

费马小定理与初等数论笔记

第五版 · 2026-10-11

从同余、乘法阶和原根，走到RSA、随机分解的概率证明，以及签名安全的计算关系。

本篇以一般推导为主。每个符号在使用时说明含义，每一步推理交代依据；具体例子用于解释容易混淆的地方。第1—13章是连续的主线，第14—18章保留完整基础证明、拓展和练习，可在需要时回查。若主要关心概率证明，先读第8—11章；遇到阶、原根或CRT的疑问，再回到第4—6章。

来源为[第一份原对话](#)的21轮、[第二份原对话](#)的11轮，以及[加权概率补充](#)。第一份对话中的一张公式报错截图仅保留附件引用，未直接查看；正文公式重新排版。另加入[第三份原对话](#)的9轮，讨论RSA反演、签名伪造与安全假设。第19章提供全部原问题与章节的对应关系。

目录

第 1 章：同余、消去与模逆元	3
第 2 章：费马小定理与指数缩减	4
第 3 章：欧拉函数与欧拉定理	6
第 4 章：乘法阶与指数的周期	8
第 5 章：原根与循环群的含义	10
第 6 章：中国剩余定理与余数坐标	12
第 7 章：RSA的指数选择与解密正确性	14
第 8 章：已知私钥怎样随机分解模数	16
第 9 章：成功条件与两个首次到达时间	18
第 10 章：取幂的均匀性与到达时间分布	21
第 11 章：相等概率为什么是加权平均	25
第 12 章：重试、运行时间与RSA结论的范围	28
第 13 章：RSA反演、签名伪造与安全假设	30
第 14 章：补充证明：逆元、唯一分解与CRT	38
第 15 章：补充证明：质数为什么一定有原根	47
第 16 章：补充证明：群、阶与欧拉函数计数	52
第 17 章：补充：精确概率、统一指数与运行时间	58
第 18 章：辨清几个计数问题，再用练习回查	62
第 19 章：从原问题回到笔记，以及怎样分享	65

第 1 章：同余、消去与模逆元

[返回目录](#)

1.1 同余是在比较什么

固定一个正整数 n 作为模数。写 $a \equiv b \pmod{n}$ ，意思是 n 整除 $a - b$ ：两个整数相差 n 的整数倍，因此除以 n 的余数相同。例如 $17 \equiv 2 \pmod{5}$ ，因为 $17 - 2 = 3 \cdot 5$ 。

同余不要求两个整数本身相等。它只保留“除以 n 后属于哪一种余数”的信息。以后说“模 n 的一个数”，指的是一个剩余类；计算时可以用 $0, 1, \dots, n - 1$ 中的代表表示它。

为什么可以先取余再计算？若 $a = b + un$ 、 $c = d + vn$ ，其中 u, v 为整数，那么

$$a + c = (b + d) + (u + v)n, \quad ac = bd + n(ud + vb + uvn).$$

这两个差都含有因子 n ，所以加法和乘法保留同余。重复使用乘法，就得到 $a^k \equiv b^k \pmod{n}$ ，这里 k 是非负整数。这是以后所有模幂运算的依据。

1.2 为什么约分需要互质

在整数等式中，非零因子可以消去；在同余中，需要额外条件。若

$$ac \equiv bc \pmod{n},$$

我们知道的是 $n \mid c(a - b)$ 。要推出 $n \mid (a - b)$ ，必须保证 c 不会替 $a - b$ 承担模数中的质因子。条件 $\gcd(c, n) = 1$ 恰好保证这一点。这里 $\gcd$ 表示最大公约数，最大公约数为1就是互质。

严格地说，裴蜀等式告诉我们：若 $\gcd(c, n) = 1$ ，存在整数 u, v 使 $uc + vn = 1$ 。两边乘 $a - b$ ，得到

$$a - b = uc(a - b) + vn(a - b).$$

右边两项都被 n 整除，所以左边也被 n 整除。于是

$$\gcd(c, n) = 1, \quad ac \equiv bc \pmod{n} \implies a \equiv b \pmod{n}.$$

不互质时结论确实会失败： $2 \cdot 1 \equiv 2 \cdot 4 \pmod{6}$ ，但 $1 \not\equiv 4 \pmod{6}$ 。这个例子用于提醒我们检查条件；一般证明仍是上面的裴蜀等式推导。裴蜀等式自身的证明在第14章。

1.3 模逆元怎样代替除法

若 $ab \equiv 1 \pmod{n}$ ，就称 b 为 a 的模 n 逆元。它的作用是：乘 a 之后再乘 b ，会恢复原来的剩余类。因此解 $ax \equiv c \pmod{n}$ 时，可以两边乘 b ，得到 $x \equiv bc \pmod{n}$ 。

逆元存在的充要条件是 $\gcd(a, n) = 1$ 。充分性来自裴蜀等式： $au + nv = 1$ 模 n 后给出 $au \equiv 1$ 。必要性也直接：若 a 和 n 有大于1的公因子，这个公因子会整除 ab 和 n ，不可能让 ab 与1只相差 n 的倍数。

所以后面证明中出现“消去一个因子”“取逆元”时，互质条件不是形式上的附加语，而是让这一步成立的原因。

第 2 章：费马小定理与指数缩减

[返回目录](#)

2.1 定理说了什么

若 p 是质数，且 p 不整除整数 a ，则

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

质数 p 的非零剩余类都与 p 互质，因此第1章的消去律可以使用。这个条件会在证明最后一步发挥作用。

还有一种包含所有整数 a 的形式： $a^p \equiv a \pmod{p}$ 。若 $p \nmid a$ ，把第一式乘 a 即可；若 $p \mid a$ ，两边模 p 都为0。反过来，只有在 $p \nmid a$ 时，才能从后一式约去 a ，得到前一式。

2.2 为什么乘法会把非零余数重新排列

考虑非零剩余类 $1, 2, \dots, p-1$ ，把它们分别乘 a 。要证明乘后的余数仍然是这一整组数，只需排除两种情况。

第一，不会出现0。若 $ai \equiv 0 \pmod{p}$ ，因为 a 与 p 互质，可以消去 a ，得到 $i \equiv 0$ ，与 $1 \leq i \leq p-1$ 矛盾。

第二，不会有两个不同位置产生相同余数。若 $ai \equiv aj \pmod{p}$ ，消去 a 得到 $i \equiv j$ 。而 i, j 都在1至 $p-1$ 之间，同余只能意味着 $i = j$ 。

因此，乘后的 $p-1$ 个余数非零且互不相同；总共只有 $p-1$ 种非零余数，它们必然把原来的整组数全部占满。这里“重新排列”指的就是这件事，并没有增加或丢失余数。

把这组同余相乘，就有

$$(a \cdot 1)(a \cdot 2) \cdots (a \cdot (p-1)) \equiv 1 \cdot 2 \cdots (p-1) \pmod{p}.$$

左边含有 $p-1$ 个 a ，所以可写为 $a^{p-1}(p-1)!$ 。两边的 $(p-1)!$ 都与 p 互质，可以消去。剩下的正是 $a^{p-1} \equiv 1$ 。

证明的顺序是：**互质允许消去** → **乘法没有重复和零** → **整组余数只是重排** → **相乘并消去共同乘积**。一般的欧拉定理还会使用同一思路。

2.3 为什么能缩减指数

若 $a^{p-1} \equiv 1$ ，把非负整数指数 m 写成

$$m = q(p-1) + r, \quad 0 \leq r < p-1,$$

就得到

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

这一步不是直接对指数套用同余运算法则；依据是每一整段 $p-1$ 次幂都贡献一个1。例如算 $3^{100} \bmod 7$ ，由于 $100 = 16 \cdot 6 + 4$ ，只需算 $3^4 \equiv 4 \pmod{7}$ 。例子中的“对6取余”和“对7取余”承担不同任务：6用于分解指数，7用于计算幂的值。

2.4 应用和使用边界

定理还可以证明整除： $a^p \equiv a \pmod{p}$ 等价于 $p \mid (a^p - a)$ 。也可以给出逆元：当 $p \nmid a$ 时， $a \cdot a^{p-2} \equiv 1$ ，所以 a^{p-2} 是 a 的逆元。

但通过一次类似的幂同余检验，不能反过来保证模数是质数。例如 $341 = 11 \cdot 31$ ，却有 $2^{340} \equiv 1 \pmod{341}$ ，因为 $2^{10} = 1024 \equiv 1 \pmod{341}$ 。费马小定理给的是“质数必满足”的性质，并未证明“满足这个性质的数必为质数”。

第 3 章：欧拉函数与欧拉定理

[返回目录](#)

3.1 欧拉函数数的是哪些整数

$\varphi(n)$ 表示 $1, 2, \dots, n$ 中与 n 互质的整数个数。等价地，它是模 n 可逆剩余类的个数。它数的不是素数，也不是 n 的质因子。

若 $n = \prod_{i=1}^k p_i^{e_i}$ 是质因数分解，其中 p_i 互不相同，那么

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

为什么只出现不同的质因子，而没有直接出现次数 e_i ？一个整数与 n 不互质，意味着它被某个 p_i 整除。是否被 p_i 整除已经决定了它要被排除，不需要再分别排除 p_i^2, p_i^3 的倍数。幂次仍包含在前面的 n 中。

3.2 乘积公式为什么就是容斥

先看 n 恰有两个不同质因子 p, q 的情况。在 1 至 n 中, p 的倍数有 n/p 个, q 的倍数有 n/q 个。如果直接都减掉, 同时被 p, q 整除的整数会被减两次, 所以要补回 $n/(pq)$ 个:

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

有更多质因子时, 原理相同: 减去单个倍数集合, 加回两两交集, 再减去三重交集, 依次交替。展开 $\prod_i (1 - 1/p_i)$ 时, 选一个负项得到一次减法, 选两个负项得到交集的加法, 选三个负项得到三重交集的减法。乘积展开恰好记录了每种交集和符号。

