抽屉原理与数论问题

虚空若叶睦

2025 年 9 月 2 日

给定整数 $t \neq 0$. 设 $\{a_n\}, \{b_n\}$ 是严格单调递增的正整数列. 证明: 存在无穷多个素数 p, 使得存在正整数 i, j, 满足 $p \mid a_i b_j + t$.

这是一个非常典型的用抽屉原理解决的数论问题. 问题的关键在于当 $a_i b_j + t$ 的素因子有限时, 适当地做差来构造充分大的最大公约数.

证明 反证法. 设 $\{a_i b_j + t\}_{i,j=1}^{\infty}$ 只有有限多个素因子, 设这些素因子的集合为

$$P = \{p_1, p_2, ..., p_k\}.$$

对任意下标 i_1, i_2, j, 取正整数 $d = \gcd(a_{i_1} b_j + t, a_{i_2} b_j + t)$. 则

$$d \mid (a_{i_1} - a_{i_2}) b_j \Longrightarrow d | (a_{i_1} - a_{i_2}) \gcd(b_j, d) \Longrightarrow d | (a_{i_1} - a_{i_2}) \gcd(b_j, t).$$

于是当 $i_1 \neq i_2$ 时, 有不等式 $d \leqslant |a_{i_1} - a_{i_2}||t|$, 即

$$|a_{i_1} - a_{i_2}| \geqslant \frac{d}{|t|}, \quad \text{对任意 } i_1 \neq i_2. \tag{$*$}$$

记 $v_p(x)$ 为整数 x 中素数 p 的幂次. 取集合 $J_0 = \mathbb{N}$ 为正整数集. 由于当 $j \in J_0$ 时, $a_1 b_j + t$ 的素因子都在集合 $P = \{p_1, p_2, \cdots, p_k\}$ 中, 所以 $a_1 b_j + t$ 的最大的素因子次数发散, 即

$$\lim_{J_0 \ni j \to \infty} \max_{1 \leqslant l \leqslant k} v_{p_l}(a_1 b_j + t) = +\infty.$$

根据抽屉原理, 存在无穷集合 $J_1 \subset J_0$ 及 $1 \leqslant l_1 \leqslant k$ 使得

$$\lim_{J_1 \ni j \to \infty} v_{p_{l_1}}(a_1 b_j + t) = +\infty.$$

把上面的推导继续下去, 存在无穷集合 $J_2 \subset J_1$ 及 $1 \leqslant l_2 \leqslant k$ 使得

$$\lim_{J_2 \ni j \to \infty} v_{p_{l_2}}(a_2 b_j + t) = +\infty$$

$$\cdots$$

$$\lim_{J_k \ni j \to \infty} v_{p_{l_k}}(a_k b_j + t) = +\infty$$

$$\lim_{J_{k+1} \ni j \to \infty} v_{p_{l_{k+1}}}(a_{k+1} b_j + t) = +\infty.$$

这里, $J_{k+1} \subset J_k \subset \cdots J_1 \subset J_0 = \mathbb{N}$ 均为无穷集. 由于 $1 \leqslant l_1, \cdots, l_k, l_{k+1} \leqslant k$, 故由抽屉原理, 存在 $1 \leqslant m < n \leqslant k+1$ 使得 p_{l_m} 和 p_{l_n} 等于同一个素数 q. 此时

$$\lim_{J_{k+1} \ni j \to \infty} v_q(a_m b_j + t) = \lim_{J_{k+1} \ni j \to \infty} v_q(a_n b_j + t) = +\infty.$$

故对任意正整数 α, 存在 $j \in J_{k+1}$ 使得 $v_q(a_m b_j + t)$ 和 $v_q(a_n b_j + t)$ 均不小于 α, 从而

$$q^\alpha \mid \gcd(a_m b_j + t, a_n b_j + t). \tag{$**$}$$

由 $(*)(**)$ 知 $a_n - a_m \geqslant \dfrac{q^\alpha}{|t|}$. 但 α 可以充分大, 矛盾! 故原命题得证. ■

使用同样的方法, 不难证明:

> 给定整数 $t \in \mathbb{Z}$. 令 $\{a_n\}, \{b_n\}$ 是严格单调递增的正整数列. 证明: 存在无穷多个素数 p, 使得存在正整数 i, j, 满足 $p \mid a_i + b_j + t$.

证明留给读者作为练习. 还有一个类似但是证明不同的题目 (浙江 2023 预赛):

> 设 $f(x)$ 为整系数多项式, 令 $P = \{p \mid p\text{为素数且对某个}j \in \mathbb{N}, p \mid f(2023^j)\}$. 已知 P 为有限集, 求 $f(x)$.

> 设 $\{a_n\}_{n=1}^{\infty}$ 是严格单调递增的正整数列. 证明: 存在无穷多个素数 p, 使得存在正整数 n 满足 $p\,|\,a_n^2+1$.

这个问题虽然看起来和前面的 a_ib_j+1 问题非常相似, 但其证明需要用到更加深入的数论结果. 我们首先叙述有关本原素因子 (primitive prime divisor) 的 Zsigmondy 定理.

定理 1 (Zsigmondy, 1892) 设 $a>b>0$ 为互素整数, 并定义数列 $S_n=a^n-b^n$. 一个素数 p 称为 S_n 的本原素因子, 如果 $p\,|\,S_n$, 但对于所有 $1\leqslant k<n$, $p\nmid S_k$.

