目標

$ax + by = c$ の特殊解を求める。

手順

まず、$gcd(a, b) \cdot v = c$ であるような整数 v が存在するものとする。
でなければ、$ax + by = c$ に整数解はない。

以下は整数解があるものとして進める。

まず、$v = 1$ つまり $ax + by = \mathrm{gcd}(a, b)$ として解く。

ax + by = gcd(a, b) の特殊解

便宜上、$\mathrm{gcd}(a, b) = c$ とする。

$a > b$ とする。a を b で割ることを考える。
商を q とし余りは r であるとすると、
$a = qb + r$ となる。

これを $ax + by = c$ に代入すると、$(qb + r)x + by = c$ となる。

$$
\begin{align}
(qb + r)x + by &= c \tag{1} \\
qbx + rx + by &= c \tag{2} \\
b(qx + y) + rx &= c \tag{3}
\end{align}
$$

と変形できる。

a, b は実際には問題上で与えられる値であることに注意されたい。
よって、ここで q, r は数値として求められる値である。

$qx + y = x_1, x = y_1$ とすると、
$bx_1 + ry_1 = c$ となり、これは $ax + by = c$ と同様にしてまた変形できる。
また、$b = a_1, r = b_1$ とおいて、式変形を一般化すると

$$ax + by = c \tag{4}$$
$$a_1x_1 + b_1y_1 = c \tag{5}$$
$$a_2x_2 + b_2y_2 = c \tag{6}$$
$$\vdots \tag{7}$$

となる。

この手順はユークリッドの互除法とまったく一致している。
そこで、ユークリッドの互除法に従って a, b の gcd を求めると、最終的にどこかで割り切れるが、その一手前の計算で出たあまりが gcd となる。

ここで、$\gcd(a, b) = c$ である。すなわちユークリッドの互除法における割り切れる一手前の計算が $s_nx_n + t_ny_n = c$ だったとすると、

$y_n = x_{n-1}$ であることから、$x_n = a_n(q_nx_{n-1} + y_{n-1})$ より y_{n-1} の値が分かる。これを繰り返すことで、最終的に x, y の値をひとつ求めることができた。

一般化

ここで、$c = \gcd(a, b) \cdot v$ であることから、
$ax + by = c$ であるとき、何らかの整数解 d, e があって、$ad + be = \gcd(a, b)$ であるとする。
このとき両辺を v 倍すると

$$adv + bev = \gcd(a, b) \cdot v \tag{8}$$
$$adv + bev = c \tag{9}$$

と変形できる。

よって、a, b を v で割ることで $c = \gcd(a, b)$ である場合に帰着できる。
よってこの問題を解けた。