对于每一个具体整数, 这样加减后的总权重是什么? 若它不被任何 p_i 整除, 权重为 1 ; 若它被其中 $j \geq 1$ 个整除, 权重为 $(1 - 1)^j = 0$ 。因此最终恰好保留互质整数。完整容斥展开在第14章。

特别地, $\varphi(p) = p - 1$, $\varphi(p^e) = p^e - p^{e-1}$ 。若 m, n 互质, CRT把模 mn 的可逆类与一对模 m, n 的可逆类对应, 因而 $\varphi(mn) = \varphi(m)\varphi(n)$ 。这个对应在第6章解释。

3.3 欧拉定理的证明为什么仍是重排

欧拉定理把质数模数推广到一般模数: 若 $n \geq 2$ 且 $\gcd(a, n) = 1$, 则

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

设 $r_1, \dots, r_{\varphi(n)}$ 代表全部与 n 互质的剩余类。乘 a 后仍互质: 若某个质因子同时整除 ar_i 和 n , 它必整除 a 或 r_i , 而这两种情况都被互质条件排除。不同的 r_i 也不会碰到一起: $ar_i \equiv ar_j$ 可以消去 a 。

于是 $ar_1, \dots, ar_{\varphi(n)}$ 只是这一整组可逆类的重排。相乘得到

$$a^{\varphi(n)} r_1 \cdots r_{\varphi(n)} \equiv r_1 \cdots r_{\varphi(n)} \pmod{n}.$$

乘积仍与 n 互质，消去后就是欧拉定理。注意，两次消去都检查了互质：先对 a 使用，最后对 $r_1 \cdots r_{\varphi(n)}$ 使用。

3.4 欧拉指数保证了什么

当 $n = p$ 为质数时， $\varphi(p) = p - 1$ ，欧拉定理退回费马小定理。对一般互质底数，它同样允许把指数对 $\varphi(n)$ 取余，推导方式与第2.3节相同。

但 $\varphi(n)$ 只是一个一定能使幂回到1的指数，不一定最小；下一章会定义这个最小指数。若底数不与模数互质，欧拉定理就不能直接使用。这也是为什么RSA的解密正确性不能只写一句“由欧拉定理”，还必须处理不互质的消息。

第 4 章：乘法阶与指数的周期

[返回目录](#)

4.1 阶是最小的“回到1”的指数

若 $\gcd(a, n) = 1$ ，定义

$$d = \text{ord}_n(a) = \min\{k \geq 1 : a^k \equiv 1 \pmod{n}\}.$$

这个 d 称为 a 模 n 的乘法阶。它存在，因为欧拉定理已经给出一个符合条件的正指数 $\varphi(n)$ 。定义只是从所有符合条件的正指数中取最小的一个。

例如模7时， $2, 2^2, 2^3$ 的余数是 $2, 4, 1$ ，所以 $\text{ord}_7(2) = 3$ ；而费马小定理给的指数是6。这里6没有错，它只是没有声称自己最小。

4.2 为什么其他回到1的指数必为阶的倍数

若 $a^m \equiv 1$ ，把 m 除以 d ：

$$m = qd + r, \quad 0 \leq r < d.$$

因为 $a^d \equiv 1$ ，有 $a^m \equiv a^r$ ，所以 $a^r \equiv 1$ 。如果 $r > 0$ ，它就是一个比 d 更小、还能使幂回到1的正指数，违反 d 的最小性。因此 $r = 0$ ，即 $d \mid m$ 。

反过来，如果 $d \mid m$ ， a^m 是 a^d 的整数次幂，当然同余于1。于是对非负整数 m ，

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

把 $m = \varphi(n)$ 代入，得到 $d \mid \varphi(n)$ 。这是比“阶不超过欧拉函数”更强的整除结论，后面的计数需要的是它的整除性。

4.3 对指数取模，为什么不改变幂值的模数

同样把任意非负指数 k 写成 $k = qd + r$ ，有 $a^k \equiv a^r \pmod{n}$ 。因此幂的值由 $k \bmod d$ 决定。

这里有两个不同的对象： k 是指数，其周期为 d ； a^k 是幂值，仍在模 n 下计算。可以记为

$$k \bmod d \longmapsto a^k \bmod n.$$

例如8模13的阶为4，故 $8^{11} \equiv 8^3 \equiv 5 \pmod{13}$ 。指数11对4取余，是在寻找循环中的位置；最后的余数5仍是对13计算出来的。后面从 p 转到 2^α 时，发生的正是这种“指数周期改变”，不是把幂值的模数换掉。

4.4 怎样求阶，以及一个幂的阶

求阶时不必试所有正整数，只需在 $\varphi(n)$ 的因数中找最小满足 $a^d \equiv 1$ 的 d 。若已知某个合适的指数 M ，可以逐个尝试移除 M 的质因子；每次都检验移除后的幂是否仍为1。

另一个常用结论是：若 a 的阶为 d ，那么 a^k 的阶为

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

它为什么有这个形状？ $(a^k)^m \equiv 1$ 等价于 $d \mid km$ 。写 $d = cd'$ 、 $k = ck'$ ，其中 $c = \gcd(d, k)$ ，则条件变成 $d' \mid k'm$ 。由于 d', k' 互质，等价于 $d' \mid m$ ；最小正 m 就是 d' 。对 $k = 0$ ，公式也给出阶1，因为 $a^0 = 1$ 。

第 5 章：原根与循环群的含义

[返回目录](#)

5.1 原根为什么能给所有非零余数编号

模质数 p 的非零剩余类共有 $p - 1$ 个。若某个 g 的阶恰好为 $p - 1$ ，则

$$g^0, g^1, \dots, g^{p-2}$$

模 p 互不相同。否则若 $g^i \equiv g^j$ 且 $0 \leq i < j < p - 1$ ，乘 g^i 的逆元就得到 $g^{j-i} \equiv 1$ ；而 $0 < j - i < p - 1$ ，与阶的最小性矛盾。

这 $p - 1$ 个不同的非零余数必然遍历全部非零类。这样的 g 称为模 p 的原根。因此每个非零余数 a 都能唯一写为

$$a \equiv g^k \pmod{p}, \quad 0 \leq k < p - 1.$$

这里的 k 是 a 在幂循环中的编号。给余数编号，不意味着编号等于余数本身；编号的好处是把乘法转化为指数相加。

5.2 “循环群”是在概括哪件事

把模 n 的全部可逆剩余类记为 U_n ，运算是模 n 乘法。它们满足：乘积仍可逆，有单位元1，每个元素有逆元，乘法满足结合律。具有这些性质的集合称为群；“群的阶”表示它有多少个元素，因此 $|U_n| = \varphi(n)$ 。

如果整个群都能写成某个元素的幂，就称为循环群。于是“模质数 p 的非零剩余类构成 $p - 1$ 阶循环群”包含两个结论：它们在乘法下构成群；存在一个原根，能用幂遍历整个群。前一个结论来自逆元与乘法，后一个结论需要证明原根存在，不能混为一件事。

“元素的阶”是回到1所需的最小正指数；“群的阶”是元素总数。它们使用同一个词，但定义不同。有限群中，元素阶整除群阶；第16章用陪集划分证明。对于循环群，我们也可以直接从第4.4节的幂阶公式看出这一点。

5.3 为什么每个质数都有原根

每个质数 p 都存在原根。 $p = 2$ 时唯一非零类1就是原根，以下讨论 $p > 2$ 。这个结论的关键是：在模质数的运算中，一个非零多项式的根数不超过它的次数。因此，所有非零余数不可能都过早回到1。

具体说，令 $N = p - 1$ ，固定 N 的一个质数幂因子 ℓ^e ，其中 ℓ^{e+1} 不再整除 N 。多项式 $X^{N/\ell} - 1$ 的次数是 $N/\ell < N$ ，不可能让全部 N 个非零余数都成为根。因此存在一个余数 a 满足 $a^{N/\ell} \neq 1$ 。

a 的阶 d 整除 N ，但不整除 N/ℓ 。所以 d 中必须含有完整的因子 ℓ^e ；否则它的每个质数幂因子都包含在 N/ℓ 里，就会整除 N/ℓ 。具体取 $b = a^{d/\ell^e}$ ；幂阶公式给出它的阶为 $d/\gcd(d, d/\ell^e) = \ell^e$ ，因此我们得到一个阶恰为 ℓ^e 的元素。

对 N 的每个不同质因子这样做，得到一组阶两两互质的元素。在交换群中，阶互质的两个元素相乘，其阶等于两阶的乘积。逐个相乘，就得到阶为 N 的元素，也就是原根。

这里用到的多项式根数结论、幂阶公式以及“阶互质则乘积阶相乘”，在第15章逐项完整证明。这一段说明它们怎样接起来，避免把原根存在当作未经解释的口号。

5.4 为什么原根有欧拉函数那么多个

固定一个原根 g ，令 $N = p - 1$ 。全部非零类是 g^k ，且第4.4节给出

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

所以 g^k 仍为原根，当且仅当 $\gcd(N, k) = 1$ 。在 $0 \leq k < N$ 的编号中，符合条件的个数就是 $\varphi(N)$ 。因此模 p 原根的个数为 $\varphi(p-1)$ ； $p=2$ 时只有非零类1，数量也是 $\varphi(1) = 1$ 。

合数模数下不能直接沿用原根存在性。例如模8的可逆类1, 3, 5, 7都平方为1，任何一个元素的阶都不超过2，无法生成4个元素。第15章也解释为什么多项式的根数论证不能照搬到一般合数模数。

第 6 章：中国剩余定理与余数坐标

[返回目录](#)

6.1 定理怎样合并多个同余条件

设 $m_1, \dots, m_k$ 是两两互质的正整数， $M = m_1 \cdots m_k$ 。中国剩余定理（CRT）说：给定任意余数 $a_1, \dots, a_k$ ，同余组

$$x \equiv a_i \pmod{m_i} \quad (1 \leq i \leq k)$$

有解，而且模 M 只有一个解。也就是说，答案可以有很多个整数代表，但它们都相差 M 的倍数。

“两两互质”是每一对不同模数的最大公约数都为1。它使各个同余要求之间没有共同因子造成的冲突，也保证完整周期是乘积 M 。

6.2 为什么存在：构造只影响一个坐标的项

令 $M_i = M/m_i$ 。由于模数两两互质， M_i 与 m_i 互质，所以有逆元 t_i 满足 $M_i t_i \equiv 1 \pmod{m_i}$ 。

