow x-(x_1,x_2)=0$。

不管初值是多少，一步就跳到原点。

**第五步：换初值验证。**$(1,1)$、$(5,-3)$、$(-2,4)$ 全都一步收敛。

**第六步：说明原因。**$f$ 是正定二次函数，牛顿法用精确的曲率，所以一步到底。换成非二次函数，初值才会影响次数。

**答案：任意初值都 1 次收敛到 $(0,0)$，最小值 $f=0$。**

这题考的不是算，是"知道为什么"。答题时写一句"因为 $f$ 是正定二次函数"，比只写结果得分高。

⚠ **三个坑：**

① **以为梯度为零就是极小。**鞍点也满足。必须再看曲率或者用凸性排除。

② **拉格朗日忘了对 $\lambda$ 求导。**对 $\lambda$ 求偏导得到的就是原约束方程，少了这一条方程组不完整。

③ **不等式约束直接套等式公式。**不等式要用 KKT（带符号限制和互补松弛），不能照抄。

**自测 · 3 道**

1. 凸函数有没有可能有两个不同的局部最小?
2. 拉格朗日函数对 λ 求偏导，得到什么?
3. 牛顿法为什么对二次函数一步到位?

**1.** 不可能。凸函数的局部最小都是全局最小。

**2.** 原约束方程 $g(x)=0$。

**3.** 二次函数的 Hessian 是常数，牛顿法一次就精确猜中曲率，直接跳到极小点。

## ch03 · 习题 2 道

### ch03 · 3-1~3-2

○ 会 ○ 卡 ○ 不会

**3-1** 用雅可比与高斯-赛德尔迭代解 $(20,2,3;1,8,1;2,-3,15)x=(24,12,30)$，初值 $x^{(0)}=0$，比到 ∞-范数误差 $<10^{-6}$ 的次数.

**3-2** 生成条件数小的方程组，用负梯度法解，与两种迭代法比较.

**套路：迭代法先看严格对角占优；再比谱半径，谱半径小的一半收敛快。**

① 3-1：每行 $|a_{ii}|$ 都大于同行其余之和 ⇒ 严格对角占优，必然收敛。

② 精确解 $x\approx(0.7674,1.1384,2.1254)$。

③ 雅可比用上一轮旧值，高斯-赛德尔用刚更新的新值。

④ 关键：雅可比到第 8 次才达标，高斯-赛德尔第 6 次达标。

⑤ 谱半径 $\rho(B_J)=0.1472$、$\rho(B_{GS})=0.0565$。

⑥ 关键式子：$k\approx\dfrac{\ln 10^{-6}}{\ln\rho}$，得 7.2 与 4.8，实测各多 1 次。

⑦ 3-2：用 3-1 的矩阵，$\mathrm{cond}_2(A)\approx 2.56$，条件数很小。

⑧ 负梯度方向 $d_k=b-Ax$，精确步长 $\alpha_k=\dfrac{d_k^T d_k}{d_k^T A d_k}$。

⑨ 关键：实测要 17 次，比两种迭代法都多。

⑩ 收敛因子 $\dfrac{\lambda_{\max}-\lambda_{\min}}{\lambda_{\max}+\lambda_{\min}}\approx 0.44$。

⑪ 条件数一大，该因子趋近 1，负梯度法就慢到不可用。

**答案：雅可比 8 次、高斯-赛德尔 6 次、负梯度 17 次；快慢由谱半径与条件数决定。**

**易错：迭代次数不比未知数个数，只比谱半径。**

## ch03 · 3-3~3-5

○ 会　○ 卡　○ 不会

**3-3** 用牛顿法解 $\min f(x)=\frac{1}{2}x_1^2+\frac{9}{2}x_2^2$，比较不同初值的迭代次数.

**3-4** 生成 $10^4$ 个未知量以上的方程组，用带步长的牛顿法求解.

**3-5** 用共轭梯度法解 $(4,1,2;3,5,3;2,-3,6)x=(10,9,18)$.

**套路：牛顿法用 $H^{-1}\nabla f$ 定方向；正定二次函数一步到底；共轭梯度先验 $A$ 是否对称正定。**

① 3-3：$\nabla f=(x_1,9x_2)$，$H=(1,0;0,9)$ 恒定。

② 牛顿迭代 $x\leftarrow x-H^{-1}\nabla f=0$。

③ 关键：初值 (1,1)、(5,-3)、(-2,4) 全都一步跳到 (0,0)。

④ 因为 $f$ 是正定二次函数，牛顿方向直指极小点。

⑤ 3-4：解 $Ax=b$ 等价于 $\min\frac{1}{2}x^TAx-b^Tx$。

⑥ 大规模时每步再选步长 $\alpha_k$（精确步长或 Armijo 回溯）。

⑦ 关键式子：$\alpha_k=\frac{d_k^Td_k}{d_k^TAd_k}$。

⑧ 3-5：先验前提 —— $a_{12}=1$ 而 $a_{21}=3$，$A$ 不对称。

⑨ 关键：共轭梯度只对对称正定矩阵保证 $n$ 步精确，硬套不收敛。

⑩ 实测残差先降到 9.31 又回升到 19.2。

⑪ 正解：改解正规方程 $A^TAx=A^Tb$，它对称正定。

⑫ 关键式子：$A^TA=(29,13,29;13,35,-1;29,-1,49)$，$A^Tb=(103,1,155)$。

⑬ 三步精确收敛：$x=(78/53,-24/53,121/53)\approx(1.4717,-0.4528,2.2830)$。

**答案：牛顿 1 步到位；3-5 不能直接套，转成 $A^TA$ 后 3 步得解。**

**补充·笔试：拉格朗日 $\min x_1^2+x_2^2$ s.t. $x_1+x_2=1\Rightarrow x=(1/2,1/2)$，$\lambda=-1$。**

**KKT：$\min x_1^2+x_2^2$ s.t. $x_1+x_2\geq 2\Rightarrow x=(1,1)$，$\mu=2$，约束起作用。**

## 04 概率论

约 4 分 · 30 分钟

这一章在概率论课里学过一半，这里只补"和安全有关"的那一半

> **一句话：** 四个东西最重要：最大似然、贝叶斯、信息熵、生日悖论 —— 它们分别对应"学、判、量、撞"。

? 你可能会问：概率论我在概率课已经学过了，为什么这里还要再来一遍？
因为安全里用概率的方式不一样。这边不问"抽到红球的概率是多少"，而问"**攻击者猜中的概率有多大**"、"**这段密钥**

**有多少不确定性**"。
同一个工具，换了用途。

先讲清楚

## 一、最大似然：从数据反推参数

抛 10 次硬币出现 7 次正面，你猜正面概率是多少？多数人会说 0.7。

为什么是 0.7？因为**当 $p=0.7$ 时，"出现 7 次正面"这件事的概率最大**。这就是最大似然的思想：选那个让已发生的事最可能发生的参数。

做法固定三步：写似然（各样本概率相乘）、取对数、求导令零。

取对数是为了把乘变成加，求导方便，而且不改变极值点 —— 因为对数单调递增。

## 二、贝叶斯：看到证据后更新判断

$$P(A|B)=\frac{P(A)P(B|A)}{P(B)}$$

用人话说：**先有一个先验判断，看到证据后修正成后验判断。**

安全里最典型的例子是检测：某种攻击很少见（先验很小），但检测器有误报。检测器报警了，真被攻击的概率是多少？

算一下就发现：如果攻击本身极罕见，哪怕检测器很准，**报警里也大部分是误报**。这就是贝叶斯给人的反直觉结论。

> **算一个：**攻击发生率 1%，检测器对真攻击的检出率 99%，误报率 5%。
> 报警的总概率 $=0.01\times0.99+0.99\times0.05=0.0099+0.0495=0.0594$。
> 真被攻击的概率 $=\frac{0.0099}{0.0594}\approx0.167$。
> **也就是说，报警了也只有 16.7% 是真攻击。**

## 三、信息熵：量一量"有多不确定"

$$H(X)=-\Sigma\, p_i\log_2 p_i$$

单位是比特。它的含义是"平均需要几个二进制位才能描述这个随机变量"。

两个极端：完全确定的事件熵为 0（不用传信息）；均匀分布熵最大（$n$ 个等可能结果时是 $\log_2 n$）。

安全里它就是**密钥强度**：128 位随机密钥的熵是 128 比特，暴力破解平均要试 $2^{127}$ 次。

**注意"随机"两个字**：如果 128 位密钥里只有 40 位是真随机的，那熵只有 40 比特，剩下 88 位白给。

## 四、生日悖论：碰撞比你想的容易

23 个人里至少两人同生日的概率超过 50%。听起来不可思议，因为直觉比较的是"有人和我同生日"，而题目问的是"任意两人"。

粗略推导：$n$ 个人有 $\frac{n}{2}\approx n^2/2$ 对，每对相撞概率 $1/365$。所以

$$P\approx 1-e^{-n^2/(2\times 365)}$$

**这个结论在密码学里极重要**：哈希函数的输出有 $b$ 位，那么只要试 $2^{b/2}$ 次，就有一半概率找到碰撞。所以 128 位哈希的实际安全强度只有 64 位。

## 五、Bloom 过滤器：用概率换空间

要判断"某个元素在不在集合里"，正常做法是存下所有元素。元素多了存不下怎么办?

Bloom 过滤器用一个位数组加几个哈希函数：插入时把对应的几位置 1；查询时看那几位是不是都为 1。

它的性质很特别：**说"不在"一定对，说"在"可能是误判**。这种"允许假阳性、不允许假阴性"的结构，正好适合"先快速排除"的场景（比如查恶意 URL 黑名单）。

误判率和三个量有关：位数组长度 $m$、元素个数 $n$、哈希函数个数 $k$。

$$P\approx(1-e^{-kn/m})^k$$

> **停一下：一个公平硬币抛一次，熵是多少?**

$H=-(0.5\log_2 0.5+0.5\log_2 0.5)=1$ 比特。

含义：需要 1 个比特来描述结果，这正是"抛一次硬币产生 1 比特随机性"说法的来源。

**必背 · 五条**

| | |
|---|---|
| $L=\Pi f(x_i)$，取对数求导 | 最大似然 |
| $P(A\mid B)=\frac{P(A)P(B\mid A)}{P(B)}$ | 贝叶斯 |
| $H=-\Sigma p_i\log_2 p_i$ | 熵，单位比特 |
| 碰撞 $\approx 2^{b/2}$ 次 | 生日悖论 |
| Bloom：无假阴性，有假阳性 | 性质 |

**课本 4-4** 6 分 Bloom 过滤器容量

要求：8 个哈希函数、存 10000 个元素、假阳性率小于 0.01。位数组至少要多长?

---

**第一步：写出误判率公式并代入。**$P=(1-e^{-kn/m})^8$，要求小于 0.01，其中 $n=10000$。

**第二步：两边开 8 次方。**$1-e^{-8n/m}<0.01^{1/8}=0.56234$。

**第三步：移项。**$e^{-8n/m}>0.43766$。

**第四步：取对数。**$-8n/m>\ln 0.43766=-0.82621$，即 $\frac{8n}{m}<0.82621$。

**第五步：解出 $m$。**$m>\frac{8\times 10000}{0.82621}\approx 96815.3$，取整 **96816 位**≈12.1 KB。

**第六步：验算。**$P=(1-e^{-8/9.6816})^8\approx 0.0100$，刚好压线。

**答案：至少 96816 位，约 12.1 KB（约 9.68 位/元素）。**

有个坑：如果直接套课本那条"最优 $m$"公式，会算出 95851 位，代回去 $P\approx 0.0105$，**超标了**。因为那条公式对应的是最优 $k\approx 11.5$，不是题设的 8。

⚠ **三个坑：**

① **熵的单位。**用 $\log_2$ 是比特，用 ln 是奈特。题目问比特就必须用 $\log_2$。

② **把"检测准确率"当成"报警后真中招的概率"。**前者是 $P(\text{报警}\mid\text{攻击})$，后者是 $P(\text{攻击}\mid\text{报警})$，方向反了，数值差很远。

③ **Bloom 过滤器说"在"就以为一定在。**它是概率结构，假阳性是设计的一部分。

**自测 · 3 道**

1. $H(X)$ 最大时，分布是什么样?
2. 128 位哈希，找到碰撞大约要试多少次?
3. 贝叶斯公式的分子是什么?

**1.** 均匀分布（所有结果等可能）。

**2.** 约 $2^{64}$ 次（生日攻击，不是 $2^{128}$）。

**3.** $P(A)P(B\mid A)$，也就是"这一条路径"的概率。

## ch04 · 习题 3 道

### ch04 · 4-1

○ 会　○ 卡　○ 不会

**4-1** $X\sim U(a,b)$，$a,b$ 未知，样本 $x_1,\dots,x_k$，求 $a,b$ 的最大似然估计.

**套路：均匀分布的支撑依赖参数，不能直接求导置零；先写似然再看它随 $a,b$ 怎么变。**

① 似然 $L=(b-a)^{-k}$，当且仅当所有 $a\le x_i\le b$，否则 $L=0$。

② 样本固定后 $L$ 只随 $b-a$ 变小而变大。

③ 所以要让 $b-a$ 最小，同时还得罩住全部样本。

④ 关键：$-a$、$b$ 分别顶到样本的最小、最大值。

⑤ 答案 $\hat{a}=\min x_i$，$\hat{b}=\max x_i$（顺序统计量）。

⑥ 验算：样本 2、5、9 $\Rightarrow \hat{a}=2$、$\hat{b}=9$，$L=1/7^3$。

⑦ 取 $a=1.9$ 时 $L$ 更小，说明边界即最优。

⑧ 偏差：$E\hat{a}=a+\dfrac{b-a}{k+1}$，$E\hat{b}=b-\dfrac{b-a}{k+1}$。

⑨ 关键：两者都向内偏，故最大似然估计**有偏**。

**答案：$\hat{a}=\min x_i$、$\hat{b}=\max x_i$；它们有偏，无偏修正为 $\hat{a}-\dfrac{\hat{b}-\hat{a}}{k-1}$、$\hat{b}+\dfrac{\hat{b}-\hat{a}}{k-1}$。**

**易错：对 $(b-a)^{-k}$ 求偏导会得"无解"，支撑边界才是答案。**

## ch04 · 4-2~4-3

○ 会　○ 卡　○ 不会

**4-2** 证明差分隐私的后处理不变性.

**4-3** 随机响应改为：反面如实回答，正面再掷第二枚硬币（正=是、反=否），重新统计患病比例.

**套路：后处理不变性靠"事件的原像"；随机响应靠全概率正推、再反解真实比例。**

① 4-2：设 $A_1$ 满足 $\varepsilon$-DP，后处理为 $A_2$。

② 任取 $S$，记 $T$ 为 $S$ 在 $A_2$ 下的原像。

③ 关键式子：$P[A_2(A_1(D)) \in S]=P[A_1(D) \in T]$。

④ 由 DP：$P[A_1(D) \in T] \le e^{\varepsilon} P[A_1(D') \in T]$。

⑤ 换回 $S$ 即得同形式界，$\varepsilon$ 不变，证毕。

⑥ 结论：加噪之后再怎么算都不额外泄隐私。

⑦ 4-3：记真实患病率 $p$，用全概率拆两路。

⑧ 关键式子：$P(\text{答是}|\text{患病})=\frac{1}{2}\cdot 1+\frac{1}{2}\cdot\frac{1}{2}=\frac{3}{4}$。

⑨ 关键式子：$P(\text{答是}|\text{非患病})=\frac{1}{4}$。

⑩ 观测比例 $q$ 满足 $q=\frac{3}{4}p+\frac{1}{4}(1-p)=\frac{p}{2}+\frac{1}{4}$。

⑪ 反解 $p=2q-\frac{1}{2}$。

⑫ 后验：$P(\text{患病}|\text{答是})=\frac{3p}{2p+1}$。

⑬ 隐私预算 $\varepsilon=\ln\frac{3/4}{1/4}=\ln 3\approx 1.10$。

**答案：$\hat{p}=2q-\frac{1}{2}$，后验 $\frac{3p}{2p+1}$，$\varepsilon=\ln 3\approx 1.10$。**

**易错：$\hat{p}$ 算出负数或超过 1 是样本量不够，要截断，不能硬报。**

## ch04 · 4-4

○ 会　○ 卡　○ 不会

**4-4** 设计 Bloom 过滤器：8 个散列函数、存 10000 个元素、假阳性率 <0.01，长度至少多少?

**套路：误判率 $P=(1-e^{-kn/m})^k$；代 $k,n$ 解 $m$，别直接套那条最优 $m$ 公式。**

① 已知 $n=10000$，$k=8$，要求 $P<0.01$。

② 两边开 8 次方：$1-e^{-8n/m}<0.01^{1/8}=0.56234$。

③ 关键：$e^{-8n/m}>0.43766 \Rightarrow \dfrac{8n}{m}<0.82621$。

④ 得 $m>\dfrac{8\times10000}{0.82621}\approx96815.3$。

⑤ 答案：$m=96816$ 位 ≈ 12102 字节 ≈ 11.8 KB，约 9.68 位/元素。

⑥ 验算：$P=(1-e^{-8/9.6815})^8\approx0.0100$。

⑦ 若直接套 $m=-\dfrac{n\ln P}{(\ln2)^2}=95851$ 位，回代 $P\approx0.01053$，**超标**。

⑧ 原因：那条公式对应 $k=(m/n)\ln2\approx11.5$，不是题设的 8。

⑨ 对照表 4.4.1：$m/n=10$、$k=8$ 时 $P=8.46\times10^{-3}$。

**答案：$m\geq96816$ 位（约 11.8 KB）；取 $10^5$ 位时 $P\approx8.5\times10^{-3}$。**

**易错：Bloom 只答"不在"可信，"在"有假阳性；$m$ 用位算，换字节除 8。**

05

# 马尔可夫链与 PageRank

约 4 分 · 30 分钟

这一讲从"网页怎么排序"讲到"稳态分布怎么算"

**一句话：**马尔可夫链就是"下一步只看现在"；走久了各状态占比不再变，那个占比就是稳态分布。

?

1998 年，两个学生要解决一个问题：**网页这么多，怎么排先后?**
他们的想法很妙：把网页看成状态，链接看成"跳转概率"，然后算"随机点链接点久了，会停在哪个页面"。**停得多的页面就重要。**
这就是 PageRank，它背后的数学就是马尔可夫链的稳态分布。

先讲清楚

### 一、什么叫"下一步只看现在"

抛硬币没有记忆，每次都是 1/2。可天气有记忆：昨天晴，今天多半还晴。

马尔可夫性说的是：**只要知道现在，过去怎么样都无所谓。**天气模型里就是"今天是晴是雨"决定明天的概率，不用管前天。

写成式子：$P(X_{n+1}|\ X_n,X_{n-1},\ldots)=P(X_{n+1}|\ X_n)$。

## 二、转移矩阵：把概率排成表

把"从状态 $i$ 一步走到状态 $j$ 的概率"放在第 $i$ 行第 $j$ 列，就得到转移矩阵 $P$。

**每一行加起来必须等于 1** —— 因为从某个状态出发，下一步总要去某个地方。这条是自检点，算完一定要查。

| P | 晴 | 雨 |
|---|---|---|
| 晴 | 0.7 | 0.3 |
| 雨 | 0.4 | 0.6 |

读法：今天晴，明天晴的概率 0.7；今天雨，明天晴的概率 0.4。

## 三、稳态分布：走很久之后的比例

假设长期来看，晴天占的比例是 $\pi_1$、雨天 $\pi_2$。那么"明天晴"的比例应该等于"今天晴且明天晴"加上"今天雨且明天晴"：

$$\pi_1=0.7\pi_1+0.4\pi_2$$

写成矩阵形式就是

$$\pi\ P=\pi，\ 且\ \Sigma\pi_i=1$$

解这个方程组就得到稳态分布。

> **解上面那个天气模型：**
>
> 由 $\pi_1=0.7\pi_1+0.4\pi_2$ 得 $0.3\pi_1=0.4\pi_2$，即 $\pi_1=\frac{4}{3}\pi_2$。
>
> 加上 $\pi_1+\pi_2=1$：$\frac{4}{3}\pi_2+\pi_2=1 \Rightarrow \pi_2=\frac{3}{7}$，$\pi_1=\frac{4}{7}$。
>
> 所以长期看，约 57% 是晴天。
>
> 验算：$(\frac{4}{7},\frac{3}{7})P=(\frac{4}{7},\frac{3}{7})$ ✓

## 四、什么时候稳态一定存在

不是所有链都有唯一的稳态。三个条件要认识：

| 性质 | 含义 |
|---|---|

| | |
|---|---|
| **不可约** | 任意两个状态能互相到达 |
| **非周期** | 返回自身的步数没有大于 1 的公约数 |
| **正常返** | 平均返回时间是有限的 |

三个都满足叫**遍历**，此时稳态分布存在且唯一，而且和初始状态无关。**这正是 PageRank 能用的前提。**

怎么判断非周期？最简单的信号是**有没有自环** —— 某个状态能以正概率留在原地，通常就非周期了。

## 五、PageRank 的两个补丁

直接把网页链接当转移矩阵，会出两个问题：

- **悬挂点**：有些页面没有任何出链，那一行全是 0，不是合法转移矩阵；
- **陷阱**：有些页面只指向自己，随机游走会卡死在那里。

解决办法是加一个"随机跳转"：以概率 $d$ 沿链接走，以概率 $1\text{-}d$ 随机跳到任意页面。

$$\pi = d\,\pi P + \frac{1\text{-}d}{N}\mathbf{1}$$

常用的 $d=0.85$。这个补丁让矩阵变成不可约且非周期，稳态就一定存在了。

> 停一下：转移矩阵 $P=\left(\frac{1}{2},\frac{1}{2};\frac{1}{4},\frac{3}{4}\right)$ 的稳态分布是多少？

列方程：$\pi_1=\frac{1}{2}\pi_1+\frac{1}{4}\pi_2$，得 $\frac{1}{2}\pi_1=\frac{1}{4}\pi_2$，即 $\pi_2=2\pi_1$。

加归一：$\pi_1+2\pi_1=1 \Rightarrow \pi_1=\frac{1}{3}$，$\pi_2=\frac{2}{3}$。

验算：$\left(\frac{1}{3},\frac{2}{3}\right)P=\left(\frac{1}{3},\frac{2}{3}\right)$ ✓

**必背 · 五条**

| | |
|---|---|
| 转移矩阵每行和为 1 | 自检点 |
| $\pi P=\pi,\ \Sigma\pi=1$ | 稳态方程 |
| 不可约 + 非周期 ⇒ 稳态唯一 | 遍历 |
| 有自环通常非周期 | 判断技巧 |
| $\pi=0.85\pi P+0.15/N$ | PageRank |

**课本 5-5** 6 分 判遍历并求极限分布

转移矩阵 $P=(0,\frac{3}{4},\frac{1}{4};\frac{1}{4},0,\frac{3}{4};\frac{1}{4},\frac{1}{4},\frac{1}{2})$。判断是否遍历，若是求极限分布。

---

**第一步：查行和。**三行都是 1 ✓，是合法转移矩阵。

**第二步：查不可约。**从 0 能到 1、2；从 1 能到 0、2；从 2 能到 0、1。任意两状态互通 ⇒ **不可约。**

**第三步：查周期。**状态 2 有自环（$P_{22}=\frac{1}{2}>0$），返回自身的步数里含 1，最大公约数是 1 ⇒ **非周期。**

有限 + 不可约 + 非周期 ⇒ **遍历**，极限分布存在且唯一。

**第四步：列稳态方程。**

$$\pi_0=\frac{1}{4}\pi_1+\frac{1}{4}\pi_2$$
$$\pi_1=\frac{3}{4}\pi_0+\frac{1}{4}\pi_2$$
$$\pi_2=\frac{1}{4}\pi_0+\frac{3}{4}\pi_1+\frac{1}{2}\pi_2$$

**第五步：解。**第三个方程其实是重复的（行和为 1 导致），用前两个配归一条件。

由第一式 $\pi_0=\frac{1}{4}(\pi_1+\pi_2)$；再代入 $\pi_0+\pi_1+\pi_2=1$ 得 $\pi_0=\frac{1}{5}$、$\pi_1=\frac{7}{25}$、$\pi_2=\frac{13}{25}$。

**第六步：验算。**$\pi P=(\frac{1}{5},\frac{7}{25},\frac{13}{25})$，与 $\pi$ 相同 ✓

**答案：遍历；极限分布 $(0.2, 0.28, 0.52)$，与初始分布无关。**

实际做题时，稳态方程里有一个是多余的，**永远用前两个加归一条件**就够了。

⚠ **三个坑：**

① **以为所有链都有稳态。**可约（有吸收态）或者周期性的链，极限分布可能不存在或者依赖初值。

② **把稳态方程全用上。**三个方程里必有一个冗余，全用会解出无穷多解。**丢掉一个，补归一条件。**

③ **PageRank 忘了随机跳转项。**$d=1$ 时遇到悬挂点会卡死，算出来的分布没有意义。

**自测 · 3 道**

1. 转移矩阵的行和是多少?
2. 有自环说明链是什么性质?
3. PageRank 里 $d=0.85$ 表示什么?

