素数有无穷多个的 17 个证明（2）

2021-04-07 原文链接

网站版本 1c934d989f84 · 文章 ID h_e38e4aa899386a02

9. Srinivasan 的证明

由 Goldbach 和 Schorn 的证明可知，如果存在无穷多个两两互素的正整数，则可由此证明存在无穷多个素数.

引理如果在数列 $\{x_n\}$ 中，对于任意正整数 i，都有 $x_i|x_{i+1}$ 且 $\gcd\left(x_i, \dfrac{x_{i+1}}{x_i}\right)=1$. 则容易知道数列 $\left\{\dfrac{x_{n+1}}{x_n}\right\}$ 中任意两项均互素.

设 $f(x)=x^2+x+1$. 则 $f(n^2)=f(n)f(-n)$，且

$$\begin{aligned}&\gcd(n^2+n+1, n^2-n+1)\\=&\gcd(2n, n^2-n+1)\\=&\gcd n, n^2-n+1\\=&1.\end{aligned}$$

于是数列 $x_m=f\left(2^{2^m}\right)$ 符合以上要求.

数列 $x_m=2^{p^m}-1$（p 为素数）同样也符合以上要求.

当 m≥1 时，x_m/x_{m-1} 的任一素因子 q 都使 2 模 q 的乘法阶等于 p^m，故 $q\equiv 1 \pmod{p^m}$。固定 r≥1，令 m≥r，利用这些商两两互素，即得有无穷多个模 p^r 余 1 的素数。

$$\begin{aligned}\frac{x_{m+1}}{x_m}=&\frac{(x_m+1)^p-1}{(x_m+1)-1}\\=&1+(x_m+1)+\cdots+(x_m+1)^{p-1}\\\equiv&p(\mathrm{mod}\ q).\end{aligned}$$

因此如果素数 q 同时整除 x_m 和 $\dfrac{x_{m+1}}{x_m}$，则必有 $q=p$.

而由 Fermat 小定理，

$$x_m=2^{p^m}-1\equiv 1(\mathrm{mod}\ p).$$

即 p 必不整除 x_m，矛盾. 因此数列 $x_m=2^{p^m}-1$（p 为素数）也符合以上要求.

当 m≥1 时，x_m/x_{m-1} 的任一素因子 q 都使 2 模 q 的乘法阶等于 p^m，故 $q\equiv 1 \pmod{p^m}$。固定 r≥1，令 m≥r，利用这些商两两互素，即得有无穷多个模 p^r 余 1 的素数。

Srinivasan 进一步证明了对于任意正整数 $k \geq 1$，存在无穷多个模 k 余 1 的素数. 这和 Lucas 的证明本质上是一样的，这里不再赘述.

10. Thue 的证明

设正整数 n 和 k 满足 $(1+n)^k < 2^n$，并设不超过 2^n 的所有素数依次为 $p_1 = 2$，$p_2 = 3$，$\cdots$，p_r. 对于任意的 $1 \leq m \leq 2^n$，其可以被表示为

$$m = 2^{e_1} 3^{e_2} \cdots p_r^{e_r}.$$

由 $m \leq 2^n$ 可知 $e_i \leq n$ $(1 \leq i \leq r)$.

于是 $e_1, e_2, \cdots, e_r$ 的取值不超过 $(n+1)^r$ 种. 于是有

$$(1+n)^k < 2^n \leq (1+n)^r$$

即 $r > k$.

对每个正整数 k，由 $1 + 2k^2 < 2^{2k}$ 可知

$$(1+2k^2)^k < 2^{2k^2}.$$

取 $n = 2k^2$，这样的 n 和 k 是满足上述要求的.

于是对于任意正整数 k，存在至少 $k+1$ 个素数 $p < 2^n = 4^{k^2}$，从而证明了素数有无穷多个.

11. Perott 的证明

首先我们知道 $\sum\limits_{n=1}^{+\infty} \dfrac{1}{n^2}$ 是收敛的，且其值恒小于 2.

事实上，Euler 证明了 $\sum\limits_{n=1}^{+\infty} \dfrac{1}{n^2} = \dfrac{\pi^2}{6}$.

我们可以用一个简单而初等的方法证明

$$\sum_{n=1}^{+\infty} \frac{1}{n^2} < \frac{7}{4}.$$

证明

$$\begin{aligned}\sum_{n=1}^{+\infty}\frac{1}{n^2}=&1+\frac{1}{4}+\sum_{n=3}^{\infty}\frac{1}{n^2}\\<&\frac{5}{4}+\sum_{n=3}^{+\infty}\frac{1}{n(n-1)}\\=&\frac{5}{4}+\sum_{n=3}^{+\infty}\left(\frac{1}{n-1}-\frac{1}{n}\right)\\=&\frac{5}{4}+\frac{1}{2}\\=&\frac{7}{4}\end{aligned}$$

设 $\delta=2-\sum\limits_{n=1}^{\infty}\dfrac{1}{n^2}$. 由上面的证明可知 $\delta>\dfrac{1}{4}$.

将不超过 N 的所有素数依次设为 p_1，p_2，$\cdots$，p_r. 由 Erdös 的证明可知：在不超过 N 的正整数中，无除 1 外的平方因子的正整数至多有 2^r 个，能被 d^2 所整除的正整数至多有 $\dfrac{N}{d^2}$ 个. 于是有除 1 以外的平方因子的正整数个数不超过

$$\sum_{d=2}^{+\infty}\frac{N}{d^2}=N\left(\sum_{d=1}^{+\infty}\frac{1}{d^2}-1\right)=N(1-\delta)$$

于是 $N\le 2^r+N(1-\delta)$，即 $2^r\ge\delta N\ge\dfrac{N}{4}$，也即 $r>\log_2 N-2$. 从而证明了素数有无穷多个.