现在看 $E_i = M_i t_i$ ：它对 m_i 余1，对所有其他 m_j 余0，因为 M_i 含有 m_j 这个因子。于是

$$x = \sum_{i=1}^k a_i E_i$$

对 m_j 取模时，除第 j 项以外都消失，只留下 $a_j \cdot 1$ 。所以这个 x 同时满足全部要求。这不是单纯记一个求和公式，而是在构造“只负责一个余数条件”的项，再把它们相加。

6.3 为什么唯一，以及为什么可以使用两个坐标

若 x, y 都满足全部同余，所有 m_i 都整除 $x - y$ 。因为 m_i 两两互质，它们的乘积 M 也整除 $x - y$ ，即 $x \equiv y \pmod{M}$ 。这就证明模 M 的唯一性。

特别地，若 p, q 是不同质数，模 $n = pq$ 的每个剩余类都唯一对应一对坐标：

$$x \bmod n \longleftrightarrow (x \bmod p, x \bmod q).$$

任意一对坐标都能合起来，合起来的类又只有一个，这就是双射。加法、乘法、取幂都可以在两个坐标分别进行，再合并结果。

例如模55的34对应 $(4, 1)$ ，也就是模5为 -1 、模11为1。计算 34^2 时，两边分别平方都得到1，CRT就保证 $34^2 \equiv 1 \pmod{55}$ 。这个例子只用于展示坐标的含义；一般结论是上面的双射。

如果 x 与 pq 互质，两个坐标都非零；反过来，两坐标都非零也意味着 x 与 pq 互质。因此CRT还给出 $U_{pq} \longleftrightarrow U_p \times U_q$ 。第9章会用它解释随机底数为什么产生独立坐标。

6.4 模数不互质时怎样修改

对于 $x \equiv a \pmod{m}$ 、 $x \equiv b \pmod{n}$ ，若 m, n 不互质，两个要求可能冲突。正确的相容条件是

$$\gcd(m, n) \mid (b - a).$$

必要性很直接： $x - a$ 被 m 整除， $x - b$ 被 n 整除，所以二者都被最大公约数整除，相减得到 $b - a$ 也必须被它整除。

充分性可由线性同余看出。令 $c = \gcd(m, n)$ ，先写 $x = a + mk$ ，代入第二个条件得到 $mk \equiv b - a \pmod{n}$ 。若 $c \mid (b - a)$ ，把整除关系中的三项都除以 c ，就得到模 n/c 的同余； m/c 与 n/c 互质，可以用逆元解出 k 。解的周期是 $\text{lcm}(m, n) = mn/c$ ，这里 lcm 表示最小公倍数。

多个模数的情形有解，当且仅当每一对余数满足对应的相容条件；最终周期是所有模数的最小公倍数。两两相容为什么足够，以及完整构造与唯一性证明，均放在第14章。

第 7 章：RSA 的指数选择与解密正确性

[返回目录](#)

7.1 公钥、私钥和模数各自做什么

取两个不同的奇质数 p, q ，令 $n = pq$ 。消息 m 用模 n 的一个剩余类表示。公钥是 (n, e) ，加密把 m 变为 $c \equiv m^e \pmod{n}$ ；私钥指数 d 用于计算 $c^d \pmod{n}$ 。

要让解密回到 m ，需要安排 $(m^e)^d = m^{ed}$ 与 m 同余。做法是选择 e, d 满足

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

于是存在非负整数 h 使 $ed = 1 + h\varphi(n)$ 。两个指数相乘后的“多余部分”是欧拉指数的倍数，这是它与欧拉定理连接的地方。

7.2 这些指数为什么一定可以选出来

先计算 $\varphi(n)$ ，再选择与它互质的正整数 e 。由第1章的逆元条件， e 模 $\varphi(n)$ 有逆元 d ，可以用扩展欧几里得算法算出，并取一个正整数代表。

因此 e, d 并非任意设定后再假定它们满足关系；先选择互质的 e ，逆元定理保证 d 存在。这里逆元的模数是 $\varphi(n)$ ，加密时的模数是 n ，两者用途不同。

对于与 n 互质的消息，欧拉定理直接给出

$$m^{ed} = m^{1+h\varphi(n)} = m(m^{\varphi(n)})^h \equiv m \pmod{n}.$$

但这只处理了互质消息。若消息含有 p 或 q 这个因子，不能继续套用模 n 的欧拉定理；需要下面的逐质数证明。

7.3 不互质的消息为什么也能还原

先对 p 证明 $m^{ed} \equiv m$ ，分成两个互补的情况。

若 $p \mid m$ ，因为 $ed \geq 1$ ， m^{ed} 和 m 模 p 都为0。若 $p \nmid m$ ，可以用费马小定理 $m^{p-1} \equiv 1 \pmod{p}$ 。而 $p-1$ 整除 $\varphi(n)$ ，故也整除 $ed-1$ ，于是

$$m^{ed} = m(m^{p-1})^{(ed-1)/(p-1)} \equiv m \pmod{p}.$$

无论 p 是否整除消息，模 p 的结论都成立。对 q 完全同理，得到 $m^{ed} \equiv m \pmod{q}$ 。CRT再把两个结论合起来，得到 $m^{ed} \equiv m \pmod{n}$ 。

这份证明没有假设消息与 n 互质。它利用的是：在每个质数坐标上，消息要么为0，要么可用费马小定理；两种情况覆盖了全部消息。

7.4 这与分解有什么关系

若能分解 n 得到 p, q ，就能计算 $\varphi(n)$ ，再由公开的 e 计算逆元 d ，从而解密。这证明了

$$\text{分解 } n \implies \text{恢复私钥指数并解密}.$$

还可以追问：已知 d ，能不能反过来分解 n ？答案是可以使用随机算法；下一章从 $ed-1$ 出发说明为什么。这里的计算关系不直接证明完整签名方案安全；RSA反演与签名伪造的区别在第13章继续说明。

这里讨论RSA的数学幂运算。实际RSA参数可采用更弱的 $ed \equiv 1 \pmod{\lambda(n)}$ 条件，其中 $\lambda(n) = \text{lcm}(p-1, q-1)$ ；它仍足以完成上面的逐质数证明。统一指数与具体规范的关系放在第17章。标准依据见RFC 8017第3.2节。

第 8 章：已知私钥怎样随机分解模数

[返回目录](#)

8.1 私钥给了我们哪一条额外信息

沿用 $n = pq$ ，其中 p, q 为不同奇质数。原对话的私钥关系给出

$$K = ed - 1 > 0, \quad \varphi(n) \mid K.$$

对于任意与 n 互质的 a ，欧拉定理保证 $a^K \equiv 1 \pmod{n}$ 。我们知道 n, e, d ，所以能计算 K ；这一步并不要求知道 p, q 。证明中使用 p, q 解释算法，算法本身不能预先使用它们。

把 K 中的全部因子2提出，写成 $K = 2^s r$ ，其中 r 为奇数。由于 $\varphi(n)$ 是偶数，这里 $s \geq 1$ 。接着构造连续平方序列

$$x_0 = a^r \bmod n, \quad x_{j+1} = x_j^2 \bmod n.$$

第 j 项同余于 $a^{2^j r}$ ，因此终点 $x_s \equiv a^K \equiv 1$ 。我们不是盲目平方；终点已由指数条件保证，现在要研究第一次到1之前的一项。

8.2 为什么“平方为1”能产生因子

若某个 x 满足 $x^2 \equiv 1 \pmod{n}$ ，则 $n \mid (x-1)(x+1)$ 。模 p 看， p 是质数，所以 p 必须整除 $x-1$ 或 $x+1$ ，即 $x \equiv 1$ 或 $-1 \pmod{p}$ 。模 q 同理。

因此 x 的两个CRT坐标只能是下面四种组合：

模 p	模 q	合并后的意义
1	1	$x \equiv 1 \pmod{n}$
-1	-1	$x \equiv -1 \pmod{n}$
1	-1	两边符号不同
-1	1	两边符号不同

CRT保证每种组合对应一个根。因为 p, q 都为奇数，模各个质数的1与-1不同，所以这四个根也互不相同。

最后两种称为1的非平凡平方根。若 $x \equiv 1 \pmod{p}$ 、 $x \equiv -1 \pmod{q}$ ，那么 $p \mid x - 1$ ，但 $q \nmid x - 1$ ；否则 q 会同时整除 $x - 1$ 与 $x + 1$ ，进而整除它们的差2，与 q 为奇质数矛盾。因此

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

符号相反时两个因子互换。最大公约数提取因子，是因为两个质因子分别落在 $x - 1$ 和 $x + 1$ 中，不是仅凭“平方为1”就能分解。若 $x \equiv \pm 1 \pmod{n}$ ，得到的只是1或整个 n ，没有拆出因子。

8.3 第一次到1之前的一项为什么值得检查

假设 $x_0 \neq 1$ ，并设 x_j 是序列第一次出现的1，那么 $j \geq 1$ 。它的前一项 x_{j-1} 满足 $x_{j-1}^2 \equiv 1$ ，但 $x_{j-1} \not\equiv 1$ ，因为这是第一次到1。

所以前一项只剩两种可能：它等于-1，算法这次失败；或者它是非平凡平方根，可以提取因子。初始就为1时也失败，因为没有前一项可检查。

一个简短核对是 $n = 55, e = 3, d = 27$ ，从而 $K = 80 = 2^4 \cdot 5$ 。取 $a = 2$ ，初始项 $2^5 \equiv 32$ ，随后平方得到34、1。前一项34不是1或54，所以得到 $\gcd(33, 55) = 11$ 。它只是一般算法的一次实例；成功条件来自上一节的四种符号组合。

