

费马小定理与初等数论笔记

第二版 · 2026-10-10

从整除基础、欧拉定理到原根、RSA 与随机分解的概率证明

本笔记整合《介绍费马小定理》的 21 轮对话、《解释 RSA 与分解关系》的 11 轮对话，以及用户后续提供的一条加权概率补充。按证明依赖重排，合并重复内容，补全原根、群论计数与随机分解概率证明中的辅助结论。主线从良序原理、带余除法与归纳法出发。每次使用互质、质数、交换律等条件时，都说明它们发挥的作用。

来源：[原始分享对话](#) · [归档正文](#) · [读取核对报告](#)

归档保留全部可见文字、公式和原始组件源码；其中一张公式报错截图仅保留附件引用，未直接查看。本文重新排版公式，不依赖原对话的交互组件。

新增来源：[RSA 与分解分享对话](#) · [归档正文](#) · [读取核对报告](#) · [加权概率补充](#)。文末分别列出两份对话与后续补充的覆盖索引。

目录

第 1 章：路线、记号与约定	3
第 2 章：裴蜀等式、消去律与模逆元	5
第 3 章：质因数分解为何存在且唯一	7
第 4 章：费马小定理与三个应用	9
第 5 章：欧拉函数与容斥乘积	11
第 6 章：欧拉定理为何成立	13
第 7 章：乘法阶与真正最小周期	15
第 8 章：原根及质数模原根存在性	17
第 9 章：中国剩余定理的标准形式	21
第 10 章：中国剩余定理的一般形式	23
第 11 章：RSA 的指数与解密正确性	25
第 12 章：有限群、循环群与元素阶计数	28
第 13 章：有限概率、均匀映射与加权平均	33
第 14 章：已知 RSA 私钥怎样随机分解模数	37
第 15 章：随机分解成功概率的完整证明	42
第 16 章：概念辨析、拓展、练习与来源覆盖	50

第 1 章：路线、记号与约定

[返回目录](#)

1.1 这篇笔记在回答什么

大指数可以缩小，是因为模幂运算存在周期。但证明周期之前，需要知道何时能够约分；要计算周期长度和互质整数个数，又需要整数分解与计数工具。以下关系是本篇的证明骨架。

基础与结论	关键依赖	用途
裴蜀等式	良序原理、带余除法	证明互质消去律与模逆元存在
质因数分解唯一性	欧几里得引理	识别整数的质数幂结构
费马小定理	非零剩余类的排列、合法约分	质数模下缩减指数
欧拉函数乘积公式	唯一分解、容斥	计算互质剩余类个数
欧拉定理与乘法阶	互质剩余类的排列、带余除法	任意模数下的幂周期
质数模原根存在性	多项式根数上界、阶的两个引理	一个元素生成所有非零剩余类
中国剩余定理	裴蜀等式、互质消去律、质数幂分解	拆分与合并同余条件
RSA 解密正确性	模逆元、费马小定理、互质模数合并	证明加密后能够恢复消息
已知私钥的随机分解	平方根、循环群、CRT、有限概率计数	证明何时能提取因子及成功概率

RSA 解密正确性的证明不需要原根；第 15 章随机分解的精确概率证明则使用原根与循环群计数。 先读第 2—11 章可掌握正确性主线，再读第 12—15 章理解群论与概率如何解释私钥恢复和分解的联系。

1.2 整除、同余与剩余类

对整数 a, b , $a \mid b$ 表示存在整数 t , 使 $b = at$ 。本篇讨论最大公约数时, a, b 不全为零, 并取最大公约数为正数。

对正整数模数 n , 定义

$$a \equiv b \pmod{n} \iff n \mid (a - b).$$

这表示两者有相同余数, 不表示两个整数相等。一个剩余类是所有与某个整数同余的整数所组成的集合。本文常用 $0, 1, \dots, n-1$ 作为代表。

同余可以相加、相减、相乘和取非负整数次幂。以乘法为例, 若 $a \equiv b$ 、 $c \equiv d \pmod{n}$, 则

$$ac - bd = c(a - b) + b(c - d)$$

能被 n 整除。因此同余运算的规则来自普通整除性质。

同余不能无条件约分。例如 $2 \cdot 1 \equiv 2 \cdot 4 \pmod{6}$, 但 $1 \not\equiv 4 \pmod{6}$ 。第 2 章证明准确的消去条件。

1.3 范围与边界

除中国剩余定理外, 讨论欧拉定理、乘法阶与原根时默认 $n \geq 2$ 。指数默认为非负整数; 负指数只有在明确使用模逆元时才有意义。模幂中的 $a^0 = 1$ 表示乘法单位元。

欧拉函数统一定义为

$$\varphi(n) = \#\{1 \leq r \leq n : \gcd(r, n) = 1\}.$$

因此 $\varphi(1) = 1$ 。当 $n > 1$ 时, n 本身不互质, 等价于统计 $1, \dots, n-1$ 。主线中涉及 $\varphi(p-1)$ 时, 这个约定也覆盖 $p=2$ 。

第 2 章：裴蜀等式、消去律与模逆元

[返回目录](#)

2.1 从最小正线性组合证明裴蜀等式

定理。 对不全为零的整数 a, b ，存在整数 x, y ，使

$$ax + by = \gcd(a, b).$$

令

$$S = \{ax + by : x, y \in \mathbb{Z}, ax + by > 0\}.$$

集合非空：若 $a \neq 0$ ，选择 $x = 1$ 或 -1 、 $y = 0$ 即得到 $|a|$ ；否则用 $|b|$ 。由良序原理， S 有最小元素 $d > 0$ ，写作 $d = ax_0 + by_0$ 。

对 a 作带余除法： $a = qd + r$ ， $0 \leq r < d$ 。于是

$$r = a - qd = a(1 - qx_0) + b(-qy_0).$$

如果 $r > 0$ ，它也是 S 的元素，却比 d 小，矛盾。故 $r = 0$ ，即 $d \mid a$ 。同理 $d \mid b$ 。

另一方面，任意正公约数 c 都整除 a, b 的整数线性组合，所以 $c \mid d$ ，进而 $c \leq d$ 。因此 d 既是公约数，又不小于任何正公约数，正是 $\gcd(a, b)$ 。所需的 x_0, y_0 已由构造给出。证毕。

关键不是猜出线性组合，而是先取最小正组合，再用带余除法排除更小的正组合。
这个证明不依赖质因数分解，后面的论证因而没有循环。

2.2 互质消去律与欧几里得引理

若 $\gcd(a, n) = 1$ 且 $n \mid ab$ ，由裴蜀等式取 $ax + ny = 1$ ，乘以 b ：

$$b = abx + nby.$$

右侧两项均被 n 整除，故 $n \mid b$ 。这就是**互质消去律**，其中 n 不必是质数。

作为特例，若 p 是质数且 $p \mid ab$ ，则 $p \mid a$ 或 $p \mid b$ 。因为一旦 $p \nmid a$ ，质数的因数只有 $1, p$ ，所以 $\gcd(a, p) = 1$ ，可应用消去律。这称为**欧几里得引理**。

质数条件不可随意删去： $6 \mid 2 \cdot 3$ ，但 6 不整除任何一个因子。反复应用欧几里得引理，可得质数若整除有限乘积，必整除至少一个因子。

2.3 模逆元存在的充要条件

a 模 n 的逆元是满足 $au \equiv 1 \pmod{n}$ 的整数 u 。对 $n \geq 2$ ，有

$$a \text{ 模 } n \text{ 有逆元} \iff \gcd(a, n) = 1.$$

充分性：由 $ax + ny = 1$ ，取 $u = x$ 。

必要性：若 $au - nv = 1$ ， a, n 的每个公约数都整除左边，因此整除 1 ，所以只能为 1 。

逆元在模 n 意义下唯一：若 $au \equiv av \equiv 1$ ，则 $n \mid a(u - v)$ ；由互质消去律， $n \mid (u - v)$ 。

因此，当 $\gcd(a, n) = 1$ 时，从 $ab \equiv ac \pmod{n}$ 可以乘以逆元，推出 $b \equiv c \pmod{n}$ 。这是后面约去阶乘或剩余类乘积的依据。

2.4 两个常用推论

互质因子的乘积仍与模数互质。若 $ax + ny = 1$ 、 $bu + nv = 1$ ，相乘得到

$$abxu + n(axv + buy + nyv) = 1.$$

任意 ab, n 的公约数都整除 1 ，故 $\gcd(ab, n) = 1$ 。有限多个因子可归纳处理。

互质的两个数都整除一个整数，则其乘积也整除。若 $\gcd(m, n) = 1$ 、 $m \mid A$ 、 $n \mid A$ ，写 $A = mt$ 。由 $n \mid mt$ 与消去律， $n \mid t$ ，故 $mn \mid A$ 。

2.5 如何实际计算逆元

带余除法给出 $\gcd(a, b) = \gcd(b, r)$ ，因为 $a = qb + r$ 使两对数的公约数完全相同。反复除法时非零余数严格变小，最终停在最大公约数；再回代即可找到裴蜀系数。这就是扩展欧几里得算法。

例如 $40 = 13 \cdot 3 + 1$ ，所以 $1 = 40 - 13 \cdot 3$ ，从而

$$3^{-1} \equiv -13 \equiv 27 \pmod{40}.$$

这里逆元符号表示模运算中的整数剩余类，不是普通分数 $1/3$ 。

第 3 章：质因数分解为何存在且唯一

[返回目录](#)

3.1 定理的准确表述

每个整数 $n > 1$ 都能写成有限个质数的乘积。除排列顺序外，质因子及其重数唯一。将相同质因子合并，可以写成

$$n = p_1^{\alpha_1} \cdots p_k^{\alpha_k},$$

其中 p_i 两两不同， $\alpha_i \geq 1$ 。例如 $60 = 2^2 \cdot 3 \cdot 5$ 。

“存在”和“唯一”是两个不同问题，不能只证明能拆分，就认为不可能有另一种拆分。

3.2 存在性：强归纳法

$n = 2$ 自身是质数。假设所有满足 $2 \leq m < n$ 的整数均可分解。

若 n 是质数，结论立即成立。若 n 是合数，可写 $n = ab$ ，其中 $1 < a, b < n$ 。由归纳假设， a, b 都是质数的有限乘积，合在一起给出 n 的分解。因此对所有 $n > 1$ 成立。

3.3 唯一性：配对和终止分别证明

假设

$$p_1 \cdots p_r = q_1 \cdots q_s$$

是两种分解。 p_1 整除右侧，由欧几里得引理，它整除某个 q_j 。两个数都是质数，所以 $p_1 = q_j$ 。重排右边，将它放到第一位，再在普通整数等式中约去相同质数。

重复此步骤，每次都会找到并约去一对相同质因子。

为什么两边一定同时约完？假设 $r < s$ 。约去左侧全部 r 个因子后，得到

$$1 = q_{r+1} \cdots q_s.$$

右侧至少剩一个质数，每个质数都不小于 2，故乘积大于 1，矛盾。 $r > s$ 同样矛盾。所以 $r = s$ ，每一步配对后所有质因子一一相等，重数也相同。证毕。

能够配对来自欧几里得引理；必然同时结束来自非空质数乘积大于 1。这是原对话“为什么最终同时约完”的完整回答。

3.4 最大公约数与最小公倍数的质数幂描述

给定有限多个正整数，把出现的质数统一记为 p_j ，缺少某个质因子时指数记为 0。两个数的最大公约数取每个指数的最小值，最小公倍数取最大值：

$$\gcd(m, n) = \prod_j p_j^{\min(\alpha_j, \beta_j)}, \quad \text{lcm}(m, n) = \prod_j p_j^{\max(\alpha_j, \beta_j)}.$$

理由是：由唯一分解，一个正整数整除另一个，当且仅当每个质数指数都不超过对方。公约数和公倍数的条件逐指数决定。

于是 $\gcd(m, n) \operatorname{lcm}(m, n) = mn$ 。一个整数同时被所有 m_i 整除，当且仅当被 $\operatorname{lcm}(m_1, \dots, m_k)$ 整除；整数为 0 的情况也显然成立。这将说明中国剩余定理的解周期。

第 4 章：费马小定理与三个应用

[返回目录](#)

