Unit I

Modular Arithmetic : Multiplicative inverse, extended euclidean algo Refer : Chapter 2 , Fourozan

Objectives

- *To review integer arithmetic, concentrating on divisibility and finding the greatest common divisor using the Euclidean algorithm*
- *To understand how the extended Euclidean algorithm can be used to solve linear Diophantine equations, to solve linear congruent equations, and to find the multiplicative inverses*
- *To emphasize the importance of modular arithmetic and the modulo operator, because they are extensively used in cryptography*
- *To emphasize and review matrices and operations on residue matrices that are extensively used in cryptography*
- *To solve a set of congruent equations using residue matrices*

2.1.3 Integer Division

In integer arithmetic, if we divide a by n, we can get q And r . The relationship between these four integers can be shown as

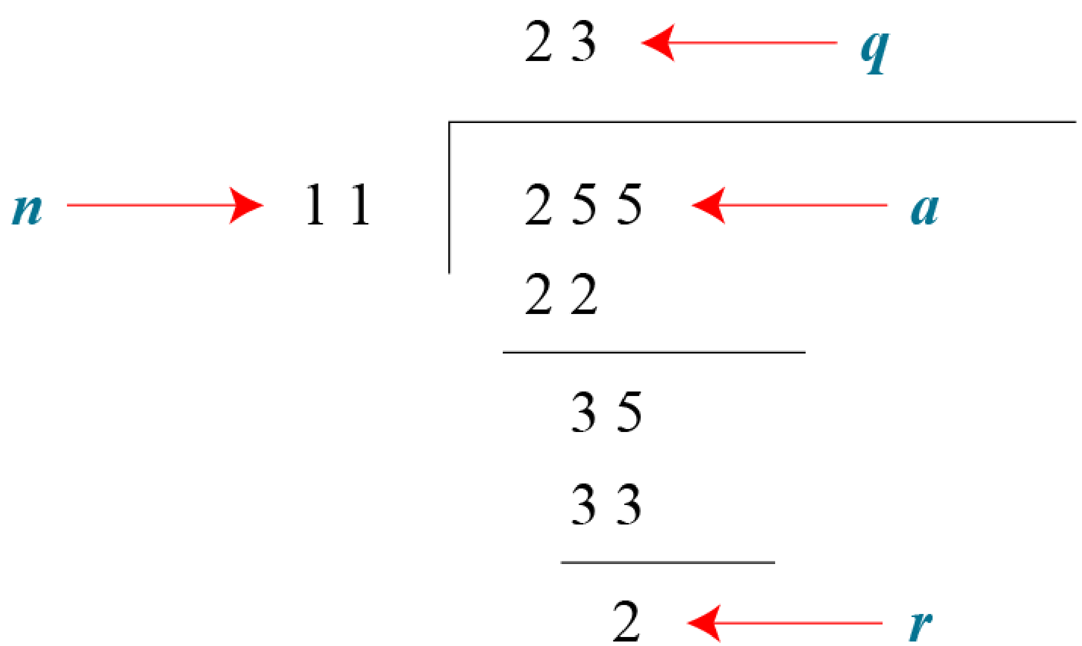
$$a = q \times n + r$$

2.1.3 Continued

Example 2.2

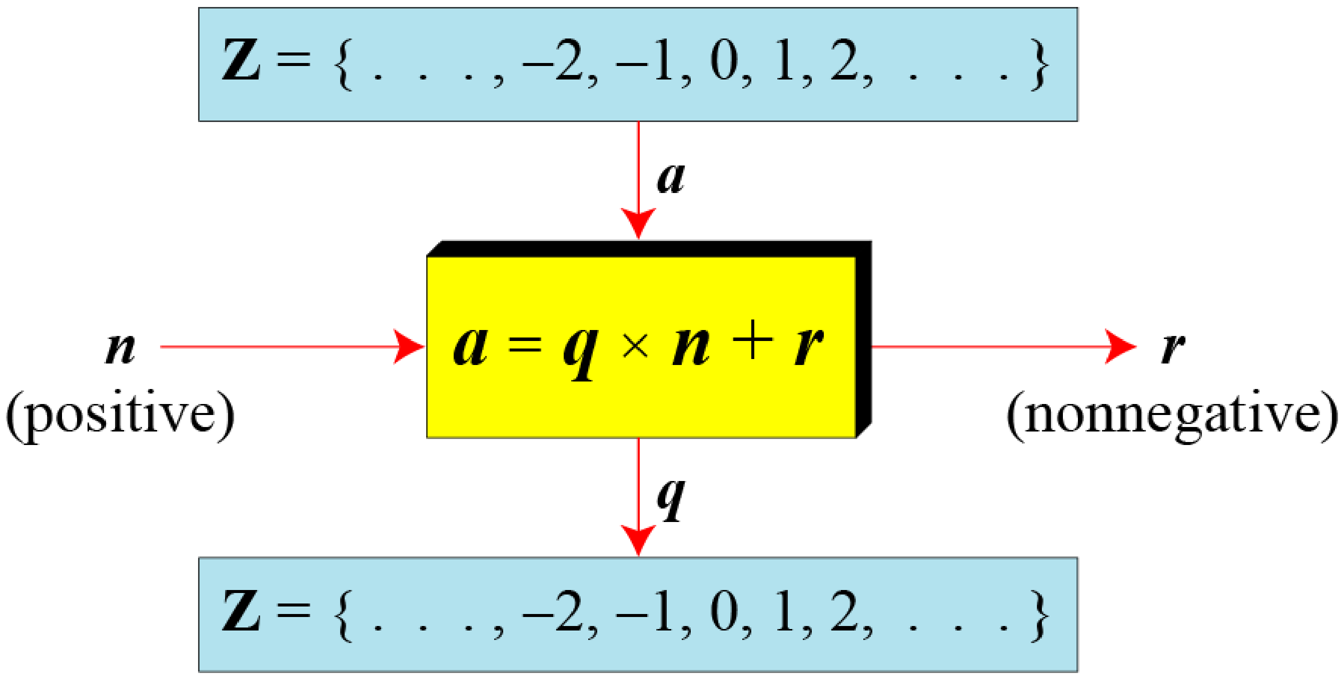
Assume that a = 255 and n = 11. We can find q = 23 and R = 2 using the division algorithm.