Perott 的证明将不超过 N 的所有正整数按照是否含有除 1 外的平方因子分成两类. 此方法是筛法的基础，而筛法本质上是用来估计满足某些特定条件的整数数量的.

12. Auric 的证明

反证法. 若只有有限个素数, 将其从小到大排列成 $p_1<p_2<\cdots<p_r$. 设 t 为任意正整数, $N=p_r^t$. 每个不超过 N 的正整数 m 可以被表示为

$$m=p_1^{f_1}p_2^{f_2}\cdots p_r^{f_r}.$$

设 $E=\dfrac{\ln p_r}{\ln p_1}$，由 $p_1^{f_i}\le p_i^{f_i}\le N=p_r^t$ 可知 $f_i\le tE$ 对任意 i 均成立. 于是

$$p_r^t=N\le(tE+1)^r\le t^r(E+1)^r$$

当 t 足够大时，上式不成立. 于是素数有无穷多个.

13. Boije 和 Gennäs 的证明

设 N 为任意正整数，$2,3,\cdots,p_n$ 为不超过 N 的所有素数. 取 $P=2^{e_1}3^{e_2}\cdots p_n^{e_n}$，其中 $e_i\ge 1$. 设正整数 A，B 满足 $\gcd(A,B)=1$，$P=AB$，且 $Q=B-A>1$. 于是 Q 不被任何不超过 N

的素数所整除，从而至少存在一个大于 N 的素数．于是素数有无穷多个.

注本方法在本质上与 Stieltjes 的证明相同.

14.Barnes 的证明

Barnes 的证明用到了周期连分数和 Pell 方程的相关理论.

反证法．若只有有限个素数，设它们为 p_1，p_2，$\cdots$，p_t．令 $P=\prod\limits_{i=1}^{t}p_i$，$Q=\prod\limits_{i=2}^{t}p_i$．考虑连分数 $x=[P,P,\cdots]$．有

$$x=\frac{P+\sqrt{P^2+4}}{2}=Q+\sqrt{Q^2+1}.$$

注意到 Q^2+1 不被除 2 外的任意素数整除，故必为 2 的幂．又 Q^2+1 不可能为完全平方数，可设 $Q^2+1=2^{2l+1}$ 即

$$Q^2-2\cdot(2^l)^2=-1$$

这说明 $\dfrac{Q}{2^l}$ 为连分数 $[1,2,2,\cdots]$ 即 $\sqrt{2}$ 的一个渐近分数．设渐近分数的分母为 B_m，则 $B_0=1$，$B_1=2$，$B_{m+1}=2B_m+B_{m-1}$．且对于任意偶数 m，B_m 为奇数．故只能是 $l=0$，$Q=1$，矛盾．因此存在无穷多个素数.

注由 $Q^2+1>2$ 以及 Q^2+1 不能被 4 整除，可以很快知道 Q^2+1 不为 2 的幂.

15. Braun 的证明

反证法．若只有有限个素数，设它们为 $p_1=2$，$p_2=3$，$\cdots$，p_t．考虑

$$\frac{m}{n}=\sum_{i=1}^{t}\frac{1}{p_i}.$$

注意道 $\dfrac{1}{2}+\dfrac{1}{3}+\dfrac{1}{5}>1$，于是 $\dfrac{m}{n}>1$ 即 $m>n\geq 1$.
于是 m 必含有某个素因子 p_i．然而，

$$m=\sum_{j=1}^{t}\prod_{k\neq j}p_k\equiv\prod_{k\neq i}p_k\neq 0(\mathrm{mod}\ p_i).$$

矛盾．因此存在无穷多个素数.

16. Harris 的证明

设 A_0，A_1，A_2 为两两互素的正整数，对于 $n\geq 3$，

$$A_n = \prod_{k=0}^{n-3} A_k \cdot A_{n-1} + A_{n-2}.$$

下面证明 A_0，A_1，$\cdots$，A_n 两两互素，从而可知存在无穷多个素数.

证明由递推关系容易证明以下两个结论：

（1）若 $p|\gcd(A_n, A_{n-2})$，则存在 $i \geq 1$，且 $i \neq 2$，使得 $p|\gcd(A_{n-i}, A_{n-2})$.

（2）若 $p|\gcd(A_n, A_{n-j})$，（$j \geq 1$，且 $j \neq 2$），则 $p|\gcd(A_{n-j}, A_{n-2})$.

由数学归纳法及 A_0，A_1，A_2 两两互素即证.

17. Chernoff 的证明

反证法. 若只有有限个素数，设它们为 p_1，p_2，$\cdots$，p_k. 对于任意正整数 N，恰好存在自然数组 $(e_1, e_2, \cdots, e_k)$ 的 N 种排列方式，使得

$$p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k} \leq N$$

即

$$e_1 \ln p_1 + e_2 \ln p_2 + \cdots + e_k \ln p_k \leq \ln N$$

满足此不等式的 k 元自然数组 $(e_1, e_2, \cdots, e_k)$ 个数恰为

$$\frac{(\ln N)^k}{k! \ln p_1 \ln p_2 \cdots \ln p_n}$$

于是存在某个常数 c，使得

$$N \leq c(\ln N)^k$$

这显然不成立，于是存在无穷多个素数.