4.1 两种形式与各自条件

若 p 是质数，则对任意整数 a ,

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

若再要求 $p \nmid a$ ，等价于 $\gcd(a, p) = 1$ ，则

$$a^{p-1} \equiv 1 \pmod{p}.$$

不能把第二式应用于 $p \mid a$ ：这时正整数次幂全部模 p 为 0。

4.2 完整证明：乘法使非零剩余类重新排列

设 $p \nmid a$ 。考察 $a, 2a, \dots, (p-1)a$ 的余数。

任何一个余数都不为 0：否则 $p \mid ai$ ，欧几里得引理推出 $p \mid i$ ，与 $1 \leq i \leq p-1$ 矛盾。

任何两个余数都不同：若 $ai \equiv aj \pmod{p}$ ，互质消去律给出 $p \mid (i-j)$ 。但 $|i-j| < p$ ，故 $i = j$ 。

因此这 $p-1$ 个余数恰好是 $1, 2, \dots, p-1$ 的一个排列。将全部同余相乘，得到

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

阶乘中的每个因子都与 p 互质，所以其乘积也与 p 互质，可以合法约去，得到第二种形式。

若 $p \nmid a$ ，将它乘以 a ，即得第一种形式；若 $p \mid a$ ， a^p 与 a 均模 p 为 0 。所以第一式覆盖任意整数。反过来，在 $p \nmid a$ 条件下，从第一式约去 a 可回到第二式。证毕。

4.3 应用一：大指数取余

对 $k \geq 0$ 作带余除法 $k = q(p-1) + r$ ， $0 \leq r < p-1$ 。若 $p \nmid a$ ，则

$$a^k = (a^{p-1})^q a^r \equiv a^r \pmod{p}.$$

例如 $100 = 16 \cdot 6 + 4$ ，所以 $2^{100} \equiv 2^4 = 16 \equiv 2 \pmod{7}$ 。

为什么需要互质？ 每消去一个长度为 $p-1$ 的幂块，依赖该幂块等于 1 。例如 $7^{12} \equiv 0 \pmod{7}$ ，不能将指数对 6 取余而改成 $7^0 = 1$ 。缩减后指数非零时偶然仍得 0 ，并不能证明这个规则普遍合法。

若底数是 p 的倍数且指数为正，直接取余 0 即可；指数为 0 时按单位元解释，余数为 1 。

4.4 应用二：整除证明

第一种形式直接等价于

$$p \mid (a^p - a).$$

例如对每个整数 a ， $5 \mid (a^5 - a)$ ，无需再假设 a 与 5 互质。若要合并多个不同质数的整除结论，可用第 2 章的互质乘积整除推论。

4.5 应用三：模逆元与线性同余

若 $p \nmid a$ ，由 $a \cdot a^{p-2} \equiv 1$ ，得到

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

$p = 2$ 时指数为 0，非零剩余类只有 1，公式仍成立。

解 $3x \equiv 2 \pmod{7}$: $3^5 \equiv 5 \pmod{7}$ ，所以 $x \equiv 5 \cdot 2 \equiv 3 \pmod{7}$ 。检验 $3 \cdot 3 = 9 \equiv 2$ 。

费马小定理提供质数模下的一种求逆方法；裴蜀等式及扩展欧几里得算法还能处理一般互质的合数模数。

4.6 两个反例防止过度使用

模数为合数时，不能直接使用指数 $n - 1$: $3^7 \equiv 3 \pmod{8}$ ，不是 1。

费马同余成立也不能反推模数是质数。 $341 = 11 \cdot 31$ ，而 $2^{10} = 1024 \equiv 1 \pmod{341}$ ，所以 $2^{340} = (2^{10})^{34} \equiv 1$ 。这只是合数通过某个底数的检验。费马小定理是必要性质，不是这一检验的充分判据。

第 5 章：欧拉函数与容斥乘积

[返回目录](#)

5.1 统计的是互质整数，不是素数

$\varphi(n)$ 统计 $1 \leq r \leq n$ 中与 n 互质的整数个数。例如 $n = 12$ 时为 1, 5, 7, 11，故 $\varphi(12) = 4$ 。这些数不必都是质数。

若 $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k} > 1$ ，由唯一分解， r 与 n 互质，当且仅当没有任何 p_i 整除 r 。

证明后一等价关系：如果某个 $p_i \mid r$ ，它就是公共因子；如果最大公约数大于 1，由存在性它有某个质因子，该质数同时整除 r, n ，由唯一分解它必为某个 p_i 。

5.2 两个、三个质因子的容斥

在 $1, \dots, n$ 中, p 的倍数有 n/p 个; 当 p, q 是 n 的不同质因子时, 同时为两者倍数, 等价于为 pq 倍数, 共 $n/(pq)$ 个。这些商都是整数。

若 $n = p^\alpha q^\beta$, 先减掉两类倍数, 再加回被减掉两次的交集:

$$\varphi(n) = n - \frac{n}{p} - \frac{n}{q} + \frac{n}{pq} = n \left(1 - \frac{1}{p}\right) \left(1 - \frac{1}{q}\right).$$

对于三个不同质因子 p, q, r ,

$$\begin{aligned} \varphi(n) = n - \left(\frac{n}{p} + \frac{n}{q} + \frac{n}{r}\right) \\ + \left(\frac{n}{pq} + \frac{n}{pr} + \frac{n}{qr}\right) - \frac{n}{pqr}. \end{aligned}$$

例如 $30 = 2 \cdot 3 \cdot 5$: $30 - 15 - 10 - 6 + 5 + 3 + 2 - 1 = 8$, 留下 $1, 7, 11, 13, 17, 19, 23, 29$ 。

中间结果 $30 - 15 - 10 - 6 = -1$ 、再加回两重交集得到 9 , 都是带符号的中间计数, 不是某个最终“剩余集合”的元素个数。三重交集最后减去, 才得正确值 8 。

5.3 一般容斥为何成立

令 A_i 是能被 p_i 整除的整数集合。统计其补集时, 按所选集合个数交替加减, 并把空交集解释为全部 n 个整数。

对一个落入恰好 j 个 A_i 的整数, 它在展开中的总权重为

$$\sum_{t=0}^j (-1)^t \binom{j}{t} = (1-1)^j.$$

若 $j = 0$, 权重为 1 ; 若 $j \geq 1$, 权重为 0 。所以恰好只计入互质整数, 每个计入一次。这证明了容斥, 而非仅把它作为未证明的工具使用。

记 $I = \{1, \dots, k\}$ 。不同质数互质，每个交集对应其乘积的倍数，故

$$\varphi(n) = n \sum_{J \subseteq I} (-1)^{|J|} \prod_{i \in J} \frac{1}{p_i}.$$

空乘积取 1。展开 $\prod_i (1 - 1/p_i)$ 时，从每个括号选 1 或 $-1/p_i$ 。选择负项的下标恰好形成子集 J ，贡献 $(-1)^{|J|} \prod_{i \in J} 1/p_i$ ；每个子集出现一次。因此

$$\boxed{\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)}.$$

乘积公式是容斥展开的因式分解表达。质因子指数虽影响 n ，排除的倍数类别却只由不同质因子决定，所以每个质数只出现一个括号。

5.4 常用值与乘法性

$$\varphi(p) = p - 1, \quad \varphi(p^\alpha) = p^\alpha - p^{\alpha-1}.$$

若 $\gcd(m, n) = 1$ ，两者的质因子集合不交，由乘积公式立即得到

$\varphi(mn) = \varphi(m)\varphi(n)$ 。这是互质条件下的乘法性，不能对任意两数使用；例如 $\varphi(4) = 2$ ，而 $\varphi(2)^2 = 1$ 。

不同质数 p, q 的乘积满足 $\varphi(pq) = (p - 1)(q - 1)$ 。一般公式例如

$$\varphi(360) = 360 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{3}\right) \left(1 - \frac{1}{5}\right) = 96.$$

第 6 章：欧拉定理为何成立

[返回目录](#)

6.1 定理与具体排列

若 $n \geq 2$ 且 $\gcd(a, n) = 1$ ，则

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

模 10 的互质代表为 1, 3, 7, 9。乘以 3 后余数是 3, 9, 1, 7，仍是同一组数。这里模数可以是合数，但底数仍然必须互质。

6.2 完整证明

取 $1, \dots, n-1$ 中全部互质代表 $r_1, \dots, r_k$ ，其中 $k = \varphi(n)$ 。考察 ar_i 的余数。

第一， ar_i 与 n 互质，因为两个互质于 n 的数，其乘积也与 n 互质；取余并不改变最大公约数，因为 $ar_i = qn + s$ 的两边给出同一组公约数。

第二，余数互不相同。若 $ar_i \equiv ar_j$ ，由 a 的逆元可消去 a ，得到 $r_i \equiv r_j$ 。它们位于同一个代表范围，故 $r_i = r_j$ 。

于是这 k 个余数就是原互质代表的一个排列。设 $R = r_1 \cdots r_k$ ，相乘得到

$$a^k R \equiv R \pmod{n}.$$

每个 r_i 都与 n 互质，所以 R 也与 n 互质，可约去，得 $a^k \equiv 1$ 。证毕。

欧拉函数出现在指数上，是因为相乘时共有 $k = \varphi(n)$ 个因子，每个因子都贡献一个 a 。

6.3 与费马小定理的联系及使用范围

当 $n = p$ 为质数时， $\varphi(p) = p - 1$ ，欧拉定理变成费马小定理的互质形式。若需要对任意底数得到 $a^p \equiv a$ ，再补 $p \mid a$ 的情形。

若 $k = q\varphi(n) + r$ ， $0 \leq r < \varphi(n)$ ，则在互质条件下 $a^k \equiv a^r \pmod{n}$ 。例如 $\varphi(10) = 4$ ，所以 $3^{100} \equiv 1 \pmod{10}$ 。

非互质时不能套用： $\varphi(8) = 4$ ，但 $2^4 \equiv 0 \pmod{8}$ ；指数取余后改成 2^0 会得 1。第 11 章处理 RSA 非互质消息时必须改用逐个质数的证明。

欧拉定理给出一个可用指数，未承诺最小。例如 $2^3 \equiv 1 \pmod{7}$ ，而 $\varphi(7) = 6$ 。这引出乘法阶。

第 7 章：乘法阶与真正最小周期

[返回目录](#)

7.1 定义与存在性

对 $\gcd(a, n) = 1$ ，满足 $a^d \equiv 1 \pmod{n}$ 的最小正整数 d ，记为 $\text{ord}_n(a)$ 。

欧拉定理保证这样的正指数集合非空，良序原理保证最小值存在。若 $a^d \equiv 1$ ，则任何 a, n 的公约数都整除 a^d 与 $a^d - 1$ ，进而整除 1；所以不互质的底数不可能存在这种乘法阶。

例如 2 模 7 的幂余数是 2, 4, 1, 2, 4, 1, ...，故 $\text{ord}_7(2) = 3$ 。

7.2 阶整除所有使幂等于一的指数

设 $d = \text{ord}_n(a)$ 。对于 $k \geq 0$ ，

$$a^k \equiv 1 \pmod{n} \iff d \mid k.$$

若 $d \mid k$ ，写 $k = qd$ ，直接得 $a^k \equiv 1$ 。

反过来，作带余除法 $k = qd + r$ ， $0 \leq r < d$ 。因为 $a^k \equiv (a^d)^q a^r \equiv a^r$ ，得到 $a^r \equiv 1$ 。若 $r > 0$ ，违背 d 的最小性，所以 $r = 0$ 。证毕。这也包括 $k = 0$ 。

将 $k = \varphi(n)$ 代入，得到

$$\text{ord}_n(a) \mid \varphi(n).$$

对非负整数 u, v ，还有 $a^u \equiv a^v$ 当且仅当 $u \equiv v \pmod{d}$ 。不妨 $u \geq v$ ，用 a^v 的逆元约分，再使用刚才结论即可。因此 d 是余数序列的真正最小正周期。

7.3 如何求阶与缩减指数

阶只能是 $\varphi(n)$ 的正因数。按从小到大检验这些因数，第一个使幂余数为 1 的就是阶。

例如 $\varphi(17) = 16$ ，候选为 1, 2, 4, 8, 16。 $4 \not\equiv 1$, $4^2 \equiv -1$, $4^4 \equiv 1 \pmod{17}$ ，所以阶为 4。