Figure 2.3 Example 2.2, finding the quotient and the remainder



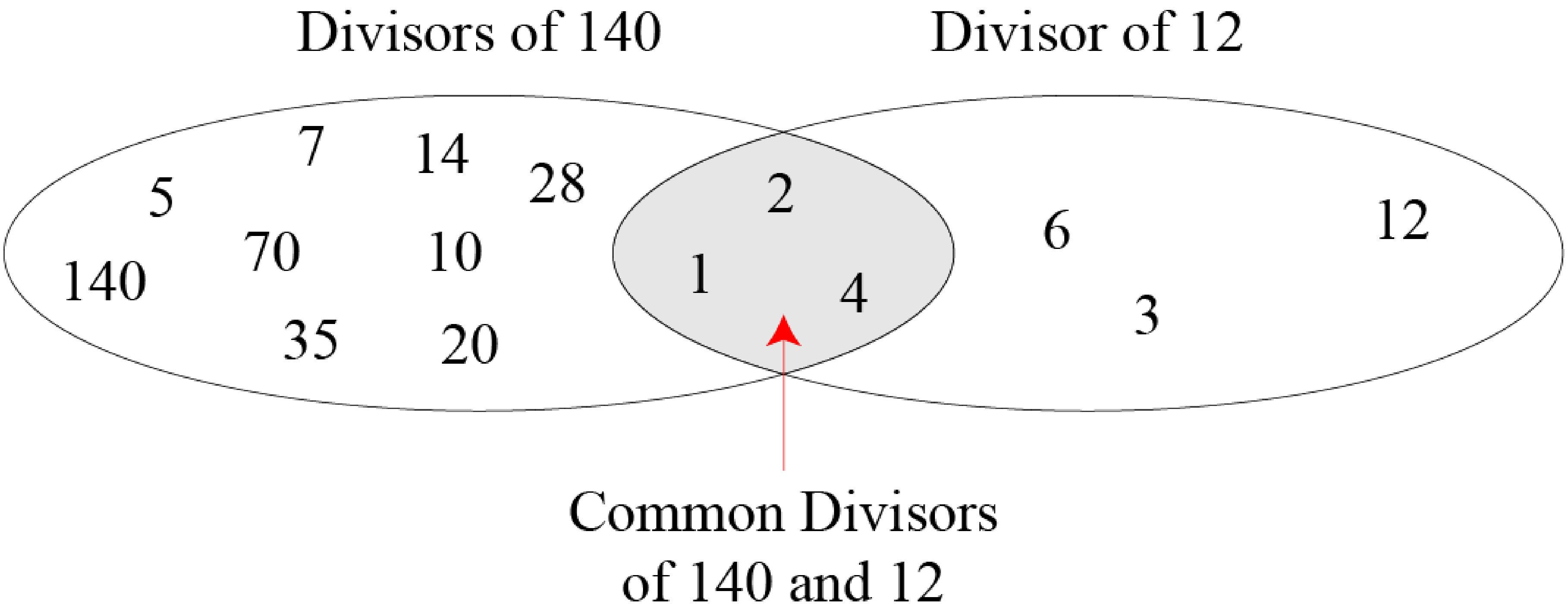
2.1.3 Continued

Figure 2.4 Division algorithm for integers



2.1.4 Continued

Figure 2.6 Common divisors of two integers



2.1.4 Continued

Note *Greatest Common Divisor*

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

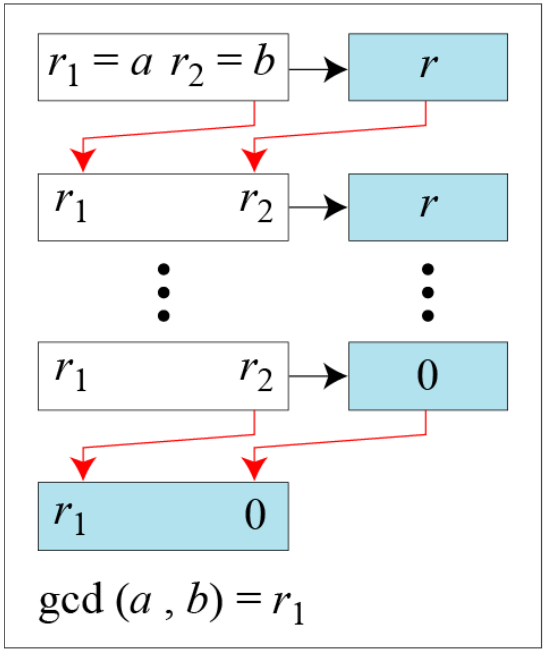
Note *Euclidean Algorithm*

Fact 1: gcd (a, 0) = a

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

2.1.4 Continued

Figure 2.7 Euclidean Algorithm



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

Note

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

2.1.4 Continued

Note

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

2.1.4 Continued

Example 2.7

Find the greatest common divisor of 2740 and 1760.

