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”

Eucliad (a,b)

Step1: A<- a; B<-b;

Step2: if B=0; return A=GCD(a,b)

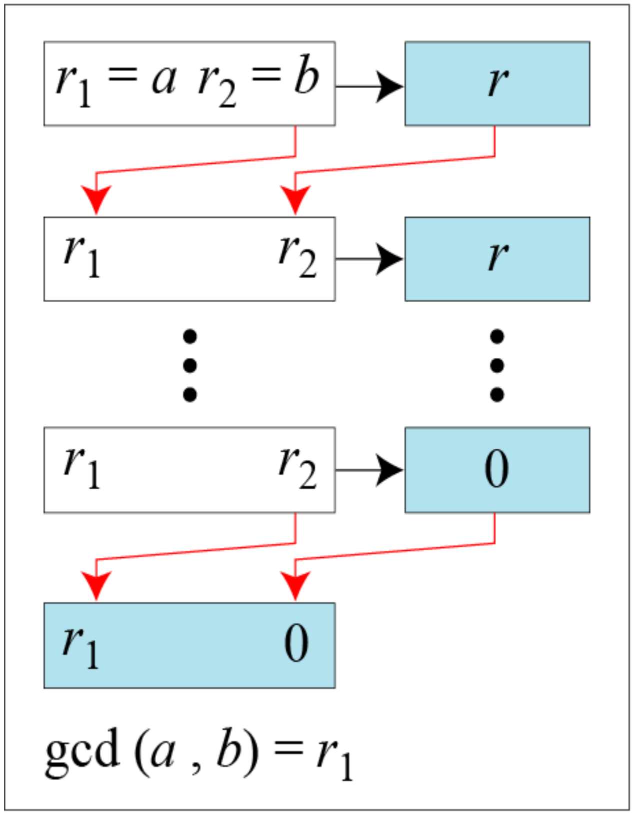
Step3: R=A mod B

Step 4: A<-B;

Step5: B<-R

goto Step2

Euclidean Algorithm Contd.



a. Process

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

while ($r_2 > 0$)

{

$q \leftarrow r_1 / r_2;$

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

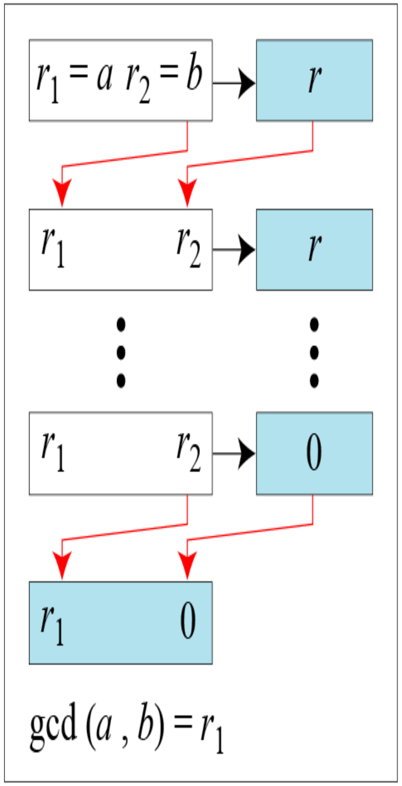
$r_1 \leftarrow r_2; \quad r_2 \leftarrow r;$

}

$\gcd(a, b) \leftarrow r_1$

b. Algorithm

Find the Greatest Common Divisor of 2740 and 1760



a. Process

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

while $(r_2 > 0)$

{

$q \leftarrow r_1 / r_2;$

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

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

}

$\text{gcd}(a, b) \leftarrow r_1$

b. Algorithm

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	

We have gcd (2740, 1760) = 20.

Find the Greatest Common Divisor of 25 and 60

Find the greatest common divisor of 25 and 60.

Solution

We have 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	

Extended Euclidean Algorithm

Given two integers *a* and *b*, we often need to find other two integers, *s* and *t*, such that

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

The extended Euclidean algorithm can calculate the gcd (*a*, *b*) and at the same time calculate the value of *s* and *t*.

Extended Euclidean Algorithm Contd.

$r_1 \leftarrow a; \quad r_2 \leftarrow b;$
$s_1 \leftarrow 1; \quad s_2 \leftarrow 0;$
$t_1 \leftarrow 0; \quad t_2 \leftarrow 1;$ (Initialization)

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

$r \leftarrow r_1 - q \times r_2;$
$r_1 \leftarrow r_2; \; r_2 \leftarrow r;$ (Updating r's)