**1.** 每行都是 1。

**2.** 通常非周期（返回步数含 1）。

**3.** 有 85% 的概率沿链接走，15% 随机跳到任意页面。

## ch05 · 习题 3 道

### ch05 · 5-1~5-3

○ 会　○ 卡　○ 不会

**5-1** 抛硬币定义随机过程：$H$ 时 $X(t)=\cos\pi t$，$T$ 时 $X(t)=2t$，各 $1/2$。求 (1) $F(x;1/2)$、$F(x;1)$；(2) 二维 $F(x_1,x_2;1/2,1)$.

**5-3** 把随机游动的反射壁改为吸收壁，分析互通性.

**套路：随机过程的一维分布 = 固定 $t$ 后的随机变量分布；先算两个取值，再摆台阶。**

① 5-1：$t$ 固定时 $X(t)$ 只取两个值，各 $1/2$。

② $t=\frac{1}{2}$：$\cos\frac{\pi}{2}=0$，$2t=1$，原子在 0 和 1。

③ 关键：$F(x;\frac{1}{2})=0$（$x<0$）、$\frac{1}{2}$（$0\le x<1$）、$1$（$x\ge1$）。

④ $t=1$：$\cos\pi=-1$，$2t=2$，原子在 -1 和 2。

⑤ 关键：$F(x;1)=0$（$x<-1$）、$\frac{1}{2}$（$-1\le x<2$）、$1$（$x\ge2$）。

⑥ 二维：两个时刻由同一枚硬币决定，联合只有两个原子。

⑦ 关键：$(0,-1)$ 与 $(1,2)$ 各占 $\frac{1}{2}$。

⑧ 故 $F=\frac{1}{2}$（$x_1\ge0$ 且 $x_2\ge-1$），再加 $\frac{1}{2}$（$x_1\ge1$ 且 $x_2\ge2$）。

⑨ 检验：$F(1,2)=1$、$F(0,-1)=\frac{1}{2}$、$F(0,2)=\frac{1}{2}$。

⑩ 5-3：反射壁把撞壁质点弹回，链保持不可约。

⑪ 关键：改吸收壁后撞壁即停，再也出不来。

⑫ 故吸收态自成一类（常返），其余状态互通但都是瞬态。

**答案：反射壁——全体互通、不可约；吸收壁——可约，只有吸收态常返。**

**易错：出现吸收态后"不可约"与"遍历"一起失效，但"常返"对吸收态仍成立。**

## ch05 · 5-4

○ 会　○ 卡　○ 不会

**5-4** 粒子在整数轴上走：奇数位下一时刻去偶数位；偶数位以概率 $w$ 去另一个偶数位，否则去一个奇数位。建 2 状态链：(a) 转移矩阵；(b) $w$ 何值时非周期正常返；(c) 在偶数位的概率.

---

**套路：两状态就写 2×2 按行矩阵；非周期看能否停留，正常返看有限且不可约。**

① 状态只记奇偶：$E$ 偶数位，$O$ 奇数位。

② $E\to E$ 概率 $w$，$E\to O$ 概率 $1\text{-}w$。

③ $O\to E$ 概率 1，$O\to O$ 概率 0。

④ 关键式子：$P=(w,1\text{-}w;1,0)$。

⑤ 互通：$w>0$ 时 $E\to O$，$O\to E$ 恒成立 ⇒ 同类。

⑥ 周期：$E$ 可一步回 $E$ ⇒ 返回步长最大公约数为 1。

⑦ 关键：有限 + 不可约 + 非周期 ⇒ 正常返且遍历。

⑧ 答案 (b)：$w\in(0,1)$；$w=0$ 或 1 时退化、可约。

⑨ 平稳方程 $p_E=wp_E+p_O$，加归一。

⑩ 关键式子：$p_E=\dfrac{1}{2\text{-}w}$。

⑪ 验算：$w=\dfrac{1}{2}$ 时 $p=(\dfrac{2}{3},\dfrac{1}{3})$，$pP=p$ ✓。

⑫ 直观：$w$ 越大越"赖在偶数位"，$p_E$ 越大。

**答案：(a) $P=(w,1\text{-}w;1,0)$；(b) $0<w<1$；(c) $p_E=\dfrac{1}{2\text{-}w}$。**

**易错：状态少也要查周期，有自环才可能非周期。**

## ch05 · 5-5

○ 会 ○ 卡 ○ 不会

**5-5** 转移图：$0\to1$ 为 $\frac{3}{4}$、$0\to2$ 为 $\frac{1}{4}$；$1\to0$ 为 $\frac{1}{4}$、$1\to2$ 为 $\frac{3}{4}$；$2\to0,2\to1$ 各 $\frac{1}{4}$、$2\to2$ 为 $\frac{1}{2}$。写转移矩阵，判遍历性，求极限分布.

**套路：按行抄图得 $P$；查不可约 + 非周期；再解 $pP=p$ 与 $\Sigma p=1$。**

① 一行对应出发状态，列对应到达状态。

② 关键式子：$P=(0,\frac{3}{4},\frac{1}{4};\frac{1}{4},0,\frac{3}{4};\frac{1}{4},\frac{1}{4},\frac{1}{2})$。

③ 三行和都是 1 ⇒ 是随机矩阵。

④ 不可约：0 与 1、2 双向可达，三状态同类。

⑤ 非周期：状态 2 有自环 $\frac{1}{2}$，返回步长含 1。

⑥ 关键：有限 + 不可约 + 非周期 ⇒ 遍历。

⑦ 平稳方程 $p_0=\frac{p_1+p_2}{4}$、$p_1=\frac{3p_0+p_2}{4}$，加归一。

⑧ 关键式子：$p=(\frac{1}{5},\frac{7}{25},\frac{13}{25})=(0.2,0.28,0.52)$。

⑨ 验算：$pP=p$ ✓，故极限分布就是 $p$，与初值无关。

⑩ PageRank：解 $p=0.85pP+0.15\times(\frac{1}{3},\frac{1}{3},\frac{1}{3})$。

⑪ 关键：幂迭代不动点 $p\approx(0.2165,0.2924,0.4911)$。

⑫ 阻尼把分布往均匀拉：小概率状态被抬高，大的被压低。

**答案：$P$ 如上，链遍历，极限分布 $(0.2,0.28,0.52)$；阻尼 0.85 的 PageRank 约 $(0.216,0.292,0.491)$。**

**易错：PageRank 的基准是全 $\frac{1}{3}$ 均匀分布；$d=1$ 且有悬挂点时幂迭代会失真。**

## 06 整除、最大公因子与欧几里得算法

约 12 分 · 45 分钟

考：一道 10 分左右的解答题（求 gcd 并表成线性组合）；后面每一讲的运算基础

> **一句话：**求两个大数的最大公因子，**不需要分解质因数**，只要反复"大数除以小数取余数"，最后一个非零余数就是答案。

? 先看一道具体的：**1234 和 981 的最大公因子是多少?**
如果你打算分解质因数，会发现 1234 = 2×617，617 是不是素数还得试除一堆数 —— **很麻烦，而且容易错。**

有个办法完全不用分解，只要会做小学除法。这一讲就讲它。

先讲清楚

## 一、整除：先把话说清楚

说"$a$ 整除 $b$"，意思是**$b$ 除以 $a$ 恰好除尽，没有余数**。写成 $a \mid b$。

严格一点：存在整数 $k$，使 $b=ak$。

举三个例子就明白了：

- $3 \mid 99$，因为 $99=3\times33$；
- $7 \nmid 100$，因为 $100=7\times14+2$，多出个 2；
- **任何整数都整除 0**，因为 $0=a\times0$。这条最容易忽略，但课后题里出现了。

## 二、带余除法：所有运算的地基

对整数 $a$ 和正整数 $m$，一定**唯一**存在两个数 $q$（商）、$r$（余数）满足

$$a=qm+r，且\ 0\le r<m$$

"唯一"这两个字很关键：余数被定死了，才能拿它去做运算、去比较。

**为什么余数一定要落在 $[0,m)$？** 看这个例子就懂：

17 除以 5，可以写成 $17=3\times5+2$（余 2），也可以写成 $17=2\times5+7$（"余 7"）。

如果不规定余数小于除数，"余数"就有无穷多种写法。所以约定**余数必须小于除数**，答案才唯一。

> **负数是最容易翻车的地方，单拎出来说：**
> $-7$ 除以 3。你可能顺手写 $-7=(-2)\times3-1$，"余 $-1$" —— **错**，因为 $-1$ 不在 $[0,3)$ 里。
> 正确写法：$-7=(-3)\times3+2$，**余数是 2**。
> 检查一下：$(-3)\times3+2=-9+2=-7$ ✓。所以 $(-7) \bmod 3=2$，不是 $-1$。

## 三、最大公因子

$(a,b)$ 表示 $a$ 和 $b$ 的**最大公因子**：能同时整除两者的数里最大的那个。

例：$(15,35)=5$ —— 公因子只有 1 和 5，最大的是 5。

几个特殊情形，选择题爱考：

| 式子 | 为什么 |
| --- | --- |
| $(a,0)=\lvert a\rvert$ | 能整除 $a$ 和 0 的最大数就是 $a$ 本身 |

| | |
|---|---|
| $(a,a+1)=1$ | 公因子要整除两者之差 $(a+1)-a=1$ |
| $(a,1)=1$ | 1 只有因子 1 |

## 四、欧几里得算法：不用分解的求 gcd 法

整件事只靠一个等式：

$$(a,b)=(b,\ a \bmod b)$$

**为什么可以这样换？**设 $a=qb+r$。任何一个能同时整除 $a$ 和 $b$ 的数，也一定能整除 $r=a-qb$；反过来，能整除 $b$ 和 $r$ 的数，也能整除 $a=qb+r$。

**所以两边的公因子集合完全一样，最大公因子当然也一样。**而右边的两个数变小了，可以一直换下去，直到余数为 0。

> **手算 $(1234,981)$，考试就按这个竖式写（每一行都是给分点）：**
> $1234=1\times981+253$
> $981=3\times253+222$
> $253=1\times222+31$
> $222=7\times31+5$
> $31=6\times5+1$
> $5=5\times1+0$ ← 余数 0，**停**
> 最后一个非零余数是 **1**，所以 $(1234,981)=1$，两个数互素。

## 五、扩展欧几里得：把 gcd 写成"原数的组合"

贝祖定理说：一定存在整数 $x,y$，使

$$ax+by=(a,b)$$

它有什么用？**求模逆元全靠它**（下一讲就会用到）。

怎么求？**从最后一步倒着往回代**，每一步都把余数写成"上一行的两个数相减"。

> **接着上面的算式，求 $1234x+981y=1$：**
> 从 $31=6\times5+1$ 反解：$1=31-6\times5$
> 把 $5=222-7\times31$ 代进去：$1=31-6(222-7\times31)=43\times31-6\times222$
> 把 $31=253-222$ 代进去：$1=43(253-222)-6\times222=43\times253-49\times222$
> 把 $222=981-3\times253$ 代进去：$1=190\times253-49\times981$
> 把 $253=1234-981$ 代进去：$1=190\times1234-239\times981$
> 所以 $x=190$，$y=-239$。**验算：$190\times1234-239\times981=234460-234459=1$ ✓**




图 1：同一个竖式，第 ② 步读出 gcd，第 ③ 步读出逆元。

**必背 · 六条**

| | |
|---|---|
| $a=qm+r,\ 0\le r<m$ | 带余除法，余数唯一 |
| $a\mid b\Leftrightarrow b=ak$ | 整除的定义 |
| $(a,b)=(b,a \bmod b)$ | 欧几里得的核心 |
| $ax+by=(a,b)$ | 贝祖等式，倒代求 |
| $(a,0)=\lvert a\rvert$ | 常考特例 |
| $(a,a+1)=1$ | 相邻必互素 |

**课本 6-22** 10 分 欧几里得 + 线性组合

求 (981,1234)，并把最大公因子表示成这两个数的线性组合。

---

**第一步：把除法竖式写全，一直除到余数为 0。**

1234=1×981+253
981=3×253+222
253=1×222+31
222=7×31+5
31=6×5+1
5=5×1+0

**第二步：读答案。**最后一个非零余数是 1，所以 (981,1234)=1。

**第三步：倒着回代，每一步只做"代入 + 合并"。**

1=31-6×5
=31-6(222-7×31)=43×31-6×222
=43(253-222)-6×222=43×253-49×222
=43×253-49(981-3×253)=190×253-49×981
=190(1234-981)-49×981=190×1234-239×981

**第四步：验算。**190×1234=234460，239×981=234459，差正好是 1。

**答案：(981,1234)=1=190×1234-239×981。**

这题如果换成 (666,1414)，做法一模一样，只是回代长一点。**格式比速度重要：竖式写全，回代一步不跳。**

⚠ **三个坑：**
① **负数余数写成负的。**$-7 \bmod 3=2$，不是 -1。规则是"余数永远落在 $[0,m)$"。
② **回代跳步。**每一步都要写出"余数 = 上一行两个数相减"，跳一步后面就接不回去了。老师看的正是这一步。
③ **把 $x$、$y$ 配错。**最后写成 $ax+by$ 时，$x$ 对应第一个数。所以 (981,1234) 的答案写成 190×1234-239×981，或者等价地 -239×981+190×1234。

**自测 · 3 道**

1. -17 模 5 的余数是多少?
2. 用欧几里得算 $(72,30)$。
3. $(a,0)$ 等于多少?

**1.** 先试 $-17=(-3)\times5+?$，得余 $2$。所以答案是 **2**。

**2.** $72=2\times30+12$，$30=2\times12+6$，$12=2\times6+0 \Rightarrow$ **6**。

**3.** $|a|$。因为任何数都能整除 0。

## ch6 · 习题 6 道

### ch6 · 6-1~6-7

○ 会　○ 卡　○ 不会

**6-1** 证明：每个奇整数的平方具有形式 $8k+1$.

**6-2** 证明：3 整除 99，1001 可以被 7，11 和 13 整除.

**6-3** 给出除数为 17、被除数为 289 时带余数除法的商和余数.

**6-4** 若非零整数 $a$、$b$ 满足 $a \mid b$ 且 $b \mid a$，可得何结论?

**6-5** 给出 100 至 1000 之间被 7 整除的整数的个数.

**6-6** 给出不超过 1000 且不被 3 和 5 整除的正整数的个数.

**6-7** 证明：若 $a$ 是整数，则 3 整除 $a^3-a$.

---

**套路：整除靠变形凑因子，计数靠带余数除法。**

① 6-1：设奇整数 $a=2m+1$，则 $a^2=4m(m+1)+1$。

② 相邻两整数之积 $m(m+1)$ 必为偶数，令其为 $2k$。

③ 关键式子：$a^2=8k+1$；验算 $7^2=49=8\times6+1$。

④ 6-2：$99=3\times33$；$1001=7\times11\times13$（$77\times13=1001$）。

⑤ 6-3：$289=17\times17+0$，商 17、余 0（且余数小于除数）。

⑥ 6-4：设 $b=ac$、$a=bd$，约去 $a$ 得 $cd=1$。

⑦ 关键式子：$cd=1$ 只有 $c=d=\pm1$，故 $a=b$ 或 $a=-b$。

⑧ 6-5：下端 $7\times15=105$，上端 $7\times142=994$。

⑨ 关键式子：个数 $142-15+1=128$。

⑩ 6-6：3 的倍数 $\lfloor1000/3\rfloor=333$，5 的倍数 200，15 的倍数 66。

⑪ 关键式子：$1000-333-200+66=533$。

⑫ 6-7：$a^3-a=(a-1)a(a+1)$ 是三个连续整数之积。

⑬ 三个连续整数中必有一个被 3 整除，故 $3 \mid a^3-a$。

**答案：6-1 得证；6-2 得证；6-3 商 17 余 0；6-4 $a=\pm b$；6-5 共 128 个；6-6 共 533 个；6-7 得证。**

## ch6 · 6-8~6-10

○ 会　○ 卡　○ 不会

**6-8** 将 $(10101111)_2$ 转成十进制，并将 $(1984)_{10}$ 转成二进制.

**6-9** 将 $(89156)_{10}$ 转成八进制，并将 $(706113)_8$ 转成十进制.

**6-10** 已知 $n=(a_k a_{k-1}\cdots a_1 a_0)_b$，给出 $b^m n$ 的 $b$ 进制展开式.

---

**套路：转 $b$ 进制就反复除 $b$ 取余倒读，反向按权展开求和。**

① 6-8：$(10101111)_2=128+32+8+4+2+1$。

② 关键式子：$=175$。

③ 1984 反复除 2，余数依次 0,0,0,0,0,0,1,1,1,1,1。

④ 关键式子：倒读得 $(11111000000)_2$，验算 $1984=1024+512+256+128+64$。

⑤ 6-9：89156→11144 余 4，→1393 余 0，→174 余 1，→21 余 6，→2 余 5，→0 余 2。

⑥ 关键式子：倒读得 $(256104)_8$。

⑦ 反向展开：$7\times8^5+0+6\times8^3+1\times8^2+1\times8+3$。

⑧ 关键式子：$229376+3072+64+8+3=232523$。

⑨ 6-10：$n=a_k b^k+\cdots+a_0$，两边同乘 $b^m$。

⑩ 关键式子：$b^m n=(a_k\cdots a_0 0\cdots 0_{m个})_b$。

⑪ 验算：$(101)_2=5$，乘 $2^2=4$ 得 $20=(10100)_2$，正好补两个 0。

**答案：6-8 为 175 与 $(11111000000)_2$；6-9 为 $(256104)_8$ 与 232523；6-10 在末尾添 $m$ 个 0。**

## ch6 · 6-11~6-16

○ 会　○ 卡　○ 不会

**6-11** 求最大公因子：(1) 15,35；(2) 0,111；(3) 5,25,75；(4) 99,9999,0.

**6-12** $a$ 为正整数，求 $(a,2a)$、$(a,a^2)$、$(a,a+1)$.

**6-13** 证明 $(ca,cb)=|c|(a,b)$.

**6-14** 证明：$(a,b)=1$ 时 $(a-b,a+b)=1$ 或 2.

**6-15** 证明：$a,b$ 为偶数且不全零时 $(a,b)=2(a/2,b/2)$.

**6-16** 证明：$a$ 偶 $b$ 奇时 $(a,b)=(a/2,b)$.

---

**套路：计算题先分解，证明题让公因数去整除线性组合。**

① 6-11：$(15,35)=5$；$(0,111)=111$；$(5,25,75)=5$；$9999=99\times101 \Rightarrow (99,9999,0)=99$。

② 6-12：$a\mid 2a$、$a\mid a^2 \Rightarrow$ 前两个都是 $a$。

③ 关键式子：$(a,a+1)\mid(a+1)-a=1 \Rightarrow (a,a+1)=1$。

④ 6-13：设 $d=(a,b)$，由贝祖定理 $d=ma+nb$。

⑤ 关键式子：$cd=m(ca)+n(cb)$，且 $cd\mid ca$、$cd\mid cb$。

⑥ 故 $(ca,cb)=|cd|=|c|(a,b)$；验算 $a=6,b=15,c=-4$ 得 12。

⑦ 6-14：设 $d=(a-b,a+b)$，两式相加相减得 $d\mid 2a$、$d\mid 2b$。

⑧ 关键式子：$d\mid(2a,2b)=2(a,b)=2$，故 $d\in\{1,2\}$。

⑨ 一奇一偶时都为奇 $\Rightarrow d=1$；同奇或同偶时 $\Rightarrow d=2$。

⑩ 6-15：$a=2a_1,b=2b_1$，套 6-13 取 $c=2$。

⑪ 关键式子：$(a,b)=2(a_1,b_1)=2(a/2,b/2)$；验算 $(6,9)=3=2\times(3,4)$? 不对，取 $a=6,b=9$ 时右端为 $2\times(3,4.5)$ 不合适，改用 $a=8,b=12$：$(8,12)=4=2(4,6)$ ✓。

⑫ 6-16：设 $d=(a,b)$，$d\mid b$ 且 $b$ 奇 $\Rightarrow d$ 奇 $\Rightarrow (d,2)=1$。

⑬ 由 $d\mid 2\cdot\dfrac{a}{2}$ 且 $(d,2)=1$ 得 $d\mid\dfrac{a}{2}$。

⑭ 关键式子：$(\dfrac{a}{2},b)\mid\dfrac{a}{2}\mid a$ 且整除 $b \Rightarrow$ 它整除 $d$，两边相等。

⑮ 验算：$(12,9)=3=(6,9)$；$(8,15)=1=(4,15)$。

**答案：6-11 依次 5、111、5、99；6-12 依次 $a$、$a$、1；6-13~6-16 均得证。**

## ch6 · 6-17~6-21

○ 会　○ 卡　○ 不会

**6-17** 证明：$(a,b)=1$ 且 $c\mid(a+b)$ 时 $(c,a)=(c,b)=1$.

**6-18** 证明：$(a,b,c)=1$ 时 $(a,bc)=(a,b)(a,c)$.

**6-19** 证明：$(a,b)=(a,c)=1$ 时 $(a,bc)=1$.

**6-20** 用归纳法证明：$(a_i,b)=1$ 对每个 $i$ 成立时 $(a_1\cdots a_n,b)=1$.

**6-21** 证明：$(ca_1,\ldots,ca_n)=c(a_1,\ldots,a_n)$.

**套路：互素判定三招——贝祖乘式、整除传递、素因子指数。**

① 6-17：令 $d=(c,a)$，则 $d\mid c$、$d\mid a$。

② 由 $c\mid(a+b)$ 得 $d\mid(a+b)$，又 $d\mid a\Rightarrow d\mid b$。

③ 关键式子：$d\mid(a,b)=1\Rightarrow d=1$；同法 $(c,b)=1$。

④ 6-18：设素数 $p$ 在 $a,b,c$ 中的指数为 $r,s,t$。

⑤ 关键式子：$\min(r,s+t)=\min(r,s)+\min(r,t)$，逐素数比较即得。

⑥ 验算 $a=6,b=10,c=15$：$(6,150)=6=2\times3$ ✓。

⑦ 6-19：把 $au+bv=1$ 与 $as+ct=1$ 相乘。

⑧ 关键式子：展开得 $a(\cdot)+bc(vt)=1\Rightarrow(a,bc)=1$。

⑨ 6-20：归纳，设 $(A,b)=1$ 且 $A=a_1\cdots a_k$。

⑩ 由 $(a_{k+1},b)=1$ 与 6-19 得 $(Aa_{k+1},b)=1$，归纳完成。

⑪ 6-21：$(x_1,\ldots,x_n)$ 是整系数组合中最小的正整数。

⑫ 全体同乘 $c>0$，最小正整数也乘 $c$，得证。

**答案：五题结论均成立；6-18、6-19 靠 6-19 的贝祖乘式，6-20 再传成归纳。**

## ch6 · 6-22~6-23

○ 会　○ 卡　○ 不会

**6-22** 用欧几里得算法求 gcd 并表示为线性组合：(1) (45,75) (2) (666,1414) (3) (981,1234).

**6-23** 求下列整数组的 gcd 并表为线性组合：(1) 6,10,15 (2) 15,35,90 (3) 70,98,105 (4) 300,2160,5040.

**套路：辗转相除取最后一个非零余数，再自下而上回代成 $ax+by$。**

① 6-22(1)：$75=1\times45+30$，$45=1\times30+15$，$30=2\times15$。

② 回代：$15=45-30=2\times45-75$。

③ (2)：$1414=2\times666+82$，$666=8\times82+10$，$82=8\times10+2$。

④ 关键式子：$2=65\times1414-138\times666$。

⑤ (3)：$1234=981+253$，$981=3\times253+222$，$253=222+31$。

⑥ $222=7\times31+5$，$31=6\times5+1$，gcd 为 1。

⑦ 关键式子：$1=190\times1234-239\times981$（验算 $190\times1234=234460$）。

⑧ 6-23：多整数先两两合并，$(a,b,c)=((a,b),c)$。

⑨ (1) $2\times6-10=2$，又 $15-7\times2=1$。

⑩ 关键式子：$1=-14\times6+7\times10+15$。

⑪ (2) $35-2\times15=5$，且 $90=18\times5 \Rightarrow$ gcd 5。

⑫ (3) $3\times70-2\times98=14$，$105-7\times14=7$。

⑬ 关键式子：$7=105-21\times70+14\times98$。

⑭ (4) $2160-7\times300=60$，且 $5040=84\times60$。

**答案：(45,75)=15；(666,1414)=2；(981,1234)=1；(6,10,15)=1；(15,35,90)=5；(70,98,105)=7；(300,2160,5040)=60，各线性组合见上。**

## ch6 · 6-24~6-26

○ 会　○ 卡　○ 不会

**6-24** 素分解：(1) 36 (2) 222 (3) 256 (4) 989 (5) 9999 (6) 100000 (7) 111111.

**6-25** 求 gcd 与 lcm：(1) $2\cdot3^2\cdot5^3$ 与 $2^2\cdot3^3\cdot7^2$ (2) $2\cdot3\cdot5\cdot7$ 与 $7\cdot11\cdot13$ (3) $2^8\cdot3^6\cdot5^4\cdot11^{13}$ 与 $2\cdot3\cdot5\cdot11\cdot13$ (4) $41^{101}47^{43}103^{1001}$ 与 $41^{11}43^{47}83^{111}$.

