

费马小定理与初等数论笔记

第三版 · 2026-10-10

从“这个式子是什么意思”开始，一步一步走到 RSA 和成功概率。

这次先看可以手算的例子，遇到一个疑问就停下来解释。符号在用到时引入，详细的基础证明和拓展放在第13—17章。第一次阅读可以先读第1—12章；如果你现在最关心概率，先读第9章的模55例子，再接着读第10—11章。

全篇主要反复使用三个例子：模7看幂的循环，模13看随机取幂，模55看RSA与分解。每次从数值换到一般式子，都说明数值对应哪个符号。

来源是第一份分享对话21轮、第二份11轮，以及你直接补充的加权概率解释。第一份原对话、第二份原对话、补充内容均保留。第一份对话中的一张公式报错截图只保留附件引用，未直接查看；正文公式重新排版。第18章提供问题与章节的对应表。

目录

第 1 章：取余、同余和模逆元到底在算什么	3
第 2 章：费马小定理为什么能把大指数变小	4
第 3 章：欧拉函数数什么，欧拉定理为什么成立	6
第 4 章：为什么有些幂更早回到1	8
第 5 章：原根为什么可以给所有非零余数编号	10
第 6 章：中国剩余定理怎样把两个余数合起来	12
第 7 章：RSA为什么能把消息还原回来	13
第 8 章：知道私钥后，为什么平方能帮我们分解	15
第 9 章：成功概率的问题，具体在数哪些底数	18
第 10 章：取幂以后为什么还均匀，怎样数到达次数	21
第 11 章：为什么一串概率求和，仍然不超过一半	25
第 12 章：失败后重试，以及这到底说明RSA什么	28
第 13 章：补充证明：逆元、唯一分解与CRT	30
第 14 章：补充证明：质数为什么一定有原根	39
第 15 章：补充证明：群、阶与欧拉函数计数	43
第 16 章：补充：精确概率、统一指数与运行时间	50
第 17 章：辨清几个计数问题，再用练习回查	53
第 18 章：从原问题回到笔记，以及怎样分享	57

第 1 章：取余、同余和模逆元到底在算什么

[返回目录](#)

1.1 先读懂一个式子

看这个式子：

$$17 \equiv 2 \pmod{5}.$$

它说的是：17除以5余2，2除以5也余2。把两个数相减， $17 - 2 = 15$ ，恰好是5的倍数。

所以一般写成

$$a \equiv b \pmod{n},$$

就是“ a 和 b 除以 n 有相同余数”，等价于“ n 整除 $a - b$ ”。记号 $n \mid (a - b)$ 也是这句话。这里的模数 n 取正整数。

以后我们只关心模5的余数时，就可以把17换成2。数本身变了，关心的余数没有变。

1.2 为什么能先取余，再做乘法

假设要算 17×23 除以5的余数。17余2，23余3，先算 $2 \times 3 = 6$ ，再取余得1。直接算391，也余1。

原因是 $17 = 5 \times 3 + 2$ 、 $23 = 5 \times 4 + 3$ 。把乘积展开，除了 2×3 ，其他项都含因子5，取余时消失了。

加法同理，连续乘很多次也同理。因此算幂时，可以每乘一次就把结果缩成余数。这是后面所有幂表和快速幂的依据。

1.3 能乘，能不能直接除

先看失败的例子：

$$2 \times 1 \equiv 2 \times 4 \pmod{6}.$$

两边都余2，但1与4模6不同余。这里不能直接约掉2，因为2与6有公因子。

再看模5。 $2 \times 3 = 6 \equiv 1 \pmod{5}$ ，所以如果 $2x \equiv 3 \pmod{5}$ ，两边乘3，就得到 $x \equiv 9 \equiv 4 \pmod{5}$ 。

这个3叫作2的**模5逆元**：它负责把乘2“乘回去”。它不是通常分数中的 $1/2$ 。

什么时候有逆元？恰好在底数与模数**互质**时。互质就是说最大公约数为1，写作 $\gcd(a, n) = 1$ 。例如2与5互质，2与6不互质。

为什么互质就够？裴蜀等式说，这时有整数 u, v 使 $au + nv = 1$ 。模 n 后， nv 消失，剩下 $au \equiv 1$ ，所以 u 就是逆元。这个基础结论的证明放在第13章；主线先记住它解决的是“什么时候能约掉一个因子”。

以后看到证明中“约掉 a ”，先检查 a 与模数是否互质。模质数 p 时，只要 a 不是 p 的倍数，就满足这个条件。

第 2 章：费马小定理为什么能把大指数变小

[返回目录](#)

2.1 先看看3的幂发生了什么

算3的幂，每一步都模7：

指数	1	2	3	4	5	6
余数	3	2	6	4	5	1

第6次乘回到1。因此再乘6次，又会回到原来的余数。比如 $100 = 6 \times 16 + 4$ ，所以

$$3^{100} \equiv (3^6)^{16} 3^4 \equiv 1^{16} \times 4 = 4 \pmod{7}.$$

这里没有计算 3^{100} 这个大整数，只计算了一个循环中的位置。

2.2 定理究竟保证了什么

把7换成任意质数 p ，把3换成不是 p 的倍数的整数 a ，费马小定理保证：

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

“质数”与“不是它的倍数”都是条件。若 $a = 7$ ，模7的正整数次幂全是0，就不可能等于1。

还有一种对任意整数 a 都成立的写法：

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

若 p 不整除 a ，在前一式两边乘 a 即可；若 p 整除 a ，这一式两边都余0。两种写法的适用范围由此看清楚了。

2.3 为什么一定能回到1：先看“乘3只是换了顺序”

把模7的六个非零余数全部乘3：

原来的余数	1	2	3	4	5	6
乘3后模7	3	6	2	5	1	4

下面一行仍是1到6，每个数出现一次，只是顺序换了。

为什么没有两个位置撞到一起？若 $3x \equiv 3y \pmod{7}$ ，因为3可约掉，就有 $x \equiv y$ ；而 x, y 都在1到6之间，这就要求 $x = y$ 。为什么没有0？若 $3x$ 模7为0，约掉3后 x 也该为0，与范围矛盾。