利用阶缩减可能更短： $1000 \equiv 1 \pmod{3}$ ，所以 $2^{1000} \equiv 2 \pmod{7}$ ；费马小定理按 6 取余则需再算 2^4 。

若已知 $D = \varphi(n)$ 的素因子分解，可从 D 开始：对质因子 q ，当 $a^{D/q} \equiv 1$ 时令 $D \leftarrow D/q$ 并继续。始终有 $d \mid D$ ；最后若 $D > d$ ， D/d 有一个质因子 q ，就仍可除去 q ，矛盾，所以最后为 d 。这里只说明数学算法，不声称分解大数很容易。

7.4 辅助引理一：一个幂的阶

若 a 的阶为 d ， $m \geq 0$ ，则

$$\text{ord}_n(a^m) = \frac{d}{\gcd(d, m)}.$$

先设 $m \geq 1$ 。令 $h = \gcd(d, m)$ ，写 $d = hd'$ 、 $m = hm'$ ，其中 $\gcd(d', m') = 1$ 。对正整数 k ，

$$(a^m)^k \equiv 1 \iff d \mid mk \iff d' \mid m'k \iff d' \mid k.$$

最后一步用互质消去律。所以最小正 k 是 d' 。当 $m = 0$ 时， a^0 的阶为 1，右边也是 $d/\gcd(d, 0) = 1$ 。这补全了原对话原根证明中直接使用的公式，也覆盖后面循环群计数的单位元。

7.5 辅助引理二：阶互质时乘积的阶

设 $\text{ord}_n(a) = r$ 、 $\text{ord}_n(b) = s$ ，且 $\gcd(r, s) = 1$ 。模整数的乘法可交换，因此

$$\boxed{\text{ord}_n(ab) = rs}.$$

先有 $(ab)^{rs} = (a^r)^s(b^s)^r \equiv 1$, 故 $t = \text{ord}_n(ab)$ 整除 rs 。

又 $(ab)^t \equiv 1$ 。取 r 次幂, 得到 $a^{rt}b^{rt} \equiv 1$ 。 $a^{rt} \equiv 1$, 所以 $b^{rt} \equiv 1$, 进而 $s \mid rt$ 。由 r, s 互质, 推出 $s \mid t$ 。同理 $r \mid t$, 再由互质乘积整除推论, $rs \mid t$ 。结合 $t \mid rs$, 得 $t = rs$ 。

这样无需使用负指数也能完成证明。在一般群中还必须要求两个元素可交换, 否则幂不一定可拆开。

若阶不互质, 结论未必成立: 模 7 时 2, 4 的阶均为 3, 但 $2 \cdot 4 \equiv 1$, 乘积的阶为 1。

对任意互质于模数的 a, b , 令 $L = \text{lcm}(r, s)$, 则 $(ab)^L \equiv 1$, 故乘积的阶总整除 L 。互质阶条件保证这个整除进一步达到等号。

第 8 章：原根及质数模原根存在性

[返回目录](#)

8.1 原根生成什么

对 $n \geq 2$, 若 g 与 n 互质且 $\text{ord}_n(g) = \varphi(n)$, 称其为模 n 的原根。对质数 p , 目标阶为 $p - 1$ 。

若阶为 $d, g^0, \dots, g^{d-1}$ 两两不同, 否则约分将产生更短周期。因此阶等于 $\varphi(n)$ 时, 这些幂恰好穷尽所有互质剩余类。

模 7 时 3 的幂余数为 3, 2, 6, 4, 5, 1, 所以 3 是原根; 2 的余数循环只有 2, 4, 1, 不是原根。

8.2 为什么非零多项式的根数不超过次数

在模质数 p 的系数运算中, 设 f 的次数为 m , 最高次系数模 p 不为 0。它最多有 m 个不同剩余类的根。

先证明因式分解的依据。对每个 $j \geq 1$,

$$x^j - r^j = (x - r)(x^{j-1} + x^{j-2}r + \cdots + r^{j-1}).$$

逐项相加给出 $f(x) - f(r) = (x - r)h(x)$ 。若 $f(r) \equiv 0$, 便在模 p 的多项式环里得到 $f(x) = (x - r)h(x)$, h 次数为 $m - 1$ 。

$m = 0$ 时非零常数没有根。归纳地, 若没有根结论显然; 若有根 r , 对另一个不同根 s , 有 $(s - r)h(s) \equiv 0$ 。因为 p 质数且 $s - r \not\equiv 0$, 可消去 $s - r$, 故 $h(s) \equiv 0$ 。归纳假设使其他根最多 $m - 1$ 个, 加上 r 至多 m 个。证毕。

质数条件在此保证非零元素可逆。模 8 的多项式 $x^2 - 1$ 有 1, 3, 5, 7 四个根, 已超过次数, 说明合数模数不能照搬。

8.3 每个质数都有原根：完整构造证明

$p = 2$ 时, 非零剩余类只有 1, 其阶为 $1 = p - 1$, 已经是原根。以下设 $p > 2$, 令

$$N = p - 1 = \prod_{i=1}^k q_i^{e_i},$$

其中 q_i 为不同质数。先为每个最大质数幂构造一个对应阶的元素。

第一步：找到不被较短指数消掉的元素。 多项式 $x^{N/q_i} - 1$ 次数为 $N/q_i < N$, 故最多有 N/q_i 个根, 而非零剩余类有 N 个。因此可选择非零 a_i , 使

$$a_i^{N/q_i} \not\equiv 1 \pmod{p}.$$

第二步：识别阶中的完整质数幂。 令 $t_i = \text{ord}_p(a_i)$ 。由第 7 章, $t_i \mid N$, 但 $t_i \nmid N/q_i$; 否则幂必等于 1。

N/q_i 与 N 只在 q_i 的指数上差 1。 t_i 的其他质数指数已由 $t_i \mid N$ 限制, 若 q_i 的指数也至多 $e_i - 1$, 便会整除 N/q_i , 矛盾。因此

$$t_i = q_i^{e_i} s_i, \quad \gcd(q_i, s_i) = 1.$$

第三步：除去阶中的其他因子。取 $b_i = a_i^{s_i}$ 。因为 $s_i \mid t_i$ ，由幂的阶公式，

$$\text{ord}_p(b_i) = \frac{t_i}{\gcd(t_i, s_i)} = \frac{t_i}{s_i} = q_i^{e_i}.$$

第四步：合并各个互质阶。取 $g = b_1 \cdots b_k$ 。各阶为不同质数的幂，两两互质；模乘法可交换。反复使用第 7.5 节，每次累积阶仍与下一个阶互质，得到

$$\text{ord}_p(g) = \prod_i q_i^{e_i} = N = p - 1.$$

所以 g 是原根。证毕。

“每个元素的阶都整除 $p - 1$ ”本身不足以证明有人达到 $p - 1$ 。多项式根数上界负责提供元素，幂的阶公式负责提取质数幂，互质阶乘积引理负责拼成完整阶。

8.4 原根有多少个

取一个模 p 的原根 g ， $N = p - 1$ 。全部非零剩余类可唯一表示为 g^m ， $1 \leq m \leq N$ 。由幂的阶公式，

$$\text{ord}_p(g^m) = \frac{N}{\gcd(N, m)}.$$

因此 g^m 是原根，当且仅当 $\gcd(N, m) = 1$ ，共有 $\varphi(N)$ 个。所以模 p 的原根数为 $\varphi(p - 1)$ 。 $p = 2$ 时用 $\varphi(1) = 1$ ，结论仍成立。

模数	原根个数	全部原根代表
5	2	2、3

模数	原根个数	全部原根代表
7	2	3、5
11	4	2、6、7、8
13	4	2、6、7、11
17	8	3、5、6、7、10、11、12、14

8.5 原根判定与合数反例

设 $p \nmid g$, $N = p - 1$ 的不同质因子为 q_i 。则

$$g \text{ 是原根} \iff g^{N/q_i} \not\equiv 1 \pmod{p} \text{ 对全部 } q_i.$$

必要性：阶为 N 时不整除任何 N/q_i 。

充分性：令阶为 $d \mid N$ 。若 $d < N$ ，商 $N/d > 1$ 有某个质因子 q_i ，于是 $d \mid N/q_i$ ，推出相应幂等于 1，矛盾。 $p = 2$ 时没有需检验的质因子，非零条件已唯一确定原根。

例：模 17 时 $N = 16 = 2^4$ 。 $3^4 \equiv 13$, $3^8 \equiv 13^2 \equiv 16 \not\equiv 1$ ，所以 3 为原根。

模 8 的互质代表 1, 3, 5, 7 全部平方为 1，因此阶最多为 2，而 $\varphi(8) = 4$ ；故没有原根。

一般分类是：在 $n \geq 2$ 的约定下，有原根的模数恰好为 $2, 4, q^k, 2q^k$ ，其中 q 为奇质数， $k \geq 1$ 。此分类是拓展结论，本篇没有给出其完整证明；可参看 [Yale 数论与密码学课程讲义](#)。

第 9 章：中国剩余定理的标准形式

[返回目录](#)

9.1 两两互质模数的定理

设正整数 $m_1, \dots, m_k$ 两两互质，余数 a_i 为任意整数，令 $M = m_1 \cdots m_k$ 。则

$$x \equiv a_i \pmod{m_i} \quad (i = 1, \dots, k)$$

一定有解，所有解恰为 $x = x_0 + tM$, $t \in \mathbb{Z}$ 。

“唯一”指模 M 的唯一剩余类，而非只有一个整数解。模数为 1 的条件不限制任何整数，可以删除；若全部为 1，全部整数就是模 1 的一个剩余类。以下构造处理剩余的模数。

9.2 存在性：构造对自己的模数余一、对其他余零的项

令 $M_i = M/m_i$ 。因为其他每个 m_j 都与 m_i 互质，第 2.4 节的乘积互质性质给出 $\gcd(M_i, m_i) = 1$ 。

由裴蜀等式，取 $M_i u_i + m_i v_i = 1$ ，令 $E_i = M_i u_i$ 。于是

$$E_i \equiv 1 \pmod{m_i}, \quad E_i \equiv 0 \pmod{m_j} \quad (j \neq i).$$

第二式来自 $m_j \mid M_i$ 。再取

$$x_0 = \sum_{i=1}^k a_i E_i = \sum_{i=1}^k a_i M_i u_i.$$

对任意固定 m_j 取模，其余项全为 0，只有 $a_j E_j \equiv a_j$ ，所以满足全部方程。存在性得证。

9.3 唯一性与全部解

若 x, y 都是解，则每个 m_i 都整除 $x - y$ 。由于模数两两互质，任意部分乘积仍与下一个模数互质，可反复用互质乘积整除推论，得 $M \mid (x - y)$ 。

反过来， $x_0 + tM$ 对各模数都与 x_0 同余，所以仍是解。因此全部解恰为该形式。

9.4 手算构造公式

求 $x \equiv 2 \pmod{3}$ 、 $x \equiv 3 \pmod{5}$ 、 $x \equiv 2 \pmod{7}$ 。

$M = 105$ ， $M_1 = 35$ 、 $M_2 = 21$ 、 $M_3 = 15$ ；各自逆元可取 $2, 1, 1$ ，因为对应乘积模自身模数均为 1 。于是

$$x_0 = 2 \cdot 35 \cdot 2 + 3 \cdot 21 + 2 \cdot 15 = 233 \equiv 23 \pmod{105}.$$

全部解 $x = 23 + 105t$ 。直接检验 23 分别余 $2, 3, 2$ 。

9.5 合并同余与环结构的联系

若两个整数模各个互质 m_i 分别同余，它们模 M 也同余。这个结论只用唯一性，在 RSA 中不需要重新构造解。

从结构上说，映射

$$\mathbb{Z}/M\mathbb{Z} \longrightarrow \prod_i \mathbb{Z}/m_i\mathbb{Z}, \quad [x]_M \longmapsto ([x]_{m_1}, \dots, [x]_{m_k})$$

是双射：存在性给出满射，唯一性给出单射。它也保持加法和乘法，因为每个坐标的取余运算保持这些运算。这给出了环同构的一种具体例子；前面的数论证明不需要预先掌握环论。

第 10 章：中国剩余定理的一般形式

[返回目录](#)

10.1 相容性条件与正确周期

对任意正整数模数 $m_1, \dots, m_k$, 方程组 $x \equiv a_i \pmod{m_i}$ 有解, 当且仅当

$$\gcd(m_i, m_j) \mid (a_i - a_j) \quad \text{对全部 } i, j.$$

若有解, 令 $L = \text{lcm}(m_1, \dots, m_k)$, 全部解恰为 $x = x_0 + tL$.