8.4 完整算法与失败分支

算法可以写成下面的顺序。所有余数均取0至 $n - 1$ 的代表，输入满足上面的指数条件。

1. 从 $1, \dots, n - 1$ 均匀选取 a ，计算 $g = \gcd(a, n)$ 。若 $g > 1$ ，因 $a < n$ ， g 已是一个真因子，输出 $g, n/g$ 。
2. 若 $g = 1$ ，计算 $x = a^r \bmod n$ 。若 $x = 1$ ，本次失败，重新独立选取底数。
3. 最多进行 s 轮：令 $y = x^2 \bmod n$ 。若 $y \neq 1$ ，令 $x = y$ 继续；若 $y = 1$ 且 $x = n - 1$ ，本次失败；若 $y = 1$ 且 $x \neq n - 1$ ，输出 $\gcd(x - 1, n)$ 及另一个因子。

最后一个分支里的 x 也不可能是1：初始为1的情况已排除，后续一出现1就终止。因此它确实是非平凡平方根。合法输入下一定能在 s 轮内到达1，因为 $x_s = a^K \equiv 1$ 。输出因子可以用乘法检查。

8.5 为什么还需要证明概率

我们已经证明：若遇到非平凡平方根，算法会成功；也说明它可能失败。尚未证明的是，随机选择底数会多频繁地产生有用的根。

不能仅凭“四个平方根有两个有用”就断言成功率为一半。连续平方产生四个根的概率未必相同。需要从随机底数 a 出发，分析算法实际到达哪一个根。接下来的三章完成这一步。

第 9 章：成功条件与两个首次到达时间

[返回目录](#)

9.1 先固定随机选择的范围

先只研究与 n 互质的底数，即从 U_n 中均匀选取 a 。均匀表示其中每个剩余类被选到的概率都为 $1/\varphi(n)$ 。一旦 a 选定，后续取幂、平方和取最大公约数都由它确定，没有新的随机选择。

第8章从全部 $1, \dots, n-1$ 抽样的算法也适用：不互质的底数直接给出因子；条件于“选到的 a 互质”，各个互质底数仍然等可能。因此先证明互质分支的成功率，再把直接成功的分支加回来即可。

9.2 为什么要定义两个到达时间

连续平方的第 j 项是 $x_j \equiv a^{2^j r} \pmod{n}$ 。用CRT拆开，模 p 和模 q 各自形成一条平方序列。两边都最终到1，但到达的时刻可能不同。

令

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

T_p 表示模 p 第一次到1时，已经做了多少次平方； T_q 含义相同。初始 a^r 已经为1时，次数记为0。这两个量都由随机底数 a 决定，因此称为随机变量。它们存在且不大于 s ，因为第 s 项已经为1；到1以后再平方，仍为1。

引入它们的目的，是把“前一项属于哪种平方根”转化为“两个坐标是否同时第一次到1”。后者更容易计数。

9.3 为什么到达时间不同就成功

设 $T_p < T_q$ 。整体序列第一次到1的时刻是 T_q ：此时两边都为1，而此前模 q 还未到1。考察前一项 $j = T_q - 1$ 。

模 p 已经到1，所以前一项的 p 坐标为1。模 q 尚未到1，但下一次平方将为1，所以前一项的 q 坐标是 -1 。这里用的是质数下方程 $x^2 = 1$ 只有 ± 1 两个根，排除1后就只剩 -1 。

因此前一项的坐标为 $(1, -1)$ ，是非平凡平方根，算法成功。若 $T_q < T_p$ ，同理得到 $(-1, 1)$ ，也成功。

若 $T_p = T_q = t > 0$ ，前一项的两边都尚未到1，下一次却都为1，所以前一项为 $(-1, -1)$ ，即整体的 -1 ，算法失败。若 $t = 0$ ，初始整体已为1，也失败。所有可能都已覆盖，因此对于互质底数，

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

这一步只解释成功与失败的条件，还没有给出概率。下一步要问两个到达时间分别怎样分布，以及它们是否独立。

9.4 CRT为什么给出独立的随机坐标

第6章给出双射 $U_n \longleftrightarrow U_p \times U_q$ 。右边共有 $(p-1)(q-1)$ 对坐标；每一对恰好对应一个底数。均匀选择 U_n 中的底数，就等价于等可能地选择这些坐标对。

记 $A_p = a \bmod p$ 、 $A_q = a \bmod q$ 。固定一个非零余数 b 和一个非零余数 c ，有

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

固定 b 而让 c 任意，一共有 $q-1$ 对，所以 $P(A_p = b) = 1/(q-1)$ ；同理 $P(A_q = c) = 1/(p-1)$ 。联合概率等于两个边缘概率的乘积，这正是独立性。

也可以把坐标对看成一个完整的行列表：模 p 余数决定行，模 q 余数决定列。知道选中了哪一行，仍不会偏向这行中的某一列，因为每行都有相同的全部列。这个理解对应的仍是上面的精确计数，而不是另外的假设。

9.5 同一个底数产生的两个到达时间为什么也独立

T_p 只需要 a 的 p 坐标就能计算， T_q 只需要 q 坐标；固定的 r 没有额外随机性。因此分别对两个独立坐标做确定的运算，不会让它们相关。

把这一点写成计数更清楚。令 B_t 为模 p 到达时间等于 t 的余数集合， C_u 为模 q 到达时间等于 u 的余数集合。事件 $T_p = t, T_q = u$ 对应 $B_t \times C_u$ ，所以

$$P(T_p = t, T_q = u) = \frac{|B_t||C_u|}{(p-1)(q-1)} = P(T_p = t)P(T_q = u).$$

这里 $|B_t|$ 表示集合中的元素个数。对任意 t, u 都成立，所以 T_p, T_q 独立。关键不是“它们来自同一个底数”或“它们来自两个质数”，而是CRT保证均匀底数对应完整、均匀的坐标对。

9.6 概率证明现在还缺哪一步

我们已把失败转化为 $T_p = T_q$ ，也证明了两者的独立。还需要知道：每个到达时间出现的概率是否有统一上界。

接下来的目标是证明，对于任意 t ， $P(T_p = t) \leq 1/2$ ，模 q 也一样。路线是：先证明取幂后的初始余数在一个较小循环群上均匀，再根据元素的阶统计首次到达时间。这里“元素均匀”与“到达时间均匀”是不同结论；后一种均匀实际上通常不成立。

第 10 章：取幂的均匀性与到达时间分布

[返回目录](#)

10.1 均匀输入怎样才能产生均匀输出

先说明一个将反复使用的计数原则。若 X 在一个有限集合 S 上均匀，令 $Y = f(X)$ 。对于一个输出 y ，

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

分子是产生 y 的输入个数，也称 y 的原像个数。因为每个输入概率相同，输出概率就由有多少个输入合到这里决定。若每个可能输出的原像一样多，输出才均匀；若 f 是双射，每个输出只有一个原像，当然也均匀。

所以“底数均匀”本身不足以推出“取幂后均匀”。下面必须实际检查这个取幂映射的原像数量，以及哪些映射是双射。

10.2 把模数的乘法周期拆成奇部和2的幂

只分析模 p ，模 q 同理。把 $p - 1$ 中的因子2全部提出，写成

$$p - 1 = 2^\alpha u, \quad u \text{ 为奇数}.$$

α 表示 $p-1$ 含有多少个因子2；因为 p 为奇质数， $\alpha \geq 1$ 。另一方面，算法的指数是 $K = 2^s r$ ， r 为奇数。由于 $p-1 \mid K$ ，有 $s \geq \alpha$ 和 $u \mid r$ 。

后一个整除关系为什么成立？ $u \mid 2^s r$ ，但 u 是奇数，与 2^s 互质，所以可以消去 2^s ，推出 $u \mid r$ 。于是写 $r = uw$ ， w 也为奇数。

取模 p 的原根 g ，令 $h = g^u$ 。因为 g 的阶为 $p-1 = 2^\alpha u$ ，第4.4节给出

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

因此 h 生成一个恰有 2^α 个元素的循环群

$$H_p = \{1, h, h^2, \dots, h^{2^\alpha-1}\} \pmod{p}.$$

提出奇部 u 的作用，就是从长度 $2^\alpha u$ 的原根循环中，得到长度纯为2的幂的循环。算法先算 a^r ，也会消去这个奇部；下一节把两件事连接起来。

10.3 为什么指数开始对2的幂取模

原根给出唯一编号 $a \equiv g^k \pmod{p}$ ，其中 $0 \leq k < 2^\alpha u$ 。取 $r = uw$ 次幂后，

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

现在底数变为 h ，它的阶是 2^α 。所以 h^{kw} 的值由指数 $kw \bmod 2^\alpha$ 决定。这就是为什么指数的模数变为 2^α 。

幂值仍在模 p 下计算，指数则按 h 的周期取模 2^α 。没有把 $a^r \bmod p$ 改成 $a^r \bmod 2^\alpha$ 。第4.3节的指数与幂值区分在这里再次出现。

10.4 为什么取幂后在这个循环群上均匀

由第9章， $a \bmod p$ 在全部非零类上均匀。原根编号是双射，所以 k 也在 $0, \dots, 2^\alpha u - 1$ 上均匀。接着沿上一节的等式分三步看分布。

首先将 k 对 2^α 取余。固定余数 j ，恰有

$$j, j + 2^\alpha, \dots, j + (u - 1)2^\alpha$$

这 u 个编号产生它。每个余数的原像数相同，所以 $k \bmod 2^\alpha$ 均匀，每个概率为 $u/(2^\alpha u) = 2^{-\alpha}$ 。

其次把这个余数乘 w 。因为 w 为奇数， $\gcd(w, 2^\alpha) = 1$ ，乘法可消去：若 $wj_1 \equiv wj_2 \pmod{2^\alpha}$ ，必有 $j_1 \equiv j_2$ 。因此乘 w 是一个排列， $kw \bmod 2^\alpha$ 仍均匀。此处只需要 w 与 2^α 互质，不需要它与整个 $p - 1$ 互质。

