Euclidean Algorithm

Dr.N.Gopika Rani,
Assistant Professor (SG),
Department of CSE

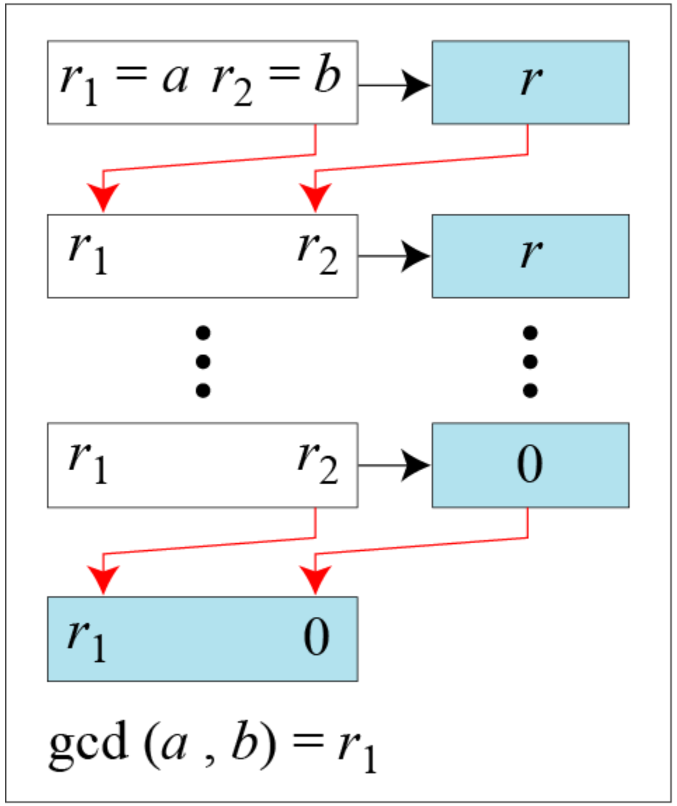
Greatest Common Divisors

- The greatest common divisor of two positive integers is the largest integer that can divide both integers.

- Euclidean Algorithm

  Fact 1: gcd (a, 0) = a
  Fact 2: gcd (a, b) = gcd (b, r), where r is the remainder of dividing a by b

Euclidean Algorithm



a. Process

$r_1 \leftarrow a; \qquad r_2 \leftarrow b;$ (Initialization)

while $(r_2 > 0)$

{

$\quad q \leftarrow r_1 / r_2;$

$\quad r \leftarrow r_1 - q \times r_2;$

$\quad r_1 \leftarrow r_2; \quad r_2 \leftarrow r;$

}

gcd $(a, b) \leftarrow r_1$

b. Algorithm

When gcd (a, b) = 1, we say that a and b are relatively prime.

Find the greatest common divisor of 2740 and 1760.

Solution

gcd (2740, 1760) = 20.

q	r_1	r_2	r
1	2740	1760	980
1	1760	980	780
1	980	780	200
3	780	200	180
1	200	180	20
9	180	20	0
	20	0	

- Find the greatest common divisor of 25 and 60.

