Mathematics of Cryptography

Note

Greatest Common Divisor

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

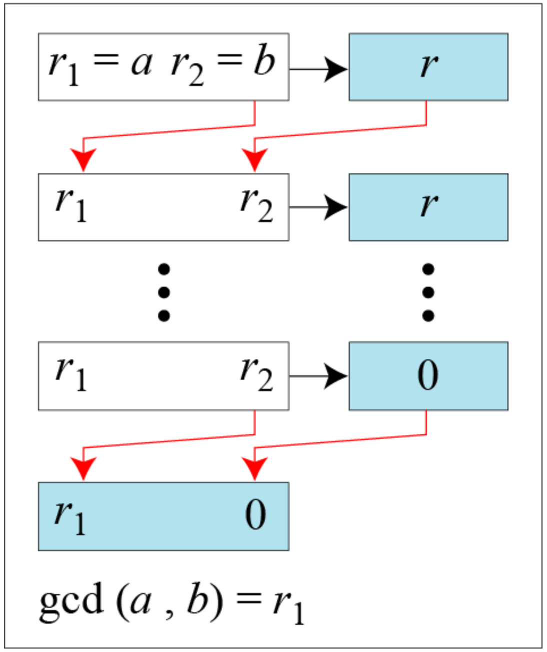
Note

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	

2.1.4 Continued

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.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)

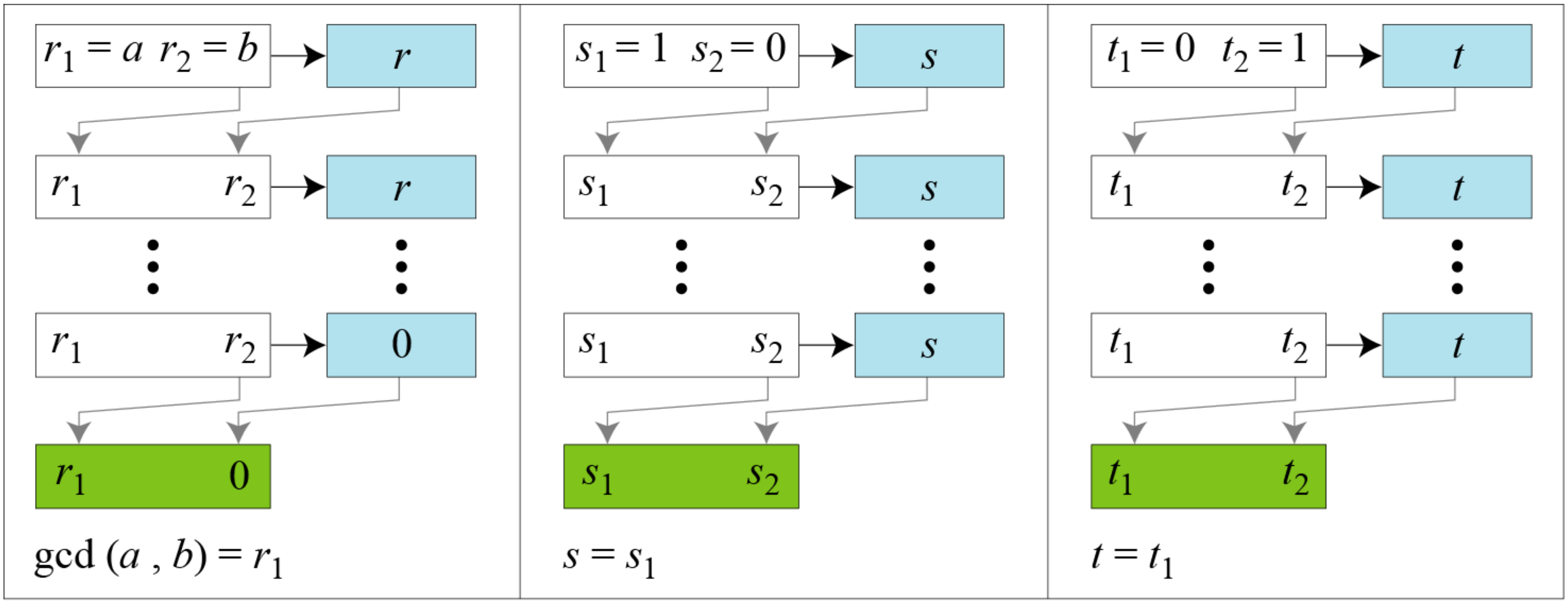
}

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

b. Algorithm

2.1.4 Continued

Figure 2.8.a *Extended Euclidean algorithm, part a*



a. Process

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	

2.1.4 Continued

Example 2.14

Find the result of the following operations:

a. 27 mod 5 **b.** 36 mod 12

c. −18 mod 14 **d.** −7 mod 10

Solution

a. Dividing 27 by 5 results in $r = 2$

b. Dividing 36 by 12 results in $r = 0$.

c. Dividing −18 by 14 results in $r = -4$. After adding the modulus $r = 10$

d. Dividing −7 by 10 results in $r = -7$. After adding the modulus to −7, $r = 3$.