模数不互质时, 相容性有实际限制。例如 $x \equiv 2 \pmod{6}$ 与 $x \equiv 4 \pmod{9}$ 无解, 因为公约数 3 不整除余数差 2。互质时公约数为 1, 条件自动满足, 且 L 等于乘积, 所以标准形式是特殊情形。

10.2 两个模数：必要性

考虑 $x \equiv a \pmod{m}$ 、 $x \equiv b \pmod{n}$, 记 $g = \gcd(m, n)$ 。

若存在 x , g 整除 $x - a$ 与 $x - b$, 也就整除两者之差 $b - a$ 。因此 $g \mid (b - a)$ 必要。

10.3 两个模数：充分性与构造

假设 $g \mid (b - a)$, 写 $m = gm'$ 、 $n = gn'$ 、 $b - a = gc$, 其中 m', n' 互质。

先令 $x = a + mt$, 保证第一个方程。第二个方程要求 $mt \equiv b - a \pmod{n}$, 等价于存在整数 s 使

$$mt - ns = b - a \quad \Longleftrightarrow \quad m't - n's = c.$$

用裴蜀等式取 $m'u + n'v = 1$, 令 $t = cu$ 、 $s = -cv$, 便满足要求, 因此可取 $x_0 = a + mcv$ 。充分性得证。

若 x, y 均为解, 则 m, n 都整除 $x - y$, 由第 3.4 节, $\text{lcm}(m, n) \mid (x - y)$ 。反过来加上该最小公倍数的任意整数倍仍是解, 因而全部解及周期成立。

10.4 非互质的手算例子

求 $x \equiv 2 \pmod{6}$ 、 $x \equiv 5 \pmod{9}$ 。公约数 3 整除余数差 3, 所以有解。

写 $x = 2 + 6t$, 代入得到 $6t \equiv 3 \pmod{9}$ 。这一同余等价于 $2t \equiv 1 \pmod{3}$: 是同时将整除等式的两边及模数除以 3, 并非保持原模数的无条件约分。

所以 $t \equiv 2 \pmod{3}$, 取 $t = 2 + 3s$, 得

$$x = 14 + 18s, \quad x \equiv 14 \pmod{18}.$$

周期是 $\text{lcm}(6, 9) = 18$, 不是乘积 54。

10.5 多个模数: 为何两两相容足以给出共同解

必要性仍来自任意两个方程的差。充分性必须另证, 不能只说“每一对有解, 所以整体有解”。以下使用质数幂分解。

写

$$L = \text{lcm}(m_1, \dots, m_k) = \prod_{j=1}^r p_j^{e_j}.$$

每个 e_j 是所有模数中该质数指数的最大值, 所以可选一个下标 $h(j)$, 使 $p_j^{e_j} \mid m_{h(j)}$ 。提取约束

$$x \equiv a_{h(j)} \pmod{p_j^{e_j}} \quad (j = 1, \dots, r).$$

这些模数是不同质数的幂, 两两互质, 由标准形式得到公共解 x_0 。

现在证明它满足原方程。固定 i , 设 p_j 在 m_i 中的指数为 $f_{ij} \leq e_j$ 。若 $f_{ij} > 0$, 该质数幂同时整除 m_i 与 $m_{h(j)}$, 故

$$p_j^{f_{ij}} \mid \gcd(m_i, m_{h(j)}) \mid (a_i - a_{h(j)}).$$

而构造保证 $x_0 \equiv a_{h(j)} \pmod{p_j^{e_j}}$, 所以降到 $p_j^{f_{ij}}$ 后仍成立, 结合相容性得 $x_0 \equiv a_i$ 模该质数幂。对 m_i 的所有不同质数幂都成立, 互质乘积整除推论给出 $m_i \mid (x_0 - a_i)$ 。

由于 i 任意, 满足全部原方程。若 $L = 1$, 则全部模数为 1, 直接取任意整数即可。

若选择最大指数的模数有多个, 相容性使它们的余数模该质数幂相同, 因此提取约束没有歧义。

10.6 唯一性与一个多模数例子

任意两个解之差被所有 m_i 整除, 因此被 L 整除; $x_0 + tL$ 又总是解。所以解模 L 唯一。 L 也是解集合的最小正平移周期: 任何保持解的正平移量都必须被全部模数整除, 因此被 L 整除。

例如取 $m_1 = 12, m_2 = 18, m_3 = 20$, 余数分别为 5, 11, 17。三个公约数为 6, 4, 2, 都整除对应余数差。 $L = 180 = 4 \cdot 9 \cdot 5$, 可提取

$$x \equiv 1 \pmod{4}, \quad x \equiv 2 \pmod{9}, \quad x \equiv 2 \pmod{5}.$$

取 $x_0 = 137$, 逐项检验模 12, 18, 20 分别余 5, 11, 17, 故全部解为 $137 + 180t$ 。

第 11 章：RSA 的指数与解密正确性

[返回目录](#)

11.1 数学设置与选择顺序

本章讨论两个不同质数的教学模型。取 $n = pq$, $F = \varphi(n) = (p-1)(q-1)$ 。消息取代表 $0 \leq m < n$ 。

先选择正整数 e , 使 $\gcd(e, F) = 1$; 再由裴蜀等式求正整数代表 d , 满足

$$ed \equiv 1 \pmod{F}.$$

公钥为 (n, e) ，私钥指数为 d 。加密取 c 为 m^e 模 n 的标准余数，解密取 c^d 模 n 的标准余数。

$$c \equiv m^e \pmod{n}, \quad c^d \equiv m^{ed} \pmod{n}.$$

因此目标是证明任意消息都满足 $m^{ed} \equiv m \pmod{n}$ ；再由两者都处于 $0, \dots, n-1$ ，同余保证真正恢复同一代表。

11.2 指数不是随意假设出来的

固定 e ，存在 d 的充要条件为 $\gcd(e, F) = 1$ ，这正是第 2.3 节的逆元定理。

例如 $p = 5, q = 11$ 时 $n = 55, F = 40$ 。若取 $e = 6$ ，方程 $6d - 40k = 1$ 左侧为偶数，不可能等于 1。若取 $e = 3$ ， $1 = 40 - 13 \cdot 3$ 给出 $d \equiv 27 \pmod{40}$ ，可取 $d = 27$ ，因为 $3 \cdot 27 = 81 = 1 + 2 \cdot 40$ 。

至少存在互质 e ：数学上可取 1；若 $F > 2$ ，也可取 $F - 1$ ，与 F 相邻所以互质。但这些都只证明存在性，**不作为安全参数建议**。例如取 $e = F - 1, d = F - 1$ 时公私指数相同，无法据此获得所期待的保密性。

11.3 互质消息：欧拉定理直接证明

e, d 均正，故写 $ed = 1 + kF$ 时 $k \geq 0$ 。若 $\gcd(m, n) = 1$ ，欧拉定理给出 $m^F \equiv 1$ ，于是

$$m^{ed} = m^{1+kF} = m(m^F)^k \equiv m \pmod{n}.$$

这段证明仅覆盖互质消息。RSA 的消息范围还包含 0 和 p, q 的倍数，需要下面的完整证明。

11.4 任意消息：逐个质数证明，再合并

先在模 p 下讨论。

若 $p \mid m$ ，由于 $ed \geq 1$ ， m^{ed} 与 m 的余数均为 0，结论成立。

若 $p \nmid m$ ，费马小定理给出 $m^{p-1} \equiv 1$ 。所以

$$\begin{aligned} m^{ed} &= m^{1+k(p-1)(q-1)} \\ &= m(m^{p-1})^{k(q-1)} \equiv m \pmod{p}. \end{aligned}$$

模 q 完全相同：若 $q \mid m$ ，两边为 0；否则将指数写为 $1 + (q-1)k(p-1)$ ，由费马小定理得到 $m^{ed} \equiv m \pmod{q}$ 。

因 p, q 不同而互质， p, q 都整除 $m^{ed} - m$ ，便有 $pq \mid (m^{ed} - m)$ ，即

$$\boxed{(m^e)^d \equiv m \pmod{pq}}.$$

这一步是中国剩余定理的唯一性结论；也可以直接由第 2.4 节的互质乘积整除推论完成。
没有要求消息与 n 互质。

11.5 两个具体消息与快速幂

继续取 $n = 55, e = 3, d = 27$ 。

互质消息 $m = 7$ ： $c \equiv 7^3 = 343 \equiv 13$ 。反复平方得

$$13^2 \equiv 4, \quad 13^4 \equiv 16, \quad 13^8 \equiv 36, \quad 13^{16} \equiv 31 \pmod{55}.$$

$27 = 16 + 8 + 2 + 1$ ，因此 $13^{27} \equiv 31 \cdot 36 \cdot 4 \cdot 13 \equiv 7 \pmod{55}$ 。

非互质消息 $m = 5$ ： $c \equiv 5^3 \equiv 15 \pmod{55}$ 。模 5 的解密结果为 0；模 11 下 $15 \equiv 4, 4^2 \equiv 5, 4^5 \equiv 1$ ，所以 $4^{27} \equiv 4^2 \equiv 5$ 。两条件共同确定模 55 的结果为 5。

快速幂不必先寻找最小周期：将指数写成二进制，反复平方并乘上所需的幂，每步取余即可。它计算的是同一同余类，正确性直接来自幂运算与同余乘法。

11.6 更弱的指数条件与实际方案的范围

完整证明真正使用的是 $p - 1 \mid (ed - 1)$ 与 $q - 1 \mid (ed - 1)$ ，所以只需

$$ed \equiv 1 \pmod{\text{lcm}(p-1, q-1)}.$$

这比模 $(p-1)(q-1)$ 的条件更弱。例如 $p = 5, q = 11$ 时最小公倍数为 20。原对话使用 40 是方便的充分条件。第 16.3 节解释它与卡迈克尔函数的关系。

知道 p, q 可计算 F 并求逆元 d 。反过来，对两个不同质数，若知道 n 与 F ，则 $p + q = n + 1 - F$ ， p, q 是方程

$$t^2 - (n + 1 - F)t + n = 0$$

的两根。这个关系说明为什么 F 的信息与分解密切相关，但不构成“破解 RSA 必须先分解”的证明。

本章给出幂运算的数学正确性；安全加密还需要消息编码、参数与实现要求。标准 RFC 8017 第 3、5、7 节 区分 RSA 幂运算原语和带编码的加密方案，并以最小公倍数定义密钥条件；RSAES-OAEP 在原语外加入 OAEP 编码。小参数手算例子只供理解，不是安全实现指南。

第 12 章：有限群、循环群与元素阶计数

[返回目录](#)

12.1 从模乘法进入群的语言

前面已经证明的模逆元、幂的周期与原根，可以用群的语言统一表达。**群**是带一种运算的集合，运算满足：封闭、结合律、有单位元、每个元素有逆元。若运算还满足交换律，称为交换群。群的**阶**是元素个数，记为 $|G|$ ；它与某个元素的阶是两种不同的数量。

对 $n \geq 2$ ，模 n 的互质剩余类组成

$$U_n = (\mathbb{Z}/n\mathbb{Z})^\times = \{[a]_n : \gcd(a, n) = 1\}.$$

其运算为剩余类乘法。第 2.4 节保证乘积仍互质，所以运算封闭；整数乘法给出结合律与交换律； $[1]_n$ 是单位元；第 2.3 节保证每个元素有逆元，而且逆元也与 n 互质。因此 U_n 是有限交换群， $|U_n| = \varphi(n)$ 。