最后由编号 j 转为 $h^j \bmod p$ 。由于 h 的阶恰好为 2^α ，这又是双射。所以

$$a^r \bmod p \text{ 在 } H_p \text{ 上均匀，每个元素的概率为 } 2^{-\alpha}.$$

完整的依据依次是：原根给出双射编号，取余有等大小原像，乘奇数是排列，最后的幂编号又是双射。取幂通常没有在全部 $p - 1$ 个非零类上保持均匀，而是在这个较小的 H_p 上均匀。

如果希望核对各步，可以取 $p = 13$ ： $p - 1 = 4 \cdot 3$ ，选原根 $g = 2$ ，则 $h = 8$ 的阶为4。取 $r = 9$ ，有 $w = 3$ ；12个编号对4取余时每个余数有3个原像，乘3再把四个余数重排，因此输出1, 8, 12, 5各占1/4。这个例子对应上面的原像数与排列，不承担一般证明。

10.5 到达时间为什么由元素阶决定

令 $z = a^r \bmod p$ ，它已在 H_p 中。假设 z 的阶为 d 。连续平方 j 次就是计算 z^{2^j} ，所以第4.2节告诉我们

$$z^{2^j} \equiv 1 \pmod{p} \iff d \mid 2^j.$$

因为 H_p 是 2^α 阶循环群， z 的阶必为 2^t ，其中 $0 \leq t \leq \alpha$ 。这可以直接从 $z = h^k$ 与幂阶公式 $d = 2^\alpha / \gcd(2^\alpha, k)$ 看出，也符合“元素阶整除群阶”的一般定理。

当 $d = 2^t$ 时, $d \mid 2^j$ 等价于 $j \geq t$, 所以最早到1的时刻恰为 $T_p = t$ 。 $t = 0$ 意味着 $d = 1$, 即初始 z 已经是1。现在问题变成: H_p 中有多少个元素的阶恰为 2^t ?

10.6 怎样从阶的个数得到概率

先做一般计数。设 h 的阶为 N , 全部元素是 h^k , $0 \leq k < N$ 。若 $d \mid N$, 由幂阶公式, h^k 的阶恰好为 d 等价于

$$\gcd(N, k) = \frac{N}{d}.$$

满足条件的编号必能写成 $k = (N/d)j$, 其中 $0 \leq j < d$ 。代入最大公约数, 条件进一步等价于 $\gcd(d, j) = 1$ 。这样的 j 恰有 $\varphi(d)$ 个, 所以循环群中阶恰为 d 的元素有 $\varphi(d)$ 个。

$d = 1$ 时只有单位元; 第16章保留完整的群论证明。

回到 $N = 2^\alpha$ 。阶为1的元素有1个; 阶为 2^t 、 $1 \leq t \leq \alpha$ 的元素有 $\varphi(2^t) = 2^{t-1}$ 个。这是因为 0 至 $2^t - 1$ 中与 2^t 互质的编号正是奇数, 恰占一半。

每个元素的概率已知为 $2^{-\alpha}$, 因此

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

这是“符合条件的元素个数除以全部元素个数”, 不是把各个到达时间直接设成等可能。比如 $\alpha = 2$ 时, 阶1、2、4分别有1、1、2个元素, 所以 T_p 取0、1、2的概率为 $1/4, 1/4, 1/2$ 。这个小例子显示: 元素均匀, 到达时间却不均匀, 因为不同阶的元素数量不同。

一般情况下, 所有概率的总和为 $(1 + 1 + 2 + \cdots + 2^{\alpha-1})/2^\alpha = 1$ 。而每个概率都不超过 $1/2$: $t = 0$ 用 $\alpha \geq 1$; $1 \leq t \leq \alpha$ 时最大值在 $t = \alpha$ 取得, 恰为 $2^{\alpha-1}/2^\alpha = 1/2$ 。模 q 完全同理, 只需把 α 换成 $q - 1$ 中因子2的次数 β 。

第 11 章：相等概率为什么是加权平均

[返回目录](#)

11.1 相等事件怎样分成互不重叠的情况

已知 T_p, T_q 独立，且 T_q 取任意具体值的概率都不超过 $1/2$ 。要计算 $T_p = T_q$ ，需要考虑它们可能同时等于0、同时等于1，等等。

不同共同取值对应互不重叠的事件：一次选择不可能既使两者同时等于0，又使它们同时等于1。因此可以把这些概率相加。独立性允许把每个“同时发生”的概率拆成乘积，于是

$$P(T_p = T_q) = \sum_t P(T_p = t, T_q = t) = \sum_t P(T_p = t)P(T_q = t).$$

求和覆盖所有可能的整数 t ；范围之外的概率为0。这里有两个不同理由：能相加，是因为共同取值的情况互不重叠；能相乘，是因为两个随机变量独立。不能把二者合并成一句“概率相加相乘”。

11.2 为什么不是把多个二分之一直接相加

令 $a_t = P(T_p = t)$ 、 $b_t = P(T_q = t)$ 。第一个概率 a_t 是“ T_p 取这个值”的比例，第二个概率 b_t 是这个值出现后，独立的 T_q 恰好匹配它的概率。

因此 $a_t b_t$ 才是这一种匹配在所有情况中所占的比例。只加 b_t ，就忽略了 T_p 取各个值的机会不同；把每一类内部的匹配率都当成全部情况的匹配率，也就不再是在算原来的事件。

这里 $a_t \geq 0$ 且 $\sum_t a_t = 1$ ，因为 T_p 总会取它的某一个可能值。因此 $\sum_t a_t b_t$ 是以 a_t 为权重，对 b_t 取加权平均。权重总和为1，是后面上界能保持为 $1/2$ 的关键。

11.3 一个短例子区分实际值与上界

用你补充过的分布核对这句话：若 a_t 依次为 $1/4, 1/4, 1/2$ ，而 b_t 为 $1/2, 1/2, 0$ ，实际相等概率是

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

只知道每个 $b_t \leq 1/2$ 时，可以把每一项的 b_t 替换成更大的上界 $1/2$ ，得到

$$P(T_p = T_q) \leq \frac{1}{4} \cdot \frac{1}{2} + \frac{1}{4} \cdot \frac{1}{2} + \frac{1}{2} \cdot \frac{1}{2} = \left(\frac{1}{4} + \frac{1}{4} + \frac{1}{2} \right) \frac{1}{2} = \frac{1}{2}.$$

第三个实际匹配率0被放宽成 $1/2$ ，所以实际值 $1/4$ 与通用上界 $1/2$ 可以同时成立。这里真正发挥作用的是三个权重加起来为1，而不是只有三个可能取值。下一节不再依赖这些具体比例。

11.4 一般情况下，上界为什么不会被求和放大

对每一个 t ，由于 $a_t \geq 0$ 且 $b_t \leq 1/2$ ，都有 $a_t b_t \leq a_t / 2$ 。逐项相加，得到

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

第二行使用每一项的上界，第三行只把公共常数 $1/2$ 提出求和，第四行使用权重总和为1。可能取值更多，并不会改变最后一步；增加一个可能值，也意味着要在总和为1的权重中分给它一部分。

这就是一般原则：若 $a_t \geq 0$ 、 $\sum_t a_t = 1$ ，且每个 $b_t \leq M$ ，那么 $\sum_t a_t b_t \leq M$ 。加权平均不会超过参与平均的各个值的最大值。

11.5 条件概率怎样解释同一个推导

全概率公式把相等事件按 T_p 的取值分类：

$$P(T_p = T_q) = \sum_{t: P(T_p=t)>0} P(T_p = t) P(T_q = t \mid T_p = t).$$

条件概率 $P(T_q = t \mid T_p = t)$ 表示：已知 $T_p = t$ 后， T_q 恰好匹配它的概率。由于独立，已知 T_p 不会改变 T_q 的分布，所以这个条件概率等于 $P(T_q = t) \leq 1/2$ 。将这些匹配概率按 T_p 各值出现的比例平均，总匹配概率仍不超过 $1/2$ 。

独立性为什么不能省略？如果 X 等可能取0、1，再令 $Y = X$ ，那么 Y 取每个值的概率都为 $1/2$ ，但 $P(X = Y) = 1$ 。原因是知道 X 以后， Y 的匹配概率变成1。RSA这里没有这个问题，因为第9章已经用CRT证明了两个坐标以及分别由它们决定的到达时间独立。

11.6 怎样得到至少一半的成功概率

第9章证明，对于互质底数，成功恰好是 $T_p \neq T_q$ 。相等与不相等互为补集，所以

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

把全部推理连起来：CRT提供独立坐标 → 取幕后在2的幂阶循环群上均匀 → 按元素阶统计到达时间 → 每个到达时间概率不超过一半 → 相等概率是加权平均 → 失败概率不超过一半。各步分别在第9—11章证明；最后一步没有省去前面条件。

结论适用于两个不同奇质数的乘积 $n = pq$ 、正整数 K 满足 $p-1, q-1 \mid K$ 、从全部互质类均匀抽样。原对话使用的 $K = ed - 1$ 且 $\varphi(n) \mid K$ 满足这些条件； $\lambda(n) \mid K$ 也足够。

若从全部 $1, \dots, n-1$ 抽样，不互质底数直接成功，互质部分的条件分布仍均匀。因此完整一次尝试也至少有一半成功率。更精确地，若 ρ 是互质分支的成功率，则

$$P(\text{完整尝试成功}) = 1 - \frac{\varphi(n)}{n-1}(1-\rho) \geq \frac{1}{2}.$$

这里 $\varphi(n)/(n-1)$ 是进入互质分支的概率；只有这一分支内的失败可能保留下来。精确概率公式在第17章，理解这条下界不必先算出它。

第 12 章：重试、运行时间与RSA结论的范围

[返回目录](#)