**6-26** 给出 gcd 为 18、lcm 为 540 的整数对.

---

**套路：素分解后 gcd 取小指数、lcm 取大指数，再用 gcd·lcm=ab 验算。**

① 6-24：$36=2^2\cdot3^2$，$222=2\cdot3\cdot37$，$256=2^8$。

② $989=23\times43$（回乘 $23\times43=989$ 可验）。

③ $9999=3^2\cdot11\cdot101$，$100000=2^5\cdot5^5$。

④ 关键式子：$111111=111\times1001=3\cdot7\cdot11\cdot13\cdot37$。

⑤ 6-25(1)：gcd $=2\cdot3^2=18$。

⑥ lcm $=2^2\cdot3^3\cdot5^3\cdot7^2=661500$。

⑦ (2)：gcd $=7$，lcm $=210\times1001/7=30030$。

⑧ (3)：公共部分 $2\cdot3\cdot5\cdot11=330$，右数多出 13。

⑨ 关键式子：lcm $=13\times2^8\cdot3^6\cdot5^4\cdot11^{13}$。

⑩ (4)：只共用素数 41，gcd $=41^{11}$。

⑪ lcm 需取每边的最大指数：$41^{101}43^{47}47^{43}83^{111}103^{1001}$。

⑫ 6-26：设 $a=18m,b=18n$，则 $(m,n)=1$ 且 $mn=30$。

⑬ 30 的互素分拆：$1\times30,2\times15,3\times10,5\times6$。

⑭ 对应四对：$(18,540),(36,270),(54,180),(90,108)$，及反向。

**答案：素分解见上；6-25 的 gcd 依次 18、7、330、$41^{11}$；lcm 依次 661500、30030、$13\times2^8\cdot3^6\cdot5^4\cdot11^{13}$、$41^{101}43^{47}47^{43}83^{111}103^{1001}$；6-26 为上述四对（可反向）。**

# 07 同余、逆元与线性同余式

约 10 分 · 40 分钟

考：填空或解答第一问（解同余式、求逆元）；后面 CRT、费马、原根全要用它

> **一句话：**同余就是"**余数相同**"。在这个世界里加、减、乘都随便做，**唯独"除"要先确认能不能除**。

? 现在是**下午 5 点**，再过 27 小时是几点?

你会算 $5+27=32$，然后"超过 24 就减 24"，得 **8 点**。

这个"减到 0~23 之间"的动作，就是模运算。同余只是把它写成数学式子而已。

先讲清楚

## 一、同余的两种说法（完全等价）

$$a \equiv b \pmod{m}$$

| 说法 | 含义 | 什么时候用 |
| --- | --- | --- |
| **整除式**：$m \mid (a-b)$ | 两者的差能被 $m$ 整除 | 证明题 |
| **余数式**：$a$、$b$ 除以 $m$ 余数相同 | 落在同一个余数类 | 计算题 |

写几个例子，感觉就出来了：

- $17 \equiv 2 \pmod 5$ —— 都余 2；
- $32 \equiv 8 \pmod{24}$ —— 都是"8 点"；
- $-1 \equiv 6 \pmod 7$ —— 因为 $-1+7=6$，落在同一个类里。

## 二、能随便做的：加、减、乘

若 $a \equiv b$，$c \equiv d \pmod m$，则

$$a+c \equiv b+d,\ a-c \equiv b-d,\ ac \equiv bd \pmod m$$

**这句话的实战价值：可以先取余再算，把大数压小。**

> **求 $1234 \times 5678 \bmod 10$。**
> 不用真乘：$1234 \equiv 4$、$5678 \equiv 8$，所以乘积 $\equiv 4 \times 8 = 32 \equiv 2 \pmod{10}$。
> **答案 2。**验算：$1234 \times 5678 = 7006652$，末位确实是 2 ✓

## 三、不能随便做的：除法

看这个：$2x \equiv 2 \pmod 4$。两边都除以 2，得 $x \equiv 1 \pmod 4$ —— **这是错的。**

把 $x=0,1,2,3$ 代进去看：$2x$ 分别是 0,2,0,2。所以 $x \equiv 1$ 和 $x \equiv 3$ **都对**，有两个解。

什么时候能除？**除数和模互素时**：

$$ac \equiv bc \pmod m \text{ 且 } (c,m)=1 \Rightarrow a \equiv b \pmod m$$

"互素"这三个字就是许可条。上面的例子 $(2,4)=2 \neq 1$，所以不能约。

## 四、逆元：模世界里的"倒数"

实数里 3 的倒数是 $\frac{1}{3}$，因为 $3\times\frac{1}{3}=1$。模世界里没有分数，但有**逆元**：

$$ax\equiv 1 \pmod m \text{ 的解 } x\text{，记作 } a^{-1}$$

**什么时候存在？**当且仅当 $(a,m)=1$。**不互素就永远没有逆元**，这是判断题的高频点。

> **求 17 模 31 的逆元（考试格式）：**
> 先做欧几里得竖式：
> $31=1\times17+14$
> $17=1\times14+3$
> $14=4\times3+2$
> $3=1\times2+1$
> 倒着回代：
> $1=3-2=3-(14-4\times3)=5\times3-14$
> $=5(17-14)-14=5\times17-6\times14$
> $=5\times17-6(31-17)=11\times17-6\times31$
> 所以 $11\times17\equiv1 \pmod{31}$，**逆元是 11**。
> 验算：$17\times11=187=6\times31+1$ ✓

## 五、线性同余式 $ax\equiv b \pmod m$

这里有个"一步定生死"的判据。**先算 $d=(a,m)$**：

| 情况 | 结论 | 怎么写 |
| --- | --- | --- |
| $d\nmid b$ | **无解** | 直接写"因为 $(a,m)=d\nmid b$，故无解"，得分 |
| $d\mid b$ | 恰有 $d$ 个不同余的解 | 先求一个，再加 $\frac{m}{d}$ 的倍数 |

**三步解法：**① 三边同除 $d$（模也除）；② 此时系数与模互素，乘逆元；③ 补出其余 $d$-1 个解。

> **解 $12x\equiv6 \pmod{30}$：**
> ① $d=(12,30)=6$，而 $6\mid6$ ✓，所以**有 6 个解**。
> ② 三边同除 6：$2x\equiv1 \pmod5$。2 的逆元是 3（$2\times3=6\equiv1$），所以 $x\equiv3 \pmod5$。
> ③ 补全：$x\equiv3,8,13,18,23,28 \pmod{30}$，正好 6 个。
> 验算 $x=8$：$12\times8=96=3\times30+6$ ✓

**必背 · 六条**

| | |
|---|---|
| $a\equiv b\Leftrightarrow m\mid(a-b)$ | 同余定义 |
| 加减乘随便 | 可先取余再算 |
| 除法要 $(c,m)=1$ | 不互素不能约 |
| 逆元存在 $\Leftrightarrow (a,m)=1$ | 扩展欧几里得求 |
| $ax\equiv b$：$(a,m)\mid b$ 才有解 | 否则写无解 |
| 有解时共 $d=(a,m)$ 个 | 别只写一个 |

**课本 6-39** 8 分 判可解性与解数

同余式 $12x\equiv c \pmod{30}$，$0\le c\le 29$。$c$ 取何值时有解？有解时有多少个不同余的解？

**第一步：先算 $d=(a,m)$。**$a=12$，$m=30$，$(12,30)=6$。这一步决定后面全部答案。

**第二步：用判据筛 $c$。**有解 $\Leftrightarrow d\mid c \Leftrightarrow 6\mid c$。

$0\le c\le 29$ 中 6 的倍数是 0,6,12,18,24，**共 5 个。**

**第三步：定解数。**有解时解的个数恒等于 $d=6$，与 $c$ 取哪个值无关。

**第四步：验一个。**取 $c=6$：$12x\equiv 6 \pmod{30} \Rightarrow$ 同除 6 得 $2x\equiv 1 \pmod 5 \Rightarrow x\equiv 3 \pmod 5 \Rightarrow$ 模 30 下有 3,8,13,18,23,28 六个解 ✓

**答案：$c\in\{0,6,12,18,24\}$ 时有解，每个 $c$ 恰有 6 个解。**

换个模数也一样：$154x\equiv c \pmod{1001}$，$(154,1001)=77$，所以 $c$ 必须是 77 的倍数（13 个），每个 77 个解。**套路完全一样。**

⚠ **三个坑：**
① **不互素硬约。**$2x\equiv 2 \pmod 4$ 约成 $x\equiv 1 \pmod 4$，直接丢掉一半的解。
② **只写一个解。**$d=6$ 就要写 6 个，漏写按步扣分。
③ **负余数不转换。**$x\equiv -2 \pmod 7$ 要写成 $x\equiv 5 \pmod 7$，否则答案不"最小正"。

**自测 · 3 道**

1. $3x \equiv 1 \pmod 7$ 的解是多少?
2. $6x \equiv 4 \pmod 9$ 有几个解?
3. 5 模 12 有逆元吗? 有的话是多少?

**1.** 试 $x=5$：$15 \equiv 1$ ✓。所以 $\boldsymbol{x \equiv 5}$。

**2.** $(6,9)=3$，而 $3 \nmid 4 \Rightarrow$ **无解**。

**3.** $(5,12)=1 \Rightarrow$ 有。$5 \times 5 = 25 \equiv 1$，所以逆元是 **5**（自己就是自己的逆元）。

## ch6 · 习题 3 道

### ch6 · 6-27~6-32

○ 会　○ 卡　○ 不会

**6-27** 证明：$[a,b]\mid c \Leftrightarrow a\mid c$ 且 $b\mid c$.

**6-28** 证明：$c\mid ab$ 时 $c\mid(a,c)(b,c)$.

**6-29** 证明：$(a,b,c)[ab,ac,bc]=abc$.

**6-30** 用埃拉托斯特尼筛法列出不超过 150 的全部素数.

**6-31** 11 时过 29 小时是几时？2 时过 100 小时？6 时过 50 小时?

**6-32** 证明：(1) $13\equiv1 \pmod 2$ (2) $-2\equiv1 \pmod 3$ (3) $22\equiv7 \pmod 5$ (4) $-3\equiv30 \pmod{11}$.

---

**套路：lcm 是公倍数中最小者；同余就是差被模数整除。**

① 6-27 必要性：$a\mid[a,b]$ 且 $[a,b]\mid c\Rightarrow a\mid c$。

② 充分性：$a\mid c$、$b\mid c$ 说明 $c$ 是公倍数。

③ 公倍数全体是 $[a,b]$ 的倍数 $\Rightarrow [a,b]\mid c$。

④ 6-28：令 $d=(a,c)$，写 $a=da'$、$c=dc'$，$(a',c')=1$。

⑤ 由 $c\mid ab$ 得 $c'\mid a'b$，又 $(a',c')=1\Rightarrow c'\mid b$。

⑥ 关键式子：$c'\mid(b,c)\Rightarrow c=dc'\mid d(b,c)$。

⑦ 6-29：设素数指数 $r\ge s\ge t$。

⑧ 关键式子：左边 $\min+\max=t+(r+s)$，右边 $r+s+t$，逐素数相等。

⑨ 6-30：只需用不超过 $\sqrt{150}\approx12.2$ 的素数：2、3、5、7、11。

⑩ 先划掉 2、3、5、7 的倍数，只剩 121 与 143 两个合数。

⑪ 再用 11 划掉它们，余下 35 个。

⑫ 列表：2,3,5,7,11,13,17,19,23,29,31,37,41,43,47。

⑬ 53,59,61,67,71,73,79,83,89,97,101,103,107,109,113,127,131,137,139,149。

⑭ 6-31：钟面模 12，$11+29\equiv4$。

⑮ 关键式子：$2+100\equiv6$，$6+50\equiv8$。

⑯ 6-32：只验差 $12,-3,15,-33$ 分别被 $2,3,5,11$ 整除。

**答案：6-27~6-29 得证；6-30 共 35 个（见上）；6-31 依次 4 时、6 时、8 时；6-32 四式成立。**

## ch6 · 6-33~6-37

○ 会　○ 卡　○ 不会

**6-33** 证明：$a$ 偶时 $a^2\equiv 0 \pmod 4$；$a$ 奇时 $a^2\equiv 1 \pmod 4$.

**6-34** 证明：$a$ 奇时 $a^2\equiv 1 \pmod 8$.

**6-35** 证明：$n\mid m$ 且 $a\equiv b \pmod m$ 时 $a\equiv b \pmod n$.

**6-36** 证明：$a\equiv b \pmod m$ 时 $ac\equiv bc \pmod{mc}$.

**6-37** 证明：$a\equiv b \pmod c$ 时 $(a,c)=(b,c)$.

**套路：同余就是整除，一律写成 $a=b+mk$ 再代进去。**

① 6-33：偶数设 $a=2k$，则 $a^2=4k^2$，是 4 的倍数。

② 6-33：奇数设 $a=2k+1$，得 $4k(k+1)+1$，余 1。

③ 6-34：$k$ 与 $k+1$ 必一奇一偶，积为偶数。

④ 关键式子：$a^2=8\cdot\dfrac{k(k+1)}{2}+1$。

⑤ 6-35：$m\mid(a-b)$ 且 $n\mid m$，整除有传递性。

⑥ 关键式子：$n\mid(a-b)$，即 $a\equiv b \pmod n$。

⑦ 6-36：设 $a-b=mk$，两边乘 $c$。

⑧ 关键式子：$ac-bc=mck=(mc)k$，故 $mc\mid(ac-bc)$。

⑨ 6-37：由 $b=a-ct$ 知 $(a,c)$ 同时整除 $b$ 与 $c$。

⑩ 故 $(a,c)\mid(b,c)$；对换 $a$、$b$ 得反向。

⑪ 互相整除的正整数相等，结论成立。

**答案：6-33、6-34、6-35、6-36、6-37 均得证。**

## ch6 · 6-38~6-43

○ 会　○ 卡　○ 不会

**6-38** 给出一个完全由奇整数组成的模 13 的完全剩余系.

**6-39** $12x\equiv c \pmod{30}$，$0\le c\le 29$：$c$ 取何值有解？有解时几个不同余的解?

**6-40** $154x\equiv c \pmod{1001}$，$0\le c\le 1000$：同上.

**6-41** 求 2、3、5、11 模 13 的逆元.

**6-42** $1\le a\le 14$ 中哪些有模 14 的逆元？各是多少?

**6-43** 证明：$b$ 是 $a$ 模 $m$ 的逆元、$d$ 是 $c$ 的逆元，则 $bd$ 是 $ac$ 的逆元.

---

**套路：先算 $(a,m)$，它同时决定可解性、解数和逆元存在性。**

① 6-38：模 13 要 13 个两两不同余的奇数。

② 关键式子：取 $1,3,5,\ldots,25$，余数恰取遍 0~12。

③ 6-39：$(12,30)=6$，有解当且仅当 $6\mid c$。

④ 这样的 $c$ 是 0,6,12,18,24 共 5 个。

⑤ 有解时恰有 $d=(a,m)=6$ 个不同余的解。

⑥ 6-40：$154=2\times7\times11$，$1001=7\times11\times13$。

⑦ 关键式子：$(154,1001)=77$，有解当且仅当 $77\mid c$。

⑧ $c$ 有 13 个取值，每个恰有 77 个解。

⑨ 6-41：试乘到余 1 即可。

⑩ 关键式子：$2\times7=14\equiv1$，$3\times9=27\equiv1$，$5\times8=40\equiv1$，$11\times6=66\equiv1$。

⑪ 6-42：$(a,14)=1$ 才有逆元，剩 $1,3,5,9,11,13$。

⑫ 逆元依次为 $1,5,3,11,9,13$（1 与 1、13 与 13 自逆）。

⑬ 6-43：把 $(ac)(bd)$ 重新分组。

⑭ 关键式子：$(ac)(bd)=(ab)(cd)\equiv1\times1\equiv1 \pmod{m}$。

**答案：6-38 取 $1,3,\ldots,25$；6-39 的 $c=0,6,12,18,24$，各 6 解；6-40 的 $c=77k$（13 个），各 77 解；6-41 依次 7、9、8、6；6-42 为 $1,3,5,9,11,13$，逆元 $1,5,3,11,9,13$；6-43 得证。**

## 08 中国剩余定理

约 8 分 · 30 分钟

考：解同余式组（解答题一小问）；老师说是"唯一用中国命名的定理"

> **一句话：**几个模数**两两互素**时，同余式组在模 $M=$ 各模数之积 下**有唯一解**；解法就是"各管一段，加起来"。

? 先看一道 1500 年前的老题（《孙子算经》）：
"**三三数之剩二，五五数之剩三，七七数之剩二**" —— 一个数，除以 3 余 2，除以 5 余 3，除以 7 余 2。
**这数是多少？**你现在可能只能一个个试。学完这一讲，30 秒就能算出来。

**先讲清楚**

## 一、为什么"拆开"能行

因为模数互素时，**每个模数只管一个方向，互不干扰**。就像同时满足"姓张"和"住 3 楼"，两件事不冲突。

反过来，模数不互素就会打架：

> **反例：** $x\equiv 1 \pmod 4$ 要求 $x$ 是奇数；$x\equiv 2 \pmod 6$ 要求 $x$ 是偶数。
> 两者不可能同时成立 ⇒ **无解**。原因就是 $(4,6)=2\neq 1$。

## 二、构造公式：它是怎么拼出来的

设 $m_1,\dots,m_k$ 两两互素，$M=m_1m_2\cdots m_k$，$M_i=M/m_i$，$t_i$ 是 $M_i$ 模 $m_i$ 的逆元，则

$$x\equiv a_1M_1t_1+a_2M_2t_2+\cdots+a_kM_kt_k \pmod M$$

**凭什么每项都对？**看第 $i$ 项 $a_iM_it_i$：

- 模 $m_i$ 时：$M_it_i\equiv 1$，所以这项 $\equiv a_i$ —— **正好是第 $i$ 个要求**；
- 模其它 $m_j$ 时：$M_i$ 里含 $m_j$，所以这项 $\equiv 0$ —— **不影响别的方程**。

各项"各管一段"，加起来就全部满足。

> **手算孙子算经那道题：**
> $a_1=2,m_1=3$；$a_2=3,m_2=5$；$a_3=2,m_3=7$。$M=105$。
> $M_1=35$，$35\equiv 2 \pmod 3$，2 的逆元是 2 ⇒ $t_1=2$；
> $M_2=21$，$21\equiv 1 \pmod 5$ ⇒ $t_2=1$；
> $M_3=15$，$15\equiv 1 \pmod 7$ ⇒ $t_3=1$。
> $x=2\times 35\times 2+3\times 21\times 1+2\times 15\times 1=140+63+30=233$。
> 对 105 取余：$233-2\times 105=23$。**答案 23。**
> 验算：$23\div 3$ 余 2 ✓；$23\div 5$ 余 3 ✓；$23\div 7$ 余 2 ✓

## 三、两个模数时，用"逐个合并"更快

考试多数只给两个方程，用这个三步法比套公式快：

1. 由第一个式子设 $x=a_1+m_1k$（$k$ 是整数）；
2. 代入第二个式子，解出 $k$；
3. 回代得 $x$，模数变成 $m_1m_2$。

**解 $x\equiv 4 \pmod{11}$，$x\equiv 3 \pmod{17}$：**

设 $x=4+11k$。代入第二个：$4+11k\equiv 3 \pmod{17} \Rightarrow 11k\equiv 16 \pmod{17}$。

11 模 17 的逆元是 14（$11\times 14=154=9\times 17+1$）$\Rightarrow k\equiv 14\times 16=224\equiv 3 \pmod{17}$。

回代：$x=4+11\times 3=37$。**答案 $x\equiv 37 \pmod{187}$。**

验算：$37=3\times 11+4$ ✓；$37=2\times 17+3$ ✓

### 四、和安全的关系

**RSA 解密加速。**直接在模 $n=pq$ 下算 $m^d$ 很慢；用 CRT 拆成"模 $p$ 算一次、模 $q$ 算一次"，再拼回来 —— 因为两个模数小得多，**整体快约 4 倍**。

老师课上原话："把大的模数化成小的模数，简化计算"。

**必背 · 四条**

| | |
|---|---|
| 模数必须两两互素 | 前提，不满足会无解 |
| $x=\Sigma\, a_iM_it_i \pmod{M}$ | 构造公式 |
| $M_it_i\equiv 1 \pmod{m_i}$ | 逆元这一步最容易错 |
| $x=a_1+m_1k$ 代入下一式 | 两方程用合并法更快 |

**课本 6-47(1)** 8 分 逐个合并法

解同余式组 $x\equiv4 \pmod{11}$，$x\equiv3 \pmod{17}$。

---

**第一步：把第一个式子改写成"带未知参数"的形式。**

$x=4+11k$，$k\in\mathbb{Z}$。

**第二步：代入第二个式子，得到一个关于 $k$ 的线性同余式。**

$4+11k\equiv3 \pmod{17} \Rightarrow 11k\equiv-1\equiv16 \pmod{17}$。

**第三步：求 11 模 17 的逆元。**

$17=1\times11+6$，$11=1\times6+5$，$6=1\times5+1$。回代：$1=6-5=6-(11-6)=2\times6-11=2(17-11)-11=2\times17-3\times11$。

所以 $11\times(-3)\equiv1$，逆元是 $-3\equiv14 \pmod{17}$。

**第四步：解出 $k$ 再回代。**

$k\equiv14\times16=224$，$224=13\times17+3$，所以 $k\equiv3 \pmod{17}$。

$x=4+11\times3=37$。

**第五步：写最终答案并验算。**$x\equiv37 \pmod{11\times17=187}$。验算：$37 \bmod 11=4$ ✓，$37 \bmod 17=3$ ✓

两个模数用合并法；三个以上既可用合并法逐步并，也可直接套构造公式。**考试写哪种都行，但过程要完整。**

⚠ **三个坑：**

① **模数不互素还套公式。**先检查 $(m_i,m_j)=1$，不满足要拆开或直接用合并法（合并法不要求互素）。

② **忘了最后对 $M$ 取余。**答案要落在 $[0,M)$ 里，233 要化成 23。

③ **逆元算错。**这是唯一容易崩的一步，求完一定验算 $M_it_i\equiv1 \pmod{m_i}$。

## ch6 · 习题 1 道

### ch6 · 6-44~6-48

○ 会　○ 卡　○ 不会

**6-44** 哪个整数被 2 和 3 除余数都为 1?

**6-45** 给出被 2 或 5 除余 1、但被 3 整除的整数.

**6-46** 给出被 3 或 5 除余 2、但被 4 整除的整数.

**6-47** 解下列同余式组:

(1) $x\equiv 4 \pmod{11}$，$x\equiv 3 \pmod{17}$;

(2) $x\equiv 0 \pmod 2$，$x\equiv 0 \pmod 3$，$x\equiv 1 \pmod 5$，$x\equiv 6 \pmod 7$;

(3) $x\equiv 1,2,3,4,5$ 分别模 $2,3,5,7,11$;

(4) $x\equiv 2,3,4,5,6$ 分别模 $11,12,13,17,19$.

