Extended Euclidean Algorithm

Let a, b be coprime integers and $q_1, q_2, \dots, q_t$ be the quotients obtained from the divisions with remainder.

		q_1	q_2	...	q_{t-1}	q_t
0	1	P_1	P_2	...	P_{t-1}	a
1	0	Q_1	Q_2	..	Q_{t-1}	b

Initial values: $P_1 = q_1$, $Q_1 = 1$, $P_2 = q_2 \cdot P_1 + 1$, $Q_2 = q_2 \cdot Q_1$

and for $i \geq 3$: $P_i = q_i \cdot P_{i-1} + P_{i-2}$

$$Q_i = q_i \cdot Q_{i-1} + Q_{i-2}.$$

The final four values in the box satisfy:

$$a \cdot Q_{t-1} - b \cdot P_{t-1} = (-1)^t.$$

This alg. gives the solution $u = (-1)^t Q_{t-1}$ and $v = (-1)^{t+1} \cdot P_{t-1}$ to the eq. $au + b \cdot v = 1$.

Example: $a = 17$, $b = 5$

$17 = 3 \cdot 5 + 2$
$3 = 1 \cdot 2 + 1$
$1 = 1 \cdot 1 + 0$

0	1	3	4	(7)
1	0	1	1	(2)

$$7 \cdot b - 2 \cdot a = 1 = \gcd(17, 5)$$