12.1 失败以后重试为什么有效

每次失败后重新独立、均匀选择底数，就得到新的一次尝试。若每次失败概率至多 $1/2$ ，独立重复 k 次都失败的概率至多

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

“独立重复”不能省略。若一直重复同一个失败底数，后续计算完全一样，重复次数增加不会改善成功率。重新抽样让前一次的失败不改变下一次的分布。

算法输出的因子始终可以验证，因此随机性影响的是需要尝试多少次，不影响成功输出是否正确。有限次全失败时，可以继续尝试；它不构成错误的分解结果。

12.2 为什么平均至多两次，不等于两次必成功

设单次成功率为 $\rho \geq 1/2$ ，令 N 为第一次成功时的尝试总次数。第 k 次恰好第一次成功，需要前 $k-1$ 次失败、第 k 次成功，所以 $P(N=k) = (1-\rho)^{k-1}\rho$ 。

期望 $E[N]$ 表示大量独立运行中尝试次数的平均值。其值为 $1/\rho \leq 2$ 。这个求和也可以从“第 $j+1$ 轮是否需要做”理解：第1轮一定需要做，第2轮只有第一次失败才需要做，第3轮只有前两次都失败才需要做。因此

$$E[N] = \sum_{j=0}^{\infty} P(N > j) = \sum_{j=0}^{\infty} (1-\rho)^j = \frac{1}{\rho} \leq 2.$$

第一等式的依据是：一个恰做 k 轮的运行，会在 $N > 0, N > 1, \dots, N > k - 1$ 这 k 个条件中各被计一次。对这些轮次指标取平均，再相加，就是平均总轮数。这解释了为什么能用尾概率计算期望。

期望至多2是平均表现，不是每次最多2轮；做很多轮仍有可能，只是尾概率按几何速度减小。

12.3 为什么是期望多项式时间

每次尝试需要求最大公约数、计算 $a^r \bmod n$ 以及最多 s 次平方。快速幂按照 r 的二进制展开进行，使用 $O(\log r)$ 次模乘法； $s \leq \log_2 K$ ，所以一次尝试的运算次数是 $O(\log K)$ 量级。

再考虑每个整数运算的位复杂度：中间余数小于 n ，有 $O(\log n)$ 位；模乘法与欧几里得算法都有关于这些位长的多项式时间实现。因此单轮耗时是关于 $\log n, \log K$ 的多项式。期望轮数至多2，所以期望总耗时仍为多项式。

“多项式时间”是按输入的位数衡量，不是按 n 本身衡量。完整位复杂度说明保留在第17章；本节说明成功概率怎样与运行时间接起来。标准结论的依据见《Handbook of Applied Cryptography》第3章Fact 3.30及第8章Fact 8.6。

12.4 恢复私钥与从密文恢复消息为什么要区分

我们证明了两个方向：分解 n 可以恢复 d ；已知满足条件的私钥指数 d ，可以随机分解 n 。因此“恢复私钥指数”与“分解模数”具有这里证明的计算联系。

但给定 (n, e, c) ，直接求出满足 $m^e \equiv c \pmod{n}$ 的消息，是另一种已知信息和计算任务，称为RSA反演。能还原一个密文，并不意味着已经得到一个对所有消息适用的私钥指数 d 。上面的随机分解算法必须从 d 构造已知的 $K = ed - 1$ ，不能从“某条消息已还原”自动得到这个输入。

所以这里没有证明“任意解密能力都能用于分解”。即便一种方法确实会解密，也不能把分解算法需要的私钥信息直接当作它已经提供的信息。RSA反演与整数分解之间的这个逻辑区别，也是第二份原对话的起点。第13章把这种区别写成明确的归约关系，并继续区分原

始RSA数值对与现代签名方案。

若已知 $\varphi(n)$ ，则另有直接分解方法。由

$$\varphi(n) = n - (p + q) + 1$$

得到 $S = p + q = n - \varphi(n) + 1$ ，再利用 $pq = n$ ， p, q 就是 $x^2 - Sx + n = 0$ 的两个根：

$$p, q = \frac{S \pm \sqrt{S^2 - 4n}}{2}.$$

这是因为和与积共同确定这两个因子。它说明欧拉函数与分解密切相关，同样没有证明一切解密方法都必须先知道欧拉函数。

12.5 怎样回查整条证明

若最后的加权平均已经理解，但仍对概率结论不踏实，可以分开检查三个来源：第9章解释为什么不同步就成功、为什么两边独立；第10章解释每个到达时间概率为什么不超过一半；第11章只把这些结论合起来。

若卡在基础定理，第14章补逆元、唯一分解、容斥与CRT；第15章补原根存在性；第16章补群论中的阶与计数；第17章给精确概率、统一指数与复杂度；第18章保留概念辨析和练习。补充章节按疑问查阅，不要求先把所有抽象结论学完再阅读主线。

第 13 章：RSA反演、签名伪造与安全假设

[返回目录](#)

第12章已经区分了恢复私钥与恢复某条消息。本章继续回答：知道消息及其签名，为什么不能直接推出私钥？能够构造一个通过数学验签的数值对，为什么还不等于能随意改写消息？这些问题需要同时看清计算任务、归约方向和签名方案的安全定义。

13.1 先分清消息、消息代表值与签名

继续固定 $n = pq$ ，其中 p, q 是不同奇质数。公开指数 $e > 1$ 与 $\lambda(n) = \text{lcm}(p-1, q-1)$ 互质，私钥指数 d 满足 $ed \equiv 1 \pmod{\lambda(n)}$ 。

用 m 表示实际消息，例如一段文字或一个文件；用 x 表示进入RSA幂运算的整数代表，取 $0 \leq x < n$ ；用 t 表示签名的整数代表。暂时只看原始RSA运算：

$$t = x^d \pmod{n}, \quad t^e \equiv x \pmod{n}.$$

签名使用 d ，验证使用公开的 e 。这里的 x 并不自动等于实际消息 m ：如何从消息得到代表值，是完整签名方案的一部分。现代PSS编码会在消息和RSA运算之间增加明确的步骤，见第13.9节。

13.2 一组消息和签名约束了哪个指数

假设 x 与 n 互质，记 $h = \text{ord}_n(x)$ 为它的乘法阶。已知 $t \equiv x^d \pmod{n}$ ，尝试求一个指数 z 满足 $x^z \equiv t \pmod{n}$ 。对于非负指数 z ，有

$$x^z \equiv x^d \pmod{n} \iff h \mid (z - d).$$

因为 x 有逆元，可把两边化成 $x^{z-d} \equiv 1$ ；第4章说明回到1的指数恰是阶的倍数。因此即使找到一个解，确定的也是 $z \equiv d \pmod{h}$ ，不是唯一的整数 d 。这个求秘密指数的任务具有离散对数的形式；它与给定 x 求 t 的RSA反演任务不同。

例如 $n = 55, e = 3, d = 27, x = 2$ 。计算得到 $2^{27} \pmod{55} = 18$ ，而 $2^7 \pmod{55}$ 也为18。由于 $\text{ord}_{55}(2) = 20$ ，全部非负指数解为 $z \equiv 7 \pmod{20}$ 。这个例子中7也恰好是有效私钥指数，因为 $3 \cdot 7 \equiv 1 \pmod{20}$ 。

但这种巧合不能推广到任意底数。取 $x = 1$ 时，任何指数都满足 $x^z \equiv 1$ ，其中 $z = 1$ 显然不能作为同一公钥的有效私钥： $3 \not\equiv 1 \pmod{20}$ 。因此“对这一组 x, t 成立”与“对全部消息完成正确私钥运算”是两个条件。

若 x 与 n 不互质，就不能直接套用乘法群中的阶；先算 $\gcd(x, n)$ ，若结果介于1和 n 之间，已经得到非平凡因子。特殊数值 $x = 0, 1$ 尤其不能代表一般实例的困难性。

13.3 三个计算问题各自要求输出什么

问题	已知输入	需要输出
整数分解	$n = pq$	p, q
私钥恢复	合法的 n, e	一个正整数 d ，满足 $ed \equiv 1 \pmod{\lambda(n)}$
RSA反演	合法的 n, e 和给定的 x	t ，满足 $t^e \equiv x \pmod{n}$

有效私钥不必是最初生成的那个整数代表；相差 $\lambda(n)$ 的指数代表可给出同样的私钥运算。RSA反演则只要求当前输入的原像，不要求输出指数。

对合法RSA参数，幂映射 $t \mapsto t^e \bmod n$ 是全部剩余类上的置换。因为第7章证明 $(t^e)^d \equiv t \pmod{n}$ ， d 次幂提供逆映射，所以每个 x 都有唯一的模 n 原像。原像唯一并不意味着知道高效求出它的方法。

讨论困难性时，通常在 U_n 上定义随机挑战；第7章的正确性则覆盖全部剩余类。不要把“某些特殊输入很容易反演”误读成“随机挑战普遍容易反演”。

13.4 归约符号为什么容易把方向写反

说 $B \leq_P A$ ，表示：可以调用问题 A 的求解算法，再用多项式时间的额外计算解决问题 B 。因此如果 A 容易， B 也容易；从这种归约看， B 不比 A 更难。

用“有 A 的解法，就能解 B ”的口头箭头时，方向是 $A \implies B$ ；用归约符号时，写的是 $B \leq_P A$ 。两种记号表达同一关系，但左右位置相反。

分解的算法可以用于恢复私钥：先得到 p, q ，计算 $\lambda(n)$ ，再求 e 的模逆元。因此私钥恢复归约到分解。

私钥恢复的算法也可以用于分解：先取得有效 d ，计算正数 $K = ed - 1$ ，再运行第8—11章的随机分解算法。因此分解随机归约到私钥恢复。该算法总能核验输出的因子，期望运行时间为多项式；也可限制重试轮数，得到失败概率可控的有界时间算法。

知道 d 以后，快速幂给出 $t = x^d \bmod n$ ，所以RSA反演归约到私钥恢复。综合起来，允许随机化归约时可写成

$$\text{RSA反演} \leq_{\text{rand-poly}} \text{私钥恢复} \equiv_{\text{rand-poly}} \text{分解}.$$

