素因子之和的估计

虚空若叶睦

2025 年 8 月 15 日

对正整数 x, 记 $S(x)$ 是 x 的素因子之和 (包含重数). 即若 $x=\prod\limits_{i=1}^{k} p_i$, 其中 $p_1,\cdots,p_k$ 为素数, 则 $S(x)=\sum\limits_{i=1}^{k} p_i$. 证明以下结论:

(1) 对任意正整数 $n\geqslant 4$, 有 $S\left(2^{2^n}+1\right)\geqslant 2^{2n+4}+\dfrac{2^{n-1}}{n+2}$.

(2) 对任意素数 $p\geqslant 2$, 有 $S\left(2^p-1\right)\geqslant \dfrac{(p-1)(2p+1)}{\log_2(2p+1)}$.

(改编自第二十届中国北方数学“龙岗杯”夏令营二试第三题)

Fermat 数的素因子和估计

在证明这个结果之前, 我们先证明一个有用的结论:

定理 (Lucas) 设正整数 $n\geqslant 2$, 若 p 是 $2^{2^n}+1$ 的一个素因子, 则 $2^{n+2}\mid p-1$.

证明 由于 p 是奇素数, 故 2^{n+1} 是 2 在模 p 意义下的阶. 由 Fermat 小定理, 可得 $2^{n+1}\mid p-1$. 下面假设

$$p=k2^{n+1}+1,$$

我们希望证明 k 是偶数. 根据 Euler 判别法, 有

$$\left(\frac{2}{p}\right)\equiv 2^{\frac{p-1}{2}}=2^{k2^n}\equiv(-1)^k \bmod p. \tag{1}$$

但另一方面, 当 $n \geqslant 2$ 时, $8 \mid p-1$ 意味着

$$p \equiv 1 \bmod 8 \Longrightarrow \left(\frac{2}{p}\right) = 1 \bmod p. \tag{2}$$

结合 (1)(2) 可知 k 必为偶数, 命题得证. ■

回到原题. 下面这个精彩的证明是由群友 p-adic 给出的.

证明 根据引理, 可假设 $2^{2^n}+1$ 的素因子分解形如

$$2^{2^n}+1 = \prod_{i=1}^{k} p_i, \quad \text{其中 } p_i = 2^{n+2}t_i + 1, \quad i = 1, \cdots, k.$$

其中 $t_1, \cdots, t_k$ 为正整数. 于是可以得到

$$2^{2^n}+1 = \prod_{i=1}^{k}(2^{n+2}t_i+1) \equiv 1 + 2^{n+2}\sum_{i=1}^{k} t_i \bmod 2^{2n+4}. \tag{3}$$

由于 $2^n \geqslant 2n+4$ 在 $n \geqslant 4$ 时成立, 故由 (3) 可得

$$2^{2n+4} \mid 2^{n+2}\sum_{i=1}^{k} t_i \Longrightarrow 2^{n+2} \mid \sum_{i=1}^{k} t_i.$$

由于 $t_1, \cdots, t_k$ 是正整数, 故由上式可得

$$\sum_{i=1}^{k} t_i \geqslant 2^{n+2}.$$

因此

$$S\big(2^{2^n}+1\big) = \sum_{i=1}^{k}(2^{n+2}t_i+1) \geqslant 2^{2n+4} + k. \tag{4}$$

而另一方面, 根据均值不等式可以得到

$$S\big(2^{2^n}+1\big) = \sum_{i=1}^{k} p_i \geqslant k\bigg(\prod_{i=1}^{k} p_i\bigg)^{\frac{1}{k}} = k(2^{2^n}+1)^{\frac{1}{k}}. \tag{5}$$

因此根据 (4)(5) 可以得到

$$S\big(2^{2^n}+1\big) \geqslant \max\Big(2^{2n+4}+k, k\cdot 2^{\frac{2^n}{k}}\Big).$$

下面只需证明: 对任意正整数 k, 都有

$$\max\left(2^{2n+4}+k, k\cdot 2^{\frac{2^n}{k}}\right) \geqslant 2^{2n+4}+\frac{2^n}{2n+4}. \tag{6}$$

若 $k \geqslant \dfrac{2^n}{2n+4}$ 或 $k=1$, 则 (6) 显然成立. 下面假设 $2 \leqslant k < \dfrac{2^n}{2n+4}$. 此时有

$$k\cdot 2^{\frac{2^n}{k}} \geqslant 2\cdot 2^{2n+4} \geqslant 2^{2n+4}+\frac{2^n}{2n+4},$$

故原命题得证. ■

扩展阅读

关于 Fermat 数的一个猜想是: 是否所有 Fermat 数都没有平方因子, 即不存在素数 p, 使得 $p^2 \mid 2^{2^n}+1$. 这个结果到目前为止都没有发现反例, 但也不知道如何证明.