现在把下面一行的六个数相乘。它们只是上面一行的重排，所以乘积模7相同：

$$3^6(1 \times 2 \times 3 \times 4 \times 5 \times 6) \equiv 1 \times 2 \times 3 \times 4 \times 5 \times 6 \pmod{7}.$$

括号中的乘积与7互质，可以约掉，于是 $3^6 \equiv 1$ 。

一般的证明完全照这个过程做：把 $1, 2, \dots, p-1$ 乘 a ，用逆元证明没有重复、没有0，再把全部数相乘并约掉原乘积，就得到 $a^{p-1} \equiv 1$ 。对于 $p=2$ ，列表只有1，也一样成立。

2.4 它能怎么用，又不能怎么用

除了缩小指数，还能证明整除。比如 $a^7 \equiv a \pmod{7}$ ，就是 $7 \mid (a^7 - a)$ 。

也能找逆元：对 $p \nmid a$ ， $a \cdot a^{p-2} \equiv 1$ ，所以 a^{p-2} 是 a 的模 p 逆元。例如模5时， $2^3 = 8 \equiv 3$ ，与第1章算出的逆元一致。

但是，满足类似的幂同余，不能反过来保证模数是质数。比如 $2^4 \equiv 1 \pmod{15}$ ，15仍然是合数。做素性判断时，必要条件与充分条件要分开。

即使恰好用了“模数减1”的指数，也会有反例： $341 = 11 \times 31$ ，而 $2^{10} = 1024 \equiv 1 \pmod{341}$ ，所以 $2^{340} \equiv 1 \pmod{341}$ 。一次底数检验通过，仍不足以保证质数。

第 3 章：欧拉函数数什么，欧拉定理为什么成立

[返回目录](#)

3.1 你要找的欧拉公式，先从12开始数

在1到12中，与12互质的是

1, 5, 7, 11.

一共有4个。欧拉函数 $\varphi(12) = 4$ ，就是记录这个数量。它没有在数“小于12的质数”或者“12有几个质因子”。例如1不是质数，却被算进来了；2是质数，却与12不互质。

约定 $\varphi(1) = 1$ 。对 $n > 1$ ，数1到 n 或者数1到 $n - 1$ 结果一样，因为 n 本身不与 n 互质。

3.2 为什么公式里会出现乘积

12的不同质因子是2和3。不与12互质，就是被2或者3整除。在1到12中：

- 2的倍数有6个，要去掉；
- 3的倍数有4个，也要去掉；
- 6的倍数有2个，被去掉了两次，要补回来一次。

所以 $\varphi(12) = 12 - 6 - 4 + 2 = 4$ 。把共同因子12提出：

$$\varphi(12) = 12 \left(1 - \frac{1}{2} - \frac{1}{3} + \frac{1}{6} \right) = 12 \left(1 - \frac{1}{2} \right) \left(1 - \frac{1}{3} \right).$$

这就是乘积公式的来源。每个不同质因子只贡献一次“去掉它的倍数”，它在 n 里出现几次不改变排除条件。

于是，若 n 的不同质因子是 $p_1, \dots, p_k$ ，有

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

多于两个质因子时，也按“减单项、加两项交集、减三项交集……”处理。乘积展开恰好有同样的正负号。为什么每个该排除的整数最终恰好排除一次，见第13章的容斥补充。

例如 $360 = 2^3 \times 3^2 \times 5$ ，所以 $\varphi(360) = 360 \times \frac{1}{2} \times \frac{2}{3} \times \frac{4}{5} = 96$ 。质数 p 只有一个质因子，得到 $\varphi(p) = p - 1$ 。

3.3 模数换成合数，费马的思路还能用吗

模10时，有逆元的余数是1, 3, 7, 9。把它们全部乘3：

原来的余数	1	3	7	9
乘3后模10	3	9	1	7

又是同一批数的重排。把两行分别相乘，约掉 $1 \times 3 \times 7 \times 9$ ，就得到 $3^4 \equiv 1 \pmod{10}$ 。

一般地，只要 $\gcd(a, n) = 1$ ，乘 a 就能在所有与 n 互质的余数之间重新排列：没有重复，因为 a 可约；输出也互质，因为 a 和输入都有逆元，它们乘积也有逆元。列表中每个数都可约掉，得到

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

这就是欧拉定理。 n 为质数时， $\varphi(n) = n - 1$ ，它就变回费马小定理。

3.4 为什么仍要检查互质

模10时， 2^4 余6，不余1。2没有进入刚才的互质列表，排列证明根本没有覆盖它。

使用方法是：先检查底数与模数互质，再把指数按 $\varphi(n)$ 缩减。例如 3^{100} 模10，100是4的倍数，所以余1。

但 $\varphi(n)$ 只是一个保证可用的循环长度，可能比实际需要的长。这引出下一个问题。

第 4 章：为什么有些幂更早回到1

[返回目录](#)

4.1 欧拉给了6，实际可能只需要3

模7时，2的幂为

$$2, 4, 1, 2, 4, 1, \dots$$

费马保证 $2^6 \equiv 1$ ，而它在第3次已经回到1了。

第一次回到1所需的正指数，叫作这个底数的乘法阶。记为 $\text{ord}_7(2) = 3$ 。同一模数下，底数不同，阶可以不同：模7的3的阶是6。

阶只对与模数互质的底数这样定义。欧拉定理保证至少有一次回到1，所以能在所有这样的正指数中取最小值。

4.2 为什么其他“回到1”的指数都是阶的倍数

2模7每3步回到1，因此第6、9、12步都会回到1。反过来，也没有别的正指数能做到。

设某个指数 k 也使 $2^k \equiv 1$ 。把 k 除以3，写成 $k = 3q + r$ ，其中 r 只能是0、1、2。于是 2^k 的余数与 2^r 相同。若 $r = 1$ 或2，余数分别为2、4，不能是1，所以只能 $r = 0$ 。

