重要例題 126

***a* と *b* が互いに素　⇒　$ax+by=1$ を満たす整数 *x,y* が存在する。**

別解

証明 1

***ax+by* をその最小値 *p* で割ったときの余りの最大値が *p* より小さいことを利用**

$ax+by$ の最小の正の整数を p とすると，

$ax_0+by_0=p$ を満たす整数 x_0，y_0 が存在する。

ここで，任意の $ax+by$ を p で割った商を q，余りを r とすると，

$ax+by=pq+r$ より，

$ax+by=(ax_0+by_0)q+r \quad (0\le r\le p-1)$

$\therefore a(x-qx_0)+b(y-qy_0)=r \quad (0\le r\le p-1)$

よって，r は $ax+by$ の形で表される。

ここで，

r を正の整数とすると，$r\le p-1<p$ より，

p が $ax+by$ の最小の正の整数であることに反するので，$r=0$（背理法）

よって，

任意の $ax+by$ について，$ax+by=pq$ が成り立つ。

つまり，任意の $ax+by$ は，p の倍数である。

続いて，p の値を求める。

$ax+by$ について，

$x=1$，$y=0$ のとき

$ax+by=a$

これと $ax+by$ が p の倍数であることから，a は p の倍数である。

$x=0$，$y=1$ のとき

$ax+by=b$

これと $ax+by$ が p の倍数であることから，b は p の倍数である。

したがって，p は a と b の公約数である。

ところが，a と b は互いに素であるから，公約数は 1 しかない。

ゆえに，$p=1$

以上より，

a と b が互いに素であるとき，$ax+by=1$ を満たす整数 x，y が存在する。

証明 2

余りの個数が有限であることを利用

$ax+by=1$ を満たす整数 x， y が存在することを示せばよいから，

あらかじめ， x と y に制約をつけても構わない。

そこで，任意の ax を b で割った商を $-y$，余りを r $(0 \le r \le b-1)$ とし，

$1 \le x_1 \le x_2 \le b$ について，

$ax_1 = b(-y_1)+r_1$ ・・・①

$ax_2 = b(-y_2)+r_2$ ・・・②

のとき，

$r_1 = r_2$ とすると，

②－①より， $a(x_2-x_1)=b(-y_2+y_1)$

a と b は互いに素だから， $x_2-x_1=bk$， $-y_1+y_2=ak$

ところが， $1 \le x_1 \le x_2 \le b$ より， $0 \le x_2-x_1 \le b-1 < b$

よって， $k=0$，すなわち $x_1=x_2$

したがって， $r_1=r_2 \Rightarrow x_1=x_2$ が成り立つ。

この対偶は， $x_1 \ne x_2 \Rightarrow r_1 \ne r_2$ であり，

これは，$ax=b(-y)+r$ $(1 \le x \le b)$ において，x が異なれば r も異なることを示している。

一方，

x の要素の数は， $1 \le x \le b$ より b 個

r は ax を b で割った余りだから， $0 \le b \le b-1$ より，その要素の数も b 個

したがって， $r=1$ は必ず存在する。

ゆえに， $ax=b(-y)+1$，すなわち $ax+by=1$ を満たす整数 x， y が存在する。

となり， b の倍数にはなれない。