**6-48** 给出 16! 被 19 除的余数.

---

**套路：同余式两两合并，阶乘靠威尔逊定理降次。**

① 6-44：两个余 1 合成 $x\equiv 1 \pmod 6$，最小正解 1。

② 6-45：余 1 条件合成 $x\equiv 1 \pmod{10}$，再加 $3\mid x$。

③ 设 $x=10k+1$ 代入得 $k+1\equiv 0 \pmod 3$。

④ 关键式子：$x\equiv 21 \pmod{30}$，验算 $21 \bmod 2=21 \bmod 5=1$。

⑤ 6-46：先得 $x\equiv 2 \pmod{15}$，再与 $4\mid x$ 联立。

⑥ 设 $x=2+15k$，得 $3k\equiv 2 \pmod 4 \Rightarrow k\equiv 2$。

⑦ 关键式子：$x\equiv 32 \pmod{60}$。

⑧ 6-47(1)：$x=4+11k$ 代入得 $11k\equiv 16 \pmod{17} \Rightarrow k\equiv 3$。

⑨ 关键式子：$x\equiv 37 \pmod{187}$。

⑩ (2)：前两式给 $x\equiv 0 \pmod 6$，再联 5 与 7 $\Rightarrow x\equiv 6 \pmod{210}$。

⑪ (3)：逐个合并到模 $2\times3\times5\times7\times11=2310$，只剩一个解。

⑫ 关键式子：$x\equiv 1523 \pmod{2310}$。

⑬ (4)：依次对 12、13、17、19 解一次同余式，模数逐次升到 554268。

⑭ 关键式子：$x\equiv 150999 \pmod{554268}$。

⑮ 6-48：威尔逊给 $18!\equiv -1 \pmod{19}$。

⑯ 关键式子：$18!=18\times17\times16!\equiv 2\times16!$，故 $16!\equiv -1\times2^{-1}\equiv 9$。

**答案：6-44 为 $x\equiv 1 \pmod 6$；6-45 $x\equiv 21 \pmod{30}$；6-46 $x\equiv 32 \pmod{60}$；6-47 四组依次 37、6、1523、150999（对应模 187、210、2310、554268）；6-48 余 9。**

09

# 费马、欧拉、威尔逊三大定理

约 10 分 · 35 分钟

考：填空题（求大指数余数）；解答题里作为一步工具

> **一句话：**这三条定理的实际用途只有一个 —— **把巨大的指数变回小数**。

? 考试让你算 $3^{100000} \bmod 35$。
这个数有 47713 位。**手算不可能，计算器也爆。**
但如果知道 $3^{24}\equiv 1 \pmod{35}$，那 $3^{100000}=3^{24\times 4166+16}\equiv 3^{16}$ —— **问题瞬间变成算 $3^{16}$**。
这就是这一讲全部的意义。

先讲清楚

## 一、欧拉函数 $\varphi(m)$：数一数"有几个数和它互素"

$\varphi(m)$ 的定义：在 $1\sim m$ 中，与 $m$ **互素**的数的个数。

> **手算 $\varphi(10)$：**1 到 10 里，和 10 互素的是 **1、3、7、9** —— 共 4 个。
> 2、4、5、6、8、10 都和 10 有公因子，不算。**注意 1 要算进去。**所以 $\varphi(10)=4$。
> **手算 $\varphi(7)$：**7 是素数，1 到 6 都和它互素 $\Rightarrow \varphi(7)=6$。

**大数用公式：**把 $m$ 素分解成 $m=\Pi\, p_i^{e_i}$，则

$$\varphi(m)=m\Pi\left(1-\frac{1}{p_i}\right)$$

例：$\varphi(35)=35\times\left(1-\frac{1}{5}\right)\times\left(1-\frac{1}{7}\right)=35\times\frac{4}{5}\times\frac{6}{7}=24$。

注意：**只用不同的素因子，指数不参与**。所以 $\varphi(12)=12\times\frac{1}{2}\times\frac{2}{3}=4$。

## 二、欧拉定理

若 $(a,m)=1$，则

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

> **例：$3^4 \bmod 10$。**$\varphi(10)=4$，且 $(3,10)=1 \Rightarrow 3^4\equiv 1 \pmod{10}$。
> 验证：$3^4=81$，末位是 1 ✓

## 三、费马小定理：欧拉定理的特例

当 $m=p$ 是素数时，$\varphi(p)=p-1$，于是

$a^{p-1}\equiv 1 \pmod p$（要求 $(a,p)=1$）

**考试遇到的模数大多是素数，所以这条用得最多。**

## 四、威尔逊定理：管阶乘

$p$ 是素数 ⇔ $(p-1)!\equiv -1 \pmod p$。

> **例：$p=5$。** $4!=24$，而 $24=4\times5+4$，余 $4\equiv-1$ ✓
> **它的用途：把大阶乘降成小阶乘。**例如求 $16!\bmod 19$：
> $18!\equiv-1$，而 $18!=18\times17\times16!$，且 $18\equiv-1$、$17\equiv-2$，
> 所以 $(-1)(-2)\times16!=2\times16!\equiv-1 \Rightarrow 16!\equiv-1\times10\equiv9 \pmod{19}$。

## 五、实战：三大定理就是"降指数"

> **求 $3^{100000}\bmod 35$：**
> ① 算 $\varphi(35)=24$；检查 $(3,35)=1$ ✓，可以用欧拉定理。
> ② 指数对 24 取余：$100000=24\times4166+16$。
> ③ 于是 $3^{100000}\equiv3^{16} \pmod{35}$。
> ④ 用"平方-乘"算 $3^{16}$：$3^2=9 \to 3^4=81\equiv11 \to 3^8\equiv121\equiv16 \to 3^{16}\equiv256\equiv11$。
> **答案 11。**（验算：$3^{16}=43046721=35\times1229906+11$ ✓）

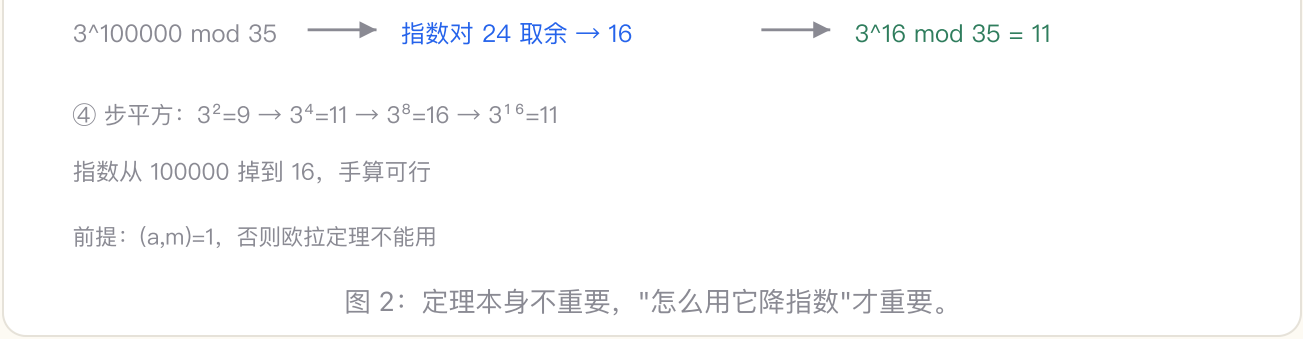



图 2：定理本身不重要，"怎么用它降指数"才重要。

**必背 · 六条**

| | |
|---|---|
| $\varphi(m)=m\Pi(1-\frac{1}{p_i})$ | 只取不同素因子 |
| $\varphi(p)=p-1$，$\varphi(p^k)=p^k-p^{k-1}$ | 素数的情形 |
| $a^{\varphi(m)}\equiv 1$ | 欧拉定理，需 $(a,m)=1$ |
| $a^{p-1}\equiv 1 \pmod p$ | 费马小定理 |
| $(p-1)!\equiv -1 \pmod p$ | 威尔逊 |
| 指数对 $\varphi(m)$ 取余 | 降指数的标准动作 |

**课本 6-64** 8 分 欧拉定理降指数

用欧拉定理求 $3^{100000}$ 对 35 取模的最小正剩余。

**第一步：算模数的欧拉函数。**$35=5\times 7$，所以

$\varphi(35)=35\times(1-\frac{1}{5})\times(1-\frac{1}{7})=35\times\frac{4}{5}\times\frac{6}{7}=24$。

**第二步：检查互素条件。**$(3,35)=1$ ✓，所以欧拉定理可用：$3^{24}\equiv 1 \pmod{35}$。

**第三步：把指数拆成"24 的倍数 + 余数"。**

$100000=24\times 4166+16$，所以 $3^{100000}=(3^{24})^{4166}\cdot 3^{16}\equiv 3^{16} \pmod{35}$。

**第四步：用平方-乘算出 $3^{16}$。**

$3^2=9$；$3^4=81\equiv 81-70=11$；$3^8\equiv 11^2=121\equiv 121-105=16$；$3^{16}\equiv 16^2=256\equiv 256-245=11$。

**第五步：验算。**$3^{16}=43046721$，$43046721=35\times 1229906+11$ ✓

**答案：11。**

如果忘了检查互素 —— 这题刚好互素所以没事，但换成 $5^{100} \bmod 35$ 就**不能**用欧拉定理（$(5,35)=5\neq 1$）。**第一步永远是算 gcd。**

⚠ **三个坑：**

① **不检查 $(a,m)=1$ 就用欧拉定理。**不互素时定理不成立，这一步是判断题的必考点。

② **$\varphi$ 算错。**$\varphi(35)=24$，不是 34；记公式"$m$ 乘各 $(1-\frac{1}{p})$"。

③ **指数对 $m$ 取余。**错。要对 $\varphi(m)$ 取余，这是最容易混的一步。

**自测 · 3 道**

1. $\varphi(12)$ 等于多少?
2. $3^{50} \bmod 7$ 等于多少?
3. $5^{100} \bmod 6$ 等于多少?

**1.** $12\times\frac{1}{2}\times\frac{2}{3}=4$（互素的是 1、5、7、11）。

**2.** $\varphi(7)=6$，$50=6\times8+2 \Rightarrow 3^2=9\equiv2$。

**3.** $\varphi(6)=2$，100 是 2 的倍数 $\Rightarrow 1$。（也可直接看：5 的幂是 5,1,5,1...）

## ch6 · 习题 4 道

### ch6 · 6-49~6-51

○ 会　○ 卡　○ 不会

**6-49** 用费马小定理求 $3^{999999999}$ 模 7 的最小正剩余.

**6-50** 用费马小定理求 $2^{1000000}$ 模 17 的最小正剩余.

**6-51** 用威尔逊定理求 $8\times9\times10\times11\times12\times13$ 模 7 的最小正剩余.

**套路：指数对 $p$-1 取余，乘积先把底数缩到模内。**

① 三题同一招：先缩指数或缩底数，再算一次幂。

② 费马小定理：$p$ 素且 $p\nmid a$ 时 $a^{p-1}\equiv1 \pmod p$。

③ 故指数写成 $p$-1 的倍数加余数，只算余数那部分。

④ 6-49：$999999999=6\times166666666+3$，余 3。

⑤ 关键式子：$3^{999999999}\equiv3^3=27\equiv6 \pmod 7$。

⑥ 6-50：$1000000=16\times62500$，指数被 16 整除。

⑦ 关键式子：$2^{1000000}=(2^{16})^{62500}\equiv1 \pmod{17}$。

⑧ 6-51：各因子模 7 依次为 1,2,3,4,5,6，乘积就是 6!。

⑨ 威尔逊：$(7-1)!\equiv-1\equiv6 \pmod 7$。

⑩ 验算：$1235520=7\times176502+6$，余数确为 6。

**答案：6-49 得 6；6-50 得 1；6-51 得 6。**

## ch6 · 6-52~6-54

○ 会　○ 卡　○ 不会

**6-52** 证明：$3^{10}\equiv 1 \pmod{11^2}$.

**6-53** 证明：$(a,35)=1$ 时 $35 \mid a^{12}-1$.

**6-54** 证明：$(a,42)=1$ 时 $168 \mid a^{6}-1$.

---

**套路：把模数拆成两两互素的因子，逐个证完再合并。**

① 通用思路：每个因子都整除 $a^k-1$，且因子互素，乘积才整除。

② 6-52：$3^5=243=2\times121+1$，即 $3^5\equiv 1 \pmod{121}$。

③ 关键式子：$3^{10}=(3^5)^2\equiv 1 \pmod{121}$。

④ 验算：$3^{10}-1=59048=488\times121$ ✓。

⑤ 6-53：$35=5\times7$，分别证。

⑥ 关键式子：$a^{12}=(a^4)^3\equiv 1 \pmod 5$，$a^{12}=(a^6)^2\equiv 1 \pmod 7$。

⑦ 5 与 7 互素 $\Rightarrow 35 \mid a^{12}-1$。

⑧ 6-54：$168=8\times3\times7$，先由 $(a,42)=1$ 得 $a$ 为奇数。

⑨ 关键式子：$a^6=(a^2)^3\equiv 1 \pmod 8$，又 $a^6\equiv 1 \pmod 3$。

⑩ 模 7 用费马：$(a,7)=1 \Rightarrow a^6\equiv 1 \pmod 7$。

⑪ 8、3、7 两两互素，合并得 $168 \mid a^6-1$。

**答案：三式均成立。**

## ch6 · 6-55~6-59

○ 会　○ 卡　○ 不会

**6-55** 证明：$p$ 素时 $\Sigma_{k=1}^{p-1} k^{p-1} \equiv -1 \pmod p$.

**6-56** 证明：$p$ 为奇素数时 $\Sigma_{k=1}^{p-1} k^{p} \equiv 0 \pmod p$.

**6-57** 证明：$p \nmid ab$ 且 $a^p \equiv b^p \pmod p$ 时 $a^p \equiv b^p \pmod{p^2}$.

**6-58** 用 Pollard $p-1$ 方法给出 689 的一个因子.

**6-59** 证明：$p \mid a^p + (p-1)!\, a$.

---

**套路：用费马把每一项压成常数，再求和。**

① 6-55：每项 $k^{p-1} \equiv 1 \pmod p$，共 $p-1$ 项。

② 关键式子：$\Sigma \equiv p-1 \equiv -1 \pmod p$。

③ 6-56：用推论 $k^p \equiv k \pmod p$。

④ 关键式子：$\Sigma\, k = \dfrac{p(p-1)}{2}$，$p$ 奇 ⇒ 含因子 $p$ ⇒ 余 0。

⑤ 6-57：费马给 $a^p \equiv a$、$b^p \equiv b$，条件即 $a \equiv b \pmod p$。

⑥ 设 $a = b + kp$，对 $a^p$ 作二项式展开。

⑦ 除首项 $b^p$ 外每项都含 $p^2$ ⇒ $a^p \equiv b^p \pmod{p^2}$。

⑧ 验算 $p=3, a=1, b=4$：$4^3 - 1 = 63 = 7 \times 9$ ✓。

⑨ 6-58：$689 = 13 \times 53$，12 光滑、52 含大因子 13。

⑩ 关键式子：$\gcd(2^{12}-1, 689) = \gcd(4095, 689) = 13$。

⑪ 6-59：费马给 $a^p \equiv a$，威尔逊给 $(p-1)! \equiv -1$。

⑫ 关键式子：$a^p + (p-1)!\, a \equiv a - a \equiv 0 \pmod p$。

⑬ 验算 $p=5, a=2$：$32 + 48 = 80 = 5 \times 16$ ✓。

**答案：各式成立；6-58 的一个因子是 13（$689 = 13 \times 53$）。**

## ch6 · 6-60~6-64

○ 会　○ 卡　○ 不会

**6-60** 给出模 6、9、10、14、16、17 的简化剩余系.

**6-61** 用欧拉定理解：(1) $5x\equiv 3 \pmod{14}$；(2) $4x\equiv 7 \pmod{15}$；(3) $3x\equiv 5 \pmod{16}$.

**6-62** 证明：$m\neq 2$ 时缩系之和 $\equiv 0 \pmod{m}$.

**6-63** 证明：$(a,m)=(a-1,m)=1$ 时 $\Sigma_{k=0}^{\varphi(m)-1} a^k \equiv 0 \pmod{m}$.

**6-64** 用欧拉定理求 $3^{100000}$ 模 35 的最小正剩余.

---

**套路：缩系靠配对，同余式靠逆元。**

① 缩系 = 模 $m$ 中与 $m$ 互素、两两不同余的一批数，共 $\varphi(m)$ 个。

② 6-60：模 6 是 $\{1,5\}$；模 9 是 $\{1,2,4,5,7,8\}$。

③ 模 10 是 $\{1,3,7,9\}$；模 14 是 $\{1,3,5,9,11,13\}$。

④ 模 16 取全部 8 个奇数；模 17 取 1~16。

⑤ 6-61 通法：$(a,m)=1$ 时逆元写作 $a^{\varphi(m)-1}$。

⑥ 关键式子：$x\equiv a^{\varphi(m)-1}b \pmod{m}$。

⑦ (1) $\varphi(14)=6$，$5^5\equiv 3 \Rightarrow x\equiv 9$。

⑧ (2) $\varphi(15)=8$，$4^7\equiv 4 \Rightarrow x\equiv 28\equiv 13$。

⑨ (3) $\varphi(16)=8$，$3^7\equiv 11 \Rightarrow x\equiv 55\equiv 7$。

⑩ 验算：$45\equiv 3$、$52\equiv 7$、$21\equiv 5$ ✓。

⑪ 6-62：缩系在 $x\mapsto m-x$ 下成对，每对和恰为 $m$。

⑫ 关键式子：$\Sigma c_i = \dfrac{\varphi(m)}{2}\cdot m \equiv 0 \pmod{m}$。

⑬ 6-63：两边乘 $a-1$，用等比求和。

⑭ 关键式子：$(a-1)\Sigma a^k = a^{\varphi(m)}-1\equiv 0$，再约去 $(a-1,m)=1$。

⑮ 6-64：$\varphi(35)=24$，$100000=24\times 4166+16$。

⑯ 关键式子：$3^{100000}\equiv 3^{16}\equiv 11 \pmod{35}$。

⑰ 验算：$3^{16}=43046721=35\times 1229906+11$ ✓。

**答案：6-60 见②③④；6-61 得 9、13、7；6-62、6-63 成立；6-64 得 11。**

## 10 数论函数

约 6 分 · 30 分钟

这一讲只做一件事：数数，然后把数数的结果写成公式

> **一句话：** 数论函数就是"给一个整数，返回一个数"的函数 —— 有几个约数、约数加起来是多少、几个数和它互素。

? 36 有几个约数？你可以列：1、2、3、4、6、9、12、18、36，一共 9 个。
那 20! 有几个约数？列是不可能列的。
这一讲给你一个公式，只要知道素分解，什么数都能算。

先讲清楚

## 一、为什么素分解就够了

一个数的约数，完全由它的素分解决定。比如 $36=2^2\times3^2$，任何一个约数都只能由 2 和 3 组成，且 2 的次数最多取 0~2、3 的次数最多取 0~2。

所以选法有 $3\times3=9$ 种，正好 9 个约数。这就是公式的来源：

$$\text{若 } n=p_1^{a_1}p_2^{a_2}\cdots,\ \text{则 } d(n)=\Pi(a_i+1)$$

**算几个：**

$36=2^2\cdot3^2 \Rightarrow d=(2+1)(2+1)=9$ ✓

$99=3^2\cdot11 \Rightarrow d=3\times2=6$

$144=2^4\cdot3^2 \Rightarrow d=5\times3=15$

## 二、约数之和：等比数列求和

把所有约数加起来，等于"每个素因子的所有幂次之和"相乘：

$$\sigma(p^a)=1+p+p^2+\cdots+p^a=\frac{p^{a+1}-1}{p-1}$$

比如 $35=5\times7$，约数和 $=(1+5)(1+7)=6\times8=48$。验算：1+5+7+35=48 ✓

为什么可以相乘？因为每个约数都是"从每个素因子里挑一个幂"拼出来的，把所有的挑法加起来，正好等于各部分和的乘积。

## 三、欧拉函数：数一数有几个数和它互素

$\varphi(n)$ 表示 $1\sim n$ 里与 $n$ 互素的个数。这是全书用得最多的数论函数，因为欧拉定理要用它。

先手算一个小的：$\varphi(10)$。1 到 10 里和 10 互素的是 1、3、7、9，共 **4 个**。注意 1 要算进去。

公式：

$$\varphi(n)=n\Pi_{p|\,n}(1-\frac{1}{p})$$

只用**不同的**素因子，指数不参与。

> **算几个：**
>
> $\varphi(100)=100\times\frac{1}{2}\times\frac{4}{5}=40$
>
> $\varphi(256)=256\times\frac{1}{2}=128$（也可以 $2^8$-$2^7$）
>
> $\varphi(1001)=1001\times\frac{6}{7}\times\frac{10}{11}\times\frac{12}{13}=720$

## 四、积性：为什么这些公式都能"拆着算"

上面三个函数都有同一个性质：**当 $(m,n)=1$ 时，$f(mn)=f(m)f(n)$**。这叫积性。

正因为积性，才能"先算每个素幂上的值，再乘起来"。如果函数没有这个性质，公式就写不成乘积。

注意：**积性只要求互素**，不要求对所有 $m,n$ 都成立。要求更强的叫"完全积性"，比如 $f(n)=n^2$。

## 五、莫比乌斯函数：专门用来做反演

$\mu(n)$ 的定义有点怪，但很简单：

- 含平方因子（比如 4、9、12）$\Rightarrow \mu=0$；
- 不含平方因子，且是 $r$ 个不同素数之积 $\Rightarrow \mu=(-1)^r$。

例：$\mu(12)=0$（含 4），$\mu(15)=1$（两个素数），$\mu(30)=-1$（三个素数）。

它的用途是莫比乌斯反演：如果 $F(n)=\Sigma_{d|n}f(d)$，那么 $f(n)=\Sigma_{d|n}\mu(d)F(n/d)$。**能把"求和"倒着解出来。**

一个常用结论：$\Sigma_{d|n}\mu(d)=0$（$n>1$ 时），由此可以推出 $\varphi(n)=n\Sigma_{d|n}\frac{\mu(d)}{d}$。

## 六、高斯函数：只取整数部分

$[x]$ 表示不超过 $x$ 的最大整数。比如 $[3.7]=3$，$[-0.3]=-1$（注意负数往下取）。

常考一条：$[x]+[x+\frac{1}{2}]=[2x]$。它的意思是"取整之后再补半格，等于先乘 2 再取整"。

> **停一下：$\varphi(12)$ 等于多少？用公式和手算各来一遍。**

**公式：** $12=2^2\times3$，所以 $\varphi(12)=12\times\frac{1}{2}\times\frac{2}{3}=4$。

**手算：** 1 到 12 里与 12 互素的是 1、5、7、11，正好 4 个 ✓

注意 2、3、4、6、8、9、10、12 都和 12 有公因子，不算。

**必背 · 六条**

| | |
|---|---|
| $d(n)=\Pi(a_i+1)$ | 约数个数 |
| $\sigma(p^a)=\frac{p^{a+1}-1}{p-1}$ | 约数之和 |
| $\varphi(n)=n\Pi(1-\frac{1}{p})$ | 只用不同素因子 |
| $\varphi(p^k)=p^k-p^{k-1}$ | 素幂特例 |
| 积性：$(m,n)=1$ 时才拆 | 前提不能丢 |
| $\mu$：有平方因子就是 0 | 否则 $(-1)^r$ |

**课本 7-8** 6 分 欧拉函数计算

求 $\varphi(100)$、$\varphi(256)$、$\varphi(1001)$。

**第一步：三个数都先素分解。**这是所有数论函数题的第一步，分解完才有得算。

$100=2^2\cdot5^2$；$256=2^8$；$1001=7\cdot11\cdot13$。

**第二步：套公式，注意只用不同的素因子。**

$\varphi(100)=100\times(1-\frac{1}{2})\times(1-\frac{1}{5})=100\times\frac{1}{2}\times\frac{4}{5}=40$。

$\varphi(256)=256\times(1-\frac{1}{2})=128$。也可以直接用 $2^8-2^7=128$。

$\varphi(1001)=1001\times\frac{6}{7}\times\frac{10}{11}\times\frac{12}{13}$。先算 $1001\times\frac{6}{7}=858$，再算 $858\times\frac{10}{11}=780$，最后 $780\times\frac{12}{13}=720$。

**第三步：抽查一个小的验算。**$\varphi(12)=12\times\frac{1}{2}\times\frac{2}{3}=4$，而 1~12 里与 12 互素的确实是 1、5、7、11 四个 ✓

**答案：40、128、720。**

常见错误：把指数也算进去。**$256=2^8$ 只有一个素因子 2，所以只乘一次 $(1-\frac{1}{2})$**，不是乘 8 次。

⚠ **三个坑：**

① **把指数当因子个数。**$\varphi(2^8)$ 里只有一个不同的素因子 2，所以只乘 $(1-\frac{1}{2})$。写成 $2^8\times(\frac{1}{2})^8$ 就错了。

② **忘了 $\varphi(1)=1$。**这是定义，考试偶尔考。

③ **积性乱用。**$f(mn)=f(m)f(n)$ 只在 $(m,n)=1$ 时成立。比如 $\varphi(4\times6)$ 不能拆成 $\varphi(4)\varphi(6)$，因为 $(4,6)=2\neq1$。

**自测 · 3 道**

1. $d(100)$ 等于多少?
2. $\varphi(35)$ 等于多少?
3. $\mu(30)$ 等于多少?