对质数 p ， U_p 就是全部非零剩余类，阶为 $p - 1$ 。第 8 章已经完整证明原根存在，所以某个 g 的幂遍历 U_p 。这就是说

$$U_p = \langle g \rangle$$

是**循环群**。这里“循环”表示一个元素的幂生成整个群；它是比“每个元素的幂都有周期”更强的性质。

一般模数不保证循环： $U_8 = \{1, 3, 5, 7\}$ 有四个元素，却没有阶为四的元素，因而任何单个元素都无法生成全群。

12.2 有限群中的元素阶与循环子群

以下暂用 1_G 表示群单位元。对有限群中的元素 a ，它的阶是满足 $a^d = 1_G$ 的最小正整数 d 。

先说明这个正整数一定存在。若 $|G| = N$ ， $1_G, a, a^2, \dots, a^N$ 共 $N + 1$ 项，必有两项相同。设 $a^i = a^j$ 、 $i < j$ ，乘以 a^{-i} 得 $a^{j-i} = 1_G$ 。由良序原理可以取最小正指数。

与第 7.2 节同样作带余除法，可以证明对 $k \geq 0$,

$$a^k = 1_G \iff d \mid k.$$

因此 $1_G, a, \dots, a^{d-1}$ 两两不同，且任何非负整数幂都等于其中某一项。这个集合记为 $H = \langle a \rangle$ 。它包含单位元；两项乘积仍是一个幂； a^j 的逆元为 a^{d-j} ，经指数取余仍在集合中。因此 H 是 G 的子群，恰有 d 个元素。

在一般群中也可以使用整数次幂，负次幂由逆元定义；这里的计数只用非负代表。

12.3 陪集划分与拉格朗日定理的完整证明

设 H 是有限群 G 的子群。对 $g \in G$ ，左陪集定义为

$$gH = \{gh : h \in H\}.$$

第一，每个陪集与 H 等大。映射 $h \mapsto gh$ 是双射，逆映射为 $x \mapsto g^{-1}x$ ，故 $|gH| = |H|$ 。

第二，两个陪集相交就相同。若 $z = g_1h_1 = g_2h_2$ ，其中 $h_1, h_2 \in H$ ，则

$$g_2^{-1}g_1 = h_2h_1^{-1} \in H.$$

记此元素为 h_0 ，有 $g_1 = g_2h_0$ 。对子群内的 h ， $h_0h \in H$ ，所以 $g_1H \subseteq g_2H$ ；反用 $h_0^{-1} \in H$ 得反向包含。故两个陪集完全相同。

第三，陪集覆盖全群。每个 $g \in G$ 都属于 gH ，因为 $g = g1_G$ 。

综上，不同左陪集将 G 划分成若干互不重叠、每份恰有 $|H|$ 个元素的集合。若有 k 个不同陪集，则

$$|G| = k|H|, \quad \boxed{|H| \mid |G|}.$$

这就是拉格朗日定理。取 $H = \langle a \rangle$ ，便得

$$\boxed{\text{ord}(a) \mid |G|}.$$

证明没有使用交换律，适用于任意有限群。

整除条件不保证每个因数都实现为元素阶。例如 U_8 的阶为 4，其元素阶分别为 1, 2, 2, 2，没有阶为 4 的元素。后面按每个因数精确计数，依赖的是循环群这一额外条件。

12.4 循环群中的幂阶公式，包括零指数

设 $G = \langle g \rangle$, $|G| = N$, 即 g 的阶为 N 。每个元素唯一写为 g^k , 其中 $0 \leq k < N$ 。第 7.4 节的论证在群中原样成立：对 $k \geq 0$,

$$\boxed{\text{ord}(g^k) = \frac{N}{\gcd(N, k)}}.$$

若 $k > 0$, 写 $N = cn'$ 、 $k = ck'$, $c = \gcd(N, k)$ 。对正整数 m ,

$$(g^k)^m = 1_G \iff N \mid km \iff n' \mid k'm \iff n' \mid m.$$

最后一步用 $\gcd(n', k') = 1$ 与互质消去律。因此最小正 m 为 $n' = N/c$ 。

若 $k = 0$, $g^0 = 1_G$ 的阶为 1, 而 $\gcd(N, 0) = N$, 公式同样给出 1。这一步补足了概率计数必须包含单位元的边界。

12.5 为什么阶为 d 的元素恰好有欧拉函数那么多个

设 $d \mid N$, 令 $s = N/d$ 。由刚才的公式,

$$\text{ord}(g^k) = d \iff \gcd(N, k) = s.$$

右边要求 $s \mid k$, 写 $k = st$ 。由于 $0 \leq k < N = sd$, 恰有 $0 \leq t < d$ 。并且

$$\gcd(N, k) = \gcd(sd, st) = s \gcd(d, t).$$

这个等式也可由第 3.4 节的质数指数逐项取最小值证明。因此

$$\text{ord}(g^k) = d \iff \begin{cases} k = (N/d)t, \\ 0 \leq t < d, \\ \gcd(t, d) = 1. \end{cases}$$

当 $d > 1$, 这样的 t 恰有 $\varphi(d)$ 个, 因为 0 不互质, 统计范围与 $1, \dots, d$ 等价; 当 $d = 1$, 只有 $t = 0$, 且 $\gcd(0, 1) = 1$, 也与 $\varphi(1) = 1$ 一致。每个 t 对应不同的 g^k , 所以

$$\boxed{\#\{x \in G : \text{ord}(x) = d\} = \varphi(d)}.$$

若 $d \nmid N$, 由拉格朗日定理个数为 0 。由计数结果可见, 在循环群中每个正因数确实都被实现。

取 $N = 2^\alpha$, 各元素阶只能为 2^t , $0 \leq t \leq \alpha$ 。其数量为

$$\begin{cases} 1, & t = 0, \\ 2^{t-1}, & 1 \leq t \leq \alpha. \end{cases}$$

因为 $t \geq 1$ 时模 2^t 的互质代表恰为奇数, 有一半。总数检查为 $1 + \sum_{t=1}^{\alpha} 2^{t-1} = 2^\alpha$; 没有遗漏其他阶。这将直接变成第 15 章的概率分布。

12.6 原根存在性的另一条证明: 所有阶的最小公倍数

新增对话给出另一种证明, 可以与第 8.3 节的逐个质数幂构造对照。设 $p > 2$, 令

$$E = \text{lcm}\{\text{ord}_p(a) : a \in U_p\}.$$

每个阶均整除 $p - 1$, 故 $E \mid (p - 1)$ 。另一方面, 每个非零剩余类都满足 $a^E = 1$ 。多项式 $x^E - 1$ 因而至少有 $p - 1$ 个根; 由第 8.2 节的根数上界, $p - 1 \leq E$ 。于是 $E = p - 1$ 。

还需要说明有元素的阶恰好达到 E 。写 $E = \prod_i \ell_i^{c_i}$ 。由于是有限多个阶的最小公倍数, 对于每个最大质数幂 $\ell_i^{c_i}$, 存在某个 a_i , 其阶为 $\ell_i^{c_i} t_i$, 且 $\gcd(\ell_i, t_i) = 1$ 。取 $b_i = a_i^{t_i}$, 幂阶公式给出阶为 $\ell_i^{c_i}$ 。这些阶两两互质, 模乘法可交换, 第 7.5 节给出 $g = \prod_i b_i$ 的阶为 $E = p - 1$ 。故 g 是原根。 $p = 2$ 单独取 $g = 1$ 即可。

这段“最小公倍数可以由一个元素的阶达到”的构造对有限交换群成立，不能去掉交换条件。例如三元素置换群 S_3 的元素由恒等、换位和三循环组成，阶分别为 **1, 2, 3**，最小公倍数为 **6**，却没有阶为 **6** 的元素。

第 13 章：有限概率、均匀映射与加权平均

[返回目录](#)

13.1 样本空间、事件与随机变量

本篇只需要有限概率，不需要先学习连续分布或测度论。设有限样本空间 Ω 的每个结果 ω 有概率 $p_\omega \geq 0$ ，并满足 $\sum_{\omega \in \Omega} p_\omega = 1$ 。事件是其中一个子集 A ，其概率为 $P(A) = \sum_{\omega \in A} p_\omega$ 。互不相交事件的概率可以相加。

若所有结果等概率，称为均匀分布，此时

$$P(A) = \frac{|A|}{|\Omega|}.$$

随机变量 X 是由结果决定的数或标签。事件 $X = t$ 指所有满足这个条件的结果，因此

$$P(X = t) = \sum_{\omega: X(\omega)=t} p_\omega, \quad \sum_t P(X = t) = 1.$$

最后一个等式来自不同取值的事件将样本空间划分。并非任意一组概率的和都为 1；这里使用的是某个随机变量全部互斥取值的概率。

13.2 双射保持均匀，等大小原像也保持均匀

若 X 在有限集合 S 上均匀， $f: S \rightarrow R$ 是一个映射，则对 $y \in R$,

$$P(f(X) = y) = \frac{\#\{x \in S : f(x) = y\}}{|S|}.$$

这直接由均匀计数得到。如果 f 是双射，每个原像恰有一个元素，输出在 R 上均匀。如果 f 是满射，而且每个原像恰有相同的 c 个元素，则 $|S| = c|R|$ ，输出仍在 R 上均匀，概率为 $c/|S| = 1/|R|$ 。

输出均匀需要检验原像大小，不能仅因为输入均匀就断定。例如均匀取 $X \in \{0, 1, 2\}$ ，映射 $X \bmod 2$ 取 0 的概率为 $2/3$ ，取 1 的概率为 $1/3$ 。

对 k 均匀取自 $0, \dots, Mu - 1$ ，映射 $k \mapsto k \bmod M$ 的每个原像为

$$j, j + M, \dots, j + (u - 1)M,$$

恰有 u 项，故余数均匀。若 $\gcd(w, M) = 1$ ， $j \mapsto wj \bmod M$ 又是双射：相同像经互质消去律推出相同原像，有限同大小集合上的单射就是双射。两步合起来仍保持均匀。

13.3 条件概率、独立性与全概率公式

当 $P(A) > 0$ 时，条件概率定义为

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

随机变量 X, Y 独立，表示对其全部取值 x, y ,

$$P(X = x, Y = y) = P(X = x)P(Y = y).$$

因此，在 $P(X = x) > 0$ 时， $P(Y = y | X = x) = P(Y = y)$ 。零概率条件事件不使用这个除法。

设 A_t 将样本空间划分成互不相交的事件，则 B 被 $B \cap A_t$ 划分，所以

$$P(B) = \sum_t P(B \cap A_t) = \sum_{t: P(A_t) > 0} P(A_t)P(B | A_t).$$

这就是有限全概率公式。等号的依据分别是事件划分和条件概率定义，并不需要先假设独立。

如果 X, Y 独立，分别只依赖它们的 $f(X), g(Y)$ 也独立。固定输出 u, v ，将原像事件展开：

$$\begin{aligned} P(f(X) = u, g(Y) = v) &= \sum_{x: f(x)=u} \sum_{y: g(y)=v} P(X = x)P(Y = y) \\ &= P(f(X) = u)P(g(Y) = v). \end{aligned}$$

这里强调“分别”：若两个新变量都依赖同一个输入，不能自动断言独立。

13.4 为什么 CRT 给出独立均匀的坐标

设 $n = pq$ ， p, q 是不同质数。第 9 章的 CRT 双射在互质类上限制为

$$U_n \longrightarrow U_p \times U_q, \quad [a]_n \longmapsto ([a]_p, [a]_q).$$

确实是双射：互质于 n 就同时不被 p, q 整除；反过来，两个非零坐标的 CRT 解也不被任何一个质因子整除，所以属于 U_n 。

均匀取 $a \in U_n$ ，每个坐标对恰对应一个输入，故对 $b \in U_p, c \in U_q$ ，

$$P(a \bmod p = b, a \bmod q = c) = \frac{1}{(p-1)(q-1)}.$$

固定 b ，有 $q-1$ 个可能的 c ，所以边缘概率为 $1/(q-1)$ ；另一个边缘同理为 $1/(p-1)$ 。联合概率等于它们的乘积，因此两个坐标独立且各自均匀。