一般地，把阶记作 d ，同样作除法 $k = qd + r$ ， $0 \leq r < d$ 。若 $a^k \equiv 1$ ，便有 $a^r \equiv 1$ 。若 $r > 0$ ，这会比 d 更早回到1，违背 d 的定义。因此 $r = 0$ ，即 $d \mid k$ 。

所以

$$a^k \equiv 1 \pmod{n} \iff d \mid k \quad (k \geq 0).$$

取 $k = \varphi(n)$ ，得到 $d \mid \varphi(n)$ 。这就是为什么阶必须整除欧拉函数。

4.3 为什么可以对指数取模，幂的值却还是模原来的数

刚才2的阶是3，因此 2^{100} 模7只需看指数100除以3的余数：100余1，所以答案为2。

有两个不同的问题：

- **指数除以3取余**：找它位于循环的第几格；
- **幂的值除以7取余**：求这格里的数。

循环的长度是3，格子里的数却是模7的余数。不能因为指数改成模3，就把幂的值也改成模3。这一点在概率证明中还会再遇到。

4.4 如何找一个底数的阶

先算一个保证回到1的指数，比如 $\varphi(n)$ 。真实的阶必须是它的因子，所以只需检查这些因子。

模7时候选为1、2、3、6。对3检查： 3^1 余3、 3^2 余2、 3^3 余6，都不是1； 3^6 余1，所以阶是6。对2检查到3，就能找到阶3。

关于“一个幂的阶怎样由原来的阶算出”“两个阶互质时，为什么乘积的阶等于两者乘积”，详证放在第14章。先把“阶是第一次回到1的步数”这个意思建立起来。

第 5 章：原根为什么可以给所有非零余数编号

[返回目录](#)

5.1 3与2的区别，不只是回来的时间不同

模7时，3走过的余数是

1, 3, 2, 6, 4, 5,

下一次回到1。这六个数把所有非零余数走了一遍，没有漏掉任何一个。

2走过的却只有1, 2, 4，随后就回到1，没有走到3、5、6。

我们把像3这样能用连续的幂走遍所有互质余数的底数，叫作**原根**。因为互质余数有 $\varphi(n)$ 个，所以它的阶恰好是 $\varphi(n)$ 。

5.2 有了原根，能多做什么

仍取模7的原根3：

编号，也就是指数	0	1	2	3	4	5
对应余数	1	3	2	6	4	5

每个非零余数现在有一个唯一编号。例如余数5的编号是5，余数2的编号是2。

这是后面概率证明需要原根的原因：**均匀选一个余数，等价于均匀选一个编号**。因为两行一一对应，并且没有重复，每个编号的概率都相同。

理论证明中可以利用这样的编号；实际分解算法只算幂和最大公约数，不需要把编号求出来。

5.3 每个质数都有原根吗

有。模每个质数 p ，都能找到走遍 $p - 1$ 个非零余数的底数。证明要用“非零多项式的根数不超过次数”和关于阶的两个小结论；放在第14章单独展开。

第一次顺着主线读时，可以先使用这个已经明确标出的定理，继续看它怎样帮助数概率；想核查它为什么成立，再回读证明。

合数模数却不一定有原根。例如模8的互质余数是1, 3, 5, 7，而 $3^2, 5^2, 7^2$ 模8都为1。任何底数最多走两格，走不遍四个数。

5.4 原根有多少个

模7的原根有两个：3和5。用3给余数编号后，5就是 3^5 。它每次在六格循环中向前跳5格，仍能走遍六格。

为什么跳2格就不行？它只访问编号0、2、4，再回到0；跳3格只访问0、3。

一般说，长为 N 的循环，每次跳 k 格，能走遍全循环恰好要求 k 与 N 互质。因此若有原根，原根总数就是 $\varphi(\varphi(n))$ 。模质数 p 时，是 $\varphi(p - 1)$ 。第14—15章给出阶公式与计数证明。

第 6 章：中国剩余定理怎样把两个余数合起来

[返回目录](#)

6.1 先解一个真的问题

要找一个数 x ，同时满足

$$x \equiv 2 \pmod{3}, \quad x \equiv 3 \pmod{5}.$$

满足第一个条件的数是2, 5, 8, 11, 14, ...。检查模5的余数，第一个合适的是8。

加15不会改变模3和模5的余数，所以8, 23, 38, ...也都合适。事实上所有整数解恰好是 $x = 8 + 15t$ ，其中 t 是任意整数。

6.2 为什么只有一个模15的答案

如果 x, y 都合适，那么 $x - y$ 既被3整除，也被5整除。3与5互质，所以 $x - y$ 被15整除。

因此两个答案只能相差15的倍数。这里的“唯一”，指的是模15的余数唯一，并不是说世界上只有一个整数解。

这也是RSA里反复用的步骤：模 p 一样、模 q 也一样，而且 p, q 是不同质数，就能说模 pq 一样。

6.3 怎样构造答案，不靠一个个试

找两个数，让它们分别只负责一个条件：

- 10模3余1、模5余0，负责第一个余数；
- 6模3余0、模5余1，负责第二个余数。

所以 $2 \times 10 + 3 \times 6 = 38$ ，模3余2、模5余3。再模15取余，得到8。

10怎么来的？5模3有逆元2，所以 5×2 模3为1，同时仍是5的倍数。6同理，是 3×2 。

对于互质的模数 m, n ，同样能用逆元构造“模 m 余1、模 n 余0”的数和另一个相反的数，再按所需余数加权相加。这证明了解存在；上一节的差值论证证明了唯一性。多个两两互质模数的完整公式在第13章。

