

裴蜀定理：若 $ax+by = z$ 则 $\gcd(a,b) | z$  再顺手证明一下裴蜀定理：设 $k = \gcd(a,b)$ 则 $k | a$   $k | b$ 根据整除的性质，有 $k | (ax+by)$  设 $s$ 为 $ax+by$ 的最小正数值 再设 $q = [a / s]$  $a$ 整除 $s$ 的值 $r = a \bmod s = a - q(ax+by) = a(1 - qx) + b(-qy)$  由此可见 $r$ 也为 $a,b$ 的线性组合 $(ax+by$ 称为 $a,b$ 的线性组合) 又因为 $s$ 为 $a,b$ 的线性组合的最小正数值 $0 < r < s$ 所以 $r$ 的值为0，即 $a \bmod s = r = 0$  $s | a$  同理可得 $s | b$ 则 $s | k$  又因为 $k | (ax+by)$  $s$ 为 $ax+by$ 的最小正数值，所以 $k | s$  因为 $s | k$  $k | s$ 所以 $s = k$  原命题得证。

[原链接](#)

From: <https://wiki.cvbbacm.com/> - CVBB ACM Team

Permanent link: [https://wiki.cvbbacm.com/doku.php?id=2020-2021:teams:farmer\\_john:%E8%A3%B4%E8%9C%80%E5%AE%9A%E7%90%86%E8%AF%81%E6%98%8E&rev=1599291748](https://wiki.cvbbacm.com/doku.php?id=2020-2021:teams:farmer_john:%E8%A3%B4%E8%9C%80%E5%AE%9A%E7%90%86%E8%AF%81%E6%98%8E&rev=1599291748)

Last update: 2020/09/05 15:42