这里前一个归约实际可取确定性的；随机性用于从私钥到分解的方向。本章的等价性针对给定合法公钥的标准双素数RSA实例：比较同一 n, e 下的分解任务与私钥恢复任务。

多项式等价说明的是可解性能够转移，不说明最佳算法的实际耗时相同。算法的次数、成功概率与输入位长仍要分别记录。具体私钥与分解联系可参照《Handbook of Applied Cryptography》Fact 8.6。

13.5 为什么反演能力不自动交出私钥

假设有一个程序，输入 x 就输出它的RSA原像 t 。它给出的是幂映射的输出能力，并没有直接给出整数 d 。第8章的分解算法需要明确的 $K = ed - 1$ ；不能因为程序会做私钥运算，就把这个未知整数当作已知。

即使程序可处理任意输入，也不能凭上述证明断言能从它恢复 d 或分解 n 。一般RSA反演到分解的多项式归约仍不是这里已有的结论；关于两者关系，参照《Handbook of Applied Cryptography》Remark 8.7。

逻辑上， $B \leq_P A$ 允许从“A容易”推出“B容易”，也允许从“B困难”推出“A困难”；却不允许从“A困难”推出“B困难”。因此相信分解困难，仍不足以仅靠上面的归约证明RSA反演困难；同时，尚未证明等价也不足以证明反演严格更容易。

13.6 已知数值对为什么未必多出私钥信息

只用公钥，也能生成一个满足原始RSA等式的数值对：先选 t ，再算 $x = t^e \bmod n$ 。随后 $t^e \equiv x$ 当然成立；由于RSA幂映射是置换，这个 t 也就是 x 的原始RSA签名值。

所以，如果某算法只需要任意有效数值对 (x, t) 就能高效恢复有效 d ，可以先用公钥制造这样的数值对，再调用它，最后分解 n 。这是一个算法转换，不是因为“数值对没有任何信息”而直接宣告不可能。

还要核对算法要求的输入分布：若要求 x 在 U_n 上均匀，先均匀选 $t \in U_n$ ，置换保证 $x = t^e$ 也均匀；若算法要求特定消息格式、额外签名样本或特殊输入，不能直接说这个构造满足全部条件。PSS的有效消息—签名对还要满足编码验证，不能用任意 x, t 替代。

13.7 修改签名的字节，与伪造有效签名

消息和签名都是可被修改的字节串。签名的作用是让验证者检查收到的消息是否与该签名相符，而不是阻止攻击者写入新字节。

在原始RSA中，若把代表值 x 换成不同的 x' ，保留 t 就不能通过等式验证。若同时换成 t' ，就必须满足 $(t')^e \equiv x' \pmod{n}$ 。对预先给定的原始代表值 x' ，这个要求正是RSA反演。

但不能把一切伪造攻击都直接归为“求一个独立RSA挑战的原像”。攻击者可能已取得合法签名，甚至可以请求签名；这些额外能力会改变计算任务。下一节说明原始RSA怎样利用这种额外信息。

13.8 原始RSA的乘法性质怎样产生伪造

若已有两组合法原始签名 $t_1^e \equiv x_1$ 、 $t_2^e \equiv x_2$ ，相乘得到

$$(t_1 t_2)^e \equiv x_1 x_2 \pmod{n}.$$

所以 $t_1 t_2 \bmod n$ 是 $x_1 x_2 \bmod n$ 的签名。若乘积代表此前未获签名的消息，就得到一个新消息的有效签名。这说明反演困难也不能单独保证原始RSA签名安全。

允许请求原始签名时，还可对指定目标 $x \in U_n$ 构造攻击。选一个可逆 r ，令

$$y = x r^e \bmod n.$$

选取满足 $y \neq x$ 的 r ，请求 y 的合法签名 $s = y^d \bmod n$ 。因为 $r^{ed} \equiv r$ ，有 $s \equiv x^d r \pmod{n}$ ，于是

$$t = sr^{-1} \bmod n \implies t^e \equiv x \pmod{n}.$$

这里仅请求了其他代表值的签名，就得到目标 x 的签名。逆元和快速幂都可高效计算；攻击利用了签名接口，所以不意味着已经找到只输入 n, e, x 的通用反演算法。

这也补足“随便生成的 x 没有实际意义”的讨论：简单反向构造确实不能让攻击者自由指定 x ，但在更强的攻击模型中，原始RSA仍会出现针对指定目标的伪造。若消息还需经过编码，上述请求的 y 未必是某条消息的合法编码，攻击步骤就不能直接照搬。

13.9 PSS怎样把实际消息与RSA运算接起来

RSA-PSS先对实际消息 m 计算哈希，再结合盐和掩码生成函数按EMSA-PSS规则编码为字节串 EM ；将它转换成整数代表 x ，最后计算 $t = x^d \bmod n$ 。简记为

$$m \xrightarrow{\text{哈希与PSS编码}} EM \xrightarrow{\text{转成整数}} x \xrightarrow{\text{RSA私钥运算}} t.$$

验证者从 t 计算 $x' = t^e \bmod n$ ，转回编码字节串，检查编码结构、位长、盐与消息哈希的一致性。盐可由编码恢复，验证者不需要事先保存签名时使用的盐。

因此攻击者先选 t 算出的 x' ，还必须通过完整PSS验证。它不一定是合法PSS编码，更不一定与攻击者想要的 m' 一致。不能把这个要求简化为 $H(m') = x'$ ：PSS的RSA输入代表不是一个裸哈希值。

原始RSA的乘法性质仍存在，但两个合法编码代表的乘积未必是任何目标消息的合法编码。因此原始数值域中的攻击不再自动成为PSS消息域中的攻击。这个观察解释编码的作用；PSS的安全性还需正式归约，而不是仅由“乘积通常格式不对”证明。操作规则参照RFC 8017 §8.1.1—8.1.2及§9.1。

13.10 为什么“没有攻击意义”仍可能违反安全定义

实际攻击可能要求伪造有意义的转账指令。形式化签名安全采用更严格、也更便于分析的标准：允许攻击者拿到公钥并请求若干消息的签名，最后它必须难以输出一条**此前未请求签名的新消息**及其有效签名。这里允许请求的接口称为签名预言机；它是安全模型给攻击者的能力，不是说攻击者知道私钥。

攻击者可以根据先前答复选择下一条请求。如果输出的新消息通过验证，即使内容没有实际用途，也算赢得这个攻击实验。这称为选择消息攻击下的存在性不可伪造性，缩写EUFCMA。定义与实验见Boneh—Shoup 《A Graduate Course in Applied Cryptography》§13.1。

“选择消息攻击”描述攻击者能选择请求签名的消息；“存在性伪造”描述最终只需伪造某条新消息。两者不矛盾。希望伪造一条预先指定消息，是更具体的目标；若不说明目标何时选定，本章不把它直接命名为selective forgery。

原始RSA把整数代表本身当作消息，先选 t 再算 x 的构造已经破坏这种标准，即使 x 毫无实际意义。PSS把实际消息作为输入，必须在消息域上判断伪造是否成立。普通EUFCMA也不要求排除“同一已签消息的另一份新签名”；那是更强的安全定义，不能混在一起。

13.11 可证明安全到底证明了哪一步

RSA假设描述一个随机挑战实验：按指定方式生成合法公钥，均匀选取 $u \in U_n$ ，计算 $x = u^e \bmod n$ ，只向攻击者提供 n, e, x 。假设随着参数位长增加，任何经典概率多项式时间算法都不能以非可忽略的概率恢复 u 。这里“可忽略”指最终小于任意固定的位长负幂，排除了仍有逆多项式成功率的攻击。它是关于实例分布和成功概率的假设，不是声称每个输入都难。

签名安全证明则从一个假设存在的伪造算法出发，构造一个解决RSA挑战的算法。构造必须处理攻击者的签名请求，并定量控制运行时间和成功概率。因此，若反演困难，就能在证明条件下推出伪造也困难。

PSS的相关证明把哈希和掩码生成函数理想化为随机预言机：对同一个输入始终给出同一个输出，对新输入按规则给出独立均匀输出。这是模型条件；实际固定哈希函数不是数学上真正的随机预言机。RFC 8017 §8.1明确以该模型说明PSS伪造与RSA反演的联系。本文解释归约的含义，不重现PSS的完整安全证明。

需要分别记录三个判断：归约在指定模型下成立，是数学证明；RSA反演对相应随机实例困难，是假设；现实部署能否抵抗已知攻击，还涉及参数与实现。不能从其中一个判断直接省略另外两个。

13.12 为什么没有无条件困难性证明仍会研究和使用的

未证明某个问题困难，并不等于已找到容易的解法；长期未发现高效攻击，也不等于已经证明永远不存在。密码学的做法是明确假设、公开分析攻击，并用归约说明方案是否额外引入了可利用的弱点。

多项式归约是渐近结论，实际参数还需要结合已知算法的资源成本。即使数学模型中的归约成立，也不能自动涵盖不安全的随机数、错误的编码验证或实现泄漏。本章只解释安全依据，不给出现实系统的参数推荐，也不把原对话的安全强度表当作固定不变的数学定理。

原对话还提到一次一密和量子计算，作为边界比较即可。一次一密 $c = m \oplus k$ 在密钥独立均匀、与消息等长、保密且只使用一次时，可提供信息论保密：对每个固定 m, c ，恰有一个 k 产生这个 c ，所以密文分布不随明文变化。但这个结论只谈保密，不自动提供消息认证；攻击者翻转密文位会相应翻转明文位。

上述RSA假设特意限定经典算法。Shor的量子分解算法表明，允许相应量子计算模型时，可以在多项式时间分解整数；这与“目前是否具备攻击具体密钥的硬件”是不同问题。算法来源见Shor的原论文。后量子标准与迁移时间属于会变化的工程信息，不在这份初等数论笔记中固定为结论。