6.4 模数不互质，为什么有时没解

若要求 x 模4余1，同时模6余2，就没有解。第一个要求 x 是奇数，第二个要求它是偶数，两个条件矛盾。

若模4余1、模6余3，则两个条件都要求奇数，确实有解：9。此时重复的周期是12，即4与6的最小公倍数，不是24。

一般的条件是：余数之差必须被模数的最大公约数整除。对于两个模数，写作

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

有解时，答案按 $\text{lcm}(m, n)$ 重复。多个模数则检查每一对这个条件。为什么两两相容就足够、如何实际合并，完整证明留在第13章，避免现在打断RSA主线。

第 7 章：RSA为什么能把消息还原回来

[返回目录](#)

7.1 先把每个数的用途说清楚

取两个不同质数5和11，相乘得到 $n = 55$ 。在这个例子中， $\varphi(55) = 4 \times 10 = 40$ 。

接着选加密指数 $e = 3$ 。它与40互质，所以在模40下有逆元。取 $d = 27$ ，因为

$$3 \times 27 = 81 = 1 + 2 \times 40.$$

这里逆元的模数是40，不是55：我们要安排的是两个指数相乘后，比1多出一个欧拉指数的倍数。

消息 m 取0到54之间的整数，加密是 $c \equiv m^3 \pmod{55}$ ，解密是 $c^{27} \pmod{55}$ 。两步合起来，计算的是 m^{81} 模55。

公钥是 $(55, 3)$ ，私钥指数是27。这些很小的数只用来手算和理解证明。

7.2 对互质消息，欧拉定理怎样接上来

若 m 与55互质，欧拉定理给出 $m^{40} \equiv 1$ 。因此

$$m^{81} = m(m^{40})^2 \equiv m \pmod{55}.$$

于是解密恢复原消息。例如 $m = 2$ 加密得到8，而 8^{27} 模55为2。

一般地， $n = pq$ ，选 e 与 $\varphi(n)$ 互质，再用逆元得到 d ，使 $ed = 1 + k\varphi(n)$ 。对互质消息，有 $m^{ed} = m(m^{\varphi(n)})^k \equiv m$ 。

所以所需的指数不是随意假设出来的：先选互质的 e ，再求它的逆元 d 。例如 $\varphi(n) > 2$ 时， $e = d = \varphi(n) - 1$ 就给出一组形式上的逆元；这里只用它说明存在性，具体例子仍用 $e = 3, d = 27$ 。

7.3 消息不互质怎么办：把问题拆成两个质数

例如 $m = 5$ 与55不互质，不能直接使用模55的欧拉定理。但模5时，5的任何正整数次幂都余0，已经与原消息一致。

模11时，5不是11的倍数，费马小定理给 $5^{10} \equiv 1$ ；而 $81 = 1 + 8 \times 10$ ，所以 $5^{81} \equiv 5$ 。

两个质数下都对了，用中国剩余定理合起来，就有 $5^{81} \equiv 5 \pmod{55}$ 。实际加密 5^3 余15，解密 15^{27} 余5。

任意消息都按这个办法证明：固定质数 p ，若 $p \mid m$ ，两边都是0；若 $p \nmid m$ ，用费马小定理，因为 $p - 1 \mid ed - 1$ 。模 q 同理，最后合并。因此包括0、质因子的倍数在内，每个消息代表都能还原。

7.4 这为什么说明分解有用

如果知道55的因子5和11，就能算出40，再从公开的指数3求出私钥27。

一般地，知道 p, q 就能算 $\varphi(n) = (p - 1)(q - 1)$ ，从而求私钥。这证明了“能分解，就能求私钥并解密”。它还没有证明任何能解某个密文的办法都必须先分解。这个逻辑问题在第12章单独讨论。

第 8 章：知道私钥后，为什么平方能帮我们分解

[返回目录](#)

8.1 先看一个奇怪的数：34

不知道55的因子，能不能从某个算出的数找到它们？先看

$$34^2 = 1156 \equiv 1 \pmod{55}.$$

34不是1，也不是-1模55的代表54，却平方后变成1。这个现象比“回到1”本身更有用。

平方为1意味着 $55 \mid (34 - 1)(34 + 1)$ 。而 $34 - 1 = 33$ 、 $34 + 1 = 35$ 。与55分别求最大公约数：

$$\gcd(33, 55) = 11, \quad \gcd(35, 55) = 5.$$

因子就被分开了。算法想找到的，正是34这样的数。

8.2 为什么1和54没有这个效果

若 $x = 1$ ， $x - 1 = 0$ ，最大公约数是整个55，没拆开。若 $x = 54$ ，它就是模55的-1，则 $x + 1 = 55$ ，也没有拆开。

所以要找的是：平方后变成1，但自己既不是1也不是-1的余数。这叫作1的非平凡平方根。“非平凡”在这里就指排除这两个显而易见的根。

为什么它一定能拆开 $n = pq$? 模质数 p 时, $x^2 \equiv 1$ 意味着 $p \mid (x - 1)(x + 1)$, 所以 p 至少整除其中一项, 得到 $x \equiv 1$ 或者 -1 。模 q 也一样。

模 p	模 q	合起来的情况
1	1	模 n 为1
-1	-1	模 n 为-1
1	-1	两边符号不同, 可以分解
-1	1	两边符号不同, 可以分解

在最后两种情况中, 一个质因子进了 $x - 1$, 另一个进了 $x + 1$ 。因 p, q 是奇质数, 同一个质因子不能同时整除相差2的这两项。求最大公约数就恰好挑出其中一个因子。

这也说明后面的分解论证限定为**两个不同奇质数的乘积**。

8.3 私钥怎样让我们找到34

继续用 $n = 55, e = 3, d = 27$ 。先计算

$$ed - 1 = 80 = 2^4 \times 5.$$

把所有因子2拿出来, 剩下的5是奇数。任选与55互质的底数 a , 已知 $a^{80} \equiv 1$ 。与其一步算到80, 我们先算 a^5 , 再不断平方。

选 $a = 2$:

从哪里算起	指数	模55的余数
初始项	5	32
平方一次	10	34

从哪里算起	指数	模55的余数
平方两次	20	1

看到第一次出现1，就回看紧前一项34。它平方为1，又不是1或54，所以成功。

整个过程只用到了公开的55、3和已知的27。5和11只在证明及验算时使用，算法计算时不用先知道它们。

8.4 也会失败吗

会。取 $a = 1$ ，初始项已经是1，没有找到前面那个有用的数。取 $a = 54$ ，初始项是54，一平方就到1，但前一项只是 -1 ，也没有用。

所以这是一种随机尝试：有些底数成功，有些失败。下一章才讨论成功与失败怎样数。

8.5 把刚才的计算写成完整算法

令 $K = ed - 1 > 0$ ，把它写成 $K = 2^s r$ ，其中 r 为奇数。先使用原对话的条件 $\varphi(n) \mid K$ ；它保证任何互质底数都有 $a^K \equiv 1$ 。第16章说明条件还可以放宽。

1. 在 $1, 2, \dots, n-1$ 中均匀选 a ，先算 $g = \gcd(a, n)$ 。若 $g > 1$ ，因 $a < n$ ，已直接找到真因子 g ，输出 $g, n/g$ 。
2. 若 $g = 1$ ，算 $x \equiv a^r \pmod{n}$ ，取0到 $n-1$ 的余数。若 $x = 1$ ，这次失败，重新选底数。
3. 最多平方 s 次。每次令 $y \equiv x^2 \pmod{n}$ 。若 $y \neq 1$ ，用 y 替换 x 继续；若 $y = 1$ ，检查 x 。若 $x = n-1$ ，失败；否则输出 $\gcd(x-1, n)$ 和另一个因子。

为什么最后一个分支的 x 也不会是1？初始1已被排除，而过程中一出现1就结束。因此该分支确实找到非平凡平方根。

为什么不会一直平方不到1？第 s 次得到 $a^{2^s r} = a^K \equiv 1$ ，所以合法输入下必定到达。停止时输出的因子可以用乘法核验。

第 9 章：成功概率的问题，具体在数哪些底数

[返回目录](#)

9.1 先别急着写概率公式

模55时，先只看与55互质的底数。它们共有 $\varphi(55) = 40$ 个。如果每个等可能被选中，成功概率就是“成功的底数个数除以40”。

我们在研究一次随机选底数。选定底数以后，取幂和平方都由它确定，不再额外掷一次骰子。

第8章说明，算法成功取决于“第一次平方到1之前，出现的是34那样的数，还是54那样的数”。怎样不用逐个计算大幂，就描述这个区别？把模55拆成模5和模11来看。

9.2 同一个计算，在两个质数下到1的时间可能不同

取刚才的 $a = 2$ ，初始项是 2^5 。模5和模11分别算：

已经平方几次	模5的余数	模11的余数	模55的余数
0，尚未平方	2	10	32
1	4	1	34
2	1	1	1

模11先到1，模5晚一步到1。因此在中间那一行，一边是1，另一边是 -1 ，正好给出非平凡平方根34。

我们给这两个“第一次到1的时间”取名字： T_p 是模 p 到1时已平方的次数， T_q 是模 q 的次数。在这个例子中 $p = 5, q = 11$ ，所以 $T_p = 2, T_q = 1$ 。

初始项就为1时，次数记为0。两个次数都由随机选出的 a 决定，所以它们是随机变量。这个词在这里只表示“选不同底数，得到的次数可能不同”。

9.3 为什么到达时间不同就成功

假设模 q 到1较晚。在它刚要到1的那一步，模 p 早已是1；模 q 前一项还不是1，但它的平方是1，所以前一项只能是 -1 。

因此两个模数下的前一项是 $(1, -1)$ 。它就是第8章说的可分解情况。模 p 较晚时，情况相反，得到 $(-1, 1)$ 。

若两边同时首次到1，且次数大于0，那么前一步两边都还不是1，只能同时为 -1 ；合起来就是模 n 的 -1 ，算法失败。若次数都是0，初始项就为1，也失败。

于是，对互质底数，

成功 $\iff T_p \neq T_q$.

四个平方根中两个有用，并不能直接说“概率一半”：算法产生这四个根的机会未必相同。我们真正要数的是到达时间相同的底数有多少。

9.4 对模55，可以直接把40个底数分组

模5的初始项是 a^5 。指数5模4余1，所以初始余数与 a 模5相同：

a 模5	初始项	第一次到1的次数 T_p
1	1	0
4	4	1
2或3	2或3	2

所以四个等可能余数中，次数0占一个、次数1占一个、次数2占两个，概率为 $1/4, 1/4, 1/2$ 。

模11时，初始项 a^5 只能为1或 -1 。把十个非零余数都计算一次：

初始项 $a^5 \bmod 11$	对应 $a \bmod 11$	T_q
1	1、3、4、5、9	0
10, 也就是-1	2、6、7、8、10	1

所以 T_q 取0、1各有一半概率。注意：不是说所有“到达次数”都一样可能；模5的次数2就比次数0多一倍。

9.5 同一个底数的两边，为什么可以独立

把模5的四种非零余数放成四行，模11的十种非零余数放成十列，一共有40个格子。

中国剩余定理保证，每个格子都对应唯一一个模55的互质余数。所以均匀选40个底数，等价于均匀选这40个格子。

已知选中了哪一行，并不会偏向这一行中的哪一列：十列仍各有一格，仍然各占 $1/10$ 。这就是此处的独立性。

例如 $T_p = 0$ 对应一行， $T_q = 0$ 对应五列，两者同时发生有 $1 \times 5 = 5$ 个格子，占 $5/40 = 1/8$ 。 $T_p = 1, T_q = 1$ 也有5格；没有 $T_q = 2$ 的列。因此失败底数是 $5 + 5 = 10$ 个，成功底数30个。

$$P(\text{失败}) = \frac{10}{40} = \frac{1}{4}, \quad P(\text{成功}) = \frac{30}{40} = \frac{3}{4}.$$

