素数有无穷多个的 17 个证明（1）

2021-04-06 原文链接

网站版本 1c934d989f84 · 文章 ID h_d7a5ca07f73eb967

1. Euclid 的证明

使用反证法. 若只存在有限个素数，将所有素数从小到大依次排列为 $2=p_1<p_2<\cdots<p_r$，再设 $P=p_1p_2\cdots p_r+1$，且 p 为 P 的一个素因子. 由于 $p_1,p_2,\cdots,p_r$ 均不整除 $P=p_1p_2\cdots p_r+1$，p 必为不同于它们的另一素数，这与 $p_1,p_2,\cdots,p_r$ 为所有素数矛盾，故素数有无穷多个.

在素数有无穷多个的所有证明中，Euclid 的证明应该是最被大家熟知的一个了.
这个证明非常初等，此外，Euclid 的证明能够进行一些改造从而给出素数分布的一些信息：
对任意 $R\geq 2$，存在一个素数 p，使得 $R<p\leq R^R+1$.
证明将不大于 R 的所有素数从小到大依次排列为 $2=p_1<p_2<\cdots<p_r$，再设 $P=p_1p_2\cdots p_r+1$，且 p 为 P 的一个素因子. 由于 $p_1,p_2,\cdots,p_r$ 均不整除 $P=p_1p_2\cdots p_r+1$，p 必为不同于它们的另一素数. 我们有 $p\leq R^r+1\leq R^R+1$，由于 $p_1,p_2,\cdots,p_r$ 为不大于 R 的所有素数，故 $p>R$.
注意到不超过 R 的素数个数不超过 $\dfrac{R}{2}+1$，我们可以用 $R^{\frac{R}{2}+1}$ 来代替 R^R+1.
当然，这是一个非常粗糙的估计.
Euclid 的证明有很多的变体.

2. Kummer 的证明

使用反证法. 若只存在有限个素数，将所有素数从小到大依次排列为 $2=p_1<p_2<\cdots<p_r$，再设 $N=p_1p_2\cdots p_r>2$，则正整数 $N-1>p_r$ 必有一个素因子 p_i，于是 $p_i|N-(N-1)=1$，这显然不成立，故素数有无穷多个.

Kummer 的证明本质上和 Euclid 的证明一致，只不过 Kummer 的证明中考虑了 $p_1p_2\cdots p_r-1$，而 Euclid 的证明中考虑了 $p_1p_2\cdots p_r+1$. 同样地，我们可以由 Kummer 的证明得到：
对任意 $R\geq 2$，存在一个素数 p，使得 $R<p\leq R^R-1$.

3. Stieltjes 的证明

使用反证法. 若只存在有限个素数，设其为 $p_1,p_2,\cdots,p_r$. 设 $N=p_1p_2\cdots p_r$，将 N 任意分解为两个正整数 m 和 n 的乘积，即 $N=mn$. 注意到任意素数恰整除 m 和 n 其中之一，故必不整除 $m+n$. 而 $m+n>1$，这显然不成立，故素数有无穷多个.

4. Goldbach 的证明

首先证明 Fermat 数 $F_n=2^{2^n}+1$（$n\geq 0$）两两互素.
证明注意到

$$\begin{aligned} &F_m - 2 = 2^{2^n} - 1 \\ &= \left(2^{2^{n-1}} + 1\right)\left(2^{2^{n-1}} - 1\right) \\ &= \cdots = F_0 F_1 \cdots F_{m-1}. \end{aligned}$$

于是 $\gcd(F_m, F_n) = \gcd(F_m, 2) = 1$.

由于有无穷多个 Fermat 数，而每一个 Fermat 数的素因子各不相同，故存在无穷多个素数.

注前 5 个 Fermat 数：$F_0 = 3$，$F_1 = 5$，$F_2 = 17$，$F_3 = 257$，$F_4 = 65537$ 均为素数. 而 $F_5 = 4294697297$ 为合数，其最小的素因子为 641.

5. Schorn 的证明

使用反证法，假设只有 m 个素数，令 $n = m + 1$. 使用辗转相除法容易证明下列 n 个正整数

$$1 \cdot n! + 1, 2 \cdot n! + 1, \cdots, n \cdot n! + 1$$

两两互素. 这 n 个数的素因子各不相同，至少有 n 个不同的素数，矛盾. 故存在无穷多个素数.

Schorn 的证明说明对于任意正整数 n，至少有 n 个素数不大于 $n \cdot n! + 1$.

6. Euler 的证明

不同于以上的几个证明，Euler 的证明使用了分析的方法. 并且，Euler 的方法在素数的分布问题上取得了巨大的进展.