13.13 用四个问题回查整条逻辑

回看一个RSA论断时，依次问：输入究竟是什么？要输出什么？攻击者还能请求哪些运算？结论在哪个模型与假设下成立？

论断	能得出的结论	不能省略的条件
已知有效 d	可构造 $ed - 1$ 并随机分解 n	标准双素数实例， $ed - 1 > 0$
已知某条原像 t	已解出当前 x 的反演	未必得到有效 d
随便选 t 再算 x	得到原始RSA有效数值对	未必对应目标消息或PSS合法编码
可请求原始RSA签名	可利用乘法结构伪造目标代表的签名	请求代表可被签名接口接受
PSS具有条件性安全证明	在相应模型、假设下限制新消息伪造	不是无条件困难性定理

你在对话末尾提出“这个 x 不一定有攻击意义，攻击者不能随心所欲修改”，准确指出了反向构造的局限。接下来还要保留两点：形式化安全不以消息是否有用作为唯一判据；原始RSA在允许签名请求时仍可能伪造指定目标。把这两点与PSS的消息编码放在一起，才能从数学等式走到完整签名安全。

第 14 章：补充证明：逆元、唯一分解与CRT

[返回目录](#)

这一章供遇到“这一步还没证明”时回查。第1—12章已经解释主线的定理与推导；这里补足它们背后的基础结论。可按小节标题选读，不需要一次全部读完。

14.1 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。

14.2 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。

14.3 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。

14.4 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 $mn \mid A$ 。

14.5 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 $1/3$ 。

14.6 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。

14.7 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。

14.8 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。

14.9 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个数指数决定。

于是 $\gcd(m, n) \text{lcm}(m, n) = mn$ 。一个整数同时被所有 m_i 整除，当且仅当被 $\text{lcm}(m_1, \dots, m_k)$ 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。

14.10 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。

14.11 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。

14.12 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 13.4 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

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

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。

14.13 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。

14.14 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。

14.15 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

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

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。

14.16 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。

14.17 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 13.9 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。

14.18 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。

14.19 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。

14.20 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 15 章：补充证明：质数为什么一定有原根

[返回目录](#)

第5章已经说明原根的定义和存在性证明的路线。这一章只解决存在性与相关阶公式, 适合想追问“每个质数为什么都能找到这样的底数”时阅读。证明先准备两个工具, 再限制多项式的根数, 最后逐个拼出所需的质数幂周期。

15.1 辅助引理一：一个幂的阶

若 a 的阶为 d , $m \geq 0$, 则

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

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。

15.2 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。

15.3 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。

15.4 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 4 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 14.2 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。

15.5 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
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

15.6 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 16 章：补充证明：群、阶与欧拉函数计数

[返回目录](#)

第10章已经从幂阶公式解释循环群的阶计数。这里保留一般群中的定义与完整证明，并补上“元素阶整除群阶”的陪集论证。群是概括模乘法的语言；下面先从可逆剩余类说明运算，再引入一般定义。概率符号的严格定义也放在本章末尾，供回查。

16.1 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 13.4 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 13.3 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 15 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。

16.2 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 4.2 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。

16.3 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

$$|G| = k|H|, \quad |H| \mid |G|.$$

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

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

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。

16.4 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 14.1 节的论证在群中原样成立：对 $k \geq 0$ ，

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

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。

16.5 为什么阶为 d 的元素恰好有欧拉函数那么多

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 13.9 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。这就是第 10 章到达时间分布中的计数依据。

16.6 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 14.4 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 14.3 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 14.2 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。

16.7 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。

16.8 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。

16.9 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。

第 17 章：补充：精确概率、统一指数与运行时间

[返回目录](#)

第11章的至少一半已经证明完了。这一章回答三个额外问题：实际概率是多少，指数条件能否再放宽，每轮计算需要多长时间。第一次理解加权上界时可以跳过这一章。

17.1 精确概率公式与最差情形

这里延续第10章的记号： $p - 1 = 2^\alpha u$ ，再写 $q - 1 = 2^\beta v$ ，其中 u, v 为奇数， $\alpha, \beta \geq 1$ 。下面算的是均匀选互质底数时的精确概率。

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
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。

17.2 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 4.2 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。

17.3 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。

17.4 有限次失败与期望多项式时间

第 11 章已经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 18 章：辨清几个计数问题，再用练习回查

[返回目录](#)

本章保留原对话问过的素数数量、质因子数量及欧拉函数的区别。解析数论的渐近公式只作拓展，不参加前面的RSA证明。练习先挑你刚读过的主题，解答用于核对步骤。

18.1 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。

18.2 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

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

Hardy–Ramanujan 定理的核心是“正常数量”：对每个固定 $\varepsilon > 0$ ，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。

18.3 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： $16/\text{gcd}(16, 4) = 4$ 。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 7.3 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尝试次数是多少？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。

第 19 章：从原问题回到笔记，以及怎样分享

[返回目录](#)

19.1 第一份对话的21轮

这里按原来的追问顺序提供回查入口。原对话中选择的文字与公式显示问题也保留为来源数据；对于未直接查看的截图，不声称已经读过图像。

轮次	原来的问题或关注点	在哪里接着读
1	费马小定理及简单应用	第2章
2	为什么缩减指数需要互质	第1章 、 第2章
3	每个数为什么只有一种质因数分解	第14章
4	用过的基础结论还没有证明	第14章
5	两边为什么一定同时约完	第14章 唯一性证明
6	小于某个数的素数数量	第18章
7	质因子的种数及数量上界	第18章

轮次	原来的问题或关注点	在哪里接着读
8	想找欧拉相关的计数公式	第3章
9	展开欧拉函数公式	第3章、第14章
10	为什么乘积展开就是容斥	第3章、第14章
11	欧拉函数与小定理结合的结论	第3章
12	继续讲乘法阶	第4章
13	继续讲原根及存在性	第5章、第15章
14	原根回答里的公式显示异常	第5章、第15章重新排版
15	上传截图指出显示问题	只保留附件引用；原根证明在第15章重新排版
16	阶互质时乘积阶为什么相乘	第15章
17	欧拉定理怎样联系密码学	第7章
18	所需的两个指数一定存在吗	第7章、第14章
19	消息不互质时怎样证明RSA	第7章
20	中国剩余定理的一般形式	第6章、第14章
21	两种形式的详细证明	第14章

19.2 第二份对话的11轮与一条补充

后来的加权概率解释是单独补充，没有把它算成分享对话中的第12轮。

轮次	原来的问题或关注点	在哪里接着读
1	与分解有关，为什么仍不能说破解必须先分解	第12章
2	已知有效私钥为什么能恢复因子	第8章
3	平方为1，为什么质数下只能是正负1	第8章、第14章
4	非平凡平方根为什么能用最大公约数分解	第8章
5	成功概率至少一半怎么证明	第9章到第11章
6	质数下的乘法群为什么循环	第5章、第15章
7	为什么编号和取幂后的结果仍均匀	第10章
8	为什么开始把指数对2的幂取模	第4章、第10章
9	怎样从均匀余数导出到达次数的概率	第10章
10	元素阶为什么整除群阶	第16章
11	阶为 d 的元素为什么有 $\varphi(d)$ 个	第10章、第16章
补充	为什么求和后仍不超过一半	第11章

19.3 第三份对话的9轮

第三份对话从“已知消息和签名为何不能求私钥”出发，随后区分归约、反演与签名伪造。新增第13章按问题展开，已有的随机分解证明仍放在第8—11章，不重复搬入新章。

轮次	原来的问题或关注点	在哪里接着读
1	已知 n, e, x, t 为什么不能直接恢复 d	第13章13.1—13.3及13.6
2	已知私钥为什么能分解	第8—11章、第13章13.4

轮次	原来的问题或关注点	在哪里接着读
3	相互转化是否表示多项式意义下一样难	第13章13.4—13.5
4	RSA反演是不是求 d	第13章13.3
5	反演与其他两个问题究竟什么关系	第13章13.4—13.5
6	为什么用尚无无条件安全证明的方案	第13章13.11—13.12
7	内容和签名能否一起篡改	第13章13.7—13.9
8	先选签名算 x ，再把内容改成 x	第13章13.6、13.9—13.10
9	任意 x 未必有攻击意义，不能随意修改	第13章13.8—13.10及13.13

整理时明确了归约符号的方向；限定用乘法阶分析指数时的互质条件；区分满足单个等式的指数与有效私钥；将PSS验证表述为完整编码检查。增加原始RSA签名请求下的目标伪造推导，区分实际攻击价值与EUF-CMA的形式化标准。原对话提到的一次一密、量子算法保留为边界说明，参数强度表与后量子迁移时间不作为固定数学结论收录。

19.4 本版更新与旧版保存

第五版新增第13章，微调第7.4和12.4节的衔接，保留已有基础证明、概率推导和练习内容；原第13—18章顺延为第14—19章。所有章节引用与导航同步更新。新章从明确计算任务出发，解释归约与安全假设，再讨论原始RSA和PSS的签名边界。PSS的完整安全归约不在本笔记内证明，已注明模型条件和原始资料。

此前版本均已归档。第四版见[第四版HTML](#)与[第四版PDF](#)。第三版见[第三版HTML](#)和[第三版PDF](#)。第二版的完整正文与检查材料保存在[第二版HTML](#)与[第二版PDF](#)所在目录。最早版本也保留：[第一版HTML](#)。

“欧拉函数”“欧拉定理”与复数里的欧拉公式 $e^{i\theta} = \cos \theta + i \sin \theta$ 是不同内容；后者在[代数基本定理笔记](#)中阅读。原根和模质数的多项式，可接到[多项式与分圆域笔记](#)和[伽罗瓦理论笔记](#)。

配套[Markdown](#)与[阅读索引](#)保留。HTML 的正文、样式、公式、公式源码查看及复制工具都嵌入单文件，可以离线阅读；PDF 保留正文、矢量公式、带页码目录和分层书签。跨笔记和原对话链接需要对应文件，分享整套时保留目录层级。