“两个变量来自同一个底数”本身不保证独立。这里能独立，是因为均匀底数经CRT对应到一个完整、均匀的行列格子表。

9.6 现在缺哪一步一般证明

模55我们已经数清楚了。但对于别的两个奇质数，不能每次都列完所有底数。

接下来只补两件事：第一，取幂后各个到达次数的概率怎样一般地算；第二，知道每个次数的概率都不超过一半，怎样推出“到达时间相同”的总概率也不超过一半。

第10章处理第一件，第11章处理第二件。先不需要学习抽象群的全部定义。

第 10 章：取幂以后为什么还均匀，怎样数到达次数

[返回目录](#)

10.1 先承认：均匀输入不总有均匀输出

均匀从1、2、3中选一个数，再问“是不是奇数”，回答“是”的概率为 $\frac{2}{3}$ ，“否”为 $\frac{1}{3}$ 。输入的三个数等可能，输出的两种回答却不等可能。

所以“底数均匀”还不能直接推出“取幂后的结果均匀”。要检查：每种可能输出由多少个输入产生。数量相等，才会等可能。

10.2 用模13的例子，把输入和输出全部列清楚

模13的原根2把十二个非零余数写成 2^k ，其中 $k = 0, 1, \dots, 11$ 。均匀选底数，就等价于均匀选这十二个编号。

现在取奇数次幂 $r = 9$ 。因为 $9 = 3 \times 3$ ，令 $h = 2^3 = 8$ ，就有

$$a^9 = (2^k)^9 = 8^{3k} \pmod{13}.$$

8的幂依次是1, 8, 12, 5，随后又回到1，所以它的阶是4。算 8^{3k} 时，只需知道 $3k$ 在四格循环中的位置。

k 除以4的余数	十二个编号中对应的 k	$3k$ 除以4的余数	8^{3k} 模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

四种输出各有三个输入，所以每种概率都是 $3/12 = 1/4$ 。

这个表分成两步：先把十二个编号分成四组，每组恰好三个；再乘3，因3与4互质，只把四组的顺序换了。等大小分组，加上重新排列，说明这里取幂后的结果确实均匀。

10.3 为什么指数取模4，值却取模13

4是8的循环长度，13是计算幂的余数所用的模数。

比如 8^{11} ：指数11除以4余3，所以去找循环的第3号位置，得到 $8^3 \equiv 5 \pmod{13}$ 。这里最终答案是模13的余数5，完全没有把幂的值改成模4。

如果表中的乘3换成乘2，四种指数余数就只能变成0或2，输出不再覆盖四个位置。后面一般证明要求那个乘数为奇数，正是为了使它与2的幂互质。

10.4 一般情况为什么也是这两个步骤

设 p 是奇质数，把 $p - 1$ 中的所有因子2拿出来，写成

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

例如 $p = 13$ 时， $12 = 2^2 \times 3$ ，所以 $\alpha = 2, u = 3$ 。

算法使用的奇数 r 满足 $u \mid r$ 。这是因为 $p - 1$ 整除 $K = 2^s r$ ，而 u 是奇数，所有奇数因子都得留在 r 里。于是 $r = uw$ ， w 也是奇数。

取一个原根 g 。它的循环长为 $p - 1$ ，均匀底数写作 $a = g^k$ ，编号 k 均匀遍历 $0, \dots, 2^\alpha u - 1$ 。令 $h = g^u$ ，就是每次在原根的大循环中跳 u 格；走 2^α 步才回到1，所以 h 的阶是 2^α 。

取幂后，

$$a^r = h^{kw} \pmod{p}.$$

先把编号 k 按 2^α 取余，每种余数有恰好 u 个编号，所以仍均匀。再乘奇数 w ，它与 2^α 互质，只重新排列这些余数。所以输出均匀遍历

$$1, h, h^2, \dots, h^{2^\alpha-1}.$$

这是一批大小为 2^α 的余数。主线先用“幂组成的循环”理解它；群论语言把它称为一个循环子群，详细说明见第15章。

10.5 从均匀余数到到达时间，还要再数一次

回到模13的四个等可能结果：

初始项	继续平方时的变化	首次到1的次数
1	已经是1	0
12	12 → 1	1
8	8 → 12 → 1	2
5	5 → 12 → 1	2

次数0有一个结果，次数1有一个，次数2有两个。因此概率又是 $1/4, 1/4, 1/2$ 。

为什么这里的次数恰好是阶里的2的次数？初始项若阶为 2^t ，平方 j 次相当于取 2^j 次幂。第4章说，这个幂等于1恰好要求 $2^t \mid 2^j$ ，也就是 $j \geq t$ 。所以第一次到1在 $j = t$ 。

10.6 长为8的循环，次数为什么是“一个、一个、两个、四个”

想象某个余数 h 的阶是8。先算 h^k 的阶：要使它的 m 次幂等于1，就是要求 $8 \mid km$ 。

编号 k	0	1	2	3	4	5	6	7
h^k 的阶	1	8	4	8	2	8	4	8

编号 k	0	1	2	3	4	5	6	7
首次到1的次数	0	3	2	3	1	3	2	3

次数0有一个，次数1有一个，次数2有两个，次数3有四个。它们占比分别为 $1/8, 1/8, 1/4, 1/2$ 。

一般长度为 2^α 时，阶为1的只有单位元1；阶为 2^t 的有 2^{t-1} 个， $1 \leq t \leq \alpha$ 。为什么是这个数？

要让 h^k 的阶恰好为 2^t ，编号必须写成 $k = 2^{\alpha-t}j$ ，其中 j 在 $0, \dots, 2^t - 1$ 里是奇数。否则 j 再多含一个因子2，就会更早回到1。这段编号中恰好一半为奇数，即 2^{t-1} 个。阶为1的边界对应 $k = 0$ ，单独计数。

所以一般分布为

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

这些数量加起来是 $1 + 1 + 2 + \dots + 2^{\alpha-1} = 2^\alpha$ ，没有漏掉任何输出。最大的一组占一半，所以每个到达次数的概率都不超过一半。模 q 的证明相同，只需把 α 换成 $q - 1$ 中因子2的次数。