设所有素数为 $p_1, p_2, \cdots, p_n$，注意到对于任意 p_i，无穷级数

$$\sum_{k=0}^{\infty} \frac{1}{p_i^k} = \frac{1}{1 - \dfrac{1}{p_i}}$$

故

$$\prod_{i=1}^{n} \frac{1}{1 - \dfrac{1}{p_i}} = \prod_{i=1}^{n} \sum_{k=0}^{\infty} \frac{1}{p_i^k}$$

等式右侧部分展开后为所有正整数的倒数和，其为发散的，这与素数只有 n 个矛盾. 故存在无穷多个素数.

同时，Euler 也证明了素数的倒数和发散.

注意到对于任意正整数 N，有

$$\sum_{n=1}^{N} \frac{1}{n} \leq \prod_{p \leq N} \frac{1}{1 - \dfrac{1}{p}}$$

这是由于对于任意不超过 N 的正整数，其总有一个不超过 N 的素因子. 又由于

$$\ln \prod_{p\le N} \frac{1}{1-\frac{1}{p}} = -\sum_{p\le N} \ln\left(1-\frac{1}{p}\right)$$

且对于任意素数 p，有

$$\begin{aligned} -\ln\left(1-\frac{1}{p}\right) &= \sum_{m=1}^{\infty} \frac{1}{mp^m} \\ &\le \sum_{m=1}^{\infty} \frac{1}{p^m} \\ &= \frac{1}{p} + \frac{1}{p(p-1)} \\ &< \frac{1}{p} + \frac{1}{(p-1)^2}. \end{aligned}$$

于是

$$\begin{aligned} \ln \sum_{n=1}^{N} \frac{1}{n} &\le \sum_{p\le N} \left(\frac{1}{p} + \frac{1}{(p-1)^2}\right) \\ &\le \sum_{p\le N} \frac{1}{p} + \sum_{n\le N} \frac{1}{n^2} \end{aligned}$$

这说明了

$$\sum_{p\le N} \frac{1}{p} \ge \ln \sum_{n=1}^{N} \frac{1}{n} - c \ge \ln\ln N - C$$

是发散的. 其中 c 和 C 为常数.

7. Erdös 的证明

设 $p_1 = 2$，$p_2 = 3$，$\cdots$，p_j 为所有不超过 x 的素数. 设 $n = n_1^2 m$，其中 m 无大于 1 的平方因子. 于是

$$m = 2^{b_1} 3^{b_2} \cdots p_j^{b_j}$$

其中 $b_j \in \{0, 1\}$. 于是至多存在 2^j 个这样的 m.
对于每个固定的 m，满足 $n_1^2 \le n \le x$ 的 n_1 至多有 $\sqrt{x}$ 个. 于是有 $x \le 2^j\sqrt{x}$. 即 $j \le \log_4 x$.
于是至多存在 $\log_4 x$ 个不超过 x 的素数.

利用 Erdös 的方法，同样能够证明存在无穷多个素数.

证明假设存在 M，使得

$$\sum_{p>M}\frac{1}{p}<\frac{1}{2}$$

即对于任意正整数 N，有

$$\sum_{p>M}\frac{N}{p}<\frac{N}{2}$$

将不超过 N 的正整数分成两个集合. 设存在大于 M 的素因子的正整数有 N_1 个，其余正整数有 N_2 个. 于是有

$$N_1\leq\sum_{p>M}\frac{N}{p}<\frac{N}{2}$$

由前面的证明可知 $N_2<2^M\sqrt{N}$.
于是当 N 足够大时，有

$$N=N_1+N_2<\frac{N}{2}+2^M\sqrt{N}<N$$

矛盾. 故素数有无穷多个.

8. Chebysheff 的证明

我们用 $v_p(n)$ 表示 n 的素因数分解中素数 p 的次数. 于是有

$$\begin{aligned}v_p(n!)=&\sum_{k=1}^{\infty}\left[\frac{N}{p^k}\right]\\ \leq&\sum_{k=1}^{\infty}\frac{N}{p^k}\\ <&\frac{N}{p-1}\end{aligned}$$

且当 $p>n$ 时，有 $v_p(n!)=0$.

于是

$$\begin{aligned}\sum_{p\leq n}\frac{\ln p}{p-1}>&\sum_{p\leq n}\frac{v_p(n!)\ln p}{n}\\ =&\frac{1}{n}\ln n!\\ >&\ln n-1\end{aligned}$$

于是 $n\to+\infty$ 时，有 $\sum\limits_{p\leq n}\dfrac{\ln p}{p-1}\to+\infty$，由此说明素数有无穷多个.