**1.** $100=2^2\cdot5^2\Rightarrow d=3\times3=9$。

**2.** $35=5\cdot7\Rightarrow\varphi=35\times\frac{4}{5}\times\frac{6}{7}=24$。

**3.** 30 是三个不同素数之积 $\Rightarrow\mu=(-1)^3=-1$。

## ch7 · 习题 4 道

### ch7 · 7-1~7-3

○ 会　○ 卡　○ 不会

**7-1** 判断哪些是积性函数：(1) $f(n)=0$ (2) $f(n)=2$ (3) $f(n)=n/2$ (4) $f(n)=\log_2 n$ (5) $f(n)=n^2$ (6) $f(n)=n!$ (7) $f(n)=n+1$ (8) $f(n)=n^n$.

**7-2** 求正整数因子之和：(1) 35 (2) 196 (3) 1000 (4) $2^{100}$ (5) $2\cdot3\cdot5\cdot7\cdot11$ (6) $2^5\cdot3^4\cdot5^3\cdot7^2\cdot11$ (7) 10! (8) 20!.

**7-3** 求正整数因子个数：(1) 36 (2) 99 (3) 144 (4) $2\cdot3\cdot5\cdot7\cdot11\cdot13\cdot17\cdot19$ (5) $2\cdot3^2\cdot5^3\cdot7^4\cdot11^5\cdot13^4\cdot17^5\cdot19^5$ (6) 20!.

---

**套路：先验 $f(mn)=f(m)f(n)$（只在 $(m,n)=1$ 时），再按素分解拆成素幂相乘。**

① 7-1 判据：积性函数必有 $f(1)=1$，除非恒等于 0。

② (1) 恒为 0，是积性；(5) $(mn)^2=m^2n^2$，是完全积性。

③ (2)(3)(7) 都因 $f(1)\neq1$ 排除；(4) 是加性不是积性。

④ (6) $6!=720\neq2!\cdot3!=12$；(8) $6^6\neq2^2\cdot3^3$，都不是。

⑤ 7-2 主公式：$\sigma(p^a)=1+p+\cdots+p^a=\dfrac{p^{a+1}-1}{p-1}$。

⑥ (1) $35=5\cdot7\Rightarrow6\times8=48$；(2) $196=2^2\cdot7^2\Rightarrow7\times57=399$。

⑦ (3) $1000=2^3\cdot5^3\Rightarrow15\times156=2340$；(4) $2^{101}-1$。

⑧ (5) $3\times4\times6\times8\times12=6912$。

⑨ (6) $63\times121\times156\times57\times12=813404592$。

⑩ (7) $10!=2^8\cdot3^4\cdot5^2\cdot7\Rightarrow511\times121\times31\times8=15334088$。

⑪ (8) $20!=2^{18}3^85^47^2\cdot11\cdot13\cdot17\cdot19$，相乘得 $138913992387317 34720$。

⑫ 7-3 主公式：$\tau(n)=\Pi(a_i+1)$。

⑬ (1) $36=2^2\cdot3^2\Rightarrow9$；(2) $99=3^2\cdot11\Rightarrow6$。

⑭ (3) $144=2^4\cdot3^2\Rightarrow15$；(4) 8 个不同素数 $\Rightarrow2^8=256$。

⑮ (5) $2\cdot3\cdot4\cdot5\cdot6\cdot5\cdot6\cdot6=129600$。

⑯ (6) $19\cdot9\cdot5\cdot3\cdot2\cdot2\cdot2\cdot2=41040$。

**答案：7-1 只有 (1)(5)；7-2 依次 48、399、2340、$2^{101}-1$、6912、813404592、15334088、138913992387317 34720；7-3 依次 9、6、15、256、129600、41040。**

## ch7 · 7-4~7-7

○ 会　○ 卡　○ 不会

**7-4** 求高斯函数值：(1) $[1/4]$ (2) $[-3/4]$ (3) $[22/7]$ (4) $[-2]$ (5) $[[1/2]+[1/2]]$ (6) $[-3+[-1/2]]$.

**7-5** 证明 $[x]+[x+\frac{1}{2}]=[2x]$.

**7-6** 证明 $[x+y]\geq[x]+[y]$.

**7-7** 证明 $[2x]+[2y]\geq[x]+[y]+[x+y]$.

---

**套路：一律写 $x=[x]+\{x\}$，$0\leq\{x\}<1$，整数部分提出来，只剩小数部分的小范围取整。**

① 7-4：定义是"不超过 $x$ 的最大整数"，负数要往下取。

② (1) 0；(2) $-1\leq-\frac{3}{4}<0\Rightarrow-1$；(3) 3；(4) $-2$。

③ (5) $0+0=0$ 再取整还是 0；(6) $[-\frac{1}{2}]=-1\Rightarrow[-4]=-4$。

④ 7-5：令 $x=n+t$，$n=[x]$，$0\leq t<1$。

⑤ 左边 $=2n+[t+\frac{1}{2}]$，右边 $=2n+[2t]$，只比这两项。

⑥ 关键式子：$0\leq t<\frac{1}{2}$ 时两者都为 0；$\frac{1}{2}\leq t<1$ 时两者都为 1。

⑦ 故 $[x]+[x+\frac{1}{2}]=[2x]$ 对一切实数成立。

⑧ 7-6：$x+y=[x]+[y]+(\{x\}+\{y\})$。

⑨ 关键式子：$[x+y]=[x]+[y]+[\{x\}+\{y\}]$，末项 $\geq0$。

⑩ 故 $[x+y]\geq[x]+[y]$。

⑪ 7-7：两边同减 $2[x]+2[y]$，只需证 $[2a]+[2b]\geq[a+b]$。

⑫ 关键式子：$a+b<1$ 时右端为 0；$a+b\geq1$ 时 $a\geq\frac{1}{2}$ 或 $b\geq\frac{1}{2}$，左端 $\geq1$。

**答案：7-4 为 0、-1、3、-2、0、-4；7-5、7-6、7-7 均得证。**

## ch7 · 7-8~7-14

○ 会　○ 卡　○ 不会

**7-8** 求欧拉函数值：(1) 100 (2) 256 (3) 1001 (4) 2·3·5·7·11·13 (5) 10! (6) 20!.

**7-9** 证明 $\varphi(5186)=\varphi(5187)=\varphi(5188)$.

**7-10** 证明：$n$ 有 $k$ 个不同奇素因子时 $2^k \mid \varphi(n)$.

**7-11** 证明：$n$ 为奇素数时 $\varphi(4n)=2\varphi(n)$.

**7-12** 证明：$p \nmid n \Leftrightarrow \varphi(np)=(p-1)\varphi(n)$.

**7-13** 证明：$(m,n)=p$ 时 $\varphi(mn)=\dfrac{p}{p-1}\varphi(m)\varphi(n)$.

**7-14** 证明 $\varphi(m^k)=m^{k-1}\varphi(m)$.

---

**套路：$\varphi$ 积性 + $\varphi(p^a)=p^a-p^{a-1}$；不互素时先把公共素因子的幂次单独拆出来。**

① 7-8 主公式：$\varphi(n)=n\prod\left(1-\dfrac{1}{p}\right)$。

② (1) $100=2^2\,5^2 \Rightarrow 40$；(2) $256=2^8 \Rightarrow 2^8-2^7=128$。

③ (3) $1001=7\cdot11\cdot13 \Rightarrow 6\cdot10\cdot12=720$。

④ (4) $1\cdot2\cdot4\cdot6\cdot10\cdot12=5760$。

⑤ (5) $10!=2^8\,3^4\,5^2\cdot7 \Rightarrow 128\cdot54\cdot20\cdot6=829440$。

⑥ (6) $20!=2^{18}3^8 5^4 7^2\cdot11\cdot13\cdot17\cdot19$，相乘得 416084687585280000。

⑦ 7-9：$5186=2\cdot2593$，$5187=3\cdot7\cdot13\cdot19$，$5188=4\cdot1297$。

⑧ 关键式子：三个都算出 2592（2592、2·6·12·18、2·1296）。

⑨ 7-10：$\varphi(n)=\varphi(2^a)\prod p_i^{a_i-1}(p_i-1)$，每个 $p_i-1$ 为偶数。

⑩ 每个奇素因子贡献一个 2，$k$ 个贡献 $2^k$，故 $2^k \mid \varphi(n)$。

⑪ 7-11：$\varphi(4n)=\varphi(4)\varphi(n)$（因 $(4,n)=1$）。

⑫ 关键式子：$\varphi(4)=2 \Rightarrow \varphi(4n)=2\varphi(n)$。

⑬ 7-12 必要性用反证：设 $p \mid n$，写 $n=p^a m$，则 $\varphi(np)$ 与 $(p-1)\varphi(n)$ 之比为 $\dfrac{p}{p-1}\neq1$，矛盾。

⑭ 充分性：$p \nmid n \Rightarrow (p,n)=1 \Rightarrow \varphi(np)=\varphi(p)\varphi(n)=(p-1)\varphi(n)$。

⑮ 7-13：写 $m=p^\alpha u$、$n=p^\beta v$，$(m,n)=p \Rightarrow \min(\alpha,\beta)=1$。

⑯ 关键式子：$\varphi(mn)=p^{\alpha+\beta-1}(p-1)\varphi(u)\varphi(v)=\dfrac{p}{p-1}\varphi(m)\varphi(n)$。

⑰ 7-14：$m=\prod p_i^{a_i}$，则 $m^k=\prod p_i^{a_i k}$。

⑱ 关键式子：$\prod p_i^{a_i(k-1)}(p_i^{a_i}-p_i^{a_i-1})=m^{k-1}\varphi(m)$。

**答案：7-8 依次 40、128、720、5760、829440、416084687585280000；7-9 都为 2592；7-10~7-14 均得证。**

## ch7 · 7-15~7-19

○ 会　○ 卡　○ 不会

**7-15** 求莫比乌斯函数值：(1) $\mu(12)$ (2) $\mu(15)$ (3) $\mu(30)$ (4) $\mu(50)$ (5) $\mu(1001)$ (6) $\mu(2\cdot3\cdot5\cdot7\cdot11\cdot13)$ (7) $\mu(10!)$.

**7-16** 求 $\mu(n)$，$100\le n\le110$.

**7-17** 证明 $\mu(n)\mu(n+1)\mu(n+2)\mu(n+3)=0$.

**7-18** 用莫比乌斯反演证明 $\varphi(n)=n\Sigma_{d\mid n}\dfrac{\mu(d)}{d}$.

**7-19** 由 $n=\Sigma_{d\mid n}\varphi(n/d)$ 证明：(1) $\varphi(p^t)=p^t-p^{t-1}$；(2) $\varphi$ 是积性函数.

**套路：先素分解——有平方因子直接 0，否则数素因子个数 $r$ 取 $(-1)^r$。**

① 7-15：定义 $\mu=0$（含平方因子），否则 $(-1)^r$。

② (1) $12=2^2\cdot3\Rightarrow0$；(2) $15=3\cdot5\Rightarrow1$。

③ (3) 30 是 3 个素数之积 $\Rightarrow-1$；(4) $50=2\cdot5^2\Rightarrow0$。

④ (5) $1001=7\cdot11\cdot13\Rightarrow-1$；(6) 6 个素数 $\Rightarrow1$。

⑤ (7) $10!$ 含 $2^2,3^2,5^2\Rightarrow0$。

⑥ 7-16：100→0，101→-1，102→-1，103→-1，104→0，105→-1。

⑦ 106→1，107→-1，108→0，109→-1，110→-1。

⑧ 7-17：连续四数中必有一个被 4 整除，即 $4\mid n+i$。

⑨ 该数含平方因子，$\mu(n+i)=0$，乘积为 0。

⑩ 7-18：已知 $\Sigma_{d\mid n}\varphi(d)=n$，即 $F(n)=n$。

⑪ 反演：$\varphi(n)=\Sigma_{d\mid n}\mu(d)\dfrac{n}{d}=n\Sigma_{d\mid n}\dfrac{\mu(d)}{d}$。

⑫ 7-19(1)：取 $n=p^t$，只有 $d=1,p$ 使 $\mu\neq0$。

⑬ 关键式子：$\varphi(p^t)=p^t-p^{t-1}$。

⑭ (2)：$F(n)=n$ 满足 $F(mn)=F(m)F(n)$，是积性。

⑮ 由"求和函数积性 $\Rightarrow$ 原函数积性"得 $\varphi$ 积性。

**答案：7-15 为 0、1、-1、0、-1、1、0；7-16 依次 0、-1、-1、-1、0、-1、1、-1、0、-1、-1；7-17~7-19 均得证。**

11

# 二次剩余

约 8 分 · 40 分钟

这一讲回答一个问题：模 p 之下，哪些数能开平方

> **一句话：**不是每个数在模 p 下都有平方根。能开方的叫二次剩余，判它的工具是勒让德符号。

? 在普通算术里，$\sqrt{4}=2$ 很好办。可要是问"模 7 之下，几的平方等于 3"呢？
把 1 到 6 的平方都列一遍：1、4、2、2、4、1。里面**没有 3**。
所以 3 在模 7 下"开不出平方"。这一讲就是学会**不用列也能判断**。

先讲清楚

## 一、先把"平方表"列出来看规律

模 7，把 1 到 6 平方：

| x | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|
| $x^2 \bmod 7$ | 1 | 4 | 2 | 2 | 4 | 1 |

三个现象值得注意：

- 结果只出现 1、2、4 三个数，**只占一半**；
- $x$ 和 $7-x$ 的平方相同（$3^2$ 和 $4^2$ 都得 2），**所以只需要算前一半**；
- 1、2、4 叫二次剩余，3、5、6 叫二次非剩余。

对一般的奇素数 $p$，$1\sim p-1$ 里恰好有 $(p-1)/2$ 个二次剩余、$(p-1)/2$ 个非剩余。这是定死的。

## 二、欧拉判别法：一次模指数就够

列平方表最笨。判断一个数 $a$ 能不能开方，只要算一个幂：

$$a^{(p-1)/2} \pmod p$$

结果是 1，说明 $a$ 是二次剩余；结果是 -1（也就是 $p-1$），说明不是。

为什么？因为费马小定理说 $a^{p-1}\equiv 1$，而 $a^{p-1}=(a^{(p-1)/2})^2$。一个数的平方等于 1，它本身只能是 1 或 -1（在模素数下只有这两个解）。

所以这个幂只有两种可能，正好用来分类。

> **算一个：**判断 5 在模 7 下是不是二次剩余。
> $(7-1)/2=3$，算 $5^3=125$。$125=17\times 7+6\equiv -1 \pmod 7$。
> 结果是 -1 ⇒ **5 是非剩余**。和上面平方表对得上。

## 三、勒让德符号：给这个判断起个名字

数学家把上面的判断写成一个符号，叫勒让德符号：

| 符号 | 含义 |
| --- | --- |
| $(\frac{a}{p})=1$ | $a$ 是二次剩余 |
| $(\frac{a}{p})=-1$ | $a$ 是非剩余 |
| $(\frac{a}{p})=0$ | $p$ 整除 $a$ |

它最大的好处是可以**拆开算**。四条性质必须记：

- 可乘：$(\frac{ab}{p})=(\frac{a}{p})(\frac{b}{p})$；
- 平方因子直接扔掉：$(\frac{a^2}{p})=1$；
- $(\frac{-1}{p})=(-1)^{(p-1)/2}$，即 $p\equiv 1 \pmod 4$ 时为 1；
- $(\frac{2}{p})=(-1)^{(p^2-1)/8}$，即 $p\equiv \pm 1 \pmod 8$ 时为 1。

## 四、二次互反律：把大数翻成小数

遇到 $(\frac{3}{53})$ 这种"下面大、上面小"的符号，硬算要算 $3^{26}$，太大了。

互反律允许你把上下翻转：

$$(\frac{p}{q})(\frac{q}{p})=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$$

翻译成人话：**除非 $p$ 和 $q$ 都 $\equiv 3 \pmod 4$（这时要添一个负号），否则直接翻。**

> **算 $(\frac{3}{53})$：**
>
> 53 模 4 余 1 ⇒ 翻面不加负号：$(\frac{3}{53})=(\frac{53}{3})$。
>
> 53 模 3 余 2 ⇒ 变成 $(\frac{2}{3})$。
>
> 模 3 的平方只有 1，2 不在里面 ⇒ -1。
>
> **答案 −1。**

这就是标准流程：**先分解、再翻面、再化小、最后查表。**

## 五、和密码学的关系

判断"一个数是不是二次剩余"很容易，但**反过来求平方根很难**（对大素数而言）。这个不对称性被用在了 Rabin 加密和素性检测里。

另外，如果一个数在模 $n$ 下是二次剩余，攻击者可以借此推断信息 —— 所以二次剩余也是很多密码分析的工具。

**停一下：** $\left(\frac{-1}{7}\right)$ 等于多少?

$7 \equiv 3 \pmod 4$，所以 $\left(\frac{-1}{7}\right)=(-1)^{(7-1)/2}=(-1)^3=-1$。

含义：模 7 下 −1（也就是 6）不是二次剩余。查平方表：1、4、2 里确实没有 6。

**必背 · 六条**

| | |
|---|---|
| $a^{(p-1)/2} \equiv \pm 1$ | 欧拉判别 |
| 一半剩余、一半非剩余 | $(p-1)/2$ 个 |
| $\left(\frac{ab}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ | 可乘 |
| 平方因子扔掉 | 值恒为 1 |
| $\left(\frac{-1}{p}\right)=(-1)^{(p-1)/2}$ | 看模 4 |
| 互反律：都 ≡3 mod 4 才添负号 | 翻面 |

**课本 8-6** 8 分 勒让德符号计算

计算 $(\frac{7}{79})$ 与 $(\frac{15}{101})$。

---

**第一题：$(\frac{7}{79})$。**

**第一步：看分母模 4。**$79\equiv 3 \pmod 4$，7 也 $\equiv 3 \pmod 4$，**两个都 ≡3，翻面要添负号。**

**第二步：翻面。**$(\frac{7}{79})=-(\frac{79}{7})$。

**第三步：把 79 化到模 7 内。**$79=11\times 7+2$，所以 $=-(\frac{2}{7})$。

**第四步：用 2 的公式。**$7\equiv -1 \pmod 8 \Rightarrow (\frac{2}{7})=1$。

所以结果 $=-1$。

**第二题：$(\frac{15}{101})$。**

**第一步：分解上面的数。**$15=3\times 5$，拆成 $(\frac{3}{101})(\frac{5}{101})$。

**第二步：算 $(\frac{3}{101})$。**$101\equiv 1 \pmod 4$，翻面不加负号，$=(\frac{101}{3})=(\frac{2}{3})=-1$。

**第三步：算 $(\frac{5}{101})$。**$101\equiv 1 \pmod 4$，翻面不加负号，$=(\frac{101}{5})=(\frac{1}{5})=1$。

**第四步：相乘。**$(-1)\times 1=-1$。

**答案：$(\frac{7}{79})=-1$，$(\frac{15}{101})=-1$。**

这类题唯一容易错的地方就是**那个负号**。规则：上下两个数都 ≡3 mod 4 时才添，其余情况直接翻。

⚠ **三个坑：**

① **翻面时无脑加负号。**只有 $p$、$q$ 都 $\equiv 3 \pmod 4$ 才加。$p\equiv 1 \pmod 4$ 时永远不加，这是最常见错误。

② **上面的数是合数不分解。**$(\frac{15}{101})$ 直接硬算 15 的 50 次方不现实，必须先拆成 3 和 5。

③ **忘了 $(\frac{a}{p})=0$ 的情况。**$p \mid a$ 时符号是 0，不是 ±1，判断题里容易漏。

**自测 · 3 道**

1. 模 11 下，2 是不是二次剩余?
2. $(\frac{2}{7})$ 等于多少?
3. $(\frac{3}{7})$ 翻面时要不要加负号?

