素数有无穷多个的若干简单证明

陈童

如果你有耐心罗列出前100个甚至前1000个素数，你会发现，总体趋势是，相邻两个素数之间的间隔会越来越大，也就是说素数分布会逐渐稀疏。那么，可不可能到一定程度以后，就不再出现新的素数了呢？换言之，素数可不可能是有限的呢？如果你永远都能找到新的素数，那又怎么严格地证明素数无限呢？

令人吃惊的是，两千多年前，欧几里德就证明了这个定理，也就是素数是无限的。**欧几里得定理：素数有无穷多个。**

当然，今天我们已经知道了这个定理的很多证明方法，这篇文章就是收集其中最为简单的一些。

1 欧几里德的经典证明

证明方法：反证法（归谬法）

欧几里德证明素数有无穷多个的详细步骤

步骤1：假设素数有限 假设存在有限个素数，记为$p_1, p_2, p_3, \ldots, p_n$，其中$n$ 是某个确定的自然数。例如，假设所有素数为$2, 3, 5$（实际证明中不依赖具体数值）。

步骤2：构造新数N 构造一个新数N，定义为所有已知素数的乘积加1：

$$N = p_1 \times p_2 \times p_3 \times \cdots \times p_n + 1$$

例如，若已知素数为$2, 3, 5$，则$N = 2 \times 3 \times 5 + 1 = 31$。

步骤3：分析N 的性质

- **情况1：N 是素数** 若N 本身是素数，则N 不在原素数列表$p_1, p_2, \ldots, p_n$中（因为$N > p_i$ 对所有i 成立），与“所有素数已被列出”的假设矛盾。

- **情况2：N 是合数** 若N 是合数，则它必然有至少一个素因数q。但q不能是原列表中的任意一个p_i，因为：

$$N/p_i = (p_1 p_2 \cdots p_n)/p_i + \frac{1}{p_i} \implies \text{余数为1}$$

即$N \equiv 1 \mod p_i$，故p_i 不整除N。因此，q 必是一个新素数，不在原列表中，同样导致矛盾。

步骤4：结论 无论N 是素数还是合数，均会导致与“素数有限”的假设矛盾。因此，原假设不成立，**素数有无穷多个**。

核心逻辑总结 通过构造N，无论其是否为素数，均需引入原列表外的素数，从而证明有限素数的假设无法成立。这一简洁而深刻的证明体现了数学中反证法的威力。

2 欧几里德证明的变种

证明：素数有无穷多个

我们通过构造一个递增的正整数序列，每个新项均与之前所有项互质，从而证明素数必须有无穷多个。

构造序列： 定义序列$\{a_n\}$ 如下：$a_1 = 2$, $a_{n+1} = a_n(a_n - 1) + 1$，对所有$n \geq 1$。

性质分析： 1. **递增性**：显然，$a_{n+1} = a_n(a_n - 1) + 1 > a_n$，故序列严格递增。2. **互质性**：对任意$n \geq 1$，有$a_{n+1} \equiv 1 \pmod{a_n}$。进一步，若$a_n \equiv 1 \pmod{a_{n-1}}$，则$a_n - 1 \equiv 0 \pmod{a_{n-1}}$，从而：

$$a_{n+1} = a_n(a_n - 1) + 1 \equiv 0 + 1 \equiv 1 \pmod{a_{n-1}}.$$

递推可知，a_{n+1} 与所有前项$a_1, a_2, \ldots, a_n$ 互质。

矛盾导出： 假设素数仅有有限个$p_1, p_2, \ldots, p_k$。由于序列$\{a_n\}$ 无限递增，且每个a_n 的素因子必不在之前的项中出现，故每个a_n 至少引入一个新的素因子。然而，有限素数无法为无限序列提供无限多新素因子，矛盾。

结论： 因此，素数必有无穷多个。证毕。

注：该证明通过构造互质序列，巧妙地将素数的无限性转化为序列的增长性，与欧几里得经典证明互为补充，提供了新的视角。

上述证明的本质

为了进一步看清楚上述证明的本质，根据序列$\{a_n\}$的定义，也就是$a_1 = 2$, $a_{n+1} = a_n(a_n - 1) + 1$，不难递推出如下关系式

$$a_{n+1} = a_1 a_2 ... a_n + 1, \tag{1}$$

所以这里用到的依然是欧几里德经典证明中的那个构造！

3 利用费马数进行证明

定理: 素数有无穷多个。 **证明：基于费马数的互质性**

证明步骤

1. **费马数的定义** 费马数定义为：

$$F_n = 2^{2^n} + 1 \quad (n \geq 0).$$

前几个费马数为：

$$F_0 = 3, \quad F_1 = 5, \quad F_2 = 17, \quad F_3 = 257, \quad F_4 = 65537, \quad \ldots$$

