**補題 1.** $a, b$ を自然数, $a$ を $b$ で割った商を $q$, あまりを $r$ とする．この時, $a$ と $b$ の最大公約数を $G$, $b$ と $r$ の最大公約数を $g$ とすると,

$$G = g$$

である．

*Proof.* $a = bq + r$ より, $bq + r$ は $g$ で割り切れるので, $a$ は $g$ で割り切れる．また, $G$ は公約数の中で最大なので,

$$g \leq G$$

同様に, $a - bq = r$ より, $a - bq$ は $G$ で割り切れるので, $r$ は $G$ で割り切れる．また, $g$ は公約数の中で最大なので,

$$G \leq g$$

したがって, $G = g$ である． □

**補題 2.** $a, b$ を自然数とする．また, $r_0 = a, r_1 = b$, $a$ を $b$ で割った商を $q_0$ とする．$r_i$ を $r_{i+1}$ で割った時の商を $q_i$, あまりを $r_{i+2}$ とするとき, ある自然数 $n$ で $r_n$ が $a$ と $b$ の最大公約数となることを示せ（数列 $r_i$ はこの $n$ で止まるものとする）．

*Proof.* 任意の $i$ に対して, $r_i$ は $r_{n-2}$ を $r_{n-1}$ で割ったあまりなので, 数列 $r_i$ は単調減少列である（つまり任意の $i$ に対して, $r_i > r_{i+1}$）．また, 補題 1 より, 任意の $i$ に対して $r_i$ と $r_{i+1}$ の最大公約数は $a$ と $b$ の最大公約数に等しい。したがって, $r_n$ が最大公約数となる $n$ が存在する。 □

**定理 1.** $a, b$ を互いに素な整数、つまり $a$ と $b$ の最大公約数が 1 とする．この時, $ax + by = 1$ となる整数の組 $(x, y)$ が存在することを示せ．

*Proof.* 補題 2 の数列 $r_i, q_i$ を今回の $a, b$ に対して考える．補題 2 より,

$$r_n - r_{n+1}q_n = 1$$

任意の $i$ に対して, $ax + by = r_i$ となる整数の組 $(x_i, y_i)$ が存在することを示す．$a$ を $b$ で割った商が $q_0$, あまりが $r_0$ なので,

$$a - bq_0 = r_2$$

よって, $x_2 = 1, y_2 = -q$ とすれば $r_2 = ax_2 + by_2$ である．ここで, 任意の $i$ に対して $r_i - r_{i+1}q_i = r_{i+2}$ だが, $r_i$ と $r_{i+1}$ も整数組 $(x_i, y_i), (x_{i+1}, y_{i+1})$ が存在するので, 帰納的に示される．したがって, 補題 2 で求めた $n$ について, $ax_n + by_n = 1$ となる． □