更一般的“阶为 d 的元素有 $\varphi(d)$ 个”，就是把这里“编号必须为奇数”换成“编号必须与 d 互质”；详证放在第15章。

第 11 章：为什么一串概率求和，仍然不超过一半

[返回目录](#)

11.1 先只解决你最后问的那个疑问

我们已经知道： T_q 取每个具体值的概率都不超过一半。可它有几个可能值，难道把几个“一半”加起来还能不超过一半？

先把问题说成一句话：**先看 T_p 产生了什么结果，再问 T_q 能否恰好匹配它。**两者独立，因此知道 T_p 的结果，不改变 T_q 原来的分布。无论 T_p 产生什么，匹配它的概率都不超过一半。

最后把各种 T_p 的情况按出现比例合起来，就是对这些匹配概率取平均。参与平均的数都不超过一半，平均也不超过一半。

下面用模55的分布把“按比例合起来”算出来。

11.2 想象按模5的到达次数分成三堆

第9章得到的分布为：

次数	模5的出现比例	模11的匹配比例
0	1/4	1/2
1	1/4	1/2
2	1/2	0

为了看清比例，想象有100份等权重的情况： $T_p = 0$ 占25份， $T_p = 1$ 占25份， $T_p = 2$ 占50份。这是把概率按100份表达，并不是声称实际随机做100次一定出现这些数量。

在第一堆里，匹配成功的比例是1/2；第二堆也是1/2；第三堆是0。所以所有情况中，匹配的比例为

$$\frac{25}{100} \times \frac{1}{2} + \frac{25}{100} \times \frac{1}{2} + \frac{50}{100} \times 0 = \frac{1}{4}.$$

乘前面的 $25/100$ ，就是在提醒：这一堆只占全部情况的四分之一。不能把这一堆内部的一半，当成全部情况的一半。

11.3 只知道上界，也能算出总上界

现在不用 T_q 的精确分布，只知道三种匹配概率都不超过 $1/2$ 。把第三堆的0也换成更宽的上界 $1/2$ ，得到

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

三个权重 $1/4, 1/4, 1/2$ 加起来是1，所以右边为

$$\left(\frac{1}{4} + \frac{1}{4} + \frac{1}{2} \right) \times \frac{1}{2} = \frac{1}{2}.$$

实际概率是 $1/4$ ，通用上界是 $1/2$ ；两者可以同时成立。上界只是说“再大也不会超过这里”，没有说实际值必须等于它。

11.4 把这个已经看懂的过程写成一般式子

相等可以发生在0、1、2等不同值上。不同值的相等情况互不重叠，因此把它们加起来。

独立性允许把“两个都取 t ”的概率写成乘积：

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

求和号 $\sum_t$ 只是“对所有可能的 t 重复这项加法”。令 $a_t = P(T_p = t)$ 作为权重，令 $b_t = P(T_q = t)$ 作为每堆内的匹配概率。每项都满足 $b_t \leq 1/2$ ，且权重非负、总和为1。所以

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

每一行都在做前面那个三堆例子的同一件事。关键是权重总和为1。如果真的是直接相加三个 $1/2$ ，当然会得到 $3/2$ ，那就不是这里的计算了。

11.5 独立性不能省：否则“每堆内匹配概率”会改变

让 X 等可能取0或1，再直接令 $Y = X$ 。 Y 取每个值的概率确实都是 $1/2$ ，但它与 X 总相等，相等概率为1。

原因是：一旦知道 $X = 0$ ， Y 必为0，匹配概率变成1，而不是原来的 $1/2$ 。这一例子中不能把联合概率拆成乘积。

回到RSA，独立性来自第9章的完整行列格子表。一般 p, q 下，表有 $p - 1$ 行、 $q - 1$ 列，每个格子对应一个互质底数，均匀抽样后，各行列独立。 T_p 只读行， T_q 只读列，分别对行列作计算也不改变这种独立性：任意选定的行组与列组，其格子数仍是两组大小的乘积。

11.6 至少一半的成功率，终于接出来了

第9章证明：对互质底数，失败恰好是 $T_p = T_q$ 。因此

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

这句话的完整前提是：两个不同奇质数的乘积；正的指数 K 保证所有互质底数的 K 次幂为1；从全部互质底数均匀抽样。原对话的 $K = ed - 1$ 且 $\varphi(n) \mid K$ 满足这些要求。

若按第8章从 $1, \dots, n - 1$ 全部候选抽样，不互质的底数直接给因子，剩余互质底数的条件分布仍均匀。因此全部候选下的成功率也至少一半。

对55，40个互质底数中30个成功，另外14个非互质底数都直接成功，所以全部54个候选中44个成功，概率为 $44/54 = 22/27$ 。它与 $3/4$ 对应不同的抽样范围。

读到这里，通用下界的证明已经完成。精确概率的长公式放在第16章，不需要用它才能理解“至少一半”。

第 12 章：失败后重试，以及这到底说明RSA什么

[返回目录](#)

12.1 一次失败不推翻算法

算法允许选到1或-1这样的失败底数。失败后重新独立选一个底数，才是一轮新的尝试。

单次失败概率至多 $1/2$ ，独立重复两次都失败，概率至多 $1/4$ ；三次至多 $1/8$ ； k 次至多 2^{-k} 。

例如20次全部失败的概率至多 $1/1048576$ ，约为百万分之一。它很小，仍不是0。

12.2 平均两次，为什么不是两次一定成功

“期望次数至多2”说的是许多独立运行的平均表现：有的第一次成功，有的要好几次。这不承诺每次都在第二次以内成功。

若每次成功概率为 ρ ，第一次成功恰好第 k 次的概率为 $(1 - \rho)^{k-1}\rho$ 。对于 $\rho = 1/2$ ，平均次数就是

$$1 \times \frac{1}{2} + 2 \times \frac{1}{4} + 3 \times \frac{1}{8} + \cdots = 2.$$

