Euclidean Algorithm

GONDRO

October 22, 2021

1 Proof

Suppose a and b are positive integers. By *Euclidean division lemma*,

$$(\forall a, b \in \mathbb{Z})(b \neq 0)(\exists b, r \in \mathbb{Z})(0 \leqslant r < |b|)(a = bq + r)$$

Thus,

$$(\exists b, r \in \mathbb{Z})(0 \leqslant r < |b|)(a = bq + r \wedge r = a - bq)$$

Let $h = \gcd(a, b)$ and $g = \gcd(b, r)$.

$$\begin{aligned} g &= \gcd(b, r) \\ \implies g &\mid b \wedge g \mid r \\ \implies (\exists m, n \in \mathbb{Z})&(gm = b \wedge gn = r) \\ \implies gqm &= bq \wedge gn = r \\ \implies gqm + gn &= bq + r \\ \implies g(qm + n) &= bq + r \\ \implies g &\mid bq + r \\ \implies g &\mid a \end{aligned}$$

$$g \mid a \wedge g \mid b \implies g \mid h \implies g \leqslant h$$

$$\begin{aligned} h &= \gcd(a, b) \\ \implies h &\mid a \wedge h \mid b \\ \implies (\exists m, n \in \mathbb{Z})&(hk = a \wedge hj = b) \\ \implies hk &= a \wedge hqj = qb \\ \implies hk - hqj &= a - qb \\ \implies h(k - qj) &= a - qb \\ \implies h &\mid a - qb \\ \implies h &\mid r \end{aligned}$$

$$h \mid b \wedge h \mid r \implies h \mid g \implies h \leqslant g$$

$$g \leqslant h \wedge h \leqslant g \implies h = g$$

$$\therefore a = bq + r \implies \gcd(a, b) = \gcd(b, r) \quad \square$$

2 Example Application

Compute $\gcd(2322, 654)$.

$$
\begin{array}{l|r}
\gcd(2322, 654) & \\
= \gcd(654, 360) & 2322 = 654 \cdot 3 + 360 \\
= \gcd(360, 294) & 654 = 360 \cdot 1 + 294 \\
= \gcd(294, 66) & 360 = 294 \cdot 1 + 66 \\
= \gcd(66, 30) & 294 = 66 \cdot 4 + 30 \\
= \gcd(30, 6) & 66 = 30 \cdot 2 + 6 \\
= \boxed{6} & 30 = 6 \cdot 5 + 0
\end{array}
$$

Solve for all integer solutions of $2322x + 654y = \gcd(2322, 654)$.
By rearranging the equations above,

$$
\begin{aligned}
360 &= 2322 - 654 \cdot 3 \\
294 &= 654 - 360 \cdot 1 \\
66 &= 360 - 294 \cdot 1 \\
30 &= 294 - 66 \cdot 4 \\
6 &= 66 - 30 \cdot 2
\end{aligned}
$$

$$
\begin{aligned}
\gcd(2322, 654) &= 6 \\
&= 66 - 30 \cdot 2 \\
&= 66 - (294 - 66 \cdot 4) \cdot 2 \\
&= 66 - 294 \cdot 2 + 66 \cdot 8 \\
&= 66 \cdot 9 - 294 \cdot 2 \\
&= (360 - 294 \cdot 1) \cdot 9 - 294 \cdot 2 \\
&= 360 \cdot 9 - 294 \cdot 9 - 294 \cdot 2 \\
&= 360 \cdot 9 - 294 \cdot 11 \\
&= 360 \cdot 9 - (654 - 360 \cdot 1) \cdot 11 \\
&= 360 \cdot 9 - 654 \cdot 11 + 360 \cdot 11 \\
&= 360 \cdot 20 - 654 \cdot 11 \\
&= (2322 - 654 \cdot 3) \cdot 20 - 654 \cdot 11 \\
&= 2322 \cdot 20 - 654 \cdot 60 - 654 \cdot 11 \\
&= 2322 \cdot 20 - 654 \cdot 71
\end{aligned}
$$

$$2322(20) + 654(-71) = \gcd(2322, 654)$$

Now solve for the homogeneous case: $2322x + 654y = 0$.
Notice that $2322 = 6 \cdot 387$ and $654 = 6 \cdot 109$.
Hence, the lowest common multiple of 2322 and 654 is $6 \cdot 109 \cdot 387$.
Thus, $2322(109t) + 654(-387t) = 0$

$$\therefore 2322(20 + 109t) + 654(-71 - 387t) = \gcd(2322, 654)$$

$$
\begin{cases}
x = \boxed{20 + 109t} \\
y = \boxed{-71 - 387t}
\end{cases}, \; t \in \mathbb{Z}
$$