素数有无穷多个之九类证明

卢昌海

引言：素数（prime number）是除去1和本身之外不存在其他因子的大于1的正整数。单纯从这个定义看，素数没什么先验的理由必须有无穷多个，然而对数学家来说，很幸运的是：素数有无穷多个。

有关这一命题的最早书面证明出现于公元前300年左右，有“几何之父”美誉的古希腊数学家欧几里得在《几何原本》中陈述了这一命题并给出了证明（列于《几何原本》第9卷的第20个命题），这一命题也因此被称为了“欧几里得定理”（Euclid's theorem）或“欧几里得第二定理”，后者是由于《几何原本》第7卷的第30个命题——即一个素数若整除两个整数之乘积，则至少整除两者之一——有时被称为“欧几里得第一定理”，素数有无穷多个相应地被挤成“老二”。

素数有无穷多个这一命题简单却魅力无穷，且牵涉甚广，故自欧几里得以来的2,300多年间，后世数学家们又给出了数以百计的新证明。那些新证明繁简不一，且很多只是互为变种，在本文中，我们挑其中有代表性的九类证明略作介绍，以飨读者。

1. 欧几里得的证明

首先当然是欧几里得的证明——虽然由于《几何原本》既是欧几里得本人的著作，又是前人成就之汇集，很难确切知晓该证明是来自前人还是欧几里得自创（只能说并无前者的直接证据）。欧几里得的证明已进入初等数学课堂，因而几乎已是所有读者烂熟于胸的，但知识意义上的平凡掩不去它的美。 英国数学家哈代（G. H. Hardy）在《一位数学家的辩白》一书中称这一证明历久弥新，依然如初发现时一样重要，两千年的时光不曾刻下丝毫褶痕。

当然，“不曾刻下丝毫褶痕”是有所夸张的，比如欧几里得对素数有无穷多个的表述是“素数比任何指定个数的素数更多”，证明过程采用了几何术语（其中的“数”是用线段长度来表示的），“指定个数”则被选为了3个，而不像现代证明中那样用一个代表任意数目的字母来表示，以示普遍。不过跟“两千年的

最早给出初等证明的欧几里得

时光”相比，这些措辞习惯上的“褶痕”实是微不足道的，证明的本质——即证明已知素数的连乘积加 1 是新素数或以新素数为因子——则无需丝毫改变。

欧几里得的证明通常被视为归谬法的范例，这种方法曾被哈代称为“数学家最好的武器之一”，并被比喻为国际象棋中的“弃子开局法”。所不同的是——哈代补充说，棋手只能牺牲个别棋子，数学家却敢于假设整个游戏的失败——即假设所要证明的命题不成立。

不过，归谬法虽得到哈代的力挺，却不是所有数学家都认可的。比如数学基础研究中的一个名为直觉主义的流派就并不承认归谬法[1]。但另一方面，欧几里得的证明并非单纯的归谬证明，而是同时给出了算法，一种通过已知素数的连乘积加 1 所含的素因子构造新素数的算法[2]。事实上，在欧几里得的原始表述中，算法的意味要明显强于归谬的意味，从这点上讲，欧几里得的证明与其说是归谬证明，不如说是构造性证明，而构造性证明是连直觉主义这种在丢弃数学成果方面最大刀阔斧的流派也认可的。因此，欧几里得的证明尽管既古老又简单，同时却是极其强大的。

在后世数学家给出的新证明中，有很多是欧几里得证明的变种。比如德国数学家库默尔（Ernst Kummer）于 1878 年，荷兰数学家斯蒂尔杰斯（Thomas Stieltjes）于 1890 年，分别给出了这样的变种：假设只存在有限多个素数 $p_1, \cdots, p_n$，令 $N = p_1 \cdots p_n$，则所有 p_i $(i = 1, \cdots, n)$ 都是 N 的素因子。由于 $p_1, \cdots, p_n$ 是全部素数，其中必有一个是 $N-1$ 的素因子，设其为 p_r $(1 \le r \le n)$，则 p_r 同时是 N 与 $N-1$ 的素因子，从而也是两者之差——也就是 1——的素因子。由于这是不可能的，故素数有无穷多个。读者想必看出了，这只是将欧几里得证