2.2.3 Congruence

To show that two integers are congruent, we use the congruence operator (≡). For example, we write:

$$2 \equiv 12 \pmod{10} \qquad 13 \equiv 23 \pmod{10}$$
$$3 \equiv 8 \pmod{5} \qquad 8 \equiv 13 \pmod{5}$$

2.2.4 Continued

Properties

First Property:	$(a + b) \bmod n = [(a \bmod n) + (b \bmod n)] \bmod n$
Second Property:	$(a - b) \bmod n = [(a \bmod n) - (b \bmod n)] \bmod n$
Third Property:	$(a \times b) \bmod n = [(a \bmod n) \times (b \bmod n)] \bmod n$

2.2.5 *Continue*

Multiplicative Inverse

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

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

Note

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.

Example 2.22

Find the multiplicative inverse of 8 in Z_{10}.

Solution

There is no multiplicative inverse because gcd (10, 8) = 2 ≠ 1. In other words, we cannot find any number between 0 and 9 such that when multiplied by 8, the result is congruent to 1.

Example 2.23

Find all multiplicative inverses in Z_{10}.

Solution

There are only three pairs: (1, 1), (3, 7) and (9, 9). The numbers 0, 2, 4, 5, 6, and 8 do not have a multiplicative inverse.

2.2.5 *Continued*

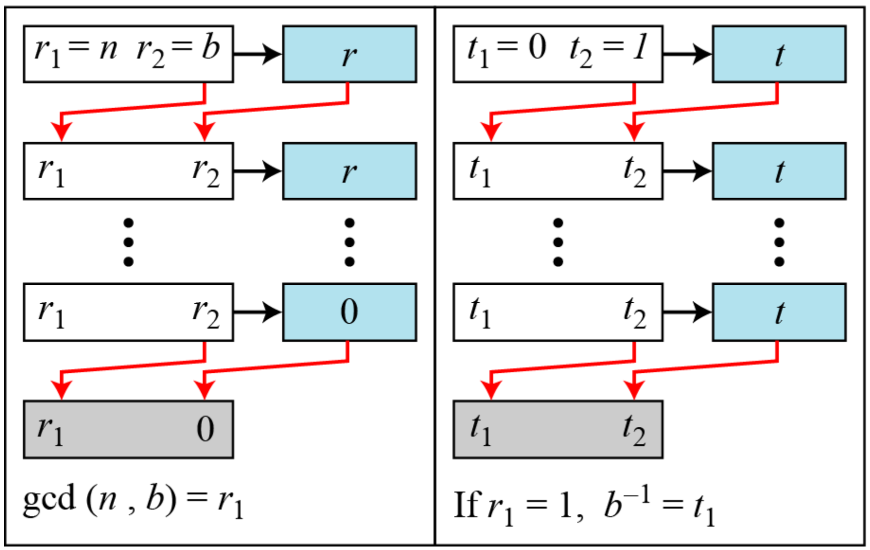
Example 2.24

Find all multiplicative inverse pairs in Z_{11}.

Solution

We have seven pairs: (1, 1), (2, 6), (3, 4), (5, 9), (7, 8), (9, 5), and (10, 10).

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.

9.1.4 Euler's Phi-Function

Euler's phi-function, $\phi(n)$, which is sometimes called the Euler's totient function plays a very important role in cryptography.

1. $\phi(1) = 0$.
2. $\phi(p) = p - 1$ if p is a prime.
3. $\phi(m \times n) = \phi(m) \times \phi(n)$ if m and n are relatively prime.
4. $\phi(p^e) = p^e - p^{e-1}$ if p is a prime.

9.1.4 Continued

We can combine the above four rules to find the value of $\phi(n)$. For example, if n can be factored as

$$n = p_1^{e_1} \times p_2^{e_2} \times \ldots \times p_k^{e_k}$$

then we combine the third and the fourth rule to find

$$\boxed{\phi(n) = (p_1^{e_1} - p_1^{e_1-1}) \times (p_2^{e_2} - p_2^{e_2-1}) \times \cdots \times (p_k^{e_k} - p_k^{e_k-1})}$$

Note

The difficulty of finding $\phi(n)$ depends on the difficulty of finding the factorization of n.

Example 9.7

What is the value of $\phi(13)$?

Solution

Because 13 is a prime, $\phi(13) = (13 - 1) = 12$.

Example 9.8

What is the value of $\phi(10)$?

Solution

We can use the third rule: $\phi(10) = \phi(2) \times \phi(5) = 1 \times 4 = 4$, because 2 and 5 are primes.

Example 9.9

What is the value of $\phi(240)$?

Solution

We can write $240 = 2^4 \times 3^1 \times 5^1$. Then

$$\phi(240) = (2^4 - 2^3) \times (3^1 - 3^0) \times (5^1 - 5^0) = 64$$

Example 9.10

Can we say that $\phi(49) = \phi(7) \times \phi(7) = 6 \times 6 = 36$?

Solution

No. The third rule applies when m and n are relatively prime. Here $49 = 7^2$. We need to use the fourth rule: $\phi(49) = 7^2 - 7^1 = 42$.