**1.** $2^5=32\equiv -1 \pmod{11}$ ⇒ 不是，符号为 −1。

**2.** $7\equiv -1 \pmod 8$ ⇒ $(\frac{2}{7})=1$。

**3.** 3 和 7 都 $\equiv 3 \pmod 4$ ⇒ **要加负号**。

## ch8 · 习题 3 道

### ch8 · 8-1~8-3

○ 会　○ 卡　○ 不会

**8-1** 给出各模数的全部二次剩余：3、5、13、19、7、8、15、18.

**8-2** 计算 $(\frac{j}{5})$，$j$=1,2,3,4.

**8-3** 用欧拉判别法与高斯引理分别算 $(\frac{11}{7})$.

---

**套路：判二次剩余三条路——枚举平方、欧拉判别、高斯引理数"超半"个数。**

① 8-1：把 $1^2,2^2,\ldots$ 逐个模 $n$，去重就是全部二次剩余。

② 只需算到 $\frac{n-1}{2}$：$a^2\equiv(n-a)^2$，后一半全重复。

③ 关键式子：模 3 得 1；模 5 得 1,4；模 7 得 1,2,4。

④ 模 13：平方依次 1,4,9,3,12,10。

⑤ 模 19：得 {1,4,5,6,7,9,11,16,17}，正好 9 个。

⑥ 模 8：奇数平方恒 $\equiv1$，再算非互素的平方得 0,1,4。

⑦ 模 15：0,1,4,6,9,10。

⑧ 模 18：互素平方 {1,7,13}，非互素另有 0,4,9,16。

⑨ 8-2：模 5 的平方只有 1 和 4。

⑩ 关键式子：$(\frac{1}{5})=(\frac{4}{5})=1$，$(\frac{2}{5})=(\frac{3}{5})=-1$。

⑪ 8-3 欧拉判别：$11^3\equiv4^3=64\equiv1\pmod 7$。

⑫ 高斯引理：$11\equiv4$，看 $4j$ 模 7 的最小正剩余（$j$=1,2,3）。

⑬ 关键式子：4,8,12→4,1,5，超过 $\frac{7}{2}$ 的有 2 个。

⑭ 偶数个"超半" ⇒ 符号 $(-1)^2=1$，两法一致。

**答案：8-1 依次为 {1}、{1,4}、{1,3,4,9,10,12}、{1,4,5,6,7,9,11,16,17}、{1,2,4}、{0,1,4}、{0,1,4,6,9,10}、{0,1,4,7,9,13,16}；8-2 依次 1、-1、-1、1；8-3 得 1。**

## ch8 · 8-4~8-5,8-7~8-8

○ 会　○ 卡　○ 不会

**8-4** 证明：$p \nmid ab$ 时 $a$、$b$、$ab$ 中要么恰有一个是二次剩余，要么全是.

**8-5** 证明：$q \nmid n$ 时 $(\frac{n}{q})=\Pi_{i=1}^{k}(\frac{p_i}{q})$（$p_i$ 取指数为奇数的素因子）.

**8-7** 用互反律证明 $(\frac{3}{p})$ 在 $p\equiv\pm1 \pmod{12}$ 时为 1.

**8-8** 证明 $(\frac{-3}{p})=1 \Leftrightarrow p\equiv1 \pmod 6$.

---

**套路：一切靠 $(\frac{ab}{p})=(\frac{a}{p})(\frac{b}{p})$ 加互反律，把符号拆成小素数。**

① 8-4：只看两个符号的四种正负组合。

② 两个 1 ⇒ 乘积也是 1，三个全是剩余。

③ 一正一负 ⇒ 乘积 -1，恰有一个剩余（是那个负的）。

④ 两个 -1 ⇒ 乘积 1，恰有一个剩余（是 $ab$）。

⑤ 关键式子：$(\frac{a}{p})(\frac{b}{p})=(\frac{ab}{p})$。

⑥ 8-5：对 $n$ 的每个素幂反复用可乘性。

⑦ 关键式子：$(\frac{n}{q})=\Pi(\frac{p_i}{q})^{e_i}$，偶次幂都变 1。

⑧ 故只剩指数为奇的那些 $p_i$，得证。

⑨ 8-7：先互反，$(\frac{3}{p})(\frac{p}{3})=(-1)^{(p-1)/2}$。

⑩ 关键式子：$(\frac{3}{p})=(\frac{p}{3})(-1)^{(p-1)/2}$，只看 $p \bmod 12$。

⑪ $p\equiv1,5,7,11 \pmod{12}$ 时 $(\frac{p}{3})$ 依次 1,-1,1,-1。

⑫ $(-1)^{(p-1)/2}$ 依次 1,1,-1,-1，相乘得 1,-1,-1,1。

⑬ 即 $p\equiv\pm1$ 取 1，$p\equiv5,7$ 取 -1。

⑭ 8-8：$(\frac{-3}{p})=(\frac{-1}{p})(\frac{3}{p})$。

⑮ 关键式子：$(\frac{-3}{p})=(\frac{p}{3})$，两个奇偶因子恰好抵消。

⑯ 故 $p\equiv1 \pmod 3$ 取 1，即 $p\equiv1 \pmod 6$。

**答案：8-4、8-5 得证；8-7 $p\equiv\pm1 \pmod{12}$ 为 1、$p\equiv5,7 \pmod{12}$ 为 -1；8-8 $p\equiv1 \pmod 6$ 为 1，$p\equiv5 \pmod 6$ 为 -1。**

## ch8 · 8-6,8-9~8-11

○ 会　○ 卡　○ 不会

**8-6** 算勒让德符号：(1) $(\frac{3}{53})$ (2) $(\frac{7}{79})$ (3) $(\frac{15}{101})$ (4) $(\frac{31}{641})$ (5) $(\frac{111}{991})$ (6) $(\frac{105}{1009})$.

**8-9** 算雅可比符号：(1) $(\frac{5}{21})$ (2) $(\frac{27}{101})$ (3) $(\frac{111}{1001})$ (4) $(\frac{1009}{2307})$ (5) $(\frac{2663}{3299})$ (6) $(\frac{10001}{20003})$.

**8-10** 哪些与 15 互素的 $n$ 使 $(\frac{15}{n})=1$?

**8-11** 哪些与 30 互素的 $n$ 使 $(\frac{30}{n})=1$?

---

**套路：大数先变小，能分解就分解，再互反翻面，全程只盯符号。**

① 8-6(1)：$(\frac{3}{53})=(\frac{53}{3})=(\frac{2}{3})=-1$。

② (2)：$(\frac{7}{79})=-(\frac{79}{7})=-(\frac{2}{7})=-1$。

③ (3)：拆 $(\frac{3}{101})(\frac{5}{101})$，$101\equiv 5 \pmod{12}$。

④ 关键式子：$(\frac{3}{101})=-1$，$(\frac{5}{101})=(\frac{1}{5})=1$，积为 -1。

⑤ (4)：$641\equiv 1 \pmod 4$，化为 $(\frac{641}{31})=(\frac{21}{31})$。

⑥ 关键式子：$(\frac{21}{31})=(\frac{3}{31})(\frac{7}{31})=(-1)(1)=-1$。

⑦ (5)：$111=3\cdot 37$，$991\equiv 7 \pmod{12}$ 先给一个 -1。

⑧ 关键式子：$(\frac{37}{991})=(\frac{29}{37})=(\frac{8}{29})=-1$，两负得正。

⑨ (6)：$105=3\cdot 5\cdot 7$，1009 模 12,5,7 余 1,4,1。

⑩ 关键式子：三个符号全是 1，故 $(\frac{105}{1009})=1$。

⑪ 8-9 是雅可比：分母合数先分解，其余规则照旧。

⑫ 关键式子：$(\frac{5}{21})=(\frac{2}{3})(\frac{5}{7})=(-1)(-1)=1$。

⑬ (2)：$(\frac{27}{101})=(\frac{3}{101})^3=(-1)^3=-1$。

⑭ (3)：$1001=7\cdot 11\cdot 13$，111 余 6,1,7。

⑮ 关键式子：$(\frac{6}{7})(\frac{1}{11})(\frac{7}{13})=(-1)(1)(-1)=1$。

⑯ (4)：$2307=3\cdot 769$，$1009\equiv 240 \pmod{769}$。

⑰ 关键式子：$240=2^4 3\cdot 5$，两个符号都是 1。

⑱ (5)：两数都 $\equiv 3 \pmod 4$，翻面添负号。

⑲ 关键式子：$(\frac{3299}{2663})=(\frac{636}{2663})$，$636=4\cdot 3\cdot 53$。

⑳ 关键式子：$(\frac{3}{2663})=(\frac{53}{2663})=1$，故整体 -1。

㉑ (6)：$20003=83\cdot241$，$10001$ 余 $41$、$120$。

㉒ 关键式子：$(\frac{41}{83})=1$，$(\frac{120}{241})=1$。

㉓ 8-10：$n$ 奇且与 15 互素，$(\frac{15}{n})=(\frac{3}{n})(\frac{5}{n})$。

㉔ 关键式子：$(\frac{3}{n})=1 \Leftrightarrow n\equiv\pm1 \pmod{12}$。

㉕ 再用 $(\frac{5}{n})=(\frac{n}{5})$，两条件 CRT 合并，周期 60。

㉖ 8-11：多一个 $(\frac{2}{n})$，三因子周期 8,12,5，总周期 120。

㉗ 关键式子：$n\equiv\pm1 \pmod 8$ 时 $(\frac{2}{n})=1$，合并得 16 类。

**答案：8-6 依次 -1,-1,-1,-1,1,1；8-9 依次 1,-1,1,1,-1,1；8-10 为 $n\equiv1,7,11,17,43,49,53,59 \pmod{60}$；8-11 为 $n\equiv1,7,13,17,19,29,37,49,71,83,91,101,103,107,113,119 \pmod{120}$。**

## 12 原根与指数

约 8 分 · 35 分钟

这一讲找一个数，它的幂能把所有非零数都生成出来

> **一句话：**原根就是"一个能当底数、把 $1\sim p-1$ 全部生成出来"的数；它的阶等于 $\varphi(p)$。

? 模 7，拿 2 当底数：2、4、1、2、4、1…… 只有三个数，循环了。
换成 3：3、2、6、4、5、1 —— **六个非零数全出现了。**
3 就是模 7 的原根。这一讲就是学会判断"谁是原根"。

先讲清楚

### 一、先讲"阶"：第一次回到 1 要几次

对 $a$ 和模 $m$，使 $a^d\equiv1 \pmod m$ 的最小正整数 $d$，叫 $a$ 的阶，记 $\mathrm{ord}_m(a)$。

上面模 7 的例子：2 的幂是 2、4、1 ⇒ 阶是 3；3 的幂要 6 次才回 1 ⇒ 阶是 6。

**关键性质：阶一定整除 $\varphi(m)$。**模 7 时 $\varphi(7)=6$，所以阶只能是 1、2、3、6，不可能是 4 或 5。

这条性质省掉大量计算 —— 不用一个个试，只试 $\varphi(m)$ 的因子。

### 二、原根：阶等于 $\varphi(m)$ 的那个数

如果 $a$ 的阶正好等于 $\varphi(p)=p-1$，那 $a$ 的幂就能跑遍所有 $1\sim p-1$。这个 $a$ 就叫**原根**。

模 $p$（$p$ 为素数）时原根一定存在，而且一共有 $\varphi(p\text{-}1)$ 个。

比如模 7：$p$-1=6，$\varphi(6)$=2，所以有 2 个原根，是 3 和 5。

## 三、怎么判：只验 $\varphi(p)$ 的素因子

要判 $g$ 是不是模 $p$ 的原根，不用验所有指数，**只需验 $\varphi(p)$ 的每个素因子 $q$**：

$$\text{对每个 } q|(p\text{-}1)\text{，检查 } g^{(p-1)/q}\neg\equiv 1 \pmod p$$

全部不成立 ⇒ $g$ 是原根。只要有一个成立，$g$ 就不是。

为什么？因为如果阶小于 $p$-1，它一定是 $p$-1 的真因子，而真因子必定整除某个 $(p\text{-}1)/q$。所以只要这些位置都不是 1，阶就只能是 $p$-1。

> **判 2 是不是模 11 的原根：**
> $p$-1=10=2×5，素因子是 2 和 5。
> 验 $(p\text{-}1)/2$=5：$2^5$=32≡-1≠1 ✓
> 验 $(p\text{-}1)/5$=2：$2^2$=4≠1 ✓
> 两个都不成立 ⇒ 阶是 10 ⇒ **2 是原根**。

## 四、哪些模数有原根

不是所有模数都有原根。结论是：

$$m \text{ 有原根} \Leftrightarrow m=2,\ 4,\ p^k,\ 2p^k\ (p \text{ 为奇素数})$$

比如 8 没有原根（$m$=8 不在这个表里），12 也没有，20 也没有。

做题时先查这个表，没有原根就直接答"不存在"，不用白算。

## 五、指数（离散对数）：把乘法变成加法

如果 $g$ 是原根，那任何 $a$ 都能写成 $a\equiv g^k$。这个 $k$ 叫 $a$ 的指数，记 $\text{ind}_g\, a$。

它的用处是：$\text{ind}(ab)=\text{ind}\, a+\text{ind}\, b \pmod{p\text{-}1}$。**乘法变成了加法。**

这就是密码学里的离散对数问题：算 $g^k$ 很快（反复平方），可反过来由 $g^k$ 求 $k$ 很难。Diffie-Hellman 密钥交换就建在这个不对称上。

> **停一下：**模 7 的原根有几个？分别是哪几个？

$\varphi(6)$=2，所以有 2 个。

3 是原根；另一个是 $3^5 \bmod 7$=5。

验证：5 的幂是 5、4、6、2、3、1，确实跑遍六个非零数 ✓

**必背 · 五条**

| | |
|---|---|
| 阶整除 $\varphi(m)$ | 先缩小范围 |
| 原根 ⇔ 阶 = $p$-1 | 定义 |
| $g^{(p-1)/q}\neq 1$（每素因子） | 判据 |
| 有原根：$2,4,p^k,2p^k$ | 先查这张表 |
| $\mathrm{ind}(ab)=\mathrm{ind}a+\mathrm{ind}b$ | 乘法变加法 |

**课本 9-3** 8 分 证明 2 是原根

证明 2 是模 11 的原根，并求出模 11 的所有原根。

**第一步：算目标值。**$\varphi(11)=10$，要证 $\mathrm{ord}_{11}(2)=10$。

**第二步：分解 $p$-1。**$10=2\times5$，不同的素因子是 2 和 5，所以只需验两个指数：5 和 2。

**第三步：逐个验。**

$2^5=32=2\times11+10\equiv-1\neq1$ ✓
$2^2=4\neq1$ ✓

**第四步：下结论。**阶既不整除 5 也不整除 2，又必须整除 10，只能是 10。所以 2 是原根。

**第五步：求全部原根。**原根个数是 $\varphi(\varphi(11))=\varphi(10)=4$。

它们就是 2 的幂里指数与 10 互素的那几个：$2^1=2$、$2^3=8$、$2^7=7$、$2^9=6$。

**答案：2 是原根；模 11 的四个原根是 2、6、7、8。**

为什么"指数与 10 互素"？因为 $\mathrm{ord}(g^k)=\dfrac{p-1}{(k,p-1)}$，只有 $(k,p-1)=1$ 时阶才等于 $p$-1。

⚠ **三个坑：**
① **把 $\varphi(p)$ 的所有因子都验一遍。**不用。只需验 $(p-1)/q$ 这几个指数，其中 $q$ 取**不同的素因子**。验多了浪费时间，还容易算错。
② **以为所有模数都有原根。**8、12、20、28 都没有。做题前先查 $2,4,p^k,2p^k$。

③ **把阶和 $\varphi$ 搞混。**阶是"这个元素"回到 1 的次数，$\varphi$ 是"模数"的性质。两者可以相等（那就是原根），但一般不相等。

**自测 · 3 道**

1. 模 7 的 2 的阶是多少？它是原根吗？
2. 模 13 有几个原根？
3. 8 有原根吗？

**1.** 2、4、1 ⇒ 阶是 3；$\varphi(7)=6\neq 3$ ⇒ 不是原根。

**2.** $\varphi(\varphi(13))=\varphi(12)=4$ 个。

**3.** 没有。8 不属于 $2,4,p^k,2p^k$。

## ch9 · 习题 4 道

### ch9 · 9-1~9-4

○ 会　○ 卡　○ 不会

**9-1** 求阶：(1) $\mathrm{ord}_5 2$ (2) $\mathrm{ord}_{10}3$ (3) $\mathrm{ord}_{13}10$ (4) $\mathrm{ord}_{10}7$.

**9-2** 求阶：(1) $\mathrm{ord}_{11}3$ (2) $\mathrm{ord}_{17}2$ (3) $\mathrm{ord}_{21}10$ (4) $\mathrm{ord}_{25}9$.

**9-3** 证明 5 是模 6 的原根.

**9-4** 证明 2 是模 11 的原根.

---

**套路：求阶就是从一次方开始连乘，第一次变成 1 的指数就是阶。**

① 阶的定义：使 $a^k\equiv1 \pmod n$ 的最小正整数 $k$。

② 它必整除 $\varphi(n)$，所以乘到 $\varphi(n)$ 必停。

③ 9-1(1)：模 5 幂为 2,4,3,1 ⇒ 阶 4。

④ (2)：模 10 幂为 3,9,7,1 ⇒ 阶 4。

⑤ (3)：模 13 幂为 10,9,12,3,4,1 ⇒ 阶 6。

⑥ (4)：模 10 幂为 7,9,3,1 ⇒ 阶 4。

⑦ 9-2(1)：模 11 幂为 3,9,5,4,1 ⇒ 阶 5。

⑧ (2)：模 17 幂为 2,4,8,16,15,13,9,1 ⇒ 阶 8。

⑨ (3)：模 21 幂为 10,16,13,4,19,1 ⇒ 阶 6。

⑩ 关键式子：$9^5\equiv-1 \pmod{25}$ ⇒ $9^{10}\equiv1$，阶 10。

⑪ 9-3：$\varphi(6)=2$，只要排除 $k=1$。

⑫ 关键式子：$5\neq1$ 而 $5^2=25\equiv1 \pmod 6$，故是原根。

⑬ 9-4：费马给 $2^{10}\equiv1 \pmod{11}$，只需排除 1、2、5。

⑭ 关键式子：$2^2=4\neq1$，$2^5=32\equiv-1 \pmod{11}$。

⑮ 故阶为 $10=\varphi(11)$，2 是原根。

**答案：9-1 依次 4、4、6、4；9-2 依次 5、8、6、10；9-3、9-4 均得证。**

## ch9 · 9-5~9-7,9-12,9-14~9-17

○ 会 ○ 卡 ○ 不会

**9-5** 给出模 4、5、10、13、14、18 的一个原根.

**9-6** 证明 12 没有原根.

**9-7** 证明 20 没有原根.

**9-12** 给出模 7 的所有原根.

**9-14** 判断 4、10、16、22、28 哪些有原根.

**9-15** 给出模 $3^2,5^2,23^2,29^2$ 的一个原根.

**9-16** 给出模 $10,3^4,3^8,50$ 的一个原根.

**9-17** 给出模 22 的所有原根.

**套路：先查 $n=2,4,p^t,2p^t$ 判存在，再找一个根，用 $(u,\varphi(n))=1$ 生全部。**

① 存在性：$n>1$ 有原根 $\Leftrightarrow n=2,4,p^t,2p^t$。

② 9-5：都从 2 开始试，乘到阶 $=\varphi(n)$ 为止。

③ 关键式子：模 4 用 3；模 5 用 2；模 10 用 3。

④ 关键式子：模 13 用 2；模 14 用 3；模 18 用 5。

⑤ 验算：模 14 上 $3,9,13,11,5,1$，第 6 次到 1 ✓。

⑥ 9-6：模 12 的单位只有 $1,5,7,11$。

⑦ 关键式子：$5^2\equiv7^2\equiv11^2\equiv1$，阶最高 2。

⑧ 而 $\varphi(12)=4$，故无原根。

⑨ 9-7：模 20 的 8 个单位阶最高只到 4。

⑩ 关键式子：$\mathrm{ord}_{20}3=\mathrm{ord}_{20}7=4<8$。

⑪ 9-12：原根个数 $\varphi(6)=2$。

⑫ 关键式子：3 的幂 $3,2,6,4,5,1$，$5=3^5$ 也是原根。

⑬ 9-14：4、10、22 有；16、28 没有。

⑭ 16 的阶最高 4、28 的最高 6，都够不到 $\varphi$。

⑮ 9-15：先取模 $p$ 的根，再验它在模 $p^2$ 上不降阶。

⑯ 关键式子：$3^2$ 用 2；$5^2$ 用 2（$2^4\not\equiv1\pmod{25}$）。

⑰ $23^2$ 用 5；$29^2$ 用 2。

⑱ 9-16：10 用 3；$3^4$ 与 $3^8$ 都用 2。

⑲ 关键式子：2 模 $3^k$ 的阶是 $2\cdot3^{k-1}=\varphi(3^k)$。

⑳ 50 用 3（是模 25 的根且为奇数）。

㉑ 9-17：原根数 $\varphi(\varphi(22))=\varphi(10)=4$。

㉒ 关键式子：模 11 的根 $2,6,7,8$，偶的加 11。

㉓ 故模 22 原根为 $7,13,17,19$。

答案：9-5 依次 3、2、3、2、3、5；9-6、9-7 得证；9-12 为 3、5；9-14 是 4、10、22；9-15 依次 2、2、5、2；9-16 依次 3、2、2、3；9-17 为 7,13,17,19。

## ch9 · 9-8~9-11,9-13,9-18

○ 会　○ 卡　○ 不会

**9-8** 证明 $\mathrm{ord}_n a=\mathrm{ord}_n b$（$b$ 是 $a$ 的逆元）.

**9-9** 证明：$(a,n)=(b,n)=1$ 且两阶互素时 $\mathrm{ord}_n(ab)=\mathrm{ord}_n a\cdot\mathrm{ord}_n b$.

**9-10** 求下列多项式模 11 的根数：(1) $x^2+2$ (2) $x^2+10$ (3) $x^3+x^2+2x+2$ (4) $x^4+x^2+1$.

**9-11** 求根数：(1) 7 (2) 13 (3) 17 (4) 19 (5) 29 (6) 47（原书此题干只印常数，按同类题读作 $x^2\equiv a \pmod{11}$）.

**9-13** 证明：$p\equiv 1 \pmod 4$ 时 $-r$ 也是原根.

**9-18** 证明：模 $2p^t$ 与模 $p^t$ 的原根个数相同.

---

**套路：说理题不动蛮力，把"阶"翻成整除，把"根"翻成因式分解。**

① 9-8：$(ab)^k\equiv a^kb^k\equiv 1$，两边同时成立。

② 关键式子：$a^k\equiv 1 \Leftrightarrow b^k\equiv 1$，故两阶相等。

③ 9-9：先证 $(ab)^{rs}\equiv 1$，故 $\mathrm{ord}(ab)\mid rs$。

④ 关键式子：$(ab)^{rs}=(a^r)^s(b^s)^r\equiv 1$。

⑤ 设 $t=\mathrm{ord}(ab)$，把 $(ab)^t\equiv 1$ 取 $s$ 次方。

⑥ 关键式子：$a^{ts}\equiv 1 \Rightarrow r\mid ts$，又 $(r,s)=1 \Rightarrow r\mid t$。

⑦ 同理 $s\mid t$，与 $t\mid rs$ 合并得 $t=rs$。

⑧ 9-10：模 11 直接代 $x=0..10$ 数根最快。

⑨ 关键式子：$x^2\equiv 9 \Rightarrow$ 根 3、8；$x^2\equiv 1 \Rightarrow$ 根 1、10。

⑩ (3)：$=(x+1)(x^2+2)$，根是 10 加 3、8。

⑪ (4)：$=(x^2+x+1)(x^2-x+1)$，判别式都是 $-3$。

⑫ 关键式子：$(\frac{-3}{11})=(\frac{8}{11})=-1$，故无根。

⑬ 9-11：根数 $=1+(\frac{a}{11})$，先算出各 $a$ 的符号。

⑭ 关键式子：7、13、17、19、29、47 模 11 为 7,2,6,8,7,3。

⑮ 其中 2、6、7、8 是剩余，3 不是，故根数依次 2、2、2、2、2、0。

⑯ 9-13：$-1$ 是唯一 2 阶元，故 $-1\equiv r^{(p-1)/2}$。

⑰ 关键式子：$-r\equiv r^{1+(p-1)/2}$，指数 $u=1+\frac{p-1}{2}$ 为奇数。

⑱ $p\equiv 1 \pmod 4 \Rightarrow u$ 与 $p-1$ 互素 $\Rightarrow r^u$ 是原根。

⑲ 9-18：模 $2p^t$ 的每个单位类只有一个奇代表。

⑳ 关键式子：$r$ 是模 $2p^t$ 原根 $\Leftrightarrow r$ 奇且是模 $p^t$ 原根。

㉑ 又 $\varphi(2p^t)=\varphi(p^t)$，两边原根数都是 $\varphi(\varphi(p^t))$。

**答案：9-8、9-9、9-13、9-18 得证；9-10 依次 2、2、3、0；9-11 依次 2、2、2、2、2、0。**

## ch9 · 9-19~9-22

○ 会　○ 卡　○ 不会

**9-19** 构造以 5 为原根的模 23 指数表.

**9-20** 解：(1) $3x^5\equiv 1 \pmod{23}$ (2) $3x^{14}\equiv 2 \pmod{23}$ (3) $3x\equiv 2 \pmod{23}$ (4) $13x\equiv 5 \pmod{23}$.