Solution

gcd (25, 65) = 5

q	r_1	r_2	r
0	25	60	25
2	60	25	10
2	25	10	5
2	10	5	0
	5	0	

Multiplicative Inverse

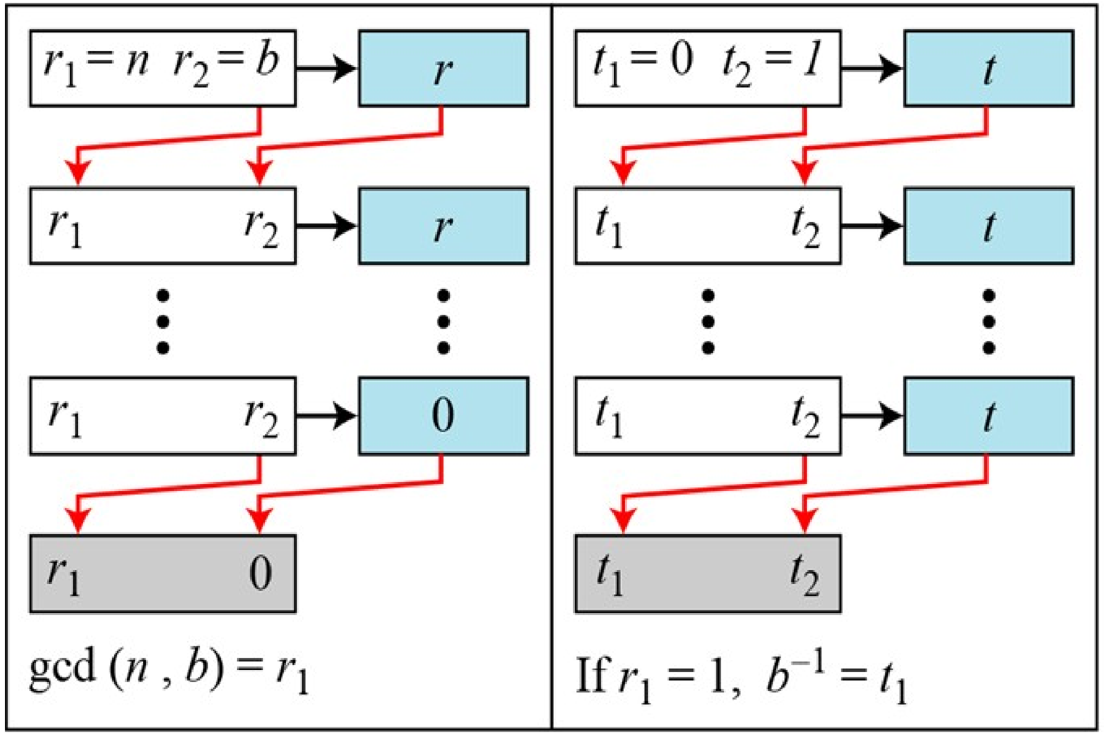
- In Z_n, two numbers a and b are the multiplicative inverse of each other if

$$a \times b \equiv 1 \pmod{n}$$

- In modular arithmetic, an integer may or may not have a multiplicative inverse.
- When it does, the product of the integer and its multiplicative inverse is congruent to 1 modulo n.

Extended Euclidean algorithm

- The extended Euclidean algorithm finds the multiplicative inverses of b in Z_n when n and b are given and gcd (n, b) = 1.
- The multiplicative inverse of b is the value of t after being mapped to Z_n.



a. Process

$r_1 \leftarrow$ n; $\quad r_2 \leftarrow b$;
$t_1 \leftarrow 0$; $\quad t_2 \leftarrow 1$;

while ($r_2 > 0$)
{
$q \leftarrow r_1 \,/\, r_2$;

$r \leftarrow r_1 - q \times r_2$;
$r_1 \leftarrow r_2$; $\quad r_2 \leftarrow r$;

$t \leftarrow t_1 - q \times t_2$;
$t_1 \leftarrow t_2$; $\quad t_2 \leftarrow t$;

}
if ($r_1 = 1$) then $b^{-1} \leftarrow t_1$

b. Algorithm

Find the multiplicative inverse of 11 in Z_{26}.

Solution

q	r_1	r_2	r	t_1	t_2	t
2	26	11	4	0	1	–2
2	11	4	3	1	–2	5
1	4	3	1	–2	5	–7
3	3	1	0	5	–7	26
	1	0		–7	26	

The gcd (26, 11) is 1; the inverse of 11 is –7 or 19.

Find the multiplicative inverse of 23 in Z_{100}.

Solution:

q	r_1	r_2	r	t_1	t_2	t
4	100	23	8	0	1	−4
2	23	8	7	1	−4	19
1	8	7	1	−4	9	−13
7	7	1	0	9	−13	100
	1	0		−13	100	

The gcd (100, 23) is 1; the inverse of 23 is −13 or 87.

Find the inverse of 12 in Z_{26}.

Solution:

q	r_1	r_2	r	t_1	t_2	t
2	26	12	2	0	1	–2
6	12	2	0	1	–2	13
	2	0		–2	13	

The gcd (26, 12) is 2; the inverse does not exist.