CRT 本身是一个确定性的双射；独立均匀的结论还使用了输入在整个 U_n 上均匀。若从一部分特殊底数中抽样，必须重新核对分布。

13.5 相等概率为什么是加权平均

设 X, Y 为独立的有限随机变量。相等事件由互斥事件 $\{X = t, Y = t\}$ 组成，所以

$$P(X = Y) = \sum_t P(X = t, Y = t) = \sum_t P(X = t)P(Y = t).$$

记 $a_t = P(X = t)$ 、 $b_t = P(Y = t)$ 。如果对每个 t 都有 $b_t \leq M$ ，则

$$\boxed{\sum_t a_t b_t \leq \sum_t a_t M = M \sum_t a_t = M}.$$

其中 $a_t \geq 0$ 保证乘法不改变不等号方向， $\sum_t a_t = 1$ 保证结果是加权平均。不能把这一步理解为直接将若干个 M 相加。

从条件概率看，

$$P(X = Y) = \sum_{t: P(X=t)>0} P(X = t)P(Y = t | X = t).$$

独立性使每个条件概率等于 $P(Y = t) \leq M$ 。无论 X 取哪个可能值， Y 恰好与它相同的概率都不超过 M ；对这些情况取概率加权平均，上界仍为 M 。

独立性不能遗漏。例如让 X 均匀取 $0, 1$ ，并令 $Y = X$ 。两者每个边缘取值概率都为 $1/2$ ，但 $P(X = Y) = 1$ 。此时不能将联合概率写成边缘概率的乘积。

13.6 重复试验、失败尾概率与期望次数

若每次独立重新抽样，单次失败概率为 $f \leq 1/2$ ，则连续 k 次全部失败的概率为

$$f^k \leq 2^{-k}.$$

不是只看单次概率就能相乘；需要独立重复。反复使用同一个底数，失败事件可能完全相同，不产生这个指数下降。

设每次成功概率为 $\rho = 1 - f > 0$ ， N 为第一次成功的尝试次数。则

$P(N \geq j) = f^{j-1}$ 。期望定义为各可能值的概率加权和，并由非负项交换求和得

$$\begin{aligned} \mathbb{E}[N] &= \sum_{k \geq 1} kP(N = k) = \sum_{j \geq 1} P(N \geq j) \\ &= \sum_{j \geq 1} f^{j-1} = \frac{1}{1-f} = \frac{1}{\rho}. \end{aligned}$$

第二个等号可将整数 k 写成 k 个 1 来理解；几何级数的极限来自 $0 \leq f < 1$ 。若 $\rho \geq 1/2$ ，期望次数至多为 2 。这是概率保证，不表示每次必在两次内成功。

第 14 章：已知 RSA 私钥怎样随机分解模数

[返回目录](#)

14.1 区分四种已知信息或计算能力

本章限定 $n = pq$ ，其中 p, q 是两个不同奇质数。以下“已知私钥指数”同时默认已知公钥 (n, e) 。恢复私钥与对某个密文进行求逆，应分别讨论。

已知信息或能力	能做什么	依据
分解 n ，知道 p, q	计算 $\varphi(n), \lambda(n)$ ，求出有效 d 并解密	第 2、11 章
知道 n 与 $\varphi(n)$	解二次方程恢复 p, q	第 11.6 节
知道 n, e 与有效 d	用本章随机算法恢复因子	第 14—15 章
仅有直接求解 $m^e \equiv c \pmod n$ 的能力	可以解决对应 RSA 求逆问题	不能从前面结论直接推出分解算法

“能够分解，所以能够解密”是一个方向的计算归约；它本身没有证明反方向。私钥指数恢复与分解之间有随机多项式时间的归约，而一般 RSA 求逆能力与分解的等价性没有由这些证明建立。相关区别可核对 [Handbook of Applied Cryptography 第 3 章 Fact 3.30](#) 与 [第 8 章 Fact 8.6](#)。

如果给出一个高效算法，它可由所有合格公钥恢复有效指数，那么与下面归约合用便得到相应模数的高效随机分解算法。单个容易恢复的明文或退化密钥，不能据此推出所有模数容易分解。数学原语与实际编码方案的安全性仍需区分，见第 11.6 节。

14.2 我们真正需要的是一个正的统一指数倍数

有效指数满足

$$ed \equiv 1 \pmod{\lambda(n)}, \quad \lambda(n) = \text{lcm}(p-1, q-1).$$

这个条件与 RFC 8017 第 3.2 节一致。令 $K = ed - 1$ ，则 $\lambda(n) \mid K$ 。原对话使用更强的 $\varphi(n) \mid K$ ；本章的全部证明只需要较弱条件。

要求 $K > 0$ 。 正整数 $e > 1, d \geq 1$ 可以保证这一点； $e = d = 1$ 给出 $K = 0$ ，无法把它写成后面所需的有限二次幂分解。它虽满足形式同余，却是公开的恒等幂运算，不能纳入这里的分解归约条件。

将 K 中所有因子 2 提取出来，得到唯一分解

$$K = 2^s r, \quad r > 0 \text{ 为奇数}.$$

因为 p, q 为奇质数， $p-1, q-1$ 都为偶数，故 $s \geq 1$ 。对任何 $a \in U_n$ ，费马小定理分别给出 $a^K \equiv 1$ 模 p 与模 q ，再由 CRT 合并得

$$a^K \equiv 1 \pmod{n}.$$

算法知道的是 K ，无需知道 $\lambda(n)$ 或 $\varphi(n)$ 的实际数值。

14.3 模两个奇质数乘积时，一的四个平方根

若 $x^2 \equiv 1 \pmod{n}$ ，则 p, q 各自整除 $(x-1)(x+1)$ 。由欧几里得引理，在每个质数坐标下都有 $x \equiv 1$ 或 $x \equiv -1$ 。

奇质数保证 $1, -1$ 不同：否则该质数整除 2，矛盾。CRT 因而给出恰好四个不同剩余类：

模 p 坐标	模 q 坐标	模 n 的性质
1	1	平凡根 1

模 p 坐标	模 q 坐标	模 n 的性质
-1	-1	平凡根 -1
1	-1	非平凡平方根
-1	1	非平凡平方根

反过来四种坐标组合的平方都为 $(1, 1)$ ，所以没有漏根。两个非平凡根占四根的一半，不足以直接证明算法成功概率是一半，因为算法产生这些根的分布尚未说明。

例如模 55 的四个根为 $1, 21, 34, 54$ 。其中 $34 \equiv 1 \pmod{11}$ 、 $34 \equiv -1 \pmod{5}$ ，所以为非平凡根。

14.4 为什么最大公约数能分离质因数

设 x 是非平凡平方根，其两个坐标必有不同符号。不妨 $x \equiv 1 \pmod{p}$ 、 $x \equiv -1 \pmod{q}$ ，则 $p \mid x - 1$ 、 $q \mid x + 1$ 。

若 q 也整除 $x - 1$ ，则它整除 $(x + 1) - (x - 1) = 2$ ，与奇质数条件矛盾；同理 $p \nmid x + 1$ 。而 n 只有 p, q 两个不同质因数，所以

$$\gcd(x - 1, n) = p, \quad \gcd(x + 1, n) = q.$$

符号相反时因子位置交换。这证明提取结果必是真因子，而非仅仅某个公约数。

对 $x = 34, n = 55$ ， $x - 1 = 33 = 3 \cdot 11$ 、 $x + 1 = 35 = 5 \cdot 7$ ，故最大公约数分别为 $11, 5$ 。

14.5 连续平方算法及全部分支

已知 n, e, d ，先计算 $K = 2^s r > 0$ 。一次尝试可以如下进行：

1. 在 $1, \dots, n - 1$ 中均匀随机选 a ，计算 $g = \gcd(a, n)$ 。若 $g > 1$ ，由于 $a < n$ ，已有 $1 < g < n$ ，直接输出 $g, n/g$ 。

2. 若 $g = 1$ ，用快速幂计算 $x = a^r \bmod n$ ，取 $0 \leq x < n$ 。若 $x = 1$ ，本次失败，独立重选底数。
3. 对 $j = 1, \dots, s$ ，计算 $y = x^2 \bmod n$ 。若 $y = 1$ ：当 $x \neq n - 1$ 时输出 $\gcd(x - 1, n)$ 及另一因子；当 $x = n - 1$ 时本次失败。若 $y \neq 1$ ，令 $x = y$ 并继续。

为什么输出分支中 x 不会等于 1？初始的 1 已被排除，之后一旦 $y = 1$ 就立即结束，不会将它带进下一轮。因此该分支确实满足 $x^2 = 1$ 、 $x \not\equiv \pm 1 \pmod{n}$ ，由第 14.4 节必输出正确因子。

互质底数的完整序列为

$$x_j = a^{2^{j_r}} \bmod n, \quad j = 0, 1, \dots, s.$$

终点 $x_s = a^K \bmod n = 1$ 。所以在有效输入假设下，必定触及 1 并落入某个成功或失败分支。若程序走完仍没有到达 1，应检查指数条件或实现，不能把错误输入当作本定理的反例。

算法用到的只有 gcd、快速幂和取模平方；证明时才引入未知的 p, q 、原根和指数坐标。算法本身不需要计算离散对数。

14.6 完整样例：由 e 、 d 恢复五十五的因子

已知 $n = 55, e = 3, d = 27$ ，不先使用因子计算：

$$K = ed - 1 = 80 = 2^4 \cdot 5, \quad s = 4, r = 5.$$

取 $a = 2$ ， $\gcd(2, 55) = 1$ 。连续平方得到：

j	x_j	运算
0	32	$2^5 \bmod 55$

j	x_j	运算
1	34	$32^2 \bmod 55$
2	1	$34^2 \bmod 55$

第 2 步平方为 1，前一项 34 既不是 1 也不是 54，故提取 $\gcd(33, 55) = 11$ ，另一因子 $55/11 = 5$ 。若继续完整序列，后两项也为 1，但算法已无须继续。

失败例子也有：取 $a = 1$ ，初始已为 1；取 $a = 54$ ，因 r 奇数，初始为 -1 ，下一平方为 1，只能得到平凡根。本次失败是算法允许的结果，需要重新抽样。

14.7 有限次失败与期望多项式时间

第 15 章将证明互质底数的一次成功概率至少为 $1/2$ 。在全部 $1, \dots, n-1$ 中抽样时，非互质分支直接成功；条件于互质时仍然均匀。因此全部候选的一次成功概率也至少为 $1/2$ 。

独立重复 k 次仍失败的概率至多为 2^{-k} 。例如 $k = 20$ ，上界为 $1/1048576 \approx 9.54 \times 10^{-7}$ 。这不保证每个随机序列都成功。

无限重试的算法一旦输出就必正确，期望尝试次数至多为 2，称为 Las Vegas 型随机算法；限次版本可以在未找到因子时明确报告失败。不能把“报告失败”写成输出一个未经验证的因子。

复杂度按输入位数计算。反复除以 2 最多进行 $O(\log K)$ 次，快速幂需要 $O(\log r)$ 次模乘，连续平方最多 $s \leq \lfloor \log_2 K \rfloor$ 次；gcd 和整数运算均可在输入位数的多项式时间完成。期望总时间因此是 $\log n + \log e + \log d$ 的多项式，而不是与巨大整数 K 的数值成正比。通常 RSA 指数代表小于 n ，此时也可按 $\log n$ 控制。

第 15 章：随机分解成功概率的完整证明

[返回目录](#)

15.1 假设、随机选择与首次到达时刻

本章固定两个不同奇质数 p, q , $n = pq$; 固定正整数 $K = 2^s r$, r 为奇数, 且 $\lambda(n) \mid K$ 。随机性只来自在整个 U_n 上均匀选择 a 。第 14.5 节实际抽样条件于互质就满足此分布。

写

$$p - 1 = 2^\alpha u, \quad q - 1 = 2^\beta v,$$

其中 u, v 奇, $\alpha, \beta \geq 1$ 。因为 $p - 1, q - 1 \mid K$, 由质数指数描述得到

$$s \geq \max(\alpha, \beta), \quad u \mid r, \quad v \mid r.$$

即使 u, v 不互质, 这些整除关系仍成立; 本证明无需假设其互质。

令

$$T_p = \min\{j \geq 0 : a^{2^j r} \equiv 1 \pmod{p}\}, \quad T_q = \min\{j \geq 0 : a^{2^j r} \equiv 1 \pmod{q}\}.$$

由终点幂等于 1, 这两个随机变量都存在且不大于 s 。一旦到达 1, 以后平方仍为 1。

15.2 为什么成功等价于两个坐标不同步

若 $T_p < T_q$, 则 $T_q \geq 1$ 。考察 $j = T_q - 1$ 时的 x_j 。

模 p 的坐标已到达 1, 故 $x_j \equiv 1 \pmod{p}$ 。模 q 的坐标尚未到达 1, 但下一平方为 1, 所以它是模 q 的另一个平方根 -1 。于是 x_j 的坐标为 $(1, -1)$, 是非平凡根。下一项第一次在两个坐标同时为 1, 算法提取因子成功。 $T_q < T_p$ 同理。