为什么这串和为2？总尝试次数可以看成“第一轮需要做吗、第二轮需要做吗……”的计数。第一轮一定做；第二轮只有首轮失败才做，概率 $1/2$ ；第三轮概率 $1/4$ ；依此类推。平均所做轮数为 $1 + 1/2 + 1/4 + \cdots = 2$ 。一般得到 $1/\rho$ ，所以 $\rho \geq 1/2$ 时至多2。

如果总是重复同一个底数，失败会一直重复，这个概率相乘和平均次数结论就不能照搬。

12.3 “能分解，所以能解密”不能倒过来读

把已经证明的事情分开看：

已知什么	能做什么	本文的位置
模数的两个因子 p, q	算欧拉函数、求私钥并解密	第7章
n 和 $\varphi(n)$	解二次方程找到 p, q	下一节
公钥 n, e 和有效私钥指数 d	用随机算法找到 p, q	第8—11章
只会从某个密文求出原消息	这项能力本身没有给出上述算法需要的 d	不能直接代入前面证明

所以“私钥指数可以帮助分解”与“任何解密办法都必须先分解”不是同一个命题。本文证明了前面的计算关系，没有证明后面的必然性。

假如一个办法能从一般公钥恢复有效的私钥指数 d ，再接上第8章，就得到对应模数的随机分解办法。但某个容易还原的密文，或者仅能求逆的黑箱，并不自动提供 d 。

这一差别可对照 [Handbook of Applied Cryptography 第3章 Fact 3.30](#)与第8章 [Fact 8.6](#)。这些讨论的是数学计算问题；实际RSA还涉及消息编码和填充，本文只解释这里的数论关系。

12.4 为什么知道欧拉函数，也会暴露两个因子

对于 $n = pq$,

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

因此知道 n 与 $\varphi(n)$ ，就知道两个因子的和 $p + q = n - \varphi(n) + 1$ ，同时已知它们的积 $pq = n$ 。

在55的例子中，和为 $55 - 40 + 1 = 16$ ，积为55。两个数就是方程 $x^2 - 16x + 55 = 0$ 的两个根，得到5与11。

一般令 $S = n - \varphi(n) + 1$ ，解得

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

这解释了为什么欧拉函数的信息与分解密切相关。但正如上一节强调的，能够还原一个消息与知道欧拉函数仍是不同的已知信息。

12.5 到这里，可以怎样回读

如果第11章的加权平均已看懂，回头只核查两个来源：第10章为什么每个到达次数概率至多一半，第9章为什么两边独立、为什么不同步就能分解。不要同时背所有公式。

若卡在某个基础定理，再读对应补充：第13章处理逆元、唯一分解和CRT；第14章证明原根存在；第15章证明群中的阶与循环群计数；第16章放精确概率及复杂度；第17章放计数辨析、拓展和练习。这些章节供按疑问回查。

第 13 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章已经给出主线使用方法；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。

13.1 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。

13.2 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。

13.3 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。

13.4 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 $mn \mid A$ 。

13.5 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 $1/3$ 。

13.6 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。

13.7 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。

13.8 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。

13.9 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。

13.10 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。

13.11 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。

13.12 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

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

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。

13.13 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。

13.14 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。

13.15 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。

13.16 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。

13.17 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

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

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 $x_0 = a + mcu$ 。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。

13.18 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。

13.19 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 $x_0 \equiv a_i \pmod{p_j^{f_{ij}}}$ 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。

13.20 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 14 章：补充证明：质数为什么一定有原根

[返回目录](#)

第5章已经用模7说明原根是什么。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。

14.1 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。

14.2 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。

14.3 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。

14.4 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。

14.5 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

14.6 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 15 章：补充证明：群、阶与欧拉函数计数

[返回目录](#)

第10章已经通过八格循环数出了一个、一个、两个、四个。这里把这个计数推广到任意循环长度，并补上“阶整除群阶”的证明。群是用来概括模乘法的语言；先读下面的模乘法例子，再读抽象定义。概率符号的严格定义也放在本章末尾，供回查。

15.1 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 14 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。

15.2 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。

15.3 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。

15.4 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 $k \geq 0$,

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

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。

15.5 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 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。这将直接变成第 11 章的概率分布。

15.6 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。

15.7 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。

15.8 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。

15.9 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 16 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。

16.1 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。

16.2 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

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

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。

16.3 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。

16.4 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 17 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。

17.1 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	$\Omega(n)$	$\Omega(360) = 3 + 2 + 1 = 6$

问题	记号	例子
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。

17.2 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

上限 n	不超过 n 的素数实际个数	$n/\ln n$ (约)
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 $\varepsilon > 0$ ，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。

17.3 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： $16/\gcd(16, 4) = 4$ 。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 18 章：从原问题回到笔记，以及怎样分享

[返回目录](#)

18.1 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13章
4	用过的基础结论还没有证明	第13章
5	两边为什么一定同时约完	第13章 唯一性证明
6	小于某个数的素数数量	第17章
7	质因子的种数及数量上界	第17章
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13章
10	为什么乘积展开就是容斥	第3章 、 第13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14章

轮次	原来的问题或关注点	在哪里接着读
14	原根回答里的公式显示异常	第5章、第14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14章重新排版
16	阶互质时乘积阶为什么相乘	第14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13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13章
21	两种形式的详细证明	第13章

18.2 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13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14章

轮次	原来的问题或关注点	在哪里接着读
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15章
11	阶为 d 的元素为什么有 $\varphi(d)$ 个	第10章、第15章
补充	为什么求和后仍不超过一半	第11章

18.3 这次怎样改写，旧版怎样保留

第三版先用模7建立循环，用模55看分解和不同到达时间，再用模13解释均匀取幂。加权平均先用分堆与具体比例说明，最后才写求和。完整基础证明仍保留，但放在第13章之后按问题回查。

上一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。