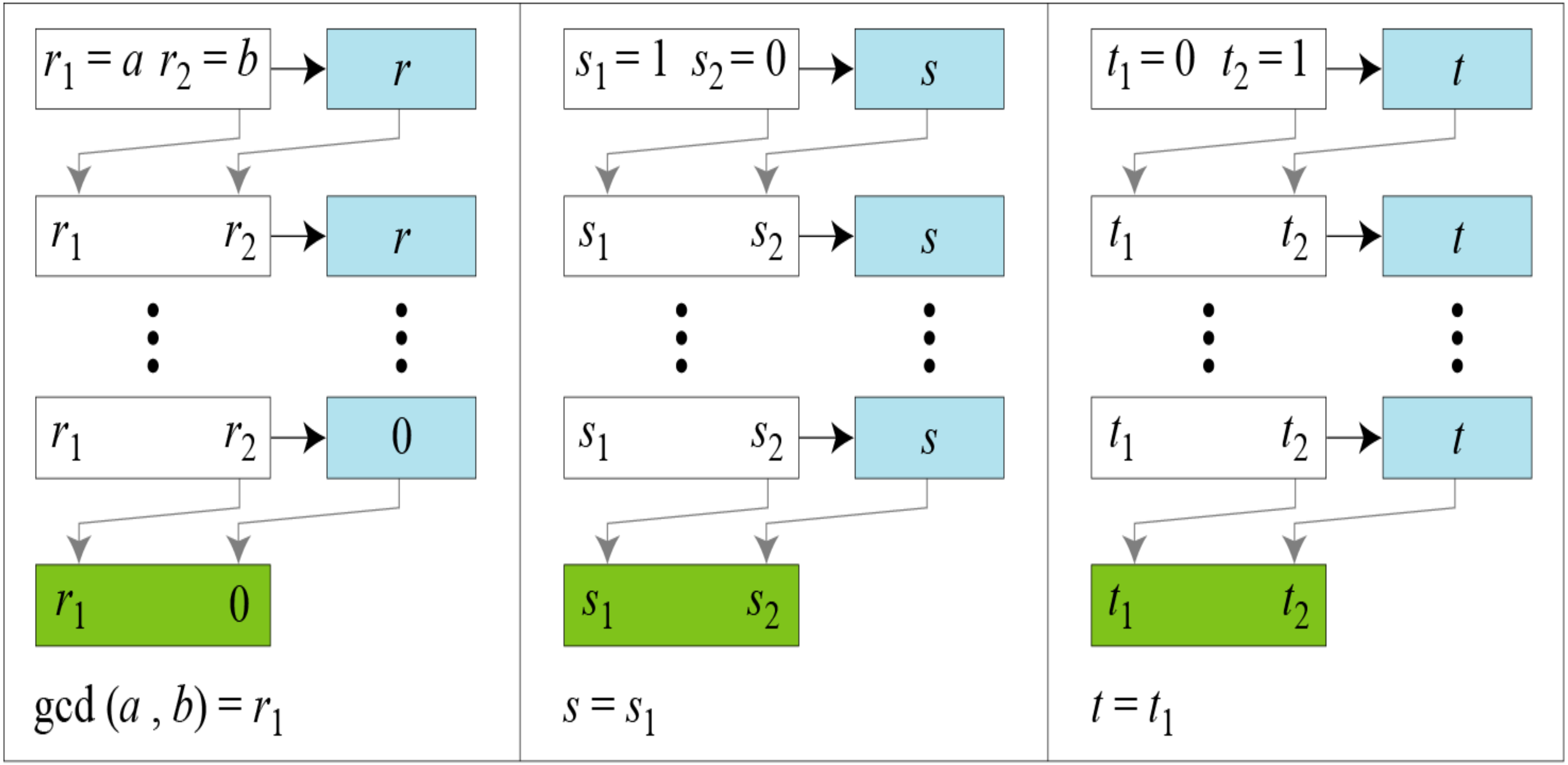
$s \leftarrow s_1 - q \times s_2;$
$s_1 \leftarrow s_2; \; s_2 \leftarrow s;$ (Updating s's)

$t \leftarrow t_1 - q \times t_2;$
$t_1 \leftarrow t_2; \; t_2 \leftarrow$ t; (Updating t's)
}

gcd $(a, b) \leftarrow r_1; \; s \leftarrow s_1; \; t \leftarrow t_1$

b. Algorithm

Extended Euclidean Algorithm Contd.



a. Process

Given $a = 161$ and $b = 28$, find gcd (a, b) and the values of s and t

```
r1 ← a;        r2 ← b;         (Initialization)
s1 ← 1;        s2 ← 0;
t1 ← 0;        t2 ← 1;
while (r2 > 0)
 {
   q ← r1 / r2;
    r ← r1 − q × r2 ;             (Updating r's)
    r1 ← r2 ;  r2 ← r ;
    s ← s1 − q × s2 ;             (Updating s's)
    s1 ← s2 ;  s2 ← s ;
    t ← t1 − q × t2;              (Updating t's)
    t1 ← t2 ;  t2 ← t;
 }
   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 $t = 6$

Given a = 17 and b = 0, find gcd (a, b) and the values of s and t

Solution

We get gcd (17, 0) = 17, s = 1, and t = 0.

q	r_1	r_2	r	s_1	s_2	s	t_1	t_2	t
	17	0		1	0		0	1	

Given a=0 and b=45, find gcd(a, b) and the values of s and t

Solution

We get gcd (0, 45) = 45, s = 0, and t = 1.

q	r_1	r_2	r	s_1	s_2	s	t_1	t_2	t
0	0	45	0	1	0	1	0	1	0
	45	0		0	1		**1**	0	