Euclidean 延伸演算法的證明

對於任意兩個非負整數 a 和 b，我們可以進一步使用歐幾里得延伸演算法找到兩個整數 s 和 t，使得 $as+bt=\gcd(a,b)$。

- 證明過程：

歐幾里得延伸演算法在 q_i 和 r_i 的基礎上增加了兩組序列，記作 s_i 和 t_i，並初始化 $s_1=1$，$s_2=0$，$t_1=0$，$t_2=1$，
在歐幾里得演算法每步計算 $r_{i+1}=r_{i-1}-r_iq_i$ 之外，額外計算 $s_{i+1}=s_{i-1}-s_iq_i$ 和 $t_{i+1}=t_{i-1}-t_iq_i$，亦即：
$r_1=a,\ r_2=b,\ldots,\ r_{i+1}=r_{i-1}-r_iq_i\ \ (0\le r_{i+1}<|r_i|)$
$s_1=1,\ s_2=0,\ldots,\ s_{i+1}=s_{i-1}-s_iq_i$
$t_1=0,\ t_2=1,\ldots,\ t_{i+1}=t_{i-1}-t_iq_i$

演算法結束條件與歐幾里得演算法一致，也是 $r_{i+1}=0$，此時所得的 s_i 和 t_i 即滿足貝祖（Bézout）等式 $\gcd(a,b)=r_i=as_i+bt_i$。

在歐幾里得演算法正確性的基礎上，又對於 $a=r_1$ 和 $b=r_2$ 有貝祖等式 $as_i+bt_i=r_i$ 在 $i=1$ 或 2 時成立。
這一關係式可由下列遞推式推得其對所有 $i>1$ 皆成立：
$r_{i+1}=r_{i-1}-r_iq_i=(as_{i-1}+bt_{i-1})-(as_i+bt_i)q_i=(as_{i-1}-as_iq_i)+(bt_{i-1}-bt_iq_i)=as_{i+1}+bt_{i+1}$

因為數學歸納法求得其滿足貝祖等式，所以證明了歐幾里得延伸演算法的正確性。