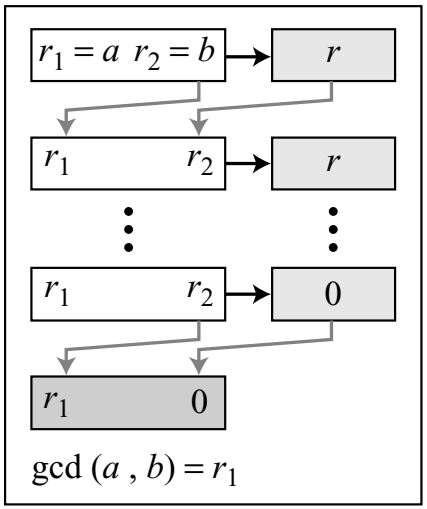
Euclid's Algorithm View



a. Process

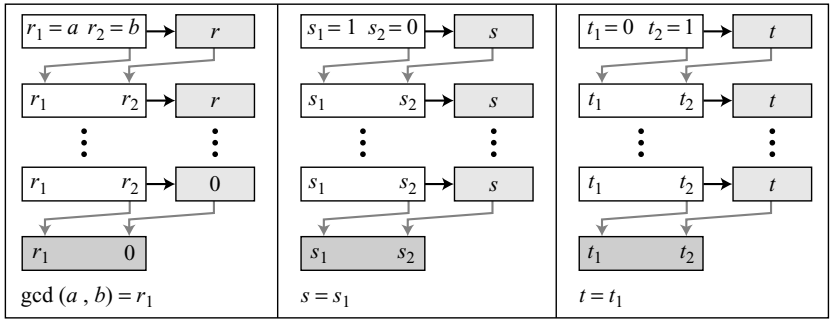
```
 r1 ← a; r2 ← b;  (Initialization)
while (r2 > 0)
 {
  q ← r1 / r2;
  r ← r1 – q × r2;
  r1 ← r2; r2 ← r;
 }

  gcd (a, b) ← r1
```

b. Algorithm

Extended Euclidean algorithm

$$d = gcd(a, b) = s \times a + t \times b$$



a. Process

```
 r1 ← a; r2 ← b;
 s1 ← 1; s2 ← 0;   (Initialization)
 t1 ← 0; t2 ← 1;
while (r2 > 0)
 {
  q ← r1 / r2;
   r  ← r1 – q × r2;
   r1 ← r2;  r2 ← r;      (Updating r's)
   s  ← s1 – q × s2;
   s1 ← s2;  s2 ← s;      (Updating s's)
   t  ← t1 – q × t2;
   t1 ← t2;  t2 ← t;      (Updating t's)
 }
  gcd (a , b) ← r1;   s ← s1;   t ← t1
```

b. Algorithm

q	r_1	r_2	r	s_1	s_2	s	t_1	t_2	t
5	161	28	21	1	0	1	0	1	−5
1	28	21	7	0	1	−1	1	−5	6
3	21	7	0	1	−1	4	−5	6	−23
	7	0		**−1**	4		**6**	−23	

We get gcd (161, 28) = 7, $s = -1$ and $t = 6$. The answers can be tested because we have

$$(-1) \times 161 + 6 \times 28 = 7$$