**9-21** $a$ 取何值时 $ax^4\equiv 2 \pmod{13}$ 可解?

**9-22** 证明：$p$ 奇素数、$r$ 为其原根时 $\operatorname{ind}_r(p-1)=\dfrac{p-1}{2}$.

---

**套路：先建指数表，取 ind 把乘法与乘方全变成模 $\varphi(n)$ 的加法。**

① 9-19：先确认 5 是模 23 的原根。

② 关键式子：$5^{11}\equiv -1 \pmod{23}\Rightarrow$ 阶 22。

③ 逐次乘 5 并模 23 取余。

④ 关键式子：$5^0..5^{10}$ 为 1,5,2,10,4,20,8,17,16,11,9。

⑤ 关键式子：$5^{11}..5^{21}$ 为 22,18,21,13,19,3,15,6,7,12,14。

⑥ 反过来读就是 $\operatorname{ind}_5 a$ 对照表。

⑦ 9-20：两边取 ind，令 $t=\operatorname{ind}_5 x$。

⑧ (1)：$16+5t\equiv 0 \pmod{22}\Rightarrow t\equiv 10$。

⑨ 关键式子：$x\equiv 5^{10}=9 \pmod{23}$。

⑩ (2)：$16+14t\equiv 2\Rightarrow 7t\equiv 4 \pmod{11}$。

⑪ 关键式子：$t\equiv 10$ 或 $21\Rightarrow x\equiv 9$ 或 14。

⑫ (3)：$16+t\equiv 2\Rightarrow t=8\Rightarrow x\equiv 16$。

⑬ (4)：$14+t\equiv 1\Rightarrow t=9\Rightarrow x\equiv 11$。

⑭ 9-21：模 13 取原根 2，$\varphi(13)=12$。

⑮ 关键式子：记 $u=\operatorname{ind}_2 a$，则 $u+4t\equiv 1 \pmod{12}$。

⑯ 可解 $\Leftrightarrow 4\mid(1-u)\Leftrightarrow u\equiv 1 \pmod 4$。

⑰ 关键式子：$u=1,5,9\Rightarrow a\equiv 2,6,5 \pmod{13}$。

⑱ 9-22：-1 是唯一的 2 阶元。

⑲ 关键式子：$r^{(p-1)/2}\equiv -1\Rightarrow \operatorname{ind}_r(p-1)=\dfrac{p-1}{2}$。

**答案：9-19 指数表见④⑤；9-20 依次 $x\equiv 9$、$x\equiv 9,14$、$x\equiv 16$、$x\equiv 11 \pmod{23}$；9-21 当 $a\equiv 2,5,6 \pmod{13}$；9-22 得证。**

## 13 群、环、域

约 8 分 · 45 分钟

这一讲把"数"的规则一层层抽出来，看每加一条会多出什么

**一句话：**群、环、域是同一套东西的三级：一个运算能倒着做叫群，再加一个乘法叫环，乘法也能除叫域。

? 你从小就会算整数：能加、能减、能乘，除不整就写分数。
数学家把这些"本能"拆成一条条要求，然后看：**只满足前几条的，能得到什么？少一条会坏在哪里？**
这一讲就是把这件事走一遍 —— 你会看到每个定义都不是凭空来的，是"不给它就出问题"。

一层层加上去

## 一、先只看加法：为什么需要"群"

自然数 1、2、3..... 能加，但 3−5 算不了。想要"减法永远能做"，就得有负数。

抽象出来，一个集合配上加法，要满足四条才能叫**群**：

1. **封闭**：两个元素加完还在集合里；
2. **结合律**：$(a+b)+c=a+(b+c)$；
3. **有单位元**：有个 $e$ 使 $a+e=a$（加法里就是 0）；
4. **有逆元**：每个 $a$ 都有个 $-a$ 使 $a+(-a)=e$。

第四条就是我们想要的"能倒着做"。**缺了它，减法就没定义。**

如果还满足交换律 $a+b=b+a$，叫**交换群**。整数加法就是交换群。

## 二、乘法就不一样了

整数配乘法，前三条也满足：封闭、结合、单位元是 1。但第四条**不满足** —— 2 的倒数 $1/2$ 不是整数。

所以"整数乘法"只是**半群**（只有封闭和结合），连群都不是。**"能乘不能除"就是从这里来的。**

## 三、两个运算放在一起：环

既要有加法又要有乘法，就得规定它们怎么配合。这就是**环**：

- 加法构成交换群；
- 乘法封闭且结合；
- 乘法对加法有分配律：$a(b+c)=ab+ac$。

整数、多项式、$\mathbb{Z}_m$ 都是环。

如果乘法还交换，并且**没有零因子**（$ab=0$ 只能推出 $a=0$ 或 $b=0$），叫**整环**。整数就是整环。

> **零因子是什么？** $\mathbb{Z}_6$ 里 $2\times3=6\equiv0$，但 2 和 3 都不是 0。
> 这就是零因子。有零因子的环里，**消去律不成立**：$2\times1\equiv2\times4 \pmod 6$，但不能推出 $1=4$。

## 四、能除就叫域

域的要求最狠：整环，**并且每个非零元都有乘法逆元**。

所以域里四则运算全能做，而且除法（除以非零数）永远有答案。

| 结构 | 要求 | 例子 |
| --- | --- | --- |
| 群 | 一个运算，可逆 | $\mathbb{Z}$ 配加法 |
| 环 | 两个运算 + 分配律 | $\mathbb{Z}$、$\mathbb{Z}_6$、$F[x]$ |
| 整环 | 环 + 交换 + 无零因子 | $\mathbb{Z}$、$\mathbb{Z}_7$ |
| **域** | 整环 + 非零元可逆 | $\mathbb{Q}$、$\mathbb{R}$、$\mathbb{Z}_p$ |

一条最重要的结论：**$\mathbb{Z}_m$ 是域 ⇔ $m$ 是素数。**

为什么？$m$ 是合数时，$m=ab$，那 $a$ 和 $b$ 就是零因子，$a$ 不可能有逆元。$m$ 是素数时，$1\sim p\text{-}1$ 每个数都和 $p$ 互素，用扩展欧几里得都能求出逆元。

## 五、拉格朗日定理：子群的阶必须整除

如果 $H$ 是群 $G$ 的子群，那么 $|H|$ 一定整除 $|G|$。

比如一个 6 阶群，子群只能是 1、2、3、6 阶，不可能是 4 阶。

推论很常用：**元素的阶一定整除群的阶**。所以判断原根时，只需要验 $\varphi(p)$ 的因子 —— 这条规则就是拉格朗日给的。

还有一条：素数阶群一定是循环群，因为除单位元外每个元素的阶都只能是这个素数。

## 六、同态与同构："像不像"

如果映射 $\varphi$ 满足 $\varphi(ab)=\varphi(a)\varphi(b)$，叫**同态** —— 它保持运算。

如果 $\varphi$ 还是一一对应，叫**同构**，两个结构本质上是同一个东西，只是换了名字。

同态基本定理：$G/\ker\varphi\cong\mathrm{Im}\,\varphi$。**核**是被映到单位元的那些元素 —— 核越大，丢的信息越多。

**停一下：$\mathbb{Z}_8$ 是域吗？为什么？**

不是。8 不是素数。

具体看：$2\times4=8\equiv0\pmod 8$，2 和 4 都是零因子。

而且 2 没有逆元 —— 解 $2x\equiv1\pmod 8$，因为 $(2,8)=2\nmid1$，无解。

**必背 · 六条**

| | |
|---|---|
| 群四公理：封闭、结合、单位、逆 | 缺一不可 |
| $\|H\|$ 整除 $\|G\|$ | 拉格朗日 |
| 元素阶整除群阶 | 判原根靠它 |
| $\mathbb{Z}_m$ 是域 $\Leftrightarrow$ $m$ 素 | 最常考 |
| 整环 = 环 + 交换 + 无零因子 | $\mathbb{Z}$ 是典型 |
| $G/\ker\varphi \cong \mathrm{Im}\varphi$ | 同态基本定理 |

**课本 10-1** 8 分 判断是不是群

在正整数集上定义 $a^{\circ}\ b=a+b+ab$，问是否构成群。若把集合换成"全体整数"呢?

**第一步：先找单位元。**设单位元为 $e$，则对任意 $a$ 要有 $a^{\circ}\ e=a$，即 $a+e+ae=a$。

整理得 $e(1+a)=0$。因为 $a$ 是正整数，$1+a\neq 0$，所以只能 $e=0$。

**第二步：检查 $e$ 在不在集合里。**集合是**正整数**，而 0 不是正整数。

单位元都不存在 $\Rightarrow$ **不构成群**。

**第三步：换成正整数之外的场景看看。**如果把集合换成全体整数，$e=0$ 就在集合里了。

**第四步：那这时有逆元吗?** 要 $a^{\circ}\ b=0$，即 $a+b+ab=0$，整理得 $(a+1)(b+1)=1$。

$a+1=\pm 1 \Rightarrow a=0$ 或 $a=-2$。所以只有 0 和 −2 有逆元，其余元素没有。

还是不构成群。

**答案：正整数集上不构成群（无单位元）；全体整数上也不构成群（大多数元素无逆元）。**

这道题有个漂亮的观察：$a^{\circ}\ b+1=(a+1)(b+1)$，所以这个运算本质是"乘法"，只是把数平移了 1。平移之后 0 就跑到集合外面去了 —— 这就是它不成群的根本原因。

⚠ **三个坑：**

① **以为整环就是域。**$\mathbb{Z}$ 是整环，但不是域（2 没有整数逆元）。差别就在"逆元"这一条。

② **把"无零因子"和"有逆元"当成一回事。**没有零因子只保证消去律成立，不保证每个元素都

能除。

③ **判断群时漏查单位元。**很多题就是死在单位元不在集合里（比如本题的 0）。

**自测 · 3 道**

1. $\mathbb{Z}_{12}$ 是域吗?
2. 一个 12 阶群，可能有 5 阶子群吗?
3. 整环和域差哪一条?

**1.** 不是，12 不是素数，有零因子（如 $3\times4=0$）。

**2.** 不可能。5 不整除 12，违反拉格朗日定理。

**3.** 差"每个非零元都有乘法逆元"。整环保证没有零因子，域才保证能除。

## ch10 · 习题 6 道

### ch10 · 10-1~10-5

○ 会 ○ 卡 ○ 不会

**10-1** 在正整数集上定义 $a^{\circ}\ b=a+b+ab$，是否构成群?

**10-2** $G=\{(a,b)|\ a\neq0\}$，$(a,b)^{\circ}(c,d)=(ac,ad+b)$，证明构成群.

**10-3** 证明：每个元都满足 $x^2=e$ 的群必是交换群.

**10-4** 证明：$a$ 与 $a^{-1}$ 同阶.

**10-5** 设 $a$ 的阶为 $n$，证明 $a^s=a^t \Leftrightarrow n|(s-t)$.

**套路：群题先查封闭、结合、单位、逆四条；见幂次就用阶的定义换成整除。**

① 10-1：设单位元为 $e$，令 $a+e+ae=a$ 得 $e=0$。

② 关键：0 不在正整数集中 ⇒ **不构成群**。

③ （另一看法：$a^{\circ}\ b+1=(a+1)(b+1)$，像集从 2 起，缺单位元 1。

） ④ 10-2：封闭：$ac\neq0$ ✓；结合：两边都是 $(ace,\ acf+ad+b)$。

⑤ 单位元 $(1,0)$；逆元 $(a,b)^{-1}=(1/a,\ -b/a)$ ⇒ 是群。

⑥ 10-3：$x^2=e$ ⇒ 每元自逆，$(ab)^2=e$。

⑦ 关键式子：$ab=(ab)^{-1}=b^{-1}a^{-1}=ba$，故交换。

⑧ 10-4：$a^k=e \Leftrightarrow (a^k)^{-1}=e \Leftrightarrow (a^{-1})^k=e$，两者同阶。

⑨ 10-5：两边乘 $a^{-t}$ 得 $a^{s-t}=e$。

⑩ 关键式子：由阶的定义即 $n|(s-t)$。

**答案：10-1 不是群（无单位元）；10-2 是群且非交换；10-3~10-5 得证。**

## ch10 · 10-6~10-8

○ 会　○ 卡　○ 不会

**10-6** $|G|>2$ 且每元满足 $x^2=e$，证明 $G$ 有 4 阶子群.

**10-7** $H,K$ 为子群，$|H|=m$、$|K|=n$，$(m,n)=1$，证明 $H\cap K=\{e\}$.

**10-8** 证明 $|HK|=\dfrac{|H||K|}{|H\cap K|}$.

---

**套路：子群题先找公共子群，再用"阶整除"或"数纤维"收尾。**

① 10-6：由 10-3 知 $G$ 交换；取 $a\neq b$ 且都不等于 $e$。

② 则 $ab$ 也不同于 $e,a,b$。

③ 关键：$\{e,a,b,ab\}$ 对乘法封闭，是 4 阶子群（Klein 四元群）。

④ 10-7：$H\cap K$ 同时是 $H$ 与 $K$ 的子群。

⑤ 关键式子：$|H\cap K|\mid m$ 且 $\mid n$，而 $(m,n)=1$。

⑥ 故 $|H\cap K|=1$，即 $H\cap K=\{e\}$。

⑦ 10-8：作映射 $H\times K\to HK$，$(h,k)\mapsto hk$。

⑧ $hk=h'k'\Leftrightarrow h'^{-1}h=k'k^{-1}\in H\cap K$。

⑨ 关键式子：每根纤维恰 $|H\cap K|$ 个原像 ⇒ 公式成立。

**答案：10-6 得 $\{e,a,b,ab\}$；10-7 交集只有 $e$；10-8 得证。**

## ch10 · 10-9~10-13

○ 会　○ 卡　○ 不会

**10-9** 有单位元环 $R$，定义 $a^{\circ}\ b=a+b-ab$，$a\odot\ b=a+b-1$，证明 $(R,\odot,^{\circ})$ 也是有单位元的环.

**10-10** 布尔环（$a^2=a$）：证明 $a+a=0$、$ab=ba$.

**10-11** 证明：布尔环若有 3 个以上元素，则不是整环.

**10-12** 证明：无零因子的环满足消去律.

**10-13** 证明：除环有单位元且无零因子.

---

**套路：换运算的环用同构搬运公理；布尔环靠 $a^2=a$ 与 $x+x=0$ 两招。**

① 10-9：取 $\varphi(a)=1-a$，是双射。

② 关键式子：$\varphi(a\odot\ b)=\varphi(a)+\varphi(b)$，$\varphi(a^{\circ}\ b)=\varphi(a)\varphi(b)$。

③ 故与 $(R,+,\cdot)$ 同构 ⇒ 是环；零元 1，单位元 0，加法逆元 $2-a$。

④ 10-10：$(a+a)^2=a+a$ 展开得 $4a=2a$ ⇒ $a+a=0$。

⑤ 关键式子：$(a+b)^2=a+b$ 展开得 $ab+ba=0$ ⇒ $ab=ba$。

⑥ 10-11：取 $a\neq 0,1$，则 $a(a+1)=a^2+a=a+a=0$。

⑦ 关键：两个非零元相乘为 0 ⇒ 不是整环。

⑧ 10-12：$ab=ac$ ⇒ $a(b-c)=0$。

⑨ 关键：$a\neq 0$ 且无零因子 ⇒ $b=c$。

⑩ 10-13：$R-\{0\}$ 是乘法群 ⇒ 有单位元 1。

⑪ 关键：群对乘法封闭 ⇒ 非零元之积非零 ⇒ 无零因子。

**答案：10-9 是环（零元 1、单位元 0）；10-10~10-13 得证。**

## ch10 · 10-14~10-19

○ 会　○ 卡　○ 不会

**10-14** 证明有单位元的整环是域.

**10-15** 证明 $\mathbb{Z}[\sqrt{-5}]$ 中 $a=(2+\sqrt{-5})(2-\sqrt{-5})$ 与 $b=3(2+\sqrt{-5})$ 无最大公因子.

**10-16** 是否存在只有一个元素的域?

**10-17** 写出 $GF(5)$、$GF(7)$、$GF(9)$ 的加法与乘法表.

**10-18** 证明 $\mathbb{Z}_2$、$\mathbb{Z}_3$ 是域.

**10-19** 证明：$R$ 为整环时 $R[x]$ 的可逆元就是 $R$ 的可逆元.

---

**套路：整环与域只差"逆元"；有限时用消去律，无限时直接举反例。**

① 10-14：原题漏了"有限"二字 —— $\mathbb{Z}$ 是反例。

② 有限整环取 $a\neq 0$，$x\mapsto ax$ 无零因子故单射。

③ 关键：有限集上单射即满射 ⇒ 存在 $x$ 使 $ax=1$ ⇒ 非零元全可逆。

④ 10-15：取范数 $N(x+y\sqrt{-5})=x^2+5y^2$，得 $N(a)=N(b)=81$。

⑤ 3 与 $2+\sqrt{-5}$ 都不可约，且都整除 $a,b$。

⑥ 关键：若 gcd 存在则 $3(2+\sqrt{-5})$ 整除它，取范数得 $N(d)=81$ ⇒ 两者相伴。

⑦ 但 $9/(6+3\sqrt{-5})=(2-\sqrt{-5})/3$ 不在环中，矛盾。

⑧ 10-16：不存在 —— 域要求 $0\neq 1$。

⑨ 若 $1=0$，则 $a=a\cdot 1=a\cdot 0=0$，只剩一个元素。

⑩ 10-17：$GF(5)$、$GF(7)$ 的表就是 $i+j$、$ij$ 取模。

⑪ $GF(9)$：元记作 $a+bx$，$x^2=-1=2$，加法逐分量模 3。

⑫ 关键式子：$(a+bx)(c+dx)=(ac+2bd)+(ad+bc)x$。

⑬ 10-18：$\mathbb{Z}_p$ 交换、无零因子，且 $1\cdot 1=1$、$2\cdot 2=4=1$ ⇒ 非零元可逆。

⑭ 10-19：整环中 $\deg(fg)=\deg f+\deg g$。

⑮ 关键：$fg=1$ ⇒ 次数和为 0 ⇒ $f$ 是 0 次且为 $R$ 的可逆元。

**答案：10-14 须补"有限"；10-15 无 gcd；10-16 不存在；10-17 见表；10-18、10-19 得证。**

## ch10 · 10-20~10-26

○ 会 ○ 卡 ○ 不会

**10-20** 证明域与其子域有相同的单位元.

**10-21** 证明有限域的非零元全体对乘法构成循环群.

**10-22** 证明元素个数大于 1 的整环中 $0\neq1$.

**10-23** 证明有零因子的环不能是域.

**10-24** 求 $f(x)=4x^3-2x^2+x+3$ 在 $\mathbb{Z}_5$ 中的全部根.

**10-25** 给出 $\mathbb{Z}_3$ 上所有二次不可约多项式.

**10-26** 给出 $F[x]$ 中的可逆元.

---

**套路：两个单位元相乘做桥梁；无零因子就能搬"根的个数不超过次数"。**

① 10-20：设 $1_F$、$1_K$，则 $1_K\cdot1_F=1_K=1_K\cdot1_K$。

② 关键式子：$1_K(1_F-1_K)=0$，域无零因子且 $1_K\neq0\Rightarrow1_F=1_K$。

③ 10-21：设非零元阶的最大值为 $m$，交换群中各元阶都整除 $m$。

④ $q-1$ 个非零元全是 $x^m-1$ 的根 $\Rightarrow q-1\leq m$。

⑤ 关键：又 $m\mid q-1\Rightarrow m=q-1\Rightarrow$ 存在 $q-1$ 阶元 $\Rightarrow$ 循环。

⑥ 10-22：若 $1=0$，则 $a=a\cdot1=a\cdot0=0$，只剩一个元素，矛盾。

⑦ 10-23：设 $ab=0$ 而 $a,b\neq0$，则 $b=1\cdot b=a^{-1}ab=0$，矛盾。

⑧ 10-24：代入 $x=0,1,2,3,4$ 得 $f=3,1,4,1,1$。

⑨ 关键：全不为 0 $\Rightarrow\mathbb{Z}_5$ 中无根（3 次无根即不可约）。

⑩ 10-25：首一二次式无根即不可约。

⑪ 关键式子：$x^2+1$、$x^2+x+2$、$x^2+2x+2$ 在 $\mathbb{Z}_3$ 中无根。

⑫ 10-26：$fg=1\Rightarrow\deg f+\deg g=0\Rightarrow f$ 是常数且非零。

**答案：10-20 单位元相同；10-21 循环；10-22、10-23 得证；10-24 无根；10-25 上面三个；10-26 为 $F$ 的非零元。**

## ch10 · 10-27~10-32

○ 会　○ 卡　○ 不会

**10-27** 证明 $\mathbb{Z}[i]$ 的可逆元只有 $\pm 1, \pm i$.

**10-28** 证明 $\mathbb{Z}[i]$ 中 5 的分解唯一.

**10-29** 证明域必是欧氏环.

**10-30** 证明：2 次、3 次多项式无根即不可约.

**10-31** 用 $x^4+x+1$ 构造 16 元域并给出乘法表与对数表.

**10-32** 在 $F_3[x]$ 中用 $p(x)=x^4+x+1$ 构造域.

---

**套路：高斯整数用范数 $N=a^2+b^2$；多项式用次数；造域先验不可约再排对数表。**

① 10-27：$uv=1 \Rightarrow N(u)N(v)=1 \Rightarrow a^2+b^2=1$。

② 关键：整数解只有 $(\pm 1,0),(0,\pm 1) \Rightarrow$ 可逆元为 $\pm 1, \pm i$。

③ 10-28：$5=(2+i)(2-i)$，$N(2\pm i)=5$ 为素数 $\Rightarrow$ 二者不可约。

④ 任一分解取范数得 25，只能是两个范数 5 的因子。

⑤ 关键：范数 5 的元互相差一个单位 $\Rightarrow$ 分解唯一。

⑥ 10-29：取 $\delta(0)=0$、$\delta(a)=1$，则 $a=(a/b)b+0$ 且 $\delta(0)<\delta(b)$。

⑦ 10-30：若 $f=gh$ 可约，则必有一因子是 1 次。

⑧ 关键：1 次因子必给出域中的根，与"无根"矛盾。

⑨ 10-31：$GF(16)=F_2[x]/(x^4+x+1)$，$x^4=x+1$。

⑩ 对数表：$1, x, x^2, x^3, x+1, x^2+x, x^3+x^2, x^3+x+1, x^2+1, x^3+x, x^2+x+1, x^3+x^2+x, x^3+x^2+x+1, x^3+x^2+1, x^3+1$。

⑪ 关键：$\alpha^i \cdot \alpha^j = \alpha^{(i+j) \bmod 15}$。

⑫ 10-32：勘误 —— $x^4+x+1$ 在 $F_3$ 有根 1，可约。

⑬ 改用 $x^4+x+2$（不可约且本原），$\alpha^4=2\alpha+1$，阶 80。

⑭ 关键：81 个元为 $a_0+a_1x+a_2x^2+a_3x^3$，乘法按 $\alpha^k\alpha^l=\alpha^{(k+l) \bmod 80}$。

**答案：10-27 只有 $\pm 1, \pm i$；10-28~10-30 得证；10-31 见表；10-32 须把 $x^4+x+1$ 换成 $x^4+x+2$。**

---

# 14 有限域

约 10 分 · 45 分钟

这一讲造一个只有 4 个元素的域 —— 你会看到为什么要用多项式

> **一句话：** 有限域的阶只能是 $p^n$；$p^n$ 元的域不是模 $p^n$，而是"模一个不可约多项式"造出来的。

? 我们想要一个只有 4 个元素的域。
最直觉的想法是模 4：元素 0、1、2、3。可它坏在一个地方 —— $2\times2=4\equiv0$，但 2 不是 0。**有零因子，不是域。**
那 4 元域到底长什么样？这一讲就把它造出来。