若 $T_p = T_q = t > 0$ ，则前一步两个坐标都不是 1，平方却都为 1，因此均为 -1 。CRT 给出前一步为 $-1 \pmod n$ ，算法失败。若 $t = 0$ ，两坐标一开始就是 1，初始分支失败。至首次整体到达 1 前，不可能出现另一个平方为 1 的项，否则整体已更早到达 1。

所以，在互质底数分支中，

$$\boxed{\text{成功} \iff T_p \neq T_q}, \quad \boxed{\text{失败} \iff T_p = T_q}.$$

例如 $n = 55, a = 2, r = 5$ 时，模 5 的序列为 2, 4, 1，首次到达时刻为 2；模 11 为 10, 1, 1，首次时刻为 1。不同步使中间项 34 的坐标为 $(-1, 1)$ 。

15.3 为什么取幂后在二次幂阶子群中均匀

先分析模 p 的坐标。由第 13.4 节，该坐标在 U_p 上均匀。取一个原根 g ，每个 $a \pmod p$ 唯一对应 g^k ， $0 \leq k < 2^\alpha u$ 。这是双射，所以 k 均匀。

因为 $u \mid r$ 且两者均奇，写 $r = uw$ ， w 为奇数。令 $h = g^u$ ，由幂阶公式

$$\text{ord}_p(h) = \frac{2^\alpha u}{\gcd(2^\alpha u, u)} = 2^\alpha.$$

取幂后

$$a^r \equiv (g^k)^{uw} = h^{kw} \pmod p.$$

现在是两个清楚的映射：

映射	均匀性的依据
$k \mapsto k \pmod{2^\alpha}$	每个余数恰有 u 个原像
$j \mapsto wj \pmod{2^\alpha}$	w 奇，故与 2^α 互质，乘法是排列

所以 $kw \pmod{2^\alpha}$ 均匀。再经 $j \mapsto h^j$ 的双射， $a^r \pmod p$ 在子群

$$H_p = \langle h \rangle = \{1, h, \dots, h^{2^\alpha-1}\}$$

上均匀，每个元素的概率为 $2^{-\alpha}$ 。模 q 同理得到 2^β 阶子群上的均匀分布。

这个结论不要求 w 与全部 $p-1$ 互质，只要求它与 2^α 互质。取幂也没有在原来的 $p-1$ 个非零类上保持均匀，输出被限制到了更小的子群。

15.4 两种取模不要混淆：p 为十三的完整例子

取 $p = 13$, $p-1 = 12 = 2^2 \cdot 3$, 原根 $g = 2$ 。因此 $\alpha = 2, u = 3, h = g^u = 8$ 的阶为 4。

指数 k	$2^k \bmod 13$	指数 k	$2^k \bmod 13$
0	1	6	12
1	2	7	11
2	4	8	9
3	8	9	5
4	3	10	10
5	6	11	7

均匀选择非零类等价于均匀选择这十二个指数。为展示取幂映射，取奇数 $r = 9 = 3 \cdot 3$, 即 $w = 3$ 。这里仅演示模 13 的均匀性，不另外指定 RSA 的另一个质数或整个 K 。

$$a^9 \equiv 8^{3k} \pmod{13}.$$

指数余数及输出为：

$k \bmod 4$	对应的三个 k	$3k \bmod 4$	$8^{3k} \bmod 13$
0	0, 4, 8	0	1
1	1, 5, 9	3	5
2	2, 6, 10	2	12
3	3, 7, 11	1	8

每行三个等概率输入，所以输出 **1, 5, 12, 8** 各有概率 $3/12 = 1/4$ 。

模 13 控制幂的值；模 4 控制指数的周期。 $8^j \bmod 13$ 按 **1, 8, 12, 5** 循环，所以 $8^{11} \equiv 8^3 \equiv 5 \pmod{13}$ 。指数里的 11 对 4 取余，并没有把幂值改成模 4。

若把奇数乘子 $w = 3$ 换成偶数 **2**，模 4 的指数只得到 **0, 2**，不能保持全部四个指数余数上的均匀。这解释了奇数条件发挥的作用。

15.5 从元素阶计数得到到达时刻分布

$a^r \bmod p$ 属于 2^α 阶循环群。由拉格朗日定理，元素阶只能为 **1, 2, 4, ..., 2 $^\alpha$** 。若其阶恰为 2^t ，则

$$(a^r)^{2^j} \equiv 1 \pmod{p} \iff 2^t \mid 2^j \iff j \geq t.$$

因此首次到达时刻恰为 $T_p = t$ ； $t = 0$ 时元素已是单位元，初始即到达。第 12.5 节的计数给出

$$P(T_p = t) = \begin{cases} 2^{-\alpha}, & t = 0, \\ 2^{t-1-\alpha}, & 1 \leq t \leq \alpha, \\ 0, & \text{其他整数 } t. \end{cases}$$

在 $p = 13$ 的例子中，子群元素及阶为：

元素	1	8	12	5
阶	1	4	2	4
T_p	0	2	1	2

每个元素概率为 $1/4$ ，故 T_p 的概率为 $1/4, 1/4, 1/2$ 。元素等概率，不表示阶的不同取值等概率；阶为 4 的元素有两个。

一般分布的总和为

$$\frac{1 + \sum_{t=1}^{\alpha} 2^{t-1}}{2^{\alpha}} = 1.$$

每个概率都不超过 $1/2$ ： $t = 0$ 用 $\alpha \geq 1$ ； $1 \leq t \leq \alpha$ 时最大为 $2^{\alpha-1-\alpha} = 1/2$ 。模 q 只需将 α 换成 β 。

15.6 独立性、加权上界与至少一半的成功率

由第 13.4 节，模 p 与模 q 坐标独立。 T_p 只依赖前一个坐标， T_q 只依赖后一个，固定的 r 没有额外随机性，所以第 13.3 节保证 T_p, T_q 独立。

相等事件按 t 分解，得到

$$P(\text{失败}) = P(T_p = T_q) = \sum_t P(T_p = t)P(T_q = t).$$

令 $a_t = P(T_p = t)$ 、 $b_t = P(T_q = t)$ 。由刚才分布， $a_t \geq 0$ 、 $\sum_t a_t = 1$ ，且每个 $b_t \leq 1/2$ 。因此

$$\begin{aligned} P(\text{失败}) &= \sum_t a_t b_t \\ &\leq \sum_t a_t \cdot \frac{1}{2} \\ &= \frac{1}{2} \sum_t a_t = \frac{1}{2}. \end{aligned}$$

求和的是带权重的概率，权重总和为 **1**，所以这一步是加权平均。不是直接相加多个 **1/2**。从条件概率看，无论 T_p 最终取哪个有可能的值，独立的 T_q 恰好取同一值的概率都不超过 **1/2**；按这些情况的概率加权后，上界仍不变。

最后，成功与失败恰为互补事件，所以

$$P(\text{成功}) = P(T_p \neq T_q) \geq \frac{1}{2}.$$

这一结论使用了所有前提：两个不同奇质数、正的统一指数倍数、均匀互质抽样、原根循环性、元素阶计数以及 CRT 的独立性。

15.7 五十五的实际失败概率与通用上界

对 $p = 5, q = 11$ ，有 $\alpha = 2, \beta = 1$ ，两个分布为：

t	$a_t = P(T_p = t)$	$b_t = P(T_q = t)$	乘积 $a_t b_t$
0	1/4	1/2	1/8
1	1/4	1/2	1/8
2	1/2	0	0
合计	1	1	1/4

实际失败概率为

$$\frac{1}{4} \cdot \frac{1}{2} + \frac{1}{4} \cdot \frac{1}{2} + \frac{1}{2} \cdot 0 = \frac{1}{4},$$

所以互质分支成功概率为 **3/4**。若只使用 $b_t \leq 1/2$ ，则得到

$$\frac{1}{4} \cdot \frac{1}{2} + \frac{1}{4} \cdot \frac{1}{2} + \frac{1}{2} \cdot \frac{1}{2} = \frac{1}{2}.$$

把第三行实际为 **0** 的概率替换成 **1/2**，使上界变宽；没有改变算法的真实概率。这正是“实际值为 **1/4**”与“普遍可保证不超过 **1/2**”能够同时成立的原因。

模 **55** 有 **40** 个互质类，其中 **30** 个底数成功、**10** 个失败。若按第 14.5 节从 **1, ..., 54** 全部候选抽样，其余 **14** 个非互质底数直接给出因子，故完整尝试的成功概率为 $44/54 = 22/27$ 。这个数与 **3/4** 对应不同的样本空间。

15.8 精确概率公式与最差情形

令 $m_0 = \min(\alpha, \beta)$ 。两边有正概率的共同取值为 $0, 1, \dots, m_0$ 。代入分布，

$$\begin{aligned} P(\text{失败}) &= \frac{1 + \sum_{t=1}^{m_0} 2^{2t-2}}{2^{\alpha+\beta}} \\ &= \frac{1 + \sum_{j=0}^{m_0-1} 4^j}{2^{\alpha+\beta}} \\ &= \frac{1 + (4^{m_0} - 1)/3}{2^{\alpha+\beta}} \\ &= \boxed{\frac{4^{m_0} + 2}{3 \cdot 2^{\alpha+\beta}}} \end{aligned}$$

因此

$$\boxed{P(\text{成功}) = 1 - \frac{4^{m_0} + 2}{3 \cdot 2^{\alpha+\beta}}}.$$

这些是互质均匀抽样下的精确概率，不依赖 K 中多出的奇因子或因子 **2**：前者在指数子群中作排列，后者只延长序列已经为 **1** 的尾部。

α	β	失败概率	成功概率
1	1	1/2	1/2
2	1	1/4	3/4
2	2	3/8	5/8

α	β	失败概率	成功概率
3	3	11/32	21/32
2	4	3/32	29/32

若 $\alpha = \beta = m_0$ ，失败概率为 $1/3 + 2/(3 \cdot 4^{m_0})$ ； $m_0 = 1$ 时为 $1/2$ ，以后严格减小。
 若两者不同，分母进一步乘以 $2^{|\alpha-\beta|}$ ，失败概率更小。因此最低成功概率 $1/2$ 确实在 $\alpha = \beta = 1$ 达到。取 $p = 3, q = 7$ 即为一个实例。

15.9 证明依赖与容易误用的地方

完整链条是：原根给出循环坐标 → 幂阶公式确定 2^α 阶子群 → 等大小原像与奇数排列保证均匀 → 拉格朗日及欧拉函数计数给出到达时刻分布 → CRT 保证两个时刻独立 → 非负权重总和为 1 保证失败上界 → 不同到达时刻给出非平凡根和真因子。

回读时可用以下表定位条件：

容易跳过的推理	必须补上的依据
阶只可能是 2 的幂	元素阶整除子群阶；也可直接用循环群幂阶公式
每种阶的数量是 $\varphi(d)$	循环群中指数的互质计数，不是任意群都如此
输入均匀所以取幂后均匀	要在正确输出子群上检查等大小原像
同一个底数的两个坐标独立	均匀输入加 CRT 的笛卡尔积双射
许多概率都至多一半，所以和至多一半	实际相加的是权重总和为 1 的加权平均
重复后失败概率相乘	每次独立重新抽样
知道私钥能分解，所以直接解密能力也能分解	两种计算能力不同，该归约只使用已知有效指数

这些条件组成理论证明。数值枚举与随机模拟可以帮助检查例子，不能替代任何一环。

第 16 章：概念辨析、拓展、练习与来源覆盖

[返回目录](#)

16.1 三种“个数”不要混淆

问题	记号	例子
不超过 x 的素数有多少个	$\pi(x)$	$\pi(12) = 5$: 2、3、5、7、11
n 有多少种不同质因子	$\omega(n)$	$\omega(360) = 3$
n 的质因子算重数后有多少个	$\Omega(n)$	$\Omega(360) = 3 + 2 + 1 = 6$
代表范围内与 n 互质的整数有多少个	$\varphi(n)$	$\varphi(360) = 96$

