如何证明有无穷多个素数

如何证明有无穷多个素数？我们用的是反证法，即假设结论不成立，推出一个矛盾。这是反证法的基本步骤。

假设结论不成立，只有有穷多个素数，设为 p1，p2，…，pi，...，pn。我们令 m=p1p2…pn+1(此处采用的是构造证明法，非常巧妙，由古希腊著名思想家亚里士多德提出)。为证明结论，我们需要先证明一个引理，即 m 不是每个 pi 的倍数，即每个 pi 都不是 m 的因子。

怎么证明这个引理呢？用的也是反证法。

不妨先假设 p1 是 m 的因子，可以令 m=k1*p1=p1p2…pn+1，那么根据因子的定义，k1 一定是整数。经过简单的处理后，k1=p2…pn+1/p1，则 k1 显然不可能是整数，与前面的 k1 一定是整数相矛盾。余下的 p2 到 pn 依此类推。这就证明了每个 pi 都不是 m 的因子。

那么，是否就直接可以说 m 是素数呢？如果 m 是素数，接下来的证明可见下面的 1。

事实上，m 可能是素数，也可能是合数。

1. 如果 m 是素数，则现在素数就变成了 n+1 个(前面 p1 到 pn，一共 n 个，加上现在的一个 m)，这就与前面的假设有 p1 到 pn 即 n 个素数相矛盾。由反证法得知当 m 是素数时结论成立，即当 m 是素数时有无穷多个。

当年亚里士多德(受时代的限制)思路就停留在这里，他武断地认为 m 就是素数。

那么 m 到底是不是一定是素数呢？结论是不一定。为什么 m 不能只是素数？因为素数的定义是：大于 1 且只能被 1 和自身整除的正整数，也就是素数是不可能找到除了 1 和它自身以外的因子的。前面已经证明了每个 pi 都不是 m 的因子，但 pi 并不一定能代表除了 1 和这个数自身以外的所有情况，到此我们可以判断 m 只能是素数的结论是武断的。当然 m 是素数也是有可能的，我们并不确定。

m 是素数的情况下结论已经成立，前面刚证明完。我们只要证明 m 是合数的情况下结论成立即可。这里我们不妨用试探法，即尝试一下 m 是否有合数的情况。

怎么入手呢？我们可以先找一个合数出来，这里我们不妨将 p1 到 pn 从小到大排列，即 pn 是 p1 到 pn 中最大的一个，因为有限个素数中总要有最大的一个，我们不妨设为 pn。

①2*3+1=7 是素数

②2*3*5+1=31 是素数

③2*3*5*7+1=211 是素数

④2*3*5*7*11+1=2311 是素数

⑤2*3*5*7*11*13+1=30031 是合数（因为 30031=59*509，其中 59 和 509 都是素数）

运气不错，推了几步就找出来了一个满足要求的 m，而 59 和 509 显然都大于 pn(=13)，也就是我们又找到了除了 p1 到 pn 的且比 pn 要大的至少一个素数，这又跟原先我们假设的 p1 到 pn 有 n 个素数相矛盾。由反证法得知，当 m=30031 时的结论成立。但当 m 是一个大于 30031 的合数是否也成立呢？即当 m>30031 时，是否也能找到大于 pn 的素数因子呢？答案是肯定的。

首先，合数 m 一定能分解成若干个素数的乘积。我们之前已经证明了 p1 到 pn 都不是 m 的因子，换句话说小于等于 pn 的所有素数都不是 m 的因子，那么 m 的素数因子就一定比 pn 还大。也就是当 m 是大于 30031 的任何一个合数时，也能找到除了 p1 到 pn 且大于 pn 的至少一个素数因子，也就是素数因子至少有 n+1 个，也即素数至少有 n+1 个，这又跟原先我们假设的 p1 到 pn 有 n 个素数相矛盾，也即当 m 是合数的情况下结论也成立，即也有无穷多个素数。

这样我们就证明了当 m 是素数和合数时，都有无穷多个素数，原题得证。

总结几点：

1. 亚里士多德构造的 m=p1p2…pn+1 和证明 pi 都不是 m 的因子的想法是怎么来的？难怪欧拉说这是“直接来自上帝的证明”。
2. 本证明用到了一次构造证明法(我们构造了 m=p1p2…pn+1)，用到了 5 次反证法和一次试探法(我们试探了 m 是否有合数的情况)。5 次反证法的运用如下：
   (1) 整个题目的证明就是用反证法。
   (2) 证明每个 pi 都不是 m 的因子这个引理时用到了反证法。
   (3) 证明 m 是素数时结论成立用的也是反证法。
   (4) 证明 m 是等于 30031 的合数时结论成立用的也是反证法。
   (5) 证明 m 是大于 30031 的合数时结论也成立，用的也是反证法。
3. 从豁然开朗的感觉到疑惑重重再到豁然开朗，数论真的难学。
4. 我们的课件 PPT 个别地方做得有点粗糙，一个难度颇大的证明过程，PPT 上几句话就写完了(见下图 1)，也难怪老师和学生会看不懂。

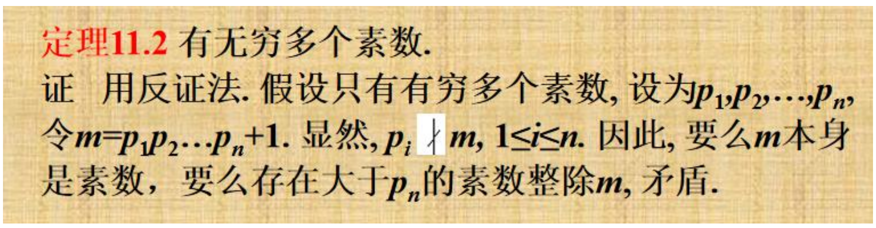

图 1

同济大学软件学院
唐剑锋
2022.05.14