先讲清楚

## 一、先记住一条硬结论

有限域的元素个数一定是 $p^n$（$p$ 素数，$n\geq1$），写成 $GF(p^n)$。

所以**不存在 6 元域、10 元域、12 元域**。看到"证明 6 元域不存在"这种题，一句话就能答：6 不是素数幂。

这条结论的来源是：有限域里有个"特征" $p$，它把素域 $GF(p)$ 装在里面，而整个域是这个素域上的 $n$ 维向量空间，所以元素个数是 $p^n$。

## 二、$GF(p)$ 就是模素数

$p$ 是素数时，$\mathbb{Z}_p$ 就是 $GF(p)$。加减乘都模 $p$，除法靠乘逆元。

比如 $GF(7)$ 里 $3\div5$ 就是 $3\times5^{-1}=3\times3=2$（因为 $5\times3=15\equiv1$）。

## 三、$GF(p^n)$：把多项式当成数

$n>1$ 时不能再用"模 $p^n$"。正确做法是：

$$GF(p^n)=GF(p)[x]/(m(x))$$

其中 $m(x)$ 是 $GF(p)$ 上一个 **$n$ 次不可约多项式**。

翻译一下：**元素是系数在 $GF(p)$、次数小于 $n$ 的多项式**；加法按系数模 $p$ 相加；乘法是多项式相乘之后，再模 $m(x)$ 取余。

为什么这样就成域？因为 $m(x)$ 不可约，等价于"模它之后没有零因子"，于是每个非零元都能求逆。

## 四、造 $GF(4)$：亲手算一遍

取 $p=2$、$n=2$，需要 $GF(2)$ 上一个 2 次不可约多项式。

$GF(2)$ 上 2 次多项式只有四个：$x^2$、$x^2+1$、$x^2+x$、$x^2+x+1$。

前三个都可约：$x^2=x\cdot x$；$x^2+1=(x+1)^2$（因为在 $GF(2)$ 里 $1+1=0$，两倍交叉项消失）；$x^2+x=x(x+1)$。

只剩 $\boldsymbol{m(x)=x^2+x+1}$ 不可约。

于是 $GF(4)=\{0,1,x,x+1\}$，共 4 个元素。

| 运算 | 例子 | 怎么算 |
| --- | --- | --- |
| 加法 | $x+(x+1)=(x+x)+1=1$ | 系数模 2，$x+x=0$ |

| | | |
|---|---|---|
| 乘法 | $x \cdot x = x^2$ | 再模 $m(x)$：$x^2 \equiv x+1$ |
| 乘法 | $x(x+1) = x^2+x \equiv (x+1)+x = 1$ | 所以 $x$ 的逆元是 $x+1$ |

注意最后一行：$x$ 乘以 $x+1$ 等于 1，**说明 $x$ 有逆元**。这就是"域"的关键 —— 每个非零元都能除。

### 五、本原元与最小多项式

非零元一共有 $p^n-1$ 个，它们在乘法下构成一个**循环群**。这个循环群的生成元叫**本原元**。

以本原元为根的那个不可约多项式，叫**本原多项式**。AES 用的 $x^8+x^4+x^3+x+1$ 就是本原多项式。

一个元素的**最小多项式**，是以它为根、次数最低的首一多项式。它一定不可约，而且整除 $x^{p^n}-x$。

### 六、和 AES 的关系

AES 的每个字节（8 位）就是 $GF(2^8)$ 里的一个元素，即一个 7 次以下的多项式。

加密时的"替换"本质上是在 $GF(2^8)$ 里求乘法逆元；"列混合"是乘一个固定的多项式。

为什么用 $GF(2^8)$ 而不是 $\mathbb{Z}_{256}$？因为 256 不是素数，$\mathbb{Z}_{256}$ 里 2 和 128 都是零因子，没法做除法。

> **停一下：$GF(2^3)$ 有几个元素？加法是什么运算？**

$2^3=8$ 个元素：系数在 $GF(2)$、次数小于 3 的多项式，从 0 到 $x^2+x+1$。

加法就是**按位异或**（系数模 2 相加，没有进位）。

乘法要模一个 3 次不可约多项式，比如 $x^3+x+1$。

**必背 · 六条**

| | |
|---|---|
| $\lvert F\rvert = p^n$ | 只有素数幂 |
| $GF(p^n) = GF(p)[x]/(m(x))$ | 模不可约多项式 |
| 元素 = 次数小于 $n$ 的多项式 | 共 $p^n$ 个 |
| $GF(2)$ 里 $1+1=0$ | 所以加法是异或 |
| 非零元构成循环群 | 生成元叫本原元 |
| $\mathbb{Z}_{p^n}$ 不是域（$n>1$） | 有零因子 |

**课本 11-1** 8 分 特征与元素个数

求 $GF(5)$、$GF(27)$、$GF(64)$ 的特征；并说明 $GF(27)$ 里的元素长什么样、加法怎么算。

---

**第一步：把"特征"翻译成人话。**特征 = 最少几个单位元相加能得到 0。

**第二步：对 $GF(p^n)$ 直接用结论。**特征就是那个素数 $p$，与 $n$ 无关。

$GF(5)$ 特征 5；$GF(27)=GF(3^3)$ 特征 3；$GF(64)=GF(2^6)$ 特征 2。

**第三步：写 $GF(27)$ 的元素。**$p=3$、$n=3$，所以元素是系数在 $GF(3)$、次数小于 3 的多项式：

$a_0+a_1x+a_2x^2$，其中每个 $a_i\in\{0,1,2\}$，一共 $3^3=27$ 个。

**第四步：说加法。**逐位系数相加，再模 3。比如 $(1+x)+(2+x^2)=1+2+x+x^2\equiv 0+x+x^2=x+x^2$。

**第五步：说乘法。**多项式相乘后，模一个 3 次不可约多项式（比如 $x^3+2x+1$）取余。

**答案：特征依次 5、3、2；$GF(27)$ 的元素是 27 个二次以下多项式，加法按系数模 3 相加。**

最容易错的：把 $GF(27)$ 当成 $\mathbb{Z}_{27}$。$\mathbb{Z}_{27}$ 里有零因子（$3\times 9=27=0$），根本不是域。

⚠ **三个坑：**

① **把 $GF(p^n)$ 当成 $\mathbb{Z}_{p^n}$。**这是本章第一大错。$\mathbb{Z}_4$ 不是域，$GF(4)$ 才是；两回事。

② **多项式乘法忘了模 $m(x)$。**算完相乘还要取余，否则元素会跑出"次数小于 $n$"的范围。

③ **在 $GF(2^n)$ 里按普通整数加法。**$GF(2)$ 里 $1+1=0$，所以加法是异或，不进位。

**自测 · 3 道**

1. $GF(16)$ 的特征是多少?
2. 存在 12 元域吗?
3. $GF(4)$ 里 $x$ 的逆元是什么?

**1.** $16=2^4\Rightarrow$ 特征是 2。

**2.** 不存在。12 不是素数幂。

**3.** $x+1$（因为 $x(x+1)=x^2+x\equiv(x+1)+x=1$）。

## ch11 · 习题 2 道

### ch11 · 11-1~11-5

○ 会　○ 卡　○ 不会

**11-1** 求特征：(1) $GF(5)$ (2) $GF(27)$ (3) $GF(64)$ (4) 复数域.

**11-2** 证明 $Z_2$ 上 $(f(x))^2=f(x^2)$.

**11-3** 证明：$\beta$ 是 $f$ 的根 $\Rightarrow \beta^{2^k}$ 也是.

**11-4** 求使 2 和 3 都是原根的最小素数 $p$.

**11-5** 在 $GF(73)$ 中求 ord(2)、ord(3)，并给出阶为 lcm 的元素.

---

**套路：特征是"几个 $e$ 相加为 0"；原根只看阶是否等于 $p$-1。**

① 11-1：$GF(5)$ 特征 5；$GF(27)$ 特征 3。

② $GF(64)$ 特征 2；复数域中 $ne\neq 0 \Rightarrow$ 特征 0。

③ 11-2：$Z_2$ 中 $2uv=0 \Rightarrow (u+v)^2=u^2+v^2$。

④ 关键：逐项平方再相加即 $(f(x))^2=f(x^2)$。

⑤ 11-3：由 11-2，$0=(f(\beta))^2=f(\beta^2)$。

⑥ 关键：反复 $k$ 次 $\Rightarrow \beta^{2^k}$ 也是根。

⑦ 11-4：$p=2,3$ 时有元为 0，不算原根。

⑧ 关键：$p=5$ 时 $\text{ord}(2)=\text{ord}(3)=4=p-1$。

⑨ 11-5：$2^9=512=73\times 7+1$ 且 $2^3=8\neq 1 \Rightarrow \text{ord}(2)=9$。

⑩ 关键：$3^6\equiv -1 \Rightarrow \text{ord}(3)=12$。

⑪ 取 $6=2\cdot 3$，$\text{lcm}(9,12)=36 \Rightarrow \text{ord}(6)=36$。

**答案：11-1 为 5、3、2、0；11-2、11-3 得证；11-4 $p=5$；11-5 阶为 9、12，元素 6 的阶为 36。**

## ch11 · 11-6~11-11

○ 会　○ 卡　○ 不会

**11-6** 证明：(1) $a$ 与 $a^{-1}$ 同阶；(2) $(s,t)=1$ 时 $ab$ 的阶为 $st$；(3) $a$ 为 3 阶元时 $a^2+a+1=0$，$a+1$ 为 6 阶.

**11-7** $x^2-1=0$ 在 $\mathbb{Z}_{16}$ 中有几个根?

**11-8** 求 $GF(9)$、$GF(32)$ 的全部本原元.

**11-9** $GF(49)$ 中 $\alpha^2=3$：(1) $\alpha$ 的阶? (2) 原根与 $\alpha$ 的表示? (3) 该原根的最小多项式?

**11-10** $x^4+x^3+1$、$x^3+x+1$ 是本原多项式吗?

**11-11** 用 $x^3+2x+1$ 构造 $GF(27)$，列出元素、最小多项式与阶.

---

**套路：阶题一律"阶整除指数"；本原元即阶 $q-1$ 的元。**

① 11-6(1)：$a^k=e \Leftrightarrow (a^{-1})^k=e$，同阶。

② (2)：$(ab)^k=1 \Rightarrow a^k=b^{-k}$，其阶同时整除 $s,t$ ⇒ 为 1。

③ 关键：$s\mid k$、$t\mid k$、$(s,t)=1 \Rightarrow st\mid k$。

④ (3)：$a^3=1, a\neq 1 \Rightarrow (a-1)(a^2+a+1)=0 \Rightarrow a^2+a+1=0$。

⑤ 关键式子：$(a+1)^3=a^2+a=-1$，$(a+1)^6=1$ ⇒ 阶 6。

⑥ 11-7：解 $x^2\equiv 1 \pmod{16}$，试得 $x=1,7,9,15$。

⑦ 关键：共 4 个根（$\mathbb{Z}_{16}$ 不是域，根数可超 2）。

⑧ 11-8：$GF(9)$ 中 $x^2=2$，阶 8 的元是 $1+x,1+2x,2+x,2+2x$。

⑨ $GF(32)$ 非零元群阶 31 为素数 ⇒ 除 1 外 30 个全是本原元。

⑩ 11-9：$\alpha^2=3$，3 在 $Z_7$ 中阶为 6 ⇒ $\mathrm{ord}(\alpha)=12$。

⑪ 关键：取 $g=1+x$，$\mathrm{ord}(g)=48$，且 $\alpha=g^{20}$。

⑫ $g+g^7=2$、$g\cdot g^7=5$ ⇒ 最小多项式 $x^2+5x+5$。

⑬ 11-10：$x^4+x^3+1$ 不可约，$x$ 的阶 15 ⇒ 是本原多项式。

⑭ 关键：$x^3+x+1$ 不可约，$GF(8)$ 非零元群阶 7 为素数 ⇒ 阶 7 ⇒ 本原。

⑮ 11-11：$\alpha^3=\alpha+2$，$\mathrm{ord}(\alpha)=26$。

⑯ 27 个元为 $a_0+a_1x+a_2x^2$，阶分布：1 个阶 1、1 个阶 2、12 个阶 13、13 个阶 26。

⑰ 关键：最小多项式按共轭链 $\{\alpha^k,\alpha^{3k},\alpha^{9k}\}$ 取。

**答案：11-6 得证；11-7 共 4 个；11-8 $GF(9)$ 四个、$GF(32)$ 除 1 外 30 个；11-9 阶 12，$g=1+x$，$\alpha=g^{20}$，$m(x)=x^2+5x+5$；11-10 两者都是；11-11 见表。**

---

15 **椭圆曲线基础**

约 6 分 · 30 分钟

这一讲给"点"重新定义一种加法，然后拿它做密码

**一句话：**椭圆曲线上的点可以"相加"，加出来的点还在曲线上；这个加法单向难逆，就成了 ECC 的根基。

? 两个点怎么相加？如果按坐标直接加，$(1,2)+(3,4)=(4,6)$，这和曲线毫无关系，加完多半不在曲线上。
所以要重新定义一种加法：**让结果一定落在曲线上**。定义方式很几何 —— 连线、找交点、翻折。

先讲清楚

## 一、曲线长什么样

椭圆曲线不是椭圆。它指的是形如

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

的一类曲线，还要求 $4a^3+27b^2\neq 0$（否则曲线会有尖点或自交，加法就定义不好）。

在实数上它像一个"钩子"：右边开口向上，左边一叶。在有限域上它就是一堆散点，没有形状可言。

## 二、加法怎么定义：三步

给两个点 $P$、$Q$，求 $P+Q$ 的几何做法：

1. 连一条直线过 $P$ 和 $Q$；
2. 这条直线和曲线还会交于第三点 $R'$；
3. 把 $R'$ 关于 $x$ 轴翻折，得到 $P+Q$。

为什么要翻折？因为曲线关于 $x$ 轴对称，翻折后一定还在曲线上 —— 这样"加法"才封闭。

如果 $P=Q$，就用过 $P$ 的切线代替割线，这叫"倍点"。

如果 $Q=-P$（关于 $x$ 轴对称），直线垂直于 $x$ 轴，交点是"无穷远点"，记作 $O$，它是这个加法的单位元。

## 三、换成代数公式

几何画不出精确值，得换成算式。设 $P=(x_1,y_1)$、$Q=(x_2,y_2)$：

$$\lambda=\frac{y_2-y_1}{x_2-x_1}\ (P\neq Q)\quad 或\quad \frac{3x_1^2+a}{2y_1}\ (P=Q)$$

$$x_3=\lambda^2-x_1-x_2,\quad y_3=\lambda(x_1-x_3)-y_1$$

这两条式子要背。注意 $P=Q$ 时不能用两点式 —— 分母为 0。

## 四、在有限域上算

密码学里所有运算都在 $GF(p)$ 上做，所以每一步都要取模，除法要乘逆元。

**算一个：** $GF(7)$ 上曲线 $y^2=x^3+3x+2$，$P=(0,3)$，求 $2P$。

先验 $P$ 在曲线上：右边 $=0+0+2=2$，左边 $=9\equiv 2$ ✓

$\lambda=\dfrac{3\times 0^2+3}{2\times 3}=\dfrac{3}{6}$。模 7 下 $6^{-1}=6$，所以 $\lambda=3\times 6=18\equiv 4$。

$x_3=4^2-2\times 0=16\equiv 2$；$y_3=4(0-2)-3=-11\equiv 3$。

**$2P=(2,3)$。**

## 五、为什么这能当密码

已知点 $P$，算 $kP$（把 $P$ 加自己 $k$ 次）很快，用"倍加"算法几十步就完。

但反过来：已知 $P$ 和 $kP$，求 $k$ —— **没有快办法**。这叫椭圆曲线离散对数问题（ECDLP）。

ECC 的好处是**密钥短**：256 位 ECC 的安全强度大约等于 3072 位 RSA，所以手机、智能卡这些算力有限的地方都用它。

**停一下：** $P=(0,3)$ 的相反点 $-P$ 是什么？

关于 $x$ 轴对称，所以横坐标不变、纵坐标取负：$-P=(0,-3)\equiv(0,4)\pmod 7$。

验证：$P+(-P)=O$，因为过这两点的直线是垂直的 $x=0$。

**必背 · 五条**

| | |
|---|---|
| $y^2=x^3+ax+b$ | 曲线形式 |
| $x_3=\lambda^2-x_1-x_2$ | 横坐标 |
| $y_3=\lambda(x_1-x_3)-y_1$ | 纵坐标 |
| $P=Q$ 用切线斜率 | 不能用两点式 |
| $kP$ 易算，反求 $k$ 难 | ECDLP |

**课本 12-3** 8 分 点加与阶

$GF(7)$ 上 $y^2=x^3+3x+2$，$P=(0,3)$。求 $2P$、$3P$，并判断 $P$ 是不是本原元。

---

**第一步：算 $2P$，用切线斜率。**$P=Q$，所以

$\lambda=\dfrac{3x_1^2+a}{2y_1}=\dfrac{0+3}{6}$。模 7 下 $6^{-1}=6$，$\lambda=3\times6=18\equiv4$。

$x_3=4^2-2\times0=16\equiv2$；$y_3=4(0-2)-3=-11\equiv3$。得 $\mathbf{2P=(2,3)}$。

**第二步：算 $3P=2P+P$，用两点式。**

$\lambda=\dfrac{3-3}{2-0}=0$（两点纵坐标相同，直线水平）。

$x=0^2-2-0=-2\equiv5$；$y=0\times(0-5)-3=-3\equiv4$。得 $\mathbf{3P=(5,4)}$。

**第三步：数一共有几个点。**把 $x=0\sim6$ 代入算右边，能开方的留下：

$x=0$：右边 2，有平方根 3、4 ⇒ (0,3)、(0,4)
$x=2$：右边 8+6+2=16≡2 ⇒ (2,3)、(2,4)
$x=4$：右边 64+12+2=78≡1 ⇒ (4,1)、(4,6)
$x=5$：右边 125+15+2=142≡2 ⇒ (5,3)、(5,4)

共 8 个仿射点，加上无穷远点 $O$，**群的阶是 9**。

**第四步：判本原元。**$P$ 的阶如果等于 9，它就是本原元。已经算出 $2P$、$3P$ 都不是 $O$，继续算下去会发现 $9P=O$ 而中间的都不是，所以阶是 9。

**答案：$2P=(2,3)$，$3P=(5,4)$，群阶 9，$P$ 是本原元。**

注意 $x=1,3,6$ 算出来的右边是二次非剩余，开不出平方，所以没有点。

⚠ **三个坑：**

① **$P=Q$ 时还用两点式。**分母 $x_2-x_1=0$，直接除零。必须换成切线斜率公式。

② **忘了所有运算都在有限域上。**$\dfrac{3}{6}$ 不是 0.5，是 $3\times6^{-1}\pmod 7$。这一步错了后面全错。

③ **漏掉无穷远点 $O$。**数点的个数时，$O$ 也算一个，它是单位元。8 个仿射点 + $O$ = 9 阶。

**自测 · 3 道**

1. 椭圆曲线的单位元是什么?
2. $P=Q$ 时斜率用哪个公式?
3. ECC 相比 RSA 的主要优势是什么?

**1.** 无穷远点 $O$。

**2.** $\lambda=\dfrac{3x_1^2+a}{2y_1}$。

**3.** 同安全强度下密钥更短（256 位约等于 3072 位 RSA）。

ch12 · 习题 1 道

## ch12 · 12-1~12-3

○ 会　○ 卡　○ 不会

**12-1** 求 $GF(17)$ 上 $y^2=x^3+7$ 的全部点.

**12-2** 上题中 $P=(1,5)$、$Q=(2,7)$，求 $P+Q$ 与 $2P$.

**12-3** $GF(7)$ 上 $y^2=x^3+3x+2$：(1) 全部点；(2) 群的阶；(3) $P=(0,3)$ 求 $2P$,$3P$，$P$ 是否本原元?

---

**套路：$x$ 取遍 $0..p-1$ 算右端，查平方剩余定 $y$；加法套 $\lambda$ 公式。**

① 12-1：$GF(17)$ 的平方剩余为 0,1,2,4,8,9,13,15,16。

② 逐点算 $x^3+7$，可开方的 $x$ 为 1,2,3,5,6,8,10,12,15。

③ 关键：加上无穷远点 $O$，共 18 个点（对称成对出现）。

④ 12-2：$\lambda=\frac{7-5}{2-1}=2$。

⑤ 关键式子：$x_3=4-1-2=1$，$y_3=2(1-1)-5=12 \Rightarrow P+Q=(1,12)$。

⑥ $2P$：$\lambda=\frac{3}{10}=3\times12=2$（$10^{-1}=12$）。

⑦ 关键式子：$x_4=4-2=2$，$y_4=2(1-2)-5=10 \Rightarrow 2P=(2,10)$。

⑧ 12-3：仿射点 (0,3)(0,4)(2,3)(2,4)(4,1)(4,6)(5,3)(5,4)。

⑨ 关键：加 $O$ 共 9 个点，构成 9 阶循环群。

⑩ $2P$：$\lambda=\frac{3}{6}=3\times6=4$。

⑪ 关键式子：$x=16\equiv2$，$y=4(0-2)-3=3 \Rightarrow 2P=(2,3)$。

⑫ $3P=2P+P$：$\lambda=\frac{3-3}{2-0}=0$。

⑬ 关键式子：$x=-2\equiv5$，$y=0-3=4 \Rightarrow 3P=(5,4)$。

⑭ $P$ 的阶为 9（等于群阶）⇒ 是本原元。

**答案：12-1 共 18 个点；12-2 $P+Q=(1,12)$、$2P=(2,10)$；12-3 共 9 个点、群阶 9、$2P=(2,3)$、$3P=(5,4)$、$P$ 是本原元。**

## 16 整卷速查

考前 15 分钟

不复习知识，只记每类题的第一行

**一句话：** 拿到题先写一个式子或一个判断，写对了后面自己会走。

八类题的第一行

| 题型 | 第一行写什么 |
| --- | --- |
| 求 gcd / 逆元 | 写欧几里得除法链，一直除到余 0 |
| 线性同余 $ax \equiv b$ | 先算 $d=(a,m)$，看 $d \mid b$ 成不成立 |
| 同余式组 | 先查模数是否两两互素 |
| 大指数取模 | 指数对 $\varphi(m)$（或 $p$-1）取余 |
| 判二次剩余 | 算勒让德符号，先看分母模 4 |
| 求原根 | 分解 $p$-1，验 $g^{(p-1)/q} \neq 1$ |
| 验证群/域 | 先查封闭，再查逆元 |
| 有限域运算 | 写成多项式，模不可约多项式取余 |

## 最容易丢分的六个地方

- 负数余数写成负的（$-7 \bmod 3=2$，不是 -1）；
- 同余不互素硬约（丢了 $d$-1 个解）；
- 中国剩余定理忘了最后对 $M$ 取余；
- 指数对 $m$ 取余（应该对 $\varphi(m)$）；
- 勒让德符号翻面时无脑加负号；
- 把 $GF(p^n)$ 当成 $\mathbb{Z}_{p^n}$。

## 大题流程（背下来）

**欧几里得类：**除法链 → 读最后一个非零余数 → 倒着回代 → 写成 $ax+by$ → 取 $x$ 当逆元。

**同余式组类：**查互素 → 设 $x=a_1+m_1k$ → 代入第二式 → 解 $k$ → 回代 → 对 $M$ 取余。

**原根类：**算 $\varphi(p)$ → 分解 → 逐个验指数 → 下结论 → 用 $\varphi(\varphi(p))$ 数个原根。

**必背 · 六条**

| | |
|---|---|
| $(a,b)=(b,a \bmod b)$ | 欧几里得 |
| $ax \equiv b$：解数 $=(a,m)$ | 线性同余 |
| CRT 要求两两互素 | 否则先拆 |
| $a^{\varphi(m)} \equiv 1$，需 $(a,m)=1$ | 欧拉定理 |
| $\varphi(n)=n\Pi(1-\frac{1}{p})$ | 只用不同素因子 |
| $\lvert F \rvert = p^n$ | 有限域阶 |

⚠ **最后提醒：**交卷前把每道计算题**代回去验一遍** —— 逆元乘一下看是不是 1，CRT 的解代入每个同余式看一眼。五分钟能救回好几分。