如果 $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, 则 $\omega(n) = k$ 、 $\Omega(n) = \sum_i \alpha_i$, 并约定 $\omega(1) = \Omega(1) = 0$ 。因每个质因子至少为 2, $n \geq 2^{\Omega(n)}$, 所以

$$\omega(n) \leq \Omega(n) \leq \lfloor \log_2 n \rfloor.$$

若有 k 个不同质因子, 把它们排序后第 i 个不小于第 i 个质数, 所以 n 至少是前 k 个质数的乘积。因此 $n < 6$ 时最多一种, $n < 30$ 时最多两种, $n < 210$ 时最多三种。这个上界讨论的是最大可能数量, 不能当成给定整数的实际数量。

16.2 素数计数与渐近公式：只介绍拓展结论

素数定理为

$$\pi(x) \sim \frac{x}{\ln x} \quad (x \rightarrow \infty).$$

$\sim$ 表示两者比值趋于 1, 不是精确相等; 相对误差趋于 0, 也不意味着绝对误差趋于 0。对整数 n , “小于 n ”的计数是 $\pi(n-1)$, 不是 $\pi(n)$ 。参看 [Carl Pomerance](#) 的数论讲义。

上限 n	不超过 n 的素数实际个数	$n/\ln n$ (约)
10	4	4.3
100	25	21.7
1000	168	144.8
10000	1229	1085.7
100000	9592	8685.9
1000000	78498	72382.4

接近大数 x 的整数“成为素数的密度约为 $1/\ln x$ ”是一种启发式解释，不是证明。对数积分是更精细的经典近似；采用从 2 起积分的记号时，可写 $\text{Li}_2(x) = \int_2^x dt/\ln t$ 。它与采用主值积分定义的 $\text{li}(x)$ 相差常数，记号应说明约定。

原对话还提到不同质因子数的最大值与平均值，其渐近量级分别是 $\ln x/\ln \ln x$ 与 $\ln \ln x$ 。它们是关于一批整数的统计结论，不是计算 $\omega(n)$ 的精确公式。为把平均与正常数量分开，准确写成

$$\max_{1 \leq m \leq x} \omega(m) \sim \frac{\ln x}{\ln \ln x}, \quad \frac{1}{[x]} \sum_{m \leq x} \omega(m) \sim \ln \ln x.$$

Hardy—Ramanujan 定理的核心是“正常数量”：对每个固定 $\epsilon > 0$ ，除占比趋于 0 的例外整数外， $\omega(m)$ 接近 $\ln \ln m$ ，相对偏差小于 ϵ 。平均值结论与正常数量结论相关，但不是同一个陈述；这一区别可参看 [Carl Pomerance 关于数量阶的讲义](#)。

以上解析数论结论不在本篇的证明范围内，也不参与 RSA 正确性证明。拓展资料可参看数论笔记中的算术函数阶。

16.3 卡迈克尔函数：统一周期与单个元素周期

对 $n \geq 2$ ，令 U_n 为互质剩余类。定义 $\lambda(n)$ 为所有 $a \in U_n$ 都满足 $a^L \equiv 1$ 的最小正整数 L 。

由第 7.2 节，一个 L 对全部元素可用，当且仅当它被每个元素的阶整除。因此

$$\lambda(n) = \text{lcm}\{\text{ord}_n(a) : a \in U_n\}, \quad \text{ord}_n(a) \mid \lambda(n) \mid \varphi(n).$$

最右边整除来自每个阶均整除 $\varphi(n)$ ，所以其最小公倍数也整除。模 8 时阶分别为 1, 2, 2, 2，故 $\lambda(8) = 2 < 4 = \varphi(8)$ 。

对质数 p ，原根的存在保证 $\lambda(p) = p - 1$ 。对两个不同质数 p, q ，中国剩余定理把 U_{pq} 对应到 $U_p \times U_q$ ，并且一个幂等于 1 当且仅当两个坐标都等于 1，所以

$$\lambda(pq) = \text{lcm}(p - 1, q - 1).$$

充分性：该最小公倍数使两个坐标的幂都为 1。必要性：由标准中国剩余定理可选互质元素，其模 p 坐标为原根、模 q 坐标为 1，所以任意统一指数必须被 $p - 1$ 整除；交换坐标又得 $q - 1$ 整除它，因而被两者最小公倍数整除。

三种指数的区别是：阶针对一个底数， $\lambda(n)$ 针对全部互质底数的最小统一指数， $\varphi(n)$ 是互质底数个数，同时提供一个统一指数。一般 λ 的质数幂公式及全部结构不在本篇展开。

16.4 练习与解答

题 1。 求 3^{100} 模 7 的余数。

解： $100 \equiv 4 \pmod{6}$ ， $3^{100} \equiv 3^4 = 81 \equiv 4$ 。

题 2。 对任意整数 a ， $a^6 \equiv 1 \pmod{7}$ 与 $a^7 \equiv a \pmod{7}$ 哪个必成立？

解：第二个。第一个还需 $7 \nmid a$ ，取 $a = 7$ 即得反例。

题 3。 解 $2x \equiv 3 \pmod{5}$ 。

解：2 的逆元为 3，所以 $x \equiv 9 \equiv 4 \pmod{5}$ 。

题 4。已知 $\text{ord}_{17}(3) = 16$ ，求 3^4 的阶。

解： $16/\gcd(16, 4) = 4$ 。直接检验 $3^4 \equiv 13$, $13^2 \equiv -1$, $13^4 \equiv 1$ 。

题 5。解 $x \equiv 1 \pmod{4}$ 、 $x \equiv 3 \pmod{6}$ 。

解：公约数 2 整除余数差 2，有解。写 $x = 1 + 4t$ ，得到 $2t \equiv 1 \pmod{3}$ ，所以 $t \equiv 2$, $x \equiv 9 \pmod{12}$ 。

题 6。对 $n = 55, e = 3, d = 27$ ，消息 $m = 0, 11, 54$ 是否都能恢复？

解：是。第 11.4 节已覆盖任意消息，包括 0 与质因子倍数。加密余数分别为 0, 11, 54，相应解密余数也是它们本身。

题 7。一个 12 阶循环群中，阶为 1, 2, 3, 4, 6, 12 的元素分别有多少个？解：分别为 $\varphi(d) = 1, 1, 2, 2, 2, 4$ ，总和为 12；其他正整数不整除 12 时个数为 0。

题 8。已知 h 模 13 的阶为 4, $h = 8$ ，求 h^{2026} 。解：指数对 4 取余为 2，幂的值仍模 13，所以 $8^{2026} \equiv 8^2 \equiv 12 \pmod{13}$ 。

题 9。两个独立随机变量的分布为 $(1/4, 1/4, 1/2)$ 与 $(1/2, 1/2, 0)$ ，它们相等的概率是多少？为何仍可写上界 $1/2$ ？解：按相同位置作乘积并求和得 $1/4$ 。第二分布每项至多 $1/2$ ，以第一分布为权重，权重总和为 1，所以通用上界为 $1/2$ 。上界不等于精确值。

题 10。对 $n = 55, e = 3, d = 7$ ，连续平方分解仍可用吗？解：

$ed - 1 = 20 = \lambda(55)$ ，不是 $\varphi(55) = 40$ 的倍数，但条件已足够。 $20 = 2^2 \cdot 5$ ；取 $a = 2$ 得 32, 34, 1，照样提取 11, 5。互质底数成功概率仍为 $3/4$ 。

题 11。若 $p - 1$ 与 $q - 1$ 中因子 2 的次数分别为 2, 4，互质均匀底数一次尝试的成功概率是多少？解： $m_0 = 2$ ，失败概率为 $(4^2 + 2)/(3 \cdot 2^6) = 3/32$ ，成功概率为 $29/32$ 。

题 12。单次失败概率为 $1/4$ ，独立重复 3 次仍全部失败的概率与期望成功次数是多少？

解：分别为 $(1/4)^3 = 1/64$ 与 $1/(1 - 1/4) = 4/3$ 。若不独立重选，这些式子未必成立。

16.5 原对话覆盖索引与整理校正

原始顺序共有 21 轮；下表每一行对应一个用户问题及其助手回答。重复回答的内容合并，关键追问保留到相应证明中。

轮次	用户的问题或关注点	对应章节
1	介绍费马小定理与简单应用	第 4 章、第 16 章练习
2	为什么缩减指数需要互质	第 2 章、第 4 章
3	质因数分解为什么唯一	第 3 章
4	使用的几个基础结论还没有证明	第 2 章、第 3 章
5	为什么两边必然同时约完	第 3 章
6	小于某数的素数个数公式	第 16 章
7	素因子个数与上界	第 16 章
8	想找欧拉相关的计数公式	第 5 章
9	展开说明欧拉函数公式	第 5 章
10	为什么乘积展开对应容斥	第 5 章
11	欧拉函数与小定理结合的结论	第 6 章
12	继续：乘法阶	第 7 章
13	继续：原根及存在性	第 8 章、第 16 章
14	原根回答公式显示异常	第 7 章、第 8 章重新排版
15	上传截图，再指出公式损坏	第 8 章补“阶不整除”及质数幂解释

轮次	用户的问题或关注点	对应章节
16	为什么阶互质时乘积阶相乘	第 7 章
17	欧拉定理如何联系密码学	第 11 章
18	不一定存在所需的两个指数吧	第 2 章、第 11 章
19	非互质消息的 RSA 怎么证明	第 11 章
20	中国剩余定理的一般表述	第 9 章、第 10 章
21	两种形式的详细证明	第 9 章、第 10 章

本版补全了互质消去律、幂的阶公式、因式定理的直接恒等式、容斥的权重证明、 $p = 2$ 与 $\varphi(1)$ 的边界；区分了素因子数的平均与正常数量，并将安全参数的存在性例子与安全建议分开。原根分类与解析数论拓展明确标注未证明。

16.6 新增对话与补充的覆盖索引

第二份分享对话单独共有 11 轮，以下独立编号；加权上界是用户后来直接粘贴的一条补充，不计作分享中的新轮次。

轮次	用户的问题或关注点	对应章节
1	与分解相关却不能证明必须分解，是什么意思	第 11 章、第 14 章
2	已知有效私钥指数为什么可以恢复因子	第 14 章、第 15 章
3	平方为一为什么模各个质数只能为正负一	第 2 章、第 14 章
4	非平凡平方根为什么可以用最大公约数分解	第 14 章
5	成功概率至少一半怎么证明	第 13 章、第 15 章

轮次	用户的问题或关注点	对应章节
6	质数模乘法群为什么循环	第 8 章、第 12 章
7	为什么指数和取幂后的元素仍均匀	第 13 章、第 15 章
8	为什么开始对二次幂取模	第 7 章、第 15 章
9	怎样由均匀元素导出时刻概率	第 12 章、第 15 章
10	元素阶为什么整除群阶	第 12 章
11	阶为 d 的元素为什么有欧拉函数那么多	第 12 章、第 15 章
补充	为什么一串加权概率的和仍不超过一半	第 13 章、第 15 章

第二版补上有限群、陪集划分、零指数阶公式、循环群的阶计数、等大小原像、条件概率与独立性；用较弱的正 $\lambda(n)$ 倍数统一分解算法，并区分互质抽样与全候选抽样。完整覆盖“指数的模数”“阶到时刻”“加权平均上界”三处反复追问，给出精确概率及独立重试的期望分析。

16.7 阅读、分享与版本关系

第一版保存在旧版本目录中的 [HTML](#)与[PDF](#)。第二版保留第一版的初等数论证明与拓展，增加群论和概率主线，目录和来源覆盖索引按新章节更新。

“欧拉函数”“欧拉定理”也与复数中的欧拉公式 $e^{i\theta} = \cos \theta + i \sin \theta$ 不同；后者可在[代数基本定理笔记](#)中阅读。模质数的多项式与乘法结构，可以接到[多项式与分圆域笔记](#)以及[伽罗瓦理论笔记](#)。

配套 [Markdown](#) 与[阅读索引](#)供整套导航。[HTML](#) 的正文、公式与公式源码查看工具嵌入单文件，可离线阅读；[PDF](#) 提供静态正文、目录页码及分层书签。跨笔记、[Markdown](#) 与来源归档链接需要对应文件，分享整套时请保留目录层级。