证明: 素数有无穷个

**证明一 欧几里得在《几何原本》里面已经给出了证明**

（反证）

假设素数是有限的，假设素数只有有限的*n*个，且最大的一个素数是*p* ，

设*q*为所有素数之积加上1，即取*q* = （2 × 3×5 × …… ×*p*）+ 1，

*q*只有两种可能：

（1）是素数，与假设矛盾；

（2）是合数，*q*可以被素数2、3、……、*p*中的数整除，但是根据*q*的构造知道：*q*被这素数2、3、……、*p*中任意一个整除都会余1，且有异于2,3,5，……，*p*的素因子，设为*m*，这样就找到了不同于2,3,5，……，*p*的素数，与假设也矛盾。

所以，素数是无限的。

（也可以这样说明：若*q*能被小于*q*的正整数整除，情况有两种，被小于*q*的素数或被小于*q*的合数整除。小于*q*的素数也就包括在2，3，5，…… *p* 中，明显不能被它们整除；如果能被小于*q*的合数*m*整除，合数*m*又可以分为两个更小的素数相乘，设*m*=*s*×*t*，则*s*<*m*<*q*，*t*<*m*<*q*，那么*q*肯定能被*s*或*t*中的任何一个整除，而*s*和*t*都是小于*q*的素数，都不能整除*q*，所以矛盾。）

假设存在最大的素数*p*，那么我们可以构造一个新的数（2 × 3×5 × …… ×*p*）+ 1（所有的素数乘起来加1）。显然这个数不能被任一素数整除（所有素数除它都余1），这说明我们找到了一个更大的素数。

这个证明被欧拉称为“直接来自上帝的证明”，历代的数学家也对其评价很高。

但是，千万不可认为，形如*p*1·*p*2·...·*p*n+1（其中*p*1, *p*2,..., *p*n均为素数）的数就一定是素数！第八届全国青少年信息学奥林匹克联赛（NOIP2002)提高组初赛试题第三题第2小题，写程序运行结果，程序要找的就是形如*p*1·*p*2·...·*p*n+1（其中*p*1, *p*2,..., *p*n均为素数）的数中第一个是合数的整数。

2×3+1=7 是素数

2×3×5+1=31 是素数

2×3×5×7+1=211 是素数

2×3×5×7×11+1=2311 是素数

2×3×5×7×11×13+1=30031 不是素数，因为30031=59×509

**证明二 用Fermat数证明素数无穷多**

     Fermat数是指形为+1的数，我们把+1记作F(*n*)，其中*n*可以取所有自然数。显然所有的Fermat数都是奇数。一会儿我们将看到任两个Fermat数都是互素的，也就是说，**每一个Fermat数的每一个素因子都与其它Fermat数的素因子不同**。这也就说明，素数个数有无穷多。

引理1：F(0)× F(1)× F(2)× …×F(*n*-1) = F(*n*) – 2, *n*>=1

证明：数学归纳法。F(0)=3且F(1)=5，那么*k*=1时显然成立。

假设*k=n*时，原命题成立，则当*k=n*+1时：

     F(0) × F(1) × F(2) × … × F(*n*)

   = ( F(0) × F(1) × F(2) × … × F(n-1) ) × F(n)

   = ( F(n)-2 ) × F(n)

   = (-1 ) × (+1 )