Solution

We have 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	

Example 2.8

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	

2.1.4 Continued

Extended Euclidean Algorithm

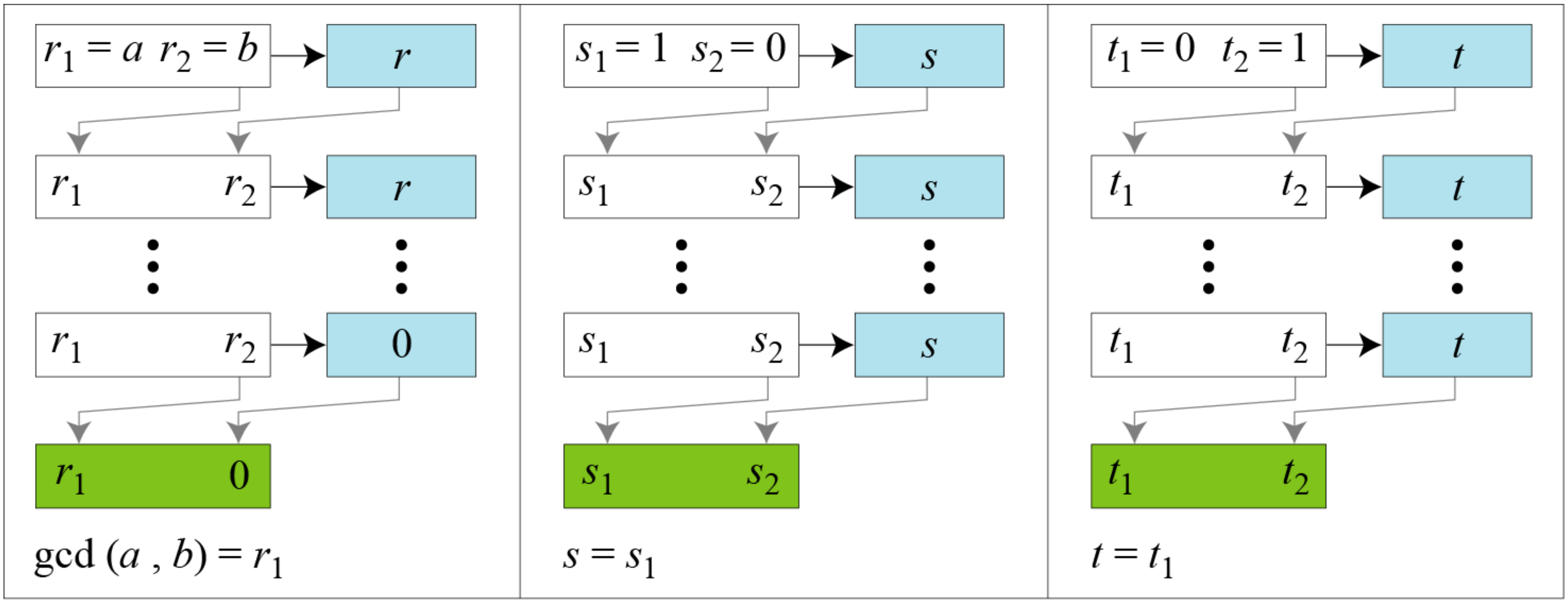
Given two integers a *and* b, *we often need to find other two integers*, s *and* t, *such that*

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

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

2.1.4 Continued

Figure 2.8.a Extended Euclidean algorithm, part a



a. Process

2.1.4 Continued

Figure 2.8.b Extended Euclidean algorithm, part b

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

while $(r_2 > 0)$

{

$q \leftarrow r_1 / r_2;$

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

2.1.4 Continued

Example 2.9

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

Solution

We get gcd (161, 28) = 7, s = *−1 and* t = *6.*

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	

2.1.4 Continued

Example 2.10

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**	

2.1.4 Continued

Example 2.11

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	

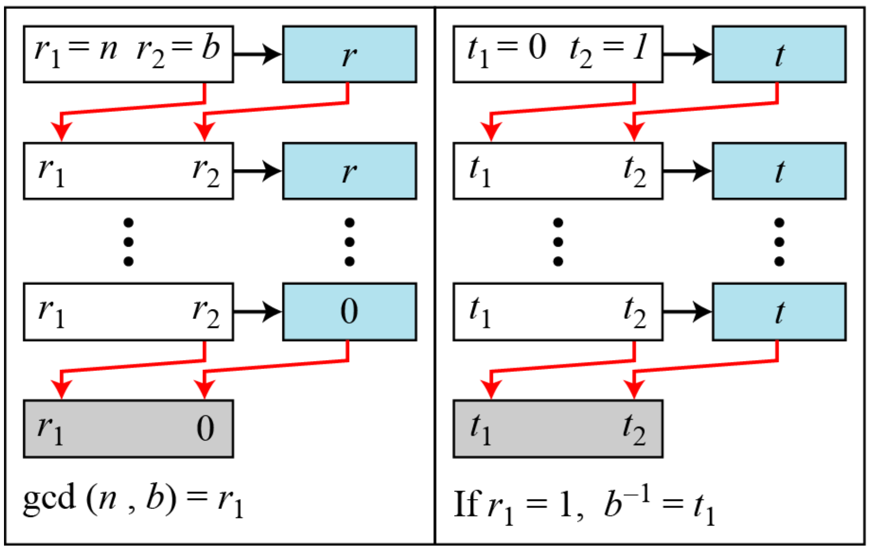
2.2.5 Continued

Note

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.

2.2.5 Continued

Figure 2.15 Using extended Euclidean algorithm to find multiplicative inverse



a. Process

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

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

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

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

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

b. Algorithm

2.2.5 Continued

Example 2.25

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.

2.2.5 Continued

Example 2.26

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.

2.2.5 Continued

Example 2.27

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.