[1] 直觉主义直接反对的是所谓排中律，归谬法的不被承认是其副产品。另外顺便说一下，有一种“精分”的看法主张对归谬法和反证法作出区分，前者意在反驳（即“归谬”），后者意在证明（即“反证”），且前者之“谬”不限于逻辑，后者则只限于用逻辑矛盾完成证明。从这一区分上讲，欧几里得的证明偏于反证而非归谬。不过此处引述的哈代称之为归谬法，本文就不予“精分”了。

[2] 如果从最小的素数 2 出发，只用这种算法寻找新素数，且每次只找最小的素因子，由此得到的素数序列被称为欧几里得 - 马林序列——因美国数学家马林（Albert A. Mullin）对其的研究而得名。欧几里得 - 马林序列目前只算出了前几十项（因计算量随项数增加太快），大小则剧烈起伏（比如前 10 项分别为：2, 3, 7, 43, 13, 53, 5, 6221671, 38709183810571, 139）。是否所有素数都会出现在欧几里得 - 马林序列中？这是一个迄今尚未解决的问题。

明中的连乘积加 1 改为减 1，优美度甚至稍逊（因原则上需对连乘积减 1 等于 1 的简单情形作出附加说明）。如此平庸的变种得以冠名而流传，有些出人意料。

另一个据说是法国数学家埃尔米特（Charles Hermite）给出的变种在新意上略胜于前一变种，具体是这样的：$n! + 1$ 的素因子必定大于 n（否则被 $n! + 1$ 除余 1，不可能是素因子），由于 n 是任意的，因而无论已找到多少素数，都还可以找到更大的，故素数有无穷多个。

2. 利用互素序列的证明

所有将一串整数乘起来再做点加减法的证明，在很大程度上都是欧几里得证明的变种，接下来要介绍的则是一些与欧几里得证明有着不同思路或视角的证明。其中第一类是利用所谓互素序列的证明。这类证明的思路很简单：假如能找到一个无穷序列，其中任意两项都是互素的（即所谓互素序列），那就等于证明了素数有无穷多个——因为每一项的素因子都彼此不同，项数无穷，素因子的个数——从而素数的个数——自然也就无穷。

因此问题归结为：什么样的序列既是无穷序列又是互素序列？

1730 年，德国数学家哥德巴赫在给著名数学家欧拉的一封信里给出了一个合乎需要的互素序列：$F_n = 2^{2^n} + 1$ $(n = 0, 1, \cdots)$，并由此证明了素数有无穷多个。有些读者想必认出来了，这个互素序列里的各项是 17 世纪的法国数学家费马引进的所谓的费马数。费马曾经猜测，所有费马数都是素数，他并且验证了 $n = 0, 1, 2, 3, 4$ 的情形，全都符合猜测。由于费马数随 n 增长极快，在没有计算机的时代，对更大的 n 进行验证极其繁琐，费马的猜测因此陷入不了之局长达近百年。不过到了 1732 年，欧拉证明了 $F_5 = 641 \times 6700417$ 不是素数，从而推翻了费马的猜测。自那之后，截至 2014 年，人们又陆续证明了从 F_6 到 F_{32} 的所有费马数都不是素数，这期间有人反费马而行之，猜测除有限多个外，费马数全都不是素数。直到今天，费马数里究竟有多少素数，多少非素数，依然是个谜[3]。

不过费马的猜测虽不成立，即费马数并非全是素数，却可以证明所有费马数彼此互素，因为费马数满足这样一个关系式：$F_n - 2 = F_0F_1 \cdots F_{n-1}$[4]。这关系式表明 $F_0, \cdots, F_{n-1}$ 全都可以整除 $F_n - 2$，从而也意味着 $F_0, \cdots, F_{n-1}$ 的所有素因子都可以整除 $F_n - 2$。假如这些素因子中有任何一个可以整除 F_n，则该素因子就可以整除 F_n 和 $F_n - 2$ 之差——也就是 2，而这是不可能的（因为能整

[3] 从基于概率的所谓“概率启发式理由”（probabilistic heuristic justification）出发，可推测费马数中的素数个数是有限的。因为 N 附近的素数分布概率为 $A/\ln(N)$（A 为常数），因此费马数中素数总数的期望值为 $\Sigma_n[A/\ln(F_n)] \sim A\Sigma_n(2^{-n}) \leq A$，是有限的。不过“概率启发式理由”假定了费马数是素数的概率跟一个普通正整数是素数的概率一样，没有任何特殊性，这一点有迹象显示未必成立，因此这一理由至多只是“启发式”的。

[4] 这一关系式的证明很容易，感兴趣的读者请用数学归纳法试试。