对所有正整数 n, S_n 几乎都会包含一个本原素因子, 但以下情况除外:

- $n=1$, 且 $a-b=1$. 此时 $a^1-b^1=1$ 无素因子.
- $n=2$, 且 $a+b$ 是 2 的幂. 此时 $a^2-b^2=(a-b)(a+b)$ 不包含任何新的奇素因子.
- $n=6$, $a=2$, $b=1$. 此时 $2^6-1^6=63$, 其中 3 出现在 2^2-1^2 中, 7 出现在 2^3-1^3 中.

接着, 我们来定义 Lucas 序列, 它定义了一类更广泛的形如 $\dfrac{\alpha^n-\beta^n}{\alpha-\beta}$ 的整数.

定义 1 给定互素的整数 P,Q. Lucas 序列 $\{U_n(P,Q)\}_{n=0}^{\infty}$ 可由下面的线性递推公式定义:

$$U_0=0,\qquad U_1=1,\qquad U_n=P\cdot U_{n-1}-Q\cdot U_{n-2}.$$

当判别式 $D=P^2-4Q\neq 0$ 时, U_n 可以表示为

$$U_n=\frac{\alpha^n-\beta^n}{\alpha-\beta},$$

其中 α,β 是特征方程 $x^2=Px-Q$ 的两个不等实根或共轭复根. 特别的, 当 $(P,Q)=(1,-1)$ 时, U_n 就是 Fibonacci 数列, 其中 $\alpha,\beta=\dfrac{1\pm\sqrt{5}}{2}$.

Lucas 序列是一个强整除序列, 这意味着对任何非负整数 m,n, 有

$$\gcd(U_m,U_n)=\left|U_{\gcd(m,n)}\right|.$$

可以证明, Lucas 序列满足如下的广义 Fermat 小定理:

定理 2 设 p 是奇素数, 且 p 不整除 Q. 令 $\left(\frac{D}{p}\right)$ 为 Legendre 符号, 则有

$$U_{p-\left(\frac{D}{p}\right)}\equiv 0\pmod{p}.$$

最后我们来叙述 Carmichael 定理, 它把 Zsigmondy 定理推广到了 Lucas 序列的情形.

定理 3 (Carmichael, 1913) 给定互素的整数 P, Q, 设 Lucas 序列 $U_n(P,Q)$ 的判别式 $\Delta = P^2 - 4Q > 0$. 对所有正整数 n, U_n 几乎都会包含一个本原素因子, 但需排除下列情况:

- $n = 1, 2, 6$.
- $n = 12$, $(P,Q) = (\pm 1, -1)$. 此时 $F_{12} = 144$.

Carmichael 定理实际上是 Zsigmondy 定理在二次数域 $\mathbb{Q}(\sqrt{D})$ 中的推广. 回到原题的证明.

证明 使用反证法, 假设 $\{a_n^2 + 1\}_{n=1}^{\infty}$ 的素因子集是有限的, 且素因子集为

$$P = \{p_1, p_2, \cdots, p_k\}.$$

对每个正整数 n, 都可以唯一地把 $a_n^2 + 1$ 分解为 $D_n \cdot b_n^2$ 的形式, 其中 D_n 是无平方因子数, b_n 是正整数. 于是 D_n 只能是 P 中若干个不同素数的乘积, 因此其取值是有限的. 根据抽屉原理, 存在无穷个正整数 n 使得 D_n 取同一个值. 不妨设无平方因子数 D 使得

$$a_n^2 + 1 = D \cdot b_n^2, \quad \text{对任意正整数 } n \text{ 成立.} \tag{1}$$

此时, 一定有 $D \neq 1$, 否则由 (1) 可得 $b_n > a_n$ 和 $1 = (b_n - a_n)(b_n + a_n) \geqslant 2$, 矛盾! 于是, (a_n, b_n) 一定是 Pell 方程 $x^2 - Dy^2 = -1$ 的非平凡解. 由于 (1) 已经有解, 故设 Pell 方程的基本解是 (X_1, Y_1), 其中 X_1, Y_1 是正整数, 则对每个正整数 n, 存在正奇数 $k(n)$ 使得

$$a_n + \sqrt{D} b_n = (X_1 + \sqrt{D} Y_1)^{k(n)}, \tag{2}$$

并且 $k(n)$ 是严格单调递增的. 由于 $a_n^2 + 1$ 的素因子集是有限的, 故由 (1) 可得 b_n 的素因子集是有限的. 令 $\alpha = X_1 + \sqrt{D} Y_1$, $\beta = X_1 - \sqrt{D} Y_1$, 并定义 Lucas 序列

$$U_k = \frac{\alpha^k - \beta^k}{\alpha - \beta}, \qquad k = 0, 1, 2, \cdots. \tag{3}$$

注意到由 Pell 方程 (2) 可得 $a_n - \sqrt{D} b_n = (X_1 - \sqrt{D} Y_1)^{k(n)}$, 从而

$$b_n = \frac{(X_1 + \sqrt{D} Y_1)^{k(n)} - (X_1 - \sqrt{D} Y_1)^{k(n)}}{2\sqrt{D}} = Y_1 U_{k(n)}.$$

由于 b_n 的素因子集是有限的, $U_{k(n)}$ 的素因子集也是有限的. 但根据 Carmichael 定理, 当 $k(n)$ 充分大时, $U_{k(n)}$ 中一定包含新的素因子, 矛盾! 故原命题得证. ∎