2. **费马数的互质性** 关键性质：**任意两个不同的费马数互质**。假设存在某个素数p 同时整除F_m 和F_n（不妨设$m < n$）。- 由$p \mid F_m$ 得：

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

- 由$p \mid F_n$ 得：

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

- 将第一个同余式平方2^{n-m} 次，得到：

$$2^{2^n} \equiv 1 \pmod{p}.$$

- 但第二个同余式表明$2^{2^n} \equiv -1 \pmod{p}$，矛盾。因此，$F_m$ 和F_n 互质。

3. **无限素数的推导** - 每个费马数F_n 至少有一个素因数（因$F_n > 1$）。- 由于任意两个费马数互质，它们的素因数完全不同。- 因此，每个F_n 引入至少一个新的素数。- 若素数有限，则无法为无限个费马数提供足够的素因数，矛盾。

4. **结论** 因此，素数必须有无穷多个。

—

数学意义 - 数论中的结构性证明：展示了数列的特殊性质（如互质性）可推导出深刻结论。- **费马数的特殊性**：尽管费马数本身未必全为素数（如$F_5 = 641 \times 6700417$），但其素因数的互异性仍成立。此证明通过费马数的代数结构，提供了一个简洁且新颖的视角，绕开了传统构造法，体现了数学中“利用对象间关系”的证明策略。

4 计数证明

关于素数有无穷多个的证明还可以通过分析自然数的素因子分解数目与自然数本身的增长之间的矛盾来实现，具体步骤如下：

—

证明:

假设素数仅有有限个，记为$p_1, p_2, \ldots, p_k$。考虑任意自然数$N \geq 2$，每个数$n \leq N$ 可唯一分解为：

$$n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k},$$

其中$a_i \geq 0$。对于每个素数p_i，指数a_i 满足：

$$p_i^{a_i} \leq N \implies a_i \leq \log_{p_i} N \leq \log_2 N \quad (\text{因} p_i \geq 2).$$

因此，每个a_i 的可能取值至多为$\lfloor \log_2 N \rfloor + 1$ 种。所有可能的分解数目不超过：

$$(\lfloor \log_2 N \rfloor + 1)^k \leq (\log_2 N + 1)^k.$$

然而，自然数$n \leq N$ 的数量为N，因此必须满足：

$$(\log_2 N + 1)^k \geq N.$$

当$N \to \infty$ 时，左边为$O((\log N)^k)$，右边为$O(N)$。显然，对于固定k，当N 足够大时，$(\log N)^k$ 的增长远慢于N，导致矛盾。故假设错误，素数必有无穷多个。

—

关键点： 通过限制有限素数下自然数的分解组合数目，发现其增长速度无法匹配自然数本身的增长，从而导出矛盾。这一证明避免了构造特定数或依赖复杂定理，仅通过计数矛盾即可完成。

5 更多证明

以下是更多关于素数有无穷多个的证明：

一. 欧拉的分析证明（18世纪）

思想：利用调和级数发散与欧拉乘积公式的矛盾。

详细步骤：

1. **调和级数发散：**已知$\sum_{n=1}^{\infty}\frac{1}{n}$发散（即其部分和趋向无穷大）。

2. **欧拉乘积公式：**对$\mathrm{Re}(s)>1$，有

$$\sum_{n=1}^{\infty}\frac{1}{n^s}=\prod_{p\text{ prime}}\frac{1}{1-p^{-s}}.$$

该公式通过唯一分解定理展开为素数的乘积形式。

3. **取**$s\to 1^+$：当s接近1时，左边的级数$\sum\frac{1}{n^s}$发散（因调和级数发散）。

4. **矛盾分析：**若素数有限，则右边乘积为有限项，显然收敛，与左边发散矛盾。

5. **结论：**素数必须无穷多。

二. 阶乘构造法（直接构造）

证明过程：

1. **对任意**$n\geq 2$，考虑$N=n!-1$。

2. **素因子存在性：**$N>1$，故至少有一个素因子p.

3. **分析**p：- 若$p\leq n$，则$n!=1\times 2\times 3\times ...\times p\times ...\times n$, 从而$p\mid n!$，从而$p\mid n!-(n!-1)=1$，矛盾。- 因此$p>n$.

4. **结论：**对任意n，存在素数$p>n$，故素数无穷多。