Mersenne 数的素因子和估计

利用 Fermat 小定理, 2^p-1 的素因子必然具有 $2tp+1$ 的情形, 其中 t 为正整数. 接下来的估计方式和 Fermat 数的素因子估计方式类似.

证明 设 $p \geqslant 3$. 任取素数 $q \mid 2^p-1$, 由 Fermat 小定理可得 $q \mid 2^{q-1}-1$, 从而有 $q \mid 2^{(p,q-1)}-1$. 若 $(p, q-1)=1$ 则可得矛盾, 因此必须有 $p \mid q-1$. 因此, 2^p-1 的每一个素因子都必须形如 $2tp+1$, 其中 t 是正整数. 于是可假设 2^p-1 的素因子分解形如

$$2^p-1=\prod_{i=1}^{k} p_i, \quad \text{其中 } p_i=2t_ip+1, \quad i=1,\cdots,k.$$

下面对 $S(2^p-1)=\sum\limits_{i=1}^{k} p_i$ 进行估计. 一方面, 显然有

$$S(2^p-1)=\sum_{i=1}^{k} p_i=\sum_{i=1}^{k}(2t_ip+1) \geqslant k(2p+1). \tag{1}$$

另一方面, 根据均值不等式,

$$S(2^p-1) \geqslant k\left(\prod_{i=1}^{k} p_i\right)^{\frac{1}{k}} = k(2^p-1)^{\frac{1}{k}}. \tag{2}$$

取 $x = 1/k$, 则实数 $x \in (0, 1]$. 下面只需证明: 对任意 $x \in (0, 1]$, 都有

$$\max\left(\frac{2p+1}{x}, \frac{(2^p-1)^x}{x}\right) \geqslant \frac{(p-1)(2p+1)}{\log_2(2p+1)}. \tag{3}$$

使用反证法. 若 (3) 不成立, 则一定有

$$\frac{2p+1}{x} < \frac{(p-1)(2p+1)}{\log_2(2p+1)} \Longrightarrow x > \frac{\log_2(2p+1)}{p-1} := x_0.$$

接下来, 定义函数 $f(x) = (2^p-1)^x/x$, 则直接计算可得

$$f'(x) = \frac{(2^p-1)^x\big(\log(2^p-1)x - 1\big)}{x^2}. \tag{4}$$

当 $x \in (x_0, +\infty)$ 时, 一定有

$$\log(2^p-1)x - 1 > \frac{\log_2(2^p-1)}{\log_2 e} \cdot \frac{\log_2(2p+1)}{p-1} - 1 > \ln(2p+1) - 1 > 0,$$

因此根据 (4), $f(x)$ 在 $(x_0, +\infty)$ 上是严格单调递增的. 因此有

$$f(x) > f\left(\frac{\log_2(2p+1)}{p-1}\right) = (2^p-1)^{x_0} \cdot \frac{p-1}{\log_2(2p+1)} \geqslant \frac{(p-1)(2p+1)}{\log_2(2p+1)}, \tag{5}$$

其中 (5) 的最后一个不等号成立是因为

$$(2^p-1)^{x_0} \geqslant 2p+1 \Longleftrightarrow x_0 \log_2(2^p-1) \geqslant \log_2(2p+1) \Longleftrightarrow \log_2(2^p-1) \geqslant p-1.$$

但不等式 (5) 与 (3) 矛盾! 故原命题得证. ■

扩展阅读

在这个证明中有一个自然的想法, 能不能像在 Fermat 素数的情况一样, 在等式

$$2^p - 1 = \prod_{i=1}^{k}(2t_i p + 1)$$

的两端直接模 p^2, 从而得到 $\sum_{i=1}^{k} t_i$ 的估计. 等价地说, 我们想研究 $2^{p-1}-1$ 何时被 p^2 整除. 具有这种性质的素数被称为 Wieferich 素数, 它在费马大定理的早期研究中起到了重要作用. 目前已知的 Wieferich 素数只有 1093 和 3511, 也不知道是否有无穷多个 Wieferich 素数.