   = -1 = F(*n*+1) -2

引理2：对任意两个不相等的自然数*n*和*m*，有F(*n*)和F(*m*)互素。

证明：假设*t*同时整除F(*n*)和F(*m*)，*m*<*n*。根据引理1，有：

F(*n*)=F(0) × F(1) × F(2) × … × F(*m*) × … × F(*n*-1) – 2

     这说明*t*可以整除

     F(0) × F(1) × F(2) × … × F(*m*) × … × F(*n*-1) – F(*n*) = 2

注意到2只有两个因数1和2。前面说过Fermat数都是奇数，因此不可能被2整除。这样，*t*只能为1，这就证明了两个费马数是互素的。

最后结论：Fermat数有无穷多个，所以素数也是无穷多个。

**证明三 用\*-集合证明素数无穷多**

\*-集合是一个正整数集合{*a1, a2, … an*}，使得对所有不相等的*i*和*j*都有*ai-aj*整除*ai*。

引理1：对所有n≥2，都存在一个大小为*n*的\*-集合。

证明：采用数学归纳法。

{1,2}显然是一个大小为2的\*-集合。

假设{*a1, a2, … an*}是一个\*-集合，定义*b*0为*a*1×*a*2×…×*a*n（即所有*a*i的乘积）。

对所有不超过*n*的正整数*k*，令*bk*=*b*0+*ak*，那么{*b*0, *b*1, *b*2, …, *b*n}就是一个大小为*n*+1的\*-集。

引理2：假设{*a1, a2, … an*}是一个\*-集合。

对所有不超过*n*的正整数*i*，定义*f*i=2*a*i+1，那么*f*1,  *f*2, …,  *f*n两两互素。

证明：显然*f*i都是奇数。假设*f*k和*f*m(*f*k>*f*m)可以被同一个素数*p*整除，那么*p*也只能是奇数，*p*可以整除*f*k-*f*m ，即 2^*am* (2^(*ak*-*am*)-1)，由于*p*是奇数，那么它只可能是整除(2^(*ak*-*am*)-1)。

如果有*s*整除*t*，那么2^*s*-1整除2^*t*-1。于是， 根据\*-集合的定义，2^( *ak*-*am*)-1整除2^*ak*-1。那么*p*就可以整除2^*ak*-1。但*p*也能整除2^*ak*+1，于是我们得出*p*整除2，这与p为奇数矛盾。

定理：素数有无穷多个

证明：根据引理1和2，对任意大的*n*，都存在大小为*n*的集合，里面的数两两互素，即至少存在*n*个不同的素因子。这就说明了素数的个数可以任意多。

证明四 集合证明法

学过初中的同学都知道*n*!与*n*!+1互质。故*n*!与1、2、3、….*.n*-1、*n*互质那么*n*!+1有2种可能（1）*n*!+1为素数，(2)*n*!+1为合数 .

（1）设*a*=*n*!+1为素数， 集合*A*={*x*|0< *x*≤ *n* ，*x*∈*N*}有*b*个素数，则集合*B*={*x*|0<*x*≤*n*!+1 *x*∈*N*}内至少有*b*+1个素数

（2）设*a*=*n*!+1为合数则在集合*B*\*A*中至少有2个元素可以被*a*整除

易证：*c*=min{*x*| *x*∈*B*\*A* 且*a*/*x*=*h* ，*h*∈*N*}为素数。同（1）设集合*A*内有*b*个素数。则集合*B*内至少有*b*+1个素数

综合（1）、（2）可得：设集合*A*={*x*|0< *x*≤ *n* ，*x*∈*N*}有*b*个素数， 则集合*B*={*x*|0<*x*≤*n*!+1 *x*∈*N*}内至少有*b*+1个素数。

重复操作可得集合C={x|o<x≤（n!+1）!+1 x∈N}内至少有b+2个素数。

继续沿用上述的操作，用数学归纳法可证：设集合A={x|0<x≤n x∈N}有b个素数，则集合D={x|o<x≤{[(n!+1)!+1]!+1…..}内至少有b+d个素数

d重

由此：当d→+∞时，e=素数的个数≥b+d=+∞   
证明完毕。 （？？？）

**证明五 梅森素数序列证明法**

假定素数的个数只有有限多个，设为2，3，...，p

考虑梅森数2P-1，命2P-1的某一个素因子为*q*, 有2p=1(mod *q*), 故2模q的阶为*P*，所以*p*|*q*-1,进而有*q*>*p*, 与*P*是最大质数矛盾。

证明 6 n大于2时，n和2n之间至